PAPUA NEW GUINEA

Department of Information and Communication Technology (DICT)

PNG Government

Digital Identification (ID) Standards 2024

Table of Contents

Papua New Guinea Government Digital Identification (ID)Standards 2023.

PART I. - PRELIMINARY.

1. NAME.

This instrument is the PNG Government ***Digital Identification Standards*** and Guidelines 2023.

2. COMMENCEMENT.

This instrument commences on 1st July 2024.

3. AUTHORITY.

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

(2) This instrument acknowledge Section 37 of the Digital Government Act 2022.

4. SIMPLIFIED OUTLINE.

4.1. This instrument prescribes standards and guidelines for government ***Digital Identification (ID).*** All public bodies must comply with this instrument.4.2. This instrument has been developed by the Department of Information and Communication Technology.4.3. Part 1 sets out preliminary matters.

4.4. Parts 2 sets out General Standards and Part 3 sets out Guidelines and Best Practices

4.5. Part 4 contains other relevant matters together with Appendix 1.

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

1. Introduction

A digital identity, usually referred to as a digital ID, is an electronic or digital type of identification.

In a variety of online engagements and transactions, it is used for verifying and authenticating the identity of people or other entities.

Online banking, social networking platforms, government agencies, and other digital settings where identity verification is required frequently employ digital IDs.

This instrument establishes standards, guidelines, processes, and technologies that must be used in the development, usage and management of a digital identification system.

1.1 Scope

This instrument ensures to;

1. establish a secure and user-centric ecosystem for digital identities.
2. enhance online security, simplifies identity management, and enables individuals
3. Support Public bodies to confidently participate in digital transactions and access digital services while safeguarding privacy and trust.

1.2 Purpose

(1) The purpose of Digital ID Standards in Papua New Guinea is to create a safe and user-friendly digital identity environment.

(2) It aims to make online activities more secure, simplify how identities are managed, and enable people and organizations to confidently engage in digital transactions and services while protecting privacy and trust. These standards aim to;

- Promote the secure and efficient management of digital identities.
- Safeguard individual privacy and data protection.
- Enable interoperability between digital ID systems.
- Establish compliance and audit procedures for ongoing monitoring and improvement.

1.3 Application

This instrument must be used to manage Digital Identification across platforms and applications.

Developers must consider;

- Security and privacy
- Technology literacy levels
- National cybersecurity and data governance
- Existing critical infrastructure
- Existing business systems and applications as well as emerging technologies
- Strong legal, regulatory and operational instruments.

1.4 Objectives

The key objectives of the Papua New Guinea Government Digital Identification (ID) Standards 2023 are to:

- establish a secure and user-centric ecosystem for digital identities. Enhance online security
- simplify identity management, and
- enable individuals and organizations to confidently participate in digital transactions and access digital services while safeguarding privacy and trust.
- Establish a robust and secure digital ID ecosystem.
- Enhance the trust and confidence of individuals and service providers in digital IDs.
- Facilitate seamless integration with existing and future government services.
- Protect personal data and ensure compliance with applicable laws and regulations.
- Access for Government-to-Government Services

1.5 Acronyms

Acronyms	**Meanings**
2FA	Two-Factor Authentication.
AML	Anti-Money Laundering.
API	Application Programming Interfaces.
CTF	Counter-Terrorism Financing.
DICT	Department of Information & Communication Technology
DIRC	Department of Internal Revenue Commission.
EDIFACT	Electronic Data Interchange for Administration, Commerce, and Transport.
FHIR	Fast Healthcare Interoperability Resources.
GDPR	General Data Protection Regulation.
HMAC	Hash-based Message Authentication Code.
HOTP	Hash-based One-Time Password.
ICT	Information & Communication Technology.
KYC	Know Your Customer
MFA	Multi-Factor Authentication.
OTP	One-Time Password.

PKI	Public Key Infrastructure.
PNGCIR	Papua New Guinea Civil and Identity Registry.
PNGICA	Papua New Guinea Immigration and Citizenship Authority.
SSO	Single Sign-On.
TOTP	Time-based One-Time Password.
UID	Unique Identifier

1.6 Terms & Definitions

Access Control	Access control is a process of limiting access to a system or to physical or virtual resources. In computing, access control is a process by which users are granted access and certain privileges to systems, resources or information. Access control is a fundamental component of data security that dictates who's allowed to access and use company information and resources. Through authentication and authorization, access control policies make sure users are who they say they are and that they have appropriate access to company data.
Application Programming Interfaces (APIs)	APIs are sets of rules and protocols that allow different software applications to communicate and interact with each other.
Asymmetric cryptography	Also known as public-key cryptography, it is a cryptographic system that uses a pair of keys: a public key for encryption and a private key for decryption. It is widely used for secure data transmission and authentication.
Audit Trails	Audit trails refers to a record of activities, events, or actions that are logged and maintained for the purpose of security, compliance, and accountability. They provide a chronological trail of activities for analysis and review.
Authorization	Authorization is the process of granting or denying access rights to resources or services based on the privileges and permissions assigned to a user or entity.

Biometric Authentication	“Biometric Authentication (Iris scans)” involves using unique biological characteristics, such as iris scans, fingerprints, or facial recognition, to verify and authenticate a person's identity.
Biometric Data	“Biometric Data” refers to measurable physical or behavioral characteristics unique to an individual, such as fingerprints, facial features, or DNA. It is used for biometric authentication and identification purposes.
Biometric System	A biometric system is a technological system that uses unique biological traits to identify a person. These traits can be physiological, behavioral or both. Biometric systems are used for identification and authentication. They rely on specific data about unique biological traits to work effectively. Biometric systems are considered more convenient and secure compared to traditional authentication schemes.
Data Anonymization	“Data Anonymization” is the process of removing or altering personally identifiable information from datasets to ensure that individuals cannot be identified from the data. It is commonly used to protect privacy when sharing or analyzing sensitive data.
Data Pseudonymization	“Data Pseudonymization” involves replacing personally identifiable information with pseudonyms or artificial identifiers, making it more difficult to directly identify individuals while retaining the ability to re-identify them if necessary.
Digital ID	“Digital ID” A digital ID, or digital identity, is a unique electronic representation of an individual or entity used to authenticate their identity in digital transactions or online interactions.
Electronic Data Interchange for Administration, Commerce, and Transport (EDIFACT)	EDIFACT is an international standard for the electronic exchange of structured data, commonly used in business-to-business transactions.
“Fast Healthcare Interoperability Resources” (FHIR)	FHIR is a standard for exchanging healthcare information electronically. It provides a set of resources and APIs to enable interoperability and data exchange between different healthcare systems and applications.

“General Data Protection Regulation” (GDPR)	GDPR is a comprehensive data protection and privacy regulation implemented in the European Union. It sets out rules and requirements for the processing, storage, and transfer of personal data to protect individuals' privacy rights.
Hardware Token	“Hardware Token” is a physical device or token that generates one-time passwords or authentication codes for secure access to systems or services. It provides an additional layer of security in two-factor authentication systems.
Interoperability	Interoperability in the context of digital identification refers to the ability of different functional units, such as systems, databases, devices, or applications, to communicate, execute programs, or transfer data in a manner that requires the user to have little or no knowledge of those functional units. It allows different components and devices to communicate with each other and work together. Interoperability occurs at three levels for ID systems: between ID subsystems (components/devices), within the ID system itself (standards-based technical interoperability), and with other domestic systems.
Single Sign-on (SSO)	Single sign-on (SSO) is an authentication method that allows users to sign in using one set of credentials to multiple independent software systems. This means that users don’t have to sign-in to every application they use, and they can access all needed applications without being required to authenticate using different credentials.
Technology Literacy	Technology literacy is the ability to use, manage, understand, and assess technology. It involves thinking critically and communicating by utilizing technology. Technology literacy is related to digital literacy and is increasingly essential in a modern learning environment. Technology literacy can enhance the learning process through problem-solving and critical thinking.
Unique Identifier	A unique identifier is an identifier that is guaranteed to be unique among all identifiers used for those objects and for a specific purpose. It is a way of selecting, tracking, or counting any object or entity. A unique identifier can be composed of alphanumeric characters and is often associated with an atomic data type.
User-friendly Interface	A user-friendly interface is a software design that is intuitive, easy to navigate, and efficient in meeting the needs of the user. It is not difficult to learn or understand, and it provides quick access to

	common features or commands. A user-friendly interface also avoids unnecessary elements and uses clear language.

1.7 Stakeholders:

In the context of implementing a Digital ID framework in Papua New Guinea, the following stakeholders and departments must consider:

1. **Department of Information and Communication Technology (DICT)**: The DICT plays a crucial role in formulating and implementing policies related to information and communication technologies. They are responsible for overseeing the development and implementation of the Digital ID framework.
2. T**he Papua New Guinea Civil and Identity Registry (PNGCIR)**: This office would be responsible for the overall management of the Digital ID system, including the registration, issuance, and verification of digital identities.

3. **Department of Finance:** The Department of Finance is involved in financial management and budget allocation. They may provide funding and support for the development and maintenance of the Digital ID framework.

4. **Department of Justice and Attorney General**: This department is responsible for legal matters and can provide guidance on compliance with relevant laws, regulations, and privacy considerations related to the Digital ID system.

5. **Department of Internal Revenue (IRC)** : The tax department plays a significant role in implementing the Digital ID system, particularly in terms of linking identities to tax records and enabling secure online tax-related services.

6. **PNG Immigration and Citizenship Authority (ICA)**: This department deals with passport and immigration matters. Integrating the Digital ID system with their processes can help enhance border security and facilitate efficient immigration processes.

7. **Department of Health:** The Department of Health can be a key stakeholder, especially if the Digital ID system is used to access healthcare services or store health-related information securely.

8. **Financial Institutions:** Banks and other financial institutions are important stakeholders as they may integrate the Digital ID system into their processes for customer identification, KYC (Know Your Customer), and secure online banking services.

9. **Telecommunications Providers**: Telecommunication companies play a vital role in providing the infrastructure and connectivity required for the Digital ID system. Collaboration with them can ensure seamless access to digital services.

10. **National Department of Personal Management:** The National Department of Personal Management plays a pivotal role as a key stakeholder in the implementation of a Digital ID system. They can utilize the system for various administrative purposes, including employee identity verification, attendance tracking, and access control to secure government facilities. By integrating the Digital ID system, the department can enhance security measures, ensure accurate personnel records, and streamline administrative processes, leading to increased operational efficiency and data accuracy.

11. **Office of Censorship:** The Office of Censorship serves as a significant stakeholder in the Digital ID system, particularly concerning online content regulation and user identification. With the Digital ID system, the office can enforce age restrictions for certain content, verify the identities of content creators and distributors, and monitor online activities to ensure compliance with regulations. This collaboration enables the office to maintain a safer online environment, protect users from inappropriate content, and enforce regulatory standards effectively.

12. **Office of Electoral Commission:** The Office of Electoral Commission plays a crucial role in democratic processes, and a Digital ID system can enhance the integrity of elections and voter registration. By employing the Digital ID system, the commission can authenticate voters, prevent fraudulent voting, and ensure accurate voter registration. This collaboration fosters trust in electoral processes, enhances transparency, and contributes to the overall credibility of democratic elections.

13. **Office of PNG Customs:** The Office of PNG Customs is a vital stakeholder in trade and border security. By integrating the Digital ID system, customs can streamline customs clearance processes, verify the identities of importers and exporters, and enhance cargo tracking and inspection procedures. This collaboration improves trade facilitation, strengthens border security measures, and mitigates the risks associated with illegal trade activities, ensuring compliance with international trade standards.

14. **Department of Agriculture and Livestock:** The Department of Agriculture and Livestock plays a key role in food production and supply chain management. Through the Digital ID system, the department can track agricultural activities, verify the identities of farmers and stakeholders, and monitor the quality and origin of agricultural products. This collaboration enhances agricultural productivity, ensures food safety, and promotes fair trade practices, benefiting both farmers and consumers.

15. **National Institute of Standards and Technology:** The National Institute of Standards and Technology (NIST) is crucial for setting standards and ensuring the accuracy of measurements. In the context of the Digital ID system, NIST can contribute by validating the accuracy and reliability of biometric and authentication technologies. By collaborating with the Digital ID system, NIST ensures that the standards employed meet international benchmarks, fostering confidence in the system's security and accuracy.

16. **National Statistics Office:** The National Statistics Office plays a vital role in data collection, analysis, and reporting. By integrating the Digital ID system, the office can enhance the accuracy of demographic data, ensure respondent authentication for surveys, and improve the overall reliability of statistical information. This collaboration strengthens the credibility of national statistics, enabling evidence-based decision-making and policy formulation.

17. **Department of Commerce and Trade:** The Department of Commerce and Trade is central to economic activities and trade regulations. Through the Digital ID system, the department can authenticate businesses, verify trade licenses, and monitor trade transactions. This collaboration streamlines business registration processes, enhances trade transparency, and reduces the risks associated with fraudulent business activities, fostering a secure and trustworthy business environment

18. **Civil Society Organizations:** Non-governmental organizations and advocacy groups can provide valuable input and represent the interests of the general public in discussions related to the Digital ID system's design, privacy, and security.

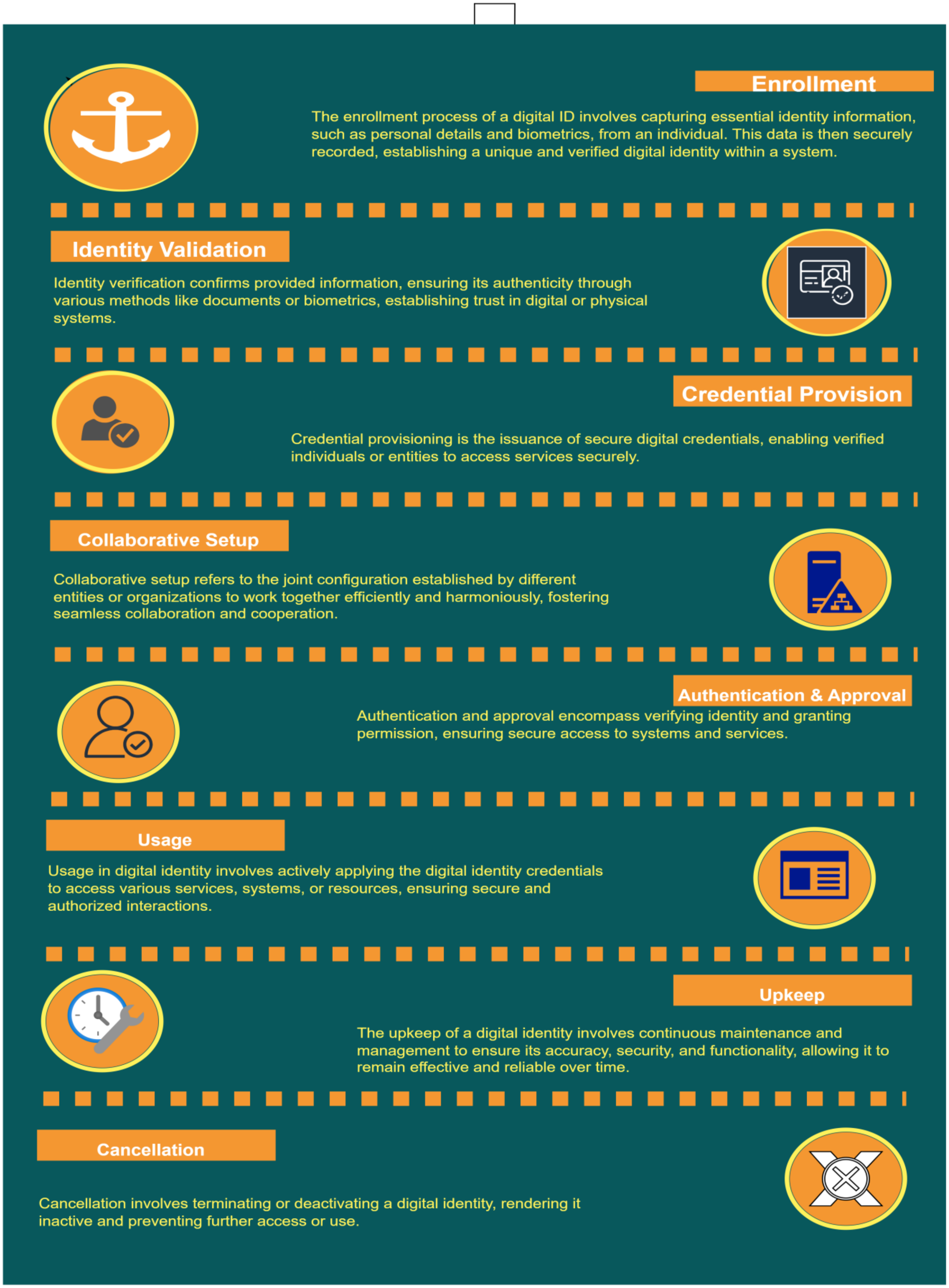
19. **Citizens and Users:** Ultimately, the citizens of Papua New Guinea are the primary stakeholders. Their needs, concerns, and feedback should be considered throughout the development and implementation of the Digital ID framework.

20. **Entrepreneurs and Companies: SMEs and etc**

1.8 Legal and Regulatory Considerations:

- Data Protection and Privacy Laws: The Data Protection Act 2020 in PNG sets forth provisions for the protection and handling of personal data, ensuring that individuals' privacy rights are respected within the digital ID ecosystem.
- Electronic Transactions Act: The Electronic Transactions Act 2000 establishes the legal framework for electronic transactions and recognizes the validity and enforceability of electronic signatures and records in PNG.
- Telecommunications Laws: The Telecommunications Act 1996 and the National Information and Communications Technology Act 2009 regulate 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 the Banking Act and the Anti-Money Laundering and Counter-Terrorism Financing Act, govern financial services and promote measures to prevent money laundering and terrorist financing within the context of digital ID-enabled financial transactions.
- Human Rights Considerations: The development and implementation of the Digital ID framework in PNG must uphold fundamental human rights and freedoms as enshrined in the PNG Constitution, ensuring that individuals' rights to privacy and personal data protection are respected.
- Collaboration with National Security and Law Enforcement: The Digital ID framework should facilitate appropriate collaboration between the digital ID system and national security and law enforcement agencies to address security concerns while respecting legal requirements and individuals' rights.
- Establishing Regulatory Authority: (3) Any government sanctioned digital identity verification and authentication service must be secured by the secured data exchange.
    - As stated in the *Digital Government Act 2021- Under section 31 of* ***Secured Data Exchange Platform****: (3) A*ny government sanctioned digital identity verification and authentication service must be secured by the secured data exchange.

2.Digital ID Management Process Overview"



Enrollment

The enrollment process of a digital ID involves capturing essential identity information, such as personal details and biometrics, from an individual. This data is then securely recorded, establishing a unique and verified digital identity within a system.

Identity Validation

Identity verification confirms provided information, ensuring its authenticity through various methods like documents or biometrics, establishing trust in digital or physical systems.

Credential Provision

Credential provisioning is the issuance of secure digital credentials, enabling verified individuals or entities to access services securely.

Collaborative Setup

Collaborative setup refers to the joint configuration established by different entities or organizations to work together efficiently and harmoniously, fostering seamless collaboration and cooperation.

Authentication & Approval

Authentication and approval encompass verifying identity and granting permission, ensuring secure access to systems and services.

Usage

Usage in digital identity involves actively applying the digital identity credentials to access various services, systems, or resources, ensuring secure and authorized interactions.

Upkeep

The upkeep of a digital identity involves continuous maintenance and management to ensure its accuracy, security, and functionality, allowing it to remain effective and reliable over time.

Cancellation

Cancellation involves terminating or deactivating a digital identity, rendering it inactive and preventing further access or use.

1. **Enrollment/Establishment**

   In this stage, we gather important information from someone who is claiming a specific identity. This information can include things like their name, birthdate, gender, address, and email. We also collect biometric data like fingerprints and iris scans. The choices made about what information to collect and how it's collected are really important because they determine how reliable identity is. It also affects how well identity can work with identity systems both in our own country and around the world.

2. **Identity Validation**

   Once someone claims their identity during enrollment, the next step is validation. This means checking the information they provided against existing data. Validation confirms that the claimed identity is real (making sure the person is alive) and that it's unique within the system. In digital systems, we use biometric data to ensure this uniqueness. We also might link the claimed identity to information in other databases, like civil or population registries, to double-check its accuracy. This process helps guarantee the identity's authenticity and prevents duplicates in the system.

3. **Credential Provisioning**

   Before a person can use their identity for confirmation, their registered identity must go through a credentialing process. In this phase, authorized identity providers can issue various credentials, such as ID numbers, smart cards, or certificates. To qualify as digital, these credentials need to be electronic, meaning they store and transmit data electronically. Electronic credentials generally fall into these categories:

- **Something You Know (like a password):** This includes knowledge-based credentials, such as passwords, that only the individual knows.
- **Something You Have (like an ID card, mobile phone, or cryptographic key):** These credentials involve physical items owned by the individual, like smart cards, mobile phones, or cryptographic keys.
- **Something You Are (like a fingerprint or other biometric data):** Biometric data, such as fingerprints or facial recognition, serves as a unique and inherent credential.
- Different types of electronic credential systems include:
- **Smart Cards:** These cards have advanced security features and store digital cryptographic keys and/or biometric data on a built-in computer chip. Smart cards can be contact or contactless cards, or Near Field Communication (NFC)-enabled SIM cards. Data on a smart card can be accessed offline, allowing authentication even in areas without internet or mobile network connectivity.
- **2D Barcode Cards:** These cards feature an encrypted 2D barcode containing personal data and biometrics. They provide a cost-effective digital identity solution. Authentication occurs by comparing live biometric data with the data stored on the card. This method has been widely adopted in regions like Africa, Latin America, and the Middle East, and is

used in countries like Lebanon, Mali, Ghana, and recently in Egypt for election authentication.

- **Mobile Identity:** Mobile phones and other devices can offer portable digital identity and authentication for various online transactions. Providers can issue SIM cards with digital certificates or use mobile network assets to enable secure identity verification. This method is particularly useful for eGovernment (eGov) services and other public or private platforms.
- **Identity (Credential) in a Central Store/Cloud:** In some systems, certificates and biometrics are stored on a central server instead of portable credentials like smart cards or SIM cards. In these cases, a physical credential storage device might not be issued. Identity numbers may be provided in non-electronic forms (like India's Aadhaar program issuing paper receipts). To enhance security, a tamper-resistant environment is established for cryptographic key generation and management, securing the ID credential in the central store against theft.

4. Collaborative Setup/ Federation

Federation is all about one organization recognizing identity credentials issued by another organization. This mutual recognition is built on trust between organizations. The trusting organization needs to be confident that the trusted organization follows similar policies and rules. Key to making this work are federation protocols and assurance frameworks. These tools enable digital identity federation within and across organizations and even countries.

Protocols and Frameworks: Protocols like SAML (Security Assertion Markup Language) are used to communicate authentication results from the credential provider to the trusting organization. Here's how it works: the trusting organization receives the credential, then sends it to the issuing organization for verification. Once verified, the issuing organization sends back a set of claims. These claims contain user information, details about authentication, and the strength of the credentials used for authentication.

Global Standards and Alignment: For a federation to work on a global scale, it's vital to align and integrate with internationally recognized standards like the ones defined by ISO. This alignment helps establish federation protocols as universal standards.

Levels of Federation: Federation can happen at various levels:

- **Acceptance of Credentials:** An organization acknowledges credentials issued by another organization but still authenticates and authorizes the individual locally. For example, a foreign country might accept a passport issued by another country but still conduct its authentication process.
- **Acceptance of Attributes:** An organization acknowledges specific characteristics (attributes) of an individual from another organization. For instance, a bank might request a credit score from a credit bureau instead of maintaining that information itself.

- **Acceptance of Authorization Decisions:** An organization recognizes an authorization decision made by another organization. For example, a driver's license granting driving privileges in one state is accepted by another state.

5. **Authentication and Approval**

Accessing Benefits and Services with Digital Identity

- Once an individual completes the registration and credentialing process, they can use their digital identity for various services and benefits. For example, citizens can pay taxes through an eGov portal using their eID number, and bank customers can make purchases with smart debit cards or mobile financial services. To access these services, users need to authenticate their identity. Authentication often involves one or more factors falling into three categories: something you know, something you have, or something you are. Here are some methods of authentication:
- **Smart Cards:** Individuals with smart cards can use various factors for authentication. For low-risk situations, a simple PIN might be enough, while high-risk cases could require a digital signature based on public key infrastructure (PKI) technology. Fingerprints can also be used for clear identification. Smart cards store data locally on a chip, allowing offline digital authentication. This is especially useful in remote areas without internet connectivity.
- **Mobile Identity:** Mobile identity uses smartphone applications, USSD, or SMS-based authenticators, or SIM cards for authentication. It integrates multiple factors for different assurance levels. For low-risk situations, a PIN might be sufficient, while high-risk cases might require multiple-factor authentication, including biometrics, or a mobile signature based on PKI technology with a secure element (SE). Additional factors like user location or behavior can further strengthen authentication.
- **ID in the Central Store/Cloud:** In this scenario, a digital identity system relies on biometrics for remote authentication. Identity verification happens through a computer or device with a biometric reader connected to the Cloud. Unlike physical credentials, this Cloud-based system eliminates the need and cost of physical documents. However, it requires robust ICT infrastructure for connectivity and security of the central storage.

6. **Usage**

In the phase of Utilization and Entry, registered digital identities come into active play, enabling individuals to access different services and platforms. During this stage, people use their digital credentials to enter secure systems or conduct online transactions. Utilization methods encompass actions such as logging into secure portals, conducting financial transactions, or entering restricted digital spaces. This phase represents the real-world application of digital identity for accessing services and resources.

7. **Upkeep or Maintenance**

Ongoing Maintenance and Enhancements represent the continuous efforts involved in managing digital identities post-creation. During this stage, identity attributes might be updated, credentials might be renewed, and security measures could be strengthened. This phase ensures that the digital identity remains accurate, up-to-date, and secure. Additionally, enhancements might involve incorporating new technologies or standards to improve the overall effectiveness and security of the digital identity system. Maintenance and Enhancements are essential for adapting to evolving security challenges and technological advancements.

8. **Cancellation or Revoke**

   Revocation/Invalidation refers to the intentional cancellation or rendering null and void of a digital identity credential. This action is taken if a credential has been compromised, misused, or is no longer deemed trustworthy. Revocation ensures that the credential can no longer be used for authentication or authorization. Invalidating a credential involves declaring it as no longer valid, preventing its acceptance by relying parties. Both revocation and invalidation are critical measures in maintaining the integrity and security of the digital identity ecosystem.

- **Data Preservation and Confidentiality**

  Data Preservation and Confidentiality involve the secure storage and protection of digital identity-related information. During this phase, personal and biometric data associated with the digital identity are preserved for legitimate purposes, such as historical records or legal requirements. Simultaneously, maintaining confidentiality ensures that the stored data remains protected against unauthorized access or breaches. Strict protocols are in place to safeguard the data's integrity and confidentiality, adhering to privacy regulations and industry standards.
- **Termination/Removal**

  Termination/Removal signifies the deliberate discontinuation and removal of a digital identity from the system. This phase occurs when an individual's association with the organization ends, and their digital identity is no longer needed. Termination ensures that the identity is completely deactivated, preventing any future access to services or systems. Removal involves the permanent deletion of identity-related records and data from the system, ensuring that no trace of the digital identity remains in the organization's databases.

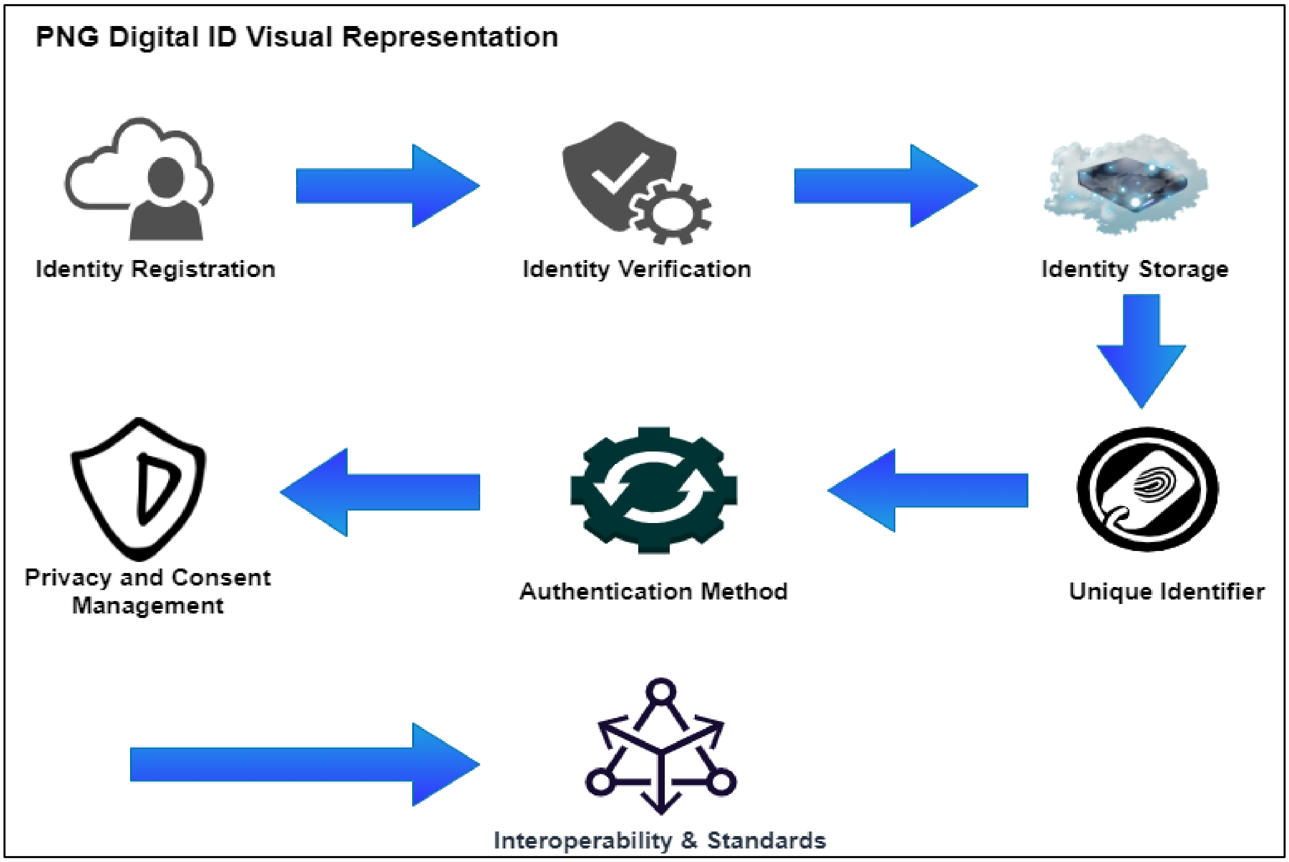
- **Renewal/Reissuance**

  Renewal/Reissuance involves the process of updating or reissuing digital identity credentials. During this phase, expired or outdated credentials are renewed, ensuring that the digital identity remains valid and up-to-date. Renewal may involve verifying the user's identity again and issuing new credentials, such as updated certificates or access tokens. Reissuance is essential for ensuring the continuity of services and maintaining the security of the digital identity system. It allows individuals to continue using their digital identities without interruption while ensuring that the credentials remain current and reliable.

0

PART II. - Digital ID Process and General Standards.

Figure 1: Digital ID Visual Representation



2. Identity Registration

Users register their identity information with a trusted authority or identity provider. This information may include personal details, such as name, address, date of birth, and biometric data.

The table below outlines specific Activities that fall under **Identity Registration.**

1. **Personal Information Collection**	- **It would be necessary for people to provide their contact details as well as their full names, dates of birth, places of birth, genders, and nationalities.**
2. **Personal Information Collection**	- Individuals would be required to show supporting documentation to authenticate their identity, such as a birth certificate, passport, national identity card, or any other official identifying document. - The information submitted upon registration is cross-referenced using these papers, which also serve as evidence of identity.
3. **Biometric Data Collection**	- Biometric data may be collected in some circumstances to improve identification verification. This may involve the collection of face recognition data, eye scans, or fingerprints. Biometric information is specific to each person and adds a further level of protection and accuracy when authenticating their identity.
4. **Registration Form Submission**	- Individuals must submit a registration form or application to the authorized registration authority once they have gathered all the essential information and papers. This might be a government agency in charge of identity registration or any other approved body.

3. Identity Verification

Various approaches are used to verify the identification information supplied during registration. Document verification, biometric matching, and multi-factor authentication are all examples of this.

The table below outlines specific activities that fall under **Identity Verification.**

1. **Document Verification**	- During registration, submitted identification documents are carefully examined and validated to ensure their legitimacy and authenticity. This involves checking passports, national identity cards, and birth certificates. The verification process includes cross-referencing the provided information with government databases or contacting the relevant issuing authorities to confirm the legal status of the documents.
2. **Biometric Matching**	- Biometric data gathered during registration is compared to validate identification using fingerprint matching, face feature

	comparisons, and iris scanning. Biometric matching is a precise method of identity verification based on unique, difficult-to-fabricate physical or behavioral features.
3. Background Checks	• Background checks may be performed in some instances to confirm an individual's identification. Checking criminal records, employment histories, or other relevant databases may be necessary. Background checks aid in identifying any discrepancies or irregularities that may raise questions about a person's identity.
4. Reference Checks	• In a few instances, the individual's references may be called to verify their identity. Contacting employers, educational institutions, or personal references to verify the individual's statements and prove their identification is one example.
5. Address Verification	• To verify its accuracy, the address or contact information provided may be validated. Cross-checking the address against government records, utility bills, or performing site visits to establish the physical existence of the address might be part of this process.
6. Data Analytics and Risk Assessment	• Advanced data analytics techniques analyze patterns, behaviors, and data points to detect identity fraud or misrepresentation. This includes comparing individual information with fraudulent profiles and detecting suspicious activities.
7. Multi-Factor Authentication (MFA)	• To enhance security, multi-factor authentication uses multiple factors for identity verification. It combines what the individual knows (password or PIN), what they have (smartphone or token), and what they are (biometric data) to establish identity.

4. Identity Storage

The verified identity information is securely stored in a digital format, usually in a centralized database or distributed ledger technology (e.g., blockchain).

The table below outlines specific activities that fall under **Identity Storage.**

1. Secure Database Management	• A database stores individuals' identity information and can be centralized or distributed. It may be a secure server or a cloud-based infrastructure and should handle large data

	volumes, ensure data integrity, and protect against unauthorized access.
2. Encryption and Data Protection	- Strong encryption techniques protect stored identity information from unauthorized access or breaches. Encryption ensures secure storage and restricts access to authorized entities with decryption keys.
3. Access Control and User Management	- Access control mechanisms manage user access to the identity storage system. This includes defining user roles, permissions, and authentication protocols to ensure authorized personnel can access and manage stored identities. User management involves adding, updating, and removing identities as needed.
4. Audit Trails and Logging	- Audit trails and logging mechanisms are implemented to track and monitor activities in identity storage. This ensures traceability and accountability, enabling the detection of unauthorized access attempts or suspicious activities.
5. Backup and Disaster Recovery	- Regular backup procedures are implemented to securely back up identity data, enabling restoration in case of data loss or system failure. Disaster recovery plans are established to minimize downtime and ensure continuity of identity storage services.
6. Compliance with Data Protection Regulations	- Identity storage systems must comply with data protection regulations and privacy laws. This involves adhering to requirements such as data retention periods, data anonymization, consent management, and empowering individuals with control over their data.
7. Data Sharing and Interoperability	- Identity storage systems may facilitate secure data sharing with authorized entities based on the context. This involves establishing protocols and standards for data exchange, enabling interoperability between different service providers or platforms while maintaining data privacy and security.
8. Regular Security Assessments and Updates	- Identity storage systems should undergo regular security assessments, vulnerability scans, and updates to address emerging threats and maintain a high level of security. This involves applying security patches, updating encryption protocols, and staying up to date with the latest best practices in identity data protection.

5. Unique Identifier

Each individual or entity is assigned a unique identifier, such as a digital certificate or token, which serves as their digital representation in online transactions.

The table below outlines specific activities that fall under **Unique Identifier (UID).**

1. Generation of Unique Identifiers	- A process is set up to generate unique identifiers for individuals or entities in the digital identity system. These identifiers can take the form of alphanumeric strings, numerical codes, or other formats, ensuring uniqueness and preventing duplication.
2. Linking Identifiers to Identity Information	- Unique identifiers generated are linked to the corresponding identity information of individuals. This association enables convenient retrieval and referencing of the relevant identity details when the identifier is utilized.
3. Issuance and Distribution of Identifiers	- Unique identifiers are assigned to individuals after successful identity verification and registration. Depending on the system, these identifiers may be issued by government authorities, identity providers, or authorized entities. The process involves securely distributing the identifiers to individuals through various means, such as digital certificates, tokens, or smart cards.
4. Integration with Digital Systems	- Unique identifiers are integrated into digital systems, platforms, or applications that require identity verification. This integration enables these systems to recognize and accept the identifiers as valid references to the corresponding identities during authentication or transaction processes.
5. Use in Online Transactions and Interactions	- Once assigned, unique identifiers are used in online transactions and interactions to establish individual identity. This involves individuals providing their unique identifier as part of the authentication process when accessing online services or verifying their identity during digital transactions.
6. Cross-Referencing and Validation	- To ensure integrity and accuracy, the unique identifiers are cross-referenced with the stored identity information. This validation process helps prevent identity theft, fraud, and misuse of the identifiers.
7. Secure Storage and Management	- The unique identifiers are securely stored and managed within the digital identity system. Robust measures are in place to safeguard the confidentiality and integrity of the identifiers, ensuring that only authorized entities and systems can access them.

6. Authentication Mechanisms

Various authentication mechanisms are employed to ensure that the digital identity holder is the legitimate owner. This can include passwords, PINs, biometrics, or hardware tokens.

The table below outlines specific activities that fall under **Authentication Mechanisms.**

1. Password-based Authentication	• During the authentication process, users provide a password compared against the stored password associated with their digital identity. A successful match between the provided password and the stored one indicates successful authentication. To enhance security, it is crucial to enforce strong password policies, including requirements for password length, complexity and other security measures.
2. Multi-Factor Authentication (MFA)	• Multi-factor authentication (MFA) enhances identity assurance by combining multiple authentication factors. These factors include: a. One-Time Passwords (OTP): Users receive time-sensitive, single-use codes via SMS, email or authenticator apps. They enter the code along with their password for authentication. b. Biometric Authentication: Unique physical or behavioral characteristics like fingerprints, facial recognition or iris scans are used for identification. Biometric data is compared to enrolled data to authenticate the user. c. Hardware Tokens: Users possess physical devices (e.g., security keys or smart cards) that generate unique codes or enable cryptographic authentication. These MFA methods provide an additional layer of security, making it more challenging for unauthorized individuals to gain access to protected systems or data.
3. Public Key Infrastructure (PKI)	• PKI uses asymmetric cryptography, involving public and private key pairs. The private key is securely stored by the user, while the public key is distributed and associated with the digital identity. Authentication occurs by encrypting a challenge with the private key, which can only be decrypted by the corresponding public key.
4. Single Sign-On (SSO)	• SSO allows users to authenticate once and gain access to multiple interconnected systems or applications without the need for repeated authentication. This streamlines the user

	experience and reduces the burden of remembering multiple passwords.
5. Risk-Based Authentication	- Risk-based authentication systems evaluate contextual factors like user location, device characteristics and behavior patterns to determine the risk level of a login attempt. Based on the risk assessment, the system applies suitable authentication measures, such as step-up authentication for high-risk events. This approach enhances security by dynamically adapting authentication requirements to match the perceived level of risk, providing a more robust defense against unauthorized access or fraudulent activities.
6. Time-Based Authentication	- Time-based authentication involves generating time-sensitive codes that have a short lifespan. Algorithms like Time-based One-Time Password (TOTP) or Hash-based message authentication code (HMAC), HMAC-based One-Time Password (HOTP) are commonly used in two-factor authentication (2FA) to achieve this. These codes provide an additional layer of security by expiring quickly, ensuring that they cannot be reused or intercepted by unauthorized individuals.
7. Single-Use Links or Tokens	- Users are given unique links or tokens that authorize access to specific resources or sessions. Once the link or token is utilized, it becomes invalid, guaranteeing its one-time use and preventing unauthorized access. This approach enhances security by ensuring that only authorized individuals can gain entry to the designated resource or session.

7. Privacy and Consent Management

Users have control over their digital identity and can manage their privacy settings, consent to data sharing and revoke access to their information when needed.

The table below outlines specific activities that fall under **Privacy and Consent Management.**

1. Privacy Policy Development	- Organizations need to develop clear and comprehensive privacy policies that outline how personal information is collected, used, stored, and shared. The policy should address the purpose of data collection, data retention practices, security measures and any third-party sharing.
2. Consent Collection	- Organizations must obtain explicit consent from individuals before collecting, processing, or sharing their

	personal information. This includes providing clear and transparent information about the purpose of data collection, its usage, and any involvement of third parties. Consent can be obtained through opt-in mechanisms, checkboxes, or other means to ensure individuals are fully informed and actively agree to the data practices.
3. Consent Management	• Once consent is obtained, organizations must establish processes to manage and document individuals' consent preferences. This includes maintaining a record of consent given, the specific purposes for which consent was granted and any subsequent changes to consent preferences.
4. Privacy Settings and Controls	• Organizations should provide individuals with privacy settings and controls that allow them to manage their personal information. This can include options to control the visibility of certain data, choose the types of communication received, or opt-out of certain data processing activities
5. Data Minimization and Purpose Limitation	• Organizations should practice data minimization, collecting and processing only necessary personal information for the intended purpose. They should also ensure that personal information is not used beyond the scope of consent, maintaining purpose limitation.
6. Data Anonymization and Pseudonymization	• To enhance privacy, organizations may employ techniques such as data anonymization or pseudonymization. Anonymization involves removing or irreversibly transforming personally identifiable information, while pseudonymization replaces identifying information with pseudonyms, protecting individual identities while still allowing data analysis or processing
7. Data Security and Protection	• Robust security measures should be implemented to protect personal information from unauthorized access, disclosure, or breaches. This includes encryption, access controls, regular security audits and employee training on data protection.
8. Data Subject Rights	• Organizations should facilitate individuals' exercise of their data subject rights, such as the right to access their personal data, rectify inaccuracies, request erasure, or

	restrict processing. Processes should be in place to handle such requests promptly and transparently
9. Data Breach Response	- Organizations must have protocols for addressing data breaches or incidents impacting personal information. This involves notifying affected individuals, regulatory authorities, and taking necessary actions to minimize the impact of the breach.
10. Regular Compliance Audits and Assessments	- Organizations should regularly audit and assess compliance with privacy regulations, industry standards, and internal policies. This involves reviewing data handling practices, privacy controls, and conducting privacy impact assessments (PIAs) for new projects or system changes.

8. Interoperability and Standards

Digital ID systems should adhere to interoperability standards to ensure compatibility and seamless integration with different service providers and platforms.

The table below outlines specific activities that fall under **Interoperability and Standards.**

1. Standardization	- Establishing and following industry-wide standards and protocols is vital for interoperability. This involves adopting widely accepted standards for data formats, communication protocols, and interfaces to enable effective information exchange between different systems.
2. Data Exchange Formats	- Defining standardized formats for data exchange is crucial for interoperability. Commonly used formats like XML (eXtensible Markup Language), JSON (JavaScript Object Notation), or HL7 (Health Level 7) in the healthcare domain enable consistent interpretation and processing of data across systems.
3. Application Programming Interfaces (APIs)	- Developing and implementing APIs allows different systems and applications to interact and exchange data in a standardized manner. APIs define the rules, data structures, and operations that can be performed, enabling seamless integration and interoperability.

4. Semantic Interoperability	• Ensuring semantic interoperability involves establishing a shared understanding of the meaning and context of exchanged data between systems. This can be achieved through standardized data models, ontologies, or controlled vocabularies that enable consistent interpretation and integration of data across diverse systems.
5. Message Exchange Standards	• Implementing message exchange standards like HL7, EDIFACT, or FHIR (Fast Healthcare Interoperability Resources) enables the structured exchange of messages between systems. These standards establish the format, content, and construction rules for messages, ensuring consistency and interoperability in data exchange.
6. Metadata Standards	• Using metadata standards ensures consistent capturing and sharing of relevant information about data, including its structure, semantics, and relationships. Standards like Dublin Core or Schema.org facilitate interoperable description and discovery of data across diverse systems.
7. Interoperability Testing and Certification	• Conducting interoperability testing and certification processes ensures that systems meet the required standards and can successfully interact with other compliant systems. This helps identify and resolve compatibility issues, ensuring seamless integration and reliable interoperability.
8. Interoperability Frameworks	• Developing interoperability frameworks or guidelines offers a comprehensive set of best practices, recommendations, and technical specifications to facilitate interoperability. These frameworks help organizations implement interoperable solutions and ensure adherence to industry standards.
9. Regulatory Compliance	• Compliance with relevant regulations, such as the General Data Protection Regulation (GDPR) or the Health Insurance Portability and Accountability Act (HIPAA), is crucial for ensuring interoperability and data exchange while maintaining data privacy and security.
10. Collaboration and Governance	• Establishing collaborative efforts, industry consortia, or governance bodies that bring together stakeholders from different domains promotes cooperation, standardization and interoperability. These initiatives facilitate the

	development and adoption of common standards and practices across sectors.

8.Compliance and Audit

The objective of the Compliance and Audit section within the Digital ID Framework in Papua New Guinea (PNG) is to ensure adherence to relevant laws, regulations, and industry standards, fostering accountability, transparency, and trust in the digital identity ecosystem.

1. **Compliance Frameworks:**

- The Digital ID Framework in PNG aligns with the following compliance frameworks:
- Personal Data Protection Act: Compliance with provisions for protecting individuals' personal information.
- Electronic Transactions Act: Ensuring legal validity and enforceability of digital transactions and identities.
- Information and Communication Technology (ICT) Policy: Compliance with relevant policy guidelines and directives issued by the PNG government.

2. **Auditing and Certification Requirements:**

- To assess and verify compliance, the framework incorporates the following elements:
- Independent Audits: Periodic independent audits to evaluate the effectiveness of controls, processes, and data protection measures.
- Certification Requirements: Establishment of certification criteria based on recognized international standards, such as ISO/IEC 27001, to demonstrate compliance with information security management practices.
- Third-Party Assessments: Engagement of external auditors or assessment bodies to validate control implementation and ensure compliance.

3. **Regulatory Compliance:**

- The Digital ID Framework ensures compliance with relevant regulations and guidelines:
- Data Protection and Privacy: Implementation of measures to safeguard the confidentiality, integrity, and availability of personal data in accordance with data protection laws.

- Consent Management: Establishment of mechanisms for obtaining and managing user consent in line with privacy regulations, ensuring individuals have control over their personal information.
- Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF): Incorporation of AML and CTF measures to mitigate risks associated with identity fraud and illegal activities.

4. **Continuous Monitoring and Evaluation:**

- To address compliance gaps and emerging risks, the framework promotes continuous monitoring and evaluation:
- Risk Assessments: Regular assessments to identify vulnerabilities, threats, and compliance gaps.
- Incident Response and Reporting: Establishment of incident response procedures and reporting mechanisms to address security incidents, breaches, and non-compliance issues promptly.
- Compliance Reporting: Generation of regular compliance reports to provide stakeholders, including regulatory authorities, with transparency on the framework's compliance status.

5. **Stakeholder Engagement:**

- Engagement with relevant stakeholders is crucial for effective compliance and audit:
- Government Agencies and Regulatory Bodies: Collaboration with agencies and bodies responsible for overseeing compliance and regulatory aspects of the digital identity ecosystem.
- User Groups: Involvement of user groups to gather feedback, address concerns, and ensure their interests are represented in compliance and audit processes.

PART III. - Digital ID Guidelines and Best Practices

9. Digital ID Management Guidelines

The following guidelines provide recommendations for each process of digital identification management as provided in the above standards.

These guidelines provide public bodies with the best practices needed to accurately identify, credential and manage digital identification.

Guideline 1 Enrollment and Identity Validation

Guideline 1.1 Understand the basic flow for enrollment and identity proofing

The process of enrollment and identity proofing as defined by NIST SP 800-63A consists of three factors: Resolution, Validation and Verification. These are the steps needed to be completed to ensure that the digital identity is mapped to and validated against an individual/user.

It is important that all users and public bodies understand these three important steps.

(a) Resolution – This step involves collecting the users core attributes and evidence to uniquely distinguish them from a given population.

(b) Validation – This step involves validating and authenticating the attributes received from the individual to determine that it is related to the individual.

(c)Verification – The link between the claimed identity and the individual is established which confirms the digital identity to the user.

Guideline 1.2 Verifying digital credentials

In the process of validating a digital identity, the data is verified to exist and be correct and real. During the verification process, the relationship and ownership of the data and the person should be established, and the identity is confirmed.

Identity verification needs to occur to establish trust and ensure that individuals accessing services, conducting transactions, etc. are indeed who they claim to be.

There are several mechanisms that can be used to establish the uniqueness of an identity. For instance, birth registers and biometrics.

Guideline 1.3 Use Identity Assurance Levels

Identity assurance levels should be used to determine the strength of assurance of the digital identity of the individual. There are typically three levels of assurance, in order of strength:

(a) Identity Assurance Level 1 (IAL1): Little or no confidence of identity

(b) Identity Assurance Level 2 (IAL2): Medium or some confidence of identity

(c) Identity Assurance Level 3 (IAL3): High level of identity

Guideline 1.4 User Notification

The individual should always be notified of the enrollment and identity proof to educate them about what is happening. This includes the purpose for collecting attributes and records, period for the records to be kept, why it is important to provide their attributes and what will happen if they don’t provide. This notification should be given in a language that is easily understood.

Guideline 1.5 Ensure multiple verification layers

To validate the identity of an individual, ensure there are multiple ways of authenticating digital identification.

Enabling multiple layers of authentication can also improve and enhance security of the individual's digital identity.

There are multiple ways that digital identities can be validated and includes;

- Document verification
- Knowledge-based verification
- Background checks
- Database verification
- Email verification
- Phone number verification
- Social media verification

Guideline 1.6 Reduce risks involved with human verification methods

Use a reliable digital validation method that will mitigate risks associated with human judgement related risks thus reducing human error in validating a digital identity.

For example, traditional methods of identity validation rely primarily on human verification techniques, such as comparing a person's photograph on a government-issued identity with those requesting certain services. Unauthorized professionals, on the other hand, can readily circumvent these verification methods by modifying the documents using many free programs available on the market.

Guideline 2 Credential Provision

Guideline 2.1 Issuance of credentials

The data that was collected in Enrollment and validated are then issued as credentials. This may include smartcards, biometrics, etc.

Guideline 3 Authentication and Approval

Guideline 3.1 Authentication infrastructures

Keep in mind that for digital identities and credentials provided to users to be useable, some type of system (i.e., authentication infrastructure) is required to provide a portal for online or offline authentication.

Note that centralized and decentralized identity management are two different approaches to managing user identity data which plays a very important part in whether it is an offline or online system.

Some authentication infrastructures may include mobile applications can be used for mobile-based authentication, smart card readers or terminals for smart cards or mobile-phone based authentication and biometric terminals for biometric-based authentication.

Guideline 3.2 Enable multifactor authentication

An individual's identity is authenticated through the use of one or more factors which may include a Personal Identification Number (PIN), password or some other factor known or possessed by the authorized individual.

Although single factor authentication is simpler and faster, it is important there are at least two or more methods of authenticating an individual's identity which is known as two-factor (2FA) or multifactor authentication (MFA). For instance, in addition to providing a PIN/password or using their smartcard, the individual must provide a biometric scan to authenticate themselves.

This enhances security of the individuals' digital identity. A pin/password or a smartcard can be stolen or forged but a biometric scan (fingerprint or eye scan) is unique to the individual and harder to replicate.

Guideline 4 Usage

Guideline 4.1 Keep safe digital identification credentials

It is important that the credential to an individual is kept safe from unauthorized usage. This is the same practice of not sharing your social media account passwords.

Ensure that all credentials are safe and always report incidents when they are lost, or related suspicious activities such as identity fraud.

Guideline 5 Upkeep

Guideline 5.1 Always keep data records updated

Maintenance of your digital identity data is a very integral part of digital identity management. Individuals should be required to maintain their records whenever there are changes in their credentials, for example, contact and address changes, etc. This ensures that the digital identity data is accurate and stays up to date.

This also helps to avoid errors that may occur in the usage of your digital identity.

Guideline 5.2 Updates to records should be maintained across agencies and platforms

These updates to credentials should be propagated across public bodies and systems or authentication infrastructures.

10. Digital ID Implementation Guidelines:

The objective of the Implementation section within the Digital ID Framework is to provide guidance and procedures for the successful deployment and operationalization of the digital identity system in Papua New Guinea (PNG).

1. Project Planning and Management:

This section outlines the key steps and considerations for planning and managing the implementation of the digital identity system:

- Project Initiation: Define project goals, scope, and stakeholders. Establish a project team and governance structure.

- Resource Allocation: Allocate resources, including budget, technology infrastructure, and human resources, necessary for implementation.

- Project Schedule: Develop a detailed project plan with timelines, milestones, and dependencies.

- Risk Management: Identify and assess risks and develop mitigation strategies.

- Change Management: Implement strategies to manage organizational change and stakeholder engagement throughout the implementation process.

2. Technical Infrastructure Setup:

This section focuses on the necessary technical components and infrastructure required for the digital

- identity system implementation: Hardware and Software: Procure and configure hardware and software components needed to support the system's operation, including servers, databases, and networking equipment.

- System Integration: Integrate the digital identity system with existing infrastructure, such as government databases, authentication services, and service provider platforms.

- Testing and Quality Assurance: Conduct comprehensive testing to ensure the system's functionality, security, and interoperability.

- Scalability and Performance: Design the system to handle increased user demands and ensure optimal performance.

3. User Onboarding and Registration:

This section provides guidelines for user onboarding and registration processes:

- Registration Methods: Define the methods for user registration, such as in-person registration centers, online registration portals, or mobile registration units.

- Identity Proofing: Establish procedures for verifying the identity of users during the registration process, including document verification, biometric data capture, and identity attribute validation.

- Privacy and Consent: Implement mechanisms to obtain user consent and inform them about the collection, use, and protection of their personal data.

- User Education and Support: Develop user education materials and support channels to assist users in understanding and navigating the registration process.

4. Service Integration and Adoption:

This section addresses the integration of digital identity services with various government

- departments and service providers:

Interoperability Framework: Define interoperability standards and protocols to enable seamless integration with government systems, databases, and service provider platforms.

- Service Provider Engagement: Collaborate with service providers to integrate digital identity services into their platforms and systems.

- User Experience Design: Ensure a user-friendly and intuitive experience for individuals accessing services through the digital identity system.

- Monitoring and Evaluation: Implement monitoring mechanisms to track service adoption, user satisfaction, and system performance.

5. Training and Capacity Building:

This section focuses on building the necessary skills and capacity among stakeholders involved in the

- implementation and operation of the digital identity system:

Training Programs: Develop training programs to equip system administrators, support staff, and user registration agents with the necessary knowledge and skills.

- Awareness Campaigns: Conduct awareness campaigns to educate users and stakeholders about the benefits, features, and proper use of the digital identity system.

- Continuous Learning: Establish mechanisms for continuous learning and knowledge sharing to keep stakeholders updated with evolving technologies and best practices.

11. Conclusion

This digital ID framework suggests a digital identification process that may be used as an alternative to the physical identification system that is current in Papua New Guinea.

This framework identifies key elements for the effective management of digital identification and associated technologies as well as ensuring all its systems are protected, secured, controlled, tested and maintained.

A digital ID plan, standards and other relevant instruments, may be derived from this framework to assist in developing a robust and interoperable digital identification system in the country.

PART IV. - Miscellaneous

Appendices

Appendix 1: Definitions

Appendix 2: References

International Organization for Standardization (ISO):

ISO/IEC 27001: Information security management systems - Requirements

ISO/IEC 27002: Code of practice for information security controls

ISO/IEC 27018: Code of practice for protection of personally identifiable information (PII) in public clouds

ISO/IEC 30107: Biometric Presentation Attack Detection

ISO/IEC 24760: A framework for identity management

Website: ISO

National Institute of Standards and Technology (NIST):

NIST SP 800-63: Digital Identity Guidelines

NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations

NIST SP 800-63B: Digital Identity Guidelines - Authentication and Lifecycle Management

NIST SP 800-63C: Digital Identity Guidelines - Federation and Assertions

NIST SP 800-63-3: Digital Identity Guidelines - Enrollment and Identity Proofing

Website: NIST

Healthcare Information and Management Systems Society (HIMSS):

HIMSS Identity Management Task Force: Link

Health Level Seven International (HL7):

HL7 FHIR (Fast Healthcare Interoperability Resources)

HL7 Standards: https://www.hl7.org/fhir/.

Identity Defined Security Alliance (IDSA): https://www.idsalliance.org/.

Open Identity Exchange (OIX):

https://openidentityexchange.org/resources/whitepapers-reports