NATIONAL INFORMATION AND COMMUNICATIONS TECHNOLOGY AUTHORITY

PUBLIC CONSULTATION- SIM CARD REGISTRTION (AMENDMENT AND CONSOLIDATION) REGULATION 2026

Issued 17th December 2025

Contents

Executive Summary

The National Information and Communications Technology Authority (NICTA) is undertaking a comprehensive review of the **SIM Card Registration Regulation 2016** to modernize Papua New Guinea's mobile identity management framework. After nearly a decade of implementation, the telecommunications landscape has changed significantly. Mobile services are now central to banking, digital payments, social media, e-government, business activity, and national security. At the same time, new threats such as mobile-enabled fraud, cybercrime, identity theft, misuse of unregistered SIM cards and emerging threats have exposed major gaps in the current regulatory framework.

The Government's introduction of the **National Digital Identity (SevisPass)**, as outlined in the **Digital Government Act 2022** and the **National Digital Identity Policy 2025**, provides an opportunity to strengthen identity verification and improve the accuracy of mobile subscriber data. The existing 2016 Regulation relies heavily on manual, paper-based identification. It is no longer adequate for PNG's digital transformation agenda or the needs of law enforcement, financial security, and consumer protection.

The proposed **SIM Registration (Amendment and Consolidation) Regulation 2026** aims to establish a modern and secure national system for SIM identity verification. The Regulation will:

- Integrate SevisPass Digital ID and enable real-time API verification.
- Allow biometric authentication to prevent fraud and impersonation.
- Introduce strong cybersecurity, data governance, and privacy protections.
- Support rural and remote communities through offline and low-connectivity verification methods.
- Strengthen agent accountability through mandatory training, licensing, and certification.
- Improve data accuracy through the re-verification of all existing SIM cards.
- Clarify governance and responsibilities for NICTA, DICT and SevisPass, MNOs, and law enforcement.
- Consolidate all previous SIM registration rules into one unified regulatory instrument

The new Regulation will improve national security through verified identities, reduce criminal misuse of mobile services, and support safer digital transactions. It will also provide stronger protections for consumers against scams, SIM-swap attacks, identity theft and other emerging threats. Rural inclusion will be supported through offline verification processes and mobile enrolment units. The Regulation will also enhance regulatory compliance and accountability across the telecommunications sector.

This Public Consultation Paper outlines the proposed amendments, the policy rationale, the financial and operational implications for stakeholders, the governance and risk considerations, and the proposed implementation timeline. NICTA invites all stakeholders, including Mobile Network Operators, government agencies, civil society,

businesses, academia, and members of the public, to review the proposal and provide feedback before the 2026 Regulation is finalised.

1. Background and Policy Context

1.1. Importance of SIM Registration

SIM cards are foundational to identity in the digital economy. They allow citizens to access mobile services, digital payments, e-government platforms, banking, and online marketplaces. Because SIMs can also be used for criminal activity, accurate registration is essential for:

- Investigations by the Royal PNG Constabulary (RPNGC).
- Countering cyber-fraud and mobile scams.
- Regulating mobile financial services.
- Preventing anonymous communication for illegal activities.
- Enhancing national security and emergency response.

1.2. Limitations of the 2016 Regulation

The SIM Card Registration Regulation 2016 was designed before the introduction of Digital ID and before PNG saw significant growth in digital financial transactions, mobile banking, and social media penetration. The regulation:

- Focuses on paper-based identification.
- Provides minimal guidance on fraud management.
- Lacks data protection and cybersecurity requirements.
- Has inadequate enforcement authority.
- Does not integrate with national identity systems.
- Does not support automated or remote verification.

As a result, database integrity remains low, with reports of multiple SIMs registered under one name, fake IDs being used, and inconsistent verification across agents.

1.3. National Digital Identity Policy 2025

The government launched **SevisPass** to provide a secure and unified digital identity for all Papua New Guineans. The policy mandates:

- Unique digital ID credentials
- Biometric identity verification
- QR and token-based authentication
- Secure API access for authorized institutions
- Consistent KYC across sectors

Integrating SIM registration with Digital ID is a key step toward national digital transformation.

2. Problem Statement

The following challenges demonstrate the need for reform:

2.1. Rising Identity Fraud and Mobile Crime

Criminals increasingly exploit gaps in manual SIM registration, leading to:

- SIM-swap fraud.
- Identity theft using forged documents.
- Mobile money scams.
- Anonymous harassment and threats.
- Challenges in tracking illicit communications.

Current procedures do not provide adequate verification capability for MNO agents.

2.2. Weak Accuracy of Subscriber Databases

NICTA and RPNGC report challenges accessing reliable subscriber information due to:

- Poor-quality ID records.
- Duplicate or mismatched SIM registrations.
- Missing, inaccurate, or outdated customer details.
- Inconsistent data entry by agents.

This weakens the effectiveness of law enforcement and emergency management.

2.3. Outdated Manual Processes

The current regulation does not support:

- Real-time identity validation.
- Biometric confirmation.
- Automated fraud detection.
- Error-free ID checks.

Manual document review is unreliable and burdensome.

2.4. Lack of Clear Data Protection and Cybersecurity Policy

There is no explicit requirement for:

- Encryption of identity data.
- Secure storage and controlled access.
- Multi-factor authentication for agent systems.
- Protection from API cyberattacks.
- Audit logging and traceability.

This leaves personal data at risk.

2.5. Difficulties in Rural and Remote Regions

Over 85% of PNG's population lives outside major urban centers, where:

- Mobile connectivity is inconsistent.
- Electricity supply is unreliable.
- Many citizens do not possess formal ID documents.
- Digital literacy is low.

A modern system must consider these realities.

3. Objectives of the 2026 Amendments

The SIM Registration (Amendment and Consolidation) Regulation 2026 seeks to achieve the following objectives:

3.1. **Improve National Security:** Create a secure, reliable, and verified database of mobile users through Digital ID and biometric authentication.

3.2. **Enhance Consumer Protection:** Protect citizens from fraud, SIM hijacking, and identity theft.

3.3. **Strengthen Verification Through Digital Identity:** Integrate SevisPass to ensure accurate, real-time identity confirmation.

3.4. **Provide Clarity in Governance:** Clearly define responsibilities between NICTA, DICT, MNOs, and agents.

3.5. **Protect User Data:** Introduce mandatory cybersecurity, data protection, encryption, retention, and disposal rules.

3.6. **Promote Inclusion:** Provide tailored mechanisms for rural, offline, and low-literacy communities so no citizen is excluded.

3.7. **Improve Enforcement:** Introduce enforceable standards, penalties, and compliance obligations.

4. Summary of Key Proposed Amendments

Amendment Area	Description of Proposed Change	Rationale / Explanation
1. **Mandatory Digital ID Integration**	All new SIM registrations must be verified through SevisPass Digital ID, including real-time API checks.	Ensures accurate identity verification, eliminates use of fake IDs, and aligns SIM registration with PNG's national identity system.
2. **Biometric Verification Enablement**	MNOs may capture facial or fingerprint verification where applicable.	Prevents impersonation, SIM-swap fraud, and enhances security for mobile financial services and high-risk customers.
3. **Offline Token / QR Verification**	Introduces rural-friendly verification via tokens or QR codes that sync when connectivity is restored.	Ensures inclusivity for remote populations where network or electricity access is limited.
4. **Registration Agent Certification**	Mandatory training, licensing, and certification for all SIM registration agents.	Reduces fraud, improves data quality, and professionalizes frontline registration practices.
5. **GPS-Enabled Registration Devices**	All devices used by agents must be GPS-tagged and approved by NICTA.	Provides traceability, prevents rogue agents, and supports compliance monitoring.
6. **Strengthened Compliance Reporting**	Requires periodic reports, breach notifications, and independent audit trails from MNOs.	Improves regulatory oversight, transparency, and accountability.
7. **Cybersecurity & Data Protection Requirements**	Mandatory encryption, secure storage, MFA for agents, and alignment with ISO 27001/NIST.	Reduces risk of data breaches, identity theft, and unauthorized access.
8. **Consolidation of Regulations**	All previous regulations + amendments merged into one unified 2026 Regulation.	Simplifies compliance, improves legal clarity, and reduces administrative fragmentation.

5. Legal Mandate

The National Information and Communications Technology Authority (NICTA) issues this Public Consultation Paper pursuant to the National Information and Communications Technology Act 2009 (the NICT Act).

The NICT Act provides the statutory basis for the development and enforcement of regulatory instruments relating to telecommunications, consumer protection and national security. Specifically:

- Section 10 empowers NICTA to regulate telecommunications services and ensure the security and integrity of ICT systems in Papua New Guinea.
- Section 213-216 provide NICTA with powers to develop, amend, and enforce regulatory instruments related to subscriber information, numbering, identity, and compliance.
- Section 229 requires NICTA to undertake public consultation before finalizing or amending regulatory instruments.

This consultation is therefore issued in compliance with NICTA's legislative mandate and in alignment with national security priorities, digital transformation objectives, and emerging identity management frameworks including Digital ID (SevisPass).

6. Scope of Governance and Institutional Responsibilities

Institution / Stakeholder	Primary Responsibilities	Explanation / Purpose
NICTA	Issue Regulation; enforce compliance; license agents; conduct audits; oversee Digital ID integration.	Acts as the regulator ensuring accurate SIM registration, national security compliance, and data integrity.
DICT or Authorized Authorithy / SevisPass	Maintain Digital ID system; provide APIs; biometric matching; identity verification; system security.	Supplies the national identity backbone enabling accurate and automated verification.
Mobile Network Operators (MNOs)	Capture customer data; integrate APIs; train agents;	Responsible for frontline registration and ensuring data accuracy for all subscribers.

	secure user data; report compliance.	
SIM Registration Agents	Perform identity checks; use approved devices; follow procedures; maintain audit logs.	Key frontline actors responsible for capturing accurate data and preventing fraud.
RPNGC & Security Agencies	Lawful access to verified subscriber data; investigate SIM-related crime.	Ensures mobile communications are traceable for national security and criminal investigations.
Department of ICT	Policy coordination; alignment with national digital transformation agenda.	Ensures Digital ID ecosystem is integrated across sectors including telecoms.
Consumers / Public	Provide accurate information; use Digital ID credentials.	Critical participants whose cooperation ensures the integrity of the national SIM database.

7. Risk Assessment Summary

Risk Category	Identified Risk	Severity	Explanation / Why It Matters
Legal & Policy Risks	Outdated Regulation; lack of data protection and privacy laws and Data Governance; unclear liability between NICTA-MNOs-SevisPass.	**Critical**	Creates legal ambiguity and blocks the integration of biometrics, APIs, and Digital ID.
Technology Risks	API downtime; cybersecurity threats; slow MNO integration; device failures.	**Critical**	API or system failure could halt nationwide SIM registration; cybersecurity is a major emerging threat.
Cybersecurity Risks	DDoS attacks, identity theft, database intrusions, insider abuse.	**Critical**	Compromises national security; exposes millions of identities; undermines trust in digital services.
Operational Risks	Inconsistent agent practices; poor data capture; rural connectivity gaps.	**High**	Leads to inaccurate subscriber records, fraud, and inefficiency in re-verification.

Financial Risks	MNO integration costs; FX shortages delaying procurement of devices.	**Critical**	Financial constraints may delay or block implementation, affecting compliance timelines.
Social & Cultural Risks	Public mistrust of biometrics; language barriers; low digital literacy rate.	**High**	Could reduce registration uptake and delay national rollout if not managed proactively.
Coordination Risks	Poor collaboration between NICTA, MNOs, DICT, and RPNGC; political interference.	**Critical**	Fragmented implementation will significantly reduce effectiveness and increase compliance costs.
Implementation Risks	Long timelines; lack of trained agents; inconsistent readiness across MNOs.	**High**	May cause uneven application of the new regulation and confusion during transitional periods.

8. Financial, Economic & Social Impact

8.1. Financial Impact on Mobile Network Operators

COST AREA	DESCRIPTION	IMPACT LEVEL	NOTES / EXPLANATION
API INTEGRATION & SYSTEM UPGRADES	Modifying backend systems to connect with SevisPass and enhanced KYC systems.	High	Largest technical cost; requires testing, cybersecurity, and certification.
BIOMETRIC/REGISTRATION DEVICES	Purchase of biometric scanners, tablets, rugged devices.	Medium-High	FX issues may delay imports; essential for frontline registration.
AGENT TRAINING & CERTIFICATION	Mandatory competency training for agents.	Medium	Improves data quality and reduces fraud.
CYBERSECURITY ENHANCEMENTS	Encryption, MFA, access controls, secure storage.	Medium-High	Required to meet ISO 27001/NIST-like standards.

OPERATIONAL ADJUSTMENTS	New procedures, workflow redesign, compliance reporting.	Medium	Transitional cost expected to reduce over time.

8.2. Financial Impact on Government / NICTA

Cost Area	Description	Impact Level	Notes / Explanation
1. **Public Awareness Campaigns**	National outreach, radio/TV messaging, materials.	Medium	Essential for acceptance of Digital ID + biometrics.
2. **Technical & Regulatory Capacity Building**	Training for NICTA officers on audits, API monitoring.	Medium	Needed for compliance oversight.
3. **Rural Outreach / Mobile Enrolment Units**	Supporting Digital ID updates in remote areas.	Medium-High	Ensures no rural exclusion.
4. **Compliance Monitoring & Audits**	Inspections, certification, system testing.	Medium	Ongoing operational cost.
5. **Legal & Policy Development**	Drafting regulation, consultations, technical working groups.	Low-Medium	Required for regulatory update.

8.3. Socio- Economic Impact

Impact Category	Positive Effects	Explanation / Notes
1. **Consumer Trust**	Increased confidence in mobile services and digital transactions.	Verified identities reduce fraud and scams.
2. **National Security**	Improved ability to track illegal communications.	Supports law enforcement and emergency services.

3. **Financial Inclusion**	Stronger identity verification supports mobile money and banking.	Reliable ID boosts fintech and digital economy growth.
4. **Rural Inclusion**	Offline and mobile enrolment solutions support remote areas.	Prevents digital divide and ensures universal service.
5. **Privacy & Safety**	Clearer data protection reduces risk of exploitation.	Protects vulnerable populations from SIM misuse.

9. Scope and Applications

Scope and Application of the 2026 Regulation

The SIM Registration (Amendment and Consolidation) Regulation 2026 will apply to all entities involved in the issuance, registration, verification, management, and deactivation of subscriber identity modules (SIM cards) in Papua New Guinea.

9.1. Entities Covered

The Regulation applies to:

- All **Mobile Network Operators (MNOs)** providing public mobile services in PNG
- Any **Mobile Virtual Network Operators (MVNOs)**, should they be authorized
- All **SIM Registration Agents**, resellers and authorized dealers
- **SevisPass / DICT**, as the provider of Digital ID verification services
- **NICTA**, in its oversight, licensing and enforcement role
- **RPNGC and authorized security agencies**, regarding lawful access to verified subscriber data

9.2. Activities Covered

The Regulation covers:

- New SIM registration and customer onboarding
- Re-verification of existing SIMs
- Identity verification via Digital ID (API-based)
- Capture of biometric data where applicable
- Storage, processing, and reporting of subscriber information
- Deactivation, suspension, or reactivation procedures

- Agent certification and authorization
- Cybersecurity and data protection controls

9.3. Exclusions

The Regulation **does not** apply to:

- Machine-to-machine (M2M) or IoT SIMs that are not associated with individual end-users
- Temporary roaming SIMs issued outside PNG
- Satellite communication services (covered under separate regulatory instruments)

9.4. Relationship with Other Laws

The Regulation aligns with:

- The Constitution of the Independent State of Papua New Guinea
- Cybercrime Code Act 2016
- Electronic Transaction Act 2021
- Digital Government Act 2022
- Identity Registration Act 2024
- Existing public safety and criminal investigation laws

Where conflicts arise, the NICT Act prevails.

10. Proposed Implementation Timeline

Phase	Timeline	Key Activities	Expected Outputs
Phase 1: Preparatory Stage	Q1 2026	- Public consultations- Technical Working Group setup- Draft regulation revisions- API testing with MNOs & SevisPass	• Finalized regulation ready for gazettal • Tested API frameworks
Phase 2: Initial Rollout & Capacity Building	Q2 2026	- MNO system integration- Agent training & certification- Deployment of GPS-enabled devices	• Certified agents • Integrated systems • Prepared operational environment
Phase 3: Mandatory Digital ID for New SIMs	Q3 2026	- National rollout for all new SIMs- Enforcement of new verification procedures	• Zero new SIMs registered without Digital ID • National compliance at point of sale

Phase 4: Nationwide Re-Verification of All Existing SIMs	2027–2028	- Progressive re-verification- Rural outreach and mobile enrolment units- Audit and cleanup of old data	• Accurate national SIM database • Removal of duplicate/fake entries
Phase 5: Enforcement, Monitoring & Optimization	2028+	- Continuous audits- Cybersecurity monitoring- Periodic regulatory updates	• Sustainable compliance • Improved cybersecurity posture

11. Considerations

Area	Consideration	Explanation
Funding Options	FX priority listing, donor support, shared cost models	Helps mitigate high capital costs and procurement delays.
Public Awareness	Culturally appropriate messaging, multilingual materials	Needed to build trust and promote digital literacy.
Legislative and Policy Alignment	Data Governance and Protection Policy, Digital ID Policy, NICT Act, Cybercrime Code Act Digital Government Act, Electronic Transaction Act, Civil Identity and Registration Act etc..	Ensures legal clarity across agencies.
Technical Oversight	Joint NICTA-DICT monitoring body	Ensures interoperability and consistent security standards.
Rural Participation	Offline verification, mobile teams, LLG partnerships	Ensures equitable access across 89 districts.

12. Consultation Questions

NICTA invites stakeholders to provide written comments on the following questions. The consultation is divided into two parts:

- **Part A – Core Consultation Questions** (for all stakeholders)
- **Part B – Technical and Operational Questions** (optional, for technical officers, MNO engineers, Cyber and ICT experts)

PART A. CORE CONSULTATONS QUESTIONS

Policy & Digital ID

1. Do you support the proposed update and consolidation of the SIM Registration Regulation?
2. Should Digital ID be mandatory for all new SIM registrations?
3. Should existing SIMs be re-verified using Digital ID?

Biometrics & Privacy

4. Should biometric verification be required?
5. What privacy safeguards should be included?

Rural Access

6. Are the proposed rural/offline verification methods sufficient?
7. What additional measures should support rural or marginalized groups?

Data Protection & Cybersecurity

8. Should the Regulation mandate minimum cybersecurity standards?
9. What should be the minimum data retention and breach reporting requirements?

Agents & Compliance

10. Should SIM registration agents be licensed and certified?
11. How can NICTA prevent or control agent fraud?

MNO Responsibilities

12. Are the roles and obligations for MNOs clear and achievable?
13. What challenges do MNOs foresee in meeting these requirements?

Implementation & Cost

14. Should the rollout be phased or immediate?
15. What is a realistic implementation timeline?

PART B: TECHNICAL SUPPLEMENTARY QUESTIONS (10)

Digital ID & API Integration

1. What technical challenges do you foresee with API integration into MNO systems?
2. What service-level standards (uptime, redundancy, fallback) should apply to Digital ID APIs?

Biometric & Identity Assurance

3. Should PNG adopt a specific Identity Assurance Level (IAL) for SIM registration?
4. What biometric modalities are most reliable in PNG environments (fingerprint vs facial)?

Cybersecurity Requirements

5. What cybersecurity controls should be mandatory (MFA, tokenization, endpoint security)?
6. Should third-party cybersecurity audits be annual or bi-annual?

Data Governance

7. What is the appropriate data retention period for SIM registration?
8. What data classification standards should apply to MNOs and agents?

Rural Implementation

9. How should offline verification systems synchronize securely once reconnected?
10. What redundancy measures are required to ensure registration continuity?

13. Submission Process for Stakeholders

NICTA invites written submissions from all stakeholders, including MNOs, government agencies, civil society, academia, businesses, and individual citizens.

13.1. Submission Deadline

All submissions must be received by:
January 30th 2026

13.2. How to Submit

Submissions may be sent electronically to:
Email: **consultation@nicta.gov.pg**

with the subject line:
"Submission – SIM Registration Regulation 2026"

or delivered physically to:
National Information and Communications Technology Authority (NICTA)

Attention: Director Economics, Consumer and International Affairs
Punaha ICT Haus, Corner of Croton and Frangipani Street, Hohola
P O Box 8444, Boroko, NCD
Papua New Guinea

13.3. Confidentiality

Submitters must clearly indicate if any part of their submission is confidential.

NICTA may publish non-confidential submissions on its website.

13.5 Next Steps After Consultation

After reviewing submissions:

- NICTA will prepare a **Consultation Summary Report**,
- Incorporate feedback into the final regulation, and
- Submit it for Board endorsement and gazettal.