PAPUA NEW GUINEA

Department of Information and Communication Technology (DICT)

Government Digital Identification (ID) Standards, Guidelines, and Specifications 2025

Document Control:

Document Name:	PNG Government Digital Identity Standards, Guidelines, and Specifications 2025
Prepared by:	Department of Information and Communications Technology
Edition:	Draft 5
Approved by:	
Date Approved:	
Effective Date:	
Next Review Date:	

<Table will be update once the standards document done>

Table of Content

Digital Identification (ID) Standards, Guidelines, and Specifications 2025

PART I. - PRELIMINARY.

1. NAME

This instrument is the PNG Government Digital Identification Standards, Guidelines and Specifications 2025.

2. COMMENCEMENT.

This instrument commences in December 2024.

3. AUTHORITY.

(1) This instrument is made under Section 64 of the Digital Government Act 2022.

(2) It references Section 37 of the Digital Government Act 2022.

4. SIMPLIFIED OUTLINE.

(1) All public bodies must comply with this instrument. This instrument prescribes the standards, guidelines and specifications that must be followed when developing, implementing and maintaining a digital identity, and while using digital credentials in Papua New Guinea.

(2) This instrument has been produced by the Department of Information and Communications Technology (DICT).

(3) All mentioned in (7) of this Part must comply with this instrument. <<insert parts when document is complete>>

(4) Notes are included in this instrument to help understanding by drawing attention to other provisions information and explanations. The notes are in small type, so that they don't disrupt the text. They do not contain statements of law.

5. DEFINITIONS

In this instrument, unless the context otherwise requires:
"biometric identifiers" means a unique physical or behavioral characteristic that can be used to identify an individual.

"credential provisioning" in a digital identification system means the processes and technologies used to issue, manage, and revoke digital credentials.

"de-provisioning" means the process of removing or disabling a user's access to systems, applications, and data when they no longer need it.

“digital identity management” means the process of creating, maintaining, and securing digital identities.

“digital signature” means a type of electronic signature to validate the authenticity and integrity of a digital document.

“identity and access management” or IAM, means a system that manages digital identities and controls access to resources.

“identity assurance level” means measurements of the reliability and accuracy of identity verification processes.

“identity proofing” means the process of establishing the identity of individuals or entities during the enrollment process through the collection, verification and validation of identity documents to create digital identities.

“public key infrastructure” means a system of hardware, software, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.

“revocation of digital identity” means the process of invalidating or disabling a user's credentials, access rights, or digital identity attributes.

“two-factor authentication” or 2FA, means a security process that requires users to provide two different types of information or credentials to verify their identity.

“Security Assertion Markup Language” or SAML, means an open federation standard used for authentication and authorization between identity provider and service provider.

“single sign-on” or SSO means an authentication process that allows a user to access multiple applications or systems with a single set of login credentials.

6. OBJECTS OF STANDARDS AND GUIDELINES

The objectives of these standards and guidelines are to:

(i) establish a secure and user-centric ecosystem for digital identities.
(ii) Enhance online security and simplify identity management, and
(iii) Establish a robust and secure digital ID ecosystem.
(iv) Facilitate seamless integration with existing and future government services.
(v) Promote the secure and efficient management of digital identities.
(vi) Enable interoperability between digital ID systems.
(vii) Establish compliance and audit procedures for ongoing monitoring and improvement.

7. SCOPE AND APPLICATION

(1) This instrument applies to all public bodies, businesses, persons and/or other entities that are involved in the process of developing or will be utilizing the digital identification system as a service.

(2) All/Any digital identification system or service provided or made accessible by a public body must comply with this instrument according to Section 37(8) of the Digital Government Act 2022.

8. NATIONAL DIGITAL IDENTIFICATION SYSTEM

(1) The Digital Transformation Policy 2020 encompasses measures for implementing secure and inclusive digital identification under the National Identification (NID) system, in line with e-Government Cloud efforts.

(2) The national digital identification system is a centralized framework designed by the government to give public bodies, businesses and people a reliable, secure, and trusted method of digital identification. The purpose is to simplify and improve the identity verification processes for accessing government services, completing transactions, and communicating online.

(3) The digital identification system will provide an effective a centralized identity management, secure authentication, interoperability, security and use convenience, while also enhancing ease access to services and will play a crucial role in digitizing public services, promoting digital inclusion and enhancing overall governance and security.

9. NATIONAL DIGITAL ID POLICY 2025

(1) The following standards outline in this instrument is guided by the principles and framework set out in the Department of Information and Communications Technology's (DICT) *National Digital ID Policy 2025*.

(2) The Digital ID policy provides a national vision for a secure, inclusive, and interoperable digital identity ecosystem in Papua New Guinea. It outlines the government's strategic approach to enabling digital identity as a foundational element for e-Government services, financial inclusion, and digital transformation across sectors.

(3) This Policy aligns with the DICT's objectives by establishing operational, legal, and technical standards for the creation, use, authentication, and governance of digital identities. It further supports multi-stakeholder engagement, promotes public trust, and ensures compliance with privacy, cybersecurity, and data protection requirements under applicable national laws.

9A. SEVISPASS DIGITAL IDENTITY ECOSYSTEM COMPONENTS

(1) The PNG Digital Identification System shall be implemented using a modular ecosystem known as the SevisPass Stack. This ecosystem includes the following digital infrastructure components:

(a) **SevisPass** – The primary digital identity credential (verifiable credential) issued to all eligible persons, uniquely identifying an individual for accessing public or private digital services.

(b) **SevisWallet** – A secure, user-managed mobile or web-based digital wallet that stores and manages verifiable credentials. Users may use it to share credentials, control consent, and receive notifications.

(c) **SevisPortal** – A self-service resident platform for pre-registration, booking enrolment appointments, requesting updates or corrections, and accessing issued credentials.

(d) **SevisAdminPortal** – The administrative and governance portal for accredited issuing entities to issue, revoke, and manage credentials. It also hosts the Trust Registry of issuers and verifiers.

(e) **SevisDEx** – The national Data Exchange Platform that enables secure, auditable, consent-driven data sharing between government systems and authorized private sector entities.

(2) All government and authorized digital ID service providers must integrate their systems with the SevisPass ecosystem using open APIs and technical guidelines provided by DICT.

10. LEGAL AND REGULATORY CONSIDERATIONS

(1) All public bodies and persons utilizing a government digital identification system must take into consideration:

a) Existing national and international laws, regulations, standards, and frameworks as listed in Appendix 1.
b) Fundamental human rights and freedoms as enshrined in the PNG Constitution, ensuring that individuals' rights to privacy and personal data protection are respected.
c) Collaboration between the digital ID system and national security and law enforcement agencies to address security concerns while respecting legal requirements and individuals' rights.
d) Establishing a regulatory authority
e) Public bodies or entities or individual must consider BPNG_Customer Due Diligence Standards, when cash transactions exceeds K10,000.00 to avoid potential money laundering or terrorist financing risks.

PART II.- GOVERNANCE AND POLICY STANDARDS AND GUIDELINES FOR DIGITAL IDENTIFICATION SYSTEMS IN PNG

11. Overview

(1) This Part establishes the governance and policy framework that governs the design, implementation, and oversight of digital identification (ID) systems in Papua New Guinea.

(2) The objectives of these standards are to ensure the development of inclusive, rights-respecting, and sustainable digital identification ecosystems across public and private sectors

(3) These standards apply to identity providers and digital identification systems.

STANDARD 1 GUIDING PRINCIPLES FOR DEVELOPMENT OF DIGITAL IDENTIFICATION SYSTEMS

(1) These following provisions outlines standards and guidelines for designing and managing a secure, inclusive, and interoperable digital identification (Digital ID) system for Papua New Guinea (PNG).

(2) The main objectives of these are to provide support for the use of digital identification systems across public and private sectors and simultaneously align with the national digital transformation agenda and international best practices.

STANDARD 1.1 DIGITAL IDENTIFICATION GOVERNANCE AND LEGAL FRAMEWORK IN PAPUA NEW GUINEA

1.1.1. Legal Compliance

(1) All digital identification systems must be in compliance with related acts, regulations, policies, standards, guidelines and specifications, including those provided in this instrument. This includes compliance with the PNG National Data Protection and Data Governance Policy 2024, the Digital Government Act 2022, Cybercrime Code Act 2016, and any provisions related to it.

(2) The digital identification system must empower existing Civil and Identity Registry act, regulation or policy.

(3) Additionally, it should allow for support for future legislative developments including the Digital Identity Act or Data Governance regulation (if any).

1.1.2. Institutional Governance

(1) Oversight should be provided by the Department of Information and Communications Technology (DICT) and working in collaboration with Civil and Identity Registry.

(2) If required or necessary, establish a close working group consisting of representatives from relevant stakeholders and technical expertise from the public, private, and civil society actors.

(3) It is also important to have regulatory enforcement and audited by an independent authority.

STANDARD 1.2 ALIGNMENT WITH REGIONAL AND GLOBAL STANDARDS

(1) All Papua New Guinea’s digital identity systems should be aligned with all relevant international standards which includes, but is not limited to:

(a) ISO/IEC 24760 Series (A framework for identity management):
(b) ISO/IEC 29115 (Entity authentication assurance framework):
(c) NIST SP 800-63 Series (Digital Identity Guidelines - U.S. standard):
(d) World Bank’s ID4D Principles:

(e) GDPR and Data Protection Laws (where applicable for cross-border or cloud services):
(f) eIDAS Regulation (EU)

(2) Digital identification systems should also consider the following regional standards and models;
(a) Australia's Trusted Digital Identity Framework
(b) APEC Privacy Framework & CBPR System

STANDARD 1.3 USABILITY, ACCESSIBILITY, AND INCLUSION STANDARDS

1.3.1 Language

(1) The digital identification system must be able support all languages, ensuring user interfaces in both English and Tok Pisin (if available).

1.3.2 Offline Capabilities

(1) Digital identification systems must allow for verification and authentication without a network connection, crucial in areas with limited or no internet access. This may be achieved through technologies like smartcards or digital wallets, providing a secure and reliable means of identity validation even when offline.

(2) Additionally, there must be SMS and USSD fallback mechanisms in place and should provide offline sync capabilities.

1.3.3 Rural and Remote Support

(1) In all development of digital identification systems, ensure it allows for remote support through prioritizing registration of users in remote and rural or marginalized communities.

(2) This may be achieved through the use of satellite internet and VSAT systems.

(3) Note that it is important citizens in the communities are trained on digital identification systems and procedures.

Standard 1.3.4 Inclusivity

(1) All digital identification systems must serve all persons regardless of geographic, economic, gender or linguistic barriers, including those persons with disabilities.

(2) There should be alternatives ti

STANDARD 1.3A USER RIGHTS AND GRIEVANCE REDRESS

(1) Digital ID systems must include grievance mechanisms accessible by all users regardless of literacy, location, or access to digital devices. The mechanisms must include:

(a) Walk-in service counters (in DICT offices or Civil Registry) (b) Toll-free call centres (c) Online complaint submission via SevisPortal (d) Community-based support via ward offices or accredited agents

(2) A grievance resolution unit must be established under the Implementation Authority to oversee complaints, including:

(a) Complaint classification and prioritization (b) Escalation procedures and defined timelines (c) Public reporting of redress performance

(3) Every user has the right to: (a) View and download their data via SevisWallet or SevisPortal (b) Request corrections to inaccurate personal data (c) Revoke access to issued credentials (except where legally mandated) (d) Be notified when their credentials or data are accessed by a third party

(4) DICT will issue guidelines to ensure user grievance data is logged, monitored, and used to improve systems and services over time.

STANDARD 1.4 DATA PROTECTION AND PRIVACY

(1) All digital identification systems must comply with relevant data protection, data governance and data privacy laws, regulations, standards and guidelines.

(2) User consent mechanisms must be implemented to ensure proper data collection and sharing practices.

(3) The data minimization principle must always be utilized during data collection and storage, ensuring necessary personal data is collected during registering a digital identity.

(4) Digital identity providers must always ensure the protection of personal data, including mechanisms for data encryption, secure storage, and access controls.

STANDARD 1.5 SECURITY AND TRUST

(1) Digital identification systems must adopt cryptographic standards and robust authentication protocols, data protection measures, and compliance frameworks.

(2) Authentication and authorization mechanisms are important to verify user identities and grant appropriate access to digital services. This may include strong passwords, multi-factor authentication, and biometric verification.

(2) All identity providers must apply a zero-trust architecture for internal systems and ensure there is regular penetration testing and auditing.

STANDARD 1.6 INTEROPERABILITY

(1) Digital identification systems must adopt open APIs and standards to ensure compatibility across government, financial institution and health systems.

(2) If applicable, ensure that the system may support international interoperability.

1.7 DISASTER RECOVERY AND BUSINESS CONTINUITY

(1) Data backups must be implemented regularly,

(2) Ensure business continuity through data backups, disaster recovery, and offline operations. All digital identification systems must be compliant with ISO 22301-compliant Disaster Recovery (DR) plan.

(3) Digital identification system infrastructure and services must be built to withstand disruptions and recover swiftly, ensuring that all services must maintain high availability and restore operations within agreed recovery times.

(4) During disaster recovery, the integrity and confidentiality of identity data must not be compromised.

(5) Essential identity verification and authentication services must be accessible during emergencies.

STANDARD 1.8 TESTING, CERTIFICATION AND COMPLIANCE

1.8.1 Testing

All digital identification system must go through the following testings;

Functional Testing

(1)Validate system features such as identity registration, verification, authentication, and revocation.

(2) Test for accessibility, multilingual support, and performance under local PNG conditions (low bandwidth, mobile-first).

Security Testing

(1) Penetration testing, vulnerability scanning, and code review.

(2) Must comply with ISO/IEC 27001 and OWASP Top 10 security risks.

(3) Evaluate resilience against:

- Identity theft
- Spoofing attacks
- Insider threats

Performance Testing

(1) Simulate load scenarios (e.g. 10,000 concurrent authentications).

(2) Stress-test backend systems (databases, APIs, identity matching engines).

(3) Ensure high availability (≥ 99.9% uptime target for Tier 1 services).

Interoperability Testing

(1) Test for seamless integration with:

(2) Government systems (e.g., Health, Education, Tax)

(3) Financial institutions (e.g., eKYC)

(4) Third-party platforms (via OpenID, OAuth, SAML, etc.)

Additionally, biometric performance testing using ISO/IEC 19795.

1.8.2 Audits and Reporting

(1) Regular auditing and reporting must be done by identity providers.

STANDARD 1.9 PRIVATE SECTOR INTEGRATION

1.9.1 eKYC and Financial Services

(1) Read-only API access for licensed entities.

(2) User consent and logging for each KYC request.

Note: Refer to Part 3 for standards relating to EKYC

1.9.2 Digital Signatures

(1) Digital signing tools for businesses and individuals.

(2) Aligned with e-Transactions Act and future e-Signature legislation.

1.9.3 Federated ID Support

(1) Login with PNG ID feature for employers, schools, and service providers.

(2) Token-based single sign-on architecture.

STANDARD 1.10 ETHICAL AND HUMAN RIGHTS GUIDELINES

(1) Digital identification systems must be inclusive and avoid reinforcing social, gender, or economic inequalities. The system should be designed to actively prevent bias. Note that if the system is not designed and implemented carefully, it can

(2) Children, persons with disabilities, and minority groups must be given additional protections to ensure safe and fair use of digital ID systems.

(3) The use of digital identities must not enable surveillance or compel users to disclose more data than necessary.

STANDARD 1.11 – GOVERNANCE MODEL AND MULTI-STAKEHOLDER STRUCTURE

(1) The governance of PNG's Digital ID System shall follow a federated model coordinated by the Department of Information and Communications Technology (DICT).

(2) Key roles include:

(a) **Policy Sponsor (DICT):** Provides national leadership, drafts standards and policies, coordinates funding and development partner support

(b) **Digital ID Regulatory Authority (NICTA or other delegated body):** Issues licenses, accredits partners, enforces compliance, and maintains the Trust Registry

(c) **Digital ID Implementation Authority:** Responsible for SevisPass operations, enrolment rollout, platform maintenance, and user support

(d) **Interagency Steering Committee:** Includes DICT, BPNG, PNGCIR, NICTA, RTA, IRC, and others to guide cross-sector policy alignment

(e) **Technical Advisory Committees:** Include academics, CSOs, technical experts to guide standards and future upgrades

(f) **Auditing Bodies (Auditor General's Office or third-party):** Conduct periodic system audits on performance, security, and user protection

(3) All institutional responsibilities shall be defined using a RACI (Responsible, Accountable, Consulted, Informed) framework, to be published in the implementation guidelines.

(4) DICT shall publish an annual governance performance report based on audit findings, partner reports, and user feedback.

GUIDELINE 1

PART III. - DIGITAL IDENTIFICATION LIFE CYCLE STANDARDS

11. Overview

(1) This Part outlines the digital identification lifecycle and associated standards that support the secure creation, management, authentication, and utilization of digital identities within an interoperable and trusted ecosystem.

(2) This Part establishes standardized procedures governing the full lifecycle of digital identities—from creation to deletion—to promote consistency, mitigate fraud risks, and safeguard individual privacy. It aims to foster trust and confidence across transactions involving individuals, identity providers, and relying parties within both the public and private sectors.

Standard 2 Identity Lifecycle Management

(1) The process of establishing a person's identity and then using this identity in later transactions involves multiple stages often referred to as the "**identity lifecycle**". This lifecycle is outlined in Figure 1 below.

(2) The following standards and specifications outline basic requirements for each phase of digital identity lifecycle.

STANDARD 2.1 REGISTRATION AND ENROLLMENT OF A DIGITAL IDENTITY

2.1.1 Claiming a Digital Identity

(1) A person may claim a digital identity by providing personal data and supporting documents and any other evidence that will enable successful registration of the identity.

2.1.2 Data Collection

(1) Data that may be collected upon registration of a digital identity include:

a) biographic data

Data Field Name	**Specification**	**Mandatory**
First Name	Data type: Text Length: 255 characters Others: Unicode (UTF-8), legally recognized first name, not nicknames, short forms, or initials, and allow for standard alphabetic characters, spaces, and possibly accented character	Mandatory
Last Name	Data type: Text Length: 255 characters Others: Unicode (UTF-8), legally recognized surname, not nicknames, short forms, or initials, and allow for standard alphabetic characters, spaces, and possibly accented character	Mandatory
Phone Number		Mandatory
Email Address		Mandatory
Date of Birth	Format: DD-MM-YYYY OR YYYY-MM-DD	Mandatory
Gender	Male, Female, Unspecified	Mandatory
Place of birth	Province > District >LLG>Ward/ Village	Mandatory
Residential Address	Lot>Section>Street>Suburb>LLG>District>Province	Mandatory
Corresponding Address (Postal)	Format: PNG National Address	Mandatory
Nationality	ISO 3166-1	Mandatory

- Optional: Clan name, Alternate names, National Health ID, Taxpayer Identification Number.

b) biometric data

Type	**Modality**	**Specification**
Biological	Fingerprints	ISO/IEC 19794-2 (fingerprint data); 500 DPI resolution; WSQ format; slap scan (4-4-2); False Match Rate (FMR) ≤ 0.01%; live scan only
	Face	ISO/IEC 19794-5 (face image data); frontal pose, neutral expression; JPEG or JPEG2000 format; liveness detection mandatory; FAR ≤ 1%; lighting must be uniform
	Iris	ISO/IEC 19794-6 (iris data); 640x480 pixels minimum; capture distance 10–40cm; FNMR ≤ 0.05%; quality assessment using ISO/IEC 29794-6
Behavioral	Keystroke dynamics	Captures dwell time, flight time; used as a secondary factor; fallback to OTP if mismatch; format follows behavioral biometric practices (NIST SP 800-63)
	Signature	ISO/IEC 19794-7 (signature data); dynamic capture (stroke, pressure, speed); biometric pad or touchscreen capture; supports audit verification and cryptographic storage
	Voice	ETSI ES 202 212 (Speaker Verification); 5–10 sec clean sample; < 40 dB background noise; anti-spoofing required; supports both text-dependent and text-independent models

- Fingerprints and facial biometrics captured per ISO/IEC 19794.
- Biometric quality checked against ISO/IEC 19795 and FMR/FNMR metrics.
- Use of mobile biometric kits for rural/remote enrolment.

(3) Enrollment of a digital identity must be conducted through NID field offices or partner locations, capturing biometrics and demographic data.

(4) The core identity attributes are further described below:

2.1.3 Enrolment Channels

(1) Digital identities may be registered at fixed enrolment offices at District HQs. Additionally, there may be mobile registration units, to provide ease of access to users and citizens.

(2) Employ Community-based agents with training and audit trails.

2.14 De-duplication and Verification

(1) Utilise Automated Biometric Identification System (ABIS), and other relevant technologies to decrease de-duplication of identities.

(2) Integration with existing systems such as the Electoral Roll, and NID system, is important to be used in cross-validation.

STANDARD 2.2 IDENTITY PROOFING

(1) All digital identities must be subject to identity proofing, a phase of digital identity lifecycle in which the claimed digital identity is validated against all evidence collected during initial enrollment. This is important to ensuring all evidence is genuine and correct, and verifies that the claimed identity exists in the real world.

2.2.1 Validation of Claimed Identity

(1) The assurance of a claimed digital identity should be established through evidence provided that meet some or all of the identity proofing objectives.

- Identity Evidence Collection
- Evidence Validation
- Identity Verification
- Deduplication Check
- Assurance Level Assignment

(2)

STANDARD 1.3 IDENTITY ASSURANCE LEVELS

(1) When identity proofing a digital identity, these claims of the digital identity is categorized into identity assurance levels which gives the level of confidence or assurance that a system can have in the users identity or credentials. This may be deducted using a combination of self-assertion, evidence and in-person verification.

(2) In alignment with international best practices, three Identity Assurance Levels (IALs) are defined and include:

IAL1: Basic Assurance

IAL2: Moderate Assurance

IAL3: High Assurance

(1) Matches data against the Civil Registry and other national databases.

(3) A claim to a digital identity can be verified using the following methods:

Type	Method
Document-based	NID card/birth certificate, passport, drivers license
Vouching	Approved village magistrate, ward councillor, LLG official (National Identity Policy)
Digital Verification	

(1) Note that higher levels of assurance reduce the risk of fraudulent identity.

STANDARD 1.4 CREDENTIAL ISSUANCE

(1) A unique digital ID and credential must be issued once the digital identity is verified.

(2) These credentials may be issued in the forms and specifications highlighted in the table below.

Form	**Details**	**Specifications**
Physical/Digital Credentials	Smartcard – a printed ID with a QR/Near Field Communication chip installed	Size: 85.60mmx54mm (CR80 standard ID card size) Features: NRF chip installed, or QR print
Digital Only	-Mobile ID stored in a secure digital wallet (app or SIM-based) -digital certificates -Username/password - Unique digital ID number -Biometrics	Mobile ID (App/SIM): - Format: W3C Verifiable Credentials (VCs) or ISO/IEC 18013-5 (mDL). - Storage: In a certified Secure Element (SE) or Trusted Execution Environment (TEE) on the mobile device. Digital Certificates: - Standard: X.509 v3 certificates, issued by a certified Registration Authority (RA). Username/Password: - Specs: Password must meet minimum complexity requirements (e.g., 12+ chars, upper/lower case, numbers, symbols). Unique Digital ID Number: - Format: Alphanumeric UUID as the primary identifier for all digital interactions. Biometrics: - Usage: Used for local device unlock and/or remote authentication. - Format: On-device matching only; biometric templates stored securely in TEE/SE (never on a server).
Additional credentials	Credentials that may be used to confirm a person is associated with a digital a digital credential including: -Pin, or password -OTP -Security Questions -Token	PIN/Password: - PIN: 6-8-digit number for local credential activation (e.g., smartcard PIN). OTP (One-Time Password): - Standard: Time-based OTP (TOTP) RFC 6238 (e.g., via Google Authenticator) or SMS-based OTP (less secure).

		Security Questions: - Specs: Pre-defined questions where answers are hashed and stored. Considered a secondary, low-assurance factor. Token: - Type: FIDO2 security keys (WebAuthn), hardware OTP tokens (e.g., YubiKey). Provides high-assurance multi-factor authentication (MFA).
Digital/Additional Features	Biometrics	Types: - Primary (for authentication): Facial Recognition (ISO/IEC 19794-5), Fingerprints (ISO/IEC 19794-2). - Secondary/Optional: Iris recognition, voice recognition. Implementation: - Liveness Detection: Required to prevent spoofing (e.g., presentation attack detection). - Template Storage: Only secure biometric templates are stored/used, never raw images. Usage: Serves as both an attribute (on the credential) and a factor for authentication (verifying the holder).

(2) The core identity attributes collected upon registration of the digital identity, including issuance data will be embedded within the credentials issued.

Data Attribute	Data Format	Details/Specifications	Mandatory/Optional
Unique Identity Number	Alphanumeric (UUID)	A Version 4 UUID, generated by the issuing authority. This is the primary, immutable key for the identity record and is embedded in all credentials.	Mandatory
Full Name	Text (Unicode)	The individual's full legal name as verified by an official source document (e.g., birth certificate, passport). Format: [Surname], [Given Names].	Mandatory
Date of Birth	ISO 8601 (YYYY-MM-DD)	The verified date of birth. Must be validated against a trusted source.	Mandatory

Gender	Text (Predefined Code)	Represented by a standard code. **Values:** M (Male), F (Female), X (Non-binary/Unspecified). Based on official documentation.	Mandatory
Nationality	Text (ISO 3166-1 Alpha-3 code)	The holder's nationality. Represented by a standardized 3-letter country code (e.g., USA, GBR, ZAF).	Mandatory
ID photograph	Binary (JPEG2000)	A recent, front-facing portrait photo. **Specs:** Size: 35x45mm (within card), Resolution: 600 DPI, Background: plain light grey or white.	Mandatory
Date of Issue	ISO 8601 (YYYY-MM-DD)	The date the credential was initially issued by the authority.	Mandatory
Date of Expiration	ISO 8601 (YYYY-MM-DD)	The date after which the credential is no longer valid. Set by policy (e.g., 5 years from issue).	Mandatory
Signature	Binary (Vector Image/PNG)	A scanned image of the holder's official signature. Stored as a secure, non-alterable digital image.	Mandatory
QR code/ NFC Reference	Alphanumeric (URI)	A unique reference number or a secure URL (e.g., https://verify.gov.qa/id/<UUID>) that points to the official verification service. This is encoded in the QR/NFC chip.	Mandatory
Biometrics Reference	Binary (Standardized Template)	**Not the raw biometric image.** A secure, mathematical template derived from facial recognition. **Standard:** ISO/IEC 19794-5 (Face). Used for 1:1 verification against the physical holder.	Mandatory
ADDITIONAL ATTRIBUTES			
Email Address	Text (RFC 5322 compliant)	A personal email address for communication, notifications, and account recovery. Must be verified through a confirmation email with a validation link.	Optional
Phone Number	Text (E.164 format)	A personal mobile number for communication, two-factor authentication (2FA), and recovery. Format: +[Country Code][Subscriber Number] (e.g., +675 71234567). Must be verified via SMS OTP.	Optional

Residential Address	Text (Structured)	The primary, verified place of residence. Format: [Street Number, Street Name], [City], [Postal Code]. Used for service eligibility and official correspondence.	Optional
Corresponding Address	Text (Structured)	An alternate mailing address for correspondence, if different from the residential address. Format: [Street Number, Street Name], [City], [Postal Code].	Optional
Marital Status	Text (Predefined values)	Standard values: Single, Married, Divorced, Widowed, Civil Union. Used for benefits, tax, or census-related services.	Optional
Disability Status	Text (Code)	Used for access to specific government services and benefits. Should use a standard classification code from an accepted framework (e.g., the International Classification of Functioning, Disability and Health - ICF by WHO).	Optional
Educational Qualification	Text (Structured)	The highest achieved educational qualification. Should be structured using a standard framework level (e.g., ISCED 2011 levels: Level 6 - Bachelor's, Level 7 - Master's, etc.).	Optional

(3) Issuance of credentials in Papua New Guineas digital identity ecosystem must follow international best practices and opend standards to ensure interoperability, privacy, security and scalability. The

(4) The issuance of digital credentials in PNG shall adhere to the OpenID for Verifiable Credential Issuance (OID4VCI) specification. This protocol enables secure, privacy-preserving, and interoperable issuance of digital credentials using OAuth 2.0. U

(4) Users must:

- Implement dynamic client registration and metadata discovery.
- Use secure credential binding (e.g., cryptographic keys).
- Support interoperable formats such as W3C Verifiable Credentials and SD-JWT VC.
- Provide deferred issuance support where needed.
- Ensure compliance with replay prevention and access token validation requirements.

STANDARD 1.5 UNIQUE IDENTIFIERS

(1) A digital identity is given a unique identifier once initial verification is complete. This may be 12-digit numeric ID generated randomly.

(2) The unique identifier should not be derived from any personal data.

(3) This may be in the format: PNG-XXXXXXXXXXXX

STANDARD 1.6 ACTIVATION AND AUTHENTICATION OF A DIGITAL IDENTITY

(1) To claim the digital identity, it must be activated or authenticated by one or more authentication factors associated with the issued credential.

(2) This may be according to three authenticators;

a) Possession factors, e.g. physical smart cards, digital card/certificate.

B) Knowledge factors, e.g. security questions, or passwords/pins.

C) Inherent factors, e.g. biometrics – fingerprint/iris scan

STANDARD 1.7 AUTHORIZATION

(1) Using a digital credential to access a service must only be granted based on roles or verified attributes.

(2) All authorizations must be based only on informed user consent.

(3) Logging and audit controls should be put in place to monitor all access and authorization of the digital identity.

(3) Ensure the digital identification system implement RBAC or ABAC to manage authorization decisions.

STANDARD 1.8 REVOCATION

(1) Digital identity credentials must be updated, revoked, or reissued, under the following conditions;

(a) Expired credential validity, failure to renew/update credentials, or prolonged account inactivity.

(b) Fraud or misuse, either use of fake identities/impersonation, false data or identity used to conduct criminal/illegal activities.

(c) Suspected identity theft, account breach or leaked or stolen credentials.

(d) If the user requests for digital identity to be deactivated, deleted or replaced (for good reason).

(e) Legal mandate (Court order, compliance issues, or regulatory breach)

(f) Deceased persons – confirmed death of digital identity holder.

(2) The digital identity holder must be notified through email or official letter.

(3) Maintain logs of revocation actions, date/time, reasons, authorized personel and revocation method.

(3) In other cases, digital identity credentials may be suspended through a temporary deactivation of the account pending investigation or resolution. The suspended account will be reinstated or revoked within a 30-day period.

(4) Persons may appeal a revocation decision through an official application with documents supporting reinstatement of the credentials. A new digital identity and credentials may be reissued if the identity is verified again. Note that account recoveries must follow KYC procedures and maintain a unique identifier, unless there are fraudulent activities involved in revocation.

PART IV TECHNICAL STANDARDS FOR DIGITAL ID SYSTEMS

STANDARD 3. RISK MANAGEMENT AND MITIGATION

(1) All implementing agencies must establish a digital ID risk management plan based on the following classifications:

(a) **Institutional Risks** governance failures, duplication of mandates, poor coordination

(b) **Technical Risks** cybersecurity threats, infrastructure outages, data leaks

(c) **Access Risks** digital exclusion, low digital literacy, service denial

(d) **Privacy Risks** unauthorized data access, non-consensual disclosure

(e) **Vendor Risks** overdependence on foreign technology, non-compliant vendors

(2) Required mitigation mechanisms shall include:

(a) Business continuity plans and ISO 22301-compliant disaster recovery processes

(b) Offline services and fallback authentication (QR codes, USSD, SMS)

(c) Two-factor or biometric authentication to protect identity access

(d) Consent logs and access trails for all credential usage

(e) Regular audits and mandatory reporting to DICT and the ID Regulatory Authority

(3) Each accredited service provider shall submit a biannual risk assessment report to the Regulatory Authority.

PART V. - TECHNICAL STANDARDS AND SPECIFICATIONS FOR DIGITAL IDENTITFICATION SYSTEMS

Standard 4. Architecture Layers

(1) The following provides an overview of the digital architechure of what all digital identification systems should look like,

Presentation Layer

- Interfaces for citizens, businesses, and government employees.
- Web and mobile platforms accessible via login.gov.pg and service portals.

Application Layer

- Identity Services: Registration, identity proofing, deduplication, and verification.
- Authentication Services: MFA, biometrics, PIN/OTP.
- Credential Management: Issue and revoke credentials, including digital ID cards and biometric templates.

Integration Layer

- Core Registries: National Identification (NID), Civil Registration, business registry (IPA), land registry, health and education databases.

- Logs and Metadata: Centralized audit trails to support non-repudiation and monitoring.
- Identity Data Exchange: API gateway layer for secure interoperability.
- Identity Provider (IdP): Central authentication broker supporting federated login across platforms.

Infrastructure Layer

- eGovernment Cloud: Provides secure compute, encrypted storage, Hardware Security Modules (HSMs), and automated backups.
- Supports containerized microservices and follows a zero-trust security model.

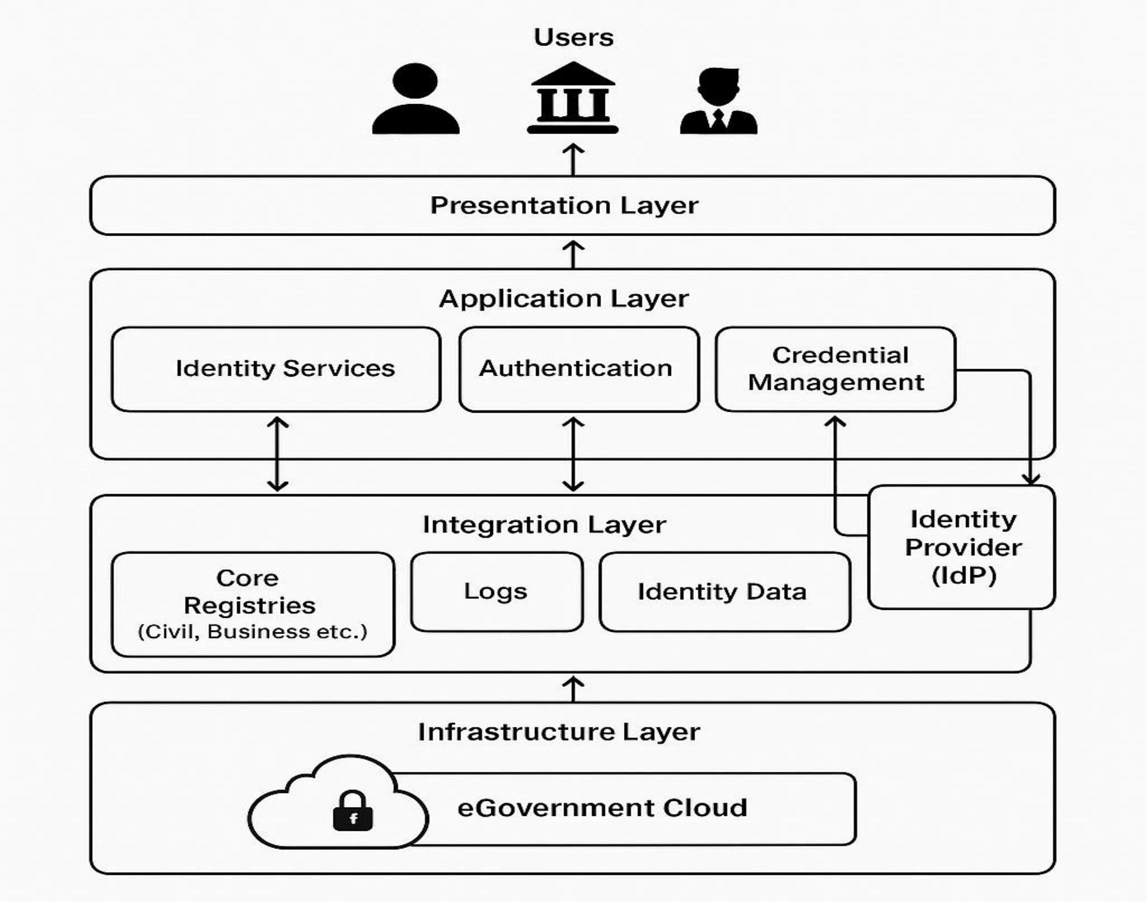

Figure above shows a visual diagram of the above architecture layers.

Standard 4.1 Standards and Protocols

The following standards and protocols must be employed in all digital identification systems;

(1) OpenID Connect, OAuth 2.0, SAML 2.0: Enable secure federated identity management.

(2) X.509 Digital Certificates: For authentication and signing.

(3) Biometric Standards: ISO/IEC 19794 series and PNG NID biometric specifications.

(4) W3C Verifiable Credentials: For future-proof and interoperable identity representation.

Standard 4.2. Security and Privacy

(1) Encryption: All data in transit uses TLS; at rest, AES-256 encryption is applied.

(2) Consent Management: Citizens are prompted to provide informed consent before sharing data.

(3) Zero Trust: Every identity and device must be continuously verified.

(4) Audit Trails: All transactions are logged and stored in tamper-proof formats on cloud infrastructure.

(5) Compliance: Aligns with the PNG Data Protection and Privacy Policy (in development).

Standard 4.3 STANDARD USABILITY AND ACCESSIBILITY

Language Support

(1) Supports English andTok Pisin (if available)

Offline Support

(1) QR code verification should allow for local signature check

Disability support

(1) Text-to-speech, screen reader compatibility

Device support

(1) Android 8+, iOS 12+, web browsers (for QR use)

<<INTEGRATION STANDARDS>>

Standard 4.4 Integration with eGovernment Cloud

(1) Identity services are hosted in the PNG eGovernment Cloud, ensuring central availability, security, and performance.

(2) Enables shared authentication service (login.gov.pg) for ministries, service portals, and provincial eServices.

(3) APIs enable secure integration with banks (eKYC), telecoms (SIM registration), education (student ID), and health (eHealth ID).

(4) Disaster recovery, monitoring, and scaling are managed centrally under DICT’s cloud operations.

Standard 4.5 Future Enhancements

(1) Self-Sovereign Identity (SSI) pilots for decentralized identity control.

(2) Mobile-first Digital Identity Wallets to expand access to remote communities.

(3) Cross-border Digital Identity Recognition, starting with Pacific Island partnerships (e.g., Pacific ID).

PART VI. - EKYC AND COUNTER – TERRORIST FINANCING/ANTI-MONEY LAUNDERING (CTF/AML) STANDARDS

12. OVERVIEW

(1) This Part establishes the standards for Electronic Know Your Customer (eKYC) processes and the use of the National Digital Identity System for Counter-Terrorist Financing and Anti-Money Laundering (CTF/AML) compliance.

(2) The objective is to leverage the SevisPass Digital ID to create a secure, efficient, and reliable digital onboarding and monitoring framework for regulated entities, primarily in the financial sector. This enhances financial inclusion, reduces fraud, and strengthens PNG's integrity against financial crimes.

(3) These standards apply to all Reporting Entities as defined under the Anti-Money Laundering and Counter-Terrorist Financing Act [or relevant Act], including:
(a) Banks and other deposit-taking institutions;
(b) Insurers;
(c) Remittance service providers;
(d) Securities dealers;
(e) Other entities prescribed by the Central Bank (Bank of Papua New Guinea - BPNG) or relevant regulator.

STANDARD 5.1 – eKYC PROCESS AND INTEGRATION

5.1.1Digital Identity Verification

(1) Reporting Entities must use the SevisPass ecosystem for customer identity verification where available and for the level of assurance required for the business relationship.

(2) The process must involve:
(a) Customer Consent: Obtaining explicit, informed, and auditable consent from the customer via the SevisWallet to share their identity data for KYC purposes.
(b) API-Based Verification: Using the standardized, secure APIs provided by DICT to query the SevisPass system.
(c) Data Minimization: Requesting only the minimum data attributes necessary for the specific KYC obligation (e.g., name, ID number, photo, and date of birth for standard verification; address may be requested separately if needed).

5.1.2 Assurance Level Mapping

(1) The required Identity Assurance Level (IAL) for a business relationship must be risk-based:
(a) IAL2 (Moderate Assurance): Mandatory for establishing all formal account-based customer relationships (e.g., bank accounts, insurance policies).
(b) IAL1 (Basic Assurance): May be sufficient for low-value, low-risk products or initial inquiries, subject to the Reporting Entity's risk assessment.

5.1.3 Record Keeping and Audit Trail

(1) Reporting Entities must maintain a secure, tamper-evident log of every eKYC transaction for a minimum period of seven (7) years after the end of the business relationship. The log must include:

(a) Timestamp of the request;
(b) Unique transaction reference;
(c) Customer consent token;
(d) Specific data attributes accessed;
(e) Purpose of the request (e.g., "Account Opening - Savings Account").

STANDARD 5.2 – ONGOING MONITORING AND SCREENING

5.2.1 Ongoing Due Diligence

(1) Reporting Entities may use the digital identity system, with customer consent, to facilitate ongoing due diligence, including:
(a) Confirming the continued validity of a customer's credentials.
(b) Updating customer information (e.g., address) if updated in the central civil registry and shared via a secure channel with consent.

5.2.2 Watchlist and Sanctions Screening

(1) Reporting Entities remain solely responsible for screening customers against relevant national and international sanctions lists, politically exposed persons (PEP) lists, and other relevant watchlists.
(2) The Digital ID system may provide a unique, verifiable identifier to enhance the accuracy of this screening process and reduce false positives.

STANDARD 5.3 – RISK-BASED APPROACH AND TRANSACTION MONITORING

5.3.1 Risk Assessment

(1) The use of a high-assurance digital identity must be a core factor in a Reporting Entity's customer risk assessment model, potentially lowering the inherent risk profile of a customer.
(2) Reporting Entities must not rely solely on digital identity verification for high-risk customers and must apply Enhanced Due Diligence (EDD) measures where required by law.

5.3.2 Triggering Events

(1) A revocation, suspension, or reported compromise of a customer's SevisPass credential must be treated as a high-risk trigger event.
(2) Upon receiving a notification (via a subscribed API alert) or otherwise becoming aware of such an event, the Reporting Entity must immediately:
(a) Temporarily suspend the customer's access to digital channels;
(b) Re-verify the customer's identity through alternative, secure means; and
(c) File a Suspicious Transaction Report (STR) with the Financial Analysis and Supervision Unit (FASU) if fraudulent activity is suspected.

STANDARD 5.4 – DATA SHARING AND PRIVACY SAFEGUARDS

5.4.1 Consent-Driven Access

(1) No personal data shall be shared from the SevisPass ecosystem to a Reporting Entity without the explicit, real-time consent of the individual via their SevisWallet.
(2) Consent must be specific to the purpose and the entity. Blanket or perpetual consent for data sharing is prohibited.

5.4.2 Privacy by Design

(1) The architecture of the eKYC system must adhere to the principles of privacy by design and by default:
(a) No Centralized Data Repository: The system shall operate on a query-and-response model. Reporting Entities do not have direct access to the central identity database.
(b) User Transparency: Individuals must be able to view a complete history of who accessed their identity data and for what purpose via their SevisPortal or SevisWallet.

STANDARD 5.5 – HIGH-RISK TRANSACTION THRESHOLDS

5.5.1 Mandatory Re-verification

(1) For cash transactions exceeding K10,000.00 (or a lower threshold set by the entity's risk policy), Reporting Entities must perform enhanced verification.
(2) This may include:
(a) Using a live biometric match (e.g., fingerprint verification via a registered agent terminal) against the stored biometric template linked to the SevisPass.
(b) Requesting additional information on the source of funds or wealth.
(3) The Digital ID system provides a secure mechanism for biometric verification to meet this standard efficiently.

STANDARD 5.6 – SECURITY REQUIREMENTS FOR REPORTING ENTITIES

5.6.1 Integration Security

(1) All API integrations with the SevisPass ecosystem must:
(a) Use mutually authenticated TLS (mTLS) for all communications.
(b) Adhere to OAuth 2.0 security best practices for client authentication and token management.
(c) Store API keys and credentials in a secure, hardware-backed vault (HSM or TEE).

5.6.2 Data Handling Security

(1) Personally Identifiable Data (PII) received from the eKYC process must be encrypted at rest and in transit using FIPS 140-2 validated cryptographic modules.
(2) Data retention and disposal policies must be strictly enforced. Upon account closure or at the end of the mandated retention period, all collected PII must be securely and irreversibly deleted.

STANDARD 5.7 – LIABILITY AND DISPUTE RESOLUTION

5.7.1 Liability Framework

(1) The Government of Papua New Guinea guarantees the integrity and authenticity of identity data at the point of issuance.
(2) Reporting Entities bear full liability for:
(a) Any losses arising from their failure to comply with these standards or applicable CTF/AML laws.
(b) Fraudulent transactions resulting from their failure to act on credential revocation alerts.
(c) Misuse or unauthorized storage of data obtained via the eKYC process.

5.7.2 Dispute Resolution

(1) A clear and accessible process must be established for individuals to dispute and rectify errors related to their digital identity used in financial transactions.
(2) Reporting Entities must resolve all such disputes within 14 business days, in coordination with the Digital ID Grievance Redressal Unit.

STANDARD 5.8 – CROSS-BORDER CONSIDERATIONS & INTERNATIONAL INTEROPERABILITY

5.8.1 Recognition of Foreign eIDs

(1) The Regulatory Authority may establish bilateral agreements to recognize selected foreign digital identity schemes for eKYC purposes for non-resident customers, provided they meet or exceed the assurance levels outlined in this instrument.

5.8.2 FATF Compliance

(1) The entire eKYC process, anchored by the SevisPass Digital ID, shall be designed to demonstrate compliance with the Financial Action Task Force (FATF) Recommendations, particularly Recommendation 10 on Customer Due Diligence.

STANDARD 5.9 – COMPLIANCE AND AUDIT

*5.9.1 Regulatory Oversigh*t

(1) The Bank of Papua New Guinea (BPNG), in collaboration with DICT, shall be responsible for monitoring Reporting Entities' compliance with these eKYC and CTF/AML standards.
(2) BPNG may issue more detailed guidelines specific to the financial sector.

5.9.2 System Audits

(1) DICT and the Digital ID Regulatory Authority shall conduct regular audits of the eKYC API infrastructure and access logs to prevent misuse and ensure system integrity.
(2) Reporting Entities must undergo annual independent audits to ensure their integration and use of the Digital ID system complies with these standards and all applicable CTF/AML laws. Audit reports must be submitted to BPNG and the Regulatory Authority.

IMPLEMENTATION SCHEDULE FOR PART VI

(1) Reporting Entities categorized as Tier 1 Financial Institutions (as defined by BPNG) must achieve full compliance with this Part within twelve (12) months of the effective date of this instrument.
(2) All other Reporting Entities must achieve full compliance within twenty-four (24) months.
(3) The Regulatory Authority may grant limited, conditional extensions on a case-by-case basis upon demonstration of a validated implementation plan.

PART VII. - MISCELLANEOUS

13. Laws, Regulations, Frameworks, Standards and Guidelines

- Data Protection and Privacy Laws:
  1. ***The Data Protection Act 2020*** - for the protection and handling of personal data, ensuring that individuals' privacy rights are respected within the digital ID ecosystem.

- Electronic Transactions Laws
  1. The Electronic Transactions Act 2000 - legal framework for electronic transactions and recognizes the validity and enforceability of electronic signatures and records in PNG.

- Telecommunications Laws:
  1. The Telecommunications Act 1996
  2. National Information and Communications Technology Act 2009

  In regulating communication and information technology in PNG, providing guidelines for the secure and reliable operation of digital ID systems.

- Financial Regulations: Relevant financial regulations, such as
  1. the Banking Act and the Anti-Money Laundering and
  2. Counter-Terrorism Financing Act,

  In governing financial services and promote measures to prevent money laundering and terrorist financing within the context of digital ID-enabled financial transactions.

14. Implementation schedule.

All public bodies must adopt the standards in Part 2 and 3 on or before [01.01. 2025].

15. Compliance and monitoring.

DICT may conduct an assessment and evaluation report of the compliance of public bodies with this instrument.

STANDARD – MONITORING AND EVALUATION FRAMEWORK

(1) DICT shall implement a Monitoring and Evaluation (M&E) framework to monitor the rollout and performance of the digital ID system across all sectors and participating entities.
(2) The framework shall include the following Key Performance Indicators (KPIs):
(a) Percentage of population issued with SevisPass;
(b) Monthly usage rate of SevisPass in government and financial services;
(c) Number of active grievance cases resolved within 14 days;
(d) Percentage of accredited entities compliant with Trust Framework rules;
(e) Number of audit findings resolved within set timelines.
(3) M&E reporting shall be compiled quarterly and shared with the Interagency Steering Committee and other relevant oversight bodies.

(4) An independent third-party evaluation shall be conducted every two years to assess inclusivity, performance, system integrity, privacy compliance, and public trust.
(5) DICT shall facilitate a Stakeholder Advisory Group including civil society, women's organizations, and organizations for persons with disabilities to provide feedback and advisory input for continuous improvement.
(6) The results of monitoring and evaluation activities shall be published annually in a public report and used to inform system upgrades, regulatory adjustments, and capacity-building priorities.

16. Supplemental standards and guidelines.

DICT may issue supplemental standards and guidelines to support this instrument.

Papua New Guinea Government Digital Identification (ID) Standards, Guidelines and Specifications 2025.

ARRANGEMENT OF CLAUSES.