DIGITAL ID POLICY

Draft Version 6.1 (24-04-2025)

THIS PAGE IS LEFT BLANK

Table of Contents

FOREWORD BY PRIME MINISTER

Papua New Guinea is forging a path toward a prosperous, inclusive, and digitally connected future, guided by our Vision 2050 and Medium Term Development Plan IV (2023–2027). The Digital ID Policy 2025 is a cornerstone of this journey, establishing a secure and accessible digital identity system to empower every citizen, from urban centers to remote villages.

The SevisPass digital identity will transform how Papua New Guineans access essential services, fostering financial inclusion, streamlining governance, and strengthening our digital economy. By bridging divides and ensuring trust through robust governance, this policy aligns with regional commitments, such as the Lagatoi Declaration, positioning Papua New Guinea as a leader in Pacific digital innovation.

I commend the Ministry for ICT, the Department of Information and Communication Technology, and our partners, including the International Telecommunication Union, the Australian Government, and the Asian Development Bank, for their collaboration. Together, we are building a digitally empowered nation where every citizen is connected and every opportunity is within reach.

Sincerely,

HON. JAMES MARAPE, MP
Prime Minister of Papua New Guinea

STATEMENT BY THE MINISTER FOR ICT

As Minister for Information and Communication 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 Communication 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 Communication Technology

STATEMENT BY THE GOVERNOR OF BPNG

As Governor of the Bank of Papua New Guinea, I endorse the Digital ID Policy 2025, which establishes SevisPass as a vital tool for financial inclusion and regulatory compliance. This policy will enable secure and efficient access to financial services, particularly for unbanked and rural populations, while strengthening our sector's resilience against illicit activities.

The Bank of Papua New Guinea is committed to guiding financial institutions in adopting SevisPass, ensuring alignment with anti-money laundering and counter-terrorist financing standards. We will collaborate with the Department of Information and Communication Technology and the Financial Analysis and Supervision Unit to deliver a trusted digital identity ecosystem that drives economic growth.

This policy marks a significant milestone toward a financially inclusive Papua New Guinea. We stand ready to support its implementation.

Sincerely,

ELIZABETH GENIA
Governor, Bank of Papua New Guinea

DEFINITIONS

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

Term	Definition
Authentication**:**	The process of verifying the identity of a user or system, ensuring that they are who they claim to be, typically through credentials such as passwords, biometric data, or tokens.
Biometric Data**:**	Unique physical or behavioral characteristics used to identify individuals, including but not limited to fingerprints, facial recognition, iris scans, and voice patterns.
Cybersecurity**:**	The practice of protecting systems, networks, and programs from digital attacks, unauthorized access, damage, or data theft.
Digital ID System**:**	An electronic identity verification system that allows individuals to prove who they are through the issuance of verifiable credentials for the purpose of accessing digital services, conducting transactions, or engaging in digital interactions.
Digital Identity Provider**:**	An entity responsible for the management, operation, and maintenance of the digital ID system, ensuring secure, efficient, and compliant identity services.
eKYC (Electronic Know Your Customer):	A digital process for verifying the identity of individuals or entities using electronic methods, ensuring compliance with regulatory requirements. eKYC streamlines the onboarding process by enabling secure and efficient collection, validation, and authentication of identification data for accessing services across various sectors.
Encryption**:**	The method by which information is converted into secret code that hides the information's true meaning, ensuring data confidentiality and protection against unauthorized access.
Interoperability**:**	The ability of different information systems, devices, and applications to communicate, exchange data, and use the information exchanged in a seamless manner.
KYC (Know Your Customer):	A standardized (paper based) process used to verify the identity of individuals or entities involved in a business relationship and to assess the potential risks of illicit activities,

	such as money laundering or fraud. The process typically involves collecting and validating information, such as identification documents and other relevant data, to ensure compliance with applicable legal and regulatory requirements.
National ID (NID):	A legally mandated, government-issued identification document used to verify the identity of individuals within a jurisdiction. It serves as an official record for administrative, legal, and regulatory purposes, ensuring compliance with national identification requirements and facilitating access to public and private services.
Open Standards**:**	Standards that are publicly available and have various rights associated with their use, ensuring that different systems can interact and integrate effectively without proprietary constraints.
Personal Data (or Personal Identity Information)**:**	Any information relating to an identified or identifiable person. This can include data such as names, identification numbers, location data, or other attributes specific to a person's physical, physiological, or social identity.
Privacy by Design**:**	An approach to system engineering that takes privacy into account throughout the whole engineering process, ensuring that data protection is built into the system architecture from the outset.
Public-Private Partnership (PPP)**:**	A cooperative arrangement between public and private sectors, aimed at funding, designing, implementing, and operating projects that benefit both parties.
SevisPass:	Government's accredited verifiable credential used as a digital public infrastructure.
Trust Framework	A structured set of rules, standards, protocols, and governance mechanisms that ensures the security, interoperability, privacy, and trustworthiness of the Digital ID System. It defines how identities are verified, authenticated, and managed across public and private sectors, fostering confidence in digital interactions while adhering to legal, regulatory, and ethical requirements.
User Consent**:**	The informed and voluntary agreement of a person to allow the collection, use, or sharing

	of their personal data under specified conditions.
Verifiable Credential	A digitally issued cryptographically secure identity document (e.g., SevisPass, digital passports) that can be authenticated against authoritative data sources to verify an individual's identity for accessing services.
Verification**:**	The process of checking that a digital identity matches the real-world identity it represents, confirming its accuracy and validity.
Vendor Neutrality**:**	The principle of designing systems that do not rely on a specific vendor's products, ensuring flexibility and avoiding lock-in to proprietary technologies.
Vulnerability Assessment**:**	The systematic process of identifying, evaluating, and addressing security weaknesses within a system to protect against potential threats.

SECTION ONE - INTRODUCTION

1. Purpose

This Digital ID Policy establishes a comprehensive framework for developing, implementing, and sustaining a secure, inclusive, and interoperable Digital ID System, with SevisPass as its flagship verifiable credential. It aims to empower all Papua New Guineans by enhancing access to essential services, fostering financial inclusion, and strengthening governance within a trusted digital ecosystem, aligned with Vision 2050 and the Lagatoi Declaration.

Section One of this document sets the vision, principles, and alignment, providing the foundation for a transformative digital identity system. Section Two builds on this by detailing operational strategies for establishing, integrating, and standardizing the system to ensure seamless service delivery. Section Three proposes a robust legislative framework to enable legal compliance and sustainability. Section Four concludes with a monitoring and evaluation framework to track progress and foster continuous improvement, ensuring a digitally inclusive future.

2. Background

Many countries around the world are embracing digital transformation to enhance economic growth and improve public service delivery. A key component of this transformation is the implementation of digital identity systems, which enable secure and efficient verification of individuals online. As government processes become more automated and businesses transition to digital platforms, the need for a reliable and integrated digital ID system becomes increasingly important. This system facilitates secure online transactions, minimizes fraud, and improves access to essential services.

Despite the potential benefits, PNG faces several challenges in implementing an effective digital ID system. The country's identity records are fragmented across different institutions, leading to slow service delivery and redundant verification processes. Additionally, limited digital infrastructure and low internet penetration, particularly in rural areas, restrict accessibility to online services. Cybersecurity threats and the absence of strong data protection regulations further raise concerns about identity theft and misuse of personal data.

Papua New Guinea has taken steps toward digital transformation through its Digital Transformation Policy 2020. This policy aims to modernize public services, strengthen the digital economy, and improve citizen engagement through digital platforms. Currently, various institutions, such as banks and government agencies, collect and manage identity records independently. However, the absence of a centralized digital ID system limits interoperability between sectors, resulting in inefficiencies and duplicated verification efforts. Establishing a unified national digital identity infrastructure could address these challenges and provide a seamless verification system across public and private sectors.

In addressing these challenges, the Digital ID Policy aims to establish a secure digital identity system that enhances interoperability, improves service delivery, and strengthens data protection in Papua New Guinea. By integrating fragmented identity records across various

institutions, the policy seeks to streamline an identity verification processes, reduce redundancies, and enhance access to essential services, particularly in remote areas. Ultimately, the Digital ID Policy supports the country's broader digital transformation agenda, fostering economic growth, efficiency in governance, and improved citizen engagement in the digital economy.

3. Policy Intent

The policy aims to establish a comprehensive framework for developing, implementing, and sustaining a secure, inclusive, and interoperable Digital ID system in Papua New Guinea.

4. Guiding Principles

This Policy is built upon the following key principles – Governance and Protection, Inclusion, and Appropriateness of Design – to ensure that the Digital ID system is robust, inclusive, secure, and sustainable.

Principle 1: Governance and Protection

The design, development, and implementation of the Digital ID System will focus on governance and protection of personal data by:

i. Carefully considering the collection, storage, management, and use of identity information.
ii. Integrating security measures into the technology and systems to meet the highest standards of protection.
iii. Maintaining privacy and confidentiality of all collected data, adhering to best practices in data protection and legal compliance.

Principle 2: Inclusion

The Digital ID System will be designed to ensure accessibility for all citizens of Papua New Guinea, including those in urban, rural, and unserved areas, by:

i. Simplifying the process of collecting and verifying personal data.
ii. Adapting to diverse cultural and societal norms across the country.
iii. Providing special consideration for marginalized and remote communities, ensuring access to digital services and participation in the digital economy.

Principle 3: Appropriateness of Design

The Digital ID System will balance security with usability, ensuring:

- Data security is maintained throughout the entire Digital ID lifecycle.
- Scalability, allowing the system to accommodate increasing users and service demand.
- Flexibility, enabling integration with future services and innovations.

- Universal access, particularly for rural and unserved citizens, ensuring easy registration and ID acquisition.
- Interoperability and compatibility through open standards, ensuring vendor and technology neutrality.
- Privacy by design, embedding user privacy from the system's inception.
- Financial and operational sustainability, making the system resilient and capable of supporting long-term digital services and infrastructure.

5. Digital Public Infrastructure Principles

The Digital ID System, with SevisPass as its flagship verifiable credential, is designed as a DPI to provide a trusted, scalable, and inclusive foundation for Papua New Guinea's digital economy. The system adheres to core DPI principles and leverages the GovStack framework to ensure global alignment, interoperability, and sustainability.

The Digital ID System is grounded in the following DPI principles to ensure it serves as a robust public good:

- Openness and Interoperability: The system adopts open standards (e.g., OAuth, OpenID Connect) and APIs to enable seamless integration with public and private sector services, fostering cross-sector collaboration and reducing vendor lock-in. This aligns with the policy's interoperability objectives (Section Two, Focus Area 2).
- Inclusivity and Accessibility: SevisPass prioritizes universal access by offering mobile registration units, offline authentication, and disability-friendly interfaces, ensuring rural and marginalized communities can participate in the digital economy (Section Two, Focus Area 1.3.6).
- User-Centricity and Trust: The system embeds privacy-by-design, requiring informed user consent and data minimization, and adheres to the Digital ID Trust Framework to build public trust through secure, transparent data management (Section Two, Focus Area 2.3).
- Scalability and Sustainability: Designed for long-term resilience, the system supports future verifiable credentials (e.g., digital passports, driver's licenses) and leverages public-private partnerships to ensure financial and operational sustainability (Section Two, Focus Area 3).
- Governance and Accountability: A multi-stakeholder governance framework, led by the Department of Information and Communication Technology (DICT), ensures compliance with national legislation (e.g., Digital Government Act 2022) and global standards, fostering accountability and stakeholder coordination (Section Three, 3.4).

The Digital ID System adopts the GovStack ID Building Block, an open-source, modular framework developed by the International Telecommunication Union (ITU), GIZ, and other partners, to ensure a standardized, interoperable, and scalable digital identity infrastructure. GovStack's alignment with global best practices enhances the system's functionality and regional integration, as outlined below:

- Modular Architecture: The GovStack ID Building Block provides reusable components for registration, issuance, and authentication, enabling the Centralized Identity and Biometric Verification Platform (CIBVP) to integrate with trusted data sources (e.g., PNGCIR, PNG ICSA) and support tiered eKYC verification (Simplified, Standard, Enhanced CDD) as per the AML/CTF Act 2015 (Refer to Appendix 1)

- Interoperability and Standards Compliance: GovStack's adherence to open standards ensures SevisPass is interoperable with financial, government, health, and education platforms, facilitating single sign-on (SSO) for SevisPortal and cross-border recognition via the Lagatoi Declaration.

- Inclusion and Accessibility: GovStack's flexible design supports diverse authentication methods (e.g., biometric, mobile, smart cards) and offline options, aligning with the policy's commitment to universal coverage for rural and marginalized communities.

- Security and Trust: GovStack incorporates robust security features, including encryption, real-time fraud detection, and audit trails, ensuring compliance with the Digital ID Trust Framework and the National Data Governance and Protection Policy 2024.

- Regional and Global Alignment: By adopting GovStack, Papua New Guinea aligns with regional commitments under the Lagatoi Declaration (Pacific ICT Ministerial Dialogue, 2023) and global frameworks like the Financial Action Task Force (FATF) recommendations, enhancing cross-border interoperability for digital passports and financial transactions.

The adoption of GovStack accelerates the deployment of SevisPass by providing a pre-tested, cost-effective framework, reducing development time and ensuring alignment with international benchmarks. Technical assistance from the ITU and Asian Development Bank, supports GovStack implementation, ensuring the Digital ID System is a cornerstone of Papua New Guinea's digital transformation.

6. Mission

To establish a secure, inclusive, and interoperable Digital ID system that enhances access to government and private sector services while safeguarding privacy and security.

7. Objectives

Emanating from the Policy 'Intent' and the 'Mission', the Policy will focus on the following key objectives:

- Establish a Secure, and Sustainable Digital ID System that is governed by a Digital ID Trust Framework
- Introduce SevisPass as a verifiable credential that operates as a DPI
- Inform appropriate legal and regulatory frameworks to enforce use of the Digital ID System including that of SevisPass and various other future verifiable credentials.

8. Policy Outcomes

The implementation of the Policy Objectives listed below, should allow the Department to achieve the following outcomes:

- Establishment of a Secure, Inclusive, and Sustainable Digital ID System — A secure and inclusive digital ID system will provide universal identification through a tiered registration framework with biometric authentication, ensuring reliable identity verification and seamless access to public and private services via SevisPass.
- Enhanced Integration and Interoperability—The Digital ID system will provide enhanced integration and interoperability by enabling integration and interoperability to a centralized data exchange, seamless multi-sector service access, reduced redundancy through database linking, and cross-border recognition for global services and secure travel authentication.
- Strengthened Data Protection and Privacy—The Digital ID system will strengthen data protection and privacy by providing enhanced data security measures and empowering citizens with control over their data.
- Inclusive and Accessible Digital Identity — The Digital ID system will ensure universal coverage, multi-mode authentication, and disability inclusion to provide accessible and inclusive identification for all citizens, including marginalized and disadvantaged communities.
- Improved Governance and Service Delivery—The adoption of a Digital ID will streamline government digital services (G2G, G2B, G2C), improving accountability, transparency, Governance, and driving economic growth through digital transformation in Papua New Guinea.
- Trusted Digital Identity Ecosystem: The establishment of a Digital ID Trust Framework will ensure that SevisPass operates as a reliable and secure DPI, fostering trust among citizens, government agencies, and private sector partners through robust governance, standardized processes, and compliance with global best practices.

9. Target Audience

The roll-out of the Digital ID system will consider the needs and requirements of multiple stakeholders. Additionally, the SevisPass verifiable credential will be designed and developed as a DPI, targeting, among others, Government agencies and government employees, financial institutions, telecommunication operators, educational institutions, health care providers, regulatory authorities, citizens and residents of Papua New Guinea, foreign nationals, businesses and organizations and law enforcement and security agencies.

10. Policy Alignment

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

10.1 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.
- *Civil Registration Act (Chapter 304) 1963* 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 into Papua New Guinea.

10.2 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 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 Papua New Guinea's Medium Term Development Plan IV (2023-2027) relating to the Strategic Priority Area 8, on Digital Government. It complements 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.

SECTION TWO – POLICY FOCUS AREAS

1. Focus Area 1: Establishment of a Digital ID System

The digital ID system will be established to facilitate secure, efficient, and inclusive access to public and private services for all citizens. The Digital ID system will consist of the following components:

i. *Registration:* Personal data including biometric data will be collected.
ii. *Issuance:* The establishment of a Digital ID Provider to verifying personal and biometric data and issue accordingly verifiable credentials for a secure and universally accepted identity.
iii. *Use:* Ensure that verifiable credentials can be issued for individuals to access public and private sector services, including welfare, health, financial transactions, and digital services.
iv. *Management:* Relevant agencies will be strengthened to oversee the Digital ID system, ensuring technology adoption, interoperability, maintenance, and grievance redressal processes to address any issues related to the system's operation.

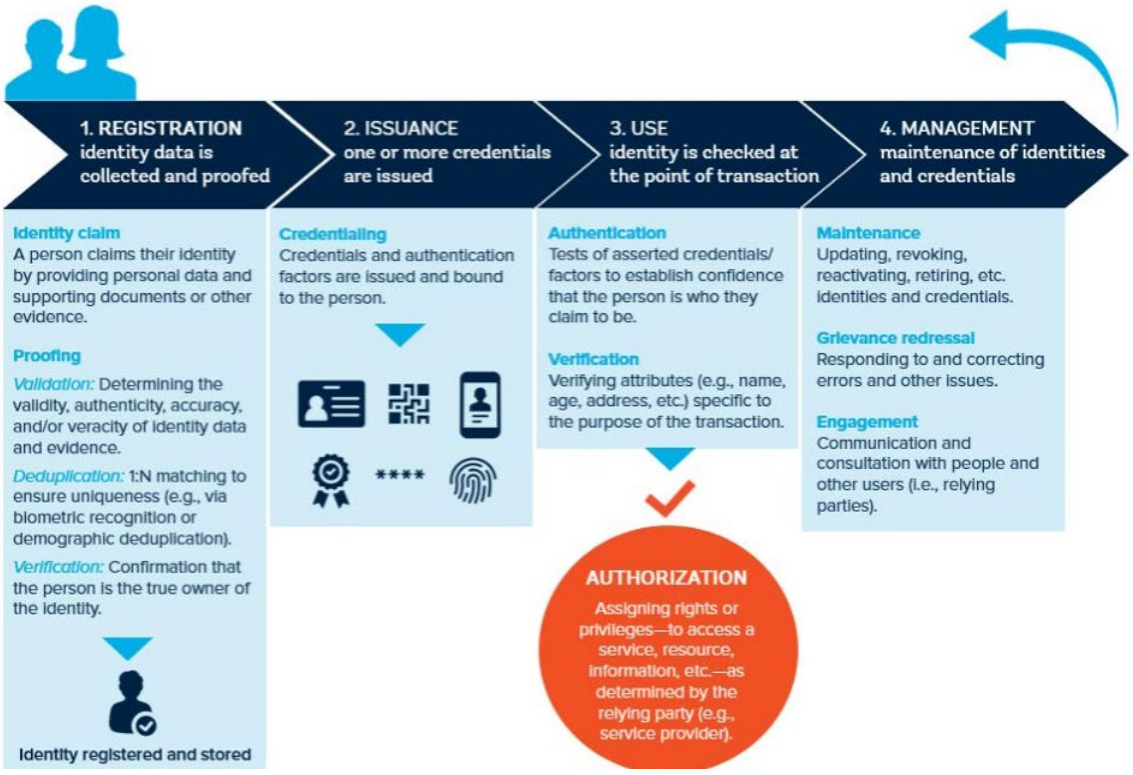

Figure 1: Components of Digital ID (Adapted from Digital Identity: Public and Private Sector Cooperation and Technology Landscape for Digital), World Bank. 2019. ID4D Practitioner' Guide: Version 1.0 (October 2019).

1.1 Registration

The registration process will require individuals to provide a combination of identity attributes, including something they know (a personal identifier like a PIN or password), something they have (a government-issued ID such as NID, passport, or driver's license), and something they are (biometric data such as fingerprints, facial recognition, or iris scans), to ensure robust authentication and prevent fraud.

Registration will ensure inclusivity through accessible channels (see Section 1.3, Principle 2).

Personal data collected will include, at a minimum, full name, date of birth, address, and biometric identifiers, verified against trusted sources such as the PNG Civil and Identity Registry (PNGCIR), PNG ICSA, or other government databases, to ensure accuracy and consistency.

All data collection will adhere to privacy-by-design principles, requiring informed user consent for the collection, storage, and use of personal and biometric data, with clear communication of data usage purposes and rights under the National Data Governance and Protection Policy 2024.

1.2 Issuance

The issuance of verifiable credentials, such as SevisPass, will follow a secure, interoperable, and tiered verification process under the Digital ID Trust Framework, ensuring credentials are trustworthy, accessible, and compliant with regulatory requirements.

The issuance process will implement tiered eKYC verification levels (Simplified, Standard, and Enhanced CDD) to balance security and accessibility, enabling basic service access with minimal data (e.g., name, address) for low-risk use cases and requiring detailed verification (e.g., biometric data, source of wealth) for high-security transactions, as outlined in the AML/CTF Act (Sections 21–29).

Credentials will be issued only after verifying personal and biometric data against authoritative sources, such as the National ID (NID), passport, driver's license, or PNGCIR databases, to ensure accuracy and prevent duplication or fraud.

Issuance will incorporate biometric verification (e.g., fingerprints, facial recognition) to link credentials to the individual's unique identity.

The issuance process 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.

Issuance will prioritize accessibility by offering multiple authentication methods (e.g., biometric, mobile, smart cards) and ensuring usability for individuals with disabilities.

The issuance process will implement robust measures, including encryption, secure data storage, and real-time monitoring, to prevent identity theft, fraud, and unauthorized access.

1.3 Use

SevisPass will serve as a single, trusted verifiable credential for accessing services across financial, telecommunication, government, health, education, insurance, and social media sectors, minimizing user friction and enhancing adoption.

SevisPass will offer multiple authentication methods (biometric, mobile, smart cards) and accessibility features (multilingual support, disability-friendly interfaces) to ensure inclusivity, particularly for rural and marginalized communities.

1.3.1 Use in Financial Sector

SevisPass will serve as a trusted tool for customer onboarding and ongoing due diligence in banks, superannuation funds, and other financial institutions.

Financial institutions will use SevisPass to verify customer identities during account opening, leveraging its biometric and demographic data (name, address, NID) to meet General, Simplified, and Standard Customer Due Diligence (CDD) requirements (AML/CTF Act, Sections 15–25), reducing onboarding time and costs.

For high-risk customers (Politically Exposed Persons), SevisPass shall facilitate Enhanced CDD by integrating with authoritative sources (PNGCIR, financial registries) to verify source of wealth and monitor transactions, subject to data ecosystem availability (AML/CTF Act, Sections 26–29).

Financial institutions will use SevisPass for real-time authentication and transaction monitoring, ensuring continuous compliance with AML/CTF requirements and detecting suspicious activities through secure APIs and fraud detection mechanisms.

SevisPass will enable unbanked and rural populations to access financial services by providing a universally accepted digital identity.

1.3.2 Use in Telecommunication Sector

SevisPass will simplify customer onboarding and regulatory compliance in the telecommunication sector, ensuring secure and efficient service access.

Telecommunication operators will use SevisPass to verify customer identities during SIM card registration and service activation, utilizing biometric authentication and verified data (NID, address) to meet eKYC requirements and prevent fraudulent registrations.

Operators will leverage SevisPass for periodic identity verification to ensure compliance with regulatory mandates, such as monitoring prepaid SIM usage, through seamless integration with the Digital ID System's centralized platform.

SevisPass will support mobile-based authentication to enable rural customers to access telecommunication services, addressing low internet penetration and enhancing connectivity, in line with the policy's inclusion objectives.

1.3.3 Use in Digital Government and Social Sector

SevisPass will enable seamless and secure access to government services through single sign-on (SSO) for government-to-government (G2G) and government-to-citizen (G2C) platforms, including the SevisPortal.

SevisPass will provide SSO for G2G platforms, allowing government agencies (e.g., Department of Finance, PNGCIR) to authenticate employees and share data securely via a centralized platform, reducing redundancy and improving inter-agency coordination.

Citizens will use SevisPass to access SevisPortal and other G2C platforms (e.g., tax filing, social benefits) through a single digital identity, with biometric or mobile authentication ensuring secure and user-friendly interactions.

SevisPass will streamline access to government services, such as welfare payments and civil registration, by integrating with public sector databases.

SevisPass will facilitate secure and equitable access to services in the health, education, and insurance sectors, ensuring verified identities and inclusive service delivery.

Healthcare providers will use SevisPass to verify patient identities for accessing medical records, scheduling appointments, and receiving subsidized care, with biometric authentication ensuring data security and compliance with privacy standards.

Educational institutions will leverage SevisPass to authenticate students for enrollment, examinations, and scholarship applications, enabling seamless access to digital learning platforms and reducing administrative burdens.

Insurers will use SevisPass for customer onboarding and claims processing, verifying identities and policy details through integration with the Digital ID System, streamlining operations and enhancing fraud prevention.

SevisPass will enforce age verification for access to social media platforms, ensuring compliance with the *Social Media Policy 2025* and protecting minors from inappropriate content.

Social media platforms operating in PNG shall integrate SevisPass to verify users' age during account creation, using verified date-of-birth data to restrict access for users below the mandated age threshold (13 or as specified by regulation and consistent with other primary laws).

SevisPass will enhance user experience and interoperability across all sectors by providing a unified digital identity, reducing the need for multiple credentials, and ensuring seamless service access.

1.4 Future Verifiable Credentials

The Digital ID System will support the integration of additional verifiable credentials, such as driver's licenses, passports, student IDs, and other government-issued or sector-specific credentials, to expand its functionality, enhance service delivery, and ensure scalability. These credentials shall adhere to the Digital ID Trust Framework**,** ensuring security, interoperability, and inclusion while complementing SevisPass.

Driver's Licenses: The PNG Road Traffic Authority (RTA) will integrate digital driver's licenses into the Digital ID System, enabling citizens to use them as verifiable credentials for identity verification, vehicle registration, and compliance with road safety regulations. SevisPass will link to driver's license data for seamless authentication in related services (insurance claims, law enforcement checks).

Passports: The PNG ICSA will incorporate digital passports as verifiable credentials, allowing citizens to use them for secure travel authentication, visa applications, and cross-border identity verification. SevisPass will facilitate interoperability with passport data to support international recognition and streamline immigration processes.

Student IDs: Educational institutions, in collaboration with the Department of Education, will issue digital student IDs as verifiable credentials for authentication in academic services, such as enrollment, examinations, and access to digital learning platforms. These credentials will integrate with SevisPass to provide a unified identity for students, enhancing administrative efficiency and access to educational opportunities.

Other Sector-Specific Credentials: The Digital ID System will support the issuance of additional credentials, such as professional licenses, health insurance cards, or voter IDs, by relevant authorities (Department of Health, Electoral Commission). These credentials will be verifiable through the Digital ID System, ensuring secure and standardized access to sector-specific services.

2. Focus Area 2: Integration, Interoperability, & Standards

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

2.1 Integration with Existing Systems

The SevisPass and other verifiable credentials will be issued based on robust integration capabilities to enable seamless verification against functional ID data sources such as the NID, driver's licenses, passports, and other government-issued identification documents recognized through legal means. This integration will allow individuals to leverage their existing records for digital identity verification. Key integration aspects include:

Centralized Identity and Biometric Verification Platform (CIBVP): A central platform will be established to facilitate identity matching between SevisPass and public sector databases, ensuring that identity verification is consistent and reliable across multiple platforms.

Leverage Existing Records: Individuals' historical records from existing systems, including NID, passports, and driver's licenses, among other systems, will be linked with the CIBVP, ensuring efficiency, and reducing the need for re-registration or redundant data entry.

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

2.2 Interoperability with Services

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

- SevisPass will be developed based on open standards and robust APIs (Application Programming Interfaces) that allow easy integration with a range of services. This will enable secure and consistent identity verification across diverse sectors.

- Government systems such as tax systems, health services, and social welfare platforms will be integrated with SevisPass, as will with private services like banking, telecommunications, and retail platforms.

By enabling seamless interaction between SevisPass and service providers, users can access various services without the need for separate logins or identity verification, streamlining service delivery and improving overall user experience.

2.3 Adoption of Standards

The Digital ID System, encompassing SevisPass and future verifiable credentials including digital driver's licenses, passports, student IDs among other verifiable credentials, will adhere to robust standards and compliance measures to ensure security, interoperability, privacy, and trust across public and private sectors. The Digital ID Trust Framework will underpin these standards, aligning with global best practices and national legislation.

2.3.1 Registration Standards

The registration process will ensure secure, inclusive, and privacy-compliant data collection to establish verifiable credentials (identities) for all citizens, including rural and marginalized communities.

The Digital ID System will implement secure data collection protocols requiring a combination of identity attributes (PIN/password, government-issued ID, biometric data such as fingerprints or facial recognition) to verify identities, adhering to ISO/IEC 19794 standards for biometric data and ISO/IEC 27001 for cybersecurity.

Registration will ensure inclusivity by accepting diverse identification documents including National ID, birth certificates, statutory declarations and offering accessible channels including mobile units, offline options, ensuring universal coverage.

All personal and biometric data collection will adhere to privacy-by-design principles, requiring informed user consent and transparent communication of data usage purposes, in compliance with the National Data Governance and Protection Policy 2024 and the Constitution.

Registration will align with *AML/CTF Act 2015* (Sections 15–20) General Customer Due Diligence (CDD) requirements, verifying identities against trusted data sources to prevent fraud and illicit activities, under oversight by the FASU.

2.3.2 Issuance Standards

The issuance of SevisPass and future verifiable credentials will follow rigorous processes to ensure trust, security, and interoperability across sectors.

Verifiable credentials will only be issued after verifying personal and biometric data against authoritative sources (PNGCIR, ICA, RTA databases), and where applicable implementing tiered eKYC verification (Simplified, Standard, Enhanced CDD) as per AML/CTF Act 2015 (Sections 21–29) to balance accessibility and security.

Issuance will incorporate biometric verification including fingerprints and facial recognition to link credentials to unique identities, adhering to ISO/IEC 19794 for biometric interoperability and ISO/IEC 27001 for fraud prevention.

Credentials will be issued using open standards (OAuth, OpenID Connect) and APIs to ensure interoperability with public and private sector systems including banking, healthcare, SevisPortal, among other systems.

The issuance process will prioritize accessibility by offering multiple authentication methods including biometric, mobile, smart cards among other authentication methods, and disability-friendly interfaces.

Issuance will implement robust security measures, including encryption, secure data storage, and real-time monitoring, to prevent identity theft and unauthorized access.

2.3.3 Usage Standards

The use of SevisPass and future credentials for accessing services will prioritize secure authentication, user consent, and data minimization to protect privacy and enhance user experience.

SevisPass will serve as a single, trusted credential for accessing services across financial, telecommunication, government, health, education, insurance, and social media sectors, using secure authentication methods including biometric and PIN among other best practices, to minimize user friction.

Usage will require user consent for data sharing, adhering to data minimization principles to limit data exposure to only what is necessary for service access, in compliance with the National Data Governance and Protection Policy 2024 and its relevant legal frameworks.

Usage will leverage open standards (OAuth, OpenID Connect) to ensure seamless integration with diverse platforms, supporting single sign-on (SSO) for government-to-government (G2G) and government-to-citizen (G2C) services, as mandated by the Digital Government Act 2022.

Usage will incorporate real-time fraud detection and transaction monitoring, particularly for financial and high-risk transactions, to ensure continuous compliance with AML/CTF Act 2015 (Sections 15–29).

2.3.4 Data Sources and Custodians Standards

To ensure the reliability, security, and interoperability of data used in the Digital ID System, specific standards and compliance measures will govern data sources and their custodians/agencies including PNGCIR, ICSA, RTA, BPNG and others. These standards address PNG's challenge of fragmented identity records and ensure trusted data for eKYC verification and credential issuance.

Data sources including National ID database, passport records, driver's license records and others will be designated as authoritative by the Digital ID Trust Framework, requiring custodians of these data including PNGCIR, ICSA, RTA to maintain accurate, up-to-date, and standardized data.

Custodians will implement secure data management protocols, including encryption, access controls, and audit trails, to protect personal and biometric data from unauthorized access or breaches, aligning with the National Cybersecurity Policy 2021 the National Cybersecurity Strategy 2024 and its associated legislation.

Data sources will be interoperable with the Digital ID System through open standards including APIs, JSON-LD among others, and a centralized data exchange platform, enabling seamless identity verification across sectors (financial, government, health), as mandated by Focus Area 2.1.
Custodians will verify and update data regularly (e.g., quarterly) to ensure accuracy and prevent duplication, with PNGCIR maintaining a master identity database linked to SevisPass for eKYC verification, in compliance with AML/CTF Act 2015 (Sections 15–20).

Custodians will be required to provide real-time access to data for Digital Identity Provider (DICT) verification processes, subject to user consent and data minimization principles, to support tiered eKYC (Simplified, Standard, Enhanced CDD) and Enhanced CDD requirements (source of wealth, PEP monitoring), as per AML/CTF Act 2015 (Sections 21–29).

Custodian will participate in a governance framework, ensuring compliance with the Digital ID Trust Framework through regular audits, data quality assessments, and incident reporting to address data discrepancies or security issues.

Custodians will support inclusion by providing offline and mobile-based data verification options for rural and marginalized communities.

Data sources for Enhanced CDD (e.g., financial registries, PEP lists) will be developed and integrated into the Digital ID System with BPNG and FASU collaborating to address data ecosystem gaps.

2.4 Compliance and Enforcement

Compliance with the above standards will be rigorously monitored and enforced to ensure the Digital ID System remains secure, accessible, and trusted.

Regular quarterly audits of the Digital ID System including data custodians; PNGCIR, ICSA, RTA, Banks, Insurance Companies and others will be undertaken to verify adherence to the Digital ID Trust Framework, ISO/IEC 27001, and AML/CTF Act 2015 standards (where applicable).

A secure audit trail of all registration, issuance, usage, and data access activities will be maintained, providing annual compliance reports to stakeholders including Department of Justice, BPNG, Individuals, and others to ensure transparency and accountability.

Non-compliance by custodians or service providers including financial institutions, social media platforms, and others will trigger corrective actions, including fines, system access restrictions, or mandatory remediation.

Compliance will align with regional and international standards, leveraging the Lagatoi Declaration (Pacific ICT Ministerial Dialogue, 2023) for technical assistance from ITU and APT to ensure cross-border interoperability and recognition, particularly for digital passports.

3. Focus Area 3: Implementation Framework & Ecosystem

3.1 Policy Sponsor

The DICT shall serve as the Policy Sponsor, responsible for overseeing the development, coordination, implementation and monitoring and evaluation of the Digital ID Policy.

Responsibilities:

- Develop and update the Digital ID Policy and Strategy in alignment with the Digital Transformation Policy 2020.
- Coordinate stakeholder engagement, including government agencies, private sector partners, and civil society, to ensure policy alignment with sectoral needs.
- Establish an industry-government working group to guide policy implementation, monitor progress, and select vendors under a white-label subscription model (where applicable) for scalability and interoperability.
- Allocate funding and resources for infrastructure development, pilot programs, and public awareness campaigns, in collaboration with the NICTA.
- Report policy outcomes and challenges to the Minister responsible for Digital Development, ensuring alignment with the Digital Transformation Policy 2020.
- Monitor the policy implementation, evaluate the impact and provide report to stakeholders including Government

3.2 Digital ID System Authority

The DICT will designate the operational development, management, and maintenance of the Digital ID System—including the Centralized Identity and Biometric Verification Platform (CIBVP)—to a state invested entity. This entity, will function as the implementing entity responsible for ensuring the system's interoperability, scalability, and security.

The Authority's mandate includes:

- Oversee the design, deployment, and operation of the Digital ID System, ensuring compliance with the Digital ID Trust Framework and global standards.
- Manage the issuance of SevisPass and future verifiable credentials (digital driver's licenses, passports), implementing tiered eKYC verification (Simplified, Standard, Enhanced CDD) as per AML/CTF Act 2015 (Sections 15–29).
- Provide document verification and biometric authentication services via the CIBVP, integrating with trusted data sources including PNGCIR, ICSA, RTA, among others to ensure accurate identity verification.
- Select and manage a Digital ID vendor under a white-label subscription model, ensuring vendor neutrality, scalability, privacy, and interoperability.
- Coordinate with accredited Digital ID Providers to ensure seamless credential issuance and system integration.

Governance:

- The designated entity must 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.

Potential Levy Collection:

- For the purpose of maintaining its development objectives around digital ID, a levy may be collected for the Ministry of ICT to be, guide through government policy, used for expanding universal access of digital services through the use of digital ID.

- Regulations may be setup up to guide these procedures.

3.3 Data Custodians

Data Custodians, comprising public and private bodies, will, based on the relevant legal mandates, maintain authoritative data sources including identity, financial, health and other authoritative data records and are required to support citizen consented identity verification and eKYC processes within the Digital ID System.

3.3.1 Public Sector Custodians

- Papua New Guinea Civil and Identity Registry (PNGCIR):
    - Role: Maintain the National ID database and civil registry (births, deaths, marriages), providing data for SevisPass registration and verification.
    - Responsibilities: Ensure data accuracy, update records quarterly, and integrate with the CIBVP for real-time verification; support rural registration via mobile units.
    - Legislation: Civil Registration Act 1963, mandating registration of vital events and issuance of National IDs.

- PNG ICSA:
    - Role: Manage passport and citizenship records, enabling digital passport issuance and cross-border verification.
    - Responsibilities: Provide passport data for eKYC verification, ensure interoperability with SevisPass, and support international recognition via the Lagatoi Declaration.
    - Legislation: Migration Act 1978 and Citizenship Act 1975, governing passport issuance and citizenship processes.

- PNG Road Traffic Authority (RTA):
    - Role: Maintain driver's license records, issuing digital driver's licenses as verifiable credentials.
    - Responsibilities: Integrate license data with SevisPass for authentication in insurance and law enforcement services; ensure data security and accessibility.
    - Legislation: Road Traffic Act 2014, regulating driver licensing and road safety.

- Department of Education:
    - Role: Oversee student ID issuance for educational institutions, enabling digital student IDs as verifiable credentials.

- Responsibilities: Integrate student data with SevisPass for enrollment and scholarship authentication; support digital learning platforms.
- Legislation: Education Act 1983, governing educational administration.

- Department of Health:
  - Role: Manage health records, supporting patient identity verification and future health insurance card issuance.
  - Responsibilities: Ensure secure data sharing for medical record access via SevisPass; support subsidized care authentication.
  - Legislation: Public Health Act 1973, regulating health service delivery.

- National Statistical Office (NSO):
  - Role: Serve as the central authority for the collection, analysis, and dissemination of official statistics, including demographic and socio-economic data.
  - Responsibilities: Coordinate with state agencies to ensure data accuracy and reliability; integrate statistical data with the Digital ID System to enhance demographic profiling and support evidence-based policy-making.
  - Legislation: Statistical Services Act 1980, mandating the NSO's role in national data governance.

- Department of Provincial & Local-Level Government Affairs (DPLGA):
  - Role: Oversee the maintenance of Ward Record Books, which capture vital socio-economic data at the village and ward levels.
  - Responsibilities: Ensure the collection and updating of data on individuals' names, clans, ethnic groups, and other relevant information; facilitate the integration of this data into the Digital ID System to support identity verification and service delivery at the local level.
  - Legislation: Local-Level Governments Administration Act 1997, specifically Section 57, mandating the establishment and maintenance of Village Books.

3.4 Private Sector Custodians

- Financial Institutions (Banks, Insurance Companies, Finance Companies, Super Funds):
  - Role: Maintain customer and financial data for eKYC verification and transaction monitoring.
  - Responsibilities: Integrate with SevisPass for customer onboarding and Enhanced CDD (e.g., source of wealth, PEP monitoring); ensure compliance with AML/CTF Act 2015 (Sections 15–29).
  - Legislation: Central Banking Act 2000 and Superannuation (General Provisions) Act 2000, governing banking, and superannuation operations.

- Telecommunications Companies (Telcos):
  - Role: Manage Subscriber Identity Module (SIM) card registration and user data for mobile network access.
  - Responsibilities: Collect and verify personal information, including full name, photograph, valid identification (National ID, driver's license, passport), residential address, and occupation, as mandated by the SIM Card Registration Regulation 2016. Share verified data with the Digital ID System for identity verification and Know

Your Customer (KYC) processes, ensuring compliance with the Data Governance and Data Protection Policy 2024.
        - Legislation: SIM Card Registration Regulation 2016 (Statutory Instrument No.7 of 2016), National Information and Communications Technology Authority Act 2009

- Private Health Clinics and Hospitals:
    - Role: Manage patient records for healthcare services, supporting identity verification.
    - Responsibilities: Use SevisPass for patient authentication, ensuring secure data sharing and compliance with privacy standards.
    - Legislation: National Data Governance and Protection Policy 2024, regulating private sector data management.

- Responsibilities:
    - Maintain accurate, up-to-date data in compliance with the Digital ID Trust Framework.
    - Implement secure data management protocols (e.g., encryption, access controls) and provide real-time access to the CIBVP for verification, subject to user consent.
    - Support inclusion by offering offline and mobile-based verification options for rural communities.
    - Participate in regular audits by NICTA to ensure data quality and compliance.

3.5 Digital ID Regulatory Authority

The NICTA will serve as the Digital ID Regulatory Authority, responsible for formulating the Digital ID Trust Framework in consultation with industry and regulating the Digital ID System.

- Responsibilities:
    - Develop and enforce the Digital ID Trust Framework, defining standards for registration, issuance, usage, and management.
    - Formulate a legal framework for the Digital ID System, proposing amendments to the National Information and Communication Technology Act 2009 to support regulatory oversight.
    - Conduct quarterly audits of the Digital ID System, Digital ID System Authority, data custodians, and accredited providers to verify compliance with the Digital ID Trust Framework.
    - Enforce corrective actions (e.g., fines, access restrictions) for non-compliance by custodians, providers, or service providers (e.g., financial institutions, social media platforms).
    - Monitor and Enforce age verification compliance for social media platforms using SevisPass, aligning with the Social Media Policy 2025.

3.6 Financial Institution Regulatory Authority

The BPNG will serve as the Financial Institution Regulatory Authority, overseeing the integration of SevisPass in the financial sector.

- Responsibilities:
    - Facilitate SevisPass adoption in banks, superannuation funds, and insurance companies for customer onboarding and ongoing due diligence, ensuring compliance with AML/CTF Act 2015 (Sections 15–29).
    - Develop guidelines for financial institutions to integrate SevisPass with eKYC processes, supporting General, Simplified, Standard, and Enhanced CDD requirements.
    - Collaborate with FASU to address data ecosystem gaps for Enhanced CDD (e.g., financial registries, PEP lists), as noted in the CDD Table (Appendix 1).
    - Promote financial inclusion by enabling unbanked and rural populations to access financial services via SevisPass.
    - Monitor financial institutions' compliance with SevisPass integration and report findings to DICT and NICTA.

3.7 AML & CTF Compliance Authority

The Financial Analysis and Supervision Unit (FASU) serves as the AML & CTF compliance Authority, ensuring the Digital ID System complies with anti-money laundering and counter-terrorist financing regulations.

- Responsibilities:
    - Monitor SevisPass use in financial institutions to ensure adherence to General, Simplified, Standard, and Enhanced CDD requirements (AML/CTF Act 2015, Sections 15–29).
    - Conduct risk-based assessments to prevent money laundering and terrorist financing, guiding Enhanced CDD implementation (e.g., PEP monitoring, source of wealth verification).
    - Collaborate with BPNG and DICT to integrate financial registries into the CIBVP for Enhanced CDD, addressing data ecosystem gaps (CDD Table, Section Four).
    - Provide training to financial institutions on AML/CTF compliance using SevisPass.
    - Report compliance issues and suspicious activities to NICTA and DICT for corrective action.

- Legislative Mandate: AML/CTF Act 2015, authorizing FASU to oversee AML/CTF compliance.

3.8 Civil Registry Authority

The PNGCIR serves as the Civil Registry Authority, providing foundational identity data for the Digital ID System.

- Responsibilities:
    - Maintain and update the National ID database and civil registry (births, deaths, marriages), ensuring data accuracy and standardization for SevisPass verification.
    - Integrate civil registry data with the CIBVP for eKYC verification, supporting tiered CDD requirements (AML/CTF Act 2015, Sections 15–29).
    - Facilitate registration for rural and marginalized communities through mobile units and offline options, aligning with inclusion objectives.
    - Support biometric data integration for SevisPass and future credentials, maintaining a secure identity database.
    - Participate in NICTA audits to ensure data quality and compliance with the Digital ID Trust Framework.

- Legislative Mandate: Civil Registration Act 1963, governing civil registration and National ID issuance.

- Alignment with Trust Framework: Adhere to data source and custodian standards.

3.9 Accredited Digital ID Providers

Digital ID Providers, for general purposes and for specific purposes, will be accredited in future by NICTA and these providers will have the authority to issue verifiable credentials under the Digital ID System, complementing SevisPass and enhancing sector-specific services, ensuring interoperability and adherence to established standards.

Relevant regulations will be developed to provide clarity and define categories and credential types of various Digital ID Providers.

All accredited Digital ID Providers are required to ensure the privacy and security of personal data, obtain informed consent from individuals for data sharing, and operate in compliance with Data Governance and Protection Policy 2024 and other relevant legislations.

Responsibilities:

- Issue credentials in compliance with the Digital ID Trust Framework, using biometric and document verification via the CIBVP.
- Ensure interoperability with SevisPass and public/private sector platforms, adhering to open standards (e.g., OAuth, OpenID Connect).
- Implement security measures (e.g., encryption, fraud detection) to prevent identity theft, aligning with set standards.
- Participate in NICTA audits and report credential issuance metrics to DICT and KTDC.
- Support inclusion by offering accessible issuance channels (e.g., mobile apps, offline options) for rural and disadvantaged communities.
- Alignment with Trust Framework: Adhere to issuance and usage standards.

3.10 Ecosystem Governance and Coordination

- NICTA as the designated Digital ID System Authority shall establish a multi-stakeholder governance body, including DICT, BPNG, FASU, PNGCIR, and private sector representatives, to oversee implementation, resolve disputes, and ensure compliance.

- Coordination Mechanisms: Regular stakeholder meetings, led by DICT, NICTA, and BPNG, shall align implementation with sectoral needs, supported by the industry-government working group.

- Monitoring and Reporting: NICTA shall submit quarterly compliance reports, while KTDC shall provide annual system performance reports, aligning with Section Four's M&E framework.

SECTION THREE – PROPOSED LEGISLATIVE FRAMEWORK

The section proposes for a robust legal and regulatory foundation to support the establishment, implementation, and sustainability of Papua New Guinea's Digital ID System**,** including SevisPass and future verifiable credentials (e.g., digital driver's licenses, passports, student IDs). This framework ensures alignment with the Digital ID Trust Framework, national legislation (e.g., AML/CTF Act 2015**,** Digital Government Act 2022), and global best practices (e.g., UK Digital Identity and Attributes Trust Framework, 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.

1. 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.

1.1 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 NICTA as the Digital ID Regulatory Authority**,** granting it powers to enforce the Digital ID Trust Framework, conduct audits, and impose penalties for non-compliance.
- 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 Digital ID Providers and regulating their operations, ensuring interoperability and compliance with open standards.
- Establish enforcement mechanisms over data custodians.
- Mandate cybersecurity protocols, including vulnerability assessments and incident reporting, to protect the CIBVP.

1.2 Civil Registration Act 1963

The Civil Registration Act 1963 mandates the registration of vital events (births, deaths, marriages) and issuance of National IDs but does not provide for digital integration or real-time data sharing with the Digital ID System. The following amendments are proposed:

- Authorize the Papua New Guinea Civil and Identity Registry (PNGCIR) to integrate its National ID database and civil registry with the CIBVP for eKYC verification, supporting tiered Customer Due Diligence (CDD) requirements.
- Mandate standardized data formats and secure data-sharing protocols (e.g., APIs, encryption) to ensure interoperability with the Digital ID System and compliance with the National Data Governance and Protection Policy 2024.
- Expand registration mechanisms to include mobile units and offline options, ensuring accessibility for rural and marginalized communities.
- Require PNGCIR to maintain a secure biometric database for SevisPass verification, adhering to ISO/IEC 19794 and privacy-by-design principles.

The overall outcome will be to Enable PNGCIR to serve as a foundational data custodian, addressing fragmented identity records and supporting inclusive registration.

1.3 Migration Act 1978 and Citizenship Act 1975

The **Migration Act 1978** and **Citizenship Act 1975** govern passport issuance and citizenship processes but lack provisions for digital passports as verifiable credentials or cross-border interoperability. The following amendments are proposed:

- Authorize the PNG ICSA to issue digital passports as verifiable credentials, integrated with SevisPass for travel authentication and visa applications.
- Mandate integration of passport and citizenship databases with the CIBVP for eKYC verification, supporting General and Standard CDD requirements.
- Incorporate provisions for cross-border recognition of digital passports, leveraging the Lagatoi Declaration (Pacific ICT Ministerial Dialogue, 2023) and international standards (e.g., ICAO Doc 9303 for machine-readable travel documents).
- Require secure data management protocols to protect passport data, aligning with the National Data Governance and Protection Policy 2024**.**

The overall outcome will be to enable PNG ICSA to support digital passport issuance and international interoperability, enhancing secure travel and identity verification.

1.4 Road Traffic Act 2014

The Road Traffic Act 2014 regulates driver licensing but does not provide for digital driver's licenses as verifiable credentials or integration with a national digital identity system. The following amendments are proposed:

- Authorize the PNG RTA to issue digital driver's licenses as verifiable credentials, integrated with SevisPass for authentication in insurance and law enforcement services.
- Mandate integration of driver's license records with the CIBVP for real-time verification, supporting eKYC processes and fraud prevention.
- Require secure data management and biometric verification for digital licenses, aligning with ISO/IEC 27001 and the Digital ID Trust Framework**.**

The outcome would be to enable PNG RTA to support digital driver's licenses, enhancing service delivery and interoperability.

1.5 Anti-Money Laundering and Counter Terrorist Financing Act 2015

The AML/CTF Act 2015 mandates KYC and CDD requirements but does not explicitly address the use of digital identities like SevisPass for compliance or integration with financial registries for Enhanced CDD. The follow amendments are proposed:

- Recognize SevisPass as a trusted tool for General, Simplified, Standard, and Enhanced CDD, enabling financial institutions to use biometric and demographic data for customer onboarding and transaction monitoring.
- Mandate integration of financial registries (e.g., beneficial ownership, PEP lists) with the CIBVP to support Enhanced CDD, addressing data ecosystem gaps noted in the CDD Table (Appendix 1).
- Authorize the FASU to oversee SevisPass compliance in financial institutions, including risk-based assessments and training.
- Require real-time transaction monitoring and fraud detection via SevisPass, aligning with Sections 15–29 of the AML/CTF Act 2015.

The outcome is to strengthen AML/CTF compliance requirements by leveraging SevisPass, promoting financial inclusion and regulatory efficiency.

1.6 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 KTDC**.** The following amendments are proposed:

- Formalize DICT's role as the Policy Authority and the designation framework for the Digital ID System Authority (Special Purpose Vehicle), with clear mandates for developing and managing the CIBVP.
- 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 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 CIBVP, ensuring governance and scalability of the Digital ID System.

2. 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**.**

2.1 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 (e.g., ISO/IEC 27001, OAuth, OpenID Connect).
    - Establish procedures for accrediting Digital ID Providers (e.g., Digizen, YuTru), 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.
    - Require custodians (e.g., PNGCIR, ICA, RTA) to maintain accurate, interoperable data sources and provide real-time access to the CIBVP, subject to privacy safeguards.
    - 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.

2.2 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 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 NICTA to conduct quarterly audits of data custodians and providers, 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.

2.3 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 (Section One).

- Key Provisions**:**
    - Mandate accessible registration and issuance channels, including mobile units, offline authentication, and disability-friendly interfaces, for SevisPass and other credentials (Focus Area 1.3.6, 3.7, 3.8).
    - Require custodians and providers to offer multilingual support and culturally appropriate processes to accommodate PNG's diverse population (Focus Area 1.2).
    - Establish funding mechanisms, via public-private partnerships, to support infrastructure development in rural areas, aligning with the Digital Government Plan 2023–2027 (Focus Area 3.1).

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

3. Legislative and Regulatory Timeline

The development and enactment of legislative amendments and new regulations shall align with the phased implementation roadmap outlined in Focus Area 3 (Section Two) to ensure timely legal support for the Digital ID System.

- *Phase 1: Foundation (0–12 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 Registration Act 1963**,** 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 (12–24 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 Registration Act 1963**,** Migration Act 1978**,** Citizenship Act 1975**,** 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 provider framework.

- Phase 3: Consolidation and Innovation (24–36 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 (Section Four).
    - 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 NICTA audit findings (Focus Area 3.4).

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

4. Governance and Oversight Mechanisms for Legislative Reforms

To ensure effective implementation and compliance, the legislative framework shall establish governance and oversight mechanisms for the Digital ID System.

The Public Service ICT Steering Committee shall establish an industry-government working group and include representatives from NICTA, BPNG, FASU, PNGCIR, Department of Justice, and private sector stakeholders, to oversee legislative implementation.

The body shall meet quarterly to align legislative progress with sectoral needs and monitor compliance with the Digital ID Trust Framework.

SECTION FOUR - MONITORING AND EVALUATION

A comprehensive Monitoring & Evaluation (M&E) framework will be established to ensure the effective implementation of the Papua New Guinea Digital ID Policy. This framework will focus on tracking key performance indicators (KPIs), assessing system impact, and addressing emerging challenges to ensure that SevisPass meets its goals and contributes to the broader digital transformation agenda.

1. Key Components

Among other indicators, these will be the basic indicators that will be monitored during the implementation and evaluated to assess the impact:

Enrollment Rates

- Regularly monitor the number of citizens enrolling in the SevisPass system.
- Ensure widespread adoption and equitable access, particularly in underserved regions.

Service Delivery Efficiency

- Measure the effectiveness and speed of service delivery using SevisPass.
- Ensure the digital ID system is facilitating seamless access to public and private sector services.

User Satisfaction

- Collect and analyze user feedback to assess satisfaction with the system.
- Identify areas for improvement in user experience, accessibility, and system usability

Security Review

- Conduct annual evaluations of the SevisPass system's security measures.
- Ensure protection against cyber threats and data breaches.

Scalability Assessment

- Evaluate the system's scalability to ensure it can accommodate future growth in user numbers and new service integration.

Impact on Financial Inclusion & Digital Service Uptake:

- Review the system's contribution to financial inclusion and increased access to digital services.
- Ensure it supports equitable growth and development.

2. Policy Review

The Policy will be reviewed two years from the official adoption to assess its effectiveness and ensure it remains relevant and up to date. It will be reviewed to ensure the following:

- Reflects current trends and practices, technological advances and business realities and contributing to the delivery of national development goals and strategic objectives.

- Ensures the implementation adheres to all relevant legal and regulatory requirements, including compliance with relevant regional and international standards and guidelines.

- Identifies Policy components that are inconsistent with and not delivering as intended to allow for adjustments and improvements to enhance efficiency and intended outcomes.

- Ensures the Policy is clear, and its implementation is understood by all stakeholders

- Identifies potential risks in the implementation and adjust the Policy directions accordingly to achieve the intended positive outcomes and mitigate any legal and regulatory inconsistencies.

APPENDIX 1: MAPPING OF CDDR AGAINST DIGITAL ID BB

This table below provides a detailed mapping of AML/CTF Act CDD requirements to GovStack's ID Building Block to guide implementation and compliance:

CDD Type	Key AML/CTF Act Requirements	GovStack ID BB Alignment	Feasibility
General CDD	Identify/verify customer, beneficial owner, agents, beneficiaries using reliable sources; ongoing due diligence; third-party reliance; block if CDD fails (Sections 15–20).	Supports enrollment/verification with registries, biometrics; real-time updates for ongoing monitoring; interoperable for third-party reliance; rules to block failed CDD.	High
Simplified CDD	Collect/verify basic data (name, address for individuals; corporate name, office for entities) for low-risk customers before transactions (Sections 21–22).	Captures basic attributes; verifies via registries or eKYC; enforces pre-transaction verification.	High
Standard CDD	Collect/verify detailed data (name, address, birth details, occupation for individuals; corporate details, ownership/control for entities; business purpose) before transactions, with low-risk exceptions (Sections 23–25).	Stores extended attributes; verifies via multi-source checks; supports beneficial owner/agent verification; configurable for timing exceptions.	High
Enhanced CDD	Collect/verify Standard CDD data plus source of assets/wealth, insurance beneficial owners; enhanced PEP monitoring; before transactions, with low-risk exceptions (Sections 26–29).	Captures additional data; verifies source of wealth via integrations (if available); supports biometrics for non-present cases; flags PEPs with risk-scoring.	Moderate to High

Notes:

- **High Feasibility**: GovStack's core features (registration, verification, interoperability) align well with General, Simplified, and Standard CDD, assuming registry integration.
- **Moderate to High for Enhanced CDD**: Source-of-wealth verification and PEP monitoring depend on Papua New Guinea's data ecosystem (e.g., financial registries, PEP lists).
- **Recommendations**: Integrate with civil/business registries, configure sanctions/PEP screening, and pilot workflows to ensure compliance with FASU oversight (Sections 61–106).

APPENDIX 2: ACRONYMS AND ABBREVIATIONS

The following table lists acronyms and abbreviations used in this policy, along with their meanings, to facilitate understanding for all stakeholders.

Acronym	Meaning
AML/CTF	Anti-Money Laundering and Counter Terrorist Financing
API	Application Programming Interface
BPNG	Bank of Papua New Guinea
CDD	Customer Due Diligence
CIBVP	Centralized Identity and Biometric Verification Platform
DICT	Department of Information and Communication Technology
DPI	Digital Public Infrastructure
eKYC	Electronic Know Your Customer
FASU	Financial Analysis and Supervision Unit
G2B	Government-to-Business
G2C	Government-to-Citizen
G2G	Government-to-Government
ICA	Immigration and Citizenship Authority (assumed as ICSA in context)
ICSA	Immigration and Citizenship Service Authority
ICT	Information and Communication Technology
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
ITU	International Telecommunication Union
KYC	Know Your Customer
M&E	Monitoring and Evaluation
NID	National ID
NICTA	National Information and Communication Technology Authority
PEP	Politically Exposed Person
PNGCIR	Papua New Guinea Civil and Identity Registry
PPP	Public-Private Partnership
RTA	Road Traffic Authority
SSO	Single Sign-On
SPV	Special Purpose Vehicle