وزارة الاتصالات وتكنولوجيا المعلومات

قرار رقم ٤٦٧ لسنة ٢٠٢٤

بتاريخ ٢٠٢٤/٦/١٢

بتعديل اللائحة التنفيذية للقانون رقم ١٥ لسنة ٢٠٠٤

بتنظيم التوقيع الإلكترونى وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات

وزير الاتصالات وتكنولوجيا المعلومات

بعد الاطلاع على الدستور ؛

وعلى القانون رقم ١٣١ لسنة ١٩٤٨ بإصدار القانون المدنى ، وتعديلاته ؛

وعلى القانون رقم ١٣ لسنة ١٩٦٨ بإصدار قانون المرافعات المدنية والتجارية وتعديلاته ؛

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

وعلى القانون رقم ١٧ لسنة ١٩٩٩ بإصدار قانون التجارة وتعديلاته ؛

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

وعلى القانون رقم ١٠ لسنة ٢٠٠٣ بشأن تنظيم الاتصالات وتعديلاته ؛

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

وعلى القانون رقم ٣ لسنة ٢٠٠٥ بإصدار قانون حماية المنافسة ومنع الممارسات الاحتكارية وتعديلاته ؛

وعلى القانون رقم ٧٢ لسنة ٢٠١٧ بإصدار قانون الاستثمار وتعديلاته ؛

وعلى القانون رقم ١٧٥ لسنة ٢٠١٨ فى شأن مكافحة جرائم تقنية المعلومات ؛

وعلى القانون رقم ١٧٨ لسنة ٢٠١٨ بإصدار قانون الهيئة الوطنية للإعلام ؛

وعلى القانون رقم ١٨٠ لسنة ٢٠١٨ بإصدار قانون تنظيم الصحافة والإعلام والمجلس الأعلى لتنظيم الإعلام ؛

وعلى القانون رقم ١٨١ لسنة ٢٠١٨ بإصدار قانون حماية المستهلك ؛

وعلى القانون رقم ١٨ لسنة ٢٠١٩ بإصدار قانون تنظيم استخدام وسائل الدفع غير النقدى ؛

وعلى القانون رقم ١٥١ لسنة ٢٠٢٠ بإصدار قانون حماية البيانات الشخصية ؛

وعلى القانون رقم ١٩٤ لسنة ٢٠٢٠ بإصدار قانون البنك المركزي والجهاز المصرفى ؛

وعلى القانون رقم ٥ لسنة ٢٠٢٢ بإصدار قانون تنظيم وتنمية استخدام التكنولوجيا المالية فى الأنشطة المالية غير المصرفية ؛

وعلى قرار وزير الاتصالات وتكنولوجيا المعلومات رقم ١٠٩ لسنة ٢٠٠٥ بإصدار اللائحة التنفيذية للقانون رقم ١٥ لسنة ٢٠٠٤ بتنظيم التوقيع الإلكترونى وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات وتعديلاتها ؛

وعلى قرار مجلس إدارة هيئة تنمية صناعة تكنولوجيا المعلومات رقم ٢ لسنة ٢٠٢٤ الصادر بجلسته المنعقدة فى ٢٠٢٤/٣/١٤ المعتمد من السيد الدكتور وزير الاتصالات وتكنولوجيا المعلومات بالموافقة على اللائحة التنفيذية للقانون رقم ١٥ لسنة ٢٠٠٤ بتنظيم التوقيع الإلكترونى وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المعدلة ؛

قـــرر :

(المادة الأولى)

يعمل بأحكام اللائحة التنفيذية للقانون رقم ١٥ لسنة ٢٠٠٤ ، بتنظيم التوقيع الإلكترونى وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات ، المُعدلة ، المُرفقة .

(المادة الثانية)

تسرى الأحكام والشروط والإجراءات المنصوص عليها فى هذه اللائحة فى شأن تنظيم خدمات الثقة والمعاملات الالكترونية الموثوق بها وأنشطة تكنولوجيا المعلومات .

(المادة الثالثة)

ينشر هذا القرار فى الوقائع المصرية ، ويعمل به من اليوم التالى لتاريخ نشره ، ويلغى كل قرار يخالف أحكامه .

وزير الاتصالات وتكنولوجيا المعلومات

د/ عمرو سميح طلعت

اللائحة التنفيذية للقانون رقم ١٥ لسنة ٢٠٠٤

بتنظيم التوقيع الإلكترونى وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات

الفصل الأول

التعريفات والأحكام العامة

مادة (١)

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

١- **إلكترونى** : كهرومغناطيسى أو كهروضوئى أو رقمى أو ضوئي أو ما شابه ذلك .

٢- **المعلومات الالكترونية** : معلومات ذات خصائص الكترونية فى شكل نصوص أو رموز أو أصوات أو رسوم أو صور أو برامج حاسب آلى أو غيرها من قواعد البيانات .

٣- **نظام المعلومات الإلكترونى** : نظام إلكترونى لإنشاء أو استخراج أو إرسال أو استلام أو تخزين أو عرض أو معالجة المعلومات أو الرسائل الكترونيا .

٤- **تكنولوجيا المعلومات** : مجموعة برامج معلوماتية ووسائل تقنية المعلومات المعدة لإنشاء ومعالجة وإدارة وتخزين وتبادل المعاملات الالكترونية وما شابه ذلك .

٥- **الكتابة الالكترونية** : كل حروف ، أو أرقام ، أو رموز ، أو أى علامات أخرى تثبت على دعامة الكترونية أو رقمية أو ضوئية أو أية وسيلة أخرى مشابهة وتعطى دلالة قابلة للإدراك .

٦- **المحرر الإلكترونى** : مستند أو وثيقة أو سجل أو رسالة بيانات تتضمن معلومات تنشأ ، أو تدمج ، أو تخزن ، أو ترسل ، أو تستقبل ، كليًا أو جزئيًا ، بوسيلة الكترونية أو رقمية ، أو ضوئية ، أو بأية وسيلة أخرى مشابهة ، ويكون قابلاً للاسترجاع بشكل يمكن فهمه .

٧- **المعاملات الالكترونية :** الإجراءات أو العمليات أو العقود التى تتم بشكل كلى أو جزئى بواسطة وسائل الكترونية .

٨- **المعاملات الالكترونية الموثوق بها :** هى المعاملات الالكترونية التى تستخدم إحدى خدمات الثقة المنصوص عليها فى هذه اللائحة .

٩- **المعاملات الالكترونية الموثوق بها المؤتمتة :** هى المعاملات الالكترونية الموثوق بها والتى يتم اتخاذها أو إبرامها أو تنفيذها دون أن تحتاج فى عملها إلى العنصر البشرى .

١٠- **الرسالة الإلكترونية :** المعلومات التى يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها بوسائل الكترونية .

١١- **المرسل :** الشخص الطبيعى أو الاعتبارى الذى يقوم أو يتم بالنيابة عنه إرسال الرسالة الإلكترونية ، ولا يعتبر مرسلاً الجهة التى تقوم بمهمة مزود خدمات فيما يتعلق بإنتاج أو معالجة أو إرسال أو حفظ تلك الرسالة الإلكترونية وغير ذلك من الخدمات المتعلقة بها .

١٢- **المرسل إليه :** الشخص الطبيعى أو الاعتبارى الذى قصد مُرسل الرسالة توجيه رسالته إليه ، ولا يعتبر مرسلاً إليه الشخص الذى يقوم بتزويد الخدمات فيما يتعلق باستقبال أو معالجة أو حفظ تلك المراسلات الإلكترونية وغير ذلك من الخدمات المتعلقة بها .

١٣- **خدمات الثقة (Trusted Service) :** خدمة التوقيع الإلكترونى ، أو خدمة الختم الإلكترونى ، أو خدمة البصمة الزمنية الالكترونية ، أو خدمة البريد الإلكترونى المُسجل ، أو خدمة التيقن من موقع الإنترنت .

١٤- **الجهات المرخص لها بمزاولة نشاط تقديم خدمات الثقة :** الشخص الاعتبارى الحاصل على ترخيص من الهيئة بتقديم خدمة أو أكثر من خدمات الثقة .

١٥- **قائمة مقدمى خدمات الثقة (Trusted list) :** هى قائمة مختومة الكترونيا ومعتمدة من الهيئة تحتوى على المعلومات الخاصة بمقدمى خدمات الثقة وشهادات التصديق الإلكترونى الخاصة بهم ، وتستخدم كوسيلة للتحقق من صحة وموثوقية مقدمى خدمات الثقة .

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

١٧- **الموقع** : الشخص الطبيعى الحائز على بيانات إنشاء التوقيع ويوقع عن نفسه أو عمن ينيبه أو يمثله قانوناً .

١٨- **شهادة التوقيع الإلكترونى** : الشهادة التى تصدر من الجهة المرخص لها بالتصديق وتُثبت الارتباط بين الموقع وبيانات إنشاء التوقيع .

١٩- **بيانات إنشاء التوقيع الإلكترونى** : عناصر متفردة خاصة بالموقع وتميزه عن غيره ، ومنها على الأخص مفاتيح الشفرة الخاصة به ، والتى تستخدم فى إنشاء التوقيع الإلكترونى .

٢٠- **الختم الإلكترونى** : التوقيع الإلكترونى الذى يسمح بتحديد الشخص الاعتبارى منشئ الختم ويميزه عن غيره .

٢١- **منشئ الختم** : الشخص الاعتبارى الحائز على بيانات إنشاء الختم الإلكترونى واستخدامه .

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

٢٣- **شهادة الختم الإلكترونى** : الشهادة التى تصدر من الجهة المرخص لها بالتصديق ، وتُثبت الارتباط بين مُنشئ الختم وبيانات إنشاء الختم الإلكترونى .

٢٤- **البصمة الزمنية الإلكترونية** : مَا يوضع على محرر إلكترونى ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها والتى تربط تلك البيانات بوقت محدد لإثبات وجود هذا المحرر الإلكترونى فى ذلك الوقت .

٢٥- **التشفير** : منظومة تقنية حسابية تستخدم مفاتيح خاصة لمعالجة وتحويل البيانات والمعلومات المقروءة إلكترونيا ، بحيث تمنع استخلاص هذه البيانات والمعلومات إلا عن طريق استخدام مفتاح أو مفاتيح فك الشفرة .

٢٦- **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 إلكترونيا ، والثانى خاص يتحكم به الشخص أو يحفظه على درجة عالية من السرية .

٢٧- **المفتاح الشفرى العام** : أداة إلكترونية متاحة للكافة ، تنشأ بواسطة عملية حسابية خاصة ، وتستخدم فى التحقق من شخصية الموقع على المحرر الإلكترونى ، والتأكد من صحة وسلامة محتوى المحرر الإلكترونى الأصلى .

٢٨- **المفتاح الشفرى الخاص** : أداة إلكترونية خاصة بصاحبها ، تنشأ بواسطة عملية حسابية خاصة ، ويتم الاحتفاظ بها على أداة إنشاء التوقيع الإلكترونى ، وتستخدم فى وضع التوقيع الإلكترونى على المحررات الإلكترونية .

٢٩- **المفتاح الشفرى الجذرى** : أداة إلكترونية تنشأ بواسطة عملية حسابية خاصة ، وتستخدمها الهيئة لإنشاء المفاتيح الشفرية الخاصة بالجهات المرخص لها بإصدار شهادات التصديق الإلكترونى للأشخاص الطبيعيين والاعتباريين .

٣٠- **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 .

٣١- **أداة التوقيع الإلكترونى** : أى وسيط إلكترونى مؤمن يستخدم فى عملية إنشاء وتثبيت التوقيع الإلكترونى على المحرر الإلكترونى ، ويشمل هذا التعريف الكروت الذكية والشرائح الإلكترونية المنفصلة ، أو غير ذلك من وسائط أو أنظمة تتطابق معه من حيث تحقيق الوظائف المطلوبة ، وفقًا للمعايير التقنية والفنية المنصوص عليها فى هذه اللائحة .

٣٢- **منظومة تكوين بيانات إنشاء التوقيع الإلكترونى** : مجموعة عناصر مترابطة ومتكاملة ، تحتوى على وسائط إلكترونية وبرامج حاسب آلى يتم بواسطتها تكوين بيانات إنشاء التوقيع الإلكترونى باستخدام المفتاح الشفرى الجذرى ، ويشمل ذلك بيانات إنشاء الختم الإلكترونى .

٣٣- **شهادة فحص بيانات إنشاء التوقيع الإلكترونى :** شهادة تصدرها الهيئة بنتيجة الفحص والتحقق من صحة بيانات إنشاء التوقيع الإلكترونى ، بما فى ذلك الختم الإلكترونى .

٣٤- **شهادة فحص التوقيع الإلكترونى :** شهادة تصدرها الهيئة بنتيجة فحصها لصحة وسلامة التوقيع الإلكترونى ، بما فى ذلك الختم الإلكترونى .

٣٥- **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 .

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

٣٧- **الهيئة :** هيئة تنمية صناعة تكنولوجيا المعلومات .

٣٨- **الوزارة المختصة :** الوزارة المختصة بشئون الاتصالات وتكنولوجيا المعلومات .

٣٩- **الوزير المختص :** الوزير المختص بشئون الاتصالات وتكنولوجيا المعلومات .

٤٠- **القانون :** القانون رقم ١٥ لسنة ٢٠٠٤ بتنظيم التوقيع الإلكترونى وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات .

مادة (٢)

لا يجوز إنكار حجية المحرر أو الرسالة لمجرد أنه تم إنشاؤها أو حفظها أو إرسالها أو استقبالها فى شكل إلكترونى .

وإذا وجب قانوناً أن يتم التعبير عن الإرادة فى شكل مكتوب ، فإنه يعتد بالكتابة الإلكترونية إذا كانت محفوظة أو مخزنة بشكل يمكن من الرجوع إليها والاطلاع عليها فى أى وقت .

مادة (٣)

فى مجال إبرام العقود أو تعديلها أو إنهائها يجوز أن يتم التعبير عن الإرادة ، سواء بالنسبة للإيجاب أو القبول ، فى شكل إلكترونى ، ما لم يتفق الأطراف أو ينص قانوناً على خلاف ذلك .

مادة (٤)

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

(أ) أن يكون متاحًا فنيا 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 منشئها على هذا المصدر وعلى الأدوات المستخدمة فى إنشائها .

(ج) 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.

مادة (٥)

الهيئة هى السلطة الجذرية العليا للتصديق الإلكترونى فى جمهورية مصر العربية ، وتتولى إصدار المفاتيح الشفرية الجذرية الخاصة بالهيئة والمفاتيح الشفرية الخاصة بالجهات المرخص لها بإصدار شهادات التصديق الإلكترونى ، وحفظ المفاتيح الشفرية الخاصة بالأشخاص الطبيعيين والاعتباريين فى حالة التوقيع الإلكترونى عن بعد ، وإعداد ونشر قائمة مقدمى خدمات الثقة .

وتتحقق الهيئة قبل منح ترخيص مزاولة نشاط تقديم خدمات التوقيع الإلكترونى من أن منظومة تكوين بيانات إنشاء التوقيع الإلكترونى لدى الجهة المرخص لها مؤمنة طبقًا للضوابط الفنية والتقنية والنظم والقواعد المشار إليها بهذه اللائحة .

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

الفصل الثاني

المعاملات الإلكترونية الموثوق بها وأنشطة تكنولوجيا المعلومات

مادة (٦)

شروط المعاملة الإلكترونية الموثوق بها

يجب أن تتوافر فى المعاملة الإلكترونية الموثوق بها الضوابط الفنية والتقنية المنصوص عليها بالملحق الفنى المرفق بهذه اللائحة ، وعلى الأخص ما يلى :

(أ) أن تسمح بتحديد هوية صاحب المعاملة .

(ب) أن تتم بطريقة تمكن من كشف أى تغيير لاحق يطرأ عليها .

(ج) أن تعتمد فى إجرائها على إحدى خدمات الثقة المنصوص عليها فى هذه اللائحة ، مستخدمة تقنية شفرة المفتاح العام Public Key Infrastructure .

مادة (٧)

حفظ المستندات بشكل الكتروني

(أ) إذا أوجب القانون حفظ مستندات أو معلومات أو سجلات معينة ، فإن هذا الالتزام يتحقق عندما يتم حفظ تلك المستندات أو المعلومات أو السجلات فى شكل إلكترونى ، شريطة مراعاة ما يلى :

١- حفظ المستند بالشكل الذى أُنشئ أو أرسل أو استلم به ، أو بشكل يمَكِّن من إثبات أنه يمثل بدقة المعلومات التى أنشئت أو أرسلت أو استلمت فى الأصل .

٢- بقاء المعلومات محفوظة على نحو يتيح استخدامها والرجوع إليها لاحقًا .

٣- حفظ المعلومات التى تمكن من معرفة مُرسل الرسالة الإلكترونية – إن وجدت – وجهة وصولها وتاريخ ووقت إرسالها واستلامها .

(ب) لا يمتد الالتزام بحفظ المستندات أو المعلومات وفقًا للفقرة السابقة إلى أية معلومات تنشأ بصورة ضرورية وتلقائية لمجرد التمكين من إرسال أو استلام الرسالة الإلكترونية .

(ج) يجوز استيفاء المتطلبات المنصوص عليها فى الفقرة (أ) من هذه المادة عن طريق الاستعانة بخدمات الغير ، طالما التزم بالشروط المنصوص عليها فى هذه الفقرة .

(د) لا تُخل الفقرات السابقة بما يلى :

١- أى قانون آخر ينص صراحة على الاحتفاظ بالمستندات أو السجلات أو المعلومات فى شكل إلكترونى وفق نظام معلومات إلكترونى معين أو الحفظ أو المراسلة باتباع إجراءات معينة .

٢- حرية الدولة فى تحديد متطلبات إضافية للاحتفاظ بمستندات إلكترونية صادرة عنها أو معتمدة منها .

مادة (٨)

المعاملات الإلكترونية الموثوق بها المؤتمتة

يجوز أن تتم المعاملة الإلكترونية الموثوق بها بين وسائل إلكترونية بطريقة آلية تتضمن إحدى الطريقتين الآتيتين :

(أ) نظامى معلومات إلكترونيين أو أكثر ، يكونان معدين ومبرمجين مسبقًا للقيام بمثل هذه العمليات ، ويكون التعاقد صحيحًا ومنتجًا لآثاره القانونية على الرغم من عدم التدخل الشخصى أو المباشر لأى شخص طبيعى فى عملية إبرام العقد فى هذه الأنظمة .

(ب) نظام معلومات إلكترونى مؤتمت بحوزة شخص وبين شخص آخر إذا كان الأخير يعلم أو من المفترض أن يعلم أن ذلك النظام سيقوم بإبرام العقد أو تنفيذه تلقائيا .

مادة (٩)

إسناد الرسالة الإلكترونية

(أ) تعتبر الرسالة الإلكترونية صادرة عن المُرسل إذا كان هو الذى أرسلها بنفسه .

(ب) فى العلاقة بين المُرسل والمُرسَل إليه ، تعتبر الرسالة الإلكترونية أنها صادرة عن المُرسل إذا أرسلت :

١- من شخص له صلاحية قانونية فى التصرف نيابة المُرسل فيما يتعلق بالرسالة الإلكترونية .

٢- أو من نظام معلومات آلى ومبرمج للعمل تلقائيا من قبل المُرسل أو نيابة عنه .

(ج) فى العلاقة بين المُرسل والمُرسَل إليه ، يحق للمرسل إليه أن يعتبر الرسالة الإلكترونية قد صدرت عن المرسل ، وأن يتصرف على أساس هذا الافتراض ، إذا :

١- طبق المُرسل إليه بطريقة سليمة إجراءً سبق أن وافق عليه المُرسل من أجل التأكد من أن الرسالة الإلكترونية قد صدرت عن المُرسل لهذا الغرض ،

٢- أو كانت الرسالة الإلكترونية ، كما تسلمها المُرسل إليه ، ناتجة عن تصرفات شخص تمكن بحكم علاقته بالمُرسل أو بأى وكيل له من الوصول إلى طريقة يستخدمها المُرسل لإثبات أن الرسالة الإلكترونية صادرة عنه .

(د) لا تسرى أحكام البنود السابقة فى الحالات التالية :

١- اعتبارًا من الوقت الذى تسلم فيه المُرسَل إليه إشعارًا من المُرسل يفيد بأن الرسالة الإلكترونية لم تصدر عنه ، ويكون قد أتيح للمُرسَل إليه وقت للتصرف على هذا الأساس .

٢- إذا علم المُرسل إليه أو كان يفترض فيه أن يعلم أن الرسالة الإلكترونية لم تصدر عن المُرسل ، وذلك إذا ما بذل عناية معقولة أو استخدم أى إجراء متفق عليه .

٣- إذا كان من غير المعقول للمُرسل إليه أن يعتبر الرسالة الإلكترونية صادرة عن المرسل أو أن يتصرف على أساس هذا الافتراض .

(هـ) عندما تكون الرسالة الإلكترونية صادرة أو تعتبر أنها صادرة عن المرسل أو عندما يكون من حق المرسل إليه أن يتصرف على أساس هذا الافتراض وفقًا للفقرات (أ،ب،ج) من هذه المادة ، يحق عندئذ للمرسل إليه ، فى إطار العلاقة بينه وبين المرسل ، أن يعتبر أن الرسالة الإلكترونية المستلمة هى الرسالة التى قصد المرسل أن يرسلها ، وأن يتصرف على هذا الأساس .

(و) يكون للمُرسل إليه الحق فى أن يعتبر كل رسالة إلكترونية يستلمها على أنها رسالة مستقلة وأن يتصرف على أساس هذا الافتراض وحده ، ولا تنطبق الفقرة (ز) من هذه المادة متى علم المرسل إليه أو كان عليه أن يعلم ، إذا بذل عناية معقولة أو استخدم أى إجراء متفق عليه ، أن الرسالة الإلكترونية كانت نسخة ثانية .

(ز) لا يكون للمُرسل إليه الحق فى الافتراضات والاستنتاجات الواردة فى الفقرتين السابقتين متى علم أو كان عليه أن يعلم إذا بذل عناية معقولة أو استخدم إجراءً متفق عليه ، بأن ثمة خطأ قد وقع أثناء إرسال الرسالة الإلكترونية كما استلمها .

مادة (١٠)

الإقرار بالاستلام

(أ) إذا تلقى المُرسل إقرارًا بالاستلام من المرسل إليه ، فإنه يفترض أن الأخير قد استلم الرسالة الإلكترونية ذات الصلة ، إلا إذا قدّم دليلا مناقضًا لذلك ، ولا ينطوى هذا الافتراض ضمناً على أن الرسالة الإلكترونية التى أرسلت من المُرسل تتطابق وفحوى الرسالة التى وردت إليه من المرسل إليه .

(ب) إذا نص الإقرار بالاستلام الذى يرد إلى المُرسل على أن الرسالة الإلكترونية ذات الصلة قد استوفت الشروط الفنية ، سواء المتفق عليها أو المحددة بموجب الملحق الفنى المرفق بهذه اللائحة ، فإنه يفترض أن تلك الشروط قد استوفيت ، ما لم يثبت العكس .

(ج) إذا لم يكن المُرسل قد اتفق مع المُرسل إليه على أن يكون الإقرار بالاستلام وفق شكل معين أو بطريقة معينة ، يجوز الإقرار بالاستلام عن طريق أية رسالة من جانب المرسل إليه ، سواء كانت بوسيلة إلكترونية أو آلية أو بأية وسيلة أخرى ، أو أى سلوك من جانب المرسل إليه ، يدل على استلام المرسل إليه الرسالة الإلكترونية .

(د) إذا كان المرسل قد ذكر أن الرسالة الإلكترونية مشروطة بتلقى إقرار بالاستلام ، تعامل هذه الرسالة فيما يتعلق بترتب أية حقوق أو التزامات قانونية بين المُرسل والمُرسَل إليه كأنها لم ترسل وذلك إلى حين استلام المرسل للإقرار .

(هـ) إذا لم يصرح المرسل بأن الرسالة مشروطة بتلقى إقرار بالاستلام ، ولم يستلم إقرارا بالاستلام خلال مدة معقولة ، فإنه يحق للمرسل أن :

١- يخطر المُرسل إليه بأنه لم يتلق إقرارًا بالاستلام ، ويحدد له مدة معقولة لإرسال الإقرار بالاستلام .

٢- إذا لم يستلم المرسل الإقرار بالاستلام خلال المدة المشار إليها فى الفقرة السابقة فإنه يجوز له بعد إخطار المُرسَل إليه أن يعتبر أن الرسالة كأنها لم ترسل أو يمارس أية حقوق أخرى مقررة له .

مادة (١١)

زمان ومكان إرسال واستلام الرسالة الإلكترونية

(أ) ما لم يتفق المرسل والمُرسل إليه على خلاف ذلك :

١- يتم إرسال الرسالة الإلكترونية عندما تدخل الرسالة نظام معلومات إلكترونى لا يخضع لسيطرة المُرسل أو الشخص الذى أرسل الرسالة نيابة عنه .

٢- يتحدد وقت استلام الرسالة الإلكترونية على النحو التالى :

إذا كان المرسل إليه قد عين نظام معلومات إلكترونى لغرض استلام الرسالة الإلكترونية : يتم الاستلام وقت دخول الرسالة الإلكترونية نظام المعلومات المعين ، أو وقت استخراج المرسل إليه الرسالة الإلكترونية إذا أرسلت إلى نظام معلومات تابع له ، ولكن ليس هو نظام المعلومات المعين لاستقبال الرسالة .

إذا لم يعين المُرسَل إليه نظام معلومات إلكتروني: يقع الاستلام عندما تدخل الرسالة الإلكترونية نظام معلومات تابع للمرسل إليه .

(ب) تنطبق الفقرة السابقة من هذه المادة على الرغم من كون المكان الذى يوجد فيه نظام المعلومات الإلكترونى يختلف عن المكان الذى يعتبر أن الرسالة الإلكترونية استلمت فيه بموجب الفقرة (ج) من هذه المادة .

(ج) تعتبر الرسالة الإلكترونية قد أرسلت من المكان الذى يقع فيه مقر عمل المُرسل وأنها استلمت فى المكان الذى يقع فيه مقر عمل المُرسل إليه ، ما لم يتفق المُرسل والمُرسَل إليه على خلاف ذلك .

(د) لأغراض هذه المادة :

١- إذا كان للمُرسل أو المُرسل إليه أكثر من مقر عمل واحد ، يكون مقر العمل هو المقر الأوثق علاقة بالرسالة الإلكترونية المعنية ، أو مقر العمل الرئيسى إذا لم توجد مثل هذه الرسالة .

٢- إذا لم يكن للمُرسل أو المُرسل إليه مقر عمل يشار إلى محل إقامته المعتاد .

٣- «مقر الإقامة المعتاد» فيما يتعلق بالشخص الاعتبارى ، يعنى مقره الرئيسى أو المقر الذى تأسس فيه .

مادة (١٢)

تقدم الهيئة بناءً على طلب كل ذى شأن ، خدمة الفحص والتحقق من صحة بيانات المعاملة الإلكترونية الموثوق بها ، نظير مقابل يحدد فئاته مجلس إدارة الهيئة .

مادة (١٣)

أنشطة تكنولوجيا المعلومات

يشترط لمزاولة أنشطة تكنولوجيا المعلومات الحصول على ترخيص بذلك من الهيئة .

ويصدر بتحديد هذه الأنشطة وشروط وقواعد ومقابل إصدار وتجديد الترخيص بها قرار من مجلس إدارة الهيئة .

الفصل الثالث

خدمات الثقة

مادة (١٤)

يشترط لمزاولة نشاط تقديم خدمات الثقة المنصوص عليها فى هذه اللائحة الحصول على ترخيص بذلك من الهيئة ، وفقًا للمعايير الفنية والتقنية المنصوص عليها بالملحق الفنى والتقنى المرفق بهذه اللائحة .

مادة (١٥)

لمجلس إدارة الهيئة أن يضع نظم وقواعد أخرى لتنظيم خدمات الثقة لمواكبة التطورات التقنية والتكنولوجية .

مادة (١٦)

تتضمن خدمات الثقة ما يلى :

أولاً – خدمة التوقيع الإلكترونى .

ثانيا – خدمة الختم الإلكترونى .

ثالثًا – خدمة البصمة الزمنية الإلكترونية .

رابعًا – خدمة البريد الإلكترونى المسجل .

خامسًا – خدمة التيقن من موقع الانترنت .

أولاً - خدمة التوقيع الإلكتروني

مادة (١٧)

التوقيع الإلكترونى Digital Signature

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 .

(ج) 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 .

(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 .

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

مادة (١٨)

يجب أن تتضمن منظومة تكوين بيانات إنشاء التوقيع الإلكترونى المؤمنة الضوابط الفنية والتقنية اللازمة المنصوص عليها بالملحق الفنى والتقنى المرفق بهذه اللائحة ، وعلى الأخص ما يلى :

(أ) أن تكون المنظومة مستندة إلى تقنية شفرة المفتاحين العام والخاص وإلى المفتاح الشفرى الخاص بالجهة المرخص لها والذى تصدره لها الهيئة ، وذلك كله وفقًا للمعايير الفنية والتقنية المشار إليها فى البند (١)/ الفقرة (أ) من الملحق الفنى والتقنى المرفق بهذه اللائحة .

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

(ج) أن تكــون أجهــزة التــأمين الإلكترونـــى (Hardware Security Modules) المستخدمة معتمدة طبقًا للضوابط الفنية والتقنية المشار إليها فى البند (١) / الفقرة (ب) من الملحق الفنى والتقنى المرفق بهذه اللائحة .

(د) أن يتم استخدام أدوات توقيع إلكترونى غير قابلة للنسخ ومحمية بكود سرى ، تحتوى على عناصر متفردة للموقع وهى بيانات إنشاء التوقيــع الإلكترونـــى وشـــهادة التصديق الإلكترونى ، ويتم تحديد مواصفات أداة التوقيع الإلكترونى وأنظمتها ، وفقًــا للمعايير الفنية والتقنية المبينة فى البند (١) الفقرة (جـــ) من الملحــق الفنـــى والتقنـــى المرفق بهذه اللائحة .

(هـــ) 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 محـــددة ومعلومة للمستخدمين حسب القواعد والضوابط التى يضعها مجلس إدارة الهيئة .

مادة (١٩)

يتحقق من الناحية الفنية والتقنية ، ارتباط التوقيع الإلكترونى بالموقع وحـــده دون غيره متى استند هذا التوقيع إلى منظومة تكوين بيانات إنشاء توقيع إلكترونـــى مؤمنـــة على النحو الوارد فى المواد (١٤ ، ١٧ ، ١٨) من هذه اللائحـــة ، وتـــوافرت إحـــدى الحالتين الآتيتين :

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

(ب) أن يتم التحقق من صحة التوقيع الإلكترونى طبقًا للمادة (٢٤) من هذه اللائحة .

مادة (٢٠)

تتحقق من الناحية الفنية والتقنية ، سيطرة الموقع وحده دون غيـــره ، علـــى أداة التوقيع الإلكترونى المستخدمة فى عملية تثبيت التوقيع الإلكترونى ، عن طريق حيـــازة الموقع أو تحكمه – عن بعد – فى أداة حفظ المفتاح الشفرى الخاص به .

مادة (٢١)

مع عدم الإخلال بما هو منصوص عليه فى المواد (١٧ ، ١٨ ، ١٩ ، ٢٠) من هذه اللائحة يتم من الناحية الفنية والتقنية ، كشف أى تعديل أو تبديل فى بيانات المحرر الإلكترونى الموقع إلكترونيا ، باستخدام تقنية شفرة المفتاحين العام والخاص وبمضاهاة شهادة التصديق الإلكترونى وبيانات إنشاء التوقيع الإلكترونى بأصل هذه الشهادة وتلك البيانات ، أو بأى وسيلة مشابهة .

ثانيا - خدمة الختم الإلكتروني

مادة (٢٢)

البصمة الختم الإلكترونى Digital Seal

تسرى على الختم الإلكترونى جميع الأحكام المنظمة للتوقيع الإلكترونى ، المنصوص عليها فى هذه اللائحة .

ثالثاً - خدمة البصمة الزمنية الإلكترونية

مادة (٢٣)

البصمة الزمنية الإلكترونية Time Stamp

يشترط لإثبات البصمة الزمنية الإلكترونية الشروط والضوابط الفنية والتقنية اللازمة المنصوص عليها بالملحق الفنى والتقنى المرفق بهذه اللائحة ، وعلى الأخص ما يلى :

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

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

(ج) أن يتم إنشاؤه بواسطة السلطة الجذرية العليا للتصديق الإلكترونى أو من إحدى الجهات المرخص لها من قبل الهيئة ، وفقًا للضوابط الفنية والتقنية المنصوص عليها فى البند (١) / الفقرتين (أ، هـ) من الملحق الفنى والتقنى المرفق بهذه اللائحة .

مادة (٢٤)

تقدم الهيئة بناءً على طلب كل ذى شأن ، خدمة الفحص والتحقق من صحة بيانات إنشاء التوقيع الإلكترونى ، أو الختم الإلكترونى ، أو البصمة الزمنية الإلكترونية نظير مقابل يحدد فئاته مجلس إدارة الهيئة ، ويجوز للهيئة أن تعهد للغير بتقديم هذه الخدمة تحت إشرافها . وتتحقق الهيئة فى سبيل القيام بذلك مما يأتى :

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

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

(ج) سهولة العلم بشخص الموقع أو منشئ الختم .

(د) توافر الشروط الفنية والتقنية والقواعد المشار إليها فى المادة (٢٣) من هذه اللائحة ، وذلك لفحص البصمة الزمنية الالكترونية .

وفى جميع الأحوال تصدر شهادة فحص بيانات خدمات الثقة المشار إليها فى هذه المادة من الهيئة .

رابعاً - خدمة البريد الإلكترونى المسجل

مادة (٢٥)

خدمة البريد الإلكترونى المسجل Registered e-mail service

خدمة البريد الإلكترونى المسجل هى الخدمة التى تتيح نقل الرسائل الإلكترونية بين المرسل والمرسل إليه عن طريق المرخص له بتقديم هذه الخدمة ، يتم من خلالها المصادقة على عملية إرسال واستلام الرسالة الإلكترونية ، وتحديد وقت وتاريخ إرسالها واستلامها بدقة ، وتأمين محتواها ومرفقاتها ضد الضياع أو التلاعب أو التلف أو أى تعديلات غير مصرح بها ، وذلك باستخدام إحدى خدمات الثقة المنصوص عليها فى البنود (أولاً أو ثانيا أو ثالثاً) من هذا الفصل .

مادة (٢٦)

بالإضافة الى المعايير الفنية والتقنية المنصوص عليها بالملحق الفنى ، والتقنى المرفق بهذه اللائحة ، يجب أن تتوافر فى خدمة البريد الإلكترونى المسجل الشروط الفنية الآتية :

(أ) أن تضمن تحديد هوية المرسل بدرجة عالية من الثقة تُحدد من قبل السلطة الجذرية العليا للتصديق الإلكترونى .

(ب) أن تضمن تحديد هوية المرسل إليه قبل تسليم محتوى الرسالة الإلكترونية .

(ج) أن تضمن سلامة إرسال الرسالة الإلكترونية واستلامها بواسطة توقيع إلكترونى أو ختم إلكترونى ، بحيث تسمح باستبعاد إمكانية حدوث أى تغيير فى محتوى الرسالة الإلكترونية غير قابل للكشف عنه .

(د) أن تسمح بإشعار المرسل والمرسل إليه ، بشكل واضح ، بكل تغيير لمحتوى الرسالة الإلكترونية يكون ضروريا لإرسالها أو استلامها .

(هـ) أن تشير بواسطة بصمة زمنية إلكترونية إلى تاريخ ووقت الإرسال والاستلام ، وإلى كل تغيير فى محتوى الرسالة الإلكترونية .

مادة (٢٧)

تعتبر الرسائل الإلكترونية المرسلة والمستلمة بواسطة خدمة البريد الإلكترونى المسجل قد تم إرسالها من المُرسل واستلامها من قبل المُرسَل إليه ما لم يثبت العكس .

خامساً - خدمة التيقن من موقع الإنترنت

مادة (٢٨)

خدمة التيقن من موقع الإنترنت Website Authentication (TLS/SSL)

خدمة التيقن من موقع الإنترنت هى خدمة يتم من خلالها إصدار شهادة للتحقق من موثوقية موقع الإنترنت وربطه بالشخص الطبيعى أو الاعتبارى الصادرة له الشهادة ، وذلك من خلال الجهة المرخص لها بتقديم هذه الخدمة .

مادة (٢٩)

بالإضافة إلى المعايير الفنية والتقنية المنصوص عليها بالملحق الفنى والتقنى المرفق بهذه اللائحة يشترط لإصدار شهادة التيقن من موقع الإنترنت Secure Sockets Layer certificate / Transport Layer securit استيفاء الشروط الفنية التالية :

(أ) إشارة – على الأقل فى شكل مناسب للمعالجة المؤتمتة – إلى أن الشهادة قد صدرت كشهادة مؤهلة لمصادقة موقع انترنت .

(ب) مجموعة من البيانات التى تحدد ، بشكل لا لبس فيه ، مُقدم خدمة التيقن من موقع الإنترنت الذى يصدر الشهادة :

فيما يتعلق بالشخص الاعتبارى : الاسم ورقم السجل التجارى – حال كونه شركة – من واقع السجلات الرسمية .

فيما يتعلق بالشخص الطبيعى : اسم الشخص .

(جـ) مجموعة من البيانات التى تمثل الشخص الذى صدرت له الشهادة :

فيما يتعلق بالأشخاص الطبيعيين: اسم الشخص الذى صدرت له الشهادة أو اسمه المستعار ، وفى حالة استخدام اسم مستعار ، يشار إليه بوضوح .

فيما يتعلق بالأشخاص الاعتبارية : على الأقل اسم الشخص – الاعتبارى الذى صدرت له الشهادة أو رقم سجله التجارى حال كونه شركة من واقع السجلات الرسمية .

(د) عناصر عنوان الشخص الطبيعى أو الاعتبارى – بما فى ذلك المدينة والمحافظة على الأقل – الذى صدرت له الشهادة من واقع السجلات الرسمية ؛

(هـ) عنوان / عناوين موقع الإنترنت الذى يديره الشخص الطبيعى أو الاعتبارى الذى صدرت له الشهادة .

(و) تفاصيل بداية ونهاية فترة صلاحية الشهادة .

(ز) موقع خدمات صلاحية الشهادة الذى يمكن من خلاله الاستعلام عن حالة صلاحية الشهادة .

الفصل الرابع

إجراءات تراخيص خدمات الثقة

مادة (٣٠)

تتبع الإجراءات الآتية للحصول على الترخيص بمزاولة أى من أنشطة خدمات الثقة الواردة بهذه اللائحة :

(أ) التقدم بالطلب على النماذج التى تعدها الهيئة فى هذا الشأن مصحوبًا بالبيانات والمستندات الدالة على توافر شروط الترخيص المنصوص عليها فى هذه اللائحة .

(ب) تقوم الهيئة بعد تسلمها الطلب وكافة المستندات والبيانات المطلوبة بفحصها والتأكد من سلامتها ، وتبت الهيئة فى طلب الحصول على الترخيص خلال مدة لا تتجاوز ستين يومًا من تاريخ استيفاء طالب الترخيص كافة الشروط والمتطلبات ، 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 .

أولاً - تراخيص خدمات التوقيع الإلكتروني والختم الإلكترونى والبصمة الزمنية الإلكترونية

مادة (٣١)

يجب أن يتوافر لدى طالب الحصول على الترخيص بمزاولة نشاط تقديم خدمة التوقيع الإلكترونى ، أو خدمة الختم الإلكترونى ، أو خدمة البصمة الزمنية الإلكترونية المتطلبات التالية :

(أ) نظام تأمين للمعلومات وحماية البيانات وخصوصيتها بمستوى حماية لا يقل عن المستوى المذكور فى المعايير والقواعد المشار إليها فى البند (١) / الفقرة (د) من الملحق الفنى والتقنى المرفق بهذه اللائحة .

(ب) دليل إرشادى يتضمن ما يلى :

١- إصدار شهادات التصديق الإلكترونى .

٢- إدارة المفاتيح الشفرية .

٣- إدارة الأعمال الداخلية .

٤- إدارة التأمين والكوارث .

وذلك وفقاً للمعايير الفنية والتقنية المذكورة فى البند (١) / الفقرة (هـ) من الملحق الفنى والتقنى المرفق بهذه اللائحة .

(جـ) منظومة تكوين بيانات إنشاء التوقيع الإلكترونى مؤمنة وفقاً للضوابط الفنية والتقنية المنصوص عليها فى 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 ، وتبعا لنوع الشهادة المصدرة ، وذلك فيما عدا مفاتيح الشفرة الخاصة التى تصدرها للموقع فلا يتم حفظها إلا بناءً 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 أداة التوقيع الإلكترونى ، أو عند الشك فى حدوث ذلك .

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

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

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

مادة (٣٢)

يجب أن تكون نماذج شهادات التصديق الإلكترونى التى يصدرها المرخص له متوافقة مع المعايير المحددة فى البند (١) / الفقرة (أ) من الملحق الفنى والتقنى المرفق بهذه اللائحة ، وأن تشتمل على البيانات الآتية :

(أ) ما يفيد صلاحية هذه الشهادة للاستخدام فى التوقيع الإلكترونى .

(ب) موضوع الترخيص الصادر للمرخص له ، موضحًا فيه نطاقه ورقمه وتاريخ إصداره وفترة سريانه .

(ج) اسم وعنوان الجهة المصدرة للشهادة ومقرها الرئيسى وكيانها القانونى والدولة التابعة لها إن وجدت .

(د) اسم الموقع الأصلى أو اسمه المستعار أو اسم شهرته ، وذلك فى حالة استخدامه لأحدهما .

(هـ) صفة الموقع .

(و) المفتاح الشفرى العام لحائز الشهادة المناظر للمفتاح الشفرى الخاص به .

(ز) تاريخ بدء صلاحية الشهادة وتاريخ انتهائها .

(ح) رقم مسلسل للشهادة .

(ط) التوقيع الإلكترونى لجهة إصدار الشهادة .

(ي) عنوان الموقع الإلكترونى المخصص لقائمة الشهادات الموقوفة أو الملغاة .

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

(أ) ما يفيد اختصاص الموقع والغرض الذى تستخدم فيه الشهادة .

(ب) حد قيمة التعاملات المسموح بها بالشهادة .

(جـ) مجالات استخدام الشهادة .

مادة (٣٣)

تتحدد النسخة الخاصة ببصمة شهادة السلطة الجذرية العليا للتصديق الإلكترونى الموقعة ذاتيا بالأحرف والأرقام والرموز المبينة فى البند (١)/ الفقرة (و) من الملحق الفنى والتقنى المرفق بهذه اللائحة ، وتستخدم البصمة من الكافة للتيقن والتثبت من صحة وسلامة شهادة التصديق الإلكترونى الجذرية الموقعة ذاتيا والمتاحة عبر شبكة المعلومات الدولية على الموقع التالى :

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

ثانيا - ترخيص خدمة البريد الإلكترونى المسجل

مادة (٣٤)

يجب أن يتوافر لدى طالب الحصول على الترخيص بمزاولة نشاط تقديم خدمة البريد الإلكترونى المسجل المتطلبات التالية :

(أ) توافر الشروط والضوابط الفنية المذكورة فى المعايير والقواعد المشار إليها فى البند (٢) فى الملحق الفنى والتقنى المرفق بهذه اللائحة .

(ب) نظام تأمين للمعلومات وحماية البيانات وخصوصيتها بمستوى حماية لا يقل عن المستوى المذكور فى المعايير والقواعد المشار إليها فى البند (١) / الفقرة (د) فى الملحق الفنى والتقنى المرفق بهذه اللائحة .

(ج) نظام لتحديد التاريخ والوقت للخدمات المرخص بها .

(د) نظام للتحقق من الأشخاص المتعاملين فى المنظومة مستخدمى الخدمة .

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

(و) نظام حفظ إلكترونى .

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

(ح) نظام لإيقاف الخدمة عند طلب ذلك من قبل العميل .

(ط) نظام يتيح وييسر للهيئة التحقق من توافر المتطلبات الفنية فى إطار أعمال الفحص والتحقق من جانب الهيئة .

ثالثاً - ترخيص خدمة التيقن من موقع الإنترنت

مادة (٣٥)

يجب أن يتوافر لدى طالب الحصول على الترخيص بمزاولة نشاط تقديم خدمة التيقن من موقع الإنترنت المتطلبات التالية :

(أ) توافر الشروط والضوابط الفنية المذكورة فى المعايير والقواعد المشار إليها فى البند (٣) فى الملحق الفنى والتقنى المرفق بهذه اللائحة .

(ب) نظام تأمين للمعلومات وحماية البيانات وخصوصيتها بمستوى حماية لا يقل عن المستوى المذكور فى المعايير والقواعد المشار إليها فى البند (١) / فقرة (د) الملحق الفنى والتقنى المرفق بهذه اللائحة .

(ج) نظام لتحديد التاريخ والوقت للخدمات المرخص بها .

(د) نظام للتحقق من الأشخاص المتعاملين فى المنظومة مستخدمى الخدمة .

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

(و) نظام حفظ إلكترونى .

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

(ح) نظام لإيقاف الخدمة عند طلب ذلك من العميل .

(ط) نظام يتيح وييسر للهيئة التحقق من توافر المتطلبات الفنية فى إطار أعمال الفحص والتحقق من جانب الهيئة .

الفصل الخامس

أحكام إجرائية عامة

مادة (٣٦)

تتولى سلطة التصديق الإلكترونى الحكومية إصدار شهادات خدمات التوقيع الإلكترونى والختم الإلكترونى والبصمة الزمنية الإلكترونية المنصوص عليها فى هذه اللائحة للجهات الحكومية وموظفيها ، ويقتصر التعامل بها فى المعاملات الإلكترونية للأغراض الحكومية سواء فيما بين هذه الجهات وبعضها البعض أو فيما بينها وبين الغير ، وذلك بذات الشروط والضوابط الفنية المنصوص عليها فى هذه اللائحة ويصدر بذلك قرار من مجلس إدارة الهيئة ، مع مراعاة أن يتم التصديق على المفاتيح الشفرية الخاصة بجهة التصديق الإلكترونى الحكومية بواسطة الهيئة .

مادة (٣٧)

للهيئة اعتماد الجهات الأجنبية المختصة بإصدار شهادات خدمات الثقة الواردة بهذه اللائحة 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 خدمات الثقة الواردة بهذه اللائحة .

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

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

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

مادة (٣٨)

يكون 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 المادة السابقة 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 .

مادة (٣٩)

للجهات الأجنبية المعتمدة أن تطلب من الهيئة اعتماد أنواع أو فئات شهادات خدمات الثقة 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 خدمات الثقة الصادرة من الجهات المرخص لها فى جمهورية مصر العربية .

مادة (٤٠)

يجب على طالب الترخيص استيفاء ما قد تتطلبه القوانين واللوائح ذات الصلة بالأنشطة المنصوص عليها فى هذه اللائحة .

مادة (٤١)

يجب على المُرخص له عدم إبرام أى عقد مع العملاء فيما يتعلق بتقديم الخدمات المرخص بها بموجب أحكام هذه اللائحة إلا بعد اعتماد نموذج هذا العقد من الهيئة ، طبقًا للقواعد والضوابط التى يضعها مجلس إدارة الهيئة لضمان حقوق ذوى الشأن .

مادة (٤٢)

على طالب الترخيص بمزاولة نشاط تقديم أيا من الخدمات المنصوص عليها فى هذه اللائحة أن يقدم الضمانات والتأمينات التى يحددها مجلس إدارة الهيئة لتغطية أى أضرار أو أخطار تتعلق بذوى الشأن ، وذلك فى حالة إلغاء الترخيص أو وقفه لأى سبب ، أو لتغطية أى إخلال من جانبه لالتزاماته الواردة فى الترخيص .

مادة (٤٣)

يحدد فى التراخيص المنصوص عليها فى هذه اللائحة التزامات المرخص له وفقًا للقانون وهذه اللائحة والقرارات الصادرة من مجلس إدارة الهيئة فى هذا الشأن .

مادة (٤٤)

ينشأ سجل خاص بالهيئة تقيد فيه الجهات المرخص لها ، ويعطى لكل جهة رقم مسلسل ويحدد فيه نوع الترخيص الممنوح لها ، ويتضمن بيانات هذه الجهة ورأس مالها وأعضاء مجلس إدارتها والمديرين بها وفروعها ومكاتبها وغير ذلك من البيانات التى يحددها مجلس إدارة الهيئة وما قد يطرأ على هذه البيانات من تغيير ، مع التزام هذه الجهات بإخطار الهيئة بأية تغييرات قد تطرأ على أى من هذه البيانات عقب منح الترخيص وطوال مدة سريانه .

مادة (٤٥)

تقوم الهيئة بشكل دورى بالتفتيش على الجهات المرخص لها للتحقق من مدى التزامها بأحكام القانون ولائحته التنفيذية والترخيص الممنوح لها ، وذلك بواقع مرة واحدة كل سنتين على الأقل .

مادة (٤٦)

تكون الهيئة هى الجهة المختصة بتقديم المشورة الفنية وأعمال الخبرة ، بشأن المنازعات التى تنشأ بين الأطراف المعنية بأنشطة خدمات الثقة والمعاملات الإلكترونية الموثوق بها وتكنولوجيا المعلومات ، على أن يتم التنسيق مع الجهات المعنية فيها بشأن أعمال الخبرة .

مادة (٤٧)

يحظر مزاولة أى نشاط من الأنشطة المنصوص عليها فى هذه اللائحة دون الحصول على ترخيص بذلك من الهيئة ، وفى حالة مخالفة هذه المادة يجوز للهيئة وقف النشاط جزئيا أو كليا بالإضافة إلى اتخاذ التدابير والإجراءات الأخرى المناسبة فى هذا الشأن .

مادة (٤٨)

تختص الهيئة وحدها دون غيرها – باعتماد منتجات وتطبيقات وأدوات خدمات الثقة المستخدمة داخل جمهورية مصر العربية ، وتنشر الهيئة دليل بهذه المنتجات والتطبيقات والأدوات بقرار من الرئيس التنفيذى .

مادة (٤٩)

مع عدم الإخلال بالعقوبات المنصوص عليها فى المادتين (٢٣ ، ٢٤) من القانون ، يجوز للهيئة فى حالة مخالفة المرخص له لشروط الترخيص ، أو توقفه عن مزاولة النشاط المرخص به أو اندماج منشأته فى جهة أخرى أو تنازله عن الترخيص للغير دون الحصول على موافقة كتابية مسبقة من الهيئة ، أن تصدر قرارًا مسببًا بإلغاء الترخيص أو وقفه لحين تدارك أو تصحيح المخالفة .

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

الملحق الفنى والتقني

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 .

خدمات الثقة

١ - التوقيع الإلكترونى ، الختم الإلكترونى والبصمة الزمنية الإلكترونية

(الفقرة - أ)

PKI Technology:

- The profiles for PKI operational management protocols must be based on PKIX (X .509-based PKI) .
- Public Key Infrastructure and Certificate Revocation List (CRL) profile must be based on X .509 5280 and its update .
- Time stamp service (TSP) profile must be according to the RFC 3161 and its update .
- Online Certificate Status Protocol (OCSP) profile must be according to the RFC 6960 and its updates .
- At least one of the following algorithms must be deployed .
  - Symmetric algorithms (AES, 3DES) .
  - Asymmetric algorithms (RSA, ECC) .
  - Hash algorithms (SHA2 with 256/384/512 bit output) .
- Minimum RSA/DSA key lengths must be at least 3072 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 .
- Cryptographic Message Syntax (CMS) must be according to the RFC 5652 and its update .
- ETSI ADES Digital Signatures (CADES, XADES, PADES, and ASiC) .
- ETSI TS 119 612- Trusted Lists .

(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 until September 21, 2026 and FIPS 140-3 level 3 after that or encluded in EU QSCD list .

(**الفقرة - جـ**)

Qualified 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 that use the most advanced security standard available in the market .
- QSCD must be certified FIPS 140-2 level 3 until September 21, 2026 and FIPS 140-3 level 3 after that or encluded in EU QSCD list and support RSA 3072 algorithm .

(**الفقرة - د**)

Security Standards:

- Information Security Management Standard (ISMS) as ISO/IEC 27001 and its guidance ISO 27002 (recommended) .
- Information technology -Public key infrastructure- Practices and policy framework ISO/IEC 27099(recommended) .
- Privacy Information Management System ISO/IEC 27701(recommended) .
- All hosting Data center/s should be at least Tier 3 design certified .

(**الفقرة - هـ**)

Operation Standards:

- ETSI (The European Telecommunications Standards Institute) ETSI EN 319 411-1 Policy requirements for certification authorities issuing qualified certificates .
- ETSI EN 319 411-2 Policy and security requirements for Trust Service Providers issuing certificates .
- ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers .
- ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps .
- ETSI TS 119 431-1: Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev .
- ETSI TS 119 431-2: Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation .
- ETSI TS 119 432: Protocols for remote digital signature creation .

(**الفقرة - و**)

Certificate Serial Number (S/N): la b6 bd a8 fa ld f7 5d **Subject Key Identifier:** 6c0c1eae8e8cecacda93d3d8315cadf31044d333 **Certificate Thumbprint:** d0ed83a8437a8c09e6ce24386405c6f3420f2fc0

٢- خدمة البريد الإلكترونى المسجل

Requirements for service providers providing electronic registered delivery service (ERDS)	
Technical Specification . Electronic Signatures and Infrastructures (ESI); . Registered Electronic Mail (REM) . "ETSI TS 102 640"	• All parts
Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers "ETSI EN 319 521"	• Electronic Registered Delivery Service ERDS • Electronic Registered Delivery Services Providers ERDS
Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 1: Framework and Architecture "Electronic 319 522"	• All parts
Electronic Signatures and Infrastructures (ESI); Policy and security Requirements for Registered Electronic Mail Service providers "ETSI EN 319 531"	• Registered Electronic Mail Service REMS
Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; providers Part 1: Framework and architecture "ETSI EN 319 532"	• All parts

The Universal Postal Union (UPU)	• S33 Interoperability framework for postal public key infrastructure • S52 Functional specification for postal registered electronic mail (PReM)

٣ - خدمة التحقق من موقع الإنترنت

Standard/ Guidelines	Scope
Requirements for service providers issuing the certificates for SSL (i.e. the Certificate Authority (CA))	
Web Trust Principles and Criteria for Certification Authorities - Extended Validation SSL - Version 1.7.8	
Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements "ETSI EN 319 411-1"	• Domain Validation Certificate Policy DVCP, • Organizational Validation Certificate Policy OVCP
Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates "ETSI EN 319 411-2"	
Electronic Signatures and Infrastructures (ESI); Certificate profiles; Part 4: Certificate profile for web site certificates "ETSI EN 319 411 -4"	

طبعت بالهيئة العامة لشئون المطابع الأميرية

رئيس مجلس الإدارة

محاسب/ أشرف إمام عبد السلام

رقم الإيداع بدار الكتب ٢٦٨ لسنة ٢٠٢٤

٢٠٢٤/٢٥٠١٧ – ٢٠٢٤/٧/١٤ – ٥٥٩