

وزارة الاتصالات وتكنولوجيا المعلومات

قرار رقم ١٠٩ لسنة ٢٠٠٥

بتاريخ ٢٠٠٥/٥/١٥

بإصدار اللائحة التنفيذية لقانون التوقيع الإلكتروني

وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات

وزير الاتصالات وتكنولوجيا المعلومات

بعد الاطلاع على الدستور ؛

وعلى القانون المدني ؛

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 ؛

قرر:

(المادة الاولى)

يعمل بأحكام اللائحة التنفيذية للقانون رقم ١٥ لسنة ٢٠٠٤ بتنظيم التوقيع الإلكتروني

وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المرفقة .

(المادة الثانية)

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

وزير الاتصالات وتكنولوجيا المعلومات

دكتور / طارق كامل

مادة (١)

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

١ - التوقيع الإلكتروني :

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

٢ - الكتابة الإلكترونية :

كل حروف ، أو أرقام ، أو رموز أو أى علامات أخرى تثبت على دعامة إلكترونية أو رقمية أو ضوئية أو أية وسيلة أخرى مشابهة وتعطى 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 التى تصدر من الجهة المرخص لها بالتصديق وتثبت الارتباط بين الموقع وبيانات إنشاء التوقيع .

٨ - بيانات إنشاء التوقيع الإلكتروني :

عناصر متفردة خاصة بالموقع وتمييزه عن غيره ، ومنها على الأخص مفاتيح الشفرة الخاصة به ، والتي تُستخدم فى إنشاء التوقيع الإلكتروني .

٩ - التشفير :

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

١٠ - تقنية شفرة المفاتيح 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 .

١١ - المفتاح الشفري العام :

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

١٢ - المفتاح الشفري الخاص :

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

١٣ - المفتاح الشفري الجذري :

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

١٤ - الدعامة الإلكترونية :

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

١٥ - البطاقة الذكية :

وسيط إلكترونى مؤمن يستخدم فى عملية إنشاء وتثبيت التوقيع الإلكتروني على المحرر الإلكتروني ، ويحتوى على شريحة إلكترونية بها معالج إلكترونى وعناصر تخزين وبرمجيات للتشفيل ، ويشمل هذا التعريف الكسوت 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 بأبئة لفة 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 الأصىلى أم فى أى شكل آخر تظهر فيه من خلال الحاسب الآلى .

١٨ - 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 الشفرى الجذرى .

١٩ - منظومة إنشاء التوقيع الإلكتروني :

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

٢٠ - شهادة فحص بيانات إنشاء التوقيع الإلكتروني :

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

٢١ - شهادة فحص التوقيع الإلكتروني :

شهادة تصدرها الهيئة بنتيجة فحصها لصحة وسلامة التوقيع الإلكتروني .

٢٢ - شهادة اعتماد جهات التصديق الإلكتروني الأجنبية :

شهادة تصدرها الهيئة باعتماد جهات التصديق الإلكتروني الأجنبية ، وما تصدره هذه الجهات من شهادات التصديق الإلكتروني النظرية 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 الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات .

مادة (٢)

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

(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 أى إتلاف بمحتوى أو مضمون المحرر الإلكتروني المراد توقيعه .

(و) ألا تحول هذه المنظومة دون علم الموقع علماً تاماً بمضمون المحرر الإلكتروني

قبل توقيعه له .

مادة (٣)

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

(أ) أن تكون المنظومة مستندة إلى تقنية شفرة المفاتيح العام والخاص وإلى المفتاح الشفرى الجذرى الخاص بالجهة المرخص لها والذي تصدره لها الهيئة ، وذلك كله وفقاً 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 الإلكتروني من التى تستعمل مفاتيح تشفير بأطوال لا تقل عن ٢٠٤٨ حرف إلكترونى (bit) .

(ج) أن تكون أجهزة التأمين الإلكتروني (Hardware Security Modules) المستخدمة معتمدة طبقاً للضوابط الفنية والتقنية المشار إليها فى الفقرة (ب) من الملحق الفنى والتقنى لللائحة .

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

(هـ) أن تضمن المنظومة لجميع أطراف التعامل إتاحة البيانات الخاصة بالتحقق من صحة التوقيع الإلكتروني ، وارتباطه بالموقع دون غيره ، وأن تضمن أيضاً 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)

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

مادة (٥)

الهيئة هي سلطة التصديق الإلكتروني العليا فى جمهورية مصر العربية ، وتتولى إصدار المفاتيح الشفوية الجذرية الخاصة للجهات المرخص لها بإصدار شهادات التصديق الإلكتروني .

وتتحقق الهيئة قبل منح ترخيص مزاولة نشاط إصدار شهادات التصديق الإلكتروني من أن منظومة تكوين بيانات إنشاء التوقيع الإلكتروني لدى الجهة المرخص لها مؤمنة طبقاً 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 .

مادة (٦)

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

مادة (٧)

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

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

(ب) إمكان تحديد مضمون المحرر الإلكتروني الموقع بدقة .

(ج) سهولة العلم بشخص الموقع ، سواء فى حالة استخدام اسمه الأصلي 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 الإلكتروني .

مادة (٨)

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

(أ) أن يكون متاحًا فنيًا 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 متاحًا فنيًا 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 ، جزئي أو كلي ، فإن حجبيتها تكون متحققة متى أمكن التحقق من وقت وتاريخ إنشائها ومن عدم العبث بهذه الكتابة أو تلك المحركات .

مادة (٩)

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 ، ٤) من هذه اللائحة ، وتوافرت إحدى الحالتين الآتيتين :

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

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

مادة (١٠)

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

مادة (١١)

مع عدم الإخلال بما هو منصوص عليه في المواد (٢ ، ٣ ، ٤) من هذه اللائحة يتم من الناحية الفنية والتقنية ، كشف أى تعديل أو تبديل فى 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 .

مادة (١٢)

يجب أن يتوافق لدى طالب الحصول على الترخيص بإصدار شهادات التصديق الإلكتروني 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 لللائحة .

(ب) دليل إرشادى يتضمن ما يلى :

- ١ - إصدار شهادات التصديق الإلكتروني .
- ٢ - إدارة المفاتيح الشفوية .
- ٣ - إدارة الأعمال الداخلية .
- ٤ - إدارة التأمين والكوارث .

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

(ج) منظومة تكوين بيانات إنشاء التوقيع الإلكتروني مؤمنة وفقاً 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 الإلكتروني ،
والتحقق من صفاتهم المميزة .

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

(ز) نظام حفظ بيانات إنشاء التوقيع الإلكتروني وشهادات التصديق الإلكتروني
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 ،
وللبينات 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 الإلكتروني ببند
العقد المبرم مع المرخص له .
- ويكون نظام إيقاف الشهادات وفقاً للقواعد والضوابط التى يضعها مجلس
إدارة الهيئة .

(ك) نظام يتيح ويسر للهيئة التحقق من صحة بيانات إنشاء التوقيع الإلكتروني ،
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 طبقاً للقواعد والضوابط التى يضعها مجلس إدارة الهيئة
فى هذا الشأن لضمان حقوق ذوى الشأن .

مادة (١٤)

على طالب الترخيص بإصدار شهادات التصديق الإلكتروني أن يقدم الضمانات والتأمينات التي يحددها مجلس إدارة الهيئة لتغطية أي أضرار أو أخطار تتعلق بذوى الشأن ، وذلك في حالة إنهاء الترخيص لأي سبب ، أو لتغطية أي إخلال من جانبه بالتزاماته الواردة في الترخيص .

مادة (١٥)

تتبع الإجراءات الآتية للحصول على الترخيص بإصدار شهادات التصديق الإلكتروني :
(أ) التقدم بالطلب على النماذج التي تعدها الهيئة في هذا الشأن مصحوباً بالبيانات والمستندات الدالة على توافر الشروط والأحكام المنصوص عليها في المواد (٣ ، ٤ ، ١٢ ، ١٤) من هذه اللائحة .

(ب) تقوم الهيئة بعد تسليمها 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 .

مادة (١٦)

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

مادة (١٧)

يحدد في الترخيص التزامات المرخص له وفقاً للقانون وهذه اللائحة والقرارات الصادرة من مجلس إدارة الهيئة في هذا الشأن .

مادة (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 التي تحددها مجلس إدارة الهيئة .

مادة (١٩)

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 بشأن أعمال الخبرة .

مادة (٢٠)

يجب أن تشمل 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 :

- ١ - ما يفيد صلاحية هذه الشهادة للاستخدام في التوقيع الإلكتروني .
- ٢ - موضوع الترخيص الصادر للمرخص له ، موضعاً فيه نطاقه ورقمه وتاريخ إصداره وفترة سريانه .
- ٣ - اسم وعنوان الجهة المصدرة للشهادة ومقرها الرئيسي وكيانها القانوني والدولة التابعة لها إن وجدت .
- ٤ - اسم الموقع الأصلي أو اسمه المستعار أو اسم شهرته ، وذلك في حالة استخدامه لأحدهما .
- ٥ - صفة الموقع .
- ٦ - المفتاح الشفري العام لحائز الشهادة المناظر للمفتاح الشفري 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 تشمل الشهادة على أي من البيانات الآتية عند الحاجة :
 - ١ - ما يفيد اختصاص الموقع والغرض الذي تستخدم فيه الشهادة .
 - ٢ - حد قيعة التعاملات المسموح بها بالشهادة .
 - ٣ - مجالات استخدام الشهادة .

مادة (٢١)

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 و ضمانات .

(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 إلكترونى من قبل جهة الترخيص فى بلدها ، وبشرط أن يكون هناك اتفاقاً 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 تسليمها للمستندات والبيانات المطلوبة بفحصها والتأكد من سلامتها وبيت 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 مسيب ، الحق فى إلغاء الاعتماد أو وقفه .

مادة (٢٢)

للجهات الأجنبية المعتمدة أن تطلب من الهيئة اعتماد أنواع أو فئات شهادات التصديق الإلكتروني 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 (٢٣)

مع عدم الإخلال بالعقوبات المنصوص عليها في المادة (٢٣) من القانون ، يلتزم المرخص له بجميع أحكام الترخيص الصادر له من الهيئة ، وفي 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 .

مادة (٢٤)

مع عدم الإخلال بأحكام القانون ، يلتزم كل من يباشر نشاط شهادات التصديق الإلكتروني قبل العمل بالقانون ، أن يوفق أوضاعه مع القانون ، بأن يتقدم بطلب خلال شهرين من تاريخ صدور هذه اللائحة ، على النموذج الذى تعده الهيئة لذلك ، مصححاً بما تطلبه الهيئة . وتبت الهيئة فى الطلب خلال ثلاثة شهور من تاريخ استيقاء مقدمه لكل ما تطلبه الهيئة منه . وبعد كل من امتنع عن توفيق أوضاعه وفقاً لما تقدم ، مزاولاً لهذا النشاط بدون ترخيص ، ويحق للهيئة فى هذه الحالة اتخاذ ما يلزم لوقف النشاط .

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 .

(الفقرة - ١)

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 - ج)

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.