



Standards for Issuance & Acceptance of Contactless Payments

In the Arab Republic of Egypt



Standards for Issuance & Acceptance of Contactless Payments

In the Arab Republic of Egypt



Table of Contents

Introduction	5
General Definitions	6
1- Scope of Regulations	7
2- Responsibilities of the Board of Directors & Top Management	8
3- Regulations of Anti-Money Laundering, terrorism financing combating and Information Security	9
4- Regulations for Issuing Contactless Payment Instruments	10
5- Regulations for accepting contactless payments instruments	12
6- Detection of Unusual Activities.	14
7- Raising Awareness among Users of Contactless Payment Instruments	15
8- license applying procedures	16



Introduction

Within the framework of CBE's efforts to support and encourage the use of the different means and channels of electronic payment in attempt to shift towards a less cash-dependant economy and to achieve financial inclusion, and in light of the current technological developments achieved in the field of electronic payment and the emergence of contactless payments, as well as the need to cope with such developments so as to ensure realization of tangible progress in the field of electronic payments in a safe manner for all stakeholders, hence the following regulations have been issued.

General Definitions

Near Field Communication “NFC”	Means close range communication via a set of communication protocols through which two devices or tools may communicate within a near field not exceeding 4 cm.
Contactless Payments	Means payments that take place without any contact, using cards (credit cards, debit cards, prepaid cards), smart devices or wearable devices that use radio-frequency identification (RFID) or near field communication (NFC), which allow the chip and the antenna to contact POS over a short distance for the safe completion of the purchase transaction.
Secure Code	The code sent to the client, whether static or dynamic code, whether through a text message or through tokens, which serves as an additional security factor when using a payment tool for the online purchase of items.
Dual Interface EMV Contactless	The card supports contactless communication via NFC and contact communication via reading the card chip data.
Dual Interface POS Terminals	The electronic points of sale terminal supports reading contactless payment instruments and contact cards at the same time.
Collision	Interference of the frequencies of contactless payment tools in the event there are more than one within the same range.

1- Scope of Regulations

- These regulations shall apply over all banks in Egypt as well as branches of foreign banks. The regulations represent the minimum requirements to provide contactless payment services in a safe manner. All banks should not suffice with such regulations and should verify that all necessary measures are taken for the management of risks associated with the provision of such types of banking services.
- These regulations shall control the issuance and acceptance of contactless payments only, without prejudice to control regulations governing electronic banking transactions previously issued by CBE, as well as the instructions and rules regulating the execution of bank transactions, anti-money laundering and combating financing terrorism issued by CBE, as well as diligence measures issued by the unit concerned with anti-money laundering and combatting financing terrorism.



2- Responsibilities & Obligations of the Board of Directors & Senior Management

The bank's Board of Directors shall be responsible for ratification of the work strategy prepared by its Senior Management and for issuing a clear strategic decision whether the bank shall provide contactless payment services or not. The Board of Directors shall particularly verify the following:

- That contactless payment service plans are compliant with the bank strategy objectives.
- Conducting risk analysis for those services.
- Setting appropriate measures for risk control and mitigation.
- Ongoing monitoring to assess the results of contactless payment services according to the set plans and objectives.
- The bank shall lay a risk policy for companies engaged in these services and shall conduct risk studies relating to the following:
 - Refunds.
 - Fraud.
 - Disputes.

3- Regulations of Anti-Money Laundering, Terrorism Financing Combating and Information Security


Banks issuing contactless payment instruments or accepting contactless payments shall follow the below:

- Abide by Law No. 80 of 2002 Promulgating Anti-Money Laundering & its Executive Regulations, bank control regulations on anti-money laundering & terrorism financing combating, and know your customer regulations issued in 2011, all amendments thereof by CBE, due diligence measures concerning prepaid card customer services issued in March 2019 by the unit of anti-money laundering and terrorism financing combating.
- Give proper attention as to the nature of the service in order to identify suspicious transactions that may include money laundering or financing terrorism according to the bank control regulations on anti-money laundering and terrorism financing combating issued by CBE in 2008.
- In case of any suspicious operations through these tools, should be reported to the unit of anti-money laundering and terrorism financing combating in accordance with the provisions of Law No. 80 of 2002 on Anti-Money Laundering.
- Abide by any instructions issued by CBE afterwards concerning payment cards of all types or any means of using/ accepting contactless payments.
- Any infringement/ hacking of any data of such services, must be immediately reported to CBE's information security department at cbe.infosec@cbe.org.eg and the cyber security sector at csirc-team@cbe.org.eg.

4- Regulations for the Issuance of Contactless Payment instruments

- With regard to banks issuing contactless payment instruments, **the maximum amount of each Tap & Go transaction (i.e. without entering a PIN) shall be EGP 300**, while each bank shall set the ceiling amount it deems appropriate, not to exceed the ceiling amount authorized by CBE, for tap & go transactions, noting that CBE Governor may change the maximum amount of tap & go transactions.
- The bank shall lay a disputes mechanism for such types of transactions.
- The bank shall set **the maximum No. of daily and monthly transactions** based on the bank's risk management vision.
- The bank issuing a contactless payment instruments must send an SMS after each contactless transaction exceeding EGP 100.
- Contactless payment instruments shall not be activated prior to handing them over to customers, which shall be activated only upon verifying delivery of the contactless payment tools to the customer, noting that the issuing bank must set a verification mechanism to confirm the customer's receipt of the tool.
- The bank shall launch awareness campaigns on how to use with contactless payment instruments provided by the bank.

If the contactless payment instruments is plastic card:

- cards must be dual interface EMV contactless complying with the international standards **ISO/IEC7816 & ISO/IEC 14443**.
- The bank may use blocking card sleeves to protect customers as well as the bank itself against any fraudulent acts that may occur as a result of stolen card data by using special devices.
- A secure code must be activated for e-commerce transactions carried out using such cards "card not present".
- A sign indicating the acceptance of contactless cards must be printed. 
- During issuance of the card "card personalization" should be a unique encryption key for each card issued while using encryption techniques ratified by the card scheme, provided that the static data authentication (SDA) technique should not be adopted. Alternatively dynamic data authentication (DDA) or combined data authentication (CDA) may be used.

- The maximum validity period of the card shall be 5 years.

In case of using the mobile phone, “NFC payment” or wearable/non-wearable devices with contactless features, the following must be satisfied:

- The issuing bank systems must support different verification mechanism consumer with consumer device cardholder verification method CDCVM that would enable the bank to process and identify movements taking place through different security means.
- The consumer device verification method “CDCVM” can be done through the below :
 - PIN.
 - Mobile phone passcode.
 - Biometric user authentication such as (retinal scan/ facial recognition/ hand recognition/ voice recognition).
- Contracting must take place with a tokenization service provider as well as a tokenization hub, in cooperation with and under the supervision of scheme.

In all cases, CBE’s approval must be obtained before accepting any tokenization service provider or any tokenization hub.

5- Regulations for accepting contactless payments

- With regard to contactless payments acquirer banks, the maximum amount of each **Tap & Go transaction (i.e. without entering a PIN) shall be EGP 300**, while the CBE Governor may amend the maximum amount of tap & go transactions.
- It is recommended that POS terminals accepting such types of cards are dual interface POS terminals.
- The international standards **ISO/IEC7816 & ISO/IEC14443** must be applied in any communications between contactless payment instruments and POS.
- A distinctive sign should be placed on devices accepting payment with contactless payment instruments.



- It must be ensured that POS terminals with this feature are placed directly facing customers and away from any source of electricity or any other source of metal, which signals may affect the payment process, so the maximum distance between the contactless payment instruments and the machine carrying out the transaction, should be 4 cm.
- A customer's signature shall not be required for such transactions with the exception of transactions that take place using contactless payment instruments issued from banks outside Egypt.
- The necessary awareness campaigns must be launched by the bank to merchants on how to use the different types of contactless payment instruments.
- The bank shall set the measures that would ensure that transactions by customers are not mistakenly duplicated by POS's at merchants.
- The POS terminal shall reject the purchase transaction if there are more than one contactless payment instruments near the device, thereby causing collision, so as to ensure that the contactless payment instrument holder does not pay using the wrong payment instrument during the purchase transaction as a result of the intervention of signals from other payment instrument..
- The bank shall provide the necessary training to its personnel on contactless payment instruments to enable them to reply to all customers' inquiries and to support them in a sound manner.

- Before activating the service, the bank shall conduct a risk assessment to activate accepting contactless payment at each merchant.

In case of payment over mobile phones (NFC payment) or any other wearable or unwearable device with a contactless feature, the following must take place:

- If the POS terminal is incapable of identifying the consumer device cardholder verification method (CDCVM), then a PIN must be entered or the transaction will be rejected.
- The bank shall study the impact of tokenization on its own systems, and shall study an alternative solution for the merchants in the event he depends on the card No. with regard to his customers' disputes/ loyalty transactions. For instance, he can rely on a payment account reference (PAR) to obtain the data concerning such transactions.
- The bank shall provide adequate training to merchants with POS terminals on the multiple consumer device card verification methods (CDCVM) that may be used during the purchase process.

In all cases, CBE's approval must be obtained before relying on any encryption service provider.

6- Detection of Unusual Activities

- Banks should set effective measures to guarantee constant monitoring to ensure the rapid detection of any unusual or suspicious contactless payment transactions that may be part of a fraud.
- The monitoring system must have the ability to send out fast alerts to monitor and detection officers overseeing contactless payment services as soon as they detect any unusual activities. In such cases, banks shall verify this with the owners of the concerned contactless payment instruments as soon as possible and shall notify the competent authorities.
- Customers shall be immediately notified in case of detecting any unusual activities raising fraud suspicions concerning their contactless payment instruments.

7- Raising Awareness among Users of Contactless Payment instruments

- Due to the rise of security risks when contactless payment users are unfamiliar with the necessary security precautions that must be followed when using the service or in cases where they misunderstand such precautions, thus, it is essential that the bank pay special attention to raising awareness among customers by providing them with clear and easily understandable advice on the necessary security precautions that should be followed when dealing with contactless payment services and the significance of abiding by such advice/ precautions.
- customers should be notified that bank employees or **agents are not allowed to ask for sensitive data from users** (such as PIN numbers, passcodes, or payment card data) whether via email or any other means, and that, if this happened, the relevant user should communicate the bank as soon as possible.
- The bank should take the necessary precautions according to the nature of the customers and the nature of the contactless payment services that are provided.
- The bank should make available effective means for raising awareness among customers and notifying them about the security precautions that they should take. The bank may use numerous means to this end (for example, without limitation the bank's websites, messages printed out on customers' bank statements, promotional material). A bank may also use promotion screens and ATMs to place guidance material to raise awareness among customers. This can also take place when front desk officers or service providers at the bank contact customers in order to stress the importance of abiding by the basic precautionary measures.

8- License Procedures

- Banks wishing to issue/ accept contactless payment instruments for its customers shall apply to obtain CBE's consent, upon satisfying the following minimum paper requirements at least :
 - List of functions and services the bank wishes to offer or amend.
 - The bank's scheme for issuance of payment tools or acceptance of contactless payments, indicating for example, without limitation, the number of cards/ contactless payment instruments targeted to be issued, the No. of new and existing POS that will support the deployment of such payments).
 - A report indicating any case of non-abidance by the rules issued by CBE, wholly or partially, concerning the issuance/ acceptance of contactless payments.
- Conducting the necessary certifications on the cards as well as the POS, to pass all certifications by schemes in this regard and to furnish CBE with evidence of passing such tests.
- If the bank wishes to add any new contactless payment services, it must obtain a new approval from CBE.
- The Bank shall provide the CBE/Payment Systems and business Technology sector at CBE with quarterly reports (in both soft and hard copy), including the following information at least:
 - The No. of POS of the bank accepting such type of contactless payment cards/ instruments.
 - The No. of cards/ payment instruments
 - The No. of monthly transactions carried out by such cards/ instruments taking place without using a PIN.
 - The total amounts paid by customers without using a PIN.
 - The No. of monthly transactions carried out by such cards/ instruments taking place using a PIN.
 - The total amounts paid by customers using a PIN.

- Totally abide by all rules issued by CBE concerning such cards/ transactions.

CBE may carry out inspections on any part of the system to verify compliance with the standards and specifications set out by CBE. Any bank's attempt to impede CBE's such mission shall be deemed a violation of these rules by the bank.







جميع المعلومات والصور والرسوم البيانية والتصاميم المتضمنة في هذا الكتاب هي ملك للبنك المركزي المصري ولا يجوز استخدامها أو نسخها بأي شكل من الأشكال إلا بإذن خطي مسبق من البنك المركزي المصري
جميع الحقوق محفوظة للبنك المركزي المصري © 2019

All Information, Photos, Charts and Designs Found in this Book Belongs to Central Bank of Egypt
Any usage or duplication without formal authorization form Central Bank of Egypt is prohibited
© 2019 Central Bank of Egypt. All Rights reserved.

البنك المركزي المصري

CENTRAL BANK OF EGYPT

54 شارع الجمهورية، وسط البلد، القاهرة، مصر

54 El Gomhoreya St., Downtown, Cairo, Egypt

info@cbe.org.eg | 16777

صندوق بريد: 11511 P.O.Box: