EXPLANATORY NOTES

TO THE

EXPOSURE DRAFT OF THE

VERIFIABLE CREDENTIAL AND TRUST SERVICES BILL 2026

6 August 2026

Contents

INTRODUCTION

These Explanatory Notes have been prepared by the Papua New Guinea Department of Information and Communications Technology to assist with public consultations into the Verifiable Credential and Trust Services Bill 2026 (the Bill). They set out the background, policy rationale, and a section-by-section commentary on each Part and provision of the Bill. These Notes are not part of the Bill and have not been endorsed by the National Executive Council or the National Parliament. Therefore, they do not constitute legal advice. References to section numbers are to provisions of the Bill as introduced.

OVERVIEW OF THE BILL

The Bill establishes the legal foundation for Papua New Guinea's National Digital Trust Ecosystem. It creates a comprehensive legislative framework governing digital identity, verifiable credentials, trusted data exchange, and digital payments for the people and institutions of Papua New Guinea.

The Bill has nine principal objects:

- To establish Papua New Guinea's National Digital Trust Ecosystem as a legally recognised operational environment.
- To recognise SevisPass as the foundational digital identity credential — the trust anchor — for that ecosystem.
- To provide for the issuance, holding, management, presentation, verification, suspension, revocation, and legal recognition of verifiable credentials held in approved digital wallets.
- To establish the National Digital Identity and Trust Services Framework (the Framework) as the governing legal, technical, operational, and institutional architecture.
- To designate an independent statutory Regulator and a separate Implementation Authority.
- To provide for accreditation, oversight, privacy, data protection, compliance, and enforcement.
- To protect the constitutional rights, privacy, security, and autonomy of individuals.
- To provide for appeals, transitional and savings matters.
- To make consequential amendments to related Acts.

POLICY BACKGROUND AND CONTEXT

Papua New Guinea faces longstanding challenges in delivering efficient public services, enabling financial inclusion, and supporting economic development, all of which are exacerbated by limited trusted identity infrastructure. A significant proportion of the population lacks reliable, verifiable proof of identity, which creates barriers to accessing government services, banking, healthcare, education, and social protection programmes.

Digital identity systems based on verifiable credentials that are cryptographically signed, tamper-evident digital statements are recognised internationally as a foundation for Digital Public Infrastructure (DPI). These systems enable trusted interactions between governments, businesses, and individuals, and are increasingly central to digital government, financial inclusion, and digital commerce.

The Marape-Rosso government has had to take decisive action through NEC Decision No. 183/2025 by endorsing the *National Digital ID Policy 2025* to address these issues. Government has had to undertake preparatory work through the civil registration system established under the *Civil and Identity Registration Act* 2024, which provides the foundational biometric and demographic identity record from which SevisPass credentials can be anchored. To implement these key policy and legislative initiatives, this Bill will now aspire to provide the legislative framework necessary to govern the digital identity and verifiable credentials layer that sits above that record.

Key policy principles underlying the Bill include:

- Trust and legal certainty ensuring that digital credentials have clear legal recognition and are underpinned by robust governance;
- Technology neutrality based on a framework that is designed to accommodate technological evolution without requiring legislative amendment;
- Privacy by design so that all systems must embed privacy protections from the outset, and that selective disclosure is a core design requirement;
- Sovereignty so that the State retains ownership and ultimate control over core trust infrastructure, including cryptographic anchors, biometric data, and the Trust Registry;
- Inclusion where no resident may be denied access to essential government services for lack of SevisPass, and special accommodations are required for vulnerable persons; and
- Proportionality so that limitations on individual rights are limited to those that are lawful, necessary, and proportionate.

TERRITORIAL EXTENT AND COMMENCEMENT

The Bill applies throughout Papua New Guinea and binds the State (clause 5).

The Bill provides for staged commencement:

- Part I (Preliminary), Part VI (Holder Rights), Part VII (Data Protection and Privacy), and the savings and transitional provisions in Part IX come into operation on the date of certification by the Speaker;

- Parts II, III, IV, V, and VIII, and Schedule 1 to the extent necessary for staged implementation, come into operation on dates fixed by the Minister by notice in the National Gazette;

- Any provision not brought into operation within 36 months of certification will automatically commence, unless the National Executive Council otherwise directs on the advice of the Minister; and

- The Minister may fix different dates for different provisions, classes of persons, credentials, sectors, transactions, or entities.

This approach enables careful, staged implementation of operational requirements while giving immediate legal effect to the rights of credential holders and the constitutional protections in the Bill from the date of enactment.

FINANCIAL IMPLICATIONS

The Bill establishes a Digital Identity Sustainability Fund (clause 26(5)) to support the long-term financial sustainability of the National Digital Trust Ecosystem. The Fund will consist of accreditation and verification fees, platform participation levies, commercial service revenues, Parliamentary appropriations, grants, and investment income. The Fund is managed by the Regulator in trust for the State, subject to Ministerial direction, and is audited by the Auditor-General.

Basic SevisPass issuance, holding, management, storage, and presentation services are free to residents (clause 26(4)). Fees may be charged to institutional and commercial participants for accreditation, verification services, platform integration, and trust services.

The Implementation Authority may, with Ministerial approval, offer commercial services on a fee-for-service basis, including enhanced identity assurance, identity-as-a-service, and consent-governed attribute data-sharing (clause 26(6)).

CONSTITUTIONAL COMPLIANCE AND RIGHTS SAFEGUARDS

The Bill contains a dedicated constitutional and rights safeguards provision (clause 3). It requires the Act to be interpreted consistently with the constitutional rights of residents, including the right to privacy under Section 49 of the Constitution. Any limitation on privacy, liberty, or access must be prescribed by law, reasonably necessary, proportionate to a legitimate public purpose, and subject to safeguards including notice, reasons, review, and appeal.

The Bill expressly provides that no person shall be denied access to an essential government service solely because they do not hold SevisPass (clause 3(3)).

The Bill also contains express privacy savings provisions in Part IX confirming that Section 49 of the Constitution is limited only to the extent expressly provided in the Act.

Clause 1 provides for compliance with constitutional requirements to be completed in consultation with the State Solicitor before introduction.

SECTION-BY-SECTION COMMENTARY

Part I — Preliminary

Clause 1 ***Compliance with constitutional requirements***

This clause serves as a placeholder for the formal certification of constitutional compliance, to be completed by the State Solicitor prior to introduction in the National Parliament. Constitutional compliance certification is a standard requirement under the Constitution for Government Bills.

Clause 2 ***Objects of this Act***

This clause sets out the five principal objects of the Act. Subsection (1) identifies the operational objects: enabling digital identity authentication, the issuance and management of verifiable credentials, trusted data exchange through SevisDEx, and secure digital payments through SevisPay or other accredited payment systems.

Subsection (2) establishes the Framework object: creating and maintaining the National Digital Identity and Trust Services Framework as the governing legal, technical, operational, and institutional architecture for the ecosystem.

Subsection (3) articulates the rights and inclusion object: protecting the constitutional rights, privacy, security, consent, and autonomy of individuals while enabling trusted digital interactions that support financial inclusion and digital government.

Subsection (4) establishes the governance object: creating a comprehensive accreditation, assurance, compliance, supervisory, and enforcement regime. The Regulator is designated as the primary regulatory authority.

Subsection (5) states the interpretive object: requiring the Act to be interpreted and administered in a manner that promotes trust, legal certainty, interoperability, innovation, technology neutrality, security, and public confidence.

Clause 3 ***Constitutional and rights safeguards***

Subsection (1) requires the Act to be interpreted, so far as possible, consistently with constitutional rights, including the right to privacy under Section 49.

Subsection (2) sets out the conditions that must be met before any limitation on privacy, liberty, or access under the Act may be imposed: it must be prescribed by law, reasonably necessary and proportionate, and subject to procedural safeguards.

Subsection (3) contains the non-exclusion guarantee: no person may be denied access to an essential government service solely because they do not hold SevisPass. This is a fundamental protection against digital exclusion and coercive enrolment.

Clause 4 ***Interpretation***

This clause defines the key terms used throughout the Act. The definitions are designed to be technology-neutral to accommodate technological evolution.

> "Accredited issuer" means a private-sector entity accredited by the Regulator to issue verifiable credentials — distinct from "authorised issuer", which refers to public bodies authorised by law.
>
> "Approved digital wallet" means a digital application approved by the Regulator for holding, managing, and presenting verifiable credentials. SevisWallet is designated as the official national wallet under clause 11.
>
> "National Digital Trust Ecosystem" encompasses the full operational environment of individuals, agencies, credential issuers, trust service providers, and relying parties governed by the Framework.
>
> "SevisPass" is defined as the verifiable credential that serves as the trust anchor, to which a holder's primary biometric is enrolled and anchored for deduplication purposes.
>
> "SevisWallet" is the official national digital wallet designated under clause 11.
>
> "Verifiable credential" means a cryptographically signed, tamper-evident digital statement capable of being presented for authentication or verification. This definition is aligned with international standards, including the W3C Verifiable Credentials Data Model.

Other key defined terms include "Regulator", "Trust Registry", "Trust Service", "National Digital Identity and Trust Services Framework", "material system failure", "serious cybersecurity incident", "continuity of service", and "national security".

Clause 5 ***Application***

Subsection (1) confirms the Act applies throughout Papua New Guinea.

Subsection (2) confirms the Act binds the State — that is, the obligations of the Act apply to government agencies and public bodies, not just to the private sector.

Subsection (3) lists the persons and entities to which the Act applies: SevisPass, SevisWallet, prescribed credentials, authorised issuers, accredited partners, approved digital wallets, verifiers subject to the Act, and any other person or entity prescribed by regulation.

Subsection (4) confirms the Act is subject to the Constitution and Constitutional Laws.

Clause 6 ***Relationship with other laws***

This clause manages the interaction between the Bill and existing legislation.

Subsection (2) lists the Acts that continue to operate unaffected except as expressly provided in the Bill or by a consequential amendment: the Citizenship Act, Migration Act, Passports Act, Anti-Money Laundering and Counter Terrorist Financing Act, Civil and Identity Registration Act, and Public Finances (Management) Act.

Subsection (3) preserves existing requirements in other written laws for physical production of documents unless those laws are amended. This ensures the Bill does not inadvertently displace physical document requirements in sectors that have not yet updated their laws.

Part II — National Digital Identity and Verifiable Credentials System

Division 1 — Establishment of SevisPass

Clause 7 ***Establishment of SevisPass***

This clause formally establishes SevisPass as a verifiable credential in law and designates it as the trust anchor of the National Digital Trust Ecosystem. Biometric deduplication is anchored to SevisPass, ensuring one credential per person for life (subject to the lifecycle provisions in clause 12).

SevisPass is to be issued under the Act in accordance with the Framework and applicable regulations. It is the primary credential to which other prescribed credentials may be anchored or linked.

Clause 8 ***Nature and effect of SevisPass***

Subsection (1) confirms SevisPass is a verifiable credential, digital by default, and may be held through SevisWallet or another approved digital wallet.

Subsection (2) contains important limiting provisions to prevent misuse or over-reach: SevisPass does not constitute proof of citizenship or nationality; it does not of itself constitute a passport, visa, travel document, licence, or entitlement; and it shall not be used to infer citizenship, migration status, or any other legal status beyond its lawfully associated attributes.

These provisions are critical to ensuring SevisPass remains a digital identity tool and does not become a de facto nationality document or gatekeeping mechanism beyond its intended purpose.

Clause 9 ***Eligibility for SevisPass***

Every resident, defined to include citizens, permanent residents, and legally recognised foreign nationals, is eligible to apply for SevisPass. Eligibility criteria, enrolment classes, and evidence requirements may be further prescribed by regulation. Eligibility provisions must be administered consistently with the Citizenship Act 1975 and the Migration Act 1978.

Clause 10 ***One SevisPass for life***

A person is issued only one SevisPass for life. Re-issuance, replacement, restoration, and update do not create a new identity record except where required for fraud control, deduplication, or system rectification. This supports the integrity and trustworthiness of the ecosystem and prevents identity fragmentation.

Clause 11 ***Characteristics of SevisPass***

Subsection (1) prescribes the technical characteristics of SevisPass: a randomly generated 12-digit non-intelligent identifier (containing no embedded personal information); cradle-to-grave validity subject to lawful suspension or revocation; capability for online and offline authentication; and authentication functionality in accordance with approved technical standards. Further characteristics may be prescribed by regulation.

Subsection (2) allows SevisPass to be issued to a child, with regulations providing for demographic-only enrolment until the prescribed age for biometric collection is reached. This enables children to be enrolled in the system early while deferring biometric collection appropriately.

Clause 12 ***SevisPass lifecycle***

This clause describes the full lifecycle of a SevisPass credential, from registration and enrolment through to archival and end-of-lifecycle matters. The lifecycle includes: registration and enrolment; verification, deduplication, and issuance; holding, management, use, authentication, and verification; correction, update, suspension, reactivation, and revocation; and archival and retention as prescribed by regulation.

Division 2 — SevisWallet and Approved Digital Wallets

Clause 13 ***Designation of SevisWallet***

SevisWallet is designated as Papua New Guinea's official national digital wallet. It must support holder rights, selective disclosure, consent controls, audit history, interoperability, and portability. SevisWallet's status as the official State-designated wallet is a protected baseline that other approved wallets must not undermine.

Clause 14 ***Approved digital wallets***

Subsection (1) empowers the Regulator to approve additional digital wallets. Subsection (2) prescribes the conditions for approval: compliance with the Framework; preservation of holder rights; interoperability with SevisWallet and SevisDEx; support for selective disclosure; adequate security, resilience, audit logging, and incident response; and not undermining SevisWallet's official status.

Approval may be granted subject to conditions. This creates a competitive market for wallet providers within a regulated and standards-based framework, promoting choice and innovation while protecting holders.

Division 3 — Verifiable Credentials Ecosystem

Clause 15 ***Establishment of verifiable credentials ecosystem***

This clause formally establishes the national verifiable credentials ecosystem as a component of the Framework. The ecosystem provides for the lawful issuance, holding, presentation, verification, suspension, revocation, and legal recognition of verifiable credentials by authorised issuers, accredited issuers, approved digital wallets, verifiers, and other trust service participants.

Clause 16 ***Prescribed credential categories***

Subsection (1) lists the categories of prescribed credentials that may be issued, recognised, held, presented, and verified under the Act. These include: driver's licences, passports, visas, work permits, birth certificates, Grade 12 certificates, Tax Identification Number certificates, police clearance certificates, student and teacher identification credentials, professional membership or licensing credentials, superannuation credentials, and any other category prescribed by regulation.

Subsection (2) makes clear that listing a credential does not amend or displace the enabling law governing that credential. For example, including passports in the list does not override the Passports Act 1982; the issuance and legal validity of passports continues to be governed by that Act, with SevisPass providing the digital presentation layer.

Clause 17 ***Authorised issuers***

Public bodies specified in regulations or other written laws may be authorised issuers for specific credential categories. Authorised issuers may only issue credentials within the scope of their statutory functions. They must ensure credentials are lawfully authorised, accurate and current, conform to the applicable credential schema, and are subject to lawful correction, update, suspension, and revocation procedures.

Clause 18 ***Accredited issuers***

Private-sector entities may not issue verifiable credentials under the Act unless accredited by the Regulator as an accredited issuer. Accreditation requires satisfaction of eligibility, governance, technical, security, financial, and compliance requirements. This maintains the integrity and trustworthiness of the ecosystem by ensuring private issuers meet prescribed standards before participating.

Clause 19 ***Credential schemas***

The Regulator may approve or prescribe credential schemas i.e. standardised data structures, formats, minimum attributes, encoding rules, and validation requirements — for each category of verifiable credential. Schemas may specify minimum and optional attributes, data quality requirements, encoding standards, validation rules, revocation and status-check requirements, and interoperability requirements. Schemas are essential for ensuring that verifiable credentials from different issuers are technically interoperable and can be reliably verified.

Clause 20 ***Legal recognition of verifiable credentials***

Subsection (1) provides that a verifiable credential issued under the Act has legal recognition for any purpose for which the underlying physical document would otherwise be recognised, unless another written law expressly requires otherwise.

Subsection (2) provides that an electronic presentation of a verifiable credential may not be denied legal effect merely because it is in digital form.

Subsection (3) prevents verifiers from unreasonably refusing to accept a verifiable credential in lieu of a physical document, subject to three exceptions: where another written law expressly requires the physical document; where the verifier has reasonable grounds to believe the credential is invalid, suspended, revoked, expired, or technically unverifiable; or where the transaction falls within a class prescribed by regulation as requiring additional evidence.

These provisions are central to the legal infrastructure of the ecosystem. They give verifiable credentials equivalent legal standing to physical documents and establish anti-refusal protections, creating legal certainty for holders and verifiers.

Clause 21 ***Presentation and verification***

A holder may present a credential through SevisWallet or another approved digital wallet. Verifiers are subject to data minimisation obligations: they must request only the minimum attributes or proof reasonably necessary for the stated lawful purpose; use selective disclosure where available and sufficient; comply with purpose limitation; and not retain data beyond what is lawful and reasonably necessary.

These obligations operationalise the privacy by design principle and ensure verifiers cannot use the verification process as a data collection mechanism beyond what is necessary.

Clause 22 ***Suspension and revocation of credentials***

Credentials may only be suspended or revoked on grounds prescribed by the Act or regulations, and only in accordance with natural justice. Except in urgent circumstances, the holder must be given prior notice, reasons, an opportunity to respond, and notice of the right to review or appeal.

Emergency temporary suspension without prior notice is permitted only where strictly necessary for fraud prevention, public safety, cybersecurity, or system integrity, with reasons to be given as soon as practicable. These protections mirror constitutional natural justice requirements and ensure holders are protected against arbitrary suspension or revocation of their credentials.

Division 4 — Mandatory Acceptance, Interoperability and Sovereign Infrastructure

Clause 23 ***Mandatory acceptance***

Subsection (1) requires all public bodies to accept SevisPass and applicable prescribed credentials for identity verification, credential validation, and digital service access within 12 months of commencement of the relevant provision, subject to maintaining reasonable alternative channels for essential government services.

Subsection (2) requires financial institutions, superannuation funds, payment service providers, and other AML/CTF-regulated or BPNG-regulated entities to accept SevisPass and prescribed credentials for eKYC and customer due diligence within 18 months.

Subsection (3) provides for a 24 to 36 month transition for telecommunications operators, educational institutions, transport authorities, professional bodies, utilities, and other prescribed sectors.

Subsection (4) allows sectoral regulators to issue implementing instructions in coordination with the Regulator but prevents them from narrowing the substantive acceptance obligation.

This phased approach is designed to drive adoption across government and regulated sectors while allowing adequate time for system integration.

Clause 24 ***Cross-border recognition and interoperability***

The Minister may approve arrangements for cross-border recognition, verification, and interoperability of SevisPass, SevisWallet, and prescribed credentials, on advice of the Regulator and after consultation with relevant authorities.

Any such arrangement must preserve constitutional protections, privacy and consent requirements, cybersecurity and trust standards, and Papua New Guinea's sovereign control over core trust infrastructure.

Clause 24A ***Foreign participation restrictions***

This clause protects national sovereignty by restricting foreign State-linked entity involvement in the Implementation Authority. A foreign State-linked entity — one owned or controlled by, or subject to direction from, a foreign government — cannot be designated as the Implementation Authority.

Changes in ownership or control that would result in a foreign person or entity acquiring a beneficial interest of 15% or more require prior written Ministerial approval. The Implementation Authority must notify the Regulator within 14 days of any proposed change of ownership or control.

The Regulator may recommend refusal of approval or revocation of designation where a change of ownership poses a risk to the State's sovereign ownership or ultimate control. Any transaction entered into in contravention of this clause is void to the extent of the contravention.

Clause 24B ***Exercise of step-in rights procedure***

This clause sets out the procedure for activating the State's step-in rights under clause 37. Step-in is activated by National Executive Council decision published in the National Gazette, on Ministerial advice, where the NEC is satisfied a triggering circumstance exists.

Upon publication, the Implementation Authority must immediately grant full access to all systems, data, credentials, source code, cryptographic materials, and facilities; cooperate fully with the State; and cease any action that would impair the State's control.

A step-in period cannot exceed 12 months, after which the NEC must either restore the Implementation Authority or commence revocation and designate a successor.

Officers and employees of the State acting in good faith in the exercise of step-in rights are not personally liable. The Implementation Authority is not entitled to compensation for loss of revenue or commercial opportunity during a step-in period, but may claim reasonable reimbursement for documented direct costs.

Clause 25 ***State ownership and sovereign control***

This clause is a cornerstone of the Bill's sovereignty framework. Subsection (1) asserts that the State retains sovereign ownership and ultimate control over SevisPass, SevisWallet, SevisDEx, the Framework, the Trust Registry, public cryptographic trust anchors, designated credential schemas, and other core digital public infrastructure.

Subsection (2) provides that no contract, licence, concession, partnership, outsourcing arrangement, or other instrument may transfer ownership or ultimate control of sovereign trust infrastructure away from the State.

Subsection (3) vests intellectual property in software, source code, APIs, cryptographic libraries, credential schemas, and related materials in the State: where created by or on behalf of the State, from the time of creation; where created by the Implementation Authority using State funding or resources, upon termination or revocation of the designation.

Subsections (3A)–(3C) regulate the Implementation Authority's use of State intellectual property: it holds a non-exclusive royalty-free licence for the duration of the designation; it may not assign, sublicence, or encumber the IP without Ministerial approval; and it must maintain a current source code and documentation repository.

Subsection (4) requires root cryptographic trust anchors, root CA private keys, master signing keys, and hardware security module credentials to be held in a secure facility in Papua New Guinea, with immediate State access upon step-in or revocation.

Subsections (4A)–(4C) establish cryptographic key escrow requirements: key material must be protected against unauthorised access; independently verified by the Regulator at 12-month intervals; and transferred to the State or a successor without condition upon activation of step-in rights or revocation. Key ceremonies must comply with Regulator-prescribed procedures and a Regulator representative may observe any key ceremony.

Subsections (5)–(5B) establish data residency requirements: personal data, biometric data, credential data, and audit logs must be stored on infrastructure physically located in Papua New Guinea. Biometric raw data and root cryptographic key material may never be stored or processed offshore. Limited offshore processing of other data requires Ministerial gazette approval of the facility and jurisdiction, encryption and jurisdictional protection throughout transit, and contractual prohibition on foreign government disclosure.

Clause 26 ***Sustainability and fees***

Subsections (1)–(3) provide for a regulated revenue and sustainability framework. Fees may be prescribed for verification services, accreditation, platform participation, institutional integration, trust services, payment-rail integration, and other commercial or institutional services. Fees must be transparent, proportionate, and non-discriminatory.

Subsection (4) contains the free access guarantee: no resident may be charged for the basic functions of receiving, holding, managing, storing, or presenting their own SevisPass or prescribed credentials through SevisWallet.

Subsections (5)–(5E) establish the Digital Identity Sustainability Fund. The Fund supports long-term financial sustainability, resilience, inclusion, and development of the ecosystem. It receives fees, levies, commercial revenues, Parliamentary appropriations, grants, and investment income. It is managed by the Regulator in trust for the State and applied to operational and capital costs of the Implementation Authority, inclusion initiatives,

cybersecurity infrastructure, research and standards development, and Regulator administration costs. The Fund is audited by the Auditor-General and reported to Parliament annually.

Subsections (6)–(6B) authorise the Implementation Authority, with Ministerial approval, to offer commercial services on a fee-for-service basis, including enhanced identity assurance, identity-as-a-service, bulk verification services, consent-governed data-sharing, technology licensing with Pacific Island states, and integration services. Accredited partners pay platform participation levies to the Fund based on transaction volumes.

Part III — Regulator

Clause 27 (Section 26) ***Designation of Regulator***

The entity responsible for regulating information and communications technology and the digital economy is designated as the Regulator for the purposes of the Act. Unless and until another entity is designated by or under the National Information and Communications Technology Act 2009, the National Information and Communications Technology Authority (NICTA) is the Regulator. This provides continuity with existing regulatory arrangements while enabling future structural change if required.

Clause 28 (Section 27) ***Functions of Regulator***

The Regulator's functions include: developing, administering, and enforcing the Framework; approving standards, credential schemas, trust services, and interoperability requirements; accrediting, supervising, and if necessary suspending or revoking accredited partners; approving and supervising approved digital wallets; maintaining the Trust Registry; monitoring compliance; conducting audits and inspections; investigating contraventions; issuing directions and administrative penalties; advising the Minister on commencement sequencing, sectoral transition, and cross-border arrangements; promoting holder rights and public awareness; and performing other functions conferred by the Act or another law.

Clause 29 (Section 28) ***Powers of Regulator***

The Regulator has power to do all things necessary or convenient to perform its functions, including: issuing standards, codes, rules, and technical requirements; requiring information, records, and reports; entering into coordination arrangements with sectoral regulators; imposing conditions on approvals and accreditations; establishing registers and digital assurance mechanisms; and applying to the National Court for an injunction.

Clause 30 (Section 29) ***Limitation concerning AML/CTF functions***

This clause makes clear that the Regulator is not authorised to require SevisPass, SevisWallet, or the Framework to perform customer risk ratings, transaction monitoring, or sanctions screening. These functions remain the legal responsibility of financial

institutions and other regulated entities under AML/CTF law. This is an important boundary that preserves the integrity of the existing AML/CTF regime.

Clause 31 (Section 30) ***Technical Standards and Advisory Committee***

The Regulator must establish a Technical Standards and Advisory Committee, including representatives of government agencies, the private sector, civil society, technical experts, and other stakeholders. The functions, procedures, and terms of reference of the Committee may be prescribed by regulation or determined by the Regulator.

Clause 32 (Section 31) ***Annual report***

The Regulator must submit an annual report to the Minister and to the National Parliament on the operation, performance, compliance, security, and development of the National Digital Trust Ecosystem. This provision supports Parliamentary accountability and public transparency.

Part IV — National Digital Identity and Trust Services Framework Implementation Authority

Clause 33 (Section 32) ***Designation of Implementation Authority***

Subsection (1) empowers the Minister, by notice in the National Gazette, to designate an entity as the Implementation Authority, unless the National Executive Council otherwise directs on Ministerial advice. The SPV established under the Bill may be designated.

Subsection (2) prescribes the mandatory contents of the designation instrument, including: the name of the entity; designated functions; commencement date; authorised commercial services; revenue allocation arrangements; intellectual property, cryptographic key custody, and data residency obligations; reporting obligations; conditions of designation; and transition arrangements.

Subsection (3) confirms the designated entity is subject to the Act notwithstanding anything in its constitution or constituting instrument.

Clause 34 (Section 33) ***Criteria for designation***

The NEC acting through the Minister must not designate an entity unless satisfied it has technical, operational, and financial capacity; can maintain continuity, resilience, and cybersecurity; can operate consistently with State ownership and sovereign control; can comply with public finance, procurement, and accountability laws; satisfies additional criteria prescribed by regulation; and has a governance structure that preserves State control through a golden share or equivalent mechanism and can operate with the neutrality required of a public utility.

Clause 35 (Section 34) ***Functions of Implementation Authority***

The Implementation Authority's functions include: designing, deploying, operating, and maintaining the core operational components of the ecosystem; operating or supporting SevisWallet, SevisDEx, SevisAdminPortal, and related systems; supporting interoperability, credential lifecycle management, and platform continuity; maintaining operational audit logs and incident response arrangements; providing reports and information to the Regulator and Minister; and developing and offering commercial services within the Framework in accordance with clause 26(6).

Clause 36 (Section 35) ***Governance requirements***

Subsection (1) prescribes mandatory governance requirements for the Implementation Authority that prevail over any inconsistent constitution or contract. These include: board representation requirements as prescribed by regulation; annual reporting on system performance, material security incidents, financial statements, and compliance; risk management protocols aligned with national security, cybersecurity policy, and cybersecurity strategy; requirements for contracts involving sovereign trust infrastructure (including public procurement compliance, prohibition on transferring sovereign ownership, pre-execution disclosure to the Regulator, termination-for-convenience clauses, and prohibition on provisions giving third parties rights over sovereign infrastructure); ring-fencing of sovereign trust infrastructure in accounts, security architecture, and asset register from other assets, business lines, and creditors; a golden share or equivalent mechanism preserving State control regardless of ownership structure; and non-discriminatory access to core services on reasonable and transparent terms.

Subsection (2) permits additional governance requirements to be prescribed by regulation or included in the designation notice.

Clause 37 (Section 36) ***Continuity and step-in powers***

Subsection (1) provides the State with step-in rights in matters involving national security, continuity of service, material system failure, serious cybersecurity incident, or protection of the public interest.

Subsection (2) provides that where the designation of an Implementation Authority is revoked or is within 12 months of expiry, the NEC may on Ministerial advice designate a successor or temporarily vest functions in the Department or another public body, to preserve continuity of service and holder access to credentials.

Clause 38 (Section 37) ***Revocation of designation***

Subsection (1) empowers the NEC on Ministerial advice to revoke a designation where the designated entity ceases to satisfy the criteria for designation; commits a serious or repeated

contravention; becomes incapable of discharging its functions; or fails to comply with a condition of designation.

Subsection (2) requires the Minister to give notice and an opportunity to respond before revoking a designation, unless urgent public interest requires immediate action.

Part V — Accredited Partners

Clause 39 (Section 38) *Categories of accredited partners*

The Act recognises seven categories of accredited partner: accredited issuers, accredited verifiers, approved digital wallet providers, enrolment agents or enrolment partners, trust service providers, technical integration providers, and any other class prescribed by regulation. This flexible categorisation allows the ecosystem to accommodate new participant types as the technology and market evolve.

Clause 40 (Section 39) *Requirement for accreditation*

No person or entity may operate as an accredited partner without being accredited or approved in accordance with the Act. This is a general prohibition on unaccredited participation in the regulated aspects of the ecosystem.

Clause 41 (Section 40) *Application for accreditation*

Applications are made to the Regulator in the prescribed form with prescribed information and fee. Applicants must demonstrate compliance with governance, security, technical capability, financial capacity, privacy, data protection, and legal compliance requirements.

Clause 42 (Section 41) *Grant, conditions and duration of accreditation*

The Regulator may grant or refuse accreditation, may impose terms and conditions, and accreditation remains in force for the prescribed period unless suspended, revoked, surrendered, or expired. This provides flexibility for the Regulator to tailor accreditation conditions to the risk profile of each participant category.

Clause 43 (Section 42) *Obligations of accredited partners*

Accredited partners must: comply with the Act, regulations, and applicable standards; protect privacy and personal data; maintain cybersecurity, resilience, and audit logging; cooperate with lawful inspections and audits; notify the Regulator of material incidents, breaches, or changes of control within the prescribed time; and comply with any conditions of accreditation.

Clause 44 (Section 43) ***Suspension and revocation of accreditation***

The Regulator may suspend or revoke accreditation on prescribed grounds. Natural justice protections apply: except where urgent action is necessary, the accredited partner must be given notice of the proposed action, reasons, and an opportunity to respond.

Part VI — Rights of Credential Holders

Part VI establishes a comprehensive bill of rights for credential holders. These rights are fundamental to ensuring that the ecosystem operates in a human-centred and rights-respecting manner. The following rights are conferred:

Clause 45 (Section 44) ***Right to enrol***

Every eligible resident has the right to apply for SevisPass and must not be unreasonably refused enrolment. This is a positive right to participate in the national digital identity system.

Clause 46 (Section 45) ***Right of access***

A holder has the right to access their SevisPass profile, credential data, and related records. This mirrors the data subject access rights recognised in modern data protection frameworks.

Clause 47 (Section 46) ***Right of correction***

A holder may apply through prescribed channels for correction of inaccurate or incomplete data. Accuracy of identity data is fundamental to the integrity and trustworthiness of the ecosystem.

Clause 48 (Section 47) ***Right to consent-based sharing***

Except where disclosure is required or authorised by written law, a holder's credential data shall not be disclosed without explicit, informed, and contemporaneous consent. Consent must be capable of being evidenced, managed, and revoked. This provision gives legal force to the privacy by design principle.

Clause 49 (Section 48) ***Right to revoke consent***

A holder may revoke consent previously given for access, disclosure, or sharing of credential data, subject to lawful retention, audit, or record-keeping obligations.

Clause 50 (Section 49) ***Right to notification***

Subject to lawful restriction, a holder is entitled to be notified when their credential data is accessed, presented, shared, or verified. This supports transparency and enables holders to detect unauthorised use.

Clause 51 (Section 50) ***Right to disclosure history***

A holder is entitled to access a record of disclosures, presentations, and verifications made from their approved digital wallet, subject to lawful restriction for law enforcement, national security, or other prescribed reasons.

Clause 52 (Section 51) ***Right to deletion or removal from wallet***

A holder may request deletion or removal of a credential from an approved digital wallet, subject to the lawful retention obligations of the issuer in respect of the underlying record.

Clause 53 (Section 52) ***Right to portability***

A holder may export, transfer, or re-establish their verifiable credentials in another approved digital wallet or successor wallet, subject to lawful security and anti-fraud requirements. This prevents holder lock-in to a particular wallet provider.

Clause 54 (Section 53) ***Right to continuity***

A holder's access to credentials shall not be unreasonably interrupted by a change in operator, implementation authority, technology vendor, or approved wallet provider. This protects holders from disruption arising from commercial or governance changes at the platform level.

Clause 55 (Section 54) ***Right to redress***

A holder whose rights are affected may lodge a complaint with the Regulator, seek corrective action, seek review under the Act, and appeal to the National Court.

Clause 56 (Section 55) ***Special provisions for vulnerable persons***

The Regulator, Implementation Authority, issuers, and wallet providers must make reasonable accommodations for persons with disabilities, elderly persons, children, persons in remote areas, and other vulnerable persons prescribed by regulation.

Part VII — Data Protection and Privacy

Clause 57 (Section 56) *Privacy by design*

Every entity operating under the Act must implement privacy by design in systems, processes, products, and services used for digital identity and verifiable credentials. This is a foundational requirement that embeds privacy into the architecture of the ecosystem rather than treating it as an add-on compliance measure.

Clause 58 (Section 57) *Selective disclosure*

Every approved digital wallet, including SevisWallet, must support selective disclosure where technically feasible. Selective disclosure enables holders to share only the minimum identity or credential attribute required for a particular transaction, without disclosing unnecessary personal data. For example, a holder proving they are over 18 can present a proof derived from their date of birth without revealing the date itself.

Clause 59 (Section 58) *Relationship with Data Governance and Data Protection Act*

Subsection (1) confirms that the Data Governance and Data Protection Act 2026 governs all aspects of personal data, data governance, data protection, privacy rights, data processing obligations, consent requirements, data sharing, data security, data breach management, and data subject rights in relation to personal data processed within the ecosystem.

Subsection (2) provides that the Bill does not duplicate the Data Governance and Data Protection Act 2026, and its requirements apply concurrently to all persons operating within the ecosystem.

Subsections (3) and (4) require the Regulator and the data protection regulator to cooperate and coordinate in administration and enforcement, including through information-sharing arrangements and joint guidance. The Data Governance and Data Protection Act 2026 is not limited in its application by this Act.

Part VIII — Enforcement, Offences and Appeals

Division 1 — Enforcement Powers

Clause 60 (Section 59) *Audits and inspections*

The Regulator may conduct audits and inspections of authorised issuers, accredited partners, approved digital wallets, verifiers, and other ecosystem participants to monitor compliance with the Act.

Clause 61 (Section 60) ***Compliance directions***

Where the Regulator reasonably believes a contravention has occurred or is occurring, it may issue a written compliance direction. A person must comply within the specified time, unless review or appeal is commenced and a stay is granted.

Clause 62 (Section 61) ***Information-gathering powers***

The Regulator may require persons subject to the Act to produce information, records, or documents reasonably required for administration or enforcement.

Clause 63 (Section 62) ***Administrative penalties***

The Regulator may impose administrative penalties for prescribed contraventions. Natural justice protections apply: notice, an opportunity to respond, and reasons must be given. The quantum of administrative penalties is to be settled following State Solicitor and Department of Justice and Attorney-General advice and will be prescribed in the final Act.

Clause 64 (Section 63) ***Injunctions***

The Regulator may apply to the National Court for an injunction to restrain an actual or apprehended contravention of the Act.

Division 2 — Offences

Clause 65 (Section 64) ***Fraudulent enrolment or use***

It is an offence to fraudulently enrol for, obtain, use, present, or cause to be issued a SevisPass or other credential under the Act. Penalties (subject to finalisation with the State Solicitor): individuals — up to PGK 50,000–100,000 fine or imprisonment; bodies corporate — up to PGK 250,000–500,000 fine.

Clause 66 (Section 65) ***Unlawful collection or use of biometric data***

It is an offence to unlawfully collect, access, disclose, sell, transfer, or use biometric data obtained under the Act. Penalties: individuals — up to PGK 50,000 fine or imprisonment; bodies corporate — up to PGK 500,000 fine. The seriousness of the penalty reflects the sensitivity of biometric data and the potential for serious harm from its misuse.

Clause 67 (Section 66) ***Unauthorised access to SevisDEx, Trust Registry or related systems***

It is an offence to access, interfere with, alter, impair, disrupt, or attempt to access or interfere with SevisDEx, the Trust Registry, SevisWallet, SevisAdminPortal, or another core system without lawful authority. Penalties: individuals — up to PGK 20,000–50,000 fine or imprisonment; bodies corporate — up to PGK 100,000–500,000 fine.

Clause 68 (Section 67) ***Operating without accreditation or approval***

It is an offence to operate as an accredited partner, accredited issuer, approved wallet provider, or other regulated participant without the required accreditation or approval. Penalties: individuals — up to PGK 10,000 fine; bodies corporate — up to PGK 100,000 fine.

Clause 69 (Section 68) ***Failure to comply with direction***

It is an offence to fail, without reasonable excuse, to comply with a lawful direction of the Regulator. Penalties: individuals — up to PGK 5,000 fine; bodies corporate — up to PGK 50,000 fine.

Clause 70 (Section 69) ***Failure to notify notifiable data breach***

It is an offence for a person or entity required to notify a data breach under the Act to fail to do so within the prescribed period without reasonable excuse. Penalties: individuals — up to PGK 5,000 fine; bodies corporate — up to PGK 50,000 fine.

Clause 71 (Section 70) ***Contravention of consent requirements***

It is an offence to knowingly cause credential data to be disclosed from an approved digital wallet without required consent and without lawful authority. Penalties: individuals — up to PGK 5,000–20,000 fine; bodies corporate — up to PGK 50,000–200,000 fine.

Clause 72 (Section 71) ***Unlawful refusal to accept prescribed credentials***

A person or entity subject to mandatory acceptance obligations who unlawfully or unreasonably refuses to accept SevisPass or a prescribed credential commits a contravention, which may be dealt with by compliance direction, administrative penalty, suspension, regulatory sanction, or other prescribed consequence.

Division 3 — Liability and Appeals

Clause 73 (Section 72) ***Allocation of liability***

This clause allocates regulatory responsibility clearly among ecosystem participants.

Authorised and accredited issuers are responsible for lawful authority, accuracy, validity, status, and timely updating of credentials they issue. Verifiers are responsible for making lawful and proportionate requests, obtaining required consent, complying with purpose limitation and data minimisation, and securely handling credential data. Approved digital wallet providers and the Implementation Authority are responsible for operational availability, integrity of wallet services, presentation functionality, audit logging, and incident response. The Regulator is responsible for accreditation, standards, supervision, enforcement, and maintenance of the Trust Registry.

Critically, subsection (5) protects holders: a holder is not liable for system errors, issuer errors, verifier misuse, operator failures, or unauthorised third-party access unless the holder knowingly commits fraud, impersonation, misrepresentation, or other unlawful conduct.

Clause 74 (Section 73) ***Review by Regulator***

A person aggrieved by a decision of an officer or delegate under the Act may apply for internal review in the prescribed manner. This provides a first-tier review mechanism before recourse to the National Court.

Clause 75 (Section 74) ***Appeal to National Court***

Subsection (1) provides a right of appeal to the National Court against specified decisions: refusal, suspension, or revocation of accreditation; suspension or revocation of a credential; imposition of an administrative penalty; a compliance direction; or any other prescribed decision. Appeals must be filed within 30 days (or such further time as the Court allows).

Subsection (2) provides that commencement of an appeal does not operate as an automatic stay, unless the National Court otherwise orders.

Part IX — Miscellaneous, Transitional and Savings

Clause 76 (Section 75) ***Regulations***

The Head of State, acting on advice, may make regulations not inconsistent with the Act prescribing matters required or permitted by the Act, or necessary or convenient for carrying out or giving effect to the Act.

Clause 77 (Section 76) ***Matters that may be prescribed by regulation***

This clause provides a non-exhaustive list of matters that may be prescribed by regulation, including: technical standards for biometric and demographic data; accreditation criteria and procedures; data retention and deletion periods; grievance handling procedures; fee schedules; the form and authentication modalities of SevisPass; trust registry rules; wallet standards and approved trust services; selective disclosure, consent, and audit requirements; staged mandatory acceptance; cross-border interoperability arrangements;

electronic signatures, seals, timestamps, and digital payment trust services; and any other matter necessary for effective administration.

Clause 78 (Section 77) ***National Executive Council oversight***

Regulations made under the Act must be laid before the National Executive Council for approval and signed by the Head of State, acting on advice. This ensures executive oversight of delegated legislation.

Clause 79 (Section 78) ***Transitional validation of existing pilots and issuances***

Any government digital identity pilot programme, provisional SevisPass issuance, trial credential, technical arrangement, or related implementation undertaken before commencement may, by regulation or ministerial notice, be validated for the purposes of the Act. A validation does not deprive a person of a right, review, or remedy under the Act. This provision provides legal certainty for activities already under way while the Bill was being finalised.

Clause 80 (Section 79) ***Continuation of certain existing instruments***

Regulations, rules, directions, memoranda of understanding, operating agreements, and technical arrangements made under the National Information and Communication Technology Act 2009 or the Digital Government Act 2022 that relate to digital identity and are not inconsistent with the Act continue in force until superseded. Persons operating under continued arrangements must comply with any accreditation or approval requirement within the prescribed transitional period.

Clause 81 (Section 80) ***Minister to designate Implementation Authority***

The Minister must designate an Implementation Authority within 12 months after commencement of Part IV, unless the NEC otherwise directs on Ministerial advice. This provides a clear timeframe for establishment of the operational entity.

Clause 82 (Section 81) ***Savings concerning citizenship and nationality***

Nothing in the Act means SevisPass constitutes proof of citizenship or nationality for any purpose under the Citizenship Act 1975 or any other law.

Clause 83 (Section 82) ***Savings concerning passports and travel***

A passport credential held in SevisWallet is not itself a travel document unless recognised as such under the Passports Act 1982, the Migration Act 1978, or another applicable law.

Clause 84 (Section 83) ***Savings concerning AML/CTF obligations***

Nothing in the Act limits or affects the rights, duties, or obligations of financial institutions

or other regulated entities under the Anti-Money Laundering and Counter Terrorist Financing Act 2015 with respect to customer risk assessment, transaction monitoring, sanctions screening, or related compliance obligations.

Clause 85 (Section 84) ***Savings concerning constitutional oversight***

Nothing in the Act affects the jurisdiction of the Ombudsman Commission, the courts, or any other body exercising oversight functions under the Constitution or another law.

Clause 86 (Section 85) ***Privacy savings***

The right of residents under Section 49 of the Constitution is limited by the Act only to the extent expressly provided. Nothing in the Act authorises any further limitation of that right.

Clause 87 (Section 86) ***Post-legislative scrutiny***

Subsection (1) requires the Minister to cause a comprehensive review of the operation and effectiveness of the Act within 3 years after the last of its provisions comes into operation.

Subsection (2) prescribes the matters the review must assess: whether the Act has achieved its stated objectives; the impact on holder rights including for vulnerable persons; the adequacy of privacy and data protection provisions; the effectiveness of enforcement mechanisms, penalty provisions, and the accreditation regime; the performance of the Regulator and Implementation Authority; any unintended consequences; and whether amendments are required.

Subsection (3) requires the Minister to consult with the Regulator, relevant government agencies, civil society organisations, the private sector, and credential holders in conducting the review.

Subsection (4) requires the Minister to table a report on the review findings and recommendations before the National Parliament within 6 months after completion of the review.

This provision reflects a commitment to evidence-based governance and Parliamentary accountability, and ensures the framework remains fit for purpose as the technology and policy landscape evolves.

Schedule 1 — Consequential Amendments

Schedule 1 provides for consequential amendments to existing legislation to give full effect to the Act:

1. National Information and Communication Technology Act 2009

Amendments designate NICTA as the Regulator for the purposes of the Act; confer the functions, powers, and duties necessary to administer the Framework; enable standards-setting, accreditation, supervision, cybersecurity, and incident reporting for digital identity and verifiable credentials; and make further amendments as necessary.

2. Digital Government Act 2022

Amendments formalise the role of the Department as policy authority for digital identity and the Framework; enable the designation framework for the Implementation Authority; provide for coordinated multi-stakeholder governance; enable SevisPass-based single sign-on for appropriate government digital platforms; and make further amendments as necessary.

3. Civil and Identity Registration Act 2024

Amendments enable lawful data-sharing arrangements between the civil registry and the Framework through SevisDEx, subject to consent and data protection safeguards; clarify that SevisPass complements and does not duplicate or replace the civil registry; and make further amendments as necessary.

4. Other Acts

A range of other Acts are to be reviewed and amended as necessary to enable issuance, recognition, verification, or presentation of prescribed credentials under the Act, including: the Anti-Money Laundering and Counter Terrorist Financing Act 2015; the Road Traffic Act 2014; and the Immigration and Citizenship Service Authority Act 2010 and related migration legislation.

COMMENCEMENT AND IMPLEMENTATION TIMETABLE

The following table summarises the staged commencement framework.

On certification by the Speaker	Part I (Preliminary); Part VI (Holder Rights); Part VII (Data Protection and Privacy); savings and transitional provisions in Part IX.
Date fixed by Minister by Gazette (within 36 months of certification)	Part II (Digital Identity and Verifiable Credentials System); Part III (Regulator); Part IV (Implementation Authority); Part V (Accredited Partners); Part VIII (Enforcement, Offences and Appeals); Schedule 1 (to extent needed for staged implementation).
Within 12 months of commencement of Part IV	Minister to designate Implementation Authority; public bodies to begin accepting SevisPass and prescribed credentials.
Within 18 months of relevant provision	Financial institutions, superannuation funds, payment service providers, and AML/CTF regulated entities to accept SevisPass for eKYC and customer due diligence.
Within 24–36 months of relevant provision	Telecommunications operators, educational institutions, transport authorities, professional bodies, utilities, and other prescribed sectors to accept SevisPass and prescribed credentials.
Within 3 years of last provision in operation	Minister to cause comprehensive post-legislative review.
Within 6 months of review completion	Minister to table review report in National Parliament.

GLOSSARY OF KEY TERMS

Accredited issuer
A private-sector entity accredited by the Regulator to issue verifiable credentials.

Accredited partner
An entity accredited by the Regulator to participate in the Framework in a prescribed category.

Approved digital wallet
A digital application approved by the Regulator for holding, managing, presenting, and verifying verifiable credentials.

Authorised issuer
A public body authorised by or under the Act or another written law to issue a verifiable credential.

Biometric data
Data derived from a person's physical, physiological, or behavioural characteristics that permits or confirms unique identification.

Credential holder/Holder
A natural person to whom a verifiable credential has been issued and in whose approved digital wallet it is held.

Digital Identity Sustainability Fund
The Fund established under clause 26(5) to support long-term financial sustainability of the National Digital Trust Ecosystem.

Framework/National Digital Identity and Trust Services Framework
The legal, technical, operational, and institutional framework established by the Act for the National Digital Trust Ecosystem.

Implementation Authority
The entity designated under clause 33 to implement, operate, and administer the operational aspects of the National Digital Trust Ecosystem.

National Digital Trust Ecosystem
The operational environment governed by the Framework, comprising individuals, government agencies, private sector entities, and system participants.

NICTA
National Information and Communications Technology Authority, established under the National Information and Communications Technology Act 2009; designated as the Regulator unless otherwise determined.

Regulator
The entity designated under clause 27 as the independent statutory regulator for the purposes of the Act.

SevisDEx
The secure government and business data exchange platform used within the Framework for consent-governed data sharing and interoperability.

SevisPass
The verifiable credential established as the trust anchor of the National Digital Trust Ecosystem, serving as Papua New Guinea's primary digital identity credential.

SevisWallet
Papua New Guinea's official national digital wallet designated for holding, managing, presenting, and verifying SevisPass and prescribed credentials.

Selective disclosure
The capability of a holder to disclose only the minimum identity or credential attribute required for a lawful purpose without disclosing unnecessary personal data.

Trust Registry
The register maintained by or under the authority of the Regulator of authorised issuers, accredited partners, approved digital wallets, credential schemas, and trust services.

Verifiable credential
A cryptographically signed, tamper-evident digital statement issued by a trusted issuer, held by a holder, and capable of being presented to a verifier for authentication or verification.

Verifier
A person, entity, or system that requests, receives, or verifies a verifiable credential for the purpose of confirming identity, attributes, entitlements, status, or authority.

[end of document]