KPMG

Hazem Hassan
Public Accountants & Consultants

# CBE Payment Tokenization Requirements

## Egypt's Tokenization Requirements as per CBE Guidelines

2023

**Point of View (PoV)**

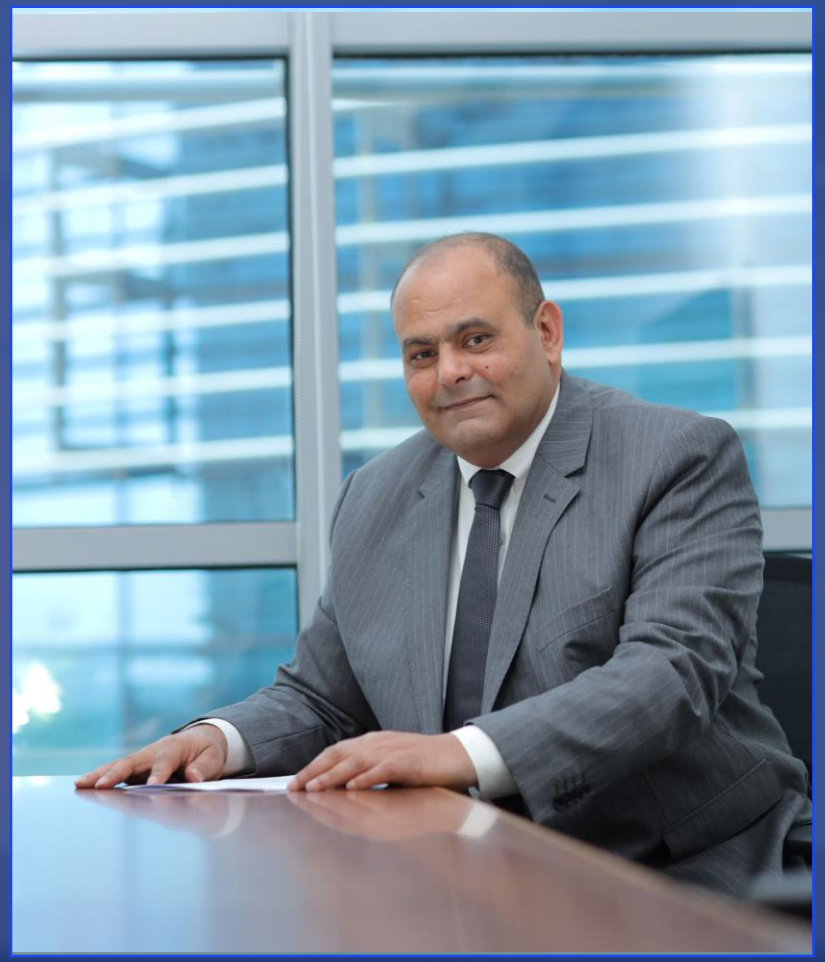
# Foreword

Payment industry has undergone a great transformation globally and the advances in technology have enabled in bringing world-class experiences to the masses in Egypt.

By incorporating Digital Payments in the KPIs to measure financial inclusion, Central Bank of Egypt (CBE) has provided a clear signal to all stakeholders that the ease and seamless integration of payments systems in business transactions is of critical importance. This is a significant opportunity for Egyptian businesses to step-up and demonstrate their IT capabilities and make a mark.

We, at KPMG Hazem Hassan, are fully geared to assist our clients in capitalizing on this immense opportunity to transform their systems, enhance customer experience and meet regulatory requirements.

**Ehab Abou Elmagd**
Managing Partner,
KPMG Hazem Hassan



# Introduction

**Payment industry is witnessing various progressive innovations as pace of change accelerates. At the same time, it requires increased protection against frauds to reduce unauthorized access to cardholder data and stop cross-channel deception. Tokenization of card-holder information is a step in that direction. Central Bank of Egypt (CBE) has also published its guidelines on the requirements for banks and payment networks to adhere to while providing digital payment services. In this POV, we discuss the requirements, key focus areas, risks to watch-out for and the future of tokenization and payments services.**

As part of the "**Egypt's Vision 2030**", Egypt has been pursuing financial inclusion as a strategic imperative. It has been identified as one of the main pillars in Egypt's achievement of **Sustainable Development Strategy (SDS).** Some key objectives for financial inclusion that have been noted as part of the **Financial Inclusion Strategy (2022-2025)**[1] by Central Bank of Egypt (CBE) are:

- Drive financial inclusion by **reaching consumers in rural and remote areas**;
- Develop **financial literacy among all consumers**;
- Enhance the **financial capabilities of all consumers**;
- Encourage **innovation in financial products and services**; and,
- Establish **strong frameworks and guidelines for consumer protection**.

Further, adoption of Digital Payments has been identified as a key KPI to determine the scale of financial inclusion in the Egypt market by CBE. As per the data published by WorldBank[2] in 2021 only 20% of Egypt's citizens over 15 years of age have used digital payments (sent or received) for transactions. What is of significance is that this remains a relatively low rate of adoption for digital payments when compared to the entire region.

For e.g., adoption of digital payments as a mode of transaction stands at approximately 40% for the MENA region while it is approximately 50% for the Sub-Saharan African region. On the other hand, the **CBE Financial Inclusion Strategy (2022-2025)** notes that financial inclusion has increased steadily and has grown by 147% between 2016-2022.

The WorldBank report also noted that over 73% of the Egyptian population remains unbanked. This, therefore, also presents an opportunity to expand the digital payment services to the unbanked masses. However, with the increased pace of adoption of digital payments, comes the heightened risk of online identity thefts and payment frauds. In order to ensure security of consumers and a robust payments network, CBE recently introduced guidelines and regulations to support the adoption of tokenization in digital payments.

CBE has mandated support for payment tokenization across the following networks:

1. International payment networks like Visa, Mastercard, etc.;
2. Government payment network under Egyptian Bank Company (EBC); and,
3. Meeza Payment Network

**50%** **Digital payments in Sub-Saharan**

50% of transactions in Sub-Saharan region are done digitally

**20%** **Egyptians have used digital payments**

Only 20% of the Egyptian citizens above the age of 15 years have performed transactions digitally (sent or received)

**40%** **Digital payments in MENA**

40% of transactions in MENA region are done digitally

**147%** **Growth in Financial Inclusion**

Egypt has witnessed a significant growth of 147% in financial inclusion between 2016-2022

**73%** **Unbanked population**

Egypt has an estimated 73% unbanked population


**Sources**:

1. **Financial Inclusion Strategy (2022-2025):** https://www.cbe.org.eg/en/financial-inclusion
2. **The Global Findex Database 2021:** https://www.worldbank.org/en/publication/globalfindex

## What are Digital Payments?

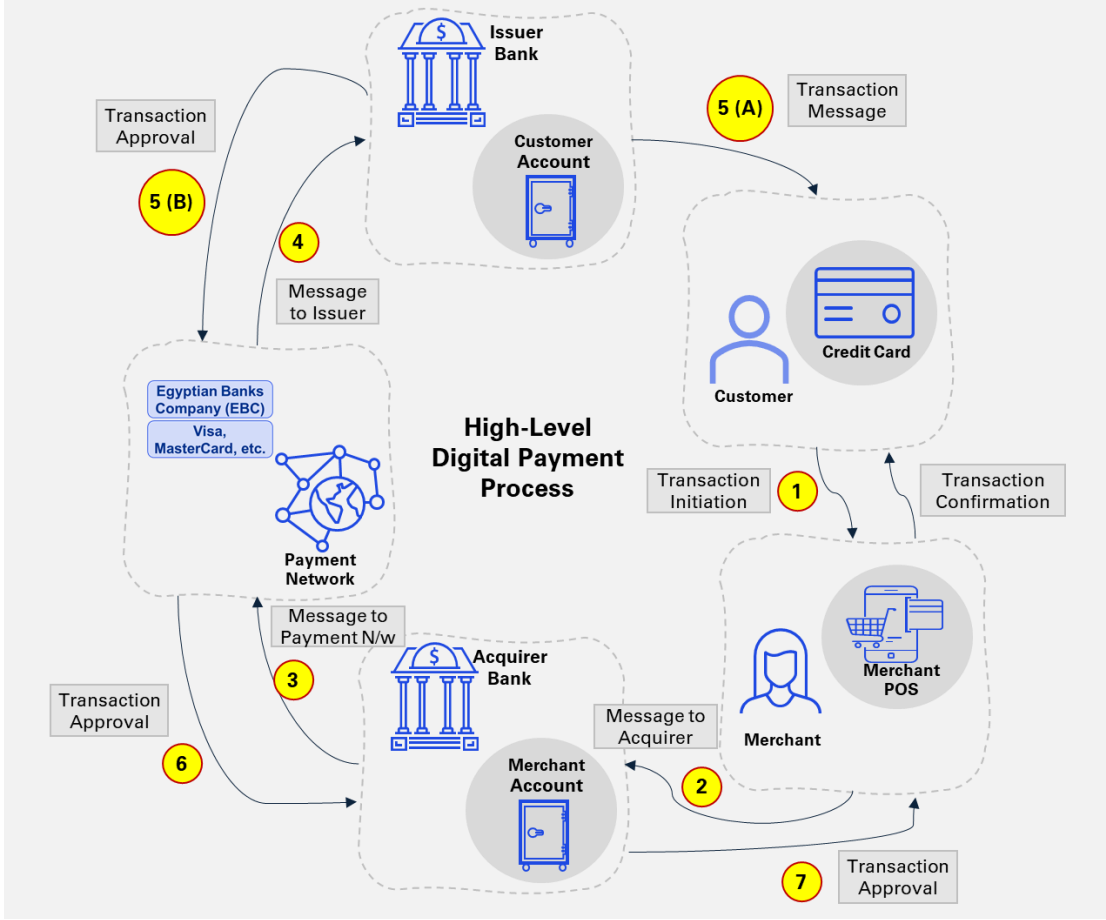
Digital Payments (also called e-payments) are payments done through an online channel without the involvement of cash. Such transactions are usually carried out through devices like mobile, laptops, POS machines, etc. The infrastructure requirement for such digital payments are that both the payee and payer for the transaction should have a bank account which is accessible online, a device/ mode through which the transaction can be carried out, and a payment network to carry the transaction information between the entities involved.

## Entities Involved

The key entities involved in such a payment system are:

- **Customer:** The end-user performing the transaction/ availing a service through an online or digital channel.
- **Issuer Bank**: This is the bank for the customer which has issued the credit/ debit card
- **Merchant:** This is the retailer/ service provider who is going to be the beneficiary of the transaction performed.
- **Acquirer Bank:** This is the bank for the merchant and will be the receiver of the payment on behalf of the merchant
- **Payment Network:** This is the private (like Visa, Mastercard, Amex, etc.) or a government network (like Egyptian Banks Company (EBC), Meeza, etc.) that is responsible for carrying the transaction and facilitating the settlement between the Acquirer and the Issuer Bank.

Although Digital payments have been around for quite some time, they have recently gained a significant traction across the world due to the ease and speed of such transactions. Further, the digital payments allow the benefit of ensuring last mile connectivity in areas where the banks may not have reached with a physical branch, thereby improving the financial inclusion of remote or under-served communities.




To understand the process of digital transactions, let's look at an example: Assume Mohamed purchases grocery worth EGP 1,500 from a store called "My Grocery Shop" in Cairo. Mohamed makes the payment using his debit card at the Point of Sale (PoS) device in the shop.

When the cashier swipes his card on the PoS machine, Mohamed is asked to enter a personal identification number (or PIN) to authenticate him. Then a message is sent by the Merchant Bank to the Issuer Bank, via the Payment Network to check for validity of the card, and sufficient balance in Mohamed's account. The payment network routes the query to the Issuer Bank and once an approval is received from the Issuer Bank, the money is debited from Mohamed's account and credited to the account maintained by the Merchant Bank of "My Grocery Shop".

## What is Tokenization?

Tokenization is a process that replaces sensitive payment data, such as credit card numbers (PAN) or bank account details, with unique and randomly generated tokens containing strings. These tokens are meaningless if not linked to customer's data. Tokenization is typically performed by a payment gateway or a token service provider.

## How does it work?

A **token vault** is a secure database or system provided by a **Token Service Provider (TSP)** that stores the mapping between the tokens and the corresponding sensitive payment data. When a transaction occurs, the token vault is accessed to retrieve relevant payment information required to process the transaction. The tokenization service provider then detokenizes information in the token received during the transaction to identify underlying customer information. This is then used to communicate with the Issuer Bank and to obtain confirmation for the transaction.

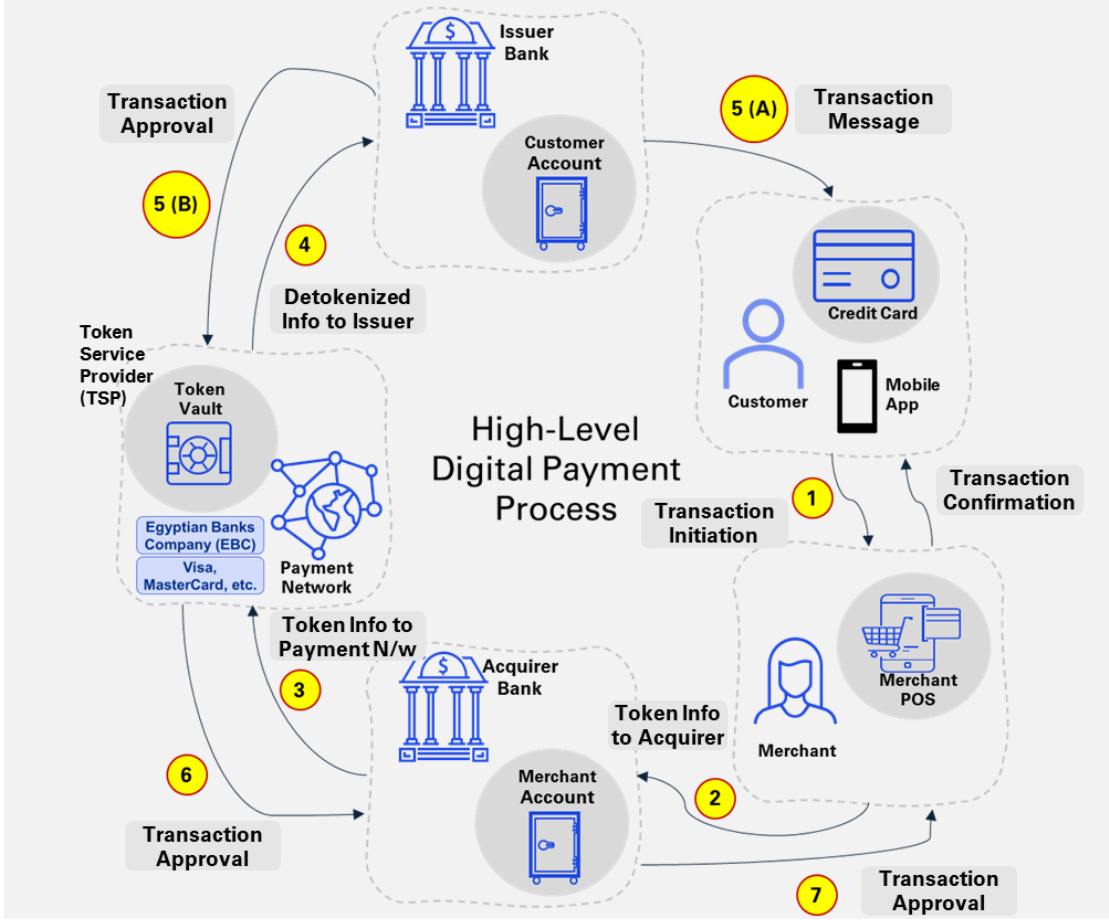
## Indicative Benefits

**Tokenization** carries many benefits, including:

- Eliminates the need for storage of sensitive payment information by intermediaries;
- Businesses are required to comply with PCI DSS, which in-turn helps merchants to simplify their compliance efforts;
- Seamless customer experience at the POS by automatically using their relevant tokens. The tokens can be used to enable "one-click" payments for any future payments;
- Integration with various payment systems makes it easier for merchants to adopt tokenization as part of their payment infrastructure. This integration, in-turn, eliminates the need for significant changes to existing payment processes.

The **token vault** benefits are equally important too:

- Enhances transaction security and reduces risk of data breaches;
- A token vault significantly reduces the value of data stored by intermediaries;
- If a token vault is compromised, the stolen tokens are of less significance without access to the original payment data, and their encryption keys;
- Token vaults must comply with all PCI DSS (Payment Card Industry Data Security Standard) standards ensuring robust security controls.




## Key Risks

Implementing tokenization and integrating token vaults into existing payment systems carries its own risks and technical challenges:

- **Business/ Transaction Resiliency:** Businesses must ensure thorough testing to avoid disruption or availability issues to payment processes.
- **Interoperability:** Another risk could arise from failing to apply a unified standardization process across tokenization practices and protocols resulting in interoperability issues.
- **Cybersecurity of TSP:** The addition of another entity in the payment process, means another point in the payment process that needs to be secured. Weak IT controls at the TSP could lead to a major cybersecurity incident impacting millions of users and transactions.

Central Bank of Egypt (CBE) released the first edition of tokenization guidelines titled ***"Payment Cards Tokenization on Electronic Devices Applications"*** earlier in 2023. The comprehensive guidelines are wide ranging and are applicable to all banks operating in Egypt, encoding service providers, payment network participants, POS devices, etc. The guidelines cover risks to be mitigated, obligations applicable, infrastructure to be secured, processes across business verticals, sub-contractor requirements, and licensing requirements among other things.

## High-Level Framework of the guidelines

**Applicability**

- Banks
- Card Encoding Service Providers
- Payment Network Participants

**Scope of Coverage**

- Entity, Fraud & Cybersecurity Risks
- Business Processes
- Payments Infrastructure (devices & applications)

**Obligations & Compliances**

- Terms & Conditions
- Periodic Reporting and Monitoring
- License Requirements
- Controls

1/2

## Risk Management

**Coding Services Risks**
- Reputational
- Non-compliance
- Cybersecurity
- Fraud

**Governance**
- Policies & Procedures

**Anti-Money Laundering**
- Security Council resolutions

## Obligations

**Issuer Bank**
- Customer Authentication & Validity
- Meeza Token Acceptance
- Employee Trainings
- Customer Support
- Digital Payments License
- Transaction Limits (Qty & Amount)
- Vendor Contracting
- Customer Education
- Card Security
- CBE Reporting

**TSP**
- Secure Communication
- Authentication & Verification
- Communication Encryption
- Token Generation
- PAN Security
- PCI Standards Compliance
- Card Security
- Tokenization/ Detokenization Requests
- Token and Transaction Analytics
- Meeza Card Support

**Acquirer Bank**
- Compliance with ISO/IEC 14443
- Transaction Limits (Qty & Amount)
- Meeza Token Acceptance
- Merchant Education
- Customer Authentication & Validity
- Customer Support
- e-Payments Approval

**Payment Network**
- Code Creation & Validation
- Authentication & Verification
- Card Security
- Chargebacks & Refund Procedures

**Token Requestor**
- Locally Hosted Digital Wallets
- OEM Digital Wallets
- Transaction Limits (Qty & Amount)
- Auxiliary Token
- Meeza Card Support
- Network Security & VAPT
- Authentication & Verification
- EMVCO Compliant Cards
- PCI Standards Compliance
- Card Security

**Egyptian Banking Company (EBC)**
- Code Creation & Validation
- PCI Standards Compliance
- SOC2 Report to CBE
- Periodic Operational Reporting
- Network Security & VAPT
- Cybersecurity Framework
- Cybersecurity Incident Reporting
- Secure Communication
- Employee Training

*** This is an indicative list based on the CBE guidelines and the applicability may differ depending on the entity's actual scenario.**

## Controls

### Confidentiality, Integrity & Security

- PCI Standards Compliance
- Encryption and Key Management
- Network Security & VAPT
- Mobile Application Security
- Cybersecurity Framework
- Segregation of Duties

### Infrastructure Security

- Physical & Environmental Security
- Security Operations Center (SOC) Setup
- Data Retention
- Third-Party Risk Management Framework
- Cybersecurity Framework
- Incident Response & Recovery
- Audit Logging

### Assessment & Reporting

- Periodic Network and Configuration Security Review
- Quarterly VAPT Assessments
- Service Provider Rotation
- Incident Response & Recovery

### Incident Response

- Incident Response Process
- Forensic Evidence Management Process
- Incident Report to CBE

### Disaster Recovery

- 24*7 Service Availability
- BCP/ DR Plan
- SLA Requirements

## Customer Security

### Applicable Terms & Conditions (T&C)

- T&C Acceptance
- Fees Transparency
- Customer Education
- Customer's Rights & Responsibility

### Transaction Monitoring

- Continuous Transaction Monitoring for frauds
- Fraud Reporting
- Suspicious Transactions Handling Procedures

## License Requirements

### Pre-requisites for Digital Payments License Application

- IT Infrastructure Details
- 3-year Business Plan
- Testing for service levels
- Implementation of Cybersecurity Controls
- VAPT Report

*** This is an indicative list based on the CBE guidelines and the applicability may differ depending on the entity's actual scenario.**

## Governance

- Bank's Board of Directors is responsible for approving the strategy for providing card coding services
- Setting clear policies and procedures to determine the bank's ability to accept the risks and to evaluate these policies atleast annually for updates
- Systems, policies and processes should support EBC and Meeza network
- Digital wallets should be hosted locally

## Operational

- Controls to be designed in order to bring the residual risks associated to acceptable levels
- Implement tools for continuous monitoring and follow-up of security controls including testing for effectiveness atleast once a year
- Ensure transaction limits in terms of quantity and amounts are enforced for transactions carried out within Egypt

## Cybersecurity

- Entities should setup a Security Operations Center (SOC) to track and respond to security incidents
- Entities should ensure an appropriate Cybersecurity framework is implemented to secure customer information and adhere to transaction security requirements
- Service provider for security assessments should be rotated after every two consecutive assessments

## Analytics & Reporting

- Banks are required to provide periodic reports to CBE for performance of the transactions and systems
- TSPs should perform and report on transaction and token analytics to CBE
- Ensure any security incidents are reported to CBE within 6 hours
- SOC2 Type2 report to be submitted to CBE

## Audit & Compliance

- Entities should perform periodic (atleast annual) Systems Audit to assess security posture of systems and software involved in transaction processing
- PoS should comply with the ISO/ IEC 14443 standards
- Systems should comply with requirements under the PCI standards
- A systems assessment report is a pre-requisite to obtaining a license for all Banks participating in the Digital Payments ecosystem

## Customer/ Merchant Education & Support

- Entities should design a customer and merchant education program to inform them of their rights and responsibilities
- Entities should inform the customers of any applicable fees transparently
- Entities (esp. Banks) should ensure appropriate customer support to address any customer queries
- Transactions should be continuously monitored for any fraud

# Future of Tokenization

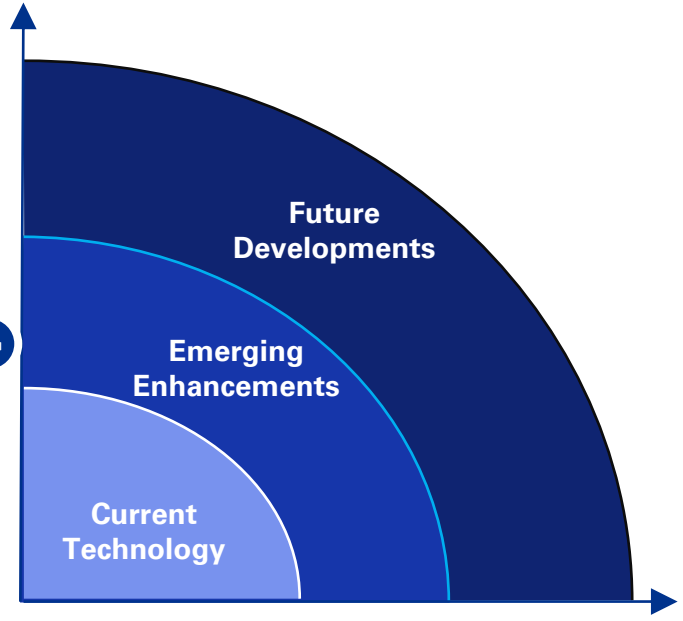
## Current Technology

- **Integration with Digital Wallets:**

Tokenization solutions have been enhanced to integrate seamlessly with digital wallets. This integration enables secure tokenized transactions within the digital wallet ecosystems, ensuring a convenient and protected payment experience for users. **E.g.: Apple Pay, Google Pay, and Samsung Pay, etc.**

- **Tokenization for E-Commerce:**

Payment tokenization fulfill the needs of e-commerce transactions, focusing on specific requirements. These developments include seamless integration of tokenization solutions into online payment gateways, ensuring secure and protected payments for online purchases. **E.g.: Visa, Mastercard, Europay, etc.**




- **Strong Customer Authentication (SCA) Support:**

Payment tokenization solutions have been updated to comply with Strong Customer Authentication (SCA) requirements, such as the Payment Services Directive (PSD2) in Europe. These updates enable tokenization solutions to support SCA, ensuring authentication compliance while preserving the security benefits of tokenization. **E.g.: Stripe, Paypal, etc.**

- **Expanded Use-Cases:**

Payment tokenization solutions have advanced to cater to a broader range of payment scenarios, going beyond traditional card-based transactions. This evolution includes support for tokenization in alternative payment methods like QR codes, peer-to-peer payments, and tokenized bank account transfers. By adapting to diverse scenarios, tokenization solutions enhance security and convenience across various use cases.

- **Self-Sovereign Identity (SSI):**

SSI solutions give individuals control over their digital identities, and tokenization helps securely represent and manage these identities. Tokenization enables trust and privacy enhancing payment transactions, ensuring individuals retain ownership and control of their personal data while maintaining security. **E.g.: Sovrin, uPort, etc.**

## Emerging Enhancements (2-5 years)

- **Blockchain-Based Tokenization:**

Blockchain technology is increasingly being adopted for payment tokenization, as it provides decentralized and immutable transaction records. This innovation enhances the security and transparency of tokenized payment processes, making them more robust and trustworthy. **E.g.: in case of Fungible & Non-Fungible Tokens for assets.**

- **Machine Learning (ML) and Artificial Intelligence (AI):**

Machine learning and AI integration in tokenization solutions empowers advanced fraud detection by analyzing tokenized payment data for patterns and anomalies. This innovation proactively identifies and mitigates fraudulent activities, enhancing the security of tokenized payment processes.

## Future Development (>5 years)

- **Enhanced Security Measures:**

Ongoing research and development will likely continue to improve the security features of payment tokenization. This includes exploring advanced encryption techniques (post-quantum cryptography), multi-factor authentication, and continuous monitoring to stay ahead of evolving cyber threats.

- **Privacy and Data Protection:**

Future work may involve enhancing privacy measures in payment tokenization, ensuring compliance with privacy regulations, and implementing mechanisms for users to control their personal data. Innovations such as zero-knowledge proofs and differential privacy could be explored to strengthen privacy protections.

- **Integration with Emerging Technologies:**

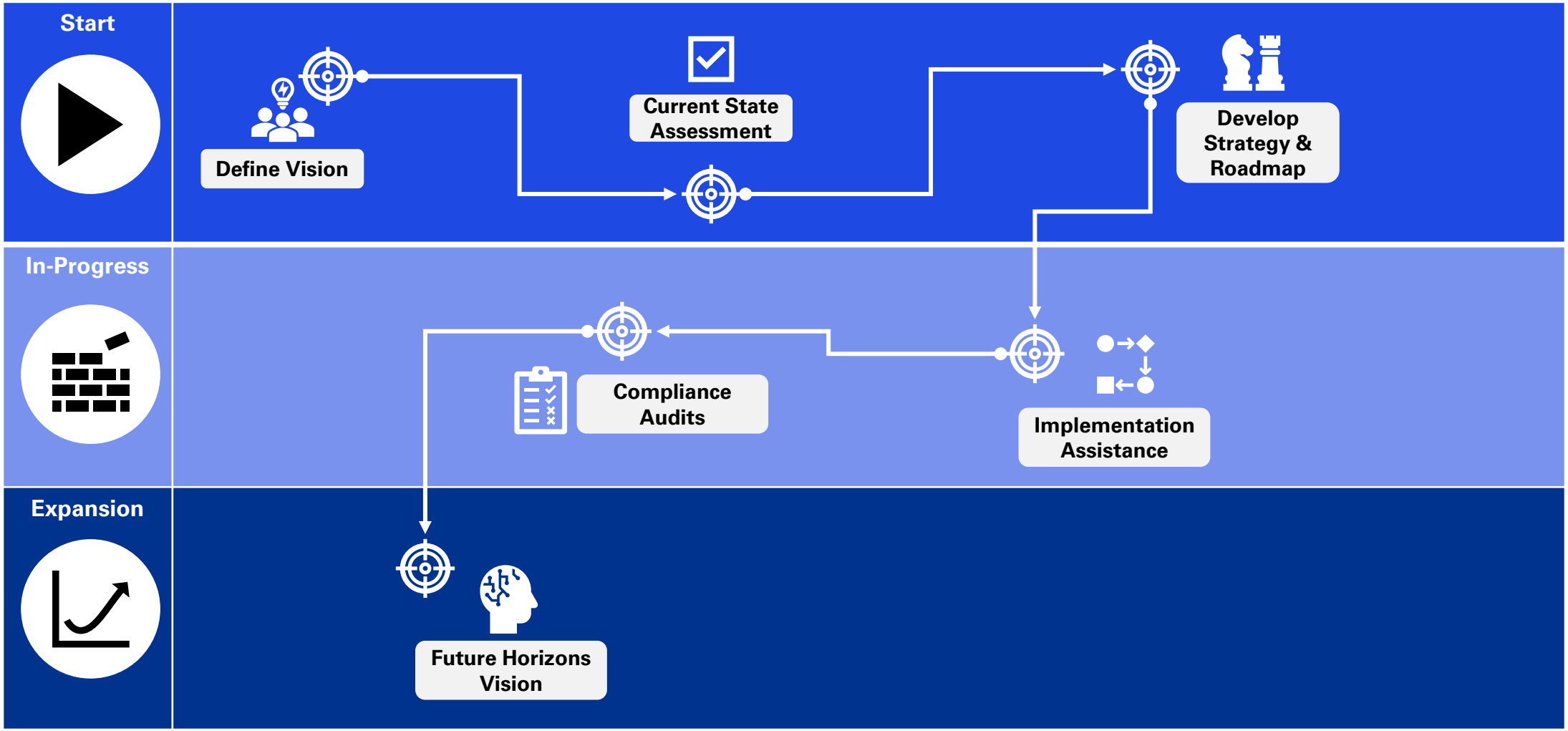
Payment tokenization could integrate with emerging technologies such as blockchain, decentralized finance (DeFi), Internet of Things (IoT), and artificial intelligence (AI). Leveraging these technologies can open new possibilities for secure, efficient, and innovative payment experiences.

**Our Point of View**

In our opinion, it would be prudent for Egyptian businesses to:

- Determine best use case for their business needs and start exploring emerging technologies early, even if in limited manner;
- Keep a strong focus on Customer Experience trends in the payments industry to deliver a “standard user experience” for today’s highly mobile, digitally savvy and privacy conscious generation;
- Perform periodic risk assessments and stay nimble to ensure alignment with emerging regulatory requirements.

## At KPMG, we have a team of experienced and highly skilled personnel who can assist you in your journey irrespective of your current stage.



Digital Payment Process

CBE Payment Tokenization Requirements

Key focus areas as per CBE Guidelines

Future of Tokenization

**How can we help?**

We work with our clients across all their requirements to advise in the design, development, implementation and/ or assessment of a secure environment for their systems and applications supporting payments that enhances the trust of the customers, management, regulators and other stakeholders.

We bring together a cross-functional and experienced team to provide a comprehensive solution to our clients for their cybersecurity requirements while meeting their strategic and operational needs.

## Our High-Level Approach

| Plan | Assess | Recommend | Operationalize |
|---|---|---|---|
| ➢ Determine stakeholder expectations<br>➢ Assess impact across cross-functional teams and payments value chain<br>➢ Baseline current processes | ➢ Identify gaps in software applications and hardware infrastructure<br>➢ Identify interface gaps<br>➢ Identify governance, process and policy gaps | ➢ Develop target state requirements<br>➢ Identify closure options (in-house/ outsourced)<br>➢ Prioritize action items | ➢ Develop roadmap for achieving compliance<br>➢ Monitor and report progress against timelines<br>➢ Conduct trainings for key stakeholders |

**Suggested KPMG Thought Leaderships**


**Cybersecurity Considerations 2023**


**10 Predictions for the future of payments**


**New Payments Architecture (NPA) Supporting your journey**


**The payments language of the future has arrived**

# Contributors

- **Tarun Kapur**, HOD, IT Audits & IT Advisory
- **Mostafa Samir**, Sr. Manager, IT Audits & IT Advisory
- **Basheer Soliman**, Sr. Manager, IT Audits & IT Advisory
- **Yasmeen Anwar**, Senior, IT Audits & IT Advisory
- **Hazem Abdulrahman**, Associate, IT Audits & IT Advisory

# Contact Us

**Mohamed Tarek**
Head of Advisory,
E: mtatek@kpmg.com

**Khaled Samir**
Head of Audit,
Non-FS Sector Audits,
E: ksamir@kpmg.com

**Abdelhadi Ibrahim**
Head of FS Sector Audits,
E: abdelhadiibrahim@kpmg.com

**Tarun Kapur**
HOD,
IT Audits and IT Advisory
E: t.kapur@kpmg.com

**Mostafa Samir**
Sr. Manager,
IT Audits and IT Advisory
E: mostafasamir@kpmg.Com

**Basheer Soliman**
Sr. Manager,
IT Audits and IT Advisory
E: bmsoliman@kpmg.com

KPMG

Hazem Hassan
Public Accountants & Consultants

KPMG.com/socialmedia



**Document Classification: KPMG Public**