وزارة الاتصالات وتكنولوجيا المعلومات

قرار رقم ١٠٩ لسنة ٢٠٠٥

بتاريخ ١٥/٥/٢٠٠٥

بإصدار اللائحة التنفيذية لقانون التوقيع الإلكترونى

وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات

وزيـر 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 الإلكترونى وبإنشاء هيئة تنمية صناعة تكنولوچيا المعلومات ؛

وعلى قرار رئيس الجمهورية رقم ٢٠١ لسنة ٢٠٠٤ بتشكيل الوزارة ؛

قـــــرر :

(المـــادة الأولى)

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

(المـــادة الثانية)

ينشر هذا القرار فى الوقائع المصرية ، ويعمل به من اليوم التالى لتاريخ نشره .

وزير الاتصالات وتكنولوجيا المعلومات

دكتور / طارق كامل

مـــادة (١)

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

١ - التوقيع الإلكترونى :

ما يوضـع على محـرر إلكترونى ويتخـذ شـكل حـروف ، أو أرقـام ، أو رمـوز ، أو إشارات أو غيرها ويكون له طابع متفرد يسمح بتحديد شخص الموقع ويميزه عن غيره .

٢ - الكتابة الإلكترونية :

كل حـروف ، أو أرقـام ، 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 ، كليًا أو جزئيًا ، 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 الحائز على بيانات إنشاء التوقيع ويوقع عن نفسه أو عمن ينيبه أو يمثله قانونًا .

٦ - جهات التصديق الإلكترونى :

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

٧ - شهادة التصديق الإلكترونى :

الشـهادة التى تصدر من الجهـة المرخص لهـا بالتصـديق 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 - التشفير :

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

١٠ - 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 إلكترونيًا ، والثانى خاص يحتفظ به الشخص ويحفظه على درجة عالية من السرية .

١١ - المفتاح الشفرى العام :

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

١٢ - المفتاح الشفرى الخاص :

أداة إلكترونية خاصة بصاحبها ، تنشأ بواسطة عملية حسابية خاصة وتستخدم فى وضع التوقيع الإلكترونى على المحررات الإلكترونية ، ويتم الاحتفاظ بها على بطاقة ذكية مؤمنة .

١٣ - المفتاح الشفرى الجذرى :

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

١٤ - 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 .

١٥ - البطاقة الذكية :

وسيط إلكترونى مؤمن يستخدم فى عملية إنشاء وتثبيت التوقيع الإلكترونى على المحرر الإلكترونى ، ويحتوى على شريحة إلكترونية بها معالج إلكترونى وعناصر تخزين وبرمجيات للتشغيل ، ويشمل هذا التعريف الكروت الذكية والشرائح الإلكترونية المنفصلة (smart tokens) ، أو ما يماثلها فى تحقيق الوظائف المطلوبة بالمعايير التقنية والفنية المحددة فى هذه اللائحة .

١٦ - الحاسب الآلى :

جهاز إلكترونى قادر على تخزين ومعالجة وتحليل واسترجاع البيانات والمعلومات بطريقة إلكترونية .

١٧ - برنامج الحاسب الآلى :

مجموعة أوامر وتعليمات معبر عنها بأية لغة أو رمز أو إشارة ، وتتخذ أى شكل من الأشكال ، ويمكن استخدامها بطريقة مباشرة أو غير مباشرة فى حاسب آلى لأداء وظيفة أو تحقيق نتيجة ، سواء أكانت هذه الأوامر والتعليمات فى شكلها الأصلى أم فى أى شكل آخر تظهر فيه من خلال الحاسب الآلى .

١٨ - منظومة تكوين بيانات إنشاء التوقيع الإلكترونى :

مجموعة عناصر مترابطة ومتكاملة ، تحتوى على وسائطالكترونية وبرامج حاسب آلى يتم بواسطتها تكوين بيانات إنشاء التوقيع الإلكترونى باستخدام المفتاح الشفرى الجذرى .

١٩ - منظومة إنشاء التوقيع الإلكترونى :

مجموعة عناصر مترابطة ومتكاملة ، تحتوى على وسائط إلكترونية وبرامج حاسب آلى ويتم بواسطتها التوقيع الكترونيًا على المحرر الإلكترونى وذلك باستخدام بيانات إنشاء التوقيع الإلكترونى وشهادة التصديق الإلكترونى ، كما يتم بواسطتها وضع وتثبيت المحرر الموقع إلكترونيًا على دعامة إلكترونية .

٢٠ - شهادة فحص بيانات إنشاء التوقيع الإلكترونى :

شهادة تصدرها الهيئة بنتيجة الفحص والتحقق من صحة بيانات إنشاء التوقيع الإلكترونى .

٢١ - شهادة فحص التوقيع الإلكترونى :

شهادة تصدرها الهيئة بنتيجة فحصها لصحة وسلامة التوقيع الإلكترونى .

٢٢ - 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 .

٢٣ - الهيئة :

هيئة تنمية صناعة تكنولوجيا المعلومات .

٢٤ - الوزارة المختصة :

الوزارة المختصة بشئون الاتصالات وتكنولوجيا المعلومات .

٢٥ - الوزير المختص :

الوزير المختص بشئون الاتصالات وتكنولوجيا المعلومات .

٢٦ - القانون :

قانون 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 ما يأتى :

(أ) الطابع المتفرد لبيانات إنشاء التوقيع الإلكترونى .

(ب) سرية بيانات إنشاء التوقيع الإلكترونى .

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

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

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

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

مـــادة (٣)

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

(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 وفقًا للمعايير الفنية والتقنية المشار إليها فى الفقرة (أ) من الملحق الفنى والتقنى لهذه اللائحة .

(ب) أن تكون التقنية المستخدمة فى إنشاء مفاتيح الشفرة الجذرية لجهات التصديق الإلكترونى من التى تستعمل مفاتيح تشفير بأطوال لا تقل عن ٢٠٤٨ حرف إلكترونى (bit) .

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

(د) أن يتم استخدام بطاقات ذكية غير قابلة للاستنساخ ومحمية بكود سرى ، تحتوى على عناصر متفردة للموقع وهى بيانات إنشاء التوقيع الإلكترونى وشهادة التصديق الإلكترونى ، ويتم تحديد مواصفات البطاقة الذكية وأنظمتها ، وفقًا للمعايير الفنية والتقنية المبينة فى الفقرة (جـ) من الملحق الفنى والتقنى للائحة .

(هـ) أن تضمن المنظومة لجميع أطراف التعامل إتاحة البيانات الخاصة بالتحقق من صحة التوقيع الإلكترونى ، 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 .

مـــادة (٤)

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

مـــادة (٥)

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

وتتحقق الهيئة قبل منح ترخيص مزاولة نشاط إصدار شهادات التصديق الإلكترونى من أن منظومة تكوين بيانات إنشاء التوقيع الإلكترونى لدى الجهة المرخص لها مؤمنة طبقًا للمادة (٢) ، ومتضمنة الضوابط الفنية والتقنية والنظم والقواعد المبينة فى المادتين (٣ ، ٤) .

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

مـــادة (٦)

تقدم الهيئة ، بناء على طلب كل ذى شأن ، خدمة الفحص والتحقق من صحة بيانات إنشاء التوقيع 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 الإلكترونى .

مـــادة (٧)

تقدم الهيئة ، بناء على طلب كل ذى شأن ، خدمة فحص التوقيع الإلكترونى نظير مقابل يحدد فئاته مجلس إدارة الهيئة ، وتتحقق الهيئة فى سبيل القيام بذلك مما يأتى :

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

(ب) إمكان تحديد مضمون المحرر الإلكترونى الموقع بدقة .

(جـ) سهولة العلم بشخص الموقع ، سواء فى حالة استخدام اسمه الأصلى أم استخدامه لاسم مستعار أم اسم شهرة .

ويجوز للهيئة أن تعهد للغير بتقديم هذه الخدمة تحت إشرافها ، وفى جميع الأحوال تصدر الهيئة شهادة فحص التوقيع الإلكترونى .

مـــادة (٨)

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 متاحًا فنيًا 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 متاحًا فنيًا 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 بشرى ، جزئى أو كلى ، فإن حجيتها تكون متحققة متى أمكن التحقق من وقت وتاريخ إنشائها ومن عدم العبث بهذه الكتابة أو تلك المحررات .

مـــادة (٩)

يتحقق من الناحية الفنية والتقنية ، ارتباط التوقيع الإلكترونى بالموقع وحده دون غيره متى استند هذا التوقيع إلى منظومة تكوين بيانات إنشاء توقيع إلكترونى مؤمنة على النحو الوارد فى المواد (٢ ، ٣ ، ٤) من هذه اللائحة ، وتوافرت إحدى الحالتين الآتيتين :

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

(ب) أن يتم التحقق من صحة التوقيع الإلكترونى طبقًا للمادة (٧) من هذه اللائحة .

مـــادة (١٠)

تتحقق من الناحية الفنية والتقنية ، سيطرة الموقع وحده دون غيره ، على الوسيط الإلكترونى المستخدم فى عملية تثبيت التوقيع الإلكترونى عن طريق حيازة الموقع لأداة حفظ المفتاح الشفرى الخاص ، متضمنة البطاقة الذكية المؤمنة والكود السرى المقترن بها .

مـــادة (١١)

مع عدم الإخلال بما هو منصوص عليه فى المواد (٢ ، ٣ ، ٤) من هذه اللائحة يتم من الناحية الفنية والتقنية ، كشف أى تعديل أو تبديل فى بيانات المحرر الإلكترونى الموقع إلكترونيًا ، باستخدام تقنية شفرة المفتاحين العام والخاص ، وبمضاهاة شهادة التصديق الإلكترونى وبيانات إنشاء التوقيع الإلكترونى بأصل هذه الشهادة وتلك البيانات ، أو بأى وسيلة مشابهة .

مـــادة (١٢)

يجب أن يتوافر لدى طالب الحصول على الترخيص بإصدار شهادات التصديق الإلكترونى المتطلبات التالية :

(أ) نظام تأمين للمعلومات وحماية البيانات وخصوصيتها بمستوى حماية لا يقل عن المستوى المذكور فى المعايير والقواعد المشار إليها فى الفقرة (د) من الملحق الفنى والتقنى للائحة .

(ب) دليل إرشادى يتضمن ما يلى :

١ - إصدار شهادات التصديق الإلكترونى .

٢ - إدارة المفاتيح الشفرية .

٣ - إدارة الأعمال الداخلية .

٤ - إدارة التأمين والكوارث .

وذلك وفقًا للمعايير الفنية والتقنية المذكورة فى الفقرة (هـ) من الملحق الفنى والتقنى للائحة .

(جـ) منظومة تكوين بيانات إنشاء التوقيع الإلكترونى مؤمنة وفقًا للضوابط الفنية والتقنية المنصوص عليها فى المواد (٢ ، ٣ ، ٤) من هذه اللائحة .

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

(هـ) نظام للتحقق من الأشخاص المصدر لهم شهادات التصديق الإلكترونى ، 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 ، وتبعًا 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 ووفقًا 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 البطاقة الذكية ، 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 وفقًا للقواعد والضوابط التى يضعها مجلس إدارة الهيئة .

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

مادة (١٣)

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

مـــادة (١٤)

على طالب الترخيص بإصدار شهادات التصديق الإلكترونى أن يقدم الضمانات والتأمينات التى يحـددها مـجلس إدارة الهـيئـة لتغطيـة أى أضـرار أو أخطـار تتعلق بذوى الشـأن ، وذلك فى حـالة إنهـاء التـرخيـص لأى سبب ، أو لتـغطيـة أى إخـلال من جـانبه لالتـزامـاته الواردة فى الترخيص .

مـــادة (١٥)

تتبع الإجراءات الآتية للحصول على الترخيص بإصدار شهادات التصديق الإلكترونى :

(أ) التقدم بالطلب على النماذج التى تعدها الهيئة فى هذا الشأن مصحوبًا بالبيانات والمستندات الدالة على توافـر الشـروط والأحـكام المنصـوص عليـهـا فى المواد (٣ ، ٤ ، ١٢ ، ١٤) من هذه اللائحة .

(ب) تقوم الهيئة بعد تسلمها لكافة المستندات والبيانات المطلوبة ، وفقًا للبند (أ) من طالب الترخيص بفحصها والتأكد من سلامتها ، وتبت الهيئة فى طلب الحصول على الترخيص خلال مدة لا تتجاوز ستين يومًا 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 مرفوضًا .

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

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

مـــادة (١٦)

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

مـــادة (١٧)

يحـدد فى التـرخـيص التـزامـات المرخص له وفـقًا للقـانون وهذه اللائحـة والقـرارات الصادرة من مجلس إدارة الهيئة فى هذا الشأن .

مـــادة (١٨)

ينشأ جدول خاص بالهيئة تقيد فيه الجهات المرخص لها ، ويعطى 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 تحددها مجلس إدارة الهيئة .

مـــادة (١٩)

تكون الهيئة هى الجهة المختصة بتقديم المشورة الفنية وأعمال الخبرة ، بشأن المنازعات التى تنشأ بين الأطراف المعنية بأنشطة التوقيع الإلكترونى والمعاملات الإلكترونية وتكنولوجيا المعلومات ، على أن يتم التنسيق مع الجهات المعنية فيما يتعلق بشأن أعمال الخبرة .

مـــادة (٢٠)

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

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

٢ - موضوع الترخيص الصادر للمرخص له ، موضحًا 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 الأصلى 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 الإلكترونى لجهة إصدار الشهادة .

١٠ - عنوان الموقع الإلكترونى (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 .

مـــادة (٢١)

للهيئة اعتماد الجهات الأجنبية المختصة بإصدار شهادات التصديق الإلكترونى فى إحدى الحالات الآتية :

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

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

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

(د) أن تكون الجهة الأجنبية ضمن الجهات المعتمدة أو المرخص لها بإصدار شهادات تصديق إلكترونى من قبل جهة الترخيص فى بلدها ، وبشرط أن يكون هناك اتفاقًا بين جهة الترخيص الأجنبية وبين الهيئة على ذلك .

ويكون اعتماد تلك الجهات الأجنبية بناء على طلب مقدم منها أو من ذوى الشأن على النماذج التى تعدها الهيئة . كما يكون للهيئة فى الحالات المشار إليها فى (أ ، ج ، د) 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 يومًا من تاريخ استيفاء الجهة الأجنبية لكل ما تطلبه الهيئة . وفى حالة انقضاء هذه المدة دون إصدار الاعتماد يعتبر الطلب مرفوضًا 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 دائمًا ، بقرار مسبب ، الحق فى إلغاء الاعتماد أو وقفه .

مـــادة (٢٢)

للجهات الأجنبية المعتمدة أن تطلب من الهيئة اعتماد أنواع أو فئات شهادات التصديق الإلكترونى التى تصدرها ، ويكون ذلك وفقًا 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 .

مـــادة (٢٣)

مع عـدم الإخـلال بالعقوبات المنصـوص عليهـا فى المـادة (٢٣) من القانـون ، يلتزم المرخص له بجميع أحكام الترخيص الصادر له من الهيئة ، وفى حالة مخالفة المرخص لأى منها أو توقفـه عن مزاولـة النشـاط المرخص ، أو اندمـاج منشـأته 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 (٢٤)

مع عدم الإخلال بأحكام القانون ، يلتزم كل من يباشر نشاط شهادات التصديق الإلكترونى قبـل العمـل بالقانـون ، أن يوفـق أوضاعـه مع القانـون ، بأن يتقدم بطلب خلال شهرين من تاريخ صدور هذه اللائحة ، على النموذج الذى تعده الهيئة لذلك ، مصحوبًا بما تطلبه الهيئة . وتبت الهيئة فى الطلب خلال ثلاثة شهور من تاريخ استيفاء مقدمه لكل ما تطلبه الهيئة منه .

ويعد كل من امتنع عن توفيق أوضاعه وفقًا لما تقدم ، مزاولاً لهذا النشاط بدون ترخيص ، ويحق للهيئة فى هذه الحالة اتخاذ ما يلزم لوقف النشاط .

الملحق الفنى والتقنى

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

(الفقرة - أ)

PKI Technology

- The profiles for PKI operational management protocols must be based on PKIX (X.509-based PKI).
- The profile for Qualified Certificates must be based on X. 509 (RFC 3739).
- At least one of the following algorithms must be deployed
  - Symmetric algorithms (AES, [n]DES, CAST5, BLOWFISH, TWOFISH, IDEA etc.)
  - Asymmetric algorithms (DSA, RSA, ElGamal, RC [n] etc.)
  - Hash algorithms (MD5, SHA-1 224 etc.)
- Minimum RSA/DSA key lengths must be at least 1024 bits until the end of 2006. Increasing the length to 2048 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.

(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 140-1 level 3 or higher, or equivalent standard such as suitable protection profile based on common criteria (ISO 15408).

(الفقرة - جـ)

Smart Cards

Smart Cards are able to store private e-signature keys for a card 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 smart card. Thus, it is required to have smart cards (Reader / Readerless / contactless) which use the most advanced security standard available in the market.

Security evaluation ITSEC E4 or NIST FIPS PUB 140-1 Level 2 or higher	
X.509v3 certificates	ISO 7816
Cryptographic algorithms must include RSA, SHA-1	
Microsoft PC/SC	Recommended: CAPI - Microsoft Cryptographic
Recommended : PKCS #11 (interface)	Recommended: PKCS #15 (syntax standard)

(الفقرة - د)

Security Standards

- General security management codes of practice, such as BS7799-2 (British Standards, Information security management systems specification with guidance for use) and its guidance ISO/IEC 17799 (recommended), or equivalent standard.

(الفقرة - هـ)

Operation Standards

Recommended: ETSI (The European Telecommunications Standards Institute) TS 101 456 V1.2.1 (2002-04) Policy requirements for certification authorities issuing qualified certificates, specifically Chapter 7 which covers the following parts:

- Certification practice statement
- Key management life cycle
- Certificate Management life cycle
- CA management and operation

Or equivalent standard.