## وزارة الاتصالات وتكنولوجيا المعلومات

## قرار رقم 109 لسنة 2005

## 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 13 لسنة 1968 بشأن المرافعات المدنية والتجارية ،
وعلى القانون رقم 25 لسنة1968 بشأن الإثبات في المواد المدنية والتجارية ،
وعلي القانون رقم 82 لسنة 2002 بشأن حماية حقوق الملكية الفكرية ،
وعلي القانون رقم 10 لسنة 2003 بشأن تنظيم الاتصالات ،
وعلى قانون رقم 15 لسنة 2004 بتنظيم التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات ،
وعلى قرار رئيس الجمهورية رقم 201 لسنة 2004 بتشكيل الوزارة.

**قـــرر**

**(المادة الأولى)**

يعمل بأحكام اللائحة التنفيذية للقانون رقم 15 لسنة 2004 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**

**صدر فى 15/5/ 2005**

**(دكتور/ طارق كامل)**

# مادة(1)

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

**1- التوقيع الإلكتروني :**

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

**2- الكتابة الإلكترونية :**

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

**3- المحرر الإلكتروني :**

رسالة بيانات تتضمن معلومات تنشا، أو تدمج ، أو تخزن، أو ترسل، أو تستقبل، كليـاً أو جزئيا، بوسيلة إلكترونية أو رقمية ، أو ضوئية ، أو بأية وسيلة أخرى مشابهة.

**4- الوسيط الإلكتروني :**

أداة أو أدوات أو أنظمة إنشاء التوقيع الالكتروني.

**5- الموقع :**

الشخص الحائز على بيانات إنشاء التوقيـع ويوقـع عـن نفسـه أو عمـن ينيبـه أو يمثله قانونا.

**6- جهات التصديق الإلكتروني :**

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

**7- شهادة التصديق الإلكتروني :**

الشهادة التى تصدر من الجهة المرخص لها بالتصديق وتثبت الارتبـاط بـين الموقـع وبيانات إنشاء التوقيع.

**8- بيانات إنشاء التوقيع الإلكتروني :**

عناصر متفردة خاصة بالموقع وتميزه عن غيره ، ومنها على الأخص مفـاتيح الشـفرة الخاصة به ، والتي تُستخدم في إنشاء التوقيع الإلكتروني.

**9- التشفير :**

منظومة تقنية حسابية تستخدم مفاتيح خاصة لمعالجة وتحويـل البيانـات والمعلومـات المقروءة إلكترونيا بحيث تمنع استخلاص هذه البيانات والمعلومات إلا عن طريـق اسـتخدام مفتاح أو مفاتيح فك الشفرة.

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

منظومة تسمح لكل شخص طبيعي أو معنوي بـان يكـون لديـة مفتـاحين متفـردين أحدهما عام متاح إلكترونيا ، والثاني خاص يحتفظ به الشخص ويحفظه على درجة عالية من السرية.

**11- المفتاح الشفري العام :**

أداة إلكترونية متاحة للكافة ، تنشأ بواسطة عملية حسـابية خاصـة ، وتسـتخدم فـي التحقق من شخصية الموقع على المحرر الإلكتروني ، والتأكد من صحة وسـلامة محتـوى المحرر الإلكتروني الأصلي.

**12- المفتاح الشفري الخاص :**

أداة إلكترونية خاصة بصاحبها ، تنشأ بواسطة عمليـة حسـابية خاصـة وتسـتخدم في وضع التوقيع الإلكتروني على المحررات الإلكترونية ، ويتم الاحتفاظ بها علـى بطاقـة ذكية مؤمنة.

**13- المفتاح الشفري الجذري :**

أداة إلكترونية تنشا بواسطة عملية حسـابية خاصـة وتسـتخدمها جهـات التصـديق الإلكتروني لإنشاء شهادات التصديق الإلكتروني وبيانات إنشاء التوقيع الإلكتروني.

**14- 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.

**15- البطاقة الذكية :**

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

**16- الحاسب الآلي :**

جهاز إلكتروني قادر على تخزين ومعالجة وتحليل واسترجاع البيانات والمعلومات بطريقة الكترونية.

**17- برنامج الحاسب الآلي:**

مجموعة أوامر وتعليمات معبر عنها بأية لغة أو رمز أو إشارة ، و تتخذ أى شكل من الأشكال ، ويمكن استخدامها بطريقه مباشرة أو غير مباشرة في حاسب آلى لأداء وظيفة أو تحقيق نتيجة ، سواء أكانت هذه الأوامر والتعليمات في شكلها الأصلي أم في أي شكل آخر تظهر فيه من خلال الحاسب الآلي.

**18- منظومة تكوين بيانات إنشاء التوقيع الإلكتروني :**

مجموعة عناصر مترابطة ومتكاملة ، تحتوى على وسائط إلكترونية وبرامج حاسب آلي يتم بواسطتها تكوين بيانات إنشاء التوقيع الالكتروني باستخدام المفتاح الشفري الجذري.

**19- منظومة إنشاء التوقيع الإلكتروني :**

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

**20- شهادة فحص بيانات إنشاء التوقيع الالكتروني :**

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

**21- شهادة فحص التوقيع الإلكتروني :**

شهادة تصدرها الهيئة بنتيجة فحصها لصحة وسلامة التوقيع الإلكتروني.

**22- 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.

**23- الهيئة :**

هيئة تنمية صناعة تكنولوجيا المعلومات.

**24- الوزارة المختصة:**

الوزارة المختصة بشئون الاتصالات و تكنولوجيا المعلومات.

**25- الوزير المختص:**

الوزير المختص بشئون الاتصالات وتكنولوجيا المعلومات.

**26- القانون:**

قانون رقم 15 لسنه 2004 بتنظيم التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات.

## مادة(2)

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.

## مادة(3)

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

أ- أن تكون المنظومة مستندة إلى تقنية شفرة المفتاحين العام والخاص والي المفتـاح الشـفري الجذري الخاص بالجهة المرخص لها والذي تصدره لها الهيئة، وذلك كله وفقا للمعايير الفنية والتقنية المشار إليها في الفقرة (أ) من الملحق الفني والتقني لهذه اللائحة.

ب- أن تكون التقنية المستخدمة في إنشاء مفاتيح الشفرة الجذرية لجهات التصديق الإلكتروني مـن التي تستعمل مفاتيح تشفير بأطوال لا تقل عن 2048 حرف إلكتروني (bit).

ج- أن تكون أجهزة التامين الإلكتروني (*Hardware Security Modules*) *المستخدمة معتمدة* طبقا للضوابط الفنية والتقنية المشار إليها في الفقرة (ب) من الملحق الفني والتقني للائحة.

د- أن يتم استخدام بطاقات ذكية غير قابلة للاستنساخ ومحمية بكود سرى ، تحتوى على عناصر متفردة للموقع وهى بيانات إنشاء التوقيع الإلكتروني وشهادة التصـديق الإلكترونـي ، ويـتم تحديد مواصفات البطاقة الذكية وأنظمتها ، وفقا للمعايير الفنية والتقنية المبينة في الفقرة (جـ) من الملحق الفني والتقني للائحة.

هـ- أن تضمن المنظومة لجميع أطراف التعامل إتاحة البيانات الخاصة بالتحقق من صحة التوقيع الإلكتروني، وارتباطه بالموقع دون غيره ، وأن تضمن أيضا عملية الإدراج الفـوري والإتاحـة اللحظية لقوائم الشهادات الموقوفة أو الملغاة وذلك فور التحقق من توافر أسباب تسـتدعي إيقـاف الشهادة، على أن يتم هذا التحقق خلال فترة محددة ومعلومة للمستخدمين حسب القواعد والضوابط التي يضعها مجلس إدارة الهيئة.

## مادة ( 4)

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

## مادة ( 5)

الهيئة هي سلطة التصديق الالكتروني العليا في جمهورية مصر العربية، وتتولي إصـدار المفاتيح الشفرية الجذرية الخاصة للجهات المرخص لها بإصدار شهادات التصديق الالكتروني.

وتتحقق الهيئة قبل منح ترخيص مزاولة نشاط إصدار شهادات التصديق الإلكتروني مـن أن منظومة تكوين بيانات إنشاء التوقيع الإلكتروني لدى الجهة المرخص لها مؤمنة طبقا للمـادة (2)، ومتضمنة الضوابط الفنية والتقنية والنظم والقواعد المبينة في المادتين (3 ، 4 ).

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

## مادة (6)

تقدم الهيئة، بناء على طلب كل ذي شأن، خدمة الفحص والتحقق من صحة بيانات إنشـاء التوقيع الإلكتروني نظير مقابل يحدد فئاته مجلس إدارة الهيئة. ويجوز للهيئة أن تعهـد للغيـر بتقديم هذه الخدمة تحت إشرافها ، وفي جميع الأحوال تصدر الهيئة شهادة فحص بيانات إنشـاء التوقيع الإلكتروني.

## مادة (7)

تقدم الهيئة، بناء على طلب كل ذي شأن، خدمة فحص التوقيع الإلكتروني نظيـر مقابـل يحدد فئاته مجلس إدارة الهيئة. وتتحقق الهيئة في سبيل القيام بذلك مما يأتي:

أ- سلامة شهادة التصديق الإلكتروني وتوافقها مع بيانات إنشاء التوقيع الالكتروني.

ب- إمكان تحديد مضمون المحرر الإلكتروني الموقع بدقة.

ج- سهولة العلم بشخص الموقع ، سواء في حالة استخدام اسمه الأصـلي أم اسـتخدامه لاسم مستعار أم اسم شهرة.

ويجوز للهيئة أن تعهد للغير بتقديم هذه الخدمة تحت إشرافها ، وفي جميع الأحوال تصـدر الهيئة شهادة فحص التوقيع الالكتروني.

## مادة(8)

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

أ- أن يكون متاحاً فنيا تحديد وقت وتـاريخ إنشـاء الكتابـة الإلكترونيـة أو المحـررات الإلكترونية الرسمية أو العرفية ، وأن تتم هذه الإتاحة من خلال نظام حفـظ إلكترونـي مستقل وغير خاضع لسيطرة منشئ هذه الكتابة أو تلك المحررات ، أو لسيطرة المعنى بها.

ب- أن يكون متاحاً فنيا تحديد مصدر إنشاء الكتابة الإلكترونية أو المحررات الإلكترونية الرسمية أو العرفية ودرجة سيطرة ُمنشئها على هذا المصدر وعلى الوسائط المستخدمة في إنشائها.

ج- في حالة إنشاء وصدور الكتابة الإلكترونية أو المحررات الإلكترونية الرسمية أو العرفية بدون تدخل بشرى، جزئي أو كلى ، فإن حجيتها تكون متحققة متى أمكن التحقق من وقت وتاريخ إنشائها ومن عدم العبث بهذه الكتابة أو تلك المحررات.

## مادة(9)

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(4،3،2) من هذه اللائحة ، و توافرت احدي الحالتين الآتيتين:-

أ- أن يكون هذا التوقيع مرتبطا بشهادة تصديق إلكتروني معتمدة ونافذة المفعول صادرة من جهة تصديق إلكتروني مرخص لها أو معتمدة.

ب-أن يتم التحقق من صحة التوقيع الإلكتروني طبقا للمادة (7) من هذه اللائحة.

## مادة(10)

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(11)

مع عدم الإخلال بما هو منصوص عليه في المواد (4،3،2) من هذه اللائحة يتم من الناحية الفنية والتقنية ، كشف أي تعديل أو تبديل في بيانات المحرر الإلكتروني الموقع إلكترونيا، باستخدام تقنية شفرة المفتاحين العام والخاص ، وبمضاهاة شهادة التصديق الإلكتروني وبيانات إنشاء التوقيع الإلكتروني بأصل هذه الشهادة وتلك البيانات ، أو بأي وسيلة مشابهة.

## مادة (12)

يجب أن يتوافر 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 في المعايير والقواعد المشار إليها في الفقرة (د) من الملحق الفني والتقني للائحة.

ب- دليل إرشادي يتضمن ما يلي:-

1- إصدار شهادات التصديق الإلكتروني.

2- إدارة المفاتيح الشفرية.

3- إدارة الأعمال الداخلية.

4- إدارة التأمين والكوارث.

وذلك وفقا للمعايير الفنية والتقنية المذكورة في الفقرة (هـ) من الملحق الفني والتقني للائحة.

ج- منظومة تكوين بيانات إنشاء التوقيع الإلكتروني مؤمنة وفقا للضوابط الفنية والتقنية المنصوص عليها في المواد (2،3،4) 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 التي تحددها الهيئة فى الترخيص ، وتبعا 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 ووفقا 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:

1- العبث ببيانات الشهادة أو انتهاء مدة صلاحيتها.

2- سرقة أو فقد المفتاح الشفري الخاص أو البطاقة الذكية ، أو عند الشك في حدوث ذلك.

3- عدم التزام الشخص المصدر له شهادة التصديق الإلكتروني ببنود العقد المبرم مع المرخص له.

ويكون نظام إيقاف الشهادات وفقا للقواعد والضوابط التي يضعها مجلس إدارة الهيئة.

ك- نظام يتيح وييسر للهيئة التحقق من صحة بيانات إنشاء التوقيع الالكتروني، وبخاصة في إطار أعمال الفحص والتحقق من جانب الهيئة.

## مادة(13)

في جميع الأحوال يلتزم المرخص له بعدم إبرام أي عقد مع العملاء إلا بعد اعتماد نموذج هذا العقد من الهيئة طبقا للقواعد والضوابط التي يضعها مجلس إدارة الهيئة في هذا الشأن لضمان حقوق ذوي الشأن.

## مادة(14)

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

## مادة(15)

تتبع الإجراءات الآتية للحصول على الترخيص بإصدار شهادات التصديق الإلكتروني:-

أ- التقدم بالطلب على النماذج التي تعدها الهيئة في هذا الشأن مصحوبا بالبيانات والمستندات الدالة على توافر الشروط والأحكام المنصوص عليها في المواد (3 ، 4، 12 ،14) من هذه اللائحة.

ب-تقوم الهيئة بعد تسلمها لكافة المستندات والبيانات المطلوبة ، وفقا للبند(أ) من طالب الترخيص بفحصها والتأكد من سلامتها ، وتبت الهيئة في طلب الحصول على الترخيص خلال مدة لا تتجاوز ستين يوما من تاريخ استيفاء طالب الترخيص لجميع ما تطلبه الهيئة منه ، ما لم

تخطر الهيئة طالب الترخيص بمد هذه المدة. وفي حالة انقضاء هـذه المـدة دون إصـدار الترخيص يعتبر الطلب مرفوضا.

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

د- تمنح الهيئة الترخيص طبقا للإجراءات والقواعد والضمانات المنصوص عليها في القانون وفي هذه اللائحة ، وما يقره مجلس إدارة الهيئة من قواعد في هذا الشأن.

## مادة(16)

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

## مادة(17)

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

## مادة(18)

ينشأ جدول خاص بالهيئة تقيد فيه الجهات المرخص لها ، ويعطى لكل جهة رقم مسلسـل ويحدد فيه نوع الترخيص الممنوح لها ، ويتضمن بيانـات عـن هـذه الجهـة ورأس مالهـا وأعضاء مجلس إدارتها والمديرين بها وفروعها ومكاتبها وغير ذلك من البيانات التي يحـددها مجلس إدارة الهيئة.

## ماده(19)

تكون الهيئة هي الجهة المختصة بتقديم المشورة الفنية وأعمال الخبرة ، بشأن المنازعات التي تنشا بين الأطراف المعنية بأنشطة التوقيع الإلكتروني والمعاملات الإلكترونية وتكنولوجيـا المعلومات ، على أن يتم التنسيق مع الجهات المعنية فيما يتعلق بشأن أعمال الخبرة.

## مادة(20)

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

1- ما يفيد صلاحية هذه الشهادة للاستخدام في التوقيع الإلكتروني.

2- موضوع الترخيص الصادر للمرخص له، موضحا فيه نطاقه ورقمه وتاريخ إصداره وفترة سريانه.

3- اسم وعنوان الجهة المصدرة للشهادة ومقرها الرئيسي وكيانها القانوني والدولة التابعة لهـا إن وجدت.

4- اسم الموقع الأصلي أو اسمه المستعار أو اسم شهرته ، وذلك في حالة استخدامه لأحدهما.

5- صفة الموقع.

6- المفتاح الشفري العام لحائز الشهادة المناظر للمفتاح الشفري الخاص به.

7- تاريخ بدء صلاحية الشهادة وتاريخ انتهائها.

8- رقم مسلسل للشهادة.

9- التوقيع الإلكتروني لجهة إصدار الشهادة.

10- عنوان الموقع الإلكتروني (Web Site) المخصص لقائمة الشهادات الموقوفة أو الملغاة .

ويجوز أن تشتمل الشهادة على اى من البيانات الآتية عند الحاجة:-

1. ما يفيد اختصاص الموقع والغرض الذي تستخدم فيه الشهادة.
2. حد قيمة التعاملات المسموح بها بالشهادة.
3. مجالات استخدام الشهادة.

## مادة(21)

للهيئة اعتماد الجهات الأجنبية المختصة بإصدار شهادات التصديق الإلكتروني في إحـدى الحالات الآتية:-

أ- أن يتوافر لدى الجهة الأجنبية القواعد والاشتراطات المبينة فـي هـذه اللائحـة بالنسبة للجهات التي ترخص لها الهيئة بمزولة نشاط إصدار شـهادات التصـديق الإلكتروني.

ب-أن يكون لدى الجهة الأجنبية وكيل في جمهورية مصر العربية مرخص له مـن قبل الهيئة بإصدار شهادات التصديق الإلكتروني، و يتوافر لديـه كـل المقومـات المطلوبة للتعامل بشهادات التصديق الإلكتروني ويكفل تلك الجهة فيما تصدره مـن شهادات تصديق إلكتروني وفيما هو مطلوب من اشتراطات وضمانات.

ج- أن تكون الجهة الأجنبية ضمن الجهات التي وافقت جمهوريـة مصـر العربيـة بموجب اتفاقية دولية نافذة فيها على اعتمادها باعتبارهـا جهـة أجنبيـة مختصـة بإصدار شهادات التصديق الإلكتروني.

د- أن تكون الجهة الأجنبية ضمن الجهات المعتمدة أو المـرخص لهـا بإصـدار شهادات تصديق الكتروني من قبل جهة الترخيص في بلادها، و بشـرط أن يكـون هناك اتفاقاً بين جهة الترخيص الأجنبية وبين الهيئة على ذلك.

ويكون اعتماد تلك الجهات الأجنبية بناء على طلب مقدم منها أو من ذوى الشأن علـى النماذج التي تعدها الهيئة. كما يكون للهيئة في الحالات المشار اليها فى (أ، ج، د) اعتماد تلـك الجهات من تلقاء نفسها.

وفي حالة التقدم بطلب للاعتماد ، تقوم الهيئة بعد تسلمها للمستندات والبيانـات المطلوبـة بفحصها والتأكد من سلامتها ويبت مجلس إدارة الهيئة في طلب الاعتماد خلال مدة لا تجـاوز ستين يوما من تاريخ استيفاء الجهة الأجنبية لكل ما تطلبه الهيئة. وفي حالة انقضاء هذه المـدة دون إصدار الاعتماد يعتبر الطلب مرفوضا ما لم تخطر الهيئة كتابة الجهة الطالبة بمـد هـذه المدة.

ويصدر قرار اعتماد الجهة الأجنبية من مجلس إدارة الهيئة بعد سداد المقابل الذي يحدده المجلس للاعتماد، ويحدد في القرار مدة الاعتماد وأحوال تجديده ، وللهيئـة دائمـا، بقـرار مسبب، الحق في إلغاء الاعتماد أو وقفه.

## مادة(22)

للجهات الأجنبية المعتمدة أن تطلب من الهيئة اعتماد أنواع أو فئات شـهادات التصـديق الالكتروني التي تصدرها ، ويكون ذلك وفقا للقواعد والضوابط التي يضعها مجلس إدارة الهيئة في هذا الشأن، وكذلك تحديد المقابل لاعتماد هذه الشهادات ، ويحدد مجلس إدارة الهيئـة عنـد اعتماده لأنواع وفئات الشهادات الأجنبية ما يناظرها من شهادات تصديق إلكتروني صادرة مـن الجهات المرخص لها في جمهورية مصر العربية.

## مادة(23)

مع عدم الإخلال بالعقوبات المنصوص عليها في المـادة (23) مـن القـانون ، يلتـزم المرخص له بجميع أحكام الترخيص الصادر له من الهيئة ، وفي حالة مخالفة المـرخص لأي منها أو توقفه عن مزاولة النشاط المرخص ، أو اندماج منشأته في جهة أخرى ، أو تنازله عن الترخيص للغير ، دون الحصول على موافقة كتابية مسبقة من الهيئة على أي من هذه الأفعـال المشار إليها ، يجوز للهيئة، بقرار مسبب، عندئذ إلغاء الترخيص أو وقفه لحـين التـدارك أو التصحيح .

ويجوز للهيئة في حالتي الإلغاء أو الوقف أن تتخذ التدابير المناسبة في هذا الشـأن لحمايـة حقوق ذوي الشأن.

## مادة(24)

مع عدم الإخلال بأحكام القانون ، يلتزم كل من يباشر نشاط إصدار شـهادات التصـديق الإلكتروني قبل العمل بالقانون، أن يوفق أوضاعه مع القانون، بأن يتقدم بطلب خلال شـهرين من تاريخ صدور هذه اللائحة، على النموذج الذي تعده الهيئة لذلك ، مصحوبا بما تطلبه الهيئة.

وتبت الهيئة في الطلب خلال ثلاثة شهور من تاريخ استيفاء مقدمة لكل ما تطلبه الهيئة منه.

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

# الملحق الفني و التقني

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 – 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.