

**BANK OF TANZANIA**



# **Electronic Payment Schemes Guidelines**

---

© Bank of Tanzania May 2007

Bank of Tanzania,  
10 Mirambo Street,  
Dar es Salaam.  
Tanzania.

Attn. Director, National Payment System Directorate

Tel: +255 22 2127470

Fax: +255 22 2138370

Email: dnps@hq.bot-tz.org

© **Bank of Tanzania, May 2007**

Reproduction of all or any parts of this publication is permitted on condition that it is for non-profit making purposes and an acknowledgment of this work is duly made in the reproduction.

## Table of Contents

Table of Contents .....	3
PART I .....	4
PRELIMINARY .....	4
PART II .....	5
GENERAL .....	5
4.0 Introduction .....	5
5.0 Purpose .....	5
6.0 Bank's Oversight Function .....	6
7.0 Compliance .....	6
PART III .....	6
LAUNCHING ELECTRONIC PAYMENT SCHEMES .....	6
8.0 Approval .....	6
9.0 Minimum Requirements .....	7
PART IV .....	9
RISK MANAGEMENT GUIDELINES .....	9
10.0 Risks Management Guidelines .....	9
11.0 Risks Category and Management Guidelines .....	9
11.1 Institutional Management Issues .....	9
11.1.1 General Guidelines for Institutional Management Issues .....	9
11.2 Managing Security Risk .....	10
11.2.1 General Guidelines for Managing Security Risk .....	10
11.3 Managing Legal and Reputational Risk Management .....	12
11.3.1 General Guidelines for Managing Legal and Reputational Risk .....	12
Annex I .....	13
MINIMUM STANDARDS REQUIREMENTS .....	13
1. Relevant ISO and de facto Standards .....	13
2. Minimum Standards for Other Electronic Schemes .....	14
REFERENCES .....	15

**PART I**  
**PRELIMINARY**

1.0 These Guidelines may be cited as the Electronic Payment Scheme Guidelines, 2007.

2.0 These Guidelines shall apply to all banks and financial institutions and to any other service providing institution or company that offers direct or indirect electronic payment schemes services.

3.0 In these Guidelines unless the context otherwise requires-

“the Act” means the Bank of Tanzania Act, 2006;

“authentication” means the techniques, procedures and processes used to verify the identity and authorisation of prospective and established customers.

“authorisation” means the procedures, techniques and processes used to determine that a customer or an employee has legitimate access to the bank or financial institution account or the authority to conduct associated transactions on that account.

“Bank” means the Bank of Tanzania;

“bank” has the meaning ascribed to it in the Act;

“Bank’s oversight function” means the function principally intended to promote smooth functioning of payment systems including electronic payment schemes by monitoring and assessing risks associated with such systems and adducing effective risk management measures;

“confidentiality” means the assurance that key information remains private to the bank or financial institution and is not viewed or used by those unauthorised to do so.

“data integrity” means the assurance that information that is in-transit or in storage is not altered without authorisation.

“electronic payment schemes” means any electronic instrument, device or system used for the purposes of facilitating payment transfers, through internet and/or wireless communication networks, and by use of service delivery products such as electronic cards, electronic payment transfers systems, mobile banking, internet banking, automated teller machines, point of sales terminals, payment switches and any other type of electronic payment transfer system.

“financial institution” has the meaning ascribed to it in the Act;

“identification” means the procedures, techniques and processes used to establish the identity of a customer when opening an account.

“interoperability” means a situation in which payment instruments belonging to a given electronic payment scheme may be used in another electronic payment scheme installed by another bank or financial institution;

“non-repudiation” involves creating proof of the origin or delivery of electronic information to protect the sender against false denial by the recipient that the data has been received, or to protect the recipient against false denial by the sender that the data has been sent.

“segregation of duties” is a basic internal control measure designed to reduce the risk of fraud in operational processes and systems and ensure that transactions and bank’s or financial institution’s assets are properly authorised, recorded and safeguarded.

## **PART II GENERAL**

### **4.0 Introduction**

- 4.1 These Guidelines (the Guidelines) have been issued by the Bank in exercise of powers conferred to it by section 6 of the Act, which empowers the Bank to regulate, monitor and supervise the payment, clearing and settlement system including all products and services thereof issued by any bank or financial institution, service provider or company.
- 4.2 The Bank has the duty to promote safety and efficiency in the national payment system and ensure that high standards are maintained in the conduct and management of risks in operations of the electronic payment schemes. The Bank also intends the market to use standardised products, with a coherent framework that ensure resilient features for business continuity.
- 4.3 All banks and financial institutions and non-banking institutions (service providers and companies) intending to introduce or have introduced electronic payment schemes are expected to adhere to these Guidelines.

### **5.0 Purpose**

- 5.1 These Guidelines intended to provide guidance to banks and financial Institutions on recommended principles and sound practices for managing risks in their introduction and operations of electronic payment schemes.

- 5.2 The Bank encourages and recommends all financial institutions to familiarize with the principles and recommendations for electronic banking schemes set forth in the Basel Committee on Banking Supervision's papers - "*Risk Management Principles for Electronic Banking*" (<http://www.bis.org/publ/bcbs98.htm>) and the "Management and Supervision of Cross-Border Electronic Banking Activities" (<http://www.bis.org/publ/bcbs99.htm>).
- 5.3 Note that these Guidelines do not provide all-exclusive or exhaustive principles for risk management in the introduction and operations of electronic payment schemes. Banks and financial institutions are required to adhere to other prudential and best banking principles in risk management and they are required to implement such technologies that have risk management controls that are appropriate and up to date.

## **6.0 Bank's Oversight Function**

- 6.1 The Bank shall conduct oversight inspections and examinations on banks and financial institutions or service providers to assess the adequacy of risk management based on the requirements provided in these Guidelines.
- 6.2 Notwithstanding section 6.1 the Bank may implement other assessment processes to facilitate its ongoing oversight of electronic payment schemes.
- 6.3 Banks and financial institutions shall promptly report any suspected or confirmed cases of fraud relating to electronic payment schemes, major security breaches, any material service interruption or other significant issues and shall ensure to timely submit any other reports requested by the Bank related to the provision of electronic payment schemes services.

## **7.0 Compliance**

- 7.1 Banks and financial institutions or service providers are required to fully comply with these Guidelines, failure of which shall attract penalties and sanctions as shall be determined by the Bank.

### **PART III**

## **LAUNCHING ELECTRONIC PAYMENT SCHEMES**

## **8.0 Approval**

- 8.1 (1) Subject to section 8.2 and 8.3 any bank or financial institution is eligible to operate an electronic payment scheme provided it meets the minimum requirements stipulated in section 9.0.

(2) A non-banking financial institutions (service providers and companies) that intends to offer electronic payment schemes which has money transfer and or deposit taking element shall submit its application through a bank or a financial institution.

8.2 (1) Notwithstanding section 8.1, a bank or financial institution shall submit a written application to the Bank for introducing and operating an electronic payment scheme or for expanding the scope of its existing electronic payment scheme or in the case of subsection 8.1(2) operating an electronic payment scheme as an agent or partner of a non-bank financial institution.

(2)The applying bank or financial institution shall explain in detail how the bank or financial institution shall meet the minimum requirements stipulated in section 9.0.

8.3 The Bank shall evaluate the application and may grant or reject the application if it does not meet the minimum requirements set forth in section 9.0 or for any other reasons deemed appropriate by the Bank.

## **9.0 Minimum Requirements**

9.1 (1) These minimum requirements are to be observed by all banks and financial institutions in applying for and in operating an electronic payment scheme.

(2) Notwithstanding subsection (1) all banks and financial institutions shall be required to comply with the Risk Management Guidelines stipulated in Part IV herein.

9.2 The bank or financial institution warrants that-

- (i) the operation of the electronic payment scheme shall not change or affect it operations, licensee or mandate;
- (ii) it has carried out a risk analysis of the project that also details the risk management measures;
- (iii) the management has reviewed the existing risk profile of its operations and considered the impact of implementing the electronic payment scheme;
- (iv) the board has concluded that there are no undue adverse implications for the safety and soundness of the operations given its resources, risk management systems and technical expertise;
- (v) the there is a proper board and senior management oversight;

- (vi) major technology-related controls relevant to the electronic payment scheme have been addressed;
- (vii) there are appropriate security measures in place, both physical and logical together with other requisite risk management controls and a strategy has been developed and documented. The strategy has clearly outline the policies, practices and procedures that address and control all of the risks associated with electronic payment scheme and that it shall be updated periodically to be in tandem with technological changes ;
- (viii) issues relating to any outsourcing and or cross border electronic payment scheme activities have been addressed;
- (ix) it shall settle all its inter-bank payments arising from the electronic payment schemes through the Tanzania Inter-bank Settlement System operated by the Bank;
- (x) the electronic payment schemes shall be open systems capable of becoming interoperable with other payment system in the country and shall comply with the minimum international acceptable standards provided in **Annex I**;
- (xi) the electronic payment schemes shall provide an accurate and fully accessible audit trail of transactions from the origin of the payment instruction to its finality;
- (xii) the electronic payment scheme has the potential of providing services to a wider country outreach;
- (xiii) The participants to the electronic payment schemes are provided certainty of finality of their payments;
- (xiv) an enforceable legal framework for the provision of the services is available which covers all parties in the transaction, the legal framework shall be transparent and shall provide efficient dispute resolution mechanisms;
- (xv) the electronic payment schemes shall be available to its participants at all times, to achieve this various backup and business continuity arrangements and other legal arrangements to protect the users of the services of the scheme have been implemented;
- (xvi) the pricing policies take into account affordability of the services to a wider market reach;
- (xvii) the access criteria for participating in the electronic payment scheme is transparent;

- (xviii) a cost-benefit analysis has been conducted of the provision of the electronic payment scheme services; and
- (xix) it has consider legal developments (including compliance) and the business environment including external and internal threats to information security have been considered in the evaluation of the electronic payment scheme and compliance hereto shall be monitored on a continuous basis.

## **PART IV**

### **RISK MANAGEMENT GUIDELINES**

#### **10.0 Risks Management Guidelines**

10.1 The Bank expects that, in addition to the recommended risk management measures set forth herein, each bank and financial institution shall implement the relevant risk management controls that are commensurate with the risks associated with the electronic payment scheme adopted by the bank or financial institution.

10.2 These risk management Guidelines follow the principles laid down by the Basel Committee on Banking Supervision “*Risk Management Principles for Electronic Banking*”(BIS, May 2001), the Principles are herein grouped into main risk categories and specific guidelines are drawn on them.

10.3 These Guidelines do not contain specific detailed security requirements or intend to provide detail and exhaustive risk management guideline, rather, they provide general guide for banks and financial institutions to develop effective risk management measures commensurate to their electronic payment scheme business.

#### **11.0 Risks Category and Management Guidelines**

##### **11.1 Institutional Management Issues**

The board of directors and senior management (Institutional Management) of a bank or financial institution are responsible for developing the institution’s business strategy.

##### **11.1.1 General Guidelines for Institutional Management Issues**

The bank’s or financials institution’s management shall at minimum ensure that-

- (i) there is a board resolution made mandating the bank or institution to provide e-banking transactional services before beginning to offer such services;
- (ii) electronic payment scheme plans are clearly integrated within corporate strategic goals,
- (iii) a risk analysis is performed of the proposed electronic payment scheme activities, appropriate risk mitigation and monitoring processes are established for identified risks, and ongoing reviews are conducted to evaluate the results of electronic payment scheme activities against the institution's business plans and objectives. Additionally, risk management measures are introduced to address risks of provision of financial services over the internet;
- (iv) ensure that the operational and security risk dimensions of the institution's electronic payment scheme business strategies are appropriately considered and addressed;
- (v) that the bank's existing risk management processes, security control processes, due diligence and oversight processes for managing the bank's outsourcing relationships and other third-party dependencies supporting electronic payment schemes are appropriately evaluated and modified to accommodate electronic payment scheme services;
- (vi) it establishes effective management oversight over the risks associated with electronic payment scheme activities, including the establishment of specific accountability, policies and controls to manage these risks; and
- (vii) it reviews and approve the key aspects of the bank's security control process, which include establishing appropriate authorisation privileges, logical and physical access controls, and adequate infrastructure security to maintain appropriate boundaries and restrictions on both internal and external user activities.

## **11.2 Managing Security Risk**

The banks management has the responsibility for ensuring that appropriate security control processes are in place for the electronic payment scheme in addressing issues of authentication, non-repudiation, data and transaction integrity, segregation of duties, authorisation controls, maintenance of audit trails and confidentiality of key bank information.

### **11.2.1 General Guidelines for Managing Security Risk**

The bank or financial institution shall at minimum ensure that-

- (i) appropriate measures to authenticate the identity and authorisation of customers with whom it conducts business over the Internet. Effective Know Your Customer principles should be applied using reliable methods for verifying the identity and authorisation of new customers as well as authenticating the identity and authorisation of established customers seeking to initiate electronic transactions;
- (ii) it establishes formal policy and procedures identifying appropriate methodology(ies) to ensure that the bank properly authenticates the identity and authorisation of an individual, agent or system by means that are unique and, as far as practical, exclude unauthorised individuals or systems. Banks can use a variety of methods to establish authentication, including PINs, passwords, smart cards, biometrics, and digital certificates. Banks can use a combination of these methods or singly;
- (iii) it determines which authentication methods to use based on its assessment of the risk posed by the electronic payment scheme as a whole or by the various subcomponents;
- (iv) it establishes robust customer identification and authentication processes for the cross-border electronic payment schemes given the additional difficulties that may arise from doing business electronically with customers across national borders;
- (v) it establishes audit trails in the electronic payment schemes to facilitate detection errors, fraud and tempering incidences and proper documentation of the same should be kept;
- (vi) it monitors and adopt industry sound practices in the area of authentication to keep pace with the changes in technology and the market;
- (vii) it uses transaction authentication methods that promote non-repudiation and establish accountability for electronic payment scheme transactions;
- (viii) electronic payment schemes are designed to reduce the likelihood that authorised users will initiate unintended transactions and that customers fully understand the risks associated with any transactions they initiate;
- (ix) appropriate measures are in place to promote adequate segregation of duties within electronic payment schemes, databases and applications;
- (x) it reviews and adapt new segregation methods of segregation of duties commensurate with the electronic payment scheme that ensure an appropriate level of control is maintained. The architecture of the straight-through processes, and adequate audit trails should be emphasised.
- (xi) proper authorisation controls and access privileges are in place for electronic payment schemes, databases and applications.

- (xii) appropriate measures are in place to protect the data integrity of electronic payment schemes transactions, records and information by ensuring *inter alia* electronic payment schemes transactions are conducted in a manner that makes them highly resistant to tampering throughout the entire process;
- (xiii) take appropriate measures to preserve the confidentiality of key electronic payment schemes information. Measures taken to preserve confidentiality should be commensurate with the sensitivity of the information being transmitted and/or stored in databases; and
- (xiv) clear audit trails exist for all electronic payment schemes transactions.

### **11.3 Managing Legal and Reputational Risk Management**

Banks and financial institutions have the responsibility of providing their customers with a level of comfort regarding information disclosures, protection of customer data and business availability. In achieving this, banks and financial institution are required to address the following issues; privacy of customer information, capacity, business continuity and contingency planning to ensure availability of electronic payment scheme services, and incident response planning.

#### **11.3.1 General Guidelines for Managing Legal and Reputational Risk**

The bank or financial institution shall at minimum ensure that-

- (i) adequate information is provided on their websites to allow potential customers to make an informed conclusion about the bank's identity and regulatory status of the bank prior to entering into electronic payment scheme transaction;
- (ii) take appropriate measures to ensure adherence to customer privacy requirements in accordance to statutory and contractual obligations;
- (iii) it has effective capacity, business continuity and contingency planning processes to help ensure the availability of electronic payment scheme and services; and
- (iv) It has developed appropriate incident response plans to manage, contain and minimise problems arising from unexpected events, including internal and external attacks, that may hamper the provision of e-banking systems and services.

**Annex I**  
**MINIMUM STANDARDS REQUIREMENTS**

**1. Relevant ISO<sup>1</sup> and de facto Standards**

**(a) For Payment Cards**

- (i) Physical characteristics, dimension and location of contacts, type of electronic signals, transmission protocols and inter-industry commands for interchange transfer, application identification for contact cards (*Refer ISO 7816-1, 2, 3, 4 and 5*);
- (ii) Physical characteristics, radio frequency interface, transmission protocols and transmission security features for “remote coupled” contactless cards (Refer ISO 10536, ISO 14442-1,2,3, & 4 and ISO 7816-4, 5, and 6);
- (iii) Electronic interchange of messages relating to financial transactions between systems (Refer ISO 8583);
- (iv) Transfer of messages between payment cards and cards accepting devices, for both contacts and contactless technology (Refer ISO 9992);
- (v) Security architecture of financial transaction systems using integrated circuit cards covering issues on card life cycle, transaction process, cryptographic key relationships, secure application modules, use of algorithms, cardholder verification, key management, general principles and overview (Refer ISO 10202- parts 1 through 8 and ISO 11568); and
- (vi) Personal identification number (PIN) protection principles and techniques in the banking industry (Refer ISO 9564).
- (vii) De facto standards that support international interoperability between cards, terminals, related devices and software should be generally observed;
- (viii) Developments undertaken by Europay, Mastercard and Visa (EMV specifications) on integrated circuit card, terminal and application specification for payment system should be considered, where necessary.

---

<sup>1</sup> International Organisation for Standardisation (ISO), a Geneva based organisation, whose members are national standardisation bodies (e.g. Tanzania Bureau of Standards).

## **2. Minimum Standards for Other Electronic Schemes**

### **(a) Internet Payments**

- (i) Developments on Secure Electronic Transaction (SET) specifications for Internet payments should also be considered; particularly any impact of such specifications on operations of electronic payment schemes in Tanzania should be evaluated and addressed.

### **(b) Switches**

- (i) De facto standards that support international interoperability between electronic switches for ATMs, cards, terminals, related devices and software should be generally observed.
- (ii) ISO 15022: Standards for securities industry.
- (iii) ISO 8583: Standard for Financial Transaction Card Originated Messages - Interchange message specifications is the International Organization for Standardization standard for systems that exchange electronic transactions made by cardholders using payment cards.
- (iv) UN/EDIFACT international EDI standard developed under the United Nations

## REFERENCES

Bank for International Settlements, Basel Committee for Banking Supervision *Risk Management Principles for Electronic Banking*. May 2001

Bank for International Settlements, Basel Committee for Banking Supervision *Management and Supervision of Cross-Border Electronic Banking Activities*. October 2002