الفصل الثامن

القواعد المنظمة لخدمات ترميز البطاقات على تطبيقات الأجهزة الإلكترونية داخل جمهورية مصر العربية[1]

مقدمة

تهدف هذه القواعد إلى تحديد إطار عمل البنوك وكافة الأطراف المشاركة في البنية التحتية لتقديم خدمات ترميز بطاقات الدفع الإلكترونية وذلك لإتاحة أقصى قدر من المرونة والأمان وتقديم الخدمات المصرفية الملائمة لكافة فئات المجتمع، بهدف نشر وسائل الدفع الإلكترونية وتحقيق الشمول المالي.

تعريفات عامة

يكون لكل من الكلمات والعبارات الآتية المعنى المبين لها أدناه أينما وردت في هذه القواعد:

ترميز البطاقات **Cards Tokenization**	**استبدال بيانات البطاقة الفعلية برمز فريد يسمى "الرمز"، ويكون ممثلا لمجموعة من البيانات مثل رقم البطاقة وطالب الرمز (Token Requestor).**
مقدم خدمات الترميز **Token Service Provider** **"TSP"**	**أي من الهيئات التي تتواجد داخل منظومة المدفوعات والمرخص لها من قبل البنك المركزي المصري والتي تختص بإصدار وادارة الرموز.**
طالب الرمز **Token Requestor**	**الجهات التي تطلب ترميز البطاقات من مقدم خدمات الترميز عبر القنوات والتطبيقات الإلكترونية.**
واجهة الترميز الموحدة للبنوك المُصدرة **Unified Issuer TSP Interface**	**الواجهة الموحدة التي تعمل على الربط بين كلاً من البنوك المُصدرة للبطاقات والشبكات صاحبة علامة القبول وذلك بغرض إدارة انشاء الرموز لكافة البطاقات المصدرة داخل جمهورية مصر العربية.**
التطبيقات الإلكترونية لمُصنعي الأجهزة الذكية **Original Equipment Manufacturer Wallet** **"OEM Wallet"**	**تطبيقات ترميز البطاقات التي يتم إصدارها من جانب مصنعي الأجهزة الإلكترونية على سبيل المثال لا الحصر (Apple Pay, Google Pay, Samsung Pay).**
التطبيقات الإلكترونية للبنوك المُصدرة او مقدمي خدمات الدفع **Host Card Emulation Wallet**	**تطبيقات ترميز البطاقات على الأجهزة الإلكترونية التي يتم إصدارها من جانب البنوك المُصدرة او مقدمي خدمات الدفع.**

[1] كتاب السيد / محافظ البنك المركزي المصري بتاريخ 8 مارس 2023

	"HCE Wallet"
أدوات الدفع الإلكترونية	**هي الأدوات المصرفية التي تتم إتاحتها من قبل البنوك المُصدرة لاستخدامها في عمليات الدفع الإلكترونية على سبيل المثال لا الحصر البطاقات الإلكترونية.**
البنك المُصدر **Issuer Bank**	**البنك المصرح له من البنك المركزي المصري بإصدار أدوات الدفع الإلكترونية بأنواعها المختلفة مع الشبكات صاحبة علامة القبول للعملاء والتصديق على المعاملات المالية والتحويلات التي تتم باستخدام أدوات الدفع، والتأكد من توافق هذه العمليات مع الضوابط الرقابية الصادرة عن البنك المركزي المصري.**
البنك القابل **Acquirer Bank**	**البنك المصرح له من البنك المركزي المصري بتقديم خدمات القبول الإلكترونية باستخدام أدوات الدفع المختلفة المصدرة من قبل البنوك وإتمام معاملات التسويات والتأكد من توافق هذه العمليات مع الضوابط الرقابية الصادرة عن البنك المركزي المصري.**
وسائل التحقق من حامل البطاقة على الأجهزة الإلكترونية **Consumer Device Cardholder Verification Method "CDCVM"**	**هي الوسائل التي يتم استخدامها للتحقق من حامل البطاقة من خلال الأجهزة الإلكترونية وذلك باستخدام أحد البدائل التالية:** - رقم التعريف الشخصي للجهاز من قبل المستخدم Mobile Phone Passcode. - الرقم السري الذي يقوم المستخدم بإنشائه. - الخصائص الحيوية للمستخدم Biometric User Authentication مثل (بصمة العين / الوجه / الأصبع / الصوت).
الاتصال قريب المدى **Near Field Communication "NFC"**	**هو الاتصال في نطاق قريب من خلال مجموعة من بروتوكولات التواصل والتي تمكن جهازين أو أداتين للتواصل عبر نطاق قريب لا يتعدى 4 سم.**
المخاطر الكامنة **Inherent Risk**	**مستوى المخاطر دون الأخذ في الاعتبار أي من الضوابط الرقابية أو إجراءات المعالجة المنفذة من قبل البنك وتتكون من عنصرين: التأثير واحتمالية الحدوث.**
المخاطر المتبقية **Residual Risk**	**المخاطر التي قد يتعرض لها البنك بعد تنفيذه الضوابط الرقابية أو إجراءات الحد من المخاطر الكامنة.**
القوائم السلبية	**تشمل قوائم الكيانات الإرهابية والإرهابيين المنظمة بموجب القانون رقم ٨ لسنة ٢٠١٥ وتعديلاته، والقوائم الصادرة عن مجلس الأمن التابع للأمم المتحدة ذات الصلة بالإرهاب وتمويله وتمويل انتشار أسلحة الدمار الشامل، وأية قوائم أخرى يعدها البنك أو يرى ضرورة الرجوع إليها ولا يمكن التعامل مع المدرجين بها.**

1. نطاق التطبيق

1-1 تسري هذه القواعد على كافة البنوك العاملة في جمهورية مصر العربية ومقدمي خدمات ترميز البطاقات على تطبيقات الأجهزة الإلكترونية المرخص لهم من قبل البنك المركزي، وتعتبر هذه القواعد والضوابط هي الحد الأدنى اللازم على البنوك ومقدمي خدمات ترميز البطاقات وعليهم ألا يكتفوا بذلك وأن يتم التأكد من اتخاذ كافة ما يلزم نحو إدارة المخاطر المرتبطة بتقديم هذا النوع من الخدمات.

2-1 تسري هذه القواعد على تقديم خدمات ترميز البطاقات على تطبيقات الأجهزة الإلكترونية وذلك مع الأخذ بعين الاعتبار الضوابط والتعليمات الرقابية ذات الصلة والسابق صدورها عن البنك المركزي المصري وتعديلاتها وكذا الضوابط الرقابية في شأن مكافحة غسل الاموال الصادرة عن البنك المركزي المصري وإجراءات العناية الواجبة الصادرة عن وحدة مكافحة غسل الأموال وتمويل الإرهاب وقانون مكافحة غسل الأموال رقم 80 لسنة 2002 وتعديلاته ولائحته التنفيذية وتعديلاتها. وكذا الالتزام بالقواعد والمواصفات الفنية لتقديم تلك الخدمات وتحديثاتها الصادرة عن شركة بنوك مصر والمعتمدة من قبل البنك المركزي المصري.

2. إدارة مخاطر خدمات ترميز البطاقات على تطبيقات الأجهزة الإلكترونية

1-2 المخاطر المرتبطة بخدمات ترميز البطاقات على تطبيقات الأجهزة الإلكترونية

يقترن تقديم خدمات ترميز البطاقات على تطبيقات الأجهزة الإلكترونية بالعديد من المخاطر، والتي لا تعتبر جديدة على البنوك مثل (مخاطر التشغيل، مخاطر عدم الالتزام، مخاطر السمعة والمخاطر الإستراتيجية) الموضحة في تعليمات- إدارة مخاطر التشغيل وفقاً لإصلاحات بازل 3 ديسمبر 2017 الصادرة في 4 يناير 2022، والرقابة الداخلية في البنوك، وكذا ضوابط مزاولة العمليات المصرفية الإلكترونية وإصدار وسائل دفع لنقود إلكترونية، إلا أن خصائص خدمات ترميز البطاقات قد تزيد من درجات المخاطر بالإضافة إلى خلق تحديات جديدة لإدارة تلك المخاطر والتي يتعين على كافة الجهات المعنية بتقديم تلك الخدمات وضع الأطر والضوابط اللازمة لإدارة والحد من تلك المخاطر، وفيما يلي بعض الأمثلة ذات الصلة المرتبطة بتقديم الخدمة المذكورة:

1-1-2 مخاطر عدم الالتزام، ومنها على سبيل المثال لا الحصر:

- الأساليب/الإجراءات الواجبة التي يستخدمها البنك للتحقق من هوية العملاء حائزي أدوات الدفع الإلكترونية المصدرة من قبل البنك.
- عملية التصديق على المعاملات المالية.

2-1-2 مخاطر السمعة ومنها على سبيل المثال لا الحصر:

- انعدام الثقة نتيجة وجود عمليات دفع غير مصرح بها على رموز بطاقات العملاء.

- الفشل في تقديم خدمات يمكن الاعتماد عليها نتيجة لتكرار تعطل الخدمة أو طول مدة توقفها أو أي خلل أو خطأ ينشأ عن ذلك.

3-1-2 مخاطر أمن المعلومات ومنها على سبيل المثال لا الحصر:

- مخاطر حجب الخدمة وتأثيرها سلبيا على سير العمل.
- مخاطر تسريب البيانات وتأثيرها سلبيا على السمعة والوقوع تحت طائلة القانون.
- مخاطر سلامة بيانات العميل وعدم التلاعب بها بما يضمن نزاهة سير العمل.

4-1-2 مخاطر الاحتيال

- والتي تتمثل في أي فعل عمدي يهدف الى الحصول على منفعة للنفس أو للغير وينتج عنه خسائر مادية أو معنوية وذلك بالمخالفة لأحكام القانون أو التعليمات واللوائح المنظمة.

2-2 مسئوليات والتزامات مجلس الإدارة والإدارة العليا

يتولى مجلس الإدارة بالبنك مسئولية اعتماد استراتيجية العمل الخاصة بتقديم خدمات ترميز البطاقات الموضوعة من قبل الإدارة العليا، واتخاذ قرار استراتيجي واضح بشأن تلك الخدمات وذلك وفقاً لتعليمات حوكمة البنوك الصادرة في 23 أغسطس 2011 السابق صدورها عن البنك المركزي وتعديلاتها، واعتماد السياسة الخاصة بتقديم الخدمة على أن يتم التأكد مما يلي:

1-2-2 وضع سياسات وإجراءات واضحة لتحديد قدرة البنك على تقبل المخاطر المصاحبة للمعاملات الناشئة عن خدمات ترميز البطاقات على تطبيقات الأجهزة الإلكترونية وكذا الحد من تلك المخاطر على أن يتم تقييم تلك السياسة على الأقل مرة سنويا، وتحديثها بصوره دورية على أن تشمل تلك السياسة على الأخص النقاط الأتية:

- التصديق على المعاملات.
- التسويات.
- عمليات الاعتراض (Disputes).
- رد العمليات (Refunds).
- الاحتيال (Fraud).
- مستوي الخدمة وكفاءتها.

2-2-2 ضرورة أن تكون منهجية التأمين قائمة على تحليل المخاطر والتهديدات الخاصة، مع الأخذ في الاعتبار المخاطر الكامنة (Inherent Risk)والضوابط الرقابية التعويضية (Compensating Controls)من أجل الوصول لمستوى من المخاطر المتبقية (Residual Risk)التي تقع ضمن مستويات المخاطر المقبولة.

3-2-2 الإشراف على التطوير والصيانة المستمرة للبنية التحتية وأنظمة التأمين الخاصة بها وكذلك أدوات المراقبة والمتابعة المستمرة للرقابة الأمنية التي توفر الحماية المناسبة لنظم وبيانات

المعاملات التي يتم تنفيذها من البطاقات التي تم ترميزها على تطبيقات الأجهزة الإلكترونية من أي تهديدات داخلية أو خارجية، ومن أجل ضمان كفاية وفعالية المعاملات المالية، يجب على الإدارة العليا التأكد من اتخاذ الإجراءات الآتية:

2-2-3-1 تحديد مسئوليات واضحة خاصة بالإشراف على وضع وإدارة سياسات الأمن السيبرانى الخاصة بالبنك.

2-2-3-2 التأكد من توفير الحماية اللازمة لمنع دخول الأشخاص غير المصرح لهم العمل على أنظمة البنية التحتية، والتي تتضمن كافة الأنظمة الحيوية وخوادم النظام وقواعد البيانات والتطبيقات والاتصالات، وأنظمة التأمين الخاصة بالخدمة.

2-2-3-3 مراجعة واعتماد الجوانب الرئيسية لأنظمة تكنولوجيا المعلومات والأمن السيبرانى الخاصة بالبنك بما يشمل المراجعة الدورية لعمليات اختبار البنية التحتية وأنظمة الأمن السيبرانى- على سبيل المثال إجراء اختبار الاختراق مرة واحدة سنويا بما في ذلك المتابعة المستمرة للتطورات والتحديثات لأنظمة البنية التحتية، التطبيقات، وأنظمة الأمن السيبرانى في هذا المجال.

2-3ضوابط مكافحة غسل الأموال وتمويل الإرهاب

يجب على البنوك التي تقدم أو تقبل خدمات ترميز البطاقات على تطبيقات الأجهزة الإلكترونية الالتزام بما يلي:

- الالتزام بقانون مكافحة غسل الأموال الصادر بالقانون رقم 80 لسنة 2002 وتعديلاته ولائحته التنفيذية وتعديلاتها والضوابط الرقابية للبنوك في شأن مكافحة غسل الأموال وتمويل الإرهاب الصادرة عن البنك المركزي المصري، وإجراءات العناية الواجبة بعملاء البنوك السارية الصادرة عن وحدة مكافحة غسل الأموال وتمويل الإرهاب، وآلية تنفيذ قرارات مجلس الأمن الخاصة بالعقوبات المالية المستهدفة الصادرة عن وحدة مكافحة غسل الأموال وتمويل الإرهاب.
- اتباع الارشادات الصادرة للبنوك في وضع آليه لتنفيذ العقوبات المالية المستهدفة والتجميد الفوري وكذا إرشادات المعنيين بالتنفيذ في شأن المدرجين بقوائم الحظر وفقا للقوائم المحدثة المنشورة على موقع وحدة مكافحة غسل الأموال تحت بند القوائم السلبية.
  - **www.mlcu.org.eg**
- وجود آلية لرصد العمليات التي يشتبه في وجود غسل الأموال او تمويل الإرهاب والتأكد من ربط الأنظمة الخاصة بالمعاملات بأنظمة مكافحة غسل الأموال وتمويل الإرهاب / أنظمة الكشف عن العملاء المدرجين بالقوائم السلبية.

- ايلاء عناية كافية بما يتفق مع طبيعة الخدمة من المؤشرات الاسترشادية للتعرف على العمليات التي يشتبه في أنها تتضمن غسل أموال أو تمويل إرهاب الواردة بالضوابط الرقابية للبنوك في شأن مكافحة غسل الأموال وتمويل الإرهاب الصادرة عن البنك المركزي المصري.
- في حالة الاشتباه في أية عمليات تتم باستخدام البطاقات التي تم ترميزها على تطبيقات الأجهزة الإلكترونية وتتضمن غسل أموال أو متحصلات جريمة أصلية أو تمويل إرهاب يجب القيام على الفور بإخطار وحدة مكافحة غسل الأموال وتمويل الإرهاب بشأنها، وذلك وفقا لأحكام قانون مكافحة غسل الأموال الصادر بالقانون رقم 80 لسنة 2002 ولائحته التنفيذية وتعديلاتها.
- متابعة موقع الوحدة بشكل دوري للتعرف على التحديثات على القوائم السلبية سواء بالحذف أو الإضافة أو التعديل.
- الاحتفاظ بالسجلات والمستندات الخاصة بالعملاء والعمليات وفقاً لما ورد بكل من قانون مكافحة غسل الأموال الصادر بالقانون رقم 80 لسنة 2002 وتعديلاته ولائحته التنفيذية وتعديلاتها والضوابط الرقابية للبنوك في شأن مكافحة غسل الأموال وتمويل الإرهاب الصادرة عن البنك المركزي المصري.

3. القواعد العامة المنظمة للبنوك لتقديم خدمات ترميز البطاقات على تطبيقات الأجهزة الإلكترونية.

3-1. الضوابط الخاصة بواجهة الترميز الموحدة للبنوك المُصدرة (Unified Issuer TSP Interface)

3-1-1 تقوم شركة بنوك مصر للتقدم التكنولوجي بدور مقدم خدمة واجهة الترميز الموحدة للبنوك المُصدرة للبطاقات داخل جمهورية مصر العربية.

3-1-2 تقوم واجهة الترميز الموحدة للبنوك المُصدرة بالربط بصورة مؤمنة يراعى من خلالها سرية البيانات والمعلومات التي يتم تبادلها بين كلاً من البنوك المُصدرة للبطاقات والشبكات صاحبة علامة القبول وذلك بغرض إدارة انشاء الرموز لكافة البطاقات المصدرة داخل جمهورية مصر العربية مع الأخذ على سبيل المثال لا الحصر في الاعتبار ما يلي:

- أليات التشفير المستخدمة لحماية الشبكات والبيانات طبقا لأفضل الممارسات العالمية.
- تأمين واجهة برمجة التطبيقات (API) طبقا للممارسات العالمية للحد من المخاطر الناتجة عن الثغرات المرتبطة بها مع اجراء اختبارات الاختراق الخاصة بها.
- القيام باختبارات الاختراق (Infrastructure Penetration Test) للتأكد من تأمين شبكات الربط وأنظمة البنية التحتية ضد اي اختراق.

3-1-3 تكون واجهة الترميز الموحدة للبنوك المُصدرة هي المسئولة عن إتمام عملية انشاء الرمز (Token Provisioning) مع جميع مقدمي خدمات الترميز (Token Service Providers TSPs) المعتمدين من الشبكات صاحبة علامة القبول المرخص لها بالعمل داخل جمهورية مصر العربية.

4-1-3 يتم إصدار رمز إضافي (Auxiliary Token) لكافة البطاقات المصدرة داخل جمهورية مصر العربية والتي تحمل علامة قبول دولية (International Card Scheme):

- الرمز الاول: صادر عن الشركات صاحبة علامة القبول الدولية.
- الرمز الإضافي (Auxiliary Token): صادر عن الشركة صاحبة علامة القبول الوطنية "ميزة".

5-1-3 يتم اصدار رمز واحد فقط لا غير يخص منظومة الدفع الوطنية لبطاقات "ميزة".

2-3. التزامات البنك المُصدر (Issuer Bank) لأدوات الدفع الإلكترونية

1-2-3 يجب على البنوك المُصدرة استخدام واجهة الترميز الموحدة للبنوك المُصدرة (Issuer TSP Unified Interface) للربط مع الشبكات صاحبة علامة القبول.

2-2-3 التأكد من إصدار رمز إضافي (Auxiliary Token) لكافة البطاقات المصدرة داخل جمهورية مصر العربية والتي تحمل علامة قبول دولية (International Card Scheme):

- الرمز الاول: صادر عن الشركات صاحبة علامة القبول الدولية.
- الرمز الإضافي: صادر عن الشركة صاحبة علامة القبول الوطنية "ميزة".

3-2-3 يلتزم البنك المُصدر الراغب في تفعيل خدمة الترميز بإتاحتها لكافة الشبكات صاحبة علامة القبول المتعاقد معها البنك، وفي حالة قيام البنك بتفعيل الخدمة لأحد الشبكات، يلتزم البنك بإستكمال تفعيل الخدمة لكافة الشبكات المتعاقد معها البنك خال عام من تاريخ تفعيل البنك للخدمة حال تفعيل الشبكة صاحبة علامة القبول للخدمة.

4-2-3 البنك المُصدر هو المسؤول عن إجراءات التعرف على هوية العميل (Identification & Verification) والتحقق من بيانات أدوات الدفع الإلكترونية الخاصة بعملائه من خلال أي من التطبيقات التكنولوجية المعتمدة وفق الضوابط والإجراءات المعتمدة من قبل البنك المركزي المصري.

5-2-3 يجب التحقق من هوية حامل أداة الدفع الإلكترونية المصدرة من قبل البنك بأي من وسائل التحقق وفقا لتقييم المخاطر لدي البنك والتي تشمل على سبيل المثال وليس الحصر (إرسال رسالة نصية تحتوي على الرقم السري المستخدم لمرة واحدة (One Time Password OTP) للهاتف المسجل لدي البنك) وذلك حال طلب ترميز البطاقات المصدرة من قبل البنك من خلال تطبيقات ترميز البطاقات عبر الأجهزة الإلكترونية.

6-2-3 المدة القصوى لصلاحية الرمز هي 5 سنوات وعلى البنك المُصدر للبطاقة وضع الاجراءات التي تضمن أن يتم إعادة عملية التحقق من العميل بعد تلك الفترة وألا ترتبط تلك الفترة بصلاحية البطاقة الاصلية إلا في الحالات الإستثنائية التي يقرها البنك المركزي المصري.

7-2-3 يتعين على البنك في ضوء تقييمه للمخاطر المرتبطة بالخدمة وضع الحدود المناسبة لقيم وعدد المعاملات اليومية والشهرية لكل رمز وفقا لتقييم المخاطر لدي البنك.

8-2-3 قدرة الأنظمة الخاصة بالبنك المُصدر على التمييز والتعامل مع الحركات الواردة بوسائل التحقق من حامل البطاقة على الأجهزة الإلكترونية (Consumer Device Cardholder Verification Method - CDCVM).

9-2-3 يجب على البنك المُصدر عدم تجاوز الحدود القصوى للمعاملات اللاتلامسية محلياً التي تتم بدون التحقق من حامل البطاقة (CVM Limit) والصادرة عن البنك المركزي المصري، ويستثنى من تلك الحدود المعاملات التي تتم خارج جمهورية مصر العربية مع قيام كل بنك بوضع الحد الأقصى المناسب له وفقا لتقييم المخاطر لدي البنك.

10-2-3 يتعين على البنك المُصدر تحديد الحد الأقصى للقيم الاجمالية وعدد المعاملات اللاتلامسية المتتالية التي تتم دون إتمام اجراءات التحقق من حامل البطاقة (CVM Limit) وفقا لتقييم المخاطر لدي البنك، وحال تخطي العميل لاي من تلك الحدود يتم طلب التحقق من حامل البطاقة باستخدام وسائل التحقق من حامل البطاقة على الأجهزة الإلكترونية (CDCVM) او ادخال الرقم السري للبطاقة (PIN).

11-2-3 يتعين على البنك المُصدر تقييم المخاطر المرتبطة بالخدمة وبالأخص تقييم تأمين المعاملات المنفذة من مختلف الوسائل الإلكترونية بما يشمل إمكانية عدم إتاحة الخدمة إلا من خلال مصنعي الهواتف المحمولة الموثوق بهم وبعد الانتهاء من التقييم الفني الذي يضمن أمان المعاملات المنفذة من خلالهم بإستخدام وسائل التحقق من حامل البطاقة على الأجهزة الإلكترونية (CDCVM) وإمكانية وضع الحدود المناسبة لتلك المعاملات بما يتوافق مع تقييم المخاطر لدي البنك.

12-2-3 في حالة المعاملات التي تتجاوز حد التحقق من حامل البطاقة (CVM Limit) وفي حالة عدم تمكن نقاط البيع الإلكترونية من التعرف على وسيلة التحقق من حامل البطاقة على الأجهزة الإلكترونية (CDCVM) فيجب إدخال الرقم السري او رفض الحركة.

13-2-3 يتعين على البنك المُصدر وضع تدابير فعالة للرقابة المستمرة لضمان سرعة اكتشاف أي معاملات غير عادية على سبيل المثال وليس الحصر (محاولات تسجيل البطاقات الخاطئة لأكثر من مرة، فشل محاولات التحقق من حامل البطاقة لأكثر من مرة،.. الخ) ويجب على البنوك في تلك الحالات أن تقوم بالتحقق من ذلك مع أصحاب هذه البطاقات التي تتم عليها هذه

المعاملات أو الأنشطة في أسرع وقت ممكن وإخطار الجهات المختصة وإخطار العملاء فوراً في حالة رصد أي أنشطة غير معتادة على بطاقاتهم.

14-2-3 التأكد من وجود الاتفاقيات التعاقدية المناسبة مع أي من الأطراف المشاركة في تقديم خدمة ترميز البطاقات والتي تشمل ما يلي على سبيل المثال لا الحصر:

- التأكد من عدم إدراج الشريك / الطرف الخارجي او (الأشخاص الطبيعيون الذين يملكون حصص مسيطرة على الشركة والتي تمثل25 % أو أكثر أو الأشخاص الطبيعيون الذين يسيطرون على الشركة من خلال أية وسائل أخري) بأي من قوائم الحظر وفقا للتعريف السابق ذكره.
- تأمين سلامة وسرية وإتاحة بيانات حامل البطاقة التي تتم معالجتها أو تخزينها أو نقلها بواسطة مقدم الخدمة.
- تحديد المسئوليات التعاقدية لكافة الأطراف الخاصة باتفاقيات التعهيد أو الشراكة أو الوكالة بوضوح ومنها على سبيل المثال:
  - يتم تحديد مسئوليات توفير المعلومات وتلقيها بشكل واضح.
  - اتفاقية لعدم الإفصاح عن المعلومات السرية لأطراف خارجية واتفاقية مستوى الخدمة والتي تشمل على سبيل المثال لا الحصر: تحديد الأدوار والمسئوليات والوقت المطلوب لتنفيذ الخدمة وإجراءات وبيانات التصعيد والعقوبات في حال عدم الالتزام، هذا بالإضافة إلى البنود التي تحفظ حق البنك في تدقيق الخدمات أو الاعتماد على تقارير التدقيق المعتمدة (الصادرة عن جهات تدقيق معتمدة).
  - خضوع كافة النظم والعمليات التي تتم من خلال عملية التعهيد أو الوكالة لنظام إدارة المخاطر وسياسات الخصوصية وأمن المعلومات التي تتفق مع المعايير الخاصة بالبنك.
  - توفير كافة تقارير التدقيق والتقييم لمفتشي قطاعي الرقابة والإشراف والأمن السيبرانى بالبنك المركزي المصري.
  - أن تتسم إجراءات فسخ/إنهاء التعاقد بالفاعلية، كما يجب أن تضمن هذه الإجراءات الحفاظ على استمرارية العمل وسلامة البيانات وكذلك نقلها والتخلص منها.

15-2-3 استيفاء موافقات قطاعي الالتزام والمخاطر بالبنك مع تنفيذ كافة الشروط والأحكام التي يتم وضعها من جانبهم للحد من المخاطر المرتبطة بتلك التعاملات.

16-2-3 وضع الإجراءات والقواعد المناسبة لإلغاء او ايقاف الرموز والمفاتيح المرتبطة بها على الفور وفق طلب العميل أو في حال أي حدث آخر قد يعرض الرموز للاستخدام غير المصرح به مع تحديد مسئوليات كل طرف.

3-2-17 يجب على البنك تحديد الآلية الخاصة بعمليات الاعتراضات التي تخص تلك النوعية من المعاملات.

3-2-18 في حالة استخدام تطبيقات ترميز البطاقات عبر الأجهزة الإلكترونية، يقوم البنك المُصدر بقبول معاملات الصراف الآلي المنفذة مثل (السحب النقدي / الإيداع النقدي / الاستعلام عن الرصيد.... الخ) بعد التحقق من حامل البطاقة عن طريق الرقم السري للبطاقة في كافة المعاملات.

3-2-19 ضرورة إخطار العملاء بالمعاملات التي تمت باستخدام الرموز على أدوات الدفع الإلكترونية بصوره واضحة من خلال رسائل نصية أو أية وسيلة فعالة أخرى يراها البنك مناسبة.

3-2-20 ضرورة وجود حملات التوعية اللازمة من قبل البنك للعملاء بكيفية التعامل مع تلك الخدمة المقدمة مع ضرورة توضيح المخاطر المرتبطة باستخدام هذه الخدمة وكيفية التعامل معها.

3-2-21 توفير أدوات الدعم الفني الكاملة للعملاء بما يتناسب مع مستوي أداء الخدمات المصرفية.

3-2-22 ضرورة وجود حملات التوعية والتدريب اللازمة لموظفي البنك المسؤولين عن تشغيل ودعم خدمة ترميز البطاقات.

3-2-23 إخطار العملاء بالرسوم الخاصة بتقديم خدمة ترميز البطاقات الخاصة بالبنك بصوره واضحة إن وجدت.

3-2-24 يلتزم البنك بإرسال كافة التقارير الخاصة بالمعاملات التي تتم باستخدام الرموز للبنك المركزي المصري.

3-2-25 يلتزم البنك المُصدر بالحصول على ترخيص من البنك المركزي المصري لإتاحة الدفع عبر تطبيقات ترميز البطاقات على الأجهزة الإلكترونية للبطاقات المصدرة بواسطته لكل تطبيق على حده سواء كان التطبيق مملوكاً للبنك أو لأحد مصنعي الأجهزة الإلكترونية وعلى سبيل المثال (Apple Pay، Google Pay، Samsung Pay) أو لأحد مقدمي خدمات الدفع المرخصين من البنك المركزي المصري.

3-2-26 يجب الحصول على موافقة البنك المركزي المصري حال رغبة البنك المُصدر استخدام خدمة ترميز البطاقات في تنفيذ أي معاملات أخري غير معاملات الشراء من خلال التجار على سبيل المثال لا الحصر (التحويلات بين البطاقات).

3- 3. التزامات البنك القابل (Acquirer Bank)

3-3-1 يجب أن تدعم نقاط البيع الإلكترونية جميع وسائل قبول الرموز على سبيل المثال لا الحصر تقنية ال (Near Field Communications - NFC).

3-3-2 ضرورة إتباع المعايير العالمية ISO/IEC 14443 وتحديثاتها في وسائل التواصل الخاصة بالمعاملات اللاتلامسية بين أداة الدفع اللاتلامسية ونقاط البيع الإلكترونية.

3-3-3 يلزم وجود علامة مميزة لنقاط البيع الإلكترونية التي تقبل الدفع باستخدام الأدوات اللاتلامسية.

3-3-4 في حالة المعاملات التي تتجاوز حد التحقق من حامل البطاقة (CVM Limit) وفي حالة عدم تمكن نقاط البيع الإلكترونية من التعرف على وسيلة التحقق من حامل البطاقة على الأجهزة الإلكترونية (CDCVM) فيجب إدخال الرقم السري أو رفض الحركة باستثناء الرموز المُصدرة لبطاقات من بنوك خارج جمهورية مصر العربية.

3-3-5 يجوز للبنك القابل وضع الحدود القصوى للمعاملات اللاتلامسية للرموز والتي يتم قبولها عن طريق وسائل التحقق من حامل البطاقة على الأجهزة الإلكترونية (CDCVM) ويتم طلب ادخال الرقم السري للبطاقة وفقا ودراسة المخاطر المتعلقة بالخدمة.

3-3-6 على البنك توفير التدريب الكافي للتجار الذين لديهم نقاط البيع الإلكترونية على تعدد وسائل التحقق من حامل البطاقة على الأجهزة الإلكترونية (CDCVM) التي يمكن استخدامها أثناء عملية الشراء.

3-3-7 ضمان وضع نقاط البيع الإلكترونية التي تعمل بتلك الخاصية مواجهة مباشرة للعميل وبعيدة عن أي مصدر للكهرباء أو مصدر معدني أخر يمكن أن تؤثر الإشارات الخاصة به على عملية الدفع بحيث يكون الحد الأقصى بين أداة الدفع اللاتلامسية والماكينة لإتمام العملية هو 4 سم فقط لا غير.

3-3-8 لا يجوز الحصول على توقيع العميل على أي من المعاملات اللاتلامسية ويستثني من ذلك الحركات التي يتم تنفيذها باستخدام أدوات دفع لاتلامسية مُصدرة من خارج جمهورية مصر العربية.

3-3-9 ضرورة وجود حملات التوعية اللازمة من قبل البنك للتجار بكيفية التعامل مع الأنواع المختلفة لأدوات الدفع اللاتلامسية، وأن تتضمن تلك الحملات توعيةً للتجار بأدوات الدفع الجديدة المستحدثة من خلال تطبيقات ترميز البطاقات على الأجهزة الإلكترونية.

3-3-10 يقوم البنك بوضع الإجراءات التي تضمن عدم تكرار الحركات على العملاء من قبل نقاط البيع الإلكترونية الخاصة بالتجار بطريقة خاطئة.

3-3-11 يجب أن تقوم نقاط البيع الإلكترونية برفض عملية الشراء في حالة وجود أكثر من أداة دفع لاتلامسية قريبة من الماكينة وذلك لضمان أن حامل أداة الدفع اللاتلامسية لم يقم بالدفع بالأداة الخاطئة (Collision) أثناء عملية الشراء نتيجة تداخل الإشارات الخاصة بالبطاقات.

12-3-3 يوفر البنك التدريب اللازم للموظفين والخاص بأدوات الدفع اللاتلامسية لكي يتم الرد على استفسارات العملاء ودعمهم بطريقة صحيحة.

13-3-3 قيام البنك قبل تفعيل الخدمة بتقييم المخاطر الناتجة عن تفعيل قبول المدفوعات اللاتلامسية لدى كل تاجر.

14-3-3 تمرير المعاملات الناشئة عن البطاقات المُصدرة داخل جمهورية مصر العربية والتي تحمل علامة قبول دولية باستخدام الرمز الإضافي لشبكة منظومة الدفع الوطنية «ميزة » فقط للمعاملات التي صدر بشأنها تعليمات من البنك المركزي المصري لتمريرها محلياً على سبيل المثال لا الحصر (معاملات نقاط البيع الحكومية ومعاملات ماكينات الصراف الآلي).

15-3-3 يمكن للبنك القابل تفعيل السداد عن طريق تطبيقات الدفع الإلكترونية في معاملات التجارة الإلكترونية (E-Commerce) بعد الحصول على موافقة البنك المركزي المصري.

4-3. التزامات الشبكات صاحبة علامة القبول

1-4-3 الربط مع شركة بنوك مصر كمقدم خدمة واجهة الترميز الموحدة للبنوك المُصدرة (Unified Issuer TSP Interface).

2-4-3 ضمان سلامة عملية إنشاء الرمز الخاص بالبطاقة في جميع الأوقات.

3-4-3 وضع آلية للتدقيق بصوره دورية على أنظمة الترميز لكافة الأطراف المشاركة في تقديم خدمات ترميز البطاقات للعملاء.

4-4-3 وضع الإجراءات التي تكفل عدم اكتشاف رقم بطاقة الدفع الإلكترونية الفعلي من الرمز والعكس من قبل أي جهة باستثناء الشبكات صاحبة علامة القبول الخاصة بالبنك المُصدر للبطاقة عن طريق قاعدة بيانات الرمز (Token Vault).

5-4-3 تحديد أليات حل المنازعات.

6-4-3 ضمان المراقبة لاكتشاف أي عطل أو سلوك مشبوه أو وجود نشاط غير مصرح به في عملية الترميز وتنفيذ إجراءات لتنبيه جميع الأطراف المعنيين.

7-4-3 أن تسمح الشبكة بمعالجة رد المبالغ المدفوعة واسترداد الأموال دون الحاجة إلى وصول البنك القابل او احتفاظه برقم البطاقة الفعلي قبل الترميز.

8-4-3 توفير خدمات الاعتماد والمصادقة اللازمة لتقديم الخدمات بصورة آمنة.

5-3. التزامات مقدم خدمات الترميز (Token Service Provider "TSP")

1-5-3 يحق للشبكات صاحبة علامة القبول تقديم خدمات الترميز مباشرةً لأعضاء الشبكة الخاصة بها، كما يحق لها الترخيص لأحد مقدمي خدمات الدفع لتقديم خدمة الترميز لأعضاء تلك الشبكة، على أن يقوم البنك المُصدر الراغب في الاستفادة من خدمات مقدم الخدمة الحصول على موافقة البنك المركزي المصري على تعهيد تلك الخدمة.

2-5-3 تنفيذ طلبات الترميز الواردة من كل من البنك المُصدر و/أو طالب الرمز، وكذلك تنفيذ طلبات فك الترميز الواردة من خلال الشبكات صاحبة علامة القبول المعتمدة.

3-5-3 يجب ألا يكشف رمز البطاقة عن رقم البطاقة الفعلي أو البيانات الأخرى مثل تاريخ الانتهاء.

4-5-3 ضرورة أن يحتفظ الرمز بجميع سمات البطاقة الاصلية بما في ذلك نوع البطاقة، وعلى سبيل المثال (بطاقات الخصم أو الائتمان).

5-5-3 يخضع نظام الترميز لكافة معايير تأمين بيانات بطاقات الدفع الإلكترونية (Payment Card Industry Token Service Provider "PCI-TSP") ويجب تأمين قاعدة بيانات البطاقات لحماية بيانات حامل البطاقة في ضوء احتفاظ النظام بكافة البيانات الخاصة بحاملي البطاقات المصدرة، ويجب أن يكون معزولًا عن كافة الانظمة غير المتوافقة مع معايير التأمين المشار اليها بهذا البند.

6-5-3 التأكد من تأمين ارقام البطاقات الفعلية (PAN) عند حفظ تلك البيانات.

7-5-3 يجب استخدام قواعد ومفاتيح التشفير المتوافقة مع معايير تأمين بيانات ومعاملات بطاقات الدفع الإلكترونية (PCI DSS) المتعارف عليها وعدم استخدام أدوات تشفير ضعيفة أو منتهية الصلاحية.

8-5-3 ضرورة تأمين الاتصالات بين التطبيق الطالب للرمز ونظام الترميز لمنع اعتراض أو التقاط بيانات حامل البطاقة.

9-5-3 أن يكون نظام الترميز قادرًا على التمييز بين بيانات حامل البطاقة ذات الرمز وبين بيانات حامل البطاقة الاصلية قبل الترميز.

10-5-3 تظل بيانات حامل البطاقة مشفرة من النقطة التي تدخل فيها إلى النظام حتى النقطة التي يتم فيها تحويلها إلى رمز لتحقيق اعلي معايير الأمان.

11-5-3 يجب إنشاء الرموز باستخدام نطاق رموز (Token BIN Ranges) مختلف عن نطاق ارقام البطاقات الفعلية (Actual PAN BIN Ranges) لضمان عدم وجود إمكانية لإنشاء رموز الدفع التي تتشابه مع ارقام البطاقات الفعلية.

12-5-3 التأكد من عدم امكانية استرداد رقم البطاقة الأصلي (PAN) من الرمز حسابيا.

13-5-3 الا يحتوي أي رد على التاجر اثناء عملية الدفع على رقم البطاقة الفعلي قبل الترميز.

14-5-3 يجب ان يوفر مقدم خدمة الترميز للبنك المُصدر الأليات التي تتيح له إمكانية إدارة الرموز بما يشمل:

- إلغاء التنشيط / إعادة التنشيط / الحذف.
- الحصول على إحصائيات حول الرموز والمعاملات.
- الاستعلام عن المعاملات.
- تحديث بيانات البطاقة الأصلية في حالة إعادة إصدار البطاقة أو إصدار بطاقة جديدة.

3- 6. مسؤوليات طالب الرمز (Token Requestor)

3-6-1 يمكن للبنك المُصدر اتاحة الدفع عبر تطبيقات ترميز البطاقات على الأجهزة الإلكترونية سواءً أن تكون تلك الخدمة مدمجة داخل تطبيق الهاتف البنكي الخاص بالبنك المُصدر أو من خال تطبيق منفصل مخصص لتلك الخدمة وذلك على أن يكون خادم إدارة تطبيقات ترميز البطاقات مستضاف لدي البنك (Locally Hosted Wallet Management Server) أو لدي أحد مقدمي الخدمة المعتمدين من قبل البنك المركزي المصري.

3-6-2 يمكن لمقدمي خدمات الدفع او مصنعي الأجهزة الإلكترونية على سبيل المثال (Apple Pay، Google Pay، Samsung Pay) توفير تطبيقات لترميز البطاقات المصدرة من البنوك (HCE & OEM Wallets) وذلك بعد الحصول على موافقة البنك المركزي المصري من قبل البنك المُصدر للبطاقات الراغب في تفعيل الخدمة من خلال التطبيقات الخاصة بهم، على ان يتم الالتزام بإبرام تعاقد مع كل من الشبكات والبنوك المُصدرة للبطاقات والمشتركة بالنظام، وفي كافة الأحوال يلتزم طالب الرمز بإبرام تعاقد مع شبكة منظومة الدفع الوطنية "ميزة" وذلك لكي يتمكن من إصدار رمز إضافي (Auxiliary Token) لكافة البطاقات الدولية.

3-6-3 في كافة الأحوال يلتزم البنك المُصدر بالحصول على ترخيص من البنك المركزي المصري لإتاحة الدفع عبر تطبيقات ترميز البطاقات على الأجهزة الإلكترونية للبطاقات المصدرة بواسطته لكل تطبيق على حده سواء كان التطبيق مملوكاً للبنك أو لأحد مصنعي الأجهزة الإلكترونية وعلى سبيل المثال (Apple Pay، Google Pay، Samsung Pay) أو لأحد مقدمي خدمات الدفع المرخصين من البنك المركزي المصري.

3-6-4 اجراء التعديلات اللازمة للحصول على الرمز الإضافي (Auxiliary Token) لكافة البطاقات التي تحمل علامة قبول دولية وتفعيل الرموز بعد التأكد من الإصدار الناجح للرمز الثنائي (الرمز الخاص بالشركة صاحبة علامة القبول للبطاقة والرمز الخاص بمنظومة الدفع الوطنية "ميزة") دون الاعتماد على أحدهما فقط.

3-6-5 فيما يخص بطاقات الدفع الوطنية "ميزة" يتم اصدار رمز واحد فقط لا غير يخص منظومة الدفع الوطنية "ميزة".

3-6-6 ضرورة ان يقوم تطبيق ترميز البطاقات على الأجهزة الإلكترونية بربط الرمز بجهاز الهاتف المحمول المُصدر للرمز.

3-6-7 يجب ان يكون التطبيق طالب الرمز متوافق مع المعايير والمتطلبات وأفضل الممارسات المصدرة من EMVCO.

3-6-8 يجب أن يوفر تطبيق ترميز البطاقات على الأجهزة الإلكترونية وسائل التحقق من حامل البطاقة على الأجهزة الإلكترونية (CDCVM).

9-6-3 يجب على التطبيق طالب الرمز التأكيد على حامل البطاقة على أهمية ضبط رقم التعريف الشخصي للجهاز من قبل المستخدم (Mobile Phone Passcode) وعدم مشاركته مع أحد قبل إتمام عملية تخزين رمز البطاقة على الجهاز.

10-6-3 في حالة المعاملات التي تتجاوز حد التحقق من حامل البطاقة (CVM Limit) على التطبيق طالب الرمز اجراء التحقق من حامل البطاقة على الأجهزة الإلكترونية (CDCVM) عند إتمام كل عملية دفع على حدي وعدم الاعتماد على أي عملية تحقق من حامل البطاقة سابقة.

11-6-3 يلتزم طالب الرمز بأن تظل بيانات البطاقة الأصلية مشفرة من نقطة إدخال العميل لها من خلال التطبيق المعد لذلك وأثناء تبادلها مع كافة الأطراف الخارجية مع ضرورة عدم الاحتفاظ بتلك البيانات بالمنظومة نهائياً.

12-6-3 إجراء جميع الاختبارات اللازمة على تطبيق ترميز البطاقات على الأجهزة الإلكترونية واجتياز جميع اختبارات الشبكات صاحبة علامة القبول في هذا الشأن.

13-6-3 يلتزم طالب الرمز بموافاة البنك المركزي المصري بتقرير اختبارات الاختراق (Penetration Test Report), وتقارير تقييم نقاط الضعف (Credential vulnerability assessment) على بيئة العمل الفعلية و كذلك الأنظمة البديلة في مركز الطوارئ بما يشمل جميع الأنظمة و التطبيقات و البنية التحتية و أساليب التأمين المتبعة على ان تكون هذه الاختبارات تتم بصورة شاملة تتيح اكتشاف جميع الثغرات و المشاكل الفنية والذي يفيد عدم وجود أي نقاط ضعف عالية أو متوسطة الخطورة عن طريق جهة مستقلة بالإضافة الى تقارير الالتزام بالمعايير (PCI DSS Report on Compliance) ومن ثم الحصول على موافقة البنك المركزي المصري بتفعيل الخدمة، على ان يتم تقديم التقرير المشار اليه إلى البنك المركزي المصري في مدة لا تتجاوز ثلاثة أشهر من تاريخ إصداره والخاصة بكافة الخدمات المذكورة اعلاه.

14-6-3 يكون للعميل الحرية في استخدام او الغاء أي من البطاقات المسجلة في تطبيق طالب الرمز.

15-6-3 ضمان الحفظ الآمن للرموز والمفاتيح المرتبطة بها بواسطة طالب الرمز عند التسجيل الناجح للبطاقة بكافة أنظمة التشغيل وتطبيقات ترميز البطاقات على الأجهزة الإلكترونية المملوكة لطالب الرمز.

7-3. مسؤوليات شركة بنوك مصر

1-7-3 توفير واجهة الترميز الموحدة للبنوك المُصدرة (Unified Issuer TSP Interface) باعتبارها الواجهة الرئيسية والموحدة في التعامل مع الشبكات صاحبة علامة القبول، وإصدار قواعد الربط الفني وتوفير البيئة اللازمة لتقديم خدمات تلك الواجهة وتحديثاتها وذلك بعد استيفاء موافقة البنك المركزي المصري.

2-7-3 تنفيذ أعمال التكامل مع كافة الشبكات الدولية المرخص لها بالعمل بجمهورية مصر العربية وذلك في إطار توفير خدمات واجهة الترميز الموحدة للبنوك المُصدرة.

3-7-3 إصدار الرمز الإضافي الخاص بمنظومة الدفع الوطنية لكافة البطاقات التي تحمل علامة قبول دولية.

4-7-3 إتاحة التقارير اللازمة للبنوك المشاركة بخدمة واجهة الترميز الموحدة للبنوك المُصدرة وخدمة إصدار الرمز الإضافي الخاص بمنظومة الدفع الوطنية.

5-7-3 إدارة المعاملات الناشئة عن البطاقات الدولية الصادرة عن البنوك المحلية باستخدام الرمز الإضافي وذلك فقط للمعاملات التي صدر بشأنها تعليمات من البنك المركزي المصري لتمريرها محلياً على سبيل المثال لا الحصر (معاملات نقاط البيع الحكومية ومعاملات ماكينات الصراف الآلي).

6-7-3 توفير أدوات رقابية وأنظمة للمراجعة الداخلية للتأكد من توافر الضوابط اللازمة لتامين الأنظمة.

7-7-3 الاخذ فالاعتبار كافة القوانين الصادرة عن البنك المركزي المصري وأطر العمل الخاصة بالأمن السيبرانى.

8-7-3 آليات حوكمة تكنولوجيا المعلومات وسبل تعزيزها من سياسات وإجراءات ونظم رقابة وإدارة المخاطر المتعلقة بالأمن السيبرانى.

9-7-3 القيام باختبارات اختراق لأنظمة الشركة وتقييم نقاط الضعف بصفة دورية على ان تتم هذه الاختبارات بصورة شاملة تتيح اكتشاف جميع الثغرات والمشاكل الفنية في التطبيقات وأنظمة البنية التحتية المستخدمة وأي أنظمة وسيطة، وإعداد تقارير عنها وعرضها على مجلس الإدارة أو لجنة الأمن السيبرانى الخاصة بالشركة واخطار البنك المركزي بمخرجات هذه التقارير.

10-7-3 تقديم التقارير الخاصة ب SOC 2 Type 2 الى البنك المركزي المصري.

11-7-3 إعداد السياسات والإجراءات الخاصة بأمن المعلومات ومراجعتها وتحديثها بصفة دورية.

12-7-3 إبلاغ مجلس الإدارة و/ أو لجنة الامن السيبرانى بأي مخاطر جوهرية ذات الصلة بأمن المعلومات.

13-7-3 أجراء تقييم مخاطر الطرف الثالث.

14-7-3 تأمين اتصالات بيانات المحور المركزي (Eco-system) والنظام البيئي التشغيلي للأنظمة المتصلة بالأطراف الخارجية.

15-7-3 توفير التكنولوجيا اللازمة وضوابط الأمن السيبراني لتأمين كافة المعلومات والبيانات المتعلقة بخزينة الرمز (Token Vault) في حالاتها المختلفة من نقل ومعالجة وتخزين وحفظ في نسخ احتياطية والتخلص منها بما يضمن الحفاظ على سرية وسلامة وإتاحة البيانات. في جميع حالاتها بما يتوافق مع الإطار العام للأمن السيبرانى.

16-7-3 يجب ضمان مراقبة ومتابعة حوادث الأمن السيبراني على مدار الساعة مع وضع الأليات والإجراءات التي سيتم اتباعها في هذا الشأن.

17-7-3 يجب ضمان تنفيذ سياسات الاستجابة لحوادث الأمن السيبرانية بما يشمل إجراءات اكتشاف هذه الحوادث وطرق الاستجابة السريعة والتعافي للحد من المخاطر الناتجة عنها.

18-7-3 وضع خطط البرامج التدريبية لمديري الأنظمة ومسؤولي الأمن السيبراني.

19-7-3 وضع خطط البرامج التدريبية الهادفة لزيادة الوعي الأمني لدى جميع موظفي الشركة وبالأخص القائمين على توفير هذه الخدمة للحد من مخاطر هجمات الهندسة الاجتماعية (Social Engineering).

20-7-3 وضع الضوابط الأمنية المتبعة للتحكم في الدخول المصرح على أنظمة البيئة الفعلية وكذلك البنية التحتية الخاصة بهذه الخدمة أو أي أنظمة أخرى قد تؤدى الى اختراق الأنظمة الخاصة بالترميز.

21-7-3 في حاله حدوث أي اختراقات او تسريبات لمعلومات تتعلق بالأمن السيبرانى يتم ابلاغ مركز الاستجابة لطوارئ الحاسب الآلي للقطاع المالي في خلال 6 ساعات.

4. الضوابط الرقابية لإدارة خدمات ترميز البطاقات على تطبيقات الأجهزة الإلكترونية

4-1. سرية وسلامة المعلومات

1-1-4 يتضمن تقديم خدمات ترميز البطاقات على تطبيقات الأجهزة الإلكترونية تداول بيانات سرية عبر تطبيقات ترميز البطاقات على الأجهزة الإلكترونية والشبكة الداخلية للبنك لذلك يجب على البنوك ومقدمي خدمات الترميز استخدام الأساليب المناسبة للحفاظ علي سرية وسلامة المعلومات المتداولة عبر الشبكة الداخلية والخارجية للبنك وذلك بما يتوافق مع متطلبات تأمين بيانات بطاقات الدفع الإلكترونية وكذا التعليمات الصادرة من جانب البنك المركزي المصري.

2-1-4 يجب على البنوك ومقدمي خدمات الترميز اختيار تكنولوجيا التشفير التي تتناسب مع حساسية وأهمية المعلومات وكذا درجة الحماية المطلوبة، وفي هذا السياق يوصى دائما بتبني البنوك لتكنولوجيا التشفير التي تستخدم طرق التشفير المتعارف عليها دولياً، حيث تخضع نقاط القوة في هذه الطرق لاختبارات شاملة. وينبغي أن تطبق البنوك الممارسات السليمة لإدارة مفاتيح التشفير اللازمة لحماية هذه المفاتيح وذلك بما يتوافق مع متطلبات تأمين بيانات بطاقات الدفع الإلكترونية وكذا التعليمات الصادرة من جانب البنك المركزي المصري.

3-1-4 يجب الحد من تخزين بيانات على الذاكرة الداخلية للهاتف المحمول، وفى حالة الاحتفاظ باي بيانات على الهاتف المحمول – للضرورة القصوى – يجب استخدام الوسائل المناسبة لحماية ما تم تخزينه.

4-1-4 يجب بان يقوم تطبيق الهاتف المحمول بتنفيذ أليات كشف كافية تضمن ان الهاتف المحمول ليس عرضة للمخاطر مثل Jailbroken/Rooted على ان تتضمن إجراءات تأمين التطبيقات على سبيل المثال لا الحصر:

- أن يطلب التطبيق الحد الأدنى من مجموعة الصلاحيات المطلوبة.
- حفظ مفاتيح تشفير التطبيق على الأجهزة الذكية بشكل امن.
- أن تكون حزمة التطبيق موقعة رقمياً.
- استخدام التطبيق لقناة اتصال امنة مثل استخدام Certificate/SSL pinning مع التأكد من ان مفاتيح التشفير مدمجة داخل التطبيق.
- ألا يخزن التطبيق أي معلومات على الجهاز تتعلق بمعاملات الدفع أو بيانات العميل بخلاف البيانات اللازمة لعمل التطبيق.
- ألا يقوم التطبيق بتخزين بيانات تسجيل الدخول وإعادة استخدامها (Back-end Authentication Required).
- عدم السماح بتثبيت التطبيقات على أنظمة تشغيل قديمة او منتهية الصلاحية.

5-1-4 يجب أن يتم حماية تطبيقات الهاتف المحمول ضد أي لقطات تلقائية Screenshots والتي يمكن أن تتم عن طريق برامج تجسس تعمل على نفس جهاز الهاتف المحمول حال وجود إمكانية فنية لتطبيقه.

6-1-4 ألا يتم اتصال انظمة البنك المشاركة في خدمات ترميز البطاقات بالشبكة العالمية (الانترنت) أو أي من الشبكات غير المعتمدة دون الحصول على موافقة البنك المركزي المصري.

7-1-4 ينبغي على البنك ومقدمي خدمات الترميز تطبيق سياسة الفصل بين المهام والرقابة الثنائية، وذلك للتأكد من عدم إمكانية قيام أي موظف داخل البنك بأي عمل غير مصرح له وإخفائه، ويتضمن هذا على سبيل المثال لا الحصر، إدارة حساب المستخدم وتنفيذ المعاملات وحفظ وإدارة مفاتيح الشفرة الخاصة بالنظام وإدارة النظام System Administration وتشغيله System Operations.

8-1-4 يجب أن تخضع أنظمة البنك ومقدمي خدمات الترميز إلى اختبارات مُتعددة قبل التشغيل للتأكد من قدرتها على القيام بالمهام المُوكلة لها وفى حالة تحديث تلك الأنظمة يتم إعادة اختبارها بذات الوسائل لضمان استمرار سلامتها.

9-1-4 يجب على البنك ومقدمي خدمات الترميز السماح بالولوج الى الانظمة بناء على المهام الوظيفية بما يضمن عدم تضارب المصالح ويجب على البنك التحكم في ولولج الموظفين ومديري الانظمة من خلال نظام تحكم مركزي مع مراعاة استخدام المصادقة الثنائية.

2-4. البنية التحتية والمتابعة الأمنية للمنظومة

1-2-4 يجب على البنوك ومقدمي خدمات الترميز إنشاء بيئة تشغيل ملائمة تعمل على دعم وحماية أنظمتها الخاصة المرتبطة بأنظمة الترميز، بحيث تحتوي تلك البيئة على بنية تحتية آمنة لتلك الخدمات - والتي تشمل على سبيل المثال لا الحصر إعداد خوادم النظام وأنظمة اكتشاف ومنع الإختراق وأجهزة جدار الحماية Firewall وأجهزه التوجيه وخلافه - كما تحتوي أيضا على إجراءات حماية ملائمة للشبكات الداخلية وروابط الشبكات مع الجهات الخارجية بما يشمل شركة بنوك مصر بصفتها الشركة المسؤولة عن إدارة واجهة الترميز الموحدة للبنوك المُصدرة، فضلاً عن خطط الطوارئ اللازمة والأنظمة البديلة حال فشل الأنظمة الأصلية.

2-2-4 تقع المسؤولية الكاملة لتقديم الخدمات على البنوك المشتركة بالخدمة ومقدمي خدمات الترميز والتي يجب عليها بذل العناية الواجبة لضمان أمان كافة المعاملات، وكذا مراقبة كل من الأنظمة المتصلة بالنظام والبنية التحتية بصورة استباقية بشكل دائم على مدار 24 ساعة طوال الأسبوع، وذلك لرصد وتسجيل أي مخالفات أمنية، أو أي اختراقات، أو نقاط ضعف مشتبه بها، وكذلك أي أنشطة غير طبيعية محل اشتباه قد تتم على الأنظمة وذلك يجب ان يتم من خلال تفعيل مركز عمليات للأمن السيبرانى SOC.

3-2-4 يجب على البنوك ومقدمي خدمات الترميز التأكد من وجود مسارات التدقيق Audit Trails لكافة العمليات التي تتم عبر أنظمة/تطبيقات ترميز البطاقات وكذلك البنية التحتية الخاصة بهذه الخدمة كما يجب ضمان حماية تلك المسارات ضد أي تلاعب أو تغيير غير مُصرَّح به، وأن يتم الاحتفاظ بها لمدة زمنية تتوافق مع ما تحدده سياسات البنك تطبيقاً للمتطلبات القانونية وطبقاً للضوابط والتعليمات الرقابية الصادرة في هذا الشأن ويهدف هذا الإجراء إلى تسهيل إجراءات التحقيق في أي عملية احتيال، وحل أي نزاع أو شكوى إذا لزم الأمر وعند تحديد ما سيتم الاحتفاظ به في مسارات التدقيق، يمكن الأخذ في الاعتبار الأنواع التالية من الأنشطة وذلك كحدٍ أدنى:

- عمليات فتح أو تعديل أو إغلاق حساب مستخدم على الانظمة المختلفة الخاصة بالخدمة.
- أي عملية ذات تبعات مالية.
- أي تصريح يمنح مستخدم لتجاوز أي من الحدود أو الصلاحيات.
- أي تعديل أو إضافة أو إلغاء لصلاحيات المستخدمين أو امتيازات خاصة بالدخول على الأنظمة.

4-2-4 يجب أن يتم مراجعة كافة ما يتم إصداره من سجلات تدقيق Audit Logs وإنذارات التأمين اللحظية Real Time Security Alerts -مثل إنذارات أنظمة كشف ومنع الاختراق - بواسطة الموظفين أو فرق العمل المعنية وذلك بطريقة دورية وفى الوقت المناسب.

5-2-4 تطبيق معايير وإجراءات حصيفة فيما يخص إمكانية الدخول إلى أماكن عمل النظام Physical Security بما في ذلك البرامج والأجهزة المُشغِلة للنظام والشبكات وأجهزة التشفير ومراكز المعلومات التي تقوم بتشغيل جزء أو أجزاء من النظام.

6-2-4 يجب الرجوع الى الإطار العام للأمن السيبرانى الخاص بالممارسات المتعلقة بتصميم، تنفيذ وسائل التأمين المختلفة وانشاء ومراقبة البنية التحتية لخدمات الترميز.

7-2-4 يتعين على البنوك الحصول على موافقة مسبقة من البنك المركزي المصري في حال ابرام اتفاقيات تتعلق بإسناد خدمات ترميز البطاقات على تطبيقات الأجهزة الإلكترونية او تطبيقاتها. وفي حالة قيام البنك بإسناد بعض الخدمات لأطراف خارجية، فإن البنك يظل مسئولاً مسئولية كاملة تجاه مستخدمي النظام وتجاه التزام الأطراف الخارجية بهذه القواعد، والتأكد مما يأتي:

- الاحتفاظ بسجل محدث يشتمل على جميع اتفاقات وتعاقدات الإسناد والاستعانة بالأطراف الخارجية.
- وضع حدود لإسناد أكثر من وظيفة إلى مقدم خدمة واحد للحد من مخاطر التركز والتشغيل.
- يلتزم البنك بوضع سياسة للموظفين لدى الأطراف الخارجية الذين تم إخلاء طرفهم أو تم تغير مسئولياتهم وإلغاء صلاحياتهم على جميع الأنظمة والأنظمة الخارجية وأنظمة المساعدة (support portals) ومراجعة الصلاحيات دورياً.

3-4. تقييم النظام الأمني للخدمة

1-3-4 يجب ان يتم تعهيد الخدمات الأمنية الى شركات او افراد تتوافق مع القوانين المصرية.

2-3-4 يجب على البنوك ومقدمي خدمات الترميز دورياً تقييم الوضع الأمني لكافة الأنظمة - التطبيقات، والشبكات، وأجهزة التأمين، وخوادم نظام أسماء النطاقات وخوادم البريد الإلكتروني، إلخ - المتعلقة بتشغيل الخدمة، وذلك فـي المركز الرئيسي للمعلومات والمركز الاحتياطي الذي يستخدم في حالات الكوارث.

3-3-4 يجب على البنوك ومقدمي خدمات الترميز إجراء تقييم دوري لنقاط الضعف Vulnerability Assessment كل ثلاثة أشهر على الأقل أو عند حدوث تغييراً جوهرياً في البيئة التشغيلية وبيئة الطوارئ للأنظمة المختلفة الخاصة بالخدمة لاكتشاف نقاط الضعف في بيئة تكنولوجيا المعلومات وتقييمها. ويمكن أن يتولى هذا التقييم مستشار أو مقدم خدمة خارجي للبنك وأن يكون مقدم الخدمة مختلف عن مقدم الخدمة القائم باختبارات الاختراق، أو أن يتولى هذا التقييم إدارة أمن المعلومات بالبنك، وذلك على النحو التالي:

- يجب أن يحتوي نطاق تقييم نقاط الضعف على اختبار الثغرات الشائعة في النظام على سبيل المثال لا الحصر (OWASP Top Ten Attacks).

- يجب على البنك ومقدمي خدمات الترميز إعداد خطة لمعالجة المشاكل التي تظهر في تقييم نقاط الضعف، والتأكيد على غلق الثغرات بالخطة خلال وقت متناسب مع تصنيف نقاط الضعف ثم التحقق من صحة هذه المعالجة عن طريق إعادة الاختبار لإثبات أنه قد تم التعامل بفعالية مع هذه المشاكل بالكامل وفي التوقيت المناسب.

4-3-4 التزام البنك بعدم إطلاق الخدمات الجديدة قبل الانتهاء من موافاة البنك المركزي المصري بتقرير اختبارات الاختراق (Penetration Test Report) وتقارير تقييم نقاط الضعف (Credential vulnerability assessment) على بيئة العمل الفعلية بما يشمل جميع الأنظمة و التطبيقات و البنية التحتية و أساليب التأمين المتبعة على ان تكون هذه الاختبارات تتم بصورة شاملة تتيح اكتشاف جميع الثغرات و المشاكل الفنية والذي يفيد عدم وجود أي نقاط ضعف عالية أو متوسطة الخطورة ومن ثم الحصول على موافقة البنك المركزي المصري بتفعيل الخدمة، على ان يتم تقديم التقرير المشار اليه إلى البنك المركزي المصري في مدة لا تتجاوز ثلاثة أشهر من تاريخ اصداره من مقدم خدمة خارجي مستقل.

5-3-4 يجب على البنك ومقدمي خدمات الترميز القيام باختبارات الاختراق (Penetration Testing) وذلك لعمل تقييم مفصل ومتعمق للوضع الأمني للنظام من خلال محاكاة للهجمات الفعلية على البيئة الفعلية والاحتياطية على أن يتم ذلك على الأقل مرة واحدة سنويا، أو عند حدوث تغيير في النظام، على أن تتم مراعاة ما يلي:

- يجب أن يتولى إجراء اختبار الاختراق أحد مقدمي الخدمة الخارجيين المستقلين، حيث يجب عليه أولاً التوقيع على اتفاقية السرية وعدم الإفصاح قبل مزاولة العمل Non-Disclosure Agreement.
- يجب أن يكون لدى البنوك ومقدمي خدمات الترميز تقرير مبدئي عن اختبار الاختراق وخطة المعالجة Penetration Test Report & Remediation Plan، التي تم اصدارها والموقعة من مقدم الخدمة الخارجي.
- يجب على البنوك ومقدمي خدمات الترميز التحقق من صحة معالجة الملاحظات الناتجة عن اختبار الاختراق سواء كان على الأنظمة الرئيسية أو الأنظمة البديلة المستخدمة لمواجهة الكوارث مع مراعاة إجراء اختبار الاختراق على الانظمة في مركز الطوارئ.
- يجب على مقدم الخدمة الخارجي إصدار تقرير نهائي موقع منه عن اختبار الاختراق لكي يقوم البنك بتقديمه إلى البنك المركزي المصري، بجانب التقرير المبدئي الأول.
- غير مسموح باختيار نفس مقدم الخدمة الخارجي لأداء أكثر من اختباري اختراق متتاليين.

4-4. الاستجابة للأحداث الطارئة وإداراتها

4-4-1 يجب على البنوك ومقدمي خدمات الترميز وضع إجراءات للاستجابة للحدث وإدارته خلال تقديم الخدمة، بهدف الإبلاغ والمعالجة الفورية لأي اختراقات أمنية سواء كانت فعلية أو مشتبه بها، وكذلك أي حالات احتيال أو انقطاع/عدم ثبات الخدمة، سواء أثناء أو بعد ساعات العمل. ويجب على البنوك اتخاذ الإجراءات الضرورية التالية (ومنها على سبيل المثال لا الحصر):

- سرعة اكتشاف مصدر الحدث، وتحديد ما إذا كان قد وقع نتيجة وجود نقاط ضعف في النظم التأمينية بالبنك من عدمه.
- تقييم النطاق المحتمل للحدث ومدي تأثيره.
- تصعيد الأمر إلى الإدارة العليا للبنك بشكل فوري، إذا كان هذا الحدث قد يضر بسمعة البنك أو يؤدى إلى خسائر مالية.
- إخطار العملاء المتضررين على الفور، إذا لزم الأمر.
- احتواء الخسائر المتعلقة بأصول البنوك وبياناتها ومدي تأثيرها علي سمعة البنوك، وبوجه خاص الخسائر المتعلقة بعملائها.
- جمع الأدلة الجنائية الرقمية والأدلة الجنائية وحفظها بطريقة مناسبة وبأسلوب يضمن الرقابة على تلك الأدلة وضمان عدم التلاعب بها لتغيير محتواها، لتسهيل التحقيقات اللاحقة وإقامة دعوى قضائية ضد مخترقي النظام والمشتبه فيهم إذا لزم الأمر بالإضافة إلى تنفيذ عملية مراجعة لهذا الحدث.

4-4-2 يجب على البنوك إعداد سجل بالأحداث العارضة المرتبطة بالخدمة المقدمة والتفاصيل الخاصة بها بالإضافة إلى إعداد تقرير دوري بحد اقصى كل ستة أشهر للعرض على الإدارة العليا لاتخاذ الإجراءات المناسبة لتلافي تكرارها.

4-4-3 يتولى مسئول الالتزام بالبنك مسئولية التأكد من إبلاغ البنك المركزي المصري بأي حادث امن سيبراني بصورة صحيحة وفي خلال 6 ساعات من اكتشاف الحادث وبكافة الحالات الواردة أدناه على سبيل المثال لا الحصر:

- أي هجمات احتيال لتسريب أو إفشاء هوية مُستخدم النظام أو وثائق اعتماد الشخصية (كالاحتيال Phishing، وملفات التجسس (حصان طروادة Trojans)، والبرمجيات الخبيثة وبرمجيات الفدية Ransomware Malware.. إلخ).
- الدخول غير المصرح به إلى أنظمة تكنولوجيا المعلومات بالبنك لتسريب بيانات مُستخدم النظام المتعلقة بالخدمات المقدمة.
- أي عملية تخريبية للبيانات المتعلقة بأنظمة الخدمات المقدمة والتي لا يمكن استرجاعها.
- الإيقاف التام المتعمد أو العارض للخدمات المقدمة لفترة تزيد عن الفترة المحددة كهدف لوقت الاسترجاع RTO المحدد من قبل البنك.

- أي هجمات سيبرانية ذات الصلة بتلك الخدمات المقدمة على أن يتم إرسال هذه التقارير بالبريد الالكتروني على العناوين التالية:
  - cbe.infosec@cbe.org.eg
  - eg-fincirt@cbe.org.eg

4-5. اعتبارات الأداء وضمان استمرارية العمل

4-5-1 يجب على البنوك ومقدمي خدمات الترميز توفير الخدمات المقدمة على مدار الساعة، مع ضمان أداء الخدمة للعملاء بالسرعة والكفاءة والدقة المناسبة طبقا لما تم ذكره في الأحكام والشروط الخاصة بالخدمة مع أخذ توقعات العملاء بعين الاعتبار مع إبلاغ العملاء مسبقا في حال توقف او تعطل الخدمة.

4-5-2 يجب على البنوك ومقدمي خدمات الترميز وضع معايير لتقييم ومتابعة مستوى أداء الخدمات المقدمة كما يجب اتخاذ التدابير اللازمة للتأكد من قدرة النظم الداخلية الخاصة بتقديم تلك الخدمات على التعامل مع حجم المعاملات المتوقعة والنمو المستقبلي لهذا النوع من الخدمات.

4-5-3 يجب أن تأخذ البنوك ومقدمي خدمات الترميز في اعتبارها التخطيط لضمان استمرارية العمل عند تطويرها للخدمات المقدمة، على أن يتم أيضا مراعاة الممارسات التالية:

- في حال حدوث عطل في الخدمة، يجب أن تحتوي خطة استمرارية العمل على خطوات محددة لكيفية استئناف أو استرجاع تلك الخدمات وتحدد هذه الخطوات بناء على أهداف وقت ونقطة الاسترجاع RTO & RPO المحددين مسبقاً مع ضرورة دورية المراجعة والتحديث بأي مستجدات أو مخاطر محتملة.
- وجود نسخ احتياطية للبيانات لاستعادتها ووجود خطط عمل بديلة للطوارئ.
- يجب أن تضمن خطة استمرارية العمل الخاصة بالخدمات المقدمة القدرة على التعامل مع أي من الحالات التي يتم فيها التعهيد لأطراف خارجية.

5. أمن العملاء وضوابط لبعض المخاطر الأخرى

5- 1 يجب على البنوك أن تحدد بدقة كافة الاحكام والشروط لعملائها من خلال تطبيقات ترميز البطاقات وبما لا يتعارض مع تعليمات حماية حقوق عملاء البنوك المُصدرة في فبراير 2019 وكافة تعديلاتها وغيرها من التعليمات ذات الصلة مع مراعاة ما يلي:

5-1-1 ألا يتم الاشتراك في الخدمة الا بعد الموافقة الكترونيا على تلك الشروط والاحكام. وبحيث تتضمن توضيح بشكل مُفصَّل الخطوات الواجب على مُستخدم النظام إتباعها لتفعيل الخدمة في حالة الاشتراك لأول مرة أو في حالة وقف الخدمة أو إعادة تشغيلها، موضحاً الوقت اللازم

لإيقاف الخدمة من لحظة طلب إيقافها من قِبل مُستخدم النظام والطرق المختلفة لطلب إيقاف الخدمة.

2-1-5 إتاحة امكانية إيقاف استخدام الخدمة عند إساءة استخدامها من قبل مستخدم النظام.

3-1-5 ايضاح إذا كان هناك أي تكلفة إضافية أو رسوم لإستخدام تلك الخدمات ومقدارها ودوريتها.

4-1-5 يقوم البنك المُصدر لأداة الدفع الإلكترونية وكذلك مقدم خدمات الدفع بإيجاد آلية لدراسة الشكاوى ويُنص صراحة في بنود واحكام تقديم الخدمة على طريقة تقديم الشكوى إلى البنك والحد الأقصى للوقت المُستغرق للتحقيق في الشكوى من قِبل الأطراف المختلفة والرد على العميل.

5-1-5 التأكيد على التزام مُستخدم النظام بقراءة التحذيرات والإطارات التنبيهية (مثل التنبيهات الأمنية أو تنبيهات محاولات الاحتيال/الهندسة الاجتماعية Social Engineering.. إلخ) والتأكيد أيضًا على أن قبول مُستخدم النظام لأي تغيير في الشروط والأحكام ا لذي سيظهر من خلال النظام إلكترونيا والموافقة عليها الكترونيا للاستمرار في الحصول على الخدمة.

6-1-5 توضيح مسئوليات المُستخدم في الحفاظ على الجهاز المقترن بالرمز الخاص به وإبلاغ البنك في حال فقدانه او اشتباه العميل في ان بياناته السرية قد تم الاطلاع عليها من قبل الغير.

2-5. رصد الأنشطة غير العادية

1-2-5 يتعين على البنوك وضع تدابير فعالة للرقابة المستمرة لضمان سرعة اكتشاف أي معاملات غير عادية أو تسريب بيانات او معلومات تحدث من خلال الخدمة يُشتبه أن تؤدى إلى عمليات احتيال او نشاط ينطوي على شبهة غسل أموال او تمويل إرهاب وعلى وجه الخصوص، ينبغي أن تكون تلك التدابير قادرة على اكتشاف حالات مثل:

- حدوث العديد من عمليات الدفع باستخدام تطبيقات ترميز البطاقات على الأجهزة الإلكترونية خلال فترة زمنية وجيزة، وخاصة على سبيل المثال لا الحصر إذا كانت المبالغ المدفوعة تقترب من الحد الأقصى المسموح به. وكذلك الزيادة المفاجئة في عمليات الدفع باستخدام الرمز.
- تفعيل السيناريوهات او التقارير اللازمة لرصد الأنشطة الغير عادية وفقا لطبيعة المنتج مع التأكد من رفع تقارير اشتباه الي وحدة مكافحة غسل الأموال وتمويل الإرهاب عند اللزوم.

2-2-5 يجب أن تتمتع آلية الرقابة المتبعة بالقدرة على سرعة إصدار تحذيرات إلى المختصين بالمتابعة والرصد للخدمات المقدمة عند حدوث أي عمليات دفع محل شبهة احتيال، وكذلك أي أنشطة غير معتادة ويجب على البنوك في تلك الحالات ان تبذل العناية الواجبة للتصدي لحالات الاحتيال المحتملة فضلا عن التحقق من ذلك مع أصحاب هذه الرموز التي تتم عليها هذه المعاملات أو الأنشطة في أسرع وقت ممكن واخطار إدارة مكافحة الاحتيال بالبنك المركزي وكذا اخطار الجهات المختصة.

3-2-5 يتم الرجوع الى العملاء فور رصد أي معاملة غير اعتيادية للتحقق من قيامهم بها.

4-2-5 يجب على البنك تطبيق إجراءات محددة ومُعتمدة للتعامل مع المعاملات المشتبه بها.

5-2-5 يجب الإبلاغ عن أي حالة من حالات الاحتيال ذات الصلة بتلك الخدمات المقدمة على أن يتم إرسال هذه التقارير بالبريد الالكتروني على العناوين التالية او أي وسيلة مستحدثة:

- fraudcombating@cbe.org.eg

3-5. توعية العملاء مستخدمين النظام

1-3-5 نظراً لأن الأجهزة التي يستخدمها العملاء للدخول على تطبيقات ترميز البطاقات على الأجهزة الإلكترونية تقع خارج نطاق سيطرة البنك، فإن احتمال ظهور مخاطر أمنية تزداد في حالة عدم معرفة مُستخدم النظام بالاحتياطات الأمنية الضرورية لاستخدام الخدمة أو سوء فهمها ولذلك يجب على البنك أن يولي اهتماماً خاصاً لتوعية العملاء عن طريق تقديم حملات توعية مختلفة وكذا نصائح سهلة الفهم وواضحة تتعلق بالاحتياطات الأمنية الواجب اتخاذها عند التعامل مع تلك الخدمات والتزامهم حيال ذلك.

2-3-5 التأكيد على العملاء وتوعيتهم أن موظفي البنك أو وكلاءه أو مقدمي خدمات الدفع لا يجوز لهم أن يطلبوا من مُستخدم النظام الإفصاح عن البيانات السرية (كأرقام البطاقات أو كلمات السر) عن طريق البريد الإلكتروني أو غيره وفي حالة وقوع ذلك يجب على مُستخدم النظام الاتصال بالبنك في أسرع وقت ممكن.

3-3-5 توعية عملاء تلك الخدمات بالطرق التي يمكنهم من خلالها التأكد من صحة التطبيق الرسمي والتزام البنك بإطلاق حملات دعائية تخص زيادة وعي العملاء فيما يخص الخدمات المشار اليها.

4-3-5 تختلف النصائح الخاصة بالاحتياطات الأمنية الواجب إتباعها وفقا لطبيعة العملاء، وطبيعة الخدمات المقدمة، وتشمل النصائح ما يلي كحد أدنى:

- اختيار وحماية وسائل التحقق الخاصة بالعميل.
- الحماية ضد تقنيات الهندسة الاجتماعية Social Engineering Techniques حيث يجب توعية العملاء بضرورة عدم الإفصاح عن أي معلومات شخصية - كبطاقة الهوية أو جواز السفر أو العناوين أو أرقام حسابات البنك الخاصة بهم - لأي شخص لم يتأكد من هويته أو استخدام تطبيقات هواتف محمولة موضع شك. كما يجب التأكيد على العملاء بعدم الإفصاح عن كلمات السر لأي شخص بما في ذلك موظفي البنك أو وكلائه.
- يجب على البنوك مراجعة النصائح والإرشادات الخاصة بالاحتياطات التأمينية التي يتم تقديمها للعملاء للتأكد من كفايتها وملائمتها للتغيرات التي تستجد على البيئة التكنولوجية والخدمات المقدمة.

- يتم إخطار مستخدم النظام بالإجراءات الواجب اتباعها في حالة اكتشاف أي شخص آخر لوسائل التحقق الخاصة بمُستخدم النظام.

6. إجراءات الحصول على التراخيص

6-1 يجب على البنوك المُصدرة التي ترغب في الحصول على تراخيص لتقديم خدمات ترميز البطاقات لعملائها أن تتقدم بطلب لقطاع الشئون المصرفية بالبنك المركزي المصري للحصول على الموافقة اللازمة، وذلك لكل تطبيق يتم قبول بطاقات البنك من خلاله على حده، وذلك مع استيفاء ما يلي:

6-1-1 دورة العمل التفصيلية.

6-1-2 بيانات البنية التحتية للمنظومة التي سيتم استخدامها.

6-1-3 التكنولوجيا اللازمة وضوابط الأمن السيبرانى لتأمين البنية التحتية والأنظمة والتطبيقات وكافة المعلومات والبيانات في حالاتها المختلفة من نقل ومعالجة وتخزين وحفظ في نسخ احتياطية بما يضمن سرية وسلامة وإتاحة البيانات والتوافق مع الإطار العام للأمن السيبرانى.

6-1-4 خطة العمل الخاصة بالربط الفني مع شركة بنوك مصر والشركات صاحبة علامة القبول.

6-1-5 البيانات المتعلقة بالتطبيق الخاص بطالب الرمز (Token Requestor) إن وجدت وذلك للبطاقات المصدرة من البنك.

6-1-6 دور البنك والجهات المصرح لها طلب ترميز البطاقات المصدرة من البنك.

6-1-7 البيانات المتعلقة بأنظمة إدارة تطبيقات ترميز البطاقات الإلكترونية (Wallet Management Server) أن وجدت.

6-1-8 تقديم خطة عمل لمدة ثلاث سنوات تتضمن التالي:

- عدد العملاء والبطاقات الخاصة بالعملاء المستهدف تقديم الخدمة لهم.
- عدد وقيم المعاملات السنوية المستهدف تنفيذها باستخدام البطاقات التي تم ترميزها.
- تقديم خطة تسويقية شاملة للتعريف بالخدمة وتفعيل استخدامها على أن يوضح بالخطة الميزانية المعتمدة لذلك.

6-2 يجب موافاة البنك المركزي المصري بما يلي قبل الإطلاق الفعلي للخدمة:

6-2-1 تقرير اختبارات الاختراق (Penetration Test Report), وتقارير تقييم نقاط الضعف (Credential vulnerability assessment) على بيئة العمل الفعلية والطوارئ بما يشمل جميع الأنظمة و التطبيقات و البنية التحتية و أساليب التأمين المتبعة على ان تكون هذه الاختبارات تتم بصورة شاملة تتيح اكتشاف جميع الثغرات و المشاكل الفنية والذي يفيد عدم وجود أي نقاط ضعف عالية أو متوسطة الخطورة ومن ثم الحصول على موافقة البنك المركزي المصري بتفعيل الخدمة، على ان يتم تقديم التقرير المشار اليه إلى البنك المركزي

المصري في مدة لا تتجاوز ثلاثة أشهر من تاريخ إصداره من مقدم خدمة خارجي مستقل والخاصة بكافة الخدمات المذكورة اعلاه.

2-2-6 ما يفيد اجتياز التطبيقات الإلكترونية لكافة الاختبارات الفنية التي سيتم تقديم الخدمة من خلالها سواء كانت تطبيقات لمصنعي الأجهزة الذكية (OEM Wallet) او تطبيقات تخص البنوك المُصدرة (HCE Wallet) أو التطبيقات من مقدم خدمة.

3-2-6 تقييم المخاطر الذي تم من جانب البنك على الخدمة والذي يوضح أن الضوابط التي سيتم تطبيقها تصل بمستوى المخاطر للمستوى المقبول وتوضح إجراءات إدارة ورصد اية مخاطر بصورة فعاله.