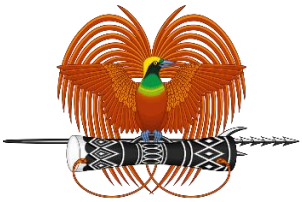

Papua New Guinea

Department of Information and Communication Technology

Government E-Payment Standards

Document Control:

Document Name	PNG Government E-Payment Standards
Prepared By	Department of Information and Communications Technology
Edition	Draft 2
Approved by	Public Service ICT Steering Committee
Date Approved	
Effective Date	
Next Review Date	

Papua New Guinea Government Cloud Standards **2024.**

ARRANGEMENT OF CLAUSES.

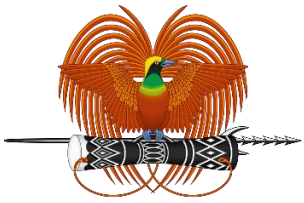

Table of Contents

Papua New Guinea Government E-Payment Standards.

PART I. - PRELIMINARY.

1.Name

This instrument is the PNG Government E-Payment Standards 2024.

2.Commencement

This instrument commences on 1 January 2025.

3.Authority

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

4. Simplified Outline

(1) This instrument prescribes standards and guidelines for government E-Payment. All public bodies must comply with this instrument.

(2) This instrument has been developed by the Department of Information and Communication Technology.

(3) Part 1 sets out preliminary matters.

(4) Parts 2 sets out Standard 1 and Part 3 sets out Standard 2. Part 2 and 3 contain mandatory standards.

(5) Part 4 contains other relevant matters together with Appendix 1.

(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.

5. Definitions

"Electronic Payment (E-Payment)" The process of making financial transactions electronically, often using digital methods such as credit cards, debit cards, bank transfers, or mobile payment apps.

"Government E-Payment Services" Payment services provided by government agencies to facilitate the collection of fees, taxes, fines, and other payments from citizens and businesses electronically.

"Payment Gateway" A service that acts as an intermediary between the government agency and the payment processor, securely facilitating the transfer of payment data.

“Payment Processor” A financial institution or third-party service provider that processes electronic payments on behalf of the government agency. This can include banks, credit card companies, and online payment platforms.

“Digital Wallet” A software-based system that allows users to store and manage their payment card information and make electronic transactions securely.

“Authentication” The process of verifying the identity of the user making an electronic payment, often through the use of usernames, passwords, PINs, biometrics, or two-factor authentication (2FA).

“Encryption” The process of converting sensitive payment data into a coded format to protect it from unauthorized access or theft during transmission.

“Tokenization” The practice of replacing sensitive payment information with a unique token, reducing the risk of exposing the actual data during transactions.

“Compliance” Adherence to relevant laws, regulations, and security standards when processing electronic payments, including data protection and privacy requirements.

“PCI DSS” (Payment Card Industry Data Security Standard) A set of security standards designed to ensure that all organizations that accept, process, store, or transmit credit card information maintain a secure environment.

“ISO 20022” An international standard for financial messaging, including payment instructions and formats, used to improve interoperability and data consistency in electronic payments.

“API” (Application Programming Interface) A set of rules and protocols that allow different software applications to communicate and exchange data, enabling integration between government e-payment systems and other services.

“Accessibility” Ensuring that government e-payment services are designed and implemented in a way that is accessible to individuals with disabilities, such as visual impairments or mobility issues.

“User Experience (UX)” The overall experience and ease of use that individuals encounter when interacting with government e-payment services, including the user interface and navigation.

“Audit Trail” A detailed, chronological record of all transactions and activities related to government e-payment services, which is essential for tracking and accountability.

“Fraud Detection and Prevention” The implementation of mechanisms and tools to identify and mitigate fraudulent activities within government e-payment systems.

“Settlement” The process of transferring funds from payer accounts to the government agency's account, often involving reconciliation and validation of payment data.

“Refund Policy” The established guidelines and procedures for issuing refunds to users who have overpaid or experienced payment errors in government e-payment services.

“Interoperability” The ability of different government e-payment systems and platforms to work together seamlessly, facilitating cross-agency or cross-border transactions.

“Mobile Payments” Payment methods that enable users to make transactions using mobile devices, such as smartphones or tablets, often through mobile apps or SMS.

“Digital Signatures” Electronic signatures that provide authentication and ensure the integrity of documents and transactions in government e-payment services.

“Token Economy” A system that uses tokens, which can represent value or assets, to facilitate transactions and interactions within a digital ecosystem.

“Cryptocurrency” Digital or virtual currencies that use cryptography for security, which may be accepted as a form of payment by some government agencies.

“Blockchain Technology” A distributed ledger technology that can be used to enhance the security and transparency of government e-payment systems by recording transactions in a tamper-resistant manner.

“Cross-Border Payments” Payments that involve transactions between individuals, businesses, or government entities in different countries, often subject to international regulations and standards.

“Fintech” (Financial Technology) Innovative technologies and startups that provide financial services, including payment solutions, which government agencies may partner with or regulate.

“Real-Time Payments” Payment processing systems that enable transactions to be completed instantly or within a few seconds, enhancing the speed and efficiency of government e-payment services.

“Direct Debit” A payment method that allows government agencies to withdraw funds directly from a user's bank account on a recurring basis, often used for taxes and bills.

“Payment Card Industry (PCI) Compliance” Compliance with the security standards and requirements set forth by the Payment Card Industry Security Standards Council to protect payment card data.

“Data Privacy” The protection of personal and financial data collected during e-payment transactions, ensuring that user information is handled securely and in compliance with privacy regulations.

“Electronic Invoicing” (e-Invoicing) The electronic generation, delivery, and processing of invoices, often integrated with e-payment systems for government procurement and vendor payments.

“KYC” (Know Your Customer) and “AML” (Anti-Money Laundering) Regulations and processes that require government agencies to verify the identity of customers and monitor transactions to prevent money laundering and fraud.

“Multi-Channel Payment” Offering various payment methods and channels (e.g., online, mobile, in-person) to accommodate user preferences and accessibility.

“Disbursement” The process of making payments or transferring funds from a government agency to individuals, businesses, or other government entities, often used for benefits, subsidies, and grants.

Payment Notification: Alerts and notifications sent to users to confirm successful payments, provide receipts, or inform them of payment-related updates.

6. Objectives of Standards and Guidelines

The objectives of these standards and guidelines are to;

a) Promote interoperability among government electronic payment service providers, financial institutions, and payment networks.
b) Enhance security measures and prevent fraud in government electronic payment transactions.
c) Standardize processes, formats, and protocols for government electronic payments.
d) Safeguard customer data and foster consumer confidence in digital transactions.
e) Support the growth and development of PNG's digital economy.
f) Ensure compliance with relevant regulations and legal frameworks.
g) Facilitate seamless and convenient government electronic transactions for consumers and businesses.
h) Encourage innovation and adoption of emerging technologies in government electronic payment systems.
i) Streamline payment processes and improve efficiency in settlement and reconciliation.
j) Enhance consumer protection and provide transparent dispute resolution mechanisms.

7. Scope and Application

(1)The instrument will guide the development and implementation of the government electronic payment.

(2) The instrument will promote interoperability within the government electronic payment ecosystem.

(3) This instrument shall be applicable to the following

- All public bodies
- Other Stakeholders engaging with PNG Government

8. Governance and Regulatory Framework

(1) The governance structure and regulatory framework for electronic-payment services play a crucial role in ensuring the integrity, security, and efficiency of government electronic payment transactions.

(2) Following are the governance and regulatory aspects in PNG:

a) **Central Bank of Papua New Guinea (BPNG)**

- As the primary regulatory authority, BPNG plays a key role in overseeing and regulating electronic payment services in PNG.

- BPNG formulates policies, issues guidelines, and grants licenses to financial institutions and non-bank payment service providers operating in the country.

b) **Laws and Regulations**

- These laws provide a legal framework for government electronic payments, protect consumer rights, and ensure compliance with international standards and best practices.

- These laws, policies, regulations, and standards are but not limited to the Central Banking Act, the Financial Institutions Act, and the Electronic Transactions Act, among others.

c) **E-Payment System Oversight**

- Bank of Papua New Guinea is the authority to oversight of the government payment system in the country to maintain its safety and efficiency.

- It monitors and supervises payment system operators, ensuring compliance with regulations, risk management practices, and data protection requirements.

- Bank of Papua New Guinea may also establish guidelines for the operation and security of government payment systems.

d) **Licensing and Authorization**

- Entities in the government electronic payment services ecosystem are required to obtain licenses and authorizations from Bank of Papua New Guinea.

- Only licensed and compliant organizations must operate within the government electronic payment ecosystem.

- Licensing and vetting criteria include;
    i. capital requirements,
    ii. security measures,
    iii. governance frameworks, and
    iv. compliance with anti-money laundering and counter-terrorism financing regulations.

e) **Consumer Protection**

- Consumer protection covers issues such as but is not limited to;
    i. transaction transparency
    ii. liability limits for unauthorized transactions,
    iii. dispute resolution mechanisms, and
    iv. the provision of clear terms and conditions to consumers.

f) **Compliance and Reporting**

- Financial institutions and payment service providers are required to comply with regulatory requirements and report to Bank of Papua New Guinea regularly.

- This includes but is not limited to;
    i. financial statements,
    ii. transaction data,
    iii. and other relevant information

g) **International Standards**

- The government **is** aligning its governance and regulatory framework for electronic payment services with international standards and best practices. Organization for Standardization (ISO), the International Electro technical Commission (IEC), and other relevant global bodies.

- Aligning with international standards promotes interoperability, security, and compliance with global best practices.

Part II. - Government E-Payment Standards and Specifications

9. Overview

(1) This Part prescribes the standards and technical specifications that establish a framework for electronic payment services for the government.

(2) These standards promote interoperability, security, and efficiency in the government electronic payment ecosystem while ensuring the protection of customer data and fostering consumer confidence in digital transactions.

(3) The objectives of these standards and specifications are to;

a) provide a comprehensive framework that enables the development, implementation, and operation of government electronic payment solutions.

b) enhance the reliability, security, and convenience of government electronic payments.

c) promote growth and development of the country's digital economy.

Standard 1 Payment Infrastructure

(1) The technical infrastructure required to support government electronic payments consists of various components;

a) Hardware

- The hardware components of the e-payment infrastructure include;
  i. point-of-sale (POS) terminals,
  ii. card readers,
  iii. mobile devices, and;
  iv. secure servers.

- These devices enable the capture and processing of payment data, ensuring the secure transmission of information between the merchant and the payment service provider.

b) Software

- Software plays a critical role in enabling e-payment transactions.

- This includes;
  i. payment processing software
  ii. encryption software for securing data,
  iii. mobile payment applications, and
  iv. backend systems for transaction management, authorization, and settlement.

c) Networks

- The payment infrastructure relies on robust and secure networks to facilitate the transmission of payment data between various stakeholders.

- This includes;
  i. the internet,
  ii. mobile networks, and;
  iii. secure private networks.

- The networks must provide reliable connectivity, ensuring that transactions can be securely transmitted in real-time, regardless of the location of the parties involved.

d) Protocols

- Standardized protocols are necessary for ensuring interoperability and compatibility between different e-payment service providers and systems.

- Common protocols used may include;
    i. ISO 8583 for card-based transactions
    ii. EMV (Europay, Mastercard, and Visa) for secure chip-based payments, and;
    iii. secure network protocols such as SSL/TLS for secure data transmission over the internet.

Standard 2 Interoperability and Compatibility Considerations

(1) Interoperability and compatibility must be considered in the government e-payment infrastructure to ensure seamless and secure transactions.

(2) The following are important and include;

a) Standardization

- Adopting industry-standard formats, protocols, and message structures promotes interoperability.

- Compliance with global payment standards allows different stakeholders, including banks, payment service providers, and merchants, to connect and transact seamlessly.

b) Card and Payment Scheme Compatibility

- Ensure payment cards and schemes are compatible with widely accepted international payment networks, such as but not limited to;
    i. Visa,
    ii. MasterCard, and;
    iii. Union Pay

c) Mobile Payment Integration

- Facilitate interoperability between mobile payment systems and traditional card-based systems is crucial.

- This enables users to seamlessly switch between different payment modes, such as but not limited to;
    i. mobile wallets and;
    ii. card payments.

d) Integration with Existing Systems

- Ensure compatibility and integration with existing financial systems and infrastructure, such as but not limited to;
    i. core banking systems and
    ii. merchant management systems

e) Security Standards

- Implementing robust security measures and encryption standards throughout the payment infrastructure ensures;
    i. secure transmission
    ii. storage of sensitive payment data and
    iii. protection against fraud and unauthorized access.

f) Regulatory Compliance

- Aligning with regulatory requirements and compliance standards, includes but not limited to;
    i. data protection regulations, and;
    ii. anti-money laundering measures.

- Fostering of interoperability by establishing a common framework for security and compliance.

Standard 3 E-Payment Services

(1) The table below list different e-payment services that must be use and include;

E-Service	Description
Mobile Wallets	• Mobile wallet services allow users to; i. store payment information, ii. make payments, and; iii. transfer funds. • Transactions are done using mobile devices.
Card Payments	• Card-based payment services include; i. debit cards, ii. credit cards, and; iii. prepaid cards • This service enables users to make payments at physical stores, online merchants, or through card-not-present transactions.
Online Payment Gateways	• Online payment gateways facilitate secure transactions for e-commerce businesses by connecting merchant websites or online platforms with financial institutions.
Bank Transfers	• Bank transfers involve the electronic transfer of funds between bank accounts.

	• This service enables individuals and businesses to initiate payments directly from their bank accounts.
Peer-to-Peer(P2P) Payments	• P2P payment services enable individuals to send money directly to other individuals. • This can be done by either using mobile apps or online platforms.
Contactless Payments	• Contactless payment methods include, i. near-field communication (NFC), and/or; ii. QR code payments. • This service allows users to make payments by tapping their cards or scanning codes on compatible terminals.
Online Banking	• Online banking services provide users with access to their bank accounts and allow them to perform various financial transactions, including fund transfers, bill payments, and account management.
In-App Payments	• In-app payments allow users to make purchases or payments within mobile applications, eliminating the need to navigate to external payment platforms.
Prepaid Cards	• Prepaid cards are loaded with a specific amount and can be used for payments at participating merchants or online platforms.
Digital Currencies	• Digital currencies are decentralized digital assets that can be used for online transactions and peer-to-peer transfers. • Digital currencies may include; i. Bitcoin ii. Ethereum
Bill Payment Services	• Bill payment services allow users to conveniently pay their utility bills, such as electricity, water, or telecommunications, through electronic channels.
Electronic Funds Transfer (EFT)	• Electronic funds transfer services enable the transfer of funds from one bank account to another electronically.

Mobile Banking	• Mobile banking services provide users with access to their bank accounts, allowing them to perform banking transactions using mobile devices.
Virtual Payment Cards	• Virtual payment cards generate temporary card details or virtual accounts for secure online transactions, offering an additional layer of security.
Cryptocurrency Wallets	• Cryptocurrency wallets store digital currencies securely and enable users to send, receive, and manage their cryptocurrency holdings.
Automatic Clearing House (ACH) Payments:	• ACH payment systems facilitate batch-based electronic fund transfers between bank accounts, commonly used for recurring payments or direct deposits.
Contactless Wearable Payments:	• Contactless payment technology integrated into wearable devices, such as smartwatches or wristbands, allows users to make payments conveniently.
Subscription Billing	• Subscription billing services automate recurring payments for subscription-based products or services, ensuring regular and hassle-free transactions.

Standard 4 Security and Fraud Prevention

(1) The objective of security and fraud prevention in e-payment systems is to;

a) establish robust security measures and
b) effectively safeguard e-payment transactions through risk management practices.

(2) Priority of the security is to; build trust and confidence among consumers, merchants, and financial institutions utilizing e-payment systems.

(3) Following are some key considerations and measures to achieve this objectives:

a) **Encryption and Secure Communication**

- Implement strong encryption protocols to protect sensitive payment data during transmission.

- Secure communication channels, such as but not limited to;
  i. Secure Sockets Layer (SSL), or;
  ii. Transport Layer Security (TLS)

b) **Tokenization**

- Utilize tokenization techniques to replace sensitive cardholder data with unique tokens.

- This practice helps prevent the exposure of actual payment information, reducing the risk of data breaches and unauthorized access to cardholder data.

c) **Two-Factor Authentication (2FA**)

- Implement two-factor authentication methods to add an extra layer of security.

- This typically involves combining something the user knows (e.g., password) with something the user possesses (e.g., mobile device or biometric authentication) to verify their identity.

d) **Fraud Detection and Prevention**

- Employ advanced fraud detection and prevention systems that leverage machine learning algorithms and data analytics to identify suspicious activities and patterns in real-time.

- These systems can help detect and prevent fraudulent transactions, account takeovers, and other malicious activities.

e) **Strong Access Controls**

- Implement robust access control measures to ensure that only authorized individuals have access to sensitive systems and data.

- This includes employing strong passwords, user authentication mechanisms, and role-based access controls.

f) **Regular Security Assessments**

- Conduct regular security assessments, vulnerability scans, and penetration testing to identify and address potential weaknesses in the e-payment infrastructure.

- Regular assessments help ensure that security measures remain up to date and effective against evolving threats.

g) **Security Awareness and Training**

- Provide regular security awareness and training programs for employees, merchants, and consumers to educate them about best security practices, phishing scams, and other potential threats.

- This promotes a culture of security and helps users make informed decisions to protect themselves and their sensitive information.

h) **Compliance with Industry Standards**

- Adhere to industry security standards and regulations, such as but not limited to;
    i. the Payment Card Industry Data Security Standard (PCI DSS) and
    ii. other relevant frameworks.

- Compliance with these standards helps ensure the implementation of appropriate security controls and practices across the e-payment ecosystem.

i) **Incident Response and Recovery**

- Establish an effective incident response plan.

- In the event of a security incident or data breach the following steps are to be taken;

    i. prompt incident detection,
    ii. investigation, and
    iii. recovery procedures

j) **Ongoing Monitoring and Updates**

- Continuously monitor the e-payment systems, networks, and applications for potential security vulnerabilities or emerging threats.

- Regularly update software and systems with the latest security patches and ensure that security measures keep pace with the evolving threat landscape.

Standard 5 Message Formats

(1) The goal of standardized message formats in e-payment systems is to create uniform and organized payment message forms.

(2) This goal provides data structure, content, and validation consistency, hence facilitating the sharing of payment information across parties participating in the transaction lifecycle.

(3) This goal seeks to improve speed, accuracy, and interoperability within the payment ecosystem by adopting standardized communication formats.

(4) Following are some of the major concerns and advantages of standardized messaging formats:

a) Consistency and Structure

- Standardized message formats provide a common structure for payment messages, ensuring that data elements are consistently organized and represented.

- This consistency simplifies data interpretation and processing by both senders and receivers, reducing errors and improving overall data quality.

b) Data Content and Validation

- Standardized formats define the specific data fields and their content within payment messages.

- This ensures that essential information, such as transaction amounts, payment references, and participant identifiers, is consistently included and properly validated.

- Validating the data against predefined rules helps identify potential errors or inconsistencies early in the payment processing cycle.

c) Interoperability

- Standardized message formats facilitate interoperability between different systems, platforms, and participants involved in the payment ecosystem.

- By adhering to common formats, payment service providers, banks, payment networks, and other stakeholders can seamlessly exchange payment messages, irrespective of their underlying technical infrastructure or internal data structures.

d) Straight-Through Processing (STP)

- Standardized message formats enable straight-through processing, where payment messages can be automatically processed without manual intervention.

- STP reduces manual errors, enhances operational efficiency, and accelerates transaction processing and settlement timeframes.

e) Integration and Scalability

- Standardized message formats facilitate integration and scalability by providing a common language for systems to communicate.

- This allows for easier integration of new participants, such as merchants, payment gateways, or mobile wallets, into the existing payment ecosystem without significant modifications to the underlying infrastructure.

f) Compliance and Regulatory Reporting

- Standardized formats assist in meeting regulatory requirements and reporting obligations.

- By capturing and structuring data in a standardized manner, financial institutions and payment service providers can easily generate reports and respond to regulatory inquiries, audits, and compliance reviews.

g) Futureproofing

- Standardized message formats can accommodate future enhancements or changes in the payment landscape.

- They provide a foundation for incorporating new payment types, emerging technologies, and evolving regulatory requirements while maintaining backward compatibility with existing systems.

h) Industry Collaboration and Harmonization

- Standardized message formats are often developed through collaboration among industry stakeholders, such as payment networks, standardization bodies, and technology providers.

- This collaboration promotes harmonization, aligning industry practices, and driving widespread adoption of common standards.

Standard 6 Consumer Protection

(1) The objectives of consumer protection are to;

a) safeguard consumers' interests,
b) address concerns related to fraud,
c) unauthorized transactions,
d) billing discrepancies, and
e) foster trust and confidence in e-payment services.

(2) Following are some key considerations and measures to achieve consumer protection, and include;

a) Liability Limitations

- Establish guidelines and policies that clearly define the liability of consumers in case of unauthorized transactions or fraudulent activities.

- These limitations should provide reasonable protection to consumers and encourage responsible behavior, while also ensuring that consumers are not unduly burdened with liabilities arising from unauthorized or fraudulent transactions.

b) Dispute Resolution Mechanisms

- Implement effective and accessible dispute resolution mechanisms for consumers to address complaints and disputes related to e-payment transactions.

- This can include establishing dedicated customer support channels, mediation services, or an ombudsman scheme to provide impartial resolution of consumer issues in a timely manner.

c) Transparency Requirements

- Ensure that consumers have access to clear and comprehensive information regarding the terms and conditions, fees, charges, and other relevant details associated with e-payment services.

- Ensure transparency in pricing, exchange rates, transaction limits, and any additional fees or charges, for consumers to make informed decisions and understand the costs and risks involved.

d) Fraud Prevention Education

- Conduct consumer awareness campaigns and educational programs to raise awareness about fraud prevention, safe online practices, and the importance of protecting personal and financial information.

- Educate consumers about common fraud schemes, phishing attacks, and how to recognize and report suspicious activities to prevent fraud.

e) Privacy and Data Protection

- Establish regulations and guidelines that protect the privacy and security of consumer data.

- Ensure that personal and financial information collected during e-payment transactions is handled securely, stored appropriately, and only used for authorized purposes.

f) Transparent Terms and Conditions

- E-payment service providers must provide consumers with clear and understandable terms and conditions.

- Ensure that consumers have access to this information to promote transparency and enable them informed decision-making.

g) **Anti-Money Laundering and Counter-Terrorism Financing Measures**

- Implement measures to prevent e-payment systems from being misused for illicit activities such as money laundering and or terrorism financing.

- Ensure compliance with relevant anti-money laundering and counter-terrorism financing regulations and

- Ensure that Know Your Customer (KYC) requirements are in place to protect consumers and maintain the integrity of the financial system.

h) Monitoring and Enforcement

- Ensure regular monitoring, compliance assessments, and enforcement mechanisms according to consumer protection guidelines.

- Ensure audits, inspections, and investigations are conducted to identify non-compliance and take appropriate actions to protect consumer rights.

Standard 7 Cross-Border and Interoperability Considerations

(1) Requirements for smooth and efficient transactions are;

a) Currency Conversion

- Cross-border e-payments often involve transactions in different currencies.
- It is essential to have mechanisms in place to facilitate accurate and transparent currency conversion.
- This includes providing real-time exchange rates, ensuring fair conversion rates, and minimizing additional fees or charges associated with currency conversion.

b) Exchange Rate Calculations

- E-payment systems must be capable of performing accurate exchange rate calculations at the time of transaction initiation or settlement.
- Reliable and up-to-date exchange rate data must be sourced from reputable financial institutions or currency exchange providers.
- Ensure consistency and accuracy in exchange rate calculations.

c) Compatibility with International Payment Standards

- Ensure Interoperability with international payment standards for seamless cross-border e-payments.
- Ensure standards, such as ISO 20022 for payment messaging.
- Ensure exchange of payment information, for transparency, and streamlines reconciliation processes.

d) Regulatory Compliance

- Ensure cross-border e-payments involve compliance with both domestic and international regulations.
- Ensure anti-money laundering (AML) and counter-terrorism financing (CTF) measures, sanctions screening, and compliance with relevant cross-border payment regulations.
- Ensure compliance with regulatory requirements to mitigate risks, prevent fraudulent activities, and maintain the integrity of cross-border e-payment transactions.

e) Interconnectivity with Payment Networks

- Ensure interoperability between domestic and international payment networks for cross-border e-payments.

- Establish secure and reliable connections between different payment networks, such as;
    i. card networks (Visa, Mastercard),
    ii. mobile payment networks (Apple Pay, Google Pay), and
    iii. international fund transfers networks (SWIFT).

- Ensure Interconnectivity for seamless routing and settlement of cross-border transactions, for efficient and timely processing.

f) Transparent Fee Structures

- Ensure clear and transparent fee structures must have established for cross-border e-payments.

- Ensure Consumers and businesses must have access to information regarding any additional fees or charges associated with cross-border transactions, such as;
    i. foreign transaction fees,
    ii. currency conversion fees and or
    iii. intermediary bank fees.

- Ensure Transparent fee structures are readily available to promote trust and enable users to make informed decisions regarding cross-border e-payments.

g) Fraud Prevention and Security

- Cross-border e-payments may face increased risks associated with fraud and cybersecurity threats.

- Implement robust fraud prevention measures to mitigate risk, such as;
    i. transaction monitoring,
    ii. risk scoring, and;
    iii. authentication protocols.

- Ensure the security of cross-border e-payment systems through;
    i. encryption,
    ii. secure data transmission, and
    iii. compliance with industry security standards

Standard 8 Compliance and Regulatory Alignment

(1) The aim of compliance and regulatory alignment in the e-payment ecosystem in Papua New Guinea (PNG) is to ensure adherence to relevant laws, regulations, and industry best practices.

(2) Following are considerations for establishing secure and compliant environment for e-payment services;

a) Regulatory Framework

- Ensure to develop and enforce a robust regulatory framework that encompasses government e-payment services.

- Regulatory framework must address;
    i. consumer protection,
    ii. privacy and data protection,
    iii. anti-money laundering (AML),
    iv. counter-terrorism financing (CTF), and
    v. fraud prevention.

- Ensure Regulatory framework is within the legal and regulatory boundaries of PNG.

b) Legal Compliance

- Ensure compliance with applicable laws and regulations specific to the e-payment industry in PNG.

- Ensure compliance with legislation related to;
    i. electronic transactions,
    ii. data protection,
    iii. financial services, and
    iv. relevant sector-specific regulations.

- All e-payment service providers must familiarize themselves with these laws and maintain ongoing compliance.

c) Industry Best Practices

- Adopt and adhere to industry best practices that are relevant to the e-payment landscape in PNG.

- Stay informed about emerging trends, technologies, and global standards in the e-payment industry and implement practices that promote security, transparency, and efficiency.

- Collaborate with relevant industry associations, standardization bodies, and regulatory authorities to identify and adopt best practices.

d) Regulatory Reporting and Compliance Monitoring

- Establish mechanisms for regulatory reporting and compliance monitoring to ensure ongoing adherence to regulations.

- Ensure regular reporting of key metrics, financial information, transaction data, and compliance-related activities to regulatory authorities as required.

- Implement internal controls and audits to assess and monitor compliance with regulatory requirements.

e) Collaboration with Regulatory Authorities

- Foster collaboration and open lines of communication with relevant regulatory authorities in PNG.

- Engage in constructive dialogue to understand regulatory expectations, seek clarifications, and contribute to the growth and stability of the e-payment industry.

- Collaborate to ensure shared understanding of regulatory objectives for compliance with requirements.

f) Consumer Education

- Promote consumer education and awareness programs to inform and educate users about their rights, responsibilities, and protections in the e-payment ecosystem.

- Educate consumers about safe online practices, fraud prevention, dispute resolution mechanisms, and their rights under consumer protection laws.

- Empower and inform consumers for effective compliance.

g) Regulatory Compliance Training

- Provide training and awareness programs for e-payment service providers, employees, and stakeholders to ensure a clear understanding of regulatory requirements and compliance obligations.

- Training programs must cover topics such as;
    i. anti-money laundering (AML) ,
    ii. CTF,
    iii. fraud prevention,
    iv. privacy, and
    v. data protection.

Standard 9 Innovation and Emerging Technologies

(1) The objective of fostering innovation and integrating emerging technologies in e-payment systems in Papua New Guinea (PNG) is to encourage the adoption of new advancements.

(2) Emerging technologies may include;

a) Regulatory Sandbox

- Establish a regulatory sandbox framework that allows e-payment service providers to experiment with emerging technologies in a controlled environment.

- The sandbox provides a space for testing and refining innovative solutions while ensuring compliance with relevant regulations and consumer protection requirements.

- It encourages collaboration between regulators, industry players, and technology innovators to foster a conducive environment for innovation.

b) **Block chain Technology**

- Explore the potential applications of blockchain technology in e-payment systems.
- Blockchain offers advantages such as enhanced security, transparency, and decentralized record-keeping.
- Assess its feasibility in areas like transaction settlement, identity verification, and supply chain finance.
- Develop guidelines and standards for blockchain implementation, ensuring compliance with existing regulations.

c) Artificial Intelligence (AI)

- Promote the responsible and ethical use of AI in e-payment systems.
- AI can be utilized for fraud detection, risk assessment, customer service automation, and personalized user experiences.
- Establish guidelines for data privacy, security, and algorithmic transparency.
- Encourage collaboration between academia, industry, and regulators to drive AI research, development, and innovation.

d) Biometrics

- Explore the integration of biometric authentication methods, such as fingerprints, facial recognition, or iris scans, in e-payment systems.
- Biometrics offer enhanced security and convenience for users.
- Establish guidelines for data protection and storage, user consent, and biometric authentication standards.
- Ensure compliance with privacy laws and educate consumers about the benefits and safeguards associated with biometric technology.

e) Interoperability and Standardization

- Ensure that emerging technologies adopted in e-payment systems align with existing standards and promote interoperability.
- Develop protocols and frameworks that facilitate seamless integration between different e-payment platforms and emerging technologies.
- Collaboration with international standardization bodies can help ensure compatibility with global best practices and foster interoperability with cross-border payment systems.

f) Collaboration and Knowledge Sharing

- Encourage collaboration and knowledge sharing among stakeholders, including financial institutions, technology providers, regulators, and academic institutions.
- Foster partnerships that drive research, development, and innovation in e-payment systems.
- Establish platforms for sharing experiences, best practices, and success stories related to the adoption of emerging technologies.

g) Cybersecurity and Risk Management

- Address the cybersecurity and risk management considerations associated with emerging technologies.
- Enhance security measures to protect against potential vulnerabilities and cyber threats.
- Develop frameworks for risk assessment, mitigation, and incident response.
- Collaboration with cybersecurity experts and conducting regular security audits can help ensure the resilience and reliability of e-payment systems.

Standard 10 Efficiency and Cost Effectiveness

(1)The objective of promoting efficiency and cost-effectiveness in e-payment processes is to optimize transactional efficiency, reduce costs, streamline operations, and improve settlement times.

(2) This includes;

a) Streamlined Transaction Processes

- Simplify and streamline the e-payment transaction processes to minimize unnecessary steps and reduce complexity.
- This includes optimizing user interfaces, eliminating redundant data entry, and automating manual processes where possible.
- By enhancing the efficiency of transaction flows, e-payment systems can provide faster and more convenient payment experiences for users.

b) Real-Time Processing

- Enable real-time processing of e-payment transactions to reduce delays in payment initiation, authorization, and settlement.

- Real-time processing ensures that funds are transferred promptly, providing faster access to funds for merchants and improved liquidity management for businesses.

- This reduces the time and effort required for reconciliation and financial reporting.

c) Interoperability and Integration

- Foster interoperability and seamless integration between different e-payment platforms, financial institutions, and payment networks.

- This allows for easy and efficient transfer of funds across various systems, reducing transaction costs and simplifying the payment experience for users.

- Integration with other financial systems, such as accounting software and enterprise resource planning (ERP) systems, can further streamline operations and improve efficiency.

d) Cost Optimization

- Implement strategies to optimize costs associated with e-payment processes.
- This includes evaluating transaction fees, pricing structures, and interchange fees to ensure they are competitive and transparent.

- Explore opportunities to leverage economies of scale and negotiate favorable agreements with payment service providers and financial institutions.

- Efficient cost management contributes to the overall affordability and cost-effectiveness of e-payment solutions.

e) Automated Reconciliation

- Implement automated reconciliation processes to streamline the matching and verification of transaction data, reducing manual effort and errors.

- Automated reconciliation ensures accurate and timely settlement of transactions, improves transparency, and minimizes discrepancies between payment records.

- This contributes to operational efficiency and cost savings for businesses and financial institutions.

f) Scalability and Flexibility

- Build e-payment systems that can scale and adapt to changing transaction volumes and user demands.

- Scalable infrastructure and flexible architecture allow for efficient processing of high transaction volumes during peak periods without sacrificing performance or incurring additional costs.

- This ensures that e-payment systems can handle growth and accommodate future advancements in the payment industry.

g) Data Analytics and Insights

- Leverage data analytics and business intelligence tools to gain insights into e-payment processes, transaction patterns, and customer behaviors.

- By analyzing transaction data, businesses and financial institutions can identify areas for process optimization, fraud detection, and personalized customer experiences.

- Data-driven insights contribute to informed decision-making and the continuous improvement of efficiency in e-payment systems.

Standard 11 Integration with Existing Systems

(1) In the framework of Papua New Guinea's arising e-payment environment, simple integration with current systems can provide several benefits while also improving the entire effectiveness and efficacy of e-payment services.

(2) This includes;

a) **Integration with Accounting Software**

- Ensure integrating e-payment systems with popular accounting software used in PNG, such as but not limited to;
    i. QuickBooks or
    ii. MYOB and
    iii. Others, which are recommended by the Government.

b) **Integration with E-commerce Platforms**

- Ensure integrating e-payment systems with local e-commerce platforms operating in PNG.

- Implement seamless integration for the purposes of online and electronic payments.

c) **Integration with Customer Relationship Management(CRM) Systems**

- CRM System allows for;
    i. seamless data sharing,
    ii. communication and;
    iii. functionality between the CRM system and other business tools

- Government organizations must ensure that CRM is utilize for payment and data management.

d) **Collaboration with Financial Institutions**

- Collaboration must happen between e-payment service providers and financial institutions operating in PNG.

- Ensure Seamless integration between e-payment systems for transactions.

e) **Government Systems Integration**

- Ensure e-payment systems with all relevant government systems in PNG.

- This integration could enable citizens to make electronic payments for government services, such as;
  i. taxes,
  ii. licenses, and;
  iii. or fines.

f) **Integration with Mobile Network Operators**

- E-payment service providers must collaborate with relevant mobile network operators (MNOs) in PNG to enable integration.

g) **Seamless Payment Collection for Small Businesses:**

- Government systems must integrate to enable E payment systems with MSMEs in the country.

- Integration will allow MSMEs to collect payments electronically, reduce reliance on cash transactions and offer convenience to customers.

h) I**nteroperability with Payment Switches:**

- Ensure secure interoperability between the payment switches, both local and international.

- Seamless integration with payment switches allows for interoperable transactions between different banks, financial institutions, and e-payment service providers, ensuring smooth and efficient payment processing across the country.

Standard 12 Government Systems

(1) Government organizations must enable integration of e-payment systems with government systems in PNG to facilitate electronic payments for government services, such as;

A) taxes,
B) licenses,
C) fines and
D) other service payment

(2) This includes;

a) Efficiency Enhancement

- Streamline government service delivery by eliminating manual payment processing.
- Reduce paperwork, manual errors, and processing delays associated with traditional payment methods.
- Enable faster and more efficient service delivery.

b) Citizen Convenience

- Offer citizens the convenience of making electronic payments from anywhere, using various devices.
- Eliminate the need for in-person visits to government offices or reliance on cash and cheques.
- Enhance citizen experience by providing a modern and convenient payment option.

c) Transparency and Accountability

- Promote transparency in financial transactions by providing real-time tracking and documentation.
- Enable citizens and the government to have clear records of payments made.
- Enhance accountability and reduce the potential for fraud or misappropriation.

d) Revenue Collection Efficiency

- Automate payment processing and tracking for government revenue collection, such as taxes and fines.
- Enable accurate and timely updates of payment status, facilitating faster revenue reconciliation.
- Improve efficiency and accuracy in revenue collection processes.

e) Cost Reduction

- Reduce costs associated with manual payment handling, including infrastructure, paperwork, and processing.
- Optimize resource allocation and redirect savings towards other priority areas.
- Enhance cost-effectiveness of government operations.

f) Compliance Enforcement

- Establish an auditable trail of transactions, ensuring citizens meet their financial obligations.
- Reduce tax evasion and non-compliance through improved tracking and documentation.
- Strengthen compliance efforts and promote financial responsibility.

g) Economic Stimulus

- Contribute to economic growth by offering an efficient payment experience for businesses and individuals.
- Enable organizations to focus more on core activities, increasing productivity.
- Support the development of a digital economy in the country.

h) Digital Transformation

- Align with the broader Government digital transformation agenda in the country.
- Promote the adoption of digital technologies and improve digital literacy.
- Advocate and drive progress towards a modern and digitally enabled public services.

PART III. – MISCELLANEOUS

10. Implementation Schedule

The Government E-payment Standard 2023 is effective from [01.01.2025]

11. Compliance and Monitoring

The Department of Information and Communications Technology may conduct an assessment and evaluation report of the compliance of public bodies with this instrument.

12. Supplemental Standards and Guidelines

The Department of Information and Communications Technology may issue supplemental standards and guidelines to support this instrument as and when required.

APPENDIX