وزارة الاتصالات وتكنولوجيا المعلومات

قرار رقم ٣٦١ لسنة ٢٠٢٠

بتاريخ ٢٠٢٠/٤/١٩

بتعديل اللائحة التنفيذية للقانون رقم ١٥ لسنة ٢٠٠٤

بتنظيم التوقيع الإلكترونى وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات

وزير الاتصالات وتكنولوجيا المعلومات

بعد الاطلاع على الدستور ؛

وعلى القانون المدنى الصادر بالقانون رقم ١٣١ لسنة ١٩٤٨ ؛

وعلى القانون رقم ١٧ لسنة ١٩٩٩ بإصدار قانون التجارة وتعديلاته ؛

وعلى القانون رقم ١٣ لسنة ١٩٦٨ بشأن المرافعات المدنية والتجارية وتعديلاته؛

وعلى القانون رقم ٢٥ لسنة ١٩٦٨ بشأن الإثبات فى المواد المدنية والتجارية وتعديلاته ؛

وعلى القانون رقم ٨٢ لسنة ٢٠٠٢ بإصدار قانون حماية حقوق الملكية الفكرية وتعديلاته ؛

وعلى القانون رقم ١٠ لسنة ٢٠٠٣ بشأن تنظيم الاتصالات ؛

وعلى قانون رقم ١٥ لسنة ٢٠٠٤ بتنظيم التوقيع الإلكترونى وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات ؛

وعلى القانون رقم ٧٢ لسنة ٢٠١٧ بإصدار قانون الاستثمار وتعديلاته ؛

وعلى القرار الوزارى رقم ١٠٩ لسنة ٢٠٠٥ بتاريخ ٢٠٠٥/٥/١٥ بإصدار اللائحة التنفيذية لقانون تنظيم التوقيع الإلكترونى وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات وتعديلاتها ؛

وعلى قرار مجلس إدارة هيئة تنمية صناعة تكنولوجيا المعلومات رقم ١ لسنة ٢٠٢٠ الصادر بجلسته المنعقدة فى ١٥/ ٣/ ٢٠٢٠بشأن الموافقة على تعديل اللائحة التنفيذية لقانون التوقيع الإلكترونى ؛

وعلى مذكرة الرئيس التنفيذى لهيئة تنمية صناعة تكنولوجيا المعلومات رقم ١ لسنة٢٠٢٠ بتاريخ ٢٠٢٠/٣/١٥، بشأن طلب اعتماد الموافقة على تعديل اللائحة التنفيذية لقانون التوقيع الإلكترونى ؛

قرر:

(المادة الأولى)

يُعمل بأحكام اللائحة التنفيذية للقانون رقم ١٥ لسنة ٢٠٠٤ بتنظيم التوقيع الإلكترونى وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، المعدَّلة، المرفقة.

(المادة الثانية)

يُنشر هذا القرار فى الوقائع المصرية، ويُعمل به من اليوم التالى لتاريخ نشره. ويُلغى كل قرار يخالف أحكامه.

وزير الاتصالات وتكنولوجيا المعلومات

د/ عمرو سميح طلعت

اللائحة التنفيذية للقانون رقم ١٥ لسنة ٢٠٠٤

بتنظيم التوقيع الإلكترونى وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات

مـــادة (١)

فى تطبيق أحكام هذه اللائحة ، يقصد بالمصطلحات الآتية المعانى المبينة قرين كل منها :

١ - التوقيع الإلكترونى :

ما يوضع على محرر إلكترونى ويتخذ شكل حروف ، أو أرقام ، أو رموز ، أو إشارات أو غيرها ويكون له طابع متفرد يسمح بتحديد شخص الموقع ويميزه عن غيره .

٢ - الكتابة الإلكترونية :

كل حروف، أو أرقام، أو رموز، أو أى علامات أخرى تثبت على دعامة الكترونية أو رقمية أو ضوئية أو أية وسيلة أخرى مشابهة وتعطى دلالة قابلة للإدراك.

٣ - المحرر الإلكترونى :

رسالة بيانات تتضمن معلومات تنشأ، أو تدمج، أو تخزن، أو ترسل، أو تستقبل، كلياً أو جزئياً، بوسيلة إلكترونية أو رقمية، أو ضوئية، أو بأية وسيلة أخرى مشابهة.

٤ - الوسيط الإلكترونى :

أداة أو أدوات أو أنظمة إنشاء التوقيع الإلكترونى .

٥ - الموقع :

الشخص الحـــائز على بيانات إنشـــاء التوقيع ويوقـــع عن نفســـه أو عمن ينيبه أو يمثله قانوناً .

٦- جهات التصديق الإلكترونى :

الجهات المرخص لها بإصدار شهادة التصديق الإلكترونى وتقديم خدمات تتعلق بالتوقيع الإلكترونى .

٧ - شهادة التصديق الإلكترونى :

الشهادة التى تصدر من الجهة المرخص لها بالتصديق وتثبت الارتباط بين الموقع وبيانات إنشاء التوقيع .

٨-بيانات إنشاء التوقيع الإلكترونى :

عناصر متفردة خاصة بالموقع وتميزه عن غيره، ومنها على الأخص مفاتيح الشفرة الخاصة به، والتى تُستخدم فى إنشاء التوقيع الإلكترونى.

٩- الختم الإلكترونى : **Electronic seal**

هو توقيع إلكترونى يسمح بتحديد – الشخص الاعتبارى – مُنشئ الختم ويميزه عن غيره.

١٠- منشئ الختم:

الشخص الاعتبارى الحائز على بيانات إنشاء الختم الالكترونى واستخدامه.

١١- بيانات إنشاء الختم الإلكترونى :

عناصر متفردة خاصة بمُنشئ الختم الإلكترونى وتميزه عن غيره، ومنها على الأخص مفاتيح الشفرة الخاصة به، والتى تُستخدم فى إنشاء الختم الإلكترونى .

١٢- شهادة الختم الإلكترونى :

الشهادة التى تصدر من الجهة المرخص لها بالتصديق، وتثبت الارتباط بين منشئ الختم وبيانات إنشاء الختم الإلكترونى .

١٣- البصمة الزمنية الالكترونية: Time Stamp

ما يوضع على محرر الكترونى ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها والتى تربط تلك البيانات بوقت محدد لإثبات وجود هذا المحرر الإلكترونى فى ذلك الوقت .

١٤- التشفير :

منظومة تقنية حسابية تستخدم مفاتيح خاصة لمعالجة وتحويل البيانات والمعلومات المقروءة إلكترونياً، بحيث تمنع استخلاص هذه البيانات والمعلومات إلا عن طريق استخدام مفتاح أو مفاتيح فك الشفرة.

١٥-تقنية شفرة المفتاحين العام والخاص (المعروفة باسم تقنية شفرة المفتاح العام):

منظومة تسمح لكل شخص طبيعى أو معنوى بأن يكون لديه مفتاحين متفردين، أحدهما عام متاح إلكترونياً، والثانى خاص يحتفظ به الشخص ويحفظه على درجة عالية من السرية .

١٦-المفتاح الشفرى العام:

أداة إلكترونية متاحة للكافة، تنشأ بواسطة عملية حسابية خاصة، وتستخدم فى التحقق من شخصية الموقع على المحرر الإلكترونى، والتأكد من صحة وسلامة محتوى المحرر الإلكترونى الأصلى .

١٧-المفتاح الشفرى الخاص:

أداة إلكترونية خاصة بصاحبها، تنشأ بواسطة عملية حسابية خاصة، ويتم الاحتفاظ بها على أداة إنشاء التوقيع الإلكتروني، وتُستخدم فى وضع التوقيع الإلكترونى على المحررات الإلكترونية.

١٨-المفتاح الشفرى الجذرى :

أداة إلكترونية تنشأ بواسطة عملية حسابية خاصة، وتستخدمها جهات التصديق الإلكترونى لإنشاء شهادات التصديق الإلكترونى وبيانات إنشاء التوقيع الإلكترونى .

١٩-الدعامة الإلكترونية :

وسيط مادى لحفظ وتداول الكتابة الإلكترونية، ومنها الأقراص المدمجة أو الأقراص الضوئية أو الأقراص الممغنطة أو الذاكرة الإلكترونية أو أى وسيط آخر مماثل.

٢٠-أداة التوقيع الإلكترونى :

وسيط إلكترونى مؤمن يُستخدم فى عملية إنشاء وتثبيت التوقيع الإلكترونى على المحرر الإلكترونى، ويشمل هذا التعريف الكروت الذكية والشرائح الإلكترونية المنفصلة، أو غير ذلك من وسائط أو أنظمة تتطابق معه من حيث تحقيق الوظائف المطلوبة، وفقاً للمعايير التقنية والفنية المحددة فى هذه اللائحة .

٢١-منظومة تكوين بيانات إنشاء التوقيع الإلكتروني:

مجموعة عناصر مترابطة ومتكاملة، تحتوى على وسائط إلكترونية وبرامج حاسب آلى يتم بواسطتها تكوين بيانات إنشاء التوقيع الإلكترونى باستخدام المفتاح الشفرى الجذري، ويشمل ذلك بيانات إنشاء الختم الالكترونى .

٢٢-شهادة فحص بيانات إنشاء التوقيع الإلكترونى :

شهادة تصدرها الهيئة بنتيجة الفحص والتحقق من صحة بيانات إنشاء التوقيع الإلكتروني، بما فى ذلك الختم الإلكترونى .

٢٣-شهادة فحص التوقيع الإلكتروني:

شهادة تصدرها الهيئة بنتيجة فحصها لصحة وسلامة التوقيع الإلكترونى، بما فى ذلك الختم الإلكترونى .

٢٤-شهادة اعتماد جهات التصديق الإلكترونى الأجنبية :

شهادة تصدرها الهيئة باعتماد جهات التصديق الإلكترونى الأجنبية، وما تصدره هذه الجهات من شهادات التصديق الإلكترونى النظيرة للشهادات الصادرة داخل جمهورية مصر العربية .

٢٥-بصمة شهادة السلطة الجذرية العليا للتصديق الإلكترونى :

هى بصمة متفردة تتكون من أحرف وأرقام ورموز، تنتج من عملية حسابية أحادية الاتجاه، يتم إجراؤها على محتويات شهادة السلطة الجذرية العليا للتصديق الإلكترونى الموقعة ذاتياً، تكون ذات مرجعية وموثوقية ودلالة على تلك الشهادة، ولا تسمح باسترجاع محتويات الشهادة بصورة منفصلة .

٢٦-الهيئة:

هيئة تنمية صناعة تكنولوجيا المعلومات .

٢٧-الوزارة المختصة :

الوزارة المختصة بشئون الاتصالات وتكنولوجيا المعلومات .

٢٨-الوزير المختص :

الوزير المختص بشئون الاتصالات وتكنولوجيا المعلومات .

٢٩-القانون :

القانون رقم ١٥ لسنة ٢٠٠٤ بتنظيم التوقيع الإلكترونى وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات .

مادة (٢)

تكون منظومة تكوين بيانات إنشاء التوقيع الإلكترونى مؤمنة متى استوفت الضوابط الآتية :

(أ) الطابع المتفرد لبيانات إنشاء التوقيع الإلكترونى .

(ب) سرية بيانات إنشاء التوقيع الإلكترونى .

(جـ) عدم قابلية الاستنتاج أو الاستنباط لبيانات إنشاء التوقيع الإلكتروني.

(د) حماية التوقيع الإلكترونى من التزوير، أو التقليد، أو التحريف، أو الاصطناع أو غير ذلك من صور التلاعب.

(هـ) عدم إحداث أى إتلاف بمحتوى أو مضمون المحرر الإلكترونى المراد توقيعه.

(و) ألا تحول هذه المنظومة دون علم الموقع علماً تاماً بمضمون المحرر الإلكترونى قبل توقيعه له.

(ز) أن تربط التوقيع الالكترونى بالمحرر الالكتروني، بطريقة متفردة تمنع إجراء أى تعديل بعد عملية التوقيع دون اكتشافه.

مادة (٣)

يجب أن تتضمن منظومة تكوين بيانات إنشاء التوقيع الإلكتروني المؤمنة الضوابط الفنية والتقنية اللازمة، وعلى الأخص ما يلي :

(أ) أن تكون المنظومة مستندة إلى تقنية شفرة المفتاحين العام والخاص وإلى المفتاح الشفرى الجذرى الخاص بالجهة المرخص لها والذى تصدره لها الهيئة، وذلك كله وفقاً للمعايير الفنية والتقنية المشار إليها فى الفقرة (أ) من الملحق الفنى والتقنى المرفق بهذه اللائحة.

(ب) أن تكون التقنية المستخدمة فى إنشاء مفاتيح الشفرة الجذرية لجهات التصديق الإلكترونى من التى تستعمل مفاتيح تشفير بأطوال لا تقل عن ٤٠٩٦ حرف إلكترونى (bit).

(جـ) أن تكون أجهزة التأمين الإلكترونى (Hardware Security Modules) المستخدمة معتمدة طبقاً للضوابط الفنية والتقنية المشار إليها فى الفقرة (ب) من الملحق الفنى والتقنى المرفق بهذه اللائحة.

(د) أن يتم استخدام أدوات توقيع إلكترونى غير قابلة للنسخ ومحمية بكود سري، تحتوى على عناصر متفردة للموقع وهى بيانات إنشاء التوقيع الإلكترونى وشهادة التصديق الإلكتروني، ويتم تحديد مواصفات أداة التوقيع الإلكترونى وأنظمتها، وفقاً للمعايير الفنية والتقنية المبينة فى الفقرة (ج) من الملحق الفنى والتقنى المرفق بهذه اللائحة.

(هـ) أن تضمن المنظومة لجميع أطراف التعامل إتاحة البيانات الخاصة بالتحقق من صحة التوقيع الإلكتروني، وارتباطه بالموقع دون غيره، وأن تضمن أيضًا عملية الإدراج الفورى والإتاحة اللحظية لقوائم الشهادات الموقوفة أو الملغاة، وذلك فور التحقق من توافر أسباب تستدعى إيقاف الشهادة، على أن يتم هذا التحقق خلال فترة محددة ومعلومة للمستخدمين، حسب القواعد والضوابط التى يضعها مجلس إدارة الهيئة.

مادة (٤)

يشترط لإثبات البصمة الزمنية الإلكترونية توافر ما يلى :

(أ) أن تربط التاريخ والوقت بالمحرر الإلكترونى بطريقة تمنع إمكانية تغيير البيانات دون اكتشافها.

(ب) أن يستند إلى مصدر زمنى دقيق معتمد من السلطة الجذرية العليا للتصديق الإلكتروني.

(جـ) يُجرى إنشاءه بواسطة السلطة الجذرية العليا للتصديق الإلكترونى أو من إحدى الجهات المرخص لها من قبل الهيئة، وفقًا للضوابط الفنية والتقنية المنصوص عليها فى الفقرة (أ) من الملحق الفنى والتقنى المرفق بهذه اللائحة.

مادة (٥)

لمجلس إدارة الهيئة أن يضع نظم وقواعد أخرى لمنظومة تكوين بيانات إنشاء التوقيع الإلكتروني؛ لمواكبة التطورات التقنية والتكنولوجية.

مادة (٦)

الهيئة هى السلطة الجذرية العليا للتصديق الإلكترونى فى جمهورية مصر العربية، وتتولى إصدار المفاتيح الشفرية الجذرية الخاصة للجهات المرخص لها بإصدار شهادات التصديق الإلكتروني.

وتتحقق الهيئة قبل منح ترخيص مزاولة نشاط تقديم خدمات التوقيع الإلكترونى من أن منظومة تكوين بيانات إنشاء التوقيع الإلكترونى لدى الجهة المرخص لها مؤمنة طبقاً للمادة (٢) من هذه اللائحة، ومتضمنة الضوابط الفنية والتقنية والنظم والقواعد المبينة فى المادتين (٣، ٥) من هذه اللائحة.

وتعتبر المنظومة بعد منح الترخيص وطوال مدة نفاذ مفعوله، مؤمنة وفعالة ما لم يثبت العكس.

مـــادة (٧)

تقدم الهيئة، بناءً على طلب كل ذى شأن، خدمة الفحص والتحقق من صحة بيانات إنشاء التوقيع الإلكترونى والختم الإلكترونى نظير مقابل يحدد فئاته مجلس إدارة الهيئة، ويجوز للهيئة أن تعهد للغير بتقديم هذه الخدمة تحت إشرافها. وفى جميع الأحوال، تصدر الهيئة شهادة فحص بيانات إنشاء التوقيع الإلكتروني.

مـــادة (٨)

تقدم الهيئة، بناءً على طلب كل ذى شأن، خدمة فحص التوقيع الإلكتروني، الختم الإلكتروني، البصمة الزمنية الإلكترونية، نظير مقابل يحدد فئاته مجلس إدارة الهيئة، وتتحقق الهيئة فى سبيل القيام بذلك مما يأتي:

(أ) سلامة شهادة التصديق الإلكترونى وتوافقها مع بيانات إنشاء التوقيع الإلكترونى أو الختم الإلكتروني.

(ب) إمكان تحديد مضمون المحرر الإلكترونى محل الفحص بدقة.

(ج) سهولة العلم بشخص الموقع أو منشئ الختم.

(د) توافر الشروط الواردة فى المادة (٤) من هذه اللائحة؛ وذلك لفحص البصمة الزمنية الإلكترونية.

مـــادة (٩)

مع عدم الإخلال بالشروط المنصوص عليها فى القانون، تتحقق حجية الإثبات المقررة للكتابة الإلكترونية والمحررات الإلكترونية الرسمية أو العرفية لمنشئها، إذا توافرت الضوابط الفنية والتقنية الآتية :

(أ) أن يكون متاحاً فنياً تحديد وقت وتاريخ إنشاء الكتابة الإلكترونية أو المحررات الإلكترونية الرسمية أو العرفية، وأن تتم هذه الإتاحة من خلال نظام حفظ إلكترونى مستقل وغير خاضع لسيطرة منشئ هذه الكتابة أو تلك المحررات، أو لسيطرة المعنى بها.

(ب) أن يكون متاحاً فنياً تحديد مصدر إنشاء الكتابة الإلكترونية أو المحررات الإلكترونية الرسمية أو العرفية ودرجة سيطرة مُنشئها على هذا المصدر وعلى الوسائط المستخدمة فى إنشائها.

(جـ) فى حالة إنشاء وصدور الكتابة الإلكترونية أو المحررات الإلكترونية الرسمية أو العرفية بدون تدخل بشري، جزئى أو كلي، فإن حجيتها تكون متحققة متى أمكن التحقق من وقت وتاريخ إنشائها ومن عدم العبث بهذه الكتابة أو تلك المحررات.

مادة (١٠)

يتحقق من الناحية الفنية والتقنية، ارتباط التوقيع الإلكتروني بالموقع وحده دون غيره متى استند هذا التوقيع إلى منظومة تكوين بيانات إنشاء توقيع إلكتروني مؤمنة على النحو الوارد في المواد (٢، ٣، ٥) من هذه اللائحة، وتوافرت إحدى الحالتين الآتيتين :

(أ) أن يكون هذا التوقيع مرتبطاً بشهادة تصديق إلكتروني معتمدة ونافذة المفعول صادرة من جهة تصديق إلكترونى مرخص لها أو معتمدة.

(ب) أن يتم التحقق من صحة التوقيع الإلكترونى طبقاً للمادة (٨) من هذه اللائحة.

مادة (١١)

تتحقق من الناحية الفنية والتقنية، سيطرة الموقع وحده دون غيره، على الوسيط الإلكترونى المستخدم فى عملية تثبيت التوقيع الإلكترونى عن طريق حيازة الموقع أو تحكمه فى أداة حفظ المفتاح الشفرى الخاص.

مادة (١٢)

مع عدم الإخلال بما هو منصوص عليه فى المواد (٢، ٣، ٥) من هذه اللائحة، يتم من الناحية الفنية والتقنية، كشف أى تعديل أو تبديل فى بيانات المحرر الإلكتروني الموقع إلكترونياً، باستخدام تقنية شفرة المفتاحين العام والخاص، وبمضاهاة شهادة التصديق الإلكتروني وبيانات إنشاء التوقيع الإلكترونى بأصل هذه الشهادة وتلك البيانات، أو بأى وسيلة مشابهة.

مادة (١٣)

يجب أن يتوافر لدى طالب الحصول على الترخيص بمزاولة نشاط تقديم خدمات التوقيع الإلكتروني المتطلبات التالية :

(أ) نظام تأمين للمعلومات وحماية البيانات وخصوصيتها، بمستوى حماية لا تقل عن المستوى المذكور فى المعايير والقواعد، المشار إليها فى الفقرة (د) من الملحق الفنى والتقنى المرفق بهذه اللائحة.

(ب) دليل إرشادى يتضمن ما يلي :

١-إصدار شهادات التصديق الإلكتروني.

٢-إدارة المفاتيح الشفرية.

٣-إدارة الأعمال الداخلية.

٤-إدارة التأمين والكوارث.

وذلك وفقاً للمعايير الفنية والتقنية المذكورة فى الفقرة (هـ) من الملحق الفنى والتقنى المرفق بهذه اللائحة.

(جـ) منظومة تكوين بيانات إنشاء التوقيع الإلكترونى مؤمنة وفقاً للضوابط الفنية والتقنية المنصوص عليها فى المواد (٢، ٣، ٥) من هذه اللائحة.

(د) نظام لتحديد تاريخ ووقت إصدار الشهادات، وإيقافها، وتعليقها، وإعادة تشغيلها ، وإلغائها.

(هـ) نظام للتحقق من الأشخاص المصدر لهم شهادات التصديق الإلكتروني، والتحقق من صفاتهم المميزة.

(و) المتخصصون من ذوى الخبرة الحاصلين على المؤهلات الضرورية لأداء الخدمات المرخص بها.

(ز) نظام حفظ بيانات إنشاء التوقيع الإلكترونى وشهادات التصديق الإلكترونى طوال المدة التى تحددها الهيئة فى الترخيص، وتبعاً لنوع الشهادة المصدرة، وذلك فيما عدا مفاتيح الشفرة الخاصة التى تصدرها للموقع فلا يتم حفظها إلا بناء على طلب من الموقع وبموجب عقد مستقل يتم إبرامه بين المرخص له والموقع ووفقاً للقواعد الفنية والتقنية لحفظ هذه المفاتيح التى يضعها مجلس إدارة الهيئة.

(ح) نظام للحفاظ على السرية الكاملة للأعمال المتعلقة بالخدمات التى يرخص بها، وللبيانات الخاصة بالعملاء.

(ط) نظام لإيقاف الشهادة فى حالة ثبوت توافر حالة من الحالات الآتية :

١ – العبث ببيانات الشهادة أو انتهاء مدة صلاحيتها.

٢ – سرقة أو فقد المفتاح الشفرى الخاص أو أداة التوقيع الإلكترونى ، أو عند الشك فى حدوث ذلك.

٣ – عدم التزام الشخص المصدر له شهادة التصديق الإلكترونى ببنود العقد المبرم مع المرخص له.

ويكون نظام إيقاف الشهادات وفقاً للقواعد والضوابط التى يضعها مجلس إدارة الهيئة.

(ك) نظام يتيح وييسر للهيئة التحقق من صحة بيانات إنشاء التوقيع الإلكتروني، وبخاصة فى إطار أعمال الفحص والتحقق من جانب الهيئة.

مادة (١٤)

فى جميع الأحوال، يلتزم المرخص له بعدم إبرام أى عقد مع العملاء إلا بعد اعتماد نموذج هذا العقد من الهيئة، طبقاً للقواعد والضوابط التى يضعها مجلس إدارة الهيئة فى هذا الشأن لضمان حقوق ذوى الشأن.

مادة (١٥)

على طالب الترخيص بمزاولة نشاط تقديم خدمات التوقيع الإلكتروني، أن يقدم الضمانات والتأمينات التى يحددها مجلس إدارة الهيئة، لتغطية أى أضرار أو أخطار تتعلق بذوى الشأن، وذلك فى حالة إنهاء الترخيص لأى سبب، أو لتغطية أى إخلال من جانبه لالتزاماته الواردة فى الترخيص.

مادة (١٦)

تُتبع الإجراءات الآتية ، للحصول على الترخيص بمزاولة نشاط تقديم خدمات التوقيع الإلكتروني :

(أ) التقدم بالطلب على النماذج التى تعدها الهيئة فى هذا الشأن مصحوباً بالبيانات والمستندات الدالة على توافر الشروط والأحكام المنصوص عليها فى المواد (٣، ٥، ١٣، ١٥) من هذه اللائحة.

(ب) تقوم الهيئة بعد تسلمها لكافة المستندات والبيانات المطلوبة، وفقاً للبند (أ) من طالب الترخيص بفحصها والتأكد من سلامتها، وتبت الهيئة فى طلب الحصول على الترخيص خلال مدة لا تتجاوز ستين يوماً من تاريخ استيفاء طالب الترخيص لجميع ما تطلبه الهيئة منه، ما لم تخطر الهيئة طالب الترخيص بمد هذه المدة، وفى حالة انقضاء هذه المدة دون إصدار الترخيص يعتبر الطلب مرفوضاً.

(ج) يحدد مجلس إدارة الهيئة مقابل إصدار وتجديد الترخيص وقواعد وإجراءات اقتضائه ، ويلتزم المرخص له بسداد هذا المقابل عند منح الترخيص.

(د) تمنح الهيئة الترخيص طبقاً للإجراءات والقواعد والضمانات المنصوص عليها فى القانون وفى هذه اللائحة ، وما يقره مجلس إدارة الهيئة من قواعد فى هذا الشأن .

مادة (١٧)

للهيئة منح ترخيص خاص لجهة التصديق الإلكترونى الحكومية، لمزاولة أنشطة خدمات التوقيع الإلكتروني، يقتصر التعامل بها على تسيير العمل الداخلى فى الجهات الحكومية وبين بعضها البعض، بذات الشروط المنصوص عليها فى القانون وهذه اللائحة، مع مراعاة أن يتم التصديق على المفاتيح الشفرية الجذرية الخاصة بجهة التصديق الإلكترونى الحكومية بواسطة الهيئة.

وللهيئة منح ترخيص خاص لبعض الجهات الحكومية الأخرى ، لتقديم خدمات التوقيع الإلكترونى ، وفقاً للشروط والضوابط التى يصدر بها قرار من مجلس إدارة الهيئة ، مع مراعاة أن يتم التصديق على المفاتيح الشفرية الجذرية الخاصة بهذه الجهات بواسطة الهيئة .

مادة (١٨)

تقوم الهيئة بالتفتيش على الجهات المرخص لها ، للتحقق من مدى التزامها بالترخيص .

مادة (١٩)

يُحدد فى الترخيص التزامات المرخص له ، وفقاً للقانون وهذه اللائحة والقرارات الصادرة من مجلس إدارة الهيئة فى هذا الشأن .

مادة (٢٠)

ينشأ جدول خاص بالهيئة تُقيد فيه الجهات المرخص لها، ويُعطى لكل جهة رقم مسلسل ، ويحدد فيه نوع الترخيص الممنوح لها، ويتضمن بيانات عن هذه الجهة ورأس مالها وأعضاء مجلس إدارتها والمديرين بها وفروعها ومكاتبها وغير ذلك من البيانات التى يحددها مجلس إدارة الهيئة .

مـــادة (٢١)

تكون الهيئة هى الجهة المختصة بتقديم المشورة الفنية وأعمال الخبـــرة ، بـــشأن المنازعات التى تنشأ بين الأطراف المعنية بأنشطة التوقيـــع الإلكترونـــى والمعـــاملات الإلكترونية وتكنولوجيا المعلومات ، على أن يتم التنسيق مع الجهات المعنية فيما يتعلق بأعمال الخبرة .

مـــادة (٢٢)

يجب أن تشتمل نماذج شهادات التصديق الإلكترونى التى يصدرها المرخص له علـــى البيانات الآتية، وذلك على نحو متوافق مع المعايير المحددة فى الفقرة (أ) من الملحق الفنـــى والتقنى المرفق بهذه اللائحة :

١- ما يفيد صلاحية هذه الشهادة للاستخدام فى التوقيع الإلكترونى .

٢- موضوع الترخيص الصادر للمرخص له، موضحاً فيه نطاقـــه ورقمـــه وتـــاريخ إصداره وفترة سريانه .

٣- اسم وعنوان الجهة المصدرة للشهادة ومقرها الرئيسى وكيانها القـــانونى والدولـــة التابعة لها (إن وجدت) .

٤- اسم الموقع الأصلى أو اسمه المستعار أو اسم شـــهرته، وذلـــك فـــى حالـــة استخدامه لأحدهما.

٥- صفة الموقع.

٦- المفتاح الشفرى العام لحائز الشهادة المناظر للمفتاح الشفرى الخاص به.

٧- تاريخ بدء صلاحية الشهادة وتاريخ انتهائها.

٨- رقم مسلسل للشهادة.

٩- التوقيع الإلكترونى لجهة إصدار الشهادة.

١٠- عنوان الموقع الإلكترونى (Web Site) المخصص لقائمة الـــشهادات الموقوفـــة أو الملغاة .

ويجوز أن تشتمل الشهادة على أى من البيانات الآتية عند الحاجة :

١- ما يفيد اختصاص الموقع والغرض الذى تستخدم فيه الشهادة.

٢- حد قيمة التعاملات المسموح بها بالشهادة.

٣- مجالات استخدام الشهادة.

مـــادة (٢٣)

تتحدد النسختان الخاصتان ببصمتى شـــهادتى الـــسلطة الجذريـــة العليـــا للتـــصديق الإلكترونى الموقعتين ذاتياً بالأحرف والأرقام والرموز المبينة بالشكلين رقمى (١، ٢) مـــن مرفق البصمات الوارد فى الفقرة (و) من الملحق الفنى والتقنى المرفـــق بهـــذه اللائحـــة، وتستخدم البصمة من الكافة للتيقن والتثبت من صحة وسلامة شهادة التصديق الإلكترونـــى الجذرية الموقعة ذاتياً والمتاحة عبر شبكة المعلومات الدولية على الموقع التالي:

https://www.itida.gov.eg/English/Uploads/RootCA_Fingerprint.pdf

مـــادة (٢٤)

للهيئة اعتماد الجهات الأجنبية المختصة بإصدار شهادات التصديق الإلكترونـــى، فـــى إحدى الحالات الآتية :

(أ) أن يتوافر لدى الجهة الأجنبية القواعد والاشتراطات المبينة فـــى هـــذه اللائحـــة بالنسبة للجهات التى ترخص لها الهيئة بمزاولـــة نـــشاط إصـــــدار شـــهادات التصديق الإلكتروني.

(ب) أن يكون لدى الجهة الأجنبية وكيل فى جمهورية مصر العربية مرخص له مـــن قبل الهيئة بإصدار شهادات التصديق الإلكتروني، ويتوافر لديه كـــل المقومـــات المطلوبة للتعامل بشهادات التصديق الإلكتروني، ويكفل تلك الجهة فيما تـــصدره من شهادات تصديق إلكترونى وفيما هو مطلوب من اشتراطات وضمانات.

(ج) أن تكون الجهة الأجنبية ضمن الجهات التى وافقت جمهوريـــة مـــصر العربيـــة بموجب اتفاقية دولية نافذة فيها على اعتمادها باعتبارها جهة أجنبيـــة مختـــصة بإصدار شهادات التصديق الإلكتروني.

(د) أن تكون الجهة الأجنبية ضمن الجهات المعتمـــدة أو المـــرخص لهـــا بإصـــدار شهادات تصديق إلكترونى من قبل جهة الترخيص فى بلدها، وبشرط أن يكـــون هناك اتفاقاً بين جهة الترخيص الأجنبية وبين الهيئة على ذلك.

ويكون اعتماد تلك الجهات الأجنبية، بناءً على طلب مقدم منها أو من ذوى الشأن على النماذج التى تعدها الهيئة، كما يكون للهيئة فى الحالات المشار إليها فى البنود (أ، ج، د) من هذه المادة، اعتماد تلك الجهات من تلقاء نفسها.

وفى حالة التقدم بطلب للاعتماد، تقوم الهيئة بعد تسلمها للمستندات والبيانات المطلوبة بفحصها والتأكد من سلامتها ويبت مجلس إدارة الهيئة فى طلب الاعتماد خلال مدة لا تجاوز ستين يوماً من تاريخ استيفاء الجهة الأجنبية لكل ما تطلبه الهيئة، وفى حالة انقضاء هذه المدة دون إصدار الاعتماد، يعتبر الطلب مرفوضاً، ما لم تخطر الهيئة كتابة الجهة الطالبة بمد هذه المدة.

ويصدر قرار اعتماد الجهة الأجنبية من مجلس إدارة الهيئة بعد سداد المقابل الذى يحدده المجلس للاعتماد، ويحدد فى القرار مدة الاعتماد وأحوال تجديده، وللهيئة دائماً، بقرار مسبب، الحق فى إلغاء الاعتماد أو وقفه.

مادة (٢٥)

للجهات الأجنبية المعتمدة أن تطلب من الهيئة اعتماد أنواع أو فئات شهادات التصديق الإلكترونى التى تصدرها، ويكون ذلك وفقاً للقواعد والضوابط التى يضعها مجلس إدارة الهيئة فى هذا الشأن، وكذلك تحديد المقابل لاعتماد هذه الشهادات، ويحدد مجلس إدارة الهيئة عند اعتماده لأنواع وفئات الشهادات الأجنبية ما يناظرها من شهادات تصديق إلكترونى صادرة من الجهات المرخص لها فى جمهورية مصر العربية.

مادة (٢٦)

مع عدم الإخلال بالعقوبات المنصوص عليها فى المادة (٢٣) من القانون، يلتزم المرخص له بجميع أحكام الترخيص الصادر له من الهيئة، وفى حالة مخالفة المرخص لأى منها أو توقفه عن مزاولة النشاط المرخص، أو اندماج منشأته فى جهة أخرى ، أو تنازله عن الترخيص للغير، دون الحصول على موافقة كتابية مسبقة من الهيئة على أى من هذه الأفعال المشار إليها، يجوز للهيئة، بقرار مسبب، عندئذ إلغاء الترخيص أو وقفه لحين التدارك أو التصحيح.

ويجوز للهيئة فى حالتى الإلغاء أو الوقف أن تتخذ التدابير المناسبة فى هذا الشأن لحماية حقوق ذوى الشأن.

مـــادة (٢٧)

تصدر الهيئة دليل اعتماد منتجات وتطبيقات وأدوات التوقيع الإلكترونـــى المـــستخدمة داخل جمهورية مصر العربية.

الملحق الفنى والتقني

يعمل بالمعايير الفنية والتقنية المنصوص عليها فى هذا الملحق، وتنشر أيـــة تعـــديلات أو إضافات لاحقة يقرها مجلس إدارة الهيئة فى الوقائع المصرية وذلك بعد اعتمادهـــا مـــن الوزير المختص.

(الفقرة – أ)

PKI Technology

- The profiles for PKI operational management protocols must be based on PKIX (X.509-based PKI).

- Public Key Infrastructure and Certificate Revocation List (CRL) profile must be based on X.509 5280 and its update

- Time stamp service (TSP) profile must be according to the RFC 3161 and its update

- Online Certificate Status Protocol (OCSP) profile must be according to the RFC 6960 and its updates

- At least one of the following algorithms must be deployed.

○ Symmetric algorithms (AES, 3DES, CAST6, BLOWFISH, TWOFISH, IDEA.)

○ Asymmetric algorithms (DSA, RSA, ELGamal)

○ Hash algorithms (SHA2 with 224/256/384/512 bit output)

- Minimum RSA/DSA key lengths must be at least 2048 bits. Increasing the length to 4096 bits is recommended with a view to guaranteeing Long term security levels.

- A baseline Certificate Policy for service providers issuing qualified certificates should be written according to the IETF (Internet Engineering Task Force) PKIX framework RFC 3647.

- electronic signature supports LTV (long term verification) that may be technically implemented through electronic signature standards e.g (XAdES (XML Advanced Electronic Signature) Baseline Profile, CAdES (CMS Advanced Electronic Signature) Baseline Profile, PAsES (PDF Advanced Electronic Signature) Baseline Profile)

(الفقرة – ب)

Hardware Security Modules

- For e-signature creation and verification product and in trustworthy hardware devices used as secure signature creation devices, it is required to have concurrent acceptance and usage of FIPS 140-2 level 3 or higher, or CC EAL5+ or higher.

(الفقرة – جـ)

Electronic signature creation devices

The creation devices are able to store private e-signature keys for its holder without delivering the key to the outside world. Therefore, the calculation of the signature algorithm as well as its storage is performed in a highly secure environment inside a creation device. Thus, it is required to have creation devices which use the most advanced security standard available in the market.

Feature	Details
Supported operating systems	Windows server 2008/R2, Windows Server 2012 and 2012 R2, Mac OS, Linux, Windows 8, Windows 10
API & Standards Support	PKCS#11, Microsoft CAPI, PC/SC, X.509 v3 certificate
On-board security algorithms	• Symmetric: 3DES (ECB, CBC), AES (128, 192, 256 bits) • Hash: SHA-256, SHA-384, SHA-512 • RSA: up to RSA 2048 bits (and optionally up to 4096 bits) • Elliptic curves: P-256, ECDSA, ECDH • On-card asymmetric key pair generation (RSA up to RSA2048 & Elliptic curves
Security certifications	FIPS 140-2 level 3 or higher or CC EAL5+ or higher

(الفقرة – د)

Security Standards

Information Security Management Standard (ISMS) as ISO/IEC 27001 and its guidance ISO 27002 (recommended)

(الفقرة – هـ)

Operation Standards

ETSI (The European Telecommunications Standards Institute)_ETSI EN 319 411-1 V1.2.2 (2018-04) Policy requirements for certification authorities issuing qualified certificates, specifically Chapter 5,6 which covers the following parts:

- Certification practice statement
- Key management life cycle
- Certificate Management life cycle
- CA management and operation
- Or equivalent standard.

(الفقرة – و)

الشكل رقم (١): بصمة شهادة السلطة الجذرية العليا للتصديق الإلكترونى الموقعة ذاتياً والتى تنتهى صلاحيتها فى ٢٠٣٩/٦/٢٨

Certificate Serial Number (S/N):
1a b6 bd a8 fa 1d f7 5d

Subject Key Identifier:
6c0c1eae8e8cecacda93d3d8315cadf31044d333

Certificate Thumbprint:
d0ed83a8437a8c09e6ce24386405c6f3420f2fc0

الشكل رقم (٢): بصمة شهادة السلطة الجذرية العليا للتصديق الإلكترونى الموقعة ذاتياً والتى تنتهى صلاحيتها فى ٢٠٢١/١٢/١٦

Certificate Serial Number (S/N):
- In Decimal format:
  316106808358849935558301793959016671478894840111
- In Hexadecimal format:
  37 5e b8 32 b4 aa a5 d5 79 01 65 af 9e 40 a2 cf 93 a4 49 2f

Certificate fingerprint(s):
SHA-256: 95B7-A513-8AD8-937F-4855-79A7-5BDC-2C07-5F91-A851-E446-C35E-B75B-856A-1684-0549