NATIONAL DIGITAL ID POLICY 2025

Draft Version 7.2

Table of Content

STATEMENT BY THE MINISTER FOR ICT

As Minister for Information and Communications Technology, I am proud to champion the Digital ID Policy 2025, a transformative step toward a secure and inclusive digital future for Papua New Guinea. This policy establishes SevisPass as a trusted digital identity, enabling seamless access to government, financial, health, and education services for all citizens.

The Ministry, through the Department of Information and Communications Technology, is committed to delivering a robust and inclusive system that prioritizes security, interoperability, and accessibility, particularly for rural and marginalized communities. Our partnerships with the National Information and Communication Technology Authority, Bank of Papua New Guinea, and international allies, including the International Telecommunication Union, reinforce our vision of regional leadership in digital transformation, as affirmed by the Lagatoi Declaration.

I extend my gratitude to Secretary Steven Matainaho and our stakeholders for their dedication. Together, we will ensure a trusted digital ecosystem that empowers every Papua New Guinean.

Sincerely,

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

1. Executive Summary

Papua New Guinea (PNG) is embarking on a transformative journey to establish a robust and inclusive **Digital Identity and Trust Framework**, a foundational step towards realizing its broader vision for **Digital Public Infrastructure (DPI)**. At the heart of this initiative lies **SevisPass**, a digital ID credential designed to serve as the cornerstone for secure, inclusive, and interoperable access to both public and private services.

This policy framework supports multiple strategic objectives: empowering individuals with secure and portable identities; facilitating trusted digital interactions between people, institutions, and systems; improving the delivery and targeting of social protection and financial services; and enabling compliance with key regulatory obligations such as Know Your Customer (KYC), Anti-Money Laundering (AML), and Financial Action Task Force (FATF) standards.

SevisPass forms part of the broader Trust Framework that includes the **SevisWallet** for verifiable credentials, the **SevisAdminPortal** for managing credentials and trust registries, and **SevisDEx**, PNG's government and business data exchange platform. Together, these components enable seamless identity verification, cross-sector authentication, and streamlined access to essential services across sectors such as health, education, and finance. SevisPass will underpin PNG's emerging Trust Framework, enabling verifiable, consent-based digital interactions across the economy. As a core component of the national DPI, it will build trust by ensuring that digital identities are secure, portable, and widely accepted.

The policy positions SevisPass as a catalyst for **digital inclusion, service innovation, and economic participation**, opening up new opportunities for individuals and institutions alike. By establishing the foundational elements of a **trustworthy, inclusive, and interoperable digital ID ecosystem**, it aims to accelerate PNG's digital transformation, enhance state capability, and deliver secure, user-centric digital services across the public and private sectors.

The design and implementation of SevisPass will be grounded in guiding principles that reflect global best practices and PNG's commitment to a rights-based and inclusive digital future. These include user-centricity, accessibility, privacy, and non-discrimination—ensuring that individuals, including those in rural and marginalized communities, can benefit from secure and seamless digital interactions. SevisPass is not merely a technical solution; it is conceived as a **trusted public infrastructure** that will enable service innovation, strengthen democratic governance, and foster digital empowerment.

A **federated and inclusive model** will govern both enrolment and authentication, with trusted public and private actors engaged to extend outreach and accessibility across all regions. Security and privacy will be embedded by design, with robust data protection safeguards, consent-based data sharing, and principles of data minimization. The framework's **public good orientation** will be reflected in the use of open APIs, transparency measures, and equitable access to foundational digital ID services. These principles will guide the system across its full lifecycle—from credential issuance to authentication and integration into PNG's broader digital ecosystem.

The Trust Framework will be built on an **open**, **modular and interoperable architecture**, aligned with international best practices such as ITU's GovStack. This ensures flexibility and scalability while promoting the reuse of infrastructure components across use cases and sectors. Each building block—whether for identity, credentials, data exchange, or consent—will operate with clearly defined standards, APIs, and roles, enabling them to work seamlessly together while maintaining independence. This architecture supports innovation, avoids duplication, and facilitates the rollout of

additional DPI components and sectoral platforms, further accelerating digital transformation across PNG.

The **governance of SevisPass** will be anchored in a robust, multi-stakeholder framework to ensure public trust, institutional accountability, and long-term sustainability. It will adopt a federated operational model with centralized policy, standards, and oversight, while enabling decentralized service delivery. Governance will be structured around clear institutional mandates and coordinated roles among the lead authority, implementing partners, and regulatory bodies.

A dedicated entity—either existing or newly established—will oversee SevisPass operations, set technical and data standards, ensure compliance, and coordinate ecosystem-wide implementation. The governance structure will include representation from government, the private sector, civil society, and technical experts to promote transparency, inclusivity, and participatory decision-making. User-centricity will be reinforced through grievance redressal mechanisms, audit trails, and strong data rights. A multi-channel grievance redress system—spanning digital, assisted, and in-person modes—will ensure accessibility, particularly for vulnerable populations. Provisions for consent management, data correction, and audit visibility will safeguard user autonomy and privacy.

To sustain the system and support innovation, targeted investments will be made in **capacity building**, enabling government institutions, service providers, and local technology partners to adopt and integrate SevisPass. Governance mechanisms will also include provisions for **future-proofing**, drawing on global innovations to ensure that the ecosystem remains current, scalable, and resilient to technological change.

The **SevisPass lifecycle** will be designed to ensure universal coverage, secure credential management, and lifelong access to digital services. It will cover the full spectrum of processes: registration, identity verification, credential issuance, authentication, updates and deactivation, and periodic revalidation. Each stage will follow standardized workflows and security protocols, with a strong emphasis on privacy and user protection.

Implementation will be **phased and federated**, starting with high-priority use cases such as eKYC for financial services and digital onboarding for government schemes. A network of trusted registration partners—including public institutions and private actors—will be mobilized to ensure nationwide outreach. Multiple authentication options (biometrics, OTPs, QR codes, PINs) will cater to varying digital literacy and device access levels. Key technology platforms such as SevisAdminPortal and SevisDEx will support real-time verification, system integrations, and scalable operations. Adoption will be driven through ecosystem-wide onboarding, developer toolkits, and training programs.

A **proactive risk management strategy** will be embedded within the policy to ensure resilience, trust, and inclusivity. Risks will be categorized across institutional, legal, technological, operational, and user domains. The framework will include safeguards against identity fraud, cybersecurity threats, digital exclusion, governance failures, and vendor dependency. Risk mitigation will be guided by adaptive policies and a layered approach to security, operations, and oversight.

A strong **Monitoring and Evaluation (M&E)** framework will be built into the implementation roadmap to ensure continuous improvement. It will define measurable indicators for inclusion, usage, user satisfaction, data protection, and system performance. Periodic evaluations and feedback loops—from users, service providers, and regulators—will guide iterative policy and technology updates. Learning and adaptation will be institutionalized across all implementing agencies and partners to support sustained performance and public trust.

A **coherent and enabling legal framework** is critical to the legitimacy and long-term viability of SevisPass and the Trust Framework. The legal architecture will define user rights, institutional responsibilities, and redress mechanisms across the identity lifecycle. It will cover key areas such as identity registration, data protection, credential issuance, authentication, and inter-agency data exchange.

This framework will align with international legal norms—including the UN Guiding Principles on Business and Human Rights, the OECD Privacy Guidelines, and FATF guidance on digital ID—while being harmonized with national laws on electronic transactions, civil registration, data protection, and financial regulation. Legal provisions will ensure enforceable rights for individuals to access, update, and revoke their data, as well as access redress in case of violations. Legal interoperability will also support future cross-border identity use cases and digital cooperation within the Pacific region and beyond.

The **implementation timeline** for the SevisPass Digital ID and Trust Framework will be phased out over 18 months (followed by 6 months of stabilization), guided by clearly defined quarterly milestones. The approach balances rapid prototyping with progressive scale-up, beginning with foundational activities such as establishing governance structures, drafting the policy and legal frameworks, and developing minimum viable products (MVPs) for key components (SevisPass, SevisWallet, SevisPortal, SevisAdminPortal, and SevisDEx). Early pilots—including provisional SevisPass issuance and biometric enrolment—will inform the full-scale rollout. In parallel, efforts will focus on onboarding early partners (e.g., financial institutions), launching grievance and monitoring mechanisms, and strengthening institutional capacity. By the second year, the Trust Framework will expand to include broader authentication, partner ecosystems, use cases, and integrations with civil registry and other government services, ensuring a scalable, inclusive, and sustainable national ID ecosystem.

2. Introduction

This section provides the overall framing for the SevisPass Digital ID Policy. It outlines the purpose and background of the initiative, articulates its long-term vision and intended outcomes, and sets out the key policy objectives that will guide implementation. The section also defines the primary audience for the policy spanning government agencies, regulators, private sector actors, implementing agencies and development partners—and explains how the policy aligns with existing laws, strategies, and digital development priorities in Papua New Guinea. Together, these elements establish the rationale and strategic direction for building a secure, inclusive, and interoperable digital identity ecosystem.

2.1 Purpose and Background

PNG is advancing toward a digitally enabled future, aligned with its Vision 2050 and the Lagatoi Declaration, through transformative policies such as the Digital Transformation Policy 2020. A secure, inclusive, and interoperable Digital ID system is foundational to this agenda—serving as a trusted mechanism to verify identity across both public and private sectors.

This Digital ID Policy establishes a comprehensive framework for developing and operationalizing SevisPass, PNG's flagship digital identity credential. The policy aims to improve access to services, foster financial and social inclusion, streamline verification processes, and promote good governance and digital trust.

While global experience shows that digital ID systems are critical enablers for secure transactions, economic participation, and service delivery, PNG faces unique challenges. Identity records remain fragmented across institutions, limiting interoperability and efficiency. Rural connectivity gaps, limited infrastructure, and low digital literacy hinder access to digital services. At the same time, evolving cybersecurity risks and limited data protection measures raise potential concerns around the misuse of personal identity.

Currently, identity information is gathered separately by various entities—including banks, health services, telecom providers, educational institutions, and government agencies—which can result in overlapping efforts and less-than-optimal user experiences. Introducing a unified, consent-based digital ID infrastructure could help streamline authentication processes, minimize repetitive verification, and improve access to services—especially for underserved communities.

By integrating existing identity records, strengthening governance frameworks, and fostering a standards-based, rights-respecting ecosystem, the Digital ID Policy aims to position SevisPass as the cornerstone of Papua New Guinea's national trust framework. This initiative will facilitate the realization of a comprehensive digital government, enhance institutional coordination, and empower citizens to engage more fully in the digital economy.

2.2 Vision, Intent, and Objectives

This policy envisions a secure, inclusive, and interoperable Digital ID ecosystem that empowers all residents of PNG by creating a unique identity, enabling access to government and private sector services, fostering trust in digital transactions, and upholding data privacy and security.

The primary intent of the policy is to establish a comprehensive and sustainable framework for developing and operationalizing PNG's Digital ID system. This system will serve as a core component of the country's digital public infrastructure and support the delivery of services across sectors.

To achieve this, the digital ID policy is anchored on the following key objectives:

- Establish a secure and sustainable Digital ID system, governed by a robust Trust Framework that ensures interoperability, inclusion, and long-term viability;

- Introduce SevisPass as a foundational digital identity credential and a verifiable credential, designed to function as a core component of Papua New Guinea's Digital Public Infrastructure (DPI).
- Enable appropriate legal and regulatory frameworks to mandate and support the trusted use of SevisPass and future verifiable credentials across government and regulated private actors.

2.3 Policy Outcomes

Implementation of the Digital ID Policy will deliver the following national-level outcomes:

- **Universal and Inclusive Identification**: A nationally recognized SevisPass credential will ensure all individuals—including marginalized groups—have access to a trusted digital ID that works across online and offline channels.
- **Interoperability and Integrated Service Delivery**: The Digital ID system will enable seamless access across sectors by linking databases through SevisDEx and ensuring secure cross-border recognition and service integration.
- **Enhanced Privacy and Data Protection**: Citizens will gain greater control over their data through user-consent mechanisms, backed by strong security standards and compliance frameworks.
- **Improved Public Sector Governance**: Streamlined digital processes will improve transparency, efficiency, and accountability in government service delivery (G2C, G2B, G2G), while reducing identity fraud and duplication.
- **Trusted Digital Ecosystem**: The policy will operationalize a Digital ID Trust Framework, anchoring SevisPass as a secure and interoperable Digital Public Infrastructure (DPI), governed by law and aligned with global standards.
- **Regulatory Compliance and Risk Mitigation:** The Digital ID system will align with national and international regulatory frameworks—including Anti-Money Laundering (AML), Counter Financing of Terrorism (CFT), and Customer Due Diligence (CDD) standards—to support financial institutions and other regulated entities in meeting their legal obligations efficiently.

2.4 Target Audience

The rollout of the Digital ID system will address the diverse needs and requirements of multiple stakeholders critical to the ecosystem's success. The SevisPass verifiable credential, developed as a Digital Public Infrastructure (DPI), is intended to serve a broad range of users and institutions, including:

- Government agencies and employees — for streamlined identity verification and improved service delivery
- Financial institutions — to facilitate secure customer onboarding and compliance with regulatory requirements
- Telecommunication operators — to support subscriber identification and authentication
- Educational and healthcare providers — to enable secure access to services and credentials
- Regulatory and law enforcement authorities — to assist with identity verification, compliance, and security functions
- Businesses and organizations — to enable trusted digital interactions and transactions
- Citizens and residents of PNG, including foreign nationals — as the primary users of digital identity services

By engaging these stakeholders, the policy aims to ensure that the Digital ID system is inclusive, secure, interoperable, and effectively supports both public and private sector needs across PNG.

2.5 Policy Alignment

This policy supports and complements the implementation of relevant national legislations, policies, and strategies outlined below:

2.5.1 Legislation

The Digital ID Policy is aligned with the existing legislative frameworks, especially the following:

- *Anti-Money Laundering and Counter Terrorism & Fraud Act 2015* – This law enforces verification of identity as part of a financial institutions' due diligence requirements.
- *National Information and Communication Technology Act 2009* as it relates to the regulatory functions of the ICT sector. Relevant regulations, standards, rules, and guidelines will be developed to guide and govern the operations of the Digital ID system.
- *Digital Government Act 2022* as it relates to the development and roll out of key public digital infrastructures and services. Digital ID will enable further progress in the delivery of public digital services provisioned by the Act.
- Papua New Guinea Civil and Identity Registration Act of 2024 as it relates to the registration of births, deaths, marriages, legitimations, and adoptions, and for other purposes. Personal data is defined within this legislation. Digital ID will complement the Act, enabling verification and authentication of citizens to access public services and participate in national events.
- *Citizenship Act 1975* as it relates to acquiring and maintaining citizenship in Papua New Guinea. Digital ID will complement and support the citizenship processes, enabling verification and authentication of citizens in acquiring and maintaining citizenship in Papua New Guinea.
- *Migration Act 1978* as it relates to the entry into Papua New Guinea, Digital ID will complement and support the migration processes, enabling verification and authentication of persons entering Papua New Guinea.

2.5.2 Policies and Strategies

This is an enabling policy that will support the overall implementation of the digital transformation in Papua New Guinea. It will complement and support the following policies and legislation:

- National Information and Communication Technology Policy 2008 relating to increasing the supply of and the demand for ICT services,
- Digital Transformation Policy 2020 relating to the implementation of Digital Government consistent with the Digital Government Act 2022, Digital Government Plan 2023-2027,
- National Cybersecurity Policy 2021 and National Cybersecurity Strategy 2024 relating to the protection of critical infrastructures and systems,
- Government Cloud Policy 2023 relating to shared services for the whole of government and the
- National Data Governance and Data Protection Policy 2024 relating to processing, storing, sharing and protection of data.

This policy aims to support the aspirations contained in Papua New Guinea's Vision 2050 and is aligned with and complements the following:

- Papua New Guinea's Medium Term Development Plan IV (2023-2027) relating to the Strategic Priority Area 8, on Digital Government.
- The 'Digital Government Plan 2023 – 2027' by enabling citizens issuance of a digital ID to access basic digital services that are rolled out under the Plan.

3. Guiding Principles for the Digital ID System

This section sets out the foundational concepts, data standards, and core policy principles that guide the design and implementation of the Digital ID system in PNG. It defines key components of the SevisPass digital identity ecosystem, outlines the attributes and standards that ensure consistency and interoperability, and articulates the rights-based and user-centric principles that underpin a secure, inclusive, and trusted identity framework.

3.1 Definitions

This section defines key terms that form the foundation of PNG's Digital Identity ecosystem, developed using a Digital Public Infrastructure (DPI) approach. The country's digital identity initiative is centred on providing individuals and entities with a secure, trusted, and user-controlled digital identity, beginning with SevisPass as the foundational digital ID credential.

The digital ID ecosystem will grow progressively — starting with issuance of SevisPass, managed through SevisWallet, and governed through the SevisAdminPortal,SevisDEx platforms (details of which have been provided below) and SevisPay platforms. Over time, other verifiable credentials (such as those for citizenship, education, health, and entitlements) could be integrated by authorized government and private sector entities.

This layered build architecture ensures interoperability, embeds privacy by design, and supports efficient service delivery, while enabling individuals to securely access both public and private sector services through a trusted digital identity.

These definitions provide a consistent and policy-aligned understanding of the components, actors, and governance mechanisms within PNG's digital ID system.

3.1.1 Digital ID

A digitally issued identity credential that uniquely and reliably identifies a person for the purposes of accessing services, signing transactions, or asserting legal presence. All individual residents of PNG, including citizens, permanent residents, legally recognized foreign nationals, and citizens living abroad, are eligible to enrol for Digital ID, in accordance with national laws and regulations.

3.1.2 SevisPass (Digital Identity Credential)

SevisPass refers specifically to the Verifiable Credential (VC) issued to residents as their Digital Identity. It is the foundational credential that uniquely identifies a person in digital interactions. SevisPass would be the first credential issued in PNG's verifiable credential ecosystem and will serve as the root of trust for digital interactions.

A VC is a cryptographically signed, tamper-evident digital statement issued by a trusted party (issuer), held by a user (holder), and shared with a service provider (verifier) when required.

3.1.3 SevisWallet (Digital Wallet for Verifiable Credentials)

SevisWallet is the official digital wallet used to store and manage Verifiable Credentials, starting with SevisPass. A digital wallet allows users to:

- Store credentials securely on their mobile device or other supported platform
- Present credentials to access services, with the ability to use selective disclosure
- Consent to data sharing and credential verification when required

- Receive new credentials from other government and trusted providers over time

SevisWallet will be designed for progressive onboarding of new credential types and issuers. While it will initially hold SevisPass, it is expected to incorporate additional credentials from:

- The Civil Registry and National ID
- Immigration and Citizenship Authority (e.g., passport, citizenship status)
- Education institutions (e.g., diplomas, transcripts)
- Banks, telecoms, and other regulated private actors (e.g., KYC credentials, payment wallet)

This approach supports a modular, scalable identity system where residents build up a portfolio of trusted credentials over time.

3.1.4 SevisPortal (Resident Self-Service Portal)

SevisPortal will be the official online interface for residents to access self-service functions related to SevisPass and other verifiable credentials. It is designed to improve accessibility, user control, and convenience across the lifecycle of digital identity and credentials.

Through SevisPortal, residents will be able to:

- Pre-register for SevisPass and other credentials
- Book appointments for biometric enrolment or in-person verification
- View, download, or manage issued Verifiable Credentials
- Link or manage their SevisWallet and other identity-linked services
- Update personal information and request corrections (where authorized)
- Access FAQs, support services, and status tracking

SevisPortal will be accessible via desktop and mobile platforms and may progressively be localized into major languages. It complements the SevisWallet by offering web-based access for those who may not use a smartphone and by providing residents with transparent, self-directed access to their digital identity profile and credentials.

3.1.5 SevisAdminPortal (VC Platform and Trust Registry)

SevisAdminPortal will be the administrative and governance platform for the verifiable credentials ecosystem. It will provide:

- Tools for credential issuance and revocation
- A managed Trust Registry of authorized credential issuers, verifiers, and wallet providers
- Policy enforcement and technical standards to ensure interoperability, security, and trust

Entities eligible to access and operate through the SevisAdminPortal include:

- Government ministries and agencies authorized to issue credentials (e.g., DICT, PNGCIR, RTA, Education, Health, etc)
- Regulated private actors such as licensed financial institutions, telecoms, and employers (subject to certification and compliance)
- Technology service providers under DPI governance frameworks

All actions within the platform will be auditable and subject to compliance oversight.

3.1.6 SevisDEx (Government [G2G] and Business [G2B] Data Exchange Platform)

SevisDEx will be PNG's secure Data Exchange Layer enabling real-time, policy-based, and consent-governed sharing of data across public and authorized private entities. It will enable both:

- Government-to-Government (G2G) exchange (e.g., between the Civil Registry and Health Ministry)
- Government-to-Business (G2B) exchange (e.g., Civil Registry to a bank for identity verification)

SevisDEx will play a foundational role in interoperability, allowing systems to communicate through standardized APIs and protocols while respecting user rights and regulatory requirements.

Two modes of data sharing will be enabled:

1. *Consent-based exchange*: Where personal data can be accessed for a service (e.g., applying for an education assistance program or a mobile SIM), explicit and informed user consent must be obtained via the SevisWallet or integrated consent mechanisms.

2. *Regulatory or mandatory data exchange*: Certain data flows mandated by law (e.g., fraud detection, national statistics, AML/CFT compliance) may occur without consent, but must comply with data protection, minimization, purpose limitation, and logging requirements.

3.1.7 SevisPay (PNG's National Digital Payment Gateway)

SevisPay is PNG's national, neutral digital payment gateway that facilitates secure, identity-linked financial transactions across government and regulated private sector services. As a core component of the SevisPass ecosystem, SevisPay:

- Enables digital payments for G2P, P2G, and P2P use cases
- Integrates with SevisPass and SevisWallet for identity-based payment authentication
- Interoperates with existing payment channels, including mobile money, bank systems, and fintech platforms
- Supports eKYC and AML/CFT compliance through integration with SevisDEx
- Helps expand financial inclusion by supporting offline and mobile payment modes

SevisPay is designed to work across banks, mobile money providers, and public service platforms, providing a secure and inclusive payment infrastructure within the digital identity ecosystem.

3.2 Data Attributes and Standards

The Digital ID system shall collect a defined set of identity attributes necessary for enrolment, authentication, and lifecycle management. These include core biographic and biometric data, aligned with principles of data minimization and proportionality.

The specific data elements and technical standards for capture, formatting, and exchange shall be prescribed through technical guidelines, ensuring compliance with national data protection policies and/or laws and international norms.

Biometric data for the purpose of SevisPass issuance will be collected only after individuals reach an age where biometric traits are considered stable and reliable, in line with international good practices. Until then, children will be issued a SevisPass linked to a parent or guardian, with demographic data only. The biometric record may be updated upon reaching the prescribed age.

3.3 Key Characteristics of SevisPass

SevisPass is being designed with a set of foundational characteristics to ensure it becomes a secure, inclusive, and trusted form of digital identity for all residents of PNG:

- **Random, Non-Intelligent Identifier**: The SevisPass number will be a randomly generated 10- to 12-digit identifier with no embedded personal information or intelligence.
- **Cradle-to-Grave Identity**: Each individual will be assigned one SevisPass for life, which will remain valid permanently and will not require renewal.
- **Digital by Default**: SevisPass will be issued and maintained as a digital credential. While printable versions may be made available for convenience or accessibility, no physical or paper credential will be mandatory.
- **Authentication over Presentation**: The validity of SevisPass will lie in its ability to be securely authenticated or verified electronically, not in the physical presentation of the number or printed copy.
- **Online and Offline Authentication**: SevisPass will support both online and offline modes of authentication to ensure continuity of service delivery and access, even in areas with limited or no internet connectivity.
- **Not Proof of Nationality or Citizenship**: SevisPass will serve to establish a unique digital identity and will not in itself serve as evidence of nationality or citizenship.
- **Uniqueness and Persistence**: Every individual will be issued only one SevisPass, with biometric deduplication ensuring uniqueness and integrity throughout the lifecycle of the ID.

3.4 Core Principles

The PNG Digital ID policy is grounded in a rights-based, user-centric, and inclusive approach that supports the progressive development of the digital identity ecosystem as a public good. Following are the core principles that guide the design, implementation, and governance of SevisPass and its associated components:

3.4.1 Public Good Orientation

Digital ID is recognized as a digital public good that provides foundational identity for all residents. It is not a commercial product, but a state-backed identity system designed to promote access to services, foster trust in digital transactions, and support national development. Its architecture, governance, and operation will remain people-centric and public purpose–driven. While core identity issuance remains publicly funded, financial sustainability may be supplemented through cost recovery mechanisms for certain value-added services (e.g., eKYC for banks and telcos) under a transparent and fair pricing framework.

3.4.2 Inclusion, Accessibility, and Non-Discrimination

Every resident of PNG is eligible for a SevisPass. The system will ensure inclusive access regardless of geographic location, socioeconomic status, disability, or lack of prior documentation. Barriers to access — whether digital, geographic, financial, physical, or social — will be addressed through proactive policy and design measures. Enrolment strategies will include assisted and self-service channels, and accommodate special cases such as individuals without any existing ID, those unable to provide biometrics (e.g., amputees or persons with disabilities), or those living in physically confined areas. Additionally, no one will be denied essential services due to lack of a digital ID.

3.4.3 Privacy and User Rights

The platform will be governed by privacy-by-design principles. Users will have control over how their identity data is shared, with consent-based mechanisms implemented for most use cases. Where disclosure is required by law (e.g., law enforcement or regulatory mandates), such access will follow

clearly defined legal processes. The Digital ID system will be designed to ensure data minimization, auditability, traceability, and non-repudiation across both the issuance and usage phases—enabling users and authorized entities to verify when, how, and by whom identity data is collected, processed, accessed, or shared, and to seek redress where necessary.

3.4.4 Security and Trust by Design

Security is integral to system design, with safeguards built across the identity lifecycle — from registration to issuance to authentication. Identity data will be protected through encryption at rest and in transit, risk-based authentication mechanisms, continuous monitoring, and audit logging to prevent unauthorized access and misuse.

A robust deduplication process will ensure the uniqueness and integrity of each Digital ID, forming a critical foundation for trust in the system. Beyond technical safeguards, the system is part of a broader trust framework aimed at building confidence among residents, institutions, and service providers. This includes ensuring transparency in ID usage, enforceable accountability, and mechanisms for redress—all of which contribute to a trusted, rights-based identity ecosystem.

3.4.5 User-Centricity and Accessibility

The ID system will be designed with a focus on ease of use, language inclusivity, and accessibility for low-literacy users. Enrolment, authentication, and credential management will be optimized for mobile and offline environments. Feedback loops and grievance redressal mechanisms will ensure continuous improvement based on user needs and experiences.

3.4.6 Interoperability and Openness

The Digital ID system will adopt open standards and be interoperable with existing and future digital systems across the public and private sectors. Through SevisDEx and SevisAdminPortal, government agencies, regulated entities, and service providers will be able to securely exchange identity-related information in real time. This enables seamless, cross-sector service delivery and supports the broader digital transformation agenda.

4. Role of Digital ID in the Trust Framework

As PNG establishes *SevisPass* as the foundational layer of its national digital identity system, it will anchor a broader, future-ready digital trust framework. This framework is designed to facilitate secure, inclusive, and efficient digital interactions between individuals, government entities, and service providers. Guided by principles of user centricity, public good orientation, and transparency, it brings together essential components including *SevisPass* and its verifiable credentials, *SevisWallet*, the trust registry via *SevisAdminPortal*, and *SevisDEx* for secure data exchange. These components will work together to form PNG's Digital Public Infrastructure (DPI) and will enable trusted transactions across sectors—from public service delivery to financial access—ensuring no one is left behind.

4.1 Digital Public Infrastructure in the PNG Context

Digital Public Infrastructure (DPI) refers to foundational digital systems and protocols that are designed for open, secure, and interoperable use by both public and private sectors. In the PNG context, DPI will include:

- A digital ID and its verifiable credential (*SevisPass*)
- A secure and user-controlled digital wallet (*SevisWallet*)
- A verifiable credential platform governed through a trust registry (*SevisAdminPortal*)
- A consent-enabled data exchange layer (*SevisDEx*)
- A digital payments platform (*SevisPay*) to enable secure and inclusive transactions across government, private services and people (*to be planned in future*)

Together, these form a cohesive and modular stack that enables identity verification, credential portability, and trusted data sharing across multiple domains. The DPI approach allows PNG to build incrementally—starting with the most critical use cases such as eKYC—while laying the foundation for broader digital transformation.

The following diagram illustrates the interaction between SevisPass, SevisWallet, trust registry, data exchange, and verifiable credentials. It also shows how these elements support the trust triangle (VC issuer – VC holder – VC verifier) in enabling secure and scalable digital services.

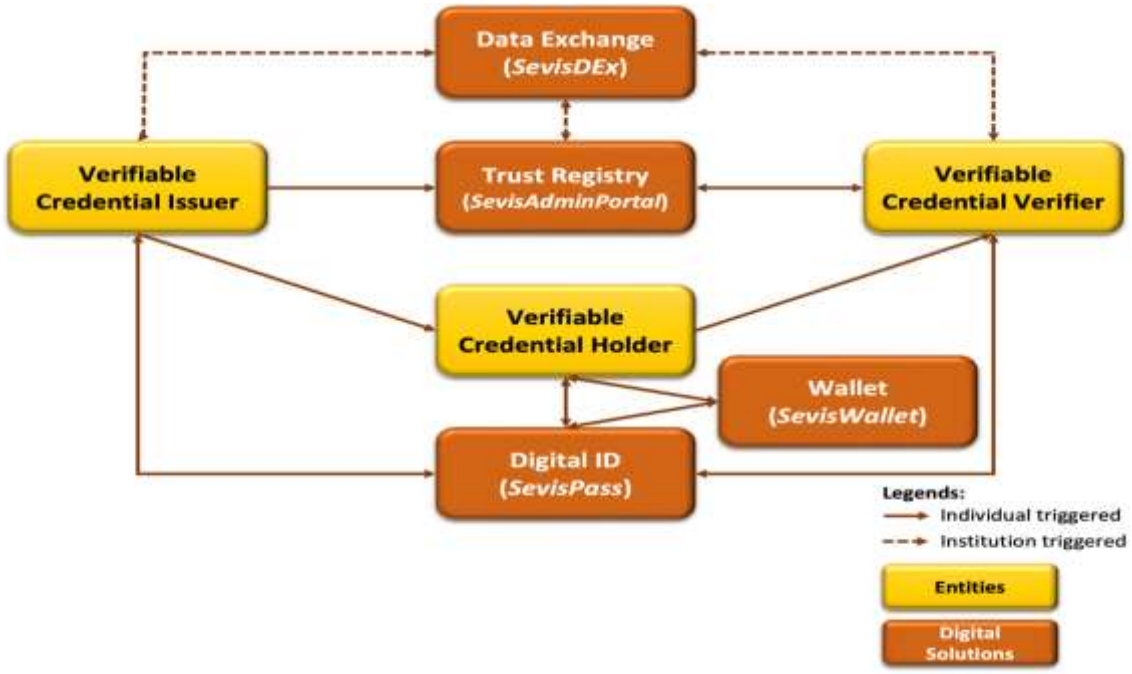

Figure 1: PNG's Digital Trust Framework — Components and Interactions

4.2 Role of SevisPass in PNG's Trust Framework

SevisPass, PNG's digital identity credential, will serve as the unique, trusted identity layer for all residents, including citizens living abroad. It will provide a verifiable, secure, and portable means for individuals to prove their identity to access services both online and offline.

SevisPass will be a foundational credential within PNG's trust framework—acting as a root identity that can be linked to other verifiable credentials issued by government agencies (e.g., citizenship, residency, education, or entitlements). This digital identity system will underpin the broader trust infrastructure, enabling reliable verification of individuals by service providers while ensuring user control, consent, and protection of personal data.

SevisPass will also serve as the unique identifier across multiple databases and systems, enabling consistent identity resolution. This will be critical for achieving interoperability across government services and private sector applications. In conjunction with SevisDEx, SevisPass will facilitate trusted and secure data sharing, allowing agencies and service providers to coordinate effectively, avoid duplication, and improve targeting of services. As such, SevisPass is not only an enabler of digital identity, but a key pillar of PNG's broader trust and service delivery infrastructure.

4.3 Linkages Across the Trust Ecosystem

To fully enable a trusted digital environment, *SevisPass* will interoperate with other core trust-enabling components:

- **Verifiable Credentials**: Government and authorized institutions will issue digital credentials—such as social protection eligibility, tax status, or licenses—based on *SevisPass*. These credentials will be tamper-proof, cryptographically secure, and machine verifiable by third parties.

- **SevisWallet**: All individuals will have access to a digital wallet (*SevisWallet*) to store and manage their credentials. This user-centric wallet will enable secure and selective sharing of credentials, both online and offline. Over time, various government agencies, as well as private sector actors such as banks, insurers, and educational institutions, will be able to issue credentials to SevisWallet holders.

- **SevisAdminPortal**: PNG will establish a national trust registry, hosted on the SevisAdminPortal, to maintain a dynamic list of authorized institutions that can issue, verify, or consume credentials and data. This registry will underpin trust across the SevisPass ecosystem, enabling validation of credential issuers and verifiers, while also supporting SevisDEx by authenticating data providers and consumers involved in secure data exchange. It will be governed by clear legal and institutional mechanisms to prevent misuse, ensure transparency, and restrict unauthorized access, thereby reinforcing the integrity of both verifiable credential flows and data sharing within the national digital infrastructure.

- **SevisDEx**: The SevisPass system will integrate with the data exchange *SevisDEx* to enable secure, purpose-limited data exchange between government agencies and with regulated private entities. All data sharing will be governed either by user consent or applicable legal and regulatory mandates. SevisDEx will drive interoperability, allowing services to access verified data directly from source systems in real time.

- **SevisPay (National Payment Gateway)**: As an established neutral payment gateway, SevisPay will enable secure, authenticated, and seamless digital payments across both public and private sectors. Integrated with SevisPass and SevisWallet, SevisPay will support real-time transactions for government-to-person (G2P) disbursements (e.g., social benefits, pensions), person-to-government (P2G) payments (e.g., taxes, fees), and business-to-consumer (B2C) or consumer-to-business (C2B) payments. By linking identity, verifiable credentials, and digital payments, SevisPay will help drive financial inclusion, improve service delivery efficiency, and strengthen transparency and accountability in national digital transactions.

Together, these systems will create a robust environment for secure transactions, inclusive service delivery, and data protection.

4.4 Regulatory Enablement and Financial Sector Integration

The combination of SevisPass and SevisDEx provides a future-proof mechanism to meet regulatory obligations across sectors, starting with finance. Banks and other regulated institutions in PNG face complex and evolving requirements under the Financial Action Task Force (FATF) framework—especially around Customer Due Diligence (CDD), Know Your Customer (KYC), and transaction monitoring.

SevisPass will serve as a foundational and verifiable digital identity that can be adopted as the **primary identifier** across regulated databases, enabling real-time and ongoing identity verification to support Simplified, Standard, and Enhanced Customer Due Diligence (CDD). SevisPass will focus solely on providing reliable identity data and verification tools, ensuring no overlap with financial institutions' responsibilities for customer risk assessments, transaction monitoring, sanctions screening, or setting transactional and service limits under the AML/CTF Act 2015, thereby maintaining consistency with PNG's AML/CTF framework to mitigate FATF grey listing risks. The SevisDEx platform, anchored by a trusted data exchange protocol and supported by the trust registry, will allow banks to query up-to-date identity information and authorized attributes (e.g., residency, age, employment status) with user consent. To mitigate cybersecurity risks, SevisDEx will implement robust encryption, access controls, and regular security assessments to protect sensitive data. The platform will ensure high availability through redundancy and disaster recovery mechanisms to minimize disruptions to bank operations. Consent management will allow users to control data sharing on a per-transaction or per-service basis, with standardized protocols to ensure efficient interoperability for financial institutions

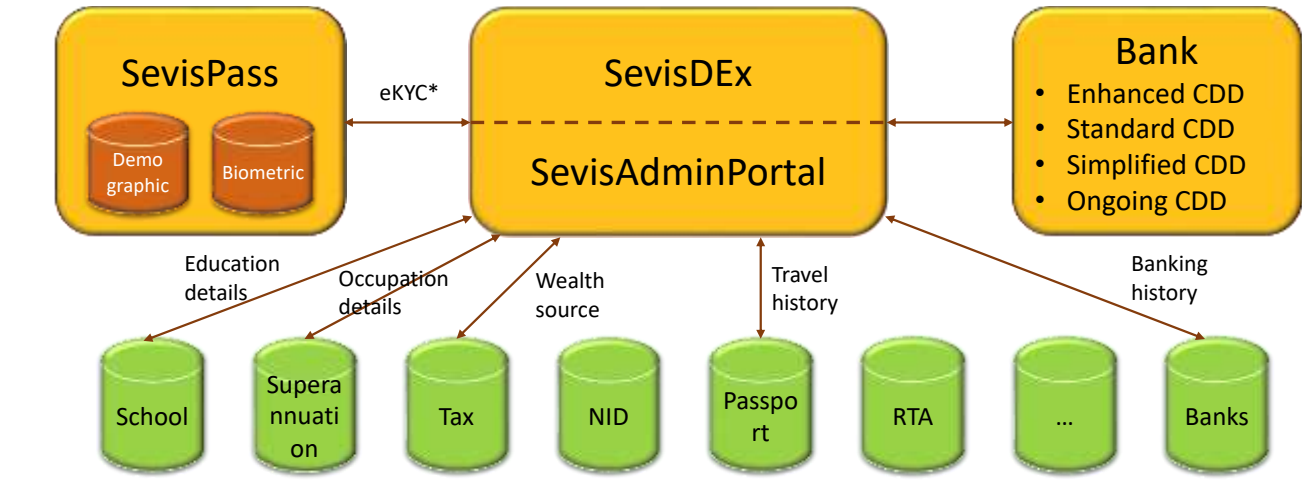

Figure 2: Illustration of CDD Needs Fulfilment Through Trust Framework

This architecture is built for **adaptability**. As new CDD rules are introduced by domestic regulators (e.g., BPNG) or international standards evolve, authorized entities can integrate additional data sources or credentials without re-engineering their systems. The trust registry ensures only authorized issuers and verifiers can participate, maintaining security and compliance integrity.

This model not only supports FATF compliance but also enables broader financial inclusion, more seamless onboarding, and cost-effective risk management.

4.5 System-Wide Outcomes from Trust Framework

The introduction of SevisPass and its supporting trust infrastructure is expected to yield transformative outcomes across PNG's public and private sectors, prioritizing financial inclusion for populations lacking digital access or literacy:

- **Service Integration and Efficiency**: Government and private sector services can authenticate users and validate credentials digitally, leading to faster, more efficient, and user-friendly service delivery.
- **Regulatory Readiness and Interoperability**: The framework supports both current and future compliance needs, including FATF recommendations and other cross-border or sector-specific verification mandates.
- **User Empowerment and Privacy**: Through user-controlled wallets and consent-based sharing, individuals gain control over who accesses their personal data, reinforcing privacy and trust.
- **Institutional Trust and Accountability**: The trust registry and SevisDEx ecosystem ensure only authorized, auditable entities participate in identity, credential, and data exchange operations.
- **Inclusion**: SevisPass will support inclusive enrolment strategies, such as mobile and offline enrolment, to ensure accessibility for underserved communities.

This outcomes-driven approach positions the trust framework as a foundational enabler for PNG's digital transformation.

5. Governance and Institutional Architecture

A strong governance framework is essential to ensure SevisPass is trusted, inclusive, secure, and aligned with national priorities. The governance framework will be guided by principles of accountability, transparency, user-centricity, and institutional coordination, while allowing for innovation and scale through partnerships.

5.1 Governance Model

The governance of SevisPass will follow a **federated operational model** underpinned by **centralized policy, standards, and oversight**. This model enables decentralised implementation—particularly for enrolment and service delivery—while maintaining consistency, integrity, and trust across the ecosystem.

Key features of the governance model include:

- Central setting of standards for technology, operations, security, and data protection
- Decentralized execution by authorized public and private entities under clearly defined protocols
- Role-based access, auditability, and compliance enforcement across all entities
- Separation of roles in ID issuance, credential management, authentication, and data exchange to reduce conflicts of interest and promote accountability

5.2 Institutional Mandates

The SevisPass Digital ID and Trust Framework will be governed by a multi-tiered institutional architecture that clearly defines the mandate, accountability, and coordination responsibilities of each key actor. This institutional arrangement aims to ensure strategic alignment across government priorities, regulatory coherence, and operational efficiency in the rollout and sustained delivery of digital identity services. The institutional arrangement is represented in the following diagram and explained further in this section.

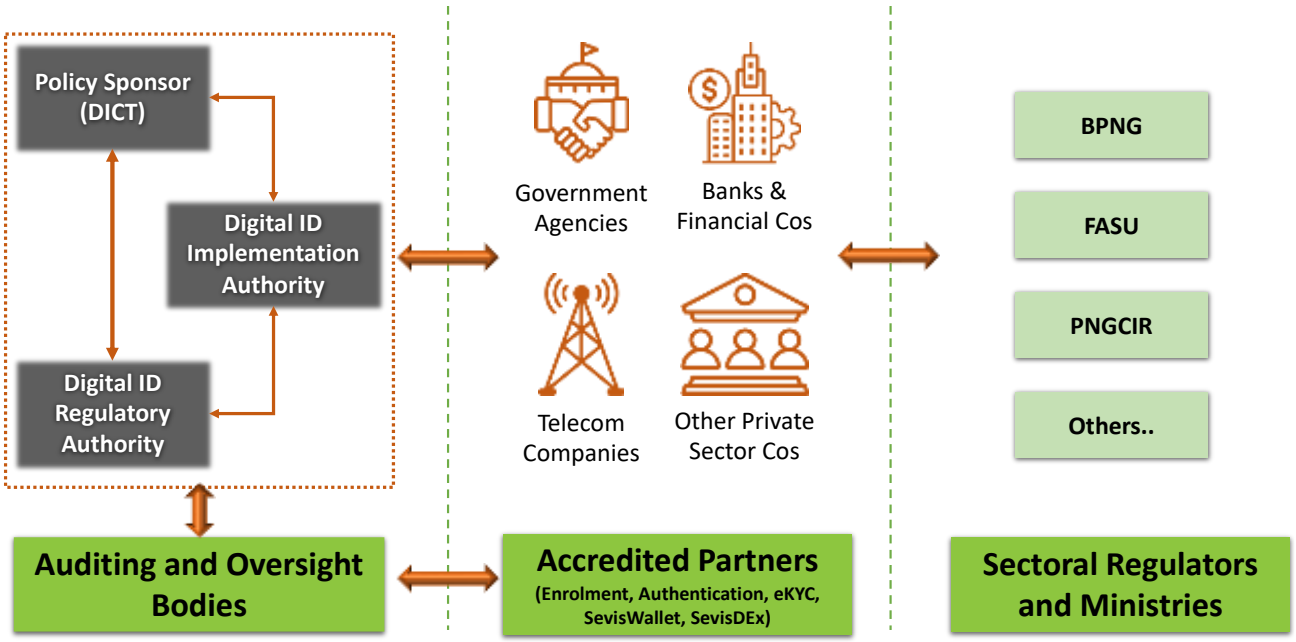

Figure 3: Institutional Arrangement for Digital ID and Trust Framework

Further, to ensure clarity in institutional responsibilities and support smooth implementation of the Digital ID and Trust Framework, a RACI (Responsible, Accountable, Consulted, Informed) matrix is provided in the Annexure.

5.2.1 Policy Sponsor

Department of Information and Communications Technology (DICT) will act as the central policy sponsor and steward of the SevisPass ecosystem.

Its responsibilities includes:

- Developing and updating the **Digital ID Policy** and Strategy in alignment with the Digital Transformation Policy 2020.
- Proposing and reviewing legislative or regulatory reforms necessary for Digital ID adoption (e.g., legal recognition of eKYC, digital credentials, data exchange, and authentication services)
- Coordinating robust and continuous stakeholder engagement, including government agencies (e.g., PNGCIR, BPNG, FASU), private sector partners (e.g., financial institutions like BSP), and civil society, to ensure policy alignment with sectoral needs.
- Anchoring the **central coordinating body** that drives the national digital identity strategy
- Convening and chairing the **Inter-Agency Steering Committee**, comprising key ministries, regulators, and private sector representatives, to foster collaboration and align policies, legislation, and regulations across the SevisPass ecosystem.

- Issuing national-level policy directives to guide ecosystem governance and inter-agency integration
- Securing budgetary allocations, coordinating development partner assistance, and mobilizing international cooperation
- Endorsing accreditation frameworks, technical standards, and M&E mechanisms as proposed by the regulatory authority
- Driving alignment with other national strategies—such as eGovernment, cybersecurity, and inclusion policies—and reporting progress to the Cabinet

5.2.2 Digital ID Regulatory Authority

The incumbent ICT and digital industry regulator will serve as the primary regulatory and oversight body for the Digital ID and Trust Framework. The regulatory agency will be responsible for formulating the Digital ID Trust Framework in consultation with industry and regulating the Digital ID System.

Key responsibilities include:

- Developing and enforcing the Digital ID Trust Framework, defining standards for registration, issuance, usage, and management, with a focus on providing reliable identity verification tools to support financial institutions' compliance with the AML/CTF Act 2015, and access to digital services.
- The Regulatory Authority will ensure SevisPass does not prescribe customer risk ratings or interfere with financial institutions' responsibilities for risk assessments, transaction monitoring, or sanctions screening, aligning with FATF standards to avoid inconsistencies
- Formulating a legal framework for the Digital ID System, proposing amendments to the relevant legislations such as National Information and Communication Technology Act 2009 to support regulatory oversight.
- The Regulatory Authority will ensure SevisPass aligns with Section 16 of the AML/CTF Act 2015 as a reliable and independent source for identity verification, without requiring specific amendments to the AML/CTF Act to recognize SevisPass for CDD.
- The Regulatory Authority will not mandate real-time transaction monitoring or fraud detection via SevisPass, preserving financial institutions' existing systems for these functions.
- Drafting and notifying technical standards, data protection regulations, and certification criteria for ecosystem partners
- Maintaining the Trust Registry at governance level and adjudicating on disputes or grievances involving ecosystem actors.
- Leading the Technical Standards and Advisory Committee, which will include private sector, civil society, and government experts
- Managing eligibility requirements for accredited partners across enrolment, authentication, eKYC and data exchange services.
- Monitoring ecosystem compliance (for areas such as data protection, consent, interoperability, and auditability norms) through periodic audits, security assessments, and partner reporting obligations
- Enforcing risk mitigation protocols and issuing enforcement directions or penalties for non-compliance
- Managing protocols for consent collection, privacy notices, and authentication logs
- Ensuring international alignment with ITU, ISO, and GDPR-equivalent norms

The Regulatory Authority will also coordinate with DICT and legal reform bodies to review and adapt existing legislation on electronic transactions, privacy, digital signatures, National ID, and data exchange.

5.2.3 Digital ID Implementation Authority

A suitable agency will be designated to act as the Digital ID Implementation Authority for designing, deploying, and maintaining the core components of the SevisPass ecosystem. The Implementation Authority will be responsible for ensuring Trust Framework's interoperability, scalability, and security.

Key responsibilities include:

- Managing the operational rollout and system lifecycle of SevisPass and related platforms
- Signing MoUs and contracts with accredited enrolment partners, authentication/eKYC providers, and data exchange entities based on the eligibility and criteria defined by the Regulatory Authority
- Managing the onboarding and technical integration of ecosystem partners
- Ensuring user support systems, grievance redress mechanisms, and helpdesk operations
- Driving adoption through capacity building, technical toolkits, developer APIs, and sectoral use-case pilots
- Developing and executing a long-term financial sustainability model, including the charging and pricing policy for digital ID and trust services in consultation with Digital ID Regulatory Authority and DICT
- Acting as the secretariat to the Inter-Agency Steering Committee, preparing technical proposals and updates
- Contracting and supervising technology vendors for the SevisPass, SevisWallet, SevisPortal, SevisAdminPortal, and SevisDEx platforms
- Managing IT infrastructure, cybersecurity, disaster recovery, and user support operations
- Developing user and partner documentation, including SOPs, training material, and technical manuals
- Designing and monitoring dashboards for tracking ecosystem performance, grievance redress, and policy compliance in close collaboration with the Regulatory Authority
- The Implementation Authority will ensure high system availability through redundancy and disaster recovery protocols to minimize disruptions to financial institutions' operations, with technical integration support for banks to address compatibility challenges.

Governance of Digital ID Implementation Authority:

- The designated entity would be a private or public company and will report to its own Governing Board to which the State must maintain a level of investment and shares.
- The board is to comprise of a representative from the government agency responsible for civil registry and/or digital development, a representative from the Financial Institutions, a representative from the Telecommunication Industry, and shareholders/investors.
- Maintain transparency through annual reports on system performance, security incidents, and compliance with the Digital ID Trust Framework.
- Implement risk management protocols, including regular vulnerability assessments and incident response plans, aligned with the National Cybersecurity Policy 2021 and National Cybersecurity Strategy 2024.

5.2.4 Other Sectoral Ministries and Regulatory Bodies

A number of other ministries and regulators will play key sectoral roles, particularly in enabling regulatory compliance and adoption of the SevisPass ecosystem. Some such entities include:

- **Bank of Papua New Guinea (BPNG)**
    - Issue sectoral directives for adoption of SevisPass-based eKYC and digital onboarding across licensed financial institutions

- Approve participation of regulated entities in pilot programs using SevisDEx for customer due diligence (CDD)
- Integrate SevisPass and SevisWallet with national payment systems such as neutral payments gateway, SevisPay, as well as national credit infrastructures
- Leverage SevisDEx data-sharing mechanisms to strengthen compliance with FATF's AML/CFT recommendations, especially those related to identity verification
- Participate in the Inter-Agency Steering Committee to align financial sector modernization with digital ID rollout
- Collaborate with DICT and Digital ID Regulatory Authority to shape legal reforms related to eKYC, data residency, the operation of SevisPay, and consent-based frameworks for financial data governance.

- **Financial Analysis and Supervision Unit (FASU)**
  - Define AML/CFT-aligned onboarding rules for SevisPass ecosystem, leveraging SevisPass as a reliable and independent identity verification tool under Section 16 of the AML/CTF Act 2015 ensuring proportionality and inclusion for underserved populations
  - FASU will not oversee SevisPass-specific compliance, risk-based assessments, or training for financial institutions, which remain under FASU's existing AML/CTF oversight framework.
  - FASU will collaborate with the Digital ID Regulatory Authority to support data audit trails and identity resolution policies, while financial institutions retain responsibility for fraud detection and transaction monitoring.
  - Issue guidance for risk-based customer due diligence using verifiable credentials and SevisDEx
  - Engage in regulatory sandbox initiatives to pilot innovative eKYC and transaction monitoring solutions with fintechs and banks
  - Coordinate with the FATF review process to demonstrate national progress on digital identity infrastructure and its linkage to financial sector integrity
  - Support development of data audit trails, fraud detection mechanisms, and identity resolution policies in collaboration with Digital ID Regulatory Authority

- **Papua New Guinea Civil and Identity Registry (PNGCIR)**
  - Support document-based SevisPass issuance using civil registry datasets to ensure accurate identity credentials, aligning with the Civil and Identity Registration Act 2024.
  - Facilitate data-sharing agreements, attribute mapping, and periodic sync protocols with SevisWallet, SevisDEx and SevisAdminPortal to support seamless integration within the national digital identity framework.
  - Explore data convergence pathways with the SevisPass ecosystem for vital events (birth, marriage, death) in the medium term to enhance interoperability and comprehensive registration.
  - Participate in legal reviews to ensure compliance with the Civil and Identity Registration Act 2024 for registry data sharing and digital credential issuance, prioritizing privacy and security.

- **National Institute of Standards and Industrial Technology (NISIT)**
  - Support the development and notification of national standards and technical specifications for Digital ID, verifiable credentials, and data exchange to ensure alignment with international best practices (e.g., ISO/IEC, ITU-T, W3C).
  - Serve as the national standards body coordinating with DICT, Digital ID Regulatory Authority, Digital ID Implementation Authority and SevisPass ecosystem actors to

standardize processes for credential issuance, authentication, encryption, and biometric data management.
- Support accreditation frameworks for technology service providers and partners participating in the Trust Framework, including testing, certification, and compliance assessment functions.
- Participate in the Inter-Agency Steering Committee and relevant Technical Working Groups to advise on interoperability, quality assurance, and conformity assessment across DPI components.
- Contribute to legal and regulatory reviews to establish enforceable mandates for compliance with notified technical standards under the national standards framework.

5.2.5 Accredited Partners

The SevisPass ecosystem will rely on a network of accredited partners—including enrolment agencies, authentication and eKYC users, VC issuers, digital wallet users, and data exchange participants—to deliver citizen-facing services and support the secure functioning of the Trust Framework. These partners may include government departments, licensed financial institutions, fintechs, telcos, and civil society organizations, subject to eligibility and sectoral clearances.

All accredited partners will be required to undergo a formal onboarding, certification, and licensing process led by the Implementation Authority, in line with accreditation guidelines and standards issued by the Regulatory Authority. Their participation will be governed through binding participation agreements that specify technical and operational standards, data protection and privacy obligations, audit compliance, permitted use cases, revocation procedures, and citizen grievance redress responsibilities.

Partners will also be subject to periodic performance reviews, data security audits, and usage reporting, and must comply with any sector-specific directions issued by regulators such as BPNG,FASU or PNGCIR. In the event of misuse or breach, the Digital ID Regulatory Authority will have the authority to suspend or revoke accreditation, and invoke penalties under applicable laws.

Specific responsibilities of these partners include:

- **Enrolment Partners:**
  - Operate field enrolment centers (fixed and mobile) as per prescribed protocols
  - Perform biometric/demographic capture using compliant/certified equipment, software, and field staff
  - Ensure validation through SevisDEx and SevisAdminPortal
  - Maintain logs, consent records, and ensure secure data transfer as per prescribed protocols

- **Authentication and eKYC Partners:**
  - Integrate SevisPass authentication APIs for service delivery or customer onboarding, supporting Simplified, Standard, and Enhanced CDD processes.
  - Generate digital logs, maintain revocation mechanisms, and ensure compliance with privacy standards
  - Support authentication methods (e.g., QR, OTP, biometric) and uphold user consent models
  - Comply with usage limits, data minimization, and risk scoring requirements issued by Digital ID Regulatory Authority, FASU, or another sectoral regulator
  - Partners, including financial institutions, will use SevisPass for identity verification but retain full responsibility for customer risk assessments and risk scoring under the AML/CTF Act 2015, ensuring compliance with usage limits and data minimization

requirements issued by the Digital ID Regulatory Authority, FASU, or other sectoral regulators.

- **SevisWallet Partners (VC Issuers):**
  - Develop and issue credentials based on approved data schemas, metadata standards, and assurance levels defined by the Digital ID Regulatory Authority
  - Implement cryptographic signing and security protocols (as per Trust Framework specifications) to ensure that all issued credentials are tamper-evident, verifiable, and privacy-preserving
  - Register and maintain status as authorized issuers in the Trust Registry
  - Issue credentials to holders only with informed consent, in compliance with data protection laws and principles of purpose limitation and data minimization
  - Support offline capabilities and integration with public/private service delivery apps
  - Adhere to applicable sectoral laws, including any guidance issued by PNGCIR, BPNG, FASU, or other domain regulators

- **SevisDEx Participants:**
  - Publish or consume digitally signed attributes (e.g., identity validation, school attendance, income status)
  - Define attribute schemas, assurance levels, and revocation mechanisms
  - Maintain audit logs, latency benchmarks, and authentication protocols for API calls
  - Facilitate legal agreements and data protection compliance in line with Data Governance and Data Protection Policy 2024 and National ICT policy, ensuring user consent is obtained on a per-transaction or per-service basis for data sharing.
  - Participants, including banks, will benefit from standardized APIs and integration protocols to ensure efficient interoperability, with robust cybersecurity measures to mitigate risks from data concentration.
  - Register and maintain status as authorized users in the Trust Registry
  - Adhere to applicable sectoral laws, including any guidance issued by PNGCIR, BPNG, FASU, or other domain regulators

- **SevisPay Integrators (Payment Gateway Partners):**
  - Integrate with **SevisPay**, the established **neutral national payment gateway**, to facilitate secure and authenticated digital payments
  - Enable a unified payments interface that supports **existing payment options** such as:
    - Mobile money (e.g., Digicel CellMoni, bmobile MyCash)
    - Traditional bank transfers
    - EFTPOS and card payments
    - Agency banking and branchless services
  - Ensure interoperability across these channels while linking payments to verified identities and credentials
  - Facilitate use cases such as government-to-person (G2P) disbursements, person-to-government (P2G) payments, and merchant transactions
  - Maintain transaction logs, fraud detection systems, and comply with AML/CFT framework

5.2.6 Work in coordination with BPNG, DICT, and the Digital ID Regulatory Authority to ensure alignment with financial inclusion, data privacy, and regulatory standards Auditing and Oversight Bodies

Oversight mechanisms are critical to ensure accountability and citizen trust. Following mechanisms are proposed for monitoring the Digital ID and Trust Framework ecosystem:

- **Auditor General / Independent Oversight Entity:**
  - Conduct periodic financial, technical, and data governance audits of implementing and regulatory bodies
  - Review ecosystem-wide compliance performance and make recommendations for remedial action

- **Civil Society–Private Sector Advisory Group (multi-stakeholder):**
  - Provide feedback on ethical and inclusive implementation of the digital identity program
  - Advise on grievance trends, outreach challenges, and barriers to adoption

- **Public Grievance Commission / DICT Designated Grievance Office:**
  - Monitor citizen complaints and escalate unresolved issues through structured workflows
  - Recommend systemic improvements based on grievance data analytics

- **Legislative Reporting Mechanism:**
  - Annual ecosystem reports tabled in Parliament, including usage metrics, regulatory performance, inclusion outcomes, and recommendations for legal or institutional reform

5.3 Multi-Stakeholder Governance Structure

The SevisPass system will be governed through a multi-layered and participatory governance structure that ensures coordination, accountability, and responsiveness across all stakeholders involved in the digital identity ecosystem. Governance mechanisms will include inputs from end-users, vulnerable groups, and local communities to ensure that the system remains inclusive, user-centric, and trusted by the public. The governance structure will include mechanisms for regular audits, reporting obligations, and public disclosures, reinforcing transparency and building public confidence in SevisPass.

5.3.1 Central Coordinating Body

The Department of Information and Communications Technology (DICT) will serve as the apex authority responsible for setting policies, defining standards, ensuring interoperability, and coordinating implementation across sectors. It may be supported by a dedicated Digital ID Implementation Authority or Secretariat.

5.3.2 Interagency Steering Committee

An inter-ministerial or cross-sectoral committee comprising key institutions such as the NICTA, BPNG, PNGCIR, IRC, ICSA, and RTA will provide strategic oversight, facilitate alignment across sectors, and resolve policy-level challenges.

5.3.3 Technical and Advisory Committees

Technical subcommittees involving experts from academia, private sector, civil society, and implementing partners will advise on system design, technology standards, and emerging risks such as AI misuse, cybersecurity threats, or exclusion risks.

5.4 Redress Mechanisms and User Control

Ensuring that SevisPass operates as a trusted and accountable digital ID system requires robust mechanisms for grievance redress, user rights protection, and continuous oversight. The policy framework will uphold these through the following institutional and technical safeguards:

5.4.1 Grievance Redress Mechanisms

- **Multi-channel access**: Individuals will be able to lodge complaints or raise queries through multiple channels—online portals, call centres, physical enrolment and service centres, and authorized partner organizations—to accommodate varying levels of digital literacy and connectivity across the population.
- **Tiered resolution process**: Complaints will be classified and resolved through a structured process with defined service levels, escalation tiers, and timelines. Categories may include issues related to enrolment, authentication failure, denial of services, data inaccuracy, or potential misuse.
- **Human oversight and accountability**: A dedicated redressal unit within the Digital ID Implementation Authority will oversee complaint management, conduct regular audits, and issue public reports on resolution performance, including data on common issues, time to resolution, and systemic improvements.
- **Partner accountability**: Entities involved in enrolment or service delivery will be contractually obligated to maintain grievance-handling procedures aligned with national standards, and to provide timely resolution of complaints within their operational scope.

5.4.2 User Rights and Data Control

- **Right to information and correction**: Users will have the right to access their SevisPass profile and request corrections to their personal data through authorized channels, subject to validation and audit processes.
- **Consent-driven data sharing**: The use of SevisPass credentials and associated data for authentication, verification, or service delivery will be governed by user consent, except where sharing is mandated by law or regulatory oversight (e.g. national security or AML/CFT compliance).
- **Revocation and withdrawal**: Users will be able to view and revoke previously granted consent to third-party access of their credentials, through SevisWallet or other user interfaces. Mechanisms will also be developed to notify users when their data is accessed or shared.
- **Support for vulnerable groups**: Additional safeguards and assisted redressal options will be provided for vulnerable populations, such as persons with disabilities, the elderly, or digitally excluded groups, including support through community-based institutions.

5.4.3 Technical and Policy Safeguards

- **Auditability and traceability**: All key system activities—enrolment, data access, authentication attempts—will be securely logged to enable traceability and resolution in case of disputes, unauthorized access, or technical failures.
- **Non-repudiation and system integrity**: Digital signatures, timestamping, and verification protocols will be used to ensure actions taken within the system cannot be denied by involved parties, thereby strengthening accountability.

- **Data minimization and purpose limitation**: Data collected and shared through SevisPass will be limited to what is strictly necessary for the stated purpose, as defined by legal and technical standards, minimizing risk of misuse.
- **Periodic review and policy updates**: The governance framework will include periodic assessment of the grievance and user rights frameworks to adapt to evolving threats, legal interpretations, and technological changes.

5.5 Governance Evolution and Capacity Building

To ensure the long-term success, adaptability, and resilience of the SevisPass ecosystem, the governance framework will include provisions for institutional evolution and targeted capacity building across the public and private sectors.

5.5.1 Institutional Strengthening

The Government recognizes that effective digital ID governance requires capable institutions. Over time, a dedicated Digital ID Implementation Authority may be established or designated to oversee the end-to-end functioning of SevisPass, including operations, standards, compliance, audits, and stakeholder coordination. This body will evolve in line with national priorities, regulatory developments, and user needs.

Key responsibilities of this body would include:

- Managing the operational rollout and system lifecycle of SevisPass and related platforms.
- Signing MoUs and contracts with accredited enrolment partners, authentication/eKYC providers, and data exchange entities based on the eligibility criteria.
- Managing the onboarding and technical integration of ecosystem partners.
- Ensuring user support systems, grievance redress mechanisms, and helpdesk operations.
- Driving adoption through capacity building, technical toolkits, developer APIs, and sectoral use-case pilots.
- Developing and executing a long-term financial sustainability model, including the charging and pricing policy for digital ID and trust services in consultation with the regulatory authority and policy sponsor.

5.5.2 Building Local Ecosystem Capacity

The success of SevisPass depends not only on centralized governance but also on the strength of the broader digital ecosystem. The government will work to build the capacity of local institutions, service providers, and implementing partners to adopt and integrate SevisPass into their programs. This includes:

- Business process re-engineering to accommodate digital ID workflows;
- Technology enablement for integrating SevisPass authentication and verification mechanisms;
- Device and infrastructure readiness, particularly in remote and underserved areas;
- Connectivity and digital literacy initiatives to bridge the digital divide.

Capacity-building efforts will be inclusive and ongoing, with support for training, knowledge sharing, and ecosystem partnerships to ensure that the digital ID system serves as a foundational enabler for digital transformation across sectors.

5.5.3 Future-Proofing the Ecosystem

The SevisPass governance model will include mechanisms to continuously monitor global technology trends and innovations in digital identity, data protection, and authentication systems. This will ensure the ecosystem does not suffer from technological obsolescence and remains adaptable to emerging standards, protocols, and user expectations. Periodic reviews and stakeholder consultations will inform upgrades to platforms, standards, and governance processes.

6. Digital ID Lifecycle and Implementation Approach

The implementation of PNG's Digital ID system will follow a phased, inclusive, and adaptive approach, anchored in a secure and scalable technology backbone and aligned with the country's development context and institutional capabilities. The objective is to progressively build a trusted national identity platform that is inclusive of the informal economy and accessible to all residents, regardless of location, digital access, or documentation status.

6.1 Digital ID Lifecycle

The SevisPass digital ID system will follow a comprehensive lifecycle that ensures secure, inclusive, and sustainable access to digital services for all residents of PNG. This lifecycle spans the full spectrum of identity operations—from registration and credential issuance to usage, updating, and oversight—enabling both public and private sector entities to confidently rely on digital identity for service delivery. The key stages are:

1. Registration: Personal data—including core demographic attributes (e.g., name, gender, address, date of birth) and biometric information (e.g., fingerprint, face photo)—will be collected through a federated enrolment model (see Section 6.3).

The Digital ID Implementation Authority will define registration standards and tools, while trusted partner agencies will conduct field enrolment using secure, certified kits. Data will be securely transmitted to the central system for deduplication and validation.

2. Issuance: Once verified, each resident will be issued a unique SevisPass identity number and associated verifiable credential (VC). These credentials will be stored in a secure digital wallet, accessible through mobile, web, or assisted channels.

Issuance processes will be governed through the SevisPortal (accessible to Residents), enabling real-time tracking, audit trails, and support for reissuance or error correction when needed.

3. Use: Service providers—across both public and private sectors—will be able to integrate SevisPass into their service workflows to identify, verify, and authenticate individuals. This can be done through two interoperable pathways:

- SevisDEx (Sevis Data Exchange): A secure, API-based data exchange layer that enables real-time identity verification by querying the Digital ID system with user consent. This is particularly suited for integrated service delivery platforms and backend verifications.
- Verifiable Credentials (VCs): Cryptographically secure credentials issued to individuals and stored in their digital wallets. These can be presented offline or online to service providers for verification, without requiring live connectivity to the central system—ideal for decentralized or low-connectivity environments.

Both approaches will operate under the national Trust Framework and managed through SevisAdminPortal, which ensures privacy, consent, data minimization, and interoperability. Service

providers can choose the approach best suited to their operational context, ensuring both inclusiveness and flexibility in adoption.

4. Management: The lifecycle includes ongoing activities such as:

- Credential updates (e.g., address, name changes)
- Lost or compromised credentials (revocation and reissuance)
- Grievance redressal and user support via contact centres and partner touchpoints
- Monitoring and Evaluation (M&E) of system performance, adoption, and inclusion metrics (see Section 8)
- Stakeholder engagement to align ongoing ecosystem needs and innovation

These functions will be overseen by the Digital ID Implementation Authority, with robust logging, auditability, and service-level monitoring.

The following diagram illustrates the key stages of the Digital ID lifecycle—spanning registration, issuance, use, and management—adapted from the ID4D Practitioner's Guide, to reflect the operational and governance model envisioned for SevisPass.

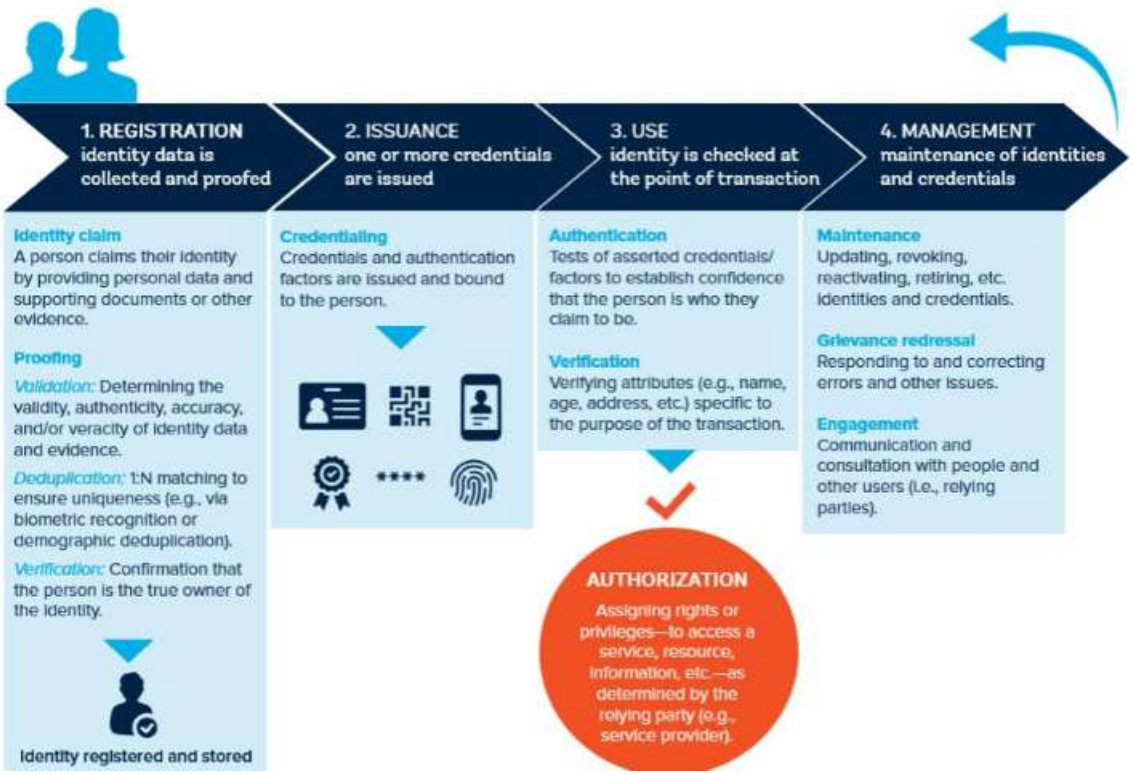

Figure 4: Stages of Digital ID Lifecycle (Adapted from Digital Identity: Public and Private Sector Cooperation and Technology Landscape for Digital), World Bank. 2019. ID4D Practitioner' Guide: Version 1.0 (October 2019).

6.2 Technology Backbone and System Architecture

The SevisPass Digital ID platform will be developed with the following foundational goals:

- Trusted national identity platform: SevisPass will be the de facto identity for accessing government and regulated services, backed by robust verification, authentication, and audit trails.

- Multiple enrolment pathways: To address low ID ownership and mobile penetration, both self-service registration and field-based assisted enrolment will be supported.
- Layered digital identity lifecycle:
    - Self-registration with an existing ID (e.g. voter ID, NID, driver's license) to generate a tracking number
    - Generation of a provisional digital ID number upon basic validation
    - Finalization into a full digital ID upon biometric enrolment and deduplication

  Layered identity lifecycle and different enrolment pathways are depicted in Figure 5.
- Privacy, security, and deduplication: The backend will support biometric deduplication, secure authentication, and issuance of verifiable credentials using open standards.
- Future-ready architecture: Modular and standards-based, AI-ready infrastructure will support eKYC, offline authentication, and cross-agency interoperability through SevisDEx while provisioning for fraud management, enhanced security and future technology adoption.

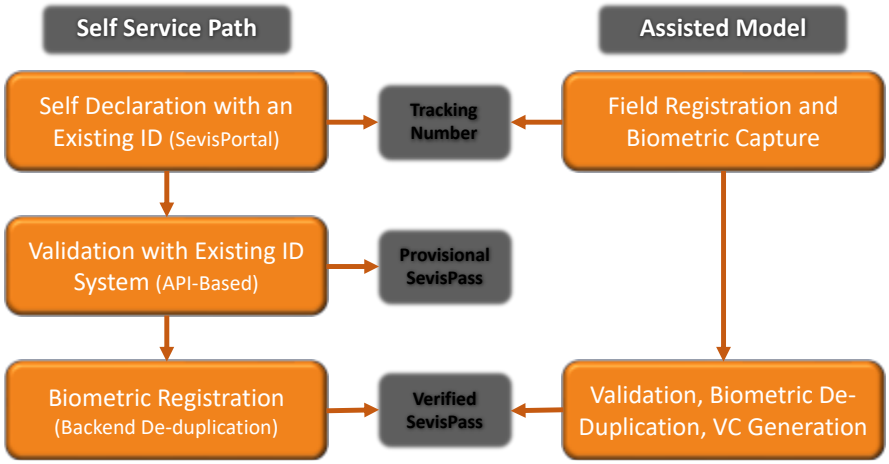

Figure 5: Designing for Multiple Pathways and Layered Digital ID Lifecycle

Further technical specifications, procurement planning, and systems integration will be detailed in the Implementation Plan document.

6.3 Inclusive and Federated Enrolment Approach

The enrolment strategy for SevisPass will follow a multi-channel and partner-driven approach to ensure wide and rapid coverage of the population, including underserved and remote communities. It will be based on federated enrolment model to maximize reach and efficiency while maintaining quality and trust. The following diagram highlights this approach, where the Digital ID Authority provides oversight while trusted partner agencies mobilize field infrastructure and personnel to ensure inclusive, community-level enrolment.

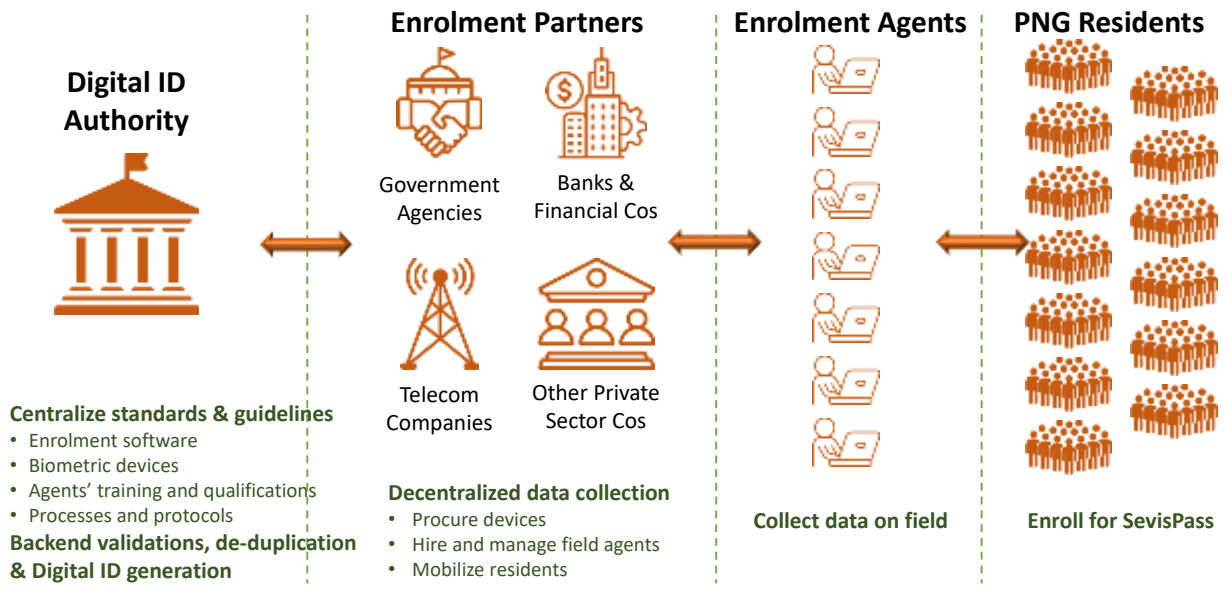

Figure 6: Federated Enrolment Implementation Model

Enrolment activities will be conducted in partnership with government agencies, financial institutions, telecom providers, civil society, and other authorised entities, leveraging their existing infrastructure and outreach capabilities. These enrolment partners will be onboarded through formal agreements and supported by clear guidelines on data handling, identity validation, and adherence to security and inclusion standards.

Enrolment partners are institutional entities responsible for planning and managing the operational aspects of field enrolment. Their responsibilities include procuring devices, hiring and supervising enrolment agents, mobilizing residents, and overseeing enrolment centre operations in accordance with the standards and guidelines provided by the Digital ID Implementation authority. Enrolment agents are trained personnel deployed by enrolment partners to directly interact with residents and carry out the capture of demographic and biometric data in accordance with established standards and procedures.

This strategy ensures:

- Inclusive access and choice to residents even in remote or underserved areas
- Lower cost and faster coverage through distributed operations
- Multiple enrolment pathways, including**:**
    - Self-service registration using existing ID credentials (where available), followed by digital validation and biometric capture.
    - Assisted enrolment through partner agencies and designated enrolment centres.
    - Field-based mobile enrolment to reach rural and hard-to-access populations.

All enrolment efforts will be governed by centrally defined standards for:

- Biometric and demographic data quality
- Enrolment software and security protocols
- Deduplication and backend verification
- Training / certification criteria and compliance frameworks for all authorized enrolment partners

All enrolment partners will be required to adhere to these standards to be eligible to participate in the SevisPass ecosystem. This central quality assurance mechanism will ensure that, despite the decentralized nature of field enrolment, the digital ID system remains robust, interoperable, and trustworthy across all sectors and regions of PNG.

6.3.1 Phased Rollout Strategy

Enrolment rollout will be done in three phases, with priority given to establishing core identity services and demonstrating quick wins.

Phase	Timeline	Key Milestones	Target Population
Phase 1: Foundational Setup	Months 0–6	• Launch self-service portal for provisional registration • Establish provisional ID issuance process • Finalize system design for deduplication backend	Urban areas and individuals with existing IDs
Phase 2: Pilot and Field Enrolment	Months 6–12	• Launch field enrolment (biometric kits) • Deploy deduplication system • Begin full SevisPass issuance • Start testing eKYC APIs with pilot agencies	Selected provinces, beneficiaries of priority services
Phase 3: Scale-up and Ecosystem Integration	Months 12–24	• Full national rollout • eKYC integration across banks, telcos, government agencies • Additional credentials added to SevisWallet	National coverage, prioritizing low-ID and rural populations

Further details on the implementation roadmap and activities across multiple workstreams are covered in Section 10.

6.4 Usage of SevisPass by Different Sectors

SevisPass will function as a single, trusted, and interoperable digital credential enabling seamless access to a wide range of services across financial, telecommunications, government, health, education, insurance, and digital platforms. By reducing identity-related friction and establishing a consistent trust layer, SevisPass will significantly accelerate digital service adoption across sectors. It will support multiple authentication modalities—such as biometric, mobile, offline, and password/PIN-based mechanisms—while incorporating accessibility features such as multilingual interfaces and disability-friendly design. These inclusive capabilities are critical to reaching underserved, rural, and marginalized populations. In conjunction with SevisDEx, SevisPass will underpin a scalable and consent-based ecosystem for secure identity verification and data sharing, driving widespread adoption and trust in PNG's digital public infrastructure.

The unique ID authentication and eKYC system will use open standards and APIs to ensure SevisPass credentials are interoperable with public and private sector systems, enabling seamless integration with services like banking, healthcare, and eGovernment platforms. This standards-based approach lays the technical foundation for SevisDEx which will facilitate secure, consent-based, and auditable data sharing between trusted institutions. Together, SevisPass and SevisDEx will enable a robust digital ecosystem, accelerating the adoption of digital ID across sectors and ensuring that identity-linked services are both accessible and accountable.

6.4.1 First Use Case: eKYC for Financial and Government Services

The first major use case for the digital ID platform will be to enable electronic Know Your Customer (eKYC) verification for banks, mobile money providers, and government schemes. This will:

- Reduce onboarding friction in the formal financial system, especially for the unbanked
- Enable faster benefit delivery and identity validation across government services
- Lay the foundation for wider adoption of SevisPass as a unified identity across sectors

eKYC services will be governed by user consent or legal mandates, depending on the context (e.g. explicit consent for account opening, regulatory access for law enforcement). Technical and policy enablers such as standard APIs, authentication protocols, and regulatory guidelines for KYC will be developed.

In addition to improving service efficiency and inclusion, the deployment of SevisPass-enabled eKYC will support PNG's compliance with international standards such as the FATF Recommendations. By enabling robust, risk-based customer due diligence and digital audit trails, SevisPass – along with SevisDEx – strengthens the national AML/CFT regime and enhances financial integrity. The identity assurance and verification mechanisms will also align with regulatory expectations around non-face-to-face onboarding and digital financial services.

6.4.2 Subsequent Use Cases Based on Authentication Services

Building on the initial rollout of eKYC, SevisPass will enable a wide array of advanced authentication use cases across public and private sectors. By serving as a unified, secure, and interoperable digital identity, SevisPass will reduce the fragmentation caused by siloed identity systems, lower user friction, and enhance trust in digital service delivery.

As authentication capabilities evolve—including biometric, mobile, offline, and device-based modalities—SevisPass will support both real-time and offline use cases, facilitated through SevisAdminPortal and SevisDEx. This will promote seamless integration of identity verification into diverse workflows, enabling digital transformation across PNG's key sectors.

Examples of downstream authentication-based use cases include:

- Government System Integration & Data Integrity
    - Linking SevisPass to existing government databases to perform demographic and biometric authentication.
    - Enabling large-scale deduplication and validation of records to eliminate ghosts, duplicates, and fake entries in programs such as voter rolls, civil registries, and beneficiary databases.
- Proof of Presence & Service Eligibility
    - Biometric or device-based proof of presence for verifying attendance at schools, training programs, public employment schemes, or examinations.
    - Authentication for receipt of subsidies, food rations, pensions, and other entitlements, ensuring benefits reach the intended recipients.
- Cross-Domain Linkage & Analytics
    - Use of the unique ID as a common identifier across databases to enable better policy targeting, fraud detection (e.g., duplicate scholarships, tax avoidance), and unified service delivery.
    - Enable longitudinal data tracking for individual welfare outcomes such as education history, immunization records, or job placement results.

- Age-Based and Contextual Access Control
  - Age verification for accessing restricted platforms (e.g., social media), or claiming age-specific benefits such as youth scholarships or senior citizen pensions.
  - Tailored service access based on verified identity attributes (e.g., region, gender, disability status).
- Digital Signature & Transaction Authentication
  - Enabling SevisPass-based digital signatures for secure online transactions such as filing taxes, business licensing, signing contracts, and accessing legal services.
  - Supporting digital notarization or consent for critical life events like marriage registration, property transfer, and inheritance claims.
- Single Sign-On (SSO) for Government Services
  - Providing one-click access across government apps, portals, and service platforms via SevisPass-backed OTP or biometric authentication.
  - Reducing password fatigue and enabling inclusive access through multilingual and disability-friendly user interfaces.

Together, these use cases demonstrate how SevisPass, underpinned by the Trust Framework and SevisDEx, will unlock scalable, privacy-preserving, and inclusive digital service delivery. As more services integrate with SevisPass for authentication, the platform will catalyze PNG's digital public infrastructure and digital economy ambitions.

6.5 Federated Authentication and Service Adoption Model

The adoption and use of SevisPass for authentication across sectors will follow a federated operating model, enabling secure, scalable, and inclusive service delivery while maintaining decentralization and autonomy for individual institutions. The approach is underpinned by PNG's broader Trust Framework, which defines the legal, technical, and governance rules for all participating entities in the digital identity and credential ecosystem.

In this model, **trusted entities**—such as government departments, financial institutions, telecom providers, and regulated private actors—act as **relying parties**. They integrate SevisPass authentication services into their workflows, using standardized protocols defined by the Trust Framework. The Digital ID Authority provides authentication as a service, acting as the trust anchor for verifying identity assertions, without becoming a data controller for the transactions themselves.

To support this model, the following components play a central role:

- SevisDEx: Enables secure, policy-based data sharing between the Digital ID system and authorized service providers. It ensures interoperability, data minimization, and auditability in every transaction involving authentication or credential verification.
- SevisAdminPortal: Acts as the control panel for onboarding, certifying, and managing relying parties. Through this portal, the Digital ID Authority can issue access credentials, monitor usage, manage incident reports, and enforce compliance with authentication assurance levels and sectoral agreements.
- Trust Framework: Establishes the foundational policies—including assurance levels, consent protocols, liability allocation, and technical standards—that all participants in the ecosystem must comply with. It provides legal legitimacy, institutional clarity, and governance mechanisms to ensure accountability and alignment across the federated network.

The following diagram illustrates this model, where the Digital ID Authority enables authentication and data verification through a central platform, while various public and private sector agencies adopt SevisPass for secure user identification and service delivery.

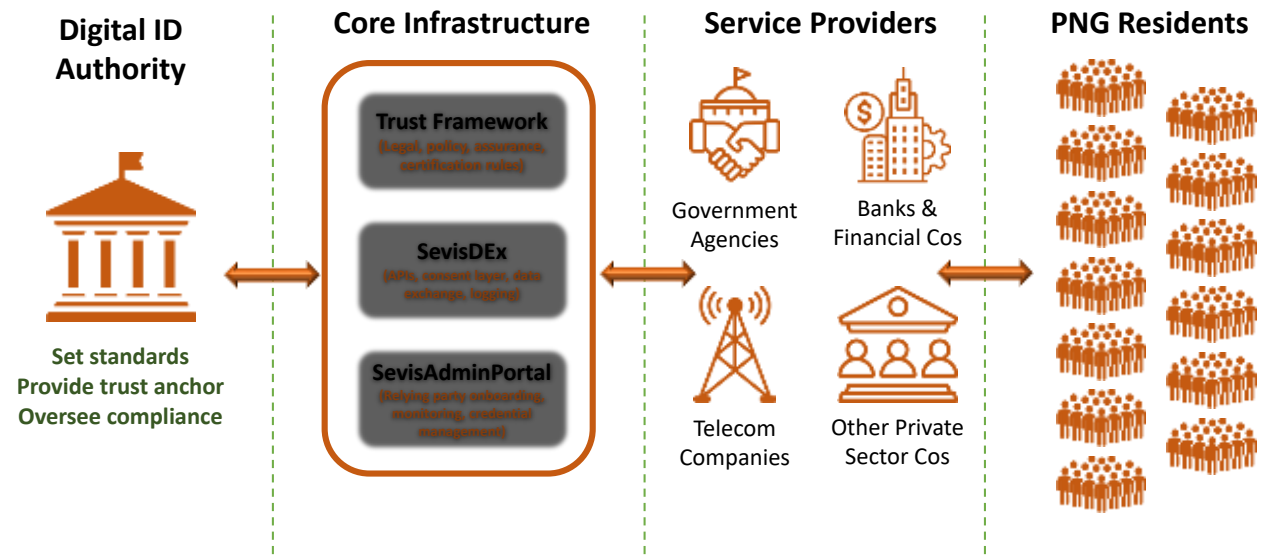

Figure 7: Federated Authentication and Service Adoption Model for SevisPass

This federated strategy enables:

- Rapid integration across sectors, through open APIs and a modular architecture governed by the Trust Framework.
- User-centric authentication, allowing residents to authenticate using biometrics, PINs, device-based credentials, or federated logins, depending on assurance level and context.
- Interoperable and inclusive service delivery, especially for remote or underserved populations.
- Distributed innovation, where each sector can independently adopt, innovate, and scale services based on common identity standards.

Adoption and authentication activities will be governed by clearly defined policies and procedures for:

- Authentication assurance levels and credential types
- Consent, data protection, and non-repudiation mechanisms
- Logging, monitoring, and redressal procedures
- Certification and lifecycle management of all relying parties

Together, the Trust Framework, SevisDEx, and SevisAdminPortal ensure that the SevisPass ecosystem remains resilient, inclusive, and trusted—while enabling secure and accountable identity usage across PNG's digital economy.

6.6 Pricing and Charging Policy

The Digital ID system shall be designed as a public good, with core enrolment and identity issuance services provided free of charge to all residents. Authentication and verification services may be priced in a regulated and transparent manner to enable ecosystem participation by commercial verifiers. Pricing shall be guided by principles of affordability, non-exclusion, and cost recovery, with oversight by the designated regulatory agency and subject to periodic review.

7. Risk Management and Mitigation Strategy

The long-term success and resilience of Papua New Guinea's digital identity ecosystem—anchored by SevisPass, verifiable credentials, and the broader trust framework—hinges on its ability to proactively identify, assess, and manage a wide range of risks across legal, institutional, technological, and user domains. Effective risk management is not merely a safeguard but a strategic enabler of inclusion, trust, interoperability, and regulatory compliance. This section categorizes the critical risks across six domains and presents mitigation strategies embedded within the overall governance, implementation, and monitoring framework. It also reinforces the need for continuous risk reassessment and adaptive management, ensuring the digital identity system remains secure, inclusive, and responsive to evolving threats and user needs.

7.1 Institutional and Governance Risks

Risk: Lack of clarity in mandates, poor inter-agency coordination, or delays in legal/policy approvals could hamper implementation.
Mitigation:

- Clearly define roles across implementing, regulatory, and coordinating institutions.
- Formalize inter-agency coordination through steering committees and MoUs.
- Establish phased legal instruments aligned with rollout milestones.
- Ensure political buy-in through regular reporting and oversight.

7.2 Technology and Security Risks

Risk: System vulnerabilities, cyberattacks, or infrastructure failures could undermine trust and service continuity.
Mitigation:

- Implement security-by-design principles including multi-factor authentication, encryption, and zero-trust architecture.
- Establish disaster recovery, failover systems, and offline credentialing mechanisms.
- Conduct third-party security audits and penetration testing periodically.
- Conduct regular vulnerability assessments and implement a structured vulnerability disclosure process to ensure timely detection, reporting, and resolution of security flaws.

7.3 Digital Exclusion and Accessibility Risks

Risk: Remote, low-literacy, and marginalized populations may face barriers to enrolment or usage.
Mitigation:

- Adopt federated enrolment models with local partners, including community-based organizations.
- Enable offline, biometric-optional credential issuance and authentication.
- Provide mobile, multilingual, and assisted user interfaces.
- Ensure disability-inclusive and gender-sensitive design standards.

7.4 Data Protection and Privacy Risks

Risk: Misuse, unauthorized sharing, or breach of personal data could lead to loss of public trust.
Mitigation:

- Implement privacy-by-design frameworks, with user consent, data minimization, and role-based access.
- Establish independent data protection oversight (aligned with future data protection legislation).
- Incorporate strong audit trails and redress mechanisms.
- Limit data retention and mandate deletion policies in line with use-case purposes.

7.5 Ecosystem and Vendor Lock-in Risks

Risk: Over-reliance on a few providers or non-interoperable systems may restrict ecosystem innovation or sustainability.
Mitigation:

- Adopt open standards and vendor-neutral APIs.
- Encourage local ecosystem development and capacity building.
- Use public-private sandbox mechanisms for innovation and testing.

7.6 Implementation and Adoption Risks

Risk: Resistance to change, lack of institutional capacity, or inadequate awareness could delay rollout or lower uptake.
Mitigation:

- Implement a phased and adaptive rollout strategy based on readiness and feedback loops.
- Develop detailed change management and training programs for key implementing agencies.
- Launch nationwide digital literacy and awareness campaigns.
- Monitor adoption metrics and iterate based on M&E feedback.

8. Monitoring, Evaluation, and Continuous Improvement

The success of the Digital ID ecosystem depends on continuous assessment, adaptability, and stakeholder feedback. This section outlines how PNG's Digital ID program—anchored by SevisPass and the Trust Framework—will be monitored, evaluated, and improved over time to ensure it remains secure, inclusive, and impactful. This will include defining performance indicators, establishing regular feedback loops, leveraging data for course correction, and involving independent oversight.

8.1 Objectives and Principles

To ensure accountability and alignment with national priorities, the Monitoring & Evaluation (M&E) function will:

- Track progress toward key policy outcomes including inclusion, trust, service delivery, and compliance.
- Promote transparency and data-driven decision-making across implementing agencies.
- Enable proactive identification of risks, bottlenecks, and areas requiring corrective action.
- Uphold principles of inclusion, privacy, responsiveness, and accountability.

8.2 Indicators and Success Metrics

M&E will be guided by a structured set of qualitative and quantitative indicators across five pillars: Coverage, Usage, Trust, Governance, and Impact.

Key indicators could include:

- **Coverage & Inclusion**
  - % of population issued with SevisPass (disaggregated by gender, geography, age, disability)
  - % of remote or rural registrations
- **Usage**
  - Number of digital authentications completed monthly via SevisPass
  - Number of services accessed using SevisPass or verifiable credentials
- **Trust & Security**
  - Number of security incidents or breaches reported and resolved
  - % of users reporting confidence in privacy and control over their data
- **Governance & Compliance**
  - % of credential issuers onboarded and verified through Trust Registry
  - Compliance with KYC/eKYC regulatory requirements by financial institutions
- **Impact**
  - Reduction in identity-related fraud
  - Time and cost saved per transaction across key services

Indicators will be reviewed and updated periodically based on evolving priorities.

8.3 Feedback Loops and Data-Driven Improvement

The system will integrate real-time and periodic feedback loops to capture user experiences, operational data, and systemic challenges:

- User surveys at service delivery touchpoints and digital platforms.
- Analytics dashboards monitoring adoption and error rates.
- Feedback integration into product and policy updates.
- Use of pilot programs and sandbox environments for testing and iteration.

This agile feedback mechanism will support continuous improvement in digital ID features, authentication services, and data-sharing protocols.

8.4 Independent Reviews and Audits

Independent oversight is vital for maintaining credibility and long-term sustainability:

- Third-party evaluations every 2–3 years to assess performance, privacy safeguards, and ecosystem health.
- Security and privacy audits for compliance with regulatory and cybersecurity standards.
- Parliamentary or public reporting on key outcomes and risks.
- Annual publication of an Accountability Scorecard against M&E indicators.

These reviews will inform governance evolution and capacity-building priorities.

8.5 Role of Stakeholders in M&E

M&E processes will be inclusive, participatory, and multistakeholder:

- Policy-makers: Use M&E data to guide reforms, budget allocation, and alignment with Vision 2050.
- Implementing agencies: Track operational progress and adopt improvements.
- Private sector and ecosystem actors: Share performance data (e.g., eKYC usage) and receive compliance feedback.
- Civil society and citizens: Provide feedback through structured forums and grievance mechanisms.

A Stakeholder M&E Advisory Group may be formed under the Central Coordinating Body to support transparency and collaboration.

8.6 Integration with Implementation Roadmap

M&E will be embedded into the implementation roadmap with:

- Baseline assessment before Phase 1 rollout.
- Periodic milestones aligned with each rollout phase (e.g., registration, wallet launch, ecosystem onboarding).
- Mid-term review aligned with SevisPass scale-up.
- Institutionalization of M&E functions within the SevisAdminPortal governance structure.

M&E timelines, tools, and accountability mechanisms will be included in the SevisPass Implementation Toolkit and reviewed annually.

8.7 M&E Framework

To ensure the Digital ID ecosystem delivers on its intended outcomes and evolves based on real-world performance, a robust M&E framework will be institutionalized. This framework will track key metrics across implementation phases, provide actionable insights to guide continuous improvement, and enable transparent accountability to stakeholders.

The proposed framework outlines core dimensions, indicators, and data sources to support data-driven governance and adaptive policy implementation.

Dimension	Indicators	Measurement Methods	Primary Data Sources	Key Stakeholders / Data Users
System Coverage & Reach	% of adult population enrolled % of marginalized groups enrolled	Enrolment analytics dashboard Demographic breakdowns Field verification studies	SevisPass enrolment data National census Surveys	DICT, Civil society, Financial regulators, Inclusion watchdogs
Inclusion & Accessibility	% enrolment from rural areas Disability-inclusive access Offline credential usage	Analytics from mobile/offline usage Accessibility audits Focus group feedback	Enrolment dashboards Accessibility reports NGO/civil society feedback loops	DICT, Disability commissions, Civil society, Human rights institutions

Service Uptake & Usage	Number of authentications per month Credentials used across sectors	SevisDEx usage logs Sectoral transaction logs Cross-sectoral service delivery dashboards	SevisDEx logs Government service portals Financial institutions' KYC logs	Service ministries, Banks, Fintechs, Civil society observers
User Satisfaction	% users reporting ease of use Grievance resolution time	Digital and paper-based user surveys Grievance redress analytics Call centre logs	Grievance portal User surveys Feedback from community orgs and NGOs	DICT, Redress bodies, Civil society, Community organisations
System Integrity & Security	# of reported fraud incidents % successful verifications	Security incident dashboards Audit reports Biometric performance tests	SevisAdminPortal security logs CERT reports 3rd party audits	NICTA, Security agencies, Regulatory authorities, Civil society observers
Regulatory Compliance	Alignment with FATF standards Compliance with data protection laws	KYC audit results Regulatory inspections Credential revocation patterns	Bank compliance reports SevisAdminPortal audit trails Data Protection Office assessments	Central Bank, Data Protection Authority, Sector regulators, Civil society
Institutional Readiness	% institutions integrated Onboarding time Training coverage	Integration logs Helpdesk and support data Capacity-building tracking systems	SevisAdminPortal integration logs Training databases Onboarding records	DICT, Implementing ministries, Development partners

9. Legal and Regulatory Framework

This section proposes for a robust legal and regulatory foundation to support the establishment, implementation, and sustainability of PNG's Digital ID System**,** including SevisPass, future verifiable credentials (e.g., digital driver's licenses, passports, student IDs), and various components of Trust Framework. This framework ensures alignment with the Digital ID Trust Framework, national legislation (e.g., AML/CTF Act 2015**, Civil and Identity Registration Act 2024,** Digital Government Act 2022), and global best practices (e.g., GovStack ID Building Block Framework). It addresses PNG's challenges, such as fragmented identity records, limited digital infrastructure, and rural accessibility, by proposing amendments to existing laws, introducing new regulations, and establishing governance mechanisms to foster a secure, inclusive, and interoperable digital identity ecosystem.

9.1 Objectives and Principles

The legal and regulatory framework for Digital ID in PNG is guided by the following objectives:

- Ensure legal recognition of Digital ID and SevisPass across public and private sectors.
- Protect individual rights, especially privacy, consent, and data protection.
- Enable trust and legal accountability through enforceable obligations for all actors.
- Promote interoperability, competition, and innovation through open standards and accreditation.

- Facilitate inclusion by establishing a legal mandate for equitable access to identity and authentication services.

These objectives are grounded in the broader goals of PNG's Digital Government Act (2022), the Digital Transformation Policy (2020), Medium Term Development Plan 2023 – 2027, Vision 2050, and the Lagatoi Declaration by Pacific ICT Ministers.

9.2 Assessment and Amendment of Existing Legislation

To enable the Digital ID System, relevant legislation shall be assessed, reviewed, and amended to formalize the roles of key entities, ensure compliance with the Digital ID Trust Framework, and support the policy's objectives of secure identity verification, interoperability, and inclusion. The Department of Justice and Attorney General shall lead the review process in collaboration with the DICT and the NICTA**,** with amendments proposed within 12 months of policy adoption.

9.2.1 National Information and Communication Technology Act 2009

The National Information and Communication Technology Act 2009 governs ICT regulation but lacks provisions for overseeing a national digital identity system, including regulatory authority for the Digital ID System and enforcement of the Digital ID Trust Framework.

The following amendments are proposed:

- Introduce a new part to designate the incumbent ICT and digital industry regulator as the Digital ID Regulatory Authority**,** granting it powers to enforce the Digital ID Trust Framework, conduct audits, and impose penalties for non-compliance.
- Delegate authority to the Digital ID Regulatory Authority to define standards for registration, issuance, usage, and data management within the Digital ID System, aligning with ISO/IEC 27001 (cybersecurity) and ISO/IEC 19794 (biometric data).
- Establish legal provisions for accrediting Verifiable Credentials Providers (e.g., General-Purpose credentials, Private Sector credentials, Professional credentials, Superannuation Fund credentials) and regulating their operations, ensuring interoperability and compliance with open standards.
- Establish enforcement mechanisms over data custodians and VC providers.
- Mandate cybersecurity protocols, including vulnerability assessments and incident reporting, to protect the SevisPass and the Trust Framework.

9.2.2 Digital Government Act 2022

The Digital Government Act 2022 mandates digital transformation but does not explicitly address the governance of a national digital identity system or the roles of entities like the Digital ID Implementation Authority**.**

The following amendments are proposed:

- Formalize DICT's role as the Policy Authority and the designation framework for the Digital ID Implementation Authority (Special Purpose Vehicle), with clear mandates for developing and managing the SevisPass and Trust Framework.
- Incorporate the establishment of a multi-stakeholder governance body, including DICT, NICTA, BPNG, FASU, PNGCIR, and private sector representatives, to oversee Digital ID System implementation.
- Mandate the use of SevisPass and Trust Framework for single sign-on (SSO) in government-to-government (G2G) and government-to-citizen (G2C) platforms, such as SevisPortal, to streamline service delivery.

The legislative outcome will be to reinforce DICT's leadership and the designation framework for the SevisPass and Trust Framework, ensuring governance and scalability of the Digital ID System.

9.2.3 Other Relevant and Complementary Acts

To operationalize the Trust Framework and accelerate broader digital transformation, a comprehensive review and harmonization of sectoral legislations will be required. This includes Acts governing key identity-issuing and service delivery agencies such as (but not limited to) PNGCIR, ICSA, RTA, BPNG, and other sectoral regulators and institutions.

Proposed legal amendments and provisions should aim to:

- Recognize SevisPass and the Trust Framework as legally valid identity instruments for customer onboarding, service delivery, and regulatory compliance.
- Enable sectoral agencies to issue digitally verifiable credentials that are integrated with the SevisPass ecosystem and accessible via SevisWallet.
- Permit secure, consent-based interoperability between agency databases through SevisDEx aligned with tiered Customer Due Diligence (CDD) protocols.

- Mandate the adoption of standardized data formats, secure APIs, and encryption protocols to ensure safe, interoperable exchange in line with the National Data Governance and Protection Policy, 2024.

These legislative enhancements will institutionalize the role of participating agencies as both **contributors to** and **beneficiaries of** the Trust Framework, thereby advancing financial and social inclusion, improving regulatory oversight, and enabling an ecosystem-wide shift toward digital governance and service delivery.

9.3 Development of New Regulations

To complement amendments, new regulations shall be developed under the Digital Government Act 2022 and National Information and Communication Technology Act 2009 to operationalize the Digital ID System while provisioning for and ensuring compliance of the Digital ID Trust Framework**.**

9.3.1 Digital ID System Regulations

- Purpose: Provide detailed rules for the operation, governance, and compliance of the Digital ID System, including SevisPass and future verifiable credentials.

- Key Provisions**:**
  - Define standards for registration, issuance, usage, and data management, aligning with the Digital ID Trust Framework and global standards
  - Establish procedures for accrediting Digital ID Providers, including eligibility criteria, security requirements, and audit obligations.
  - Mandate user consent and data minimization principles for all data collection and sharing, in compliance with the National Data Governance and Protection Policy 2024.
  - Outline penalties for non-compliance, including fines, system access restrictions, or license revocation for custodians, providers, or service providers.

- Outcome: Ensure operational clarity and regulatory enforcement for the Digital ID System, fostering trust and scalability.

9.3.2 Data Protection and Privacy Regulations

- Purpose: Strengthen data protection measures to safeguard personal and biometric data within the Digital ID System, addressing concerns about identity theft and misuse.

- Key Provisions:
  - Mandate privacy-by-design principles, requiring encryption, secure storage, and audit trails for all personal and biometric data, aligning with international standards such as ISO/IEC 27001.
  - Establish user rights, including the right to access, correct, or delete personal data, and require informed consent for data sharing, in compliance with the National Data Governance and Protection Policy 2024.
  - Require custodians and providers to implement cybersecurity protocols, including regular vulnerability assessments and incident response plans, as per the National Cybersecurity Policy 2021 and Strategy 2024.
  - Authorize Digital ID Regulatory Authority to conduct quarterly audits of accredited partners, with mandatory reporting of security incidents to DICT and affected users.

- Outcome: Enhance public trust in the Digital ID System by ensuring robust data protection and privacy safeguards.

9.3.3 Inclusion and Accessibility Regulations

- Purpose: Ensure the Digital ID System is accessible to all citizens, particularly rural and marginalized communities, addressing low internet penetration and fragmented identity records

- Key Provisions**:**
  - Mandate accessible registration and issuance channels, including mobile units, offline authentication, and disability-friendly interfaces, for SevisPass and other credentials.
  - Require custodians and providers to offer multilingual support and culturally appropriate processes to accommodate PNG's diverse population
  - Establish funding mechanisms, via public-private partnerships, to support infrastructure development in rural areas, aligning with the Digital Government Plan 2023–2027.

- Outcome**:** Promote universal coverage and equitable access to the Digital ID System, supporting inclusion objectives.

9.4 Legislative and Regulatory Timeline

The development and enactment of legislative amendments and new regulations shall align with the phased implementation roadmap outlined in Section 10 to ensure timely legal support for the Digital ID System.

- *Phase 1: Foundation (0–6 Months)**:***
  - Objective**:** Initiate legislative review and draft amendments to support core infrastructure and governance.

  - Activities**:**

        - Department of Justice, DICT, and NICTA conduct a comprehensive review of existing legislation (National Information and Communication Technology Act 2009, Civil and Identity Registration Act 2024, Central Banking Act 2000 etc.) to identify gaps.
        - Propose amendments to formalize roles of DICT, NICTA, KTDC, PNGCIR, ICA, RTA, BPNG, and FASU, with drafts submitted to Parliament within 12 months.
        - Begin drafting Digital ID System Regulations to define operational standards and compliance measures.

    - Deliverables: Legislative review report, draft amendments, initial regulatory framework.

- *Phase 2: Expansion (6-18 Months):*
    - Objective: Enact amendments and finalize new regulations to support SevisPass scaling and credential integration.

    - Activities:
        - Parliament enacts amendments to National Information and Communication Technology Act 2009, Civil and Identity Registration Act 2024 Immigration and Citizenship Service (Amendment) Act 2021, Road Traffic Act 2014, AML/CTF Act 2015, and Digital Government Act 2022.
        - NICTA and DICT finalize and gazette Digital ID System Regulations, Data Protection and Privacy Regulations, and Inclusion and Accessibility Regulations, following public consultation.
        - Establish a legal framework for accrediting Digital ID Providers and integrating financial registries for Enhanced CDD.

    - Deliverables: Enacted amendments, gazetted regulations, accredited partner framework.

- Phase 3: Consolidation and Innovation (18–36 Months):
    - Objective: Review and refine legislative framework to support universal coverage and new credentials.

    - Activities:
        - Conduct a post-implementation review of amended legislation and regulations to assess effectiveness and address gaps, aligning with the two-year policy review cycle.
        - Propose additional amendments to support new verifiable credentials (e.g., health insurance cards, voter IDs) and cross-border interoperability.
        - Strengthen enforcement mechanisms, including penalties for non-compliance, based on Digital ID Regulatory Authority's audit findings

    - Deliverables: Legislative review report, refined regulations, enhanced enforcement mechanisms.

9.5 Governance and Oversight Mechanisms for Legislative Reforms

Effective implementation of legal and regulatory reforms requires a structured governance framework. The following mechanisms are proposed:

- **Designated Lead Regulator:** Either NICTA or a newly created body will serve as the Digital ID Regulatory Authority responsible for licensing, audit, and compliance enforcement.
- **Inter-Agency Legal Working Group:** Comprising Department of ICT, Department of Justice and Attorney General, NICTA, CRVS, BPNG, IRC, and civil society representatives to steer the legislative reform agenda.
- **Parliamentary Oversight:** Regular briefings and policy updates to the Parliamentary Committee on ICT and Governance to ensure accountability and alignment with national development goals.
- **Stakeholder Consultations:** Ongoing consultations with financial institutions, telecom operators, civil society, legal experts, and provincial governments to validate proposed changes and ensure inclusivity.

9.6 Regulatory Compliance and Enforcement Mechanisms

Establishing effective enforcement mechanisms is key to ensuring legal and ethical compliance. These include:

- Regular audits of implementing agencies and private actors
- Regulatory sandboxes for new use cases (e.g., fintech, health ID)
- Licensing and accreditation regimes for authentication and credentialing services
- Penalties for non-compliance with data protection and identity governance rules Mechanisms will also include grievance redressal for rights violations, backed by independent review and judicial oversight.

10. Implementation Roadmap

The implementation of the SevisPass Trust Framework will be structured around the coordinated rollout of multiple DPI components, i.e., SevisPass (digital ID), SevisPortal (resident interface), SevisWallet (VC storage), SevisAdminPortal (administration and trust registry), SevisDEx (data exchange and eKYC), and authentication services. Along with these, the roadmap also includes readiness of institutional and legal frameworks, grievance redressal systems, monitoring and evaluation framework and sectoral onboarding.

Each component will be introduced progressively, with overlapping workstreams and a phased national scale-up. Following are the quarterly milestones planned. A detailed workstream-wise, quarter-wise list of milestones is presented in the Annexure.

Quarter	Key Milestones
Q1 (Months 1–3)	• Establish Governance Structure and Institutional Roles (Regulatory and Implementation authorities) • Finalize Digital ID Policy Document and implementation approach • Begin development of MVPs for SevisPass, SevisWallet, SevisAdminPortal • Finalize technical architecture and initiate procurement for tech platforms and devices • Design minimal SevisDEx for document-based identity validation • Design SevisPortal UX and onboarding features • Draft eKYC standards and onboarding protocol for financial sector
Q2 (Months 4–6)	• Draft and initiate approval process for SevisPass legal and regulatory framework • Conduct regulatory gap assessment (e.g., for data sharing, privacy, authentication)

	• Begin drafting legal amendments or supporting regulations as needed • Notify core policy instruments, including partners' accreditation criteria and governance model • On-board technology partners for different DPI components • Launch provisional SevisPass with validation against existing ID documents • Launch MVPs for SevisPass, SevisPortal, SevisWallet, SevisAdminPortal • Operationalize SevisDEx with basic capabilities for provisional SevisPass issuance
Q3 (Months 7–9)	• Develop draft MoU and contract templates for partner onboarding (enrolment, eKYC, data exchange • Establish inter-agency coordination mechanism (e.g., Steering Committee and Technical Working Groups) • Finalize and notify compliance and audit standards for accredited partners • Document and notify processes and standard operating procedures (SOPs) to be followed by accredited partners for field operations • Pilot biometric enrolment in select regions with early accredited partners • Launch operational dashboards for enrolment tracking • Begin onboarding of financial institutions for eKYC and SevisDEx • Deploy first version of grievance redressal mechanism • Develop M&E framework and field monitoring baseline • Finalize communication and mass outreach plan • Begin awareness and digital literacy campaigns • Initiate ecosystem capacity building exercise
Q4 (Months 10–12)	• Scale enrolment operations with multiple partners • Start onboarding of social sector agencies and service partners • Expand SevisPass use cases and issue credentials beyond pilots • Introduce basic authentication services (e.g., biometric, OTP) • Strengthen SevisDEx integrations and begin transactional data flow testing • Launch structured M&E field assessments and feedback loops • Mass campaign and awareness for SevisPass ecosystem and Trust Framework
Q5 (Months 12–15)	• Review and refine enrolment, authentication, and eKYC services including offline capabilities • Expand SevisWallet to support multiple credential types (e.g., education, civil registry) • Strengthen SevisPortal features (e.g., wallet management, VC download, consent history) • Expand grievance redressal to include escalation workflows and agent-based support • Institutionalize governance mechanisms and compliance audits for Trust Framework • Validate pricing model and sustainability scenarios • Initiate a cybersecurity audit of the Trust Framework implementation
Q6–Q8 (Months 16–24)	• Nationwide rollout of SevisPass enrolment • Continued partner onboarding across sectors (health, education, transport, social protection) • Enable broader SevisDEx integrations (civil registry, tax, licensing) • Rollout AI-supported fraud monitoring, analytics, and case tracking • Institutionalize grievance and redress dashboards with M&E linkages • Ongoing training and capacity-building across ecosystem

11. Annexure

11.1 Acronyms

Acronym	Full Form
ADB	Asian Development Bank
AML	Anti-Money Laundering
API	Application Programming Interface
BPNG	Bank of Papua New Guinea
CDD	Customer Due Diligence
CFT	Combating the Financing of Terrorism
CRVS	Civil Registration & Vital Statistics
CSO	Civil Society Organization (NGO)
DICT	Department of Information and Communications Technology
DPI	Digital Public Infrastructure
eKYC	Electronic Know Your Customer
FATF	Financial Action Task Force
FASU	Financial Analysis and Supervision Unit
GRM	Grievance Redressal Mechanism
ICSA	Immigration and Citizenship Services Authority
ICT	Information and Communications Technology
ID	Identity Document
ITU	International Telecommunication Union
KPI	Key Performance Indicator
M&E	Monitoring and Evaluation
MoU	Memorandum of Understanding
MVP	Minimum Viable Product
NICTA	National Information and Communications Technology Authority
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PNG	Papua New Guinea
PNGCIR	Papua New Guinea Civil and Identity Registry
RTA	Road Transport Authority
SOP	Standard Operating Procedure

VC	Verifiable Credential

11.2Glossary

TERM	Definition
Accredited Partner	Any entity formally recognized by the Regulatory Authority to participate in the Sevis ecosystem—this includes enrolment partners, authentication and eKYC partners, data exchange nodes, and credential issuers.
Digital ID	A digital representation of a person's identity, issued and authenticated electronically, used to access services and exercise rights.
Enrolment Partner	Organizations accredited to manage field enrolment operations, including device procurement, agent recruitment, centre planning, and public mobilization.
Enrolment Agent	Field-level personnel responsible for capturing residents' biometric and demographic data during the registration process.
eKYC	A digital process used to verify an individual's identity against official ID records or credentials, typically for onboarding to regulated services like banking.
Federated Model	An operational structure that decentralizes service delivery (e.g., enrolment, issuance) while maintaining centralized oversight, policy control, and technical standards.
Grievance Redressal Mechanism (GRM)	A system for residents to report and resolve issues related to SevisPass registration, usage, or any associated services.
Minimum Viable Product (MVP)	The initial version of a digital solution with just enough features to satisfy early use cases and collect user feedback for future improvement.
SevisAdminPortal	The administrative interface used by government authorities to issue, revoke, and manage Verifiable Credentials and maintain the Trust Registry.
SevisDEx	The Sevis Data Exchange Layer enabling secure, consent-based sharing of resident data between government and authorized service providers.
SevisPass	The foundational Digital ID credential issued to residents under the Trust Framework. It will be the first Verifiable Credential in the Sevis ecosystem.
SevisPortal	A resident-facing portal that supports self-registration, booking enrolment appointments, managing digital credentials, and accessing wallet services.
SevisWallet	The official mobile or web-based wallet for securely storing, managing, and sharing Verifiable Credentials like SevisPass.
Trust Framework	The legal, technical, and institutional framework defining the rules, standards, and governance arrangements for operating the Sevis digital ID ecosystem.
Verifiable Credential (VC)	A digitally signed credential that can be independently verified for authenticity and integrity, without needing to contact the issuer directly.

11.3RACI Matrix for Key Roles

To ensure clarity in institutional responsibilities and support smooth implementation of the Digital ID and Trust Framework, a RACI (Responsible, Accountable, Consulted, Informed) matrix is provided below. This matrix defines which stakeholders are **Responsible (R)** for execution, **Accountable (A)** for final outcomes, **Consulted (C)** for inputs and approvals, and **Informed (I)** of developments. It covers key governance, operational, and partnership functions critical to the SevisPass and SevisDEx ecosystem.

Activity	**Policy Sponsor (DICT)**	**Regulatory Authority**	**Implementation Authority**	**Sector Ministries / Regulators**	**Accredited Partners**	**Oversight / Audit Bodies**
Develop national digital ID policy	A/R	C	C	C	I	I
Define regulatory standards & accreditation criteria	C	A/R	C	C	I	I
Design and implement technology architecture	C	C	A/R	C	I	I
Develop and maintain trust registry	C	A (policy aspects)	R (Technology implementation)	C	I	I
Onboard and accredit enrolment partners	I	A (policy criteria)	R (MoUs, operational execution)	C	C	I
Onboard and accredit authentication/eKYC providers	I	A (definitions, standards)	R (implementation)	C	C	I
Onboard and accredit data exchange participants	I	A (interoperability & security standards)	R (partner agreements)	C	C	I
Approve and update pricing model / sustainability plan	A	C	R	C	I	I
Monitor partner performance and service delivery	I	A (regulatory compliance)	R (operational KPIs)	C	C	A (for audits)
Conduct audits / compliance reviews	I	A (regulatory compliance)	R (supporting info, access)	C	I	A/R
Stakeholder coordination and communications	A	C	R	C	I	I
Legal MoUs with partners	I	C	A/R	C	R	I

Legends:

- **A (Accountable):** Final decision-making authority; only one entity should be accountable for each activity.
- **R (Responsible):** Executes or manages the activity.
- **C (Consulted):** Provides input and is consulted before action or decision.
- **I (Informed):** Needs to be kept updated, but not directly involved in decision or execution.

11.4 Trust Framework Operationalization Roadmap

Workstream	Q1 (M1–3)	Q2 (M4–6)	Q3 (M7–9)	Q4 (M10–12)	Q5 (M13–15)	Q6 (M16–18)	Q7, 8 (M19–24)
Institutional & Legal	• Establish governance and institutional roles • Finalize Digital ID policy	• Draft SevisPass legal framework • Regulatory gap assessment • Notify core policy instruments	• MoUs and contracts for partners • Compliance/audit standards finalized	• Legal amendments finalized as needed	• Institutionalize governance & compliance audits	• Continued regulatory alignment	• Ecosystem-wide legal assessments • Legal framework validation review
Governance Architecture	• Define architecture and assign roles	• Notify governance model • Initiate inter-agency coordination mechanisms	• Steering Committee + TWG operational • Partner accreditation criteria notified	• Partner SOPs documented and notified	• First governance compliance review • Initiate a cybersecurity audit	• SOP and audit process refinements	• Feedback from governance review • Updated governance compliance
Technology Rollout	• MVP dev for SevisPass, SevisPortal, AdminPortal • Tech architecture finalized	• MVPs launched • Minimal SevisDEx live • Onboard tech partners	• Biometric enrolment devices deployed • Operational dashboards prepared	• Basic auth services live • SevisWallet launched • SevisDEx data testing begins	• SevisWallet expanded • SevisPortal features enriched	• AI-based fraud tools prototyped • Full feature rollout of all DPI components	• Multi-sector DEx integration • Tech performance scaling
Field Operations	• Enrolment model and partner planning	• Partner selection for pilot • Limited enrolment via SevisPortal	• Pilot biometric enrolment with early partners	• Scale enrolment operations	• Offline auth models reviewed • Scale field rollout	• Nationwide field ops ramp-up	• Field operations streamlined
Trust Framework Partners Readiness	• Define partner onboarding policy	• Begin bank onboarding on SevisDEx	• Expand financial partner onboarding • Notify audit norms	• Begin onboarding social sector partners	• Expand service sector integrations	• Multi-sector partner onboarding	• Capacity-building workshops

Communication & Outreach	• Plan outreach strategy	• Develop outreach content • Plan awareness campaigns	• Launch digital literacy & awareness campaigns • Comms plan finalized	• Mass campaign on SevisPass & TF launch	• Feedback campaigns	• Continuous outreach cycle	• Sector-specific awareness drives • Broad ecosystem engagement
Grievance Redressal, Monitoring & Evaluation	• Draft M&E framework • Define GRM approach	• Deploy v1 GRM • Baseline M&E setup	• Launch GRM v1 • Monitor feedback • Start field M&E baseline	• Launch structured M&E assessments	• GRM phase 2 with escalation, Agent support system	• GRM dashboard integration	• Linked GRM-M&E ecosystem • First annual evaluation cycle