

الوقائع المصرية - العدد ١١٥ تابع - في ٢٥ مايو سنة ٢٠٠٥

قرار وزير الاتصالات وتكنولوجيا المعلومات

رقم ١٠٩ لسنة ٢٠٠٥ بتاريخ ١٥/٥/٢٠٠٥

بشأن إصدار اللائحة التنفيذية لقانون التوقيع الإلكتروني

وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات

(وفقاً لأخر تعديل صادر في ٢ يولية عام ٢٠٢٤)

وزير الاتصالات وتكنولوجيا المعلومات

بعد الاطلاع على الدستور؛

وعلى القانون المدنى؛

وعلى قانون التجارة؛

وعلى القانون رقم ١٣ لسنة ١٩٦٨ بشأن المرافعات المدنية والتجارية؛

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

وعلى القانون رقم ٨٢ لسنة ٢٠٠٢ بشأن حماية حقوق الملكية الفكرية؛

وعلى القانون رقم ١٠ لسنة ٢٠٠٣ بشأن تنظيم الاتصالات؛

وعلى قانون رقم ١٥ لسنة ٢٠٠٤ بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة

تكنولوجيا المعلومات؛

وعلى قرار رئيس الجمهورية رقم ٢٠١ لسنة ٢٠٠٤ بتشكيل الوزارة؛

قرار

(المادة الأولى)

يعمل بأحكام اللائحة التنفيذية للقانون رقم ١٥ لسنة ٢٠٠٤ بتنظيم التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المرفقة.

(المادة الثانية)

ينشر هذا القرار في الوقائع المصرية, ويعمل به من اليوم التالي لتاريخ نشره.

وزير الاتصالات وتكنولوجيا المعلومات

دكتور/ طارق كامل

اللائحة التنفيذية للقانون رقم ١٥ لسنة ٢٠٠٤

بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات

مادة (١)

في تطبيق أحكام هذه اللائحة يقصد بالمصطلحات الآتية المعاني المبينة قرين كل منها:

١- التوقيع الإلكتروني:

ما يوضع على محرر إلكتروني 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 أي علامات أخرى تثبت على دعامة الكترونية أو رقمية أو ضوئية أو أية وسيلة أخرى مشابهة وتعطي دلالة قابلة للإدراك.

٣- المحرر الإلكتروني:

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 الإلكتروني:

أداة أو أدوات أو أنظمة إنشاء التوقيع الإلكتروني.

٥- الموقع:

الشخص الحائز على بيانات إنشاء التوقيع ويوقع عن نفسه أو عن ينيبه أو يمثله قانوناً.

٦- جهات التصديق الإلكتروني:

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

٧- شهادة التصديق الإلكتروني:

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

٨- بيانات إنشاء التوقيع الإلكتروني:

عناصر متفردة خاصة بالموقع وتميزه عن غيره، ومنها على الأخص مفاتيح الشفرة الخاصة به، والتي تستخدم في إنشاء التوقيع الإلكتروني.

٩- الختم الإلكتروني: Electronic seal

هو توقيع إلكتروني يسمح بتحديد - الشخص الاعتباري - منشئ الختم ويميزه عن غيره.

١٠- منشئ الختم:

الشخص الاعتباري الحائز على بيانات إنشاء الختم الإلكتروني واستخدامه.

١١ - بيانات إنشاء الختم الإلكتروني:

عناصر متفردة خاصة بُمُنشئ الختم الإلكتروني وتميزه عن غيره، ومنها على الأخص مفاتيح الشفرة الخاصة به، والتي تُستخدم في إنشاء الختم الإلكتروني.

١٢ - شهادة الختم الإلكتروني:

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

١٣ - البصمة الزمنية الإلكترونية: Time Stamp

ما يوضع على محرر الكتروني ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها والتي تربط تلك البيانات بوقت محدد لإثبات وجود هذا المحرر الإلكتروني في 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 طبيعي أو معنوي بأن يكون لديه مفتاحين متفردين، أحدهما عام متاح إلكترونياً، والثاني خاص يحتفظ به الشخص ويحفظه على درجة عالية من السرية.

١٦ - المفتاح الشفري العام:

أداة إلكترونية متاحة للكافة، تنشأ بواسطة عملية حسابية خاصة، وتستخدم في التحقق من شخصية الموقع على المحرر الإلكتروني، والتأكد من صحة وسلامة محتوى المحرر الإلكتروني الأصلي.

١٧-المفتاح الشفري الخاص:

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

١٨-المفتاح الشفري الجذري:

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

١٩- الدعامة الإلكترونية:

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

٢٠- أداة التوقيع الإلكتروني:

وسيط إلكتروني مؤمن يُستخدم في عملية إنشاء وتثبيت التوقيع الإلكتروني على المحرر الإلكتروني، 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 في 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 الإلكتروني باستخدام المفتاح الشفري الجذري، ويشمل ذلك بيانات إنشاء الختم الإلكتروني .

٢٢- شهادة فحص بيانات إنشاء التوقيع الإلكتروني:

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

٢٣- شهادة فحص التوقيع الإلكتروني:

شهادة تصدرها الهيئة بنتيجة فحصها لصحة وسلامة التوقيع الإلكتروني، بما في ذلك الختم الإلكتروني.

٢٤- شهادة اعتماد جهات التصديق الإلكتروني الأجنبية:

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

٢٥- بصمة شهادة السلطة الجزرية العليا للتصديق الإلكتروني:

هي بصمة متفردة تتكون من أحرف وأرقام ورموز، تنتج من عملية حسابية أحادية الاتجاه، يتم إجراؤها على محتويات شهادة السلطة الجزرية العليا للتصديق الإلكتروني 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 بشؤون الاتصالات وتكنولوجيا المعلومات.

٢٨- الوزير المختص:

الوزير المختص بشؤون الاتصالات وتكنولوجيا المعلومات.

٢٩- القانون:

القانون رقم ١٥ لسنة ٢٠٠٤ بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات. (٢)(٣)

مادة (٢)

تكون منظومة تكوين بيانات إنشاء التوقيع الإلكتروني مؤمنة متى استوفت ما يأتي:

- (أ) الطابع المتفرد لبيانات إنشاء التوقيع الإلكتروني.
- (ب) سرية بيانات إنشاء التوقيع الإلكتروني.
- (ج) عدم قابلية الاستنتاج أو الاستنباط لبيانات إنشاء التوقيع الإلكتروني.
- (د) حماية التوقيع الإلكتروني من التزوير، أو التقليد، أو التحريف، أو الاصطناع أو غير ذلك من صور التلاعب، أو من إمكان إنشائه من غير الموقع.
- (هـ) عدم إحداث أي إتلاف بمحتوى أو مضمون المحرر الإلكتروني المراد توقيعه.
- (و) ألا تحول هذه المنظومة دون علم الموقع علما تاما بمضمون المحرر الإلكتروني قبل توقيعه له.
- (ز) أن تربط التوقيع الإلكتروني بالمحرر الإلكتروني بطريقة متفردة تمنع إجراء أي تعديل بعد عملية التوقيع دون اكتشافه. (٣)

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 المفاتيح العام والخاص وإلى المفتاح الشفري الجذري الخاص بالجهة المرخص لها والذي تصدره لها الهيئة، وذلك كله وفقاً للمعايير الفنية والتقنية المشار إليها في الفقرة (أ) من الملحق الفني والتقني المرفق بهذه اللائحة.
- (ب) أن تكون التقنية المستخدمة في إنشاء مفاتيح الشفرة الجذرية لجهات التصديق الإلكتروني من التي تستعمل مفاتيح تشفير بأطوال لا تقل عن ٤٠٩٦ حرف إلكتروني. (bit)

(ج) أن تكون أجهزة التأمين الإلكتروني (Hardware Security Modules) المستخدمة معتمدة طبقاً للضوابط الفنية والتقنية المشار إليها في الفقرة (ب) من الملحق الفني والتقني المرفق بهذه اللائحة.

(د) أن يتم استخدام أدوات توقيع إلكتروني غير قابلة للنسخ ومحمية بكود سري، تحتوي على عناصر متفردة للموقع وهي بيانات إنشاء التوقيع الإلكتروني وشهادة التصديق الإلكتروني، ويتم تحديد مواصفات أداة التوقيع الإلكتروني وأنظمتها، وفقاً للمعايير الفنية والتقنية المبينة في الفقرة (ج) من الملحق الفني والتقني المرفق بهذه اللائحة.

(هـ) أن تضمن المنظومة لجميع أطراف التعامل إتاحة البيانات الخاصة بالتحقق من صحة التوقيع الإلكتروني، وارتباطه بالموقع دون غيره، وأن تضمن أيضاً عملية الإدراج الفوري والإتاحة اللحظية لقوائم الشهادات الموقوفة أو الملغاة، وذلك فور التحقق من توافر أسباب تستدعي إيقاف الشهادة، على أن يتم هذا التحقق خلال فترة محددة ومعلومة للمستخدمين، حسب القواعد والضوابط التي يضعها مجلس إدارة الهيئة. (٣)

مادة (٤)

يشترط لإثبات البصمة الزمنية الإلكترونية توافر ما يلي:

(أ) أن تربط التاريخ والوقت بال محرر الإلكتروني بطريقة تمنع إمكانية تغيير البيانات دون اكتشافها.

(ب) أن يستند إلى مصدر زمني دقيق معتمد من السلطة الجزرية العليا للتصديق الإلكتروني.

(ج) يُجرى إنشاءه بواسطة السلطة الجزرية العليا للتصديق الإلكتروني أو من إحدى الجهات

المرخص لها من قبل الهيئة، وفقاً للضوابط الفنية والتقنية المنصوص عليها في الفقرة (أ)

من الملحق الفني والتقني المرفق بهذه اللائحة. (٣)

مادة (٥)

لمجلس إدارة الهيئة أن يضع نظم وقواعد أخرى لمنظومة تكوين بيانات إنشاء التوقيع الإلكتروني؛ لمواكبة التطورات التقنية والتكنولوجية. (٣)

مادة (٦)

الهيئة هي السلطة الجذرية العليا للتصديق الإلكتروني في جمهورية مصر العربية، وتتولى إصدار المفاتيح الشفورية الجذرية الخاصة للجهات المرخص لها بإصدار شهادات التصديق الإلكتروني. وتتحقق الهيئة قبل منح ترخيص مزاولة نشاط تقديم خدمات التوقيع الإلكتروني من أن منظومة تكوين بيانات إنشاء التوقيع الإلكتروني لدى الجهة المرخص لها مؤمنة طبقاً للمادة (٢) من هذه اللائحة، ومتضمنة الضوابط الفنية والتقنية والنظم والقواعد المبينة في المادتين (٣، ٥) من هذه اللائحة. وتعتبر المنظومة بعد منح الترخيص وطوال مدة نفاذ مفعوله، مؤمنة وفعالة ما لم يثبت العكس. (٣)

مادة (٧)

تقدم الهيئة، بناءً على طلب كل ذي شأن، خدمة الفحص والتحقق من صحة بيانات إنشاء التوقيع الإلكتروني والختم الإلكتروني نظير مقابل يحدد فئاته مجلس إدارة الهيئة، ويجوز للهيئة أن تعهد للغير بتقديم هذه الخدمة تحت إشرافها. وفي جميع الأحوال، تصدر الهيئة شهادة فحص بيانات إنشاء التوقيع الإلكتروني. (٣)

مادة (٨)

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

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

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

(ج) سهولة العلم بشخص الموقع أو منشئ الختم.

(د) توافر الشروط الواردة في المادة (٤) من هذه اللائحة؛ وذلك لفحص البصمة الزمنية الإلكترونية. (٣)

مادة (٩)

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

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

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

(ج) في حالة إنشاء وصدور الكتابة الإلكترونية أو المحركات 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 المحركات. (٣)

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 إلكتروني مرخص لها أو معتمدة.

(ب) أن يتم التحقق من صحة التوقيع الإلكتروني طبقاً للمادة (٨) من هذه اللائحة. (٣)

مادة (١١)

تتحقق من الناحية الفنية والتقنية، سيطرة الموقع وحده دون غيره، على الوسيط الإلكتروني المستخدم في عملية تثبيت التوقيع الإلكتروني عن طريق حيازة الموقع أو تحكمه في أداة حفظ المفتاح الشفري الخاص. (٣)

مادة (١٢)

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

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 في المعايير والقواعد، المشار إليها في الفقرة (د) من الملحق الفني والتقني المرفق بهذه اللائحة.

(ب) دليل إرشادي يتضمن ما يلي:

١- إصدار شهادات التصديق الإلكتروني.

٢- إدارة المفاتيح الشفوية.

٣- إدارة الأعمال الداخلية.

٤- إدارة التأمين والكوارث.

وذلك وفقاً للمعايير الفنية والتقنية المذكورة في الفقرة (هـ) من الملحق الفني والتقني المرفق بهذه اللائحة.

(ج) منظومة تكوين بيانات إنشاء التوقيع الإلكتروني مؤمنة وفقاً للضوابط الفنية والتقنية المنصوص عليها في 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 ذوي الخبرة الحاصلين على المؤهلات الضرورية لأداء الخدمات المرخص بها.

(ز) نظام حفظ بيانات إنشاء التوقيع الإلكتروني وشهادات التصديق الإلكتروني طوال المدة التي تحددها الهيئة في الترخيص، وتبعاً لنوع الشهادة المصدرة، وذلك فيما عدا مفاتيح الشفرة الخاصة التي 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 التي يضعها مجلس إدارة الهيئة.

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

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

- ١- العبث ببيانات الشهادة أو انتهاء مدة صلاحيتها.
- ٢- سرقة أو فقد المفتاح الشفري الخاص أو أداة التوقيع الإلكتروني، أو عند الشك في حدوث ذلك.
- ٣- عدم التزام الشخص المصدر له شهادة التصديق الإلكتروني ببنود العقد المبرم مع المرخص له. ويكون نظام إيقاف الشهادات وفقاً للقواعد والضوابط التي يضعها مجلس إدارة الهيئة.
- (ك) نظام يتيح وييسر للهيئة التحقق من صحة بيانات إنشاء التوقيع الإلكتروني، وبخاصة في إطار أعمال الفحص والتحقق من جانب الهيئة. (٣)

مادة (١٤)

في جميع الأحوال، يلتزم المرخص له بعدم إبرام أى عقد مع العملاء إلا بعد اعتماد نموذج هذا العقد من الهيئة، طبقاً للقواعد والضوابط التي يضعها مجلس إدارة الهيئة في هذا الشأن لضمان حقوق ذوى الشأن. (٣)

مادة (١٥)

على طالب الترخيص بمزاولة نشاط تقديم خدمات التوقيع الإلكتروني، أن يقدم الضمانات والتأمينات التي 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. (٣)

مادة (١٥ مكرراً)

للهيئة منح ترخيص خاص لجهة التصديق الإلكتروني الحكومية لإصدار شهادات تصديق إلكتروني يقتصر التعامل بها على تسيير العمل الداخلي في الجهات الحكومية وبين بعضها البعض بذات الشروط المنصوص عليها في القانون وهذه اللائحة، مع مراعاة ما يلي:

"للهيئة أن تقرر استخدام تكنولوجيا وطنية بديلة لأجهزة أو أنظمة التشفير لتقديم خدمات التوقيع الإلكتروني، وما يترتب على ذلك من إعفاء تلك الأجهزة والأنظمة من شرط الحصول على شهادات المعايير الدولية المنصوص عليها في الملحق الفني الفقرة (ب) والفقرة (ج) من هذه اللائحة، وذلك مع اشتراط توافق تلك الأجهزة أو الأنظمة مع كافة المتطلبات والمواصفات المذكورة في تلك المعايير".

أن يتم التصديق على المفاتيح الشفرية الجذرية الخاصة بجهة التصديق الإلكتروني الحكومية بواسطة الهيئة. (١)

مادة (١٦)

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

(أ) التقدم بالطلب على النماذج التي 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 في 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، وفي 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 في القانون وفي هذه اللائحة ، وما يقره مجلس إدارة الهيئة من قواعد في هذا الشأن. (٣)

مادة (١٧)

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

وللهيئة منح ترخيص خاص لبعض الجهات الحكومية الأخرى لتقديم خدمات التوقيع الإلكتروني، وفقاً للشروط والضوابط التي يصدر بها قرار من مجلس إدارة الهيئة ، مع مراعاة أن يتم التصديق على المفاتيح الشفورية الجذرية الخاصة بهذه الجهات بواسطة الهيئة. (٣)

مادة (١٨)

تقوم الهيئة بالتفتيش على الجهات المرخص لها ، للتحقق من مدى التزامها بالترخيص . (٣)

مادة (١٩)

يُحدد في الترخيص التزامات المرخص له ، وفقاً للقانون وهذه اللائحة والقرارات الصادرة من مجلس إدارة الهيئة في هذا الشأن. (٣)

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 التي يحددها مجلس إدارة الهيئة. (٣)

مادة (٢٠ مكرراً)

تحدد النسختان الأساسية والاحتياطية لبصمتي شهادتي التصديق الإلكتروني الجذرية الموقعتين ذاتياً بالأحرف والأرقام والرموز المبينة بالشكلين رقمي (١ , ٢) من مرفق البصمات, وتستخدم البصمة من الكافة للتيقن والتثبت من صحة وسلامة شهادة التصديق الإلكتروني الجذرية الموقعة ذاتياً والمتاحة عبر شبكة المعلومات الدولية. (٢)

مادة (٢١)

تكون الهيئة هي الجهة المختصة بتقديم المشورة الفنية وأعمال الخبرة بشأن المنازعات التي تنشأ بين الأطراف المعنية بأنشطة التوقيع الإلكتروني والمعاملات الإلكترونية وتكنولوجيا المعلومات ، على أن يتم التنسيق مع الجهات المعنية فيما يتعلق بأعمال الخبرة. (٣)

مادة (٢٢)

يجب أن تشتمل نماذج شهادات التصديق الإلكتروني التي يصدرها المرخص له على البيانات الآتية، وذلك على نحو متوافق مع المعايير المحددة في الفقرة (أ) من الملحق الفني والتقني المرفق بهذه اللائحة:

- ١- ما يفيد صلاحية هذه الشهادة للاستخدام في التوقيع الإلكتروني.
- ٢- موضوع الترخيص الصادر للمرخص له، موضحاً فيه نطاقه ورقمه وتاريخ إصداره وفترة سريانه.
- ٣- اسم وعنوان الجهة المصدرة للشهادة ومقرها الرئيسى وكيانها القانونى والدولة التابعة لها (إن وجدت).
- ٤- اسم الموقع الأصى أو اسمه المستعار أو اسم شهرته، وذلك فى حالة 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 الإلكتروني لجهة إصدار الشهادة.
- ١٠- عنوان الموقع الإلكتروني (Web Site) المخصص لقائمة الشهادات الموقوفة 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. (٣)

مادة (٢٣)

تحدد النسختان الخاصتان ببصمتي شهادتي السلطة الجزرية العليا للتصديق الإلكتروني الموقعتين ذاتياً بالأحرف والأرقام والرموز المبينة بالشكلين رقمي (١، ٢) من مرفق البصمات الوارد في الفقرة (و) من الملحق الفني والتقني المرفق بهذه اللائحة، وتستخدم البصمة من الكافة للتيقن والتثبت من صحة وسلامة شهادة التصديق الإلكتروني الجزرية الموقعة ذاتياً والمتاحة عبر شبكة المعلومات الدولية على الموقع التالي (٣)

مادة (٢٤)

للهيئة اعتماد الجهات الأجنبية المختصة بإصدار شهادات التصديق الإلكتروني، في إحدى الحالات الآتية:

(أ) أن يتوافر لدى الجهة الأجنبية القواعد والاشتراطات المبينة في هذه اللائحة بالنسبة للجهات التي ترخص لها الهيئة بمزاولة نشاط إصدار شهادات التصديق الإلكتروني.

(ب) أن يكون لدى الجهة الأجنبية وكيل في جمهورية مصر العربية مرخص له من قبل الهيئة بإصدار شهادات التصديق الإلكتروني، ويتوافر لديه كل المقومات المطلوبة للتعامل بشهادات التصديق الإلكتروني، ويكفل تلك الجهة فيما تصدره من شهادات تصديق إلكتروني وفيما هو مطلوب من اشتراطات وضمانات.

(ج) أن تكون الجهة الأجنبية ضمن الجهات التي وافقت جمهورية مصر العربية بموجب اتفاقية دولية نافذة فيها على اعتمادها باعتبارها جهة أجنبية مختصة بإصدار شهادات التصديق الإلكتروني.

(د) أن تكون الجهة الأجنبية ضمن الجهات المعتمدة أو المرخص لها بإصدار شهادات تصديق إلكتروني من قبل جهة الترخيص في بلدها، وبشرط أن يكون 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 تتجاوز 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. (٣)

مادة (٢٥)

للجهات الأجنبية المعتمدة أن تطلب من الهيئة اعتماد أنواع أو فئات شهادات التصديق الإلكترونية 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. (٣)

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 في حالتى الإلغاء أو الوقف أن تتخذ التدابير المناسبة فى هذا الشأن لحماية حقوق ذوى الشأن.(٣)

مادة (٢٧)

تصدر الهيئة دليل اعتماد منتجات وتطبيقات وأدوات التوقيع الإلكتروني المستخدمة داخل جمهورية مصر العربية.(٣)

الملحق الفني والتقني

يعمل بالمعايير الفنية والتقنية المنصوص عليها في هذا الملحق ، وتنشر أية تعديلات أو إضافات لاحقة يقرها مجلس إدارة الهيئة في الوقائع المصرية وذلك بعد اعتمادها من الوزير المختص.(٣)

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 ٥٢٨٠ and its update

-Time stamp service (TSP) profile must be according to the RFC ٣١٦١ and its update

-Online Certificate Status Protocol (OCSP) profile must be according to the RFC ٦٩٦٠ and its updates

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

*Symmetric algorithms (AES, ٣DES, CAST٦, 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 PAdES(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 ج

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 ٢٠٠٨/R٢, Windows Server ٢٠١٢ and ٢٠١٢ R٢, Mac OS, Linux, Windows ٨, Windows ١٠
API & Standards	PKCS#١١, Microsoft CAPI, PC/SC, X.٥٠٩ v٣ certificate
On-board security algorithms	Symmetric: ٣DES (ECB, CBC), AES (١٢٨, ١٩٢, ٢٥٦ bits) Hash: SHA-٢٥٦, SHA-٣٨٤, SHA-٥١٢ RSA: up to RSA ٢٠٤٨ bits (and optionally up to ٤٠٩٦ bits) Elliptic curves: P-٢٥٦, ECDSA, ECDH On-card asymmetric key pair generation (RSA up to RSA ٢٠٤٨ & Elliptic curves
Security certifications	FIPS ١٤٠-٢ level ٣ or higher or CC EALS+ or higher

الفقرة د

Security Standards

Information Security Management Standard (ISMS) as ISO/IEC ۲۷۰۰۱ and its guidance ISO ۲۷۰۰۲ (recommended)

الفقرة هـ

Operation Standards

ETSI (The European Telecommunications Standards Institute)
ETSI EN ۳۱۹ ۴۱۱-۱ v۱,۲,۲(۲۰۱۸-۰۴) Policy requirements for certification authorities issuing qualified certificates, specifically Chapter ۵,۶ 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 (۱) بصمة شهادة السلطة الجذرية العليا للتصديق الإلكتروني الموقعة ذاتياً والتي تنتهي صلاحيتها في ۲۸/۶/۲۰۳۹

Certificate Serial Number (S/N): la b۶ bd a۸ fa ld f۷ ۵d

Subject Key Identifier:

۶c۰c۱eae۸e۸cecad۹۳d۳d۸۳۱۵cadf۳۱۰۴۴d۳۳۳

Certificate Thumbprint:

d۰ed۸۳a۸۴۳۷a۸c۰۹e۶ce۲۴۳۸۶۴۰۵c۶f۳۴۲۰f۲fc۰

الشكل رقم (٢): بصمة شهادة السلطة الجزرية العليا للتصديق الإلكتروني الموقعة ذاتياً والتي تنتهي صلاحيتها في ١٦/١٢/٢٠٢١

Certificate Serial Number (S/N):

• In Decimal format:

٣١٦١٠٦٨٠٨٣٥٨٨٤٩٩٣٥٥٥٨٣٠١٧٩٣٩٥٩٠١٦٦٧١٤٧٨٨٩٤٨٤٠١١١١

• In Hexadecimal format:

٣٧ ٥e b٨ ٣٢ b٤ aa a٥ d٥ ٧٩ ٠١ ٦٥ af ٩c ٤٠ a٢ cf ٩٣ a٤ ٤٩ ٢f

Certificates fingerprint(s):

SHA-٢٥٦:٩٥BY-A٥BY-A٥١٣-٨AD٨-٩٣٧F-٤٨٥٥-٧٩AY-٥BDC-

٢C٠٧-٥F٩١

-A٨٥١-E٤٤٦-C٣٥E-B٧٥B-٨٥٦A-١٦٨٤-٠٥٤٩

(١)تضاف مادة جديدة برقم (١٥ مكرراً) للقرار الوزاري رقم ١٠٩ لسنة ٢٠٠٥ وذلك وفقاً للقرار رقم ٧ لسنة ٢٠٠٧ المنشور بتاريخ ٢٠٠٧/١/١٤.

(٢)يضاف بند جديد للمادة الأولى برقم (٢٧) للقرار الوزاري رقم ١٠٩ لسنة ٢٠٠٥.

وتضاف مادة جديدة برقم (٢٠ مكرراً) للقرار الوزاري رقم ١٠٩ لسنة ٢٠٠٥ وذلك وفقاً للقرار رقم ٣٠٧ لسنة ٢٠١٠ المنشور بتاريخ ٢٠١٠/١١/٢١.

(٣)تعديل اللائحة التنفيذية للقانون ١٥ لسنة ٢٠٠٤ بقرار وزير الاتصالات وتكنولوجيا المعلومات رقم ٣٦١ لسنة ٢٠٢٠ المنشور بتاريخ ٢٣ / ٤ / ٢٠٢٠.

(٤)بتعديل اللائحة التنفيذية للقانون رقم ١٥ لسنة ٢٠٠٤ بتنظيم التوقيع الإلكتروني و بإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات وفقاً للقرار رقم ٤٦٧ لسنة ٢٠٢٤ المنشور بتاريخ ٢٠٢٤/٧/٢.