التوقيع الالكتروني

التوقيع الإلكتروني وسيلة التوسع وإنماء التجارة الإلكترونية

من المعلوم أن مجرد توافر الحق في حد ذاته لا يكفي للحصول عليه أو الزود عنه عند التنازع عليه. إذ يتعين لذلك وجود وسيلة إثبات لوجود هذا الحق ونسبته إلي من يتمسك به. وقد توصلت التشريعات المختلفة إلي أن الكتابة باليد هي سيدة الأدلة علي تحقق الحق أو الالتزام. وأخذ التعامل بين الأشخاص الطبيعة والمعنوية الخاصة والعامة، قوامه المستندات المكتوبة والمحررة باليد، وهي الأداة المضفية للحجية أو المحققة لصحة التصرف القانوني في أحوال أخري وهي المعول عليه في المعاملات المدنية والتجارية سواء في قيام الإلتزام أو انتقاله أو انقضائه. وعنيت التشريعات بوضع القواعد الموضوعيةو الإجرائية لقواعد الإثبات .كما جرت الإتفاقيات الدولية علي ذات النهج . وقد يستلزم القانون التوقيع لقيام الإلتزام وقد يرتب علي تخلف نتائج قانونية معينة. والكتابة قد تكون شرط إثبات أو شرط صحة المستند أو الرسالة أو الاتفاق.وفي هذا المقام نشير إلي ما ينص عليه قانون سنجابور للتوقيع الإلكتروني الصادر عام 1998 .
و مثال ذلك المادة 1 من قانون الإثبات المصري رقم 25 لسنة 1968 تنص علي أنه: "علي الدائن اثبات الإلتزام وعلي المدين لإثبات التخلص منه" وتنص الماد 14 منه علي أن المحرر العرفي يعتبر صادرا ممن وقعه ما لم ينكر صراحة ما هو منسوب إليه من خط أو امضاء أو ختم أو بصمة. أما الوارث أو الخلف فلا يطلب منه الإنكار ويكفي أن يحلف بأنه لا يعلم أن الخط أو الإمضاء أو الختم أو البصمة هي لمن تلقي عنه الحق". وتنص المادة 16 من ذات القانون علي أن الرسائل الموقع عليها قيمة المحرر العرفي في الإثبات ويكون للبرقيات هذه القيمة أيضا إذا كان أصلها المودع في مكتب التصدير موقعا عليه من مرسلها. وتعتبر البرقية مطابقة لأصلها حتي يقوم الدليل علي عكس ذلك. وإذا أعد أصل البرقية، فلا يعتد بالبرقية إلا لمجرد الاستئناس .
و كان القرن التاسع عشر اختتم سنواته الأخير، بترسيخ قدم الثورة الصناعية والكهربائية، فإن القرن العشرين كذلك اختتم سنواته الأخيرة بثورة جديدة تتمثل في قيام تكنولوجيا الحاسوب والمعلومات والتكنولوجيا الرقمية والاتصالات. ومن ثم جاء لنا بعالم افتراضي جديد قوامة الحوا سيب بمختلف مظاهرها وشبكة الإنترنت وعالم من المعلومات والاتصالات غير مسبوق أقامت عالم جديدا من التجارة هي التجارة الإلكترونية والتجارة عبر شبكة الإنترنت . جذبت لها المتعاملين والباحثين والمتراسلين سواء علي المستوي الفردي أو علي مستوي الأشخاص القانونية الإعتبارية الخاصة والعام، بل وجدت فيها الحكومات وسيلة لتقديم الخدمات للمواطنين عن طريقها.
وقد تعددت استخدمات هذا المجال وهذه الوسائل الإلكترونية .فبينما هناك من يلجأ إليها للنشر والإعلان، نجد آخرون، يسلكون هذا السبيل لتحقيق صفقات وابرام معاملات وعقود وتعاملات مع البنوك . وأصبحت الحواسيب محلا لتخزين المعلومات والحفاظ عليها وإعادة ترتيبها وتنظيمها وتحقيق أكبر فائدة منها ،أخذت طريقها إلي تعاملات البنوك والتعامل التجاري والتعامل بين الأجهزة الحكومية فيما بينها وبينها والجمهور.ومن ثم إهتمت الدول ببحث هذا الموضوع رعاية للمتعاملين ومدي أهميته في التوسع في التجارة والحركة التجارية.

كما عرض الأمر علي لجنة القانون التجاري الدولي في منظمة الأمم المتحدة Un commission on international trade law (UNCITRAL)في اجتماعها رقم 18 عام 1985 تقريرا بعنوان القيمة القانونية لسجلات الحاسابت أو قيودها (a/cn.9/265)وتبين لها أن في التجارة الإلكترونية وفي العلاقة بين حاسوب وآخر لا يوجد عائق قانوني في التعامل عن طريقهما أكثر من تطلب أن يكون التعامل بموجب مستندات ورقية مكتوبة باليد وموقعة باليد وأن القواعد السارية في التعاملات الدولية القائمة علي الإستخدام الورقي من شأنه إعاقة التعامل الإلكتروني عبر الحواسيب ويعوق تهيئة البيانات آليا. لذا بذلت الجهود من جانب المجلس الأوروبي ومجلس التعاون الجمركي واللجنة الاقتصادية لأوروبا لتشجيع الطرق الجديدة والتوصل إلي توفير الإطمئنان للتعامل عن طريقها وخلصت للجنة في اجتماعها المذكور إلي عدة توصيات منها مراجعة القواعد القانونية المؤثرة علي استخدام سجلات الحواسيب كوسيلة إثبات في المنازعات القضائية وإزالة العقبات نحو الاعتراف بها علي أن تكون متوافقة والتطور التكنولوجي الجديد. وكذلك مراجعة المتطلبات القانونية للتوقيع اليدوي وطرق الحجية القائمة علي الأوراق بهدف إمكان التعامل بالوسائل الإلكترونية لإضفاء الحجية عليها . وقد تكون عن هذه اللجنة فريق عمل لبحث هذا الموضوع الأمر الذي أسفر عن تبني القانون النموذجي للتوقيع الإلكتروني وكذلك للتجارة الالكترونية.
والتعامل عبر الحواسب والتراسل الإلكتروني بصفة عامة يثير ثلاث صعوبات تتحصل في: ثلاث مسائل حيوية تثور عن اجراء معاملة عن طريق الوسائط الإلكترونية عند رغبة الطرفين في استخدامها بدلا من استخدام الأوراق المكتوبة: 1-هل تلك الوسيلة قانونية ؟ وذلك لأن التشريعات تتطلب المستندات الورقية لقانونية التعامل. وبالتالي هل يصح التعامل وتبادل الرسائل الإلكترونية. 2- هل يمكن الوثوق بهذه الرسائل والتعامل ويكون محل ثقة الطرفين؟ - ما هي قواعد التعامل بين الأطراف؟.علي سبيل المثال ما هي مسئولية الموقع وما هي مسئولية مصدر شهادة التصديق وكيفية الرجوع عليه. وأصعب تلك العقبات هي ما دور التوقيع الإلكتروني وكيفية الوثوق بأن الموقع علي الرسالة هو الراسل؟ وما هو بيان دور التوقيع الإلكتروني إن كان له دور، وكذلك معرفة دور المشرع في تشجيع هذا التعامل الذي يؤدي إلي سرعة ويسر المعاملات والتعامل في إنجاز التراسل وعقد الصفقات.
والتساؤل عن مدي مشروعية التجارة الإلكترونية يثير في حقيقة الواقع التساؤل عن مدي انفاذ التعاملات الإلكترونية، وهذه تثير التساؤل عن مدي قانونية القيود أو السجلات الإلكترونية ومدى قانونية التوقيع الإلكتروني وبعبارة أخرى ما إذا كانت هذه القيود وهذا التوقيع يتحقق فيها المتطلبات القانونية التي تحققها المستدات المكتوبة والتوقيع اليدوي المكتوب في التشريعات المختلفة من عدمه؟ وهل السجل الإلكتروني مقبول كأداة إثبات معتمدة أمام القضاء أم يرفض اعتباره كذلك ؟ وهل السجلات الإلكترونية تكون أصل من أصول الإثبات؟ وهل يمكن الاحتفاظ بها في صورتها الإلكترونية دون اخراجها علي الورق وهل

حفظ تلك السجلات الإلكترونية هل يمكن أن يكون حجية ووحدة لتلك السجلات؟ ومن ثم يثور التساؤل عن تعريف التوقيع الإلكتروني ومتي تتحقق حجيته وشروط ذلك.
لذا يلزم الرجوع إلي مرجعية تطلب الكتابة والتوقيع اليدوي، وبعبارة أخري ما هي وظائف التوقيع اليدوي المكتوب باليد وبيان ما إذا كان التوقيع الإلكتروني يحققها من عدمه؟
ولعل العقبة الرئيسية ،فضلا عن إضفاء الحجية القانونية علي المستند والتوقيع الإلكتروني ،هو بناء الثقة في التعامل عن طريق الرسائل الإلكترونية وهنا نجد المحاولات للتوصل إلي تحقيق الأمور آنفة الذكر في السجل الإلكتروني والتوقيع الإلكتروني .

التعريف بالتوقيع الإلكتروني :

-التعريف بالتوقيع الإلكتروني :
يأتي التعريف بالتوقيع الإلكتروني ضمن مجموعة من المصطلحات التي يبدأ التشريعات الخاصة بالتوقيع الإلكتروني والتجارة الإلكترونية ببيان المقصود منها والتي تتكون منها منظومة تحقيق التعامل الإلكتروني وتحقق حجية التوقيع الإلكتروني .
و التوقيع، يعني بصفة عامة، أي رمز يعمل أو يتخذ من جانب طرف بقصد إضفاء الحجية علي الكتابة، فهو ليس مجرد سكب الحبر علي الورق ولكن يهدف الجمع بين الرمز والمستند لتأكيد قصد الأطراف. ووفقا للقانون التجاري يعتبر أي رمز، طالما وضع علي المستند من أحد أطرافه، بقصد إضفاء وتأكيد قصده، توقيعا. وبالتالي أول ما يلفت النظر إليه أنه وسيلة بيان قصد الموقع الأمر الذي يميز التوقيع من مجرد مجرد الكتابة. ولكن طبيعة هذا ا القصد قد تختلف وفقا لموضوع التعامل الذي يكشف عن هذا القصد. فقد يهدف التوقيع إلي بيان نية الإلتزام بما ورد بالمستند ، وقد يهدف إلي مجرد الموافقة علي ما جاء بهذا المستند أو مجرد الشهادة علي حصوله أمامه. أو الإفادة بأنه إطلع علي المستند ويقر بما فيه. أو انه هو محرر المستند. ولكن للتوقيع، فضلا عن كونه وسيلة إثبات، وظائف أخرى، تتمثل في أنه وسيلة التعرف علي شخصية الموقع، وكذلك الإفصاح أو الدلالة عن وحدة المستند The integrity of a documentفيعني التوقيع في نهاية المستند أن المستند متكامل ككل.

و قد تبين للدارسين أن التوقيع المكتوب باليد يطلب لتحقيق الأمور التالية: 1- تقديم اثبات ملموس عن وجود وطبيعة قصد الأطراف بالالتزام. 2- الإفصاح عن تبين الأطراف للنتائج المترتبة عن الدخول في اتفاق. 3- تقديم مستند مقروء متاح للجميع حتي الغير للتعرف عن التعامل. 4- تقديم مستند دائم يدل علي التعامل يظل غير محرفا طوال الزمن. 5- يسمح باستخراج وإعادة إنتاجه بحيث يكون لكل طرف الحصول علي نسخة مماثلة منه. 6- تسمح من بيان حجية الالمعلومات الواردة به عن طريق التوقيع. 7- تقديم مستند مقبول في الإثبات لدي السلطات العامة والمحاكم القضائية. 8- المستند يؤكد قصد كاتبة ويقدم سجل لها القصد -9 .يمكن من سهولة حفظ المعلومات في شكل ملموس. 10 – يمكن الستند من الرقابة اللاحقة والمراجعة فيما بعد لأغراض مثال ذلك الضرائب والمسائل الإجرائية. 11-يوجد الحقوق والالتزامات القانونية في الأحوال التي يتطلب القانون الكتابة فيها لأغراض الصحة .
في البيئة الإلكترونية المعادل للتوقيع المكتوب باليد هو النوقيع الإلكتروني. و هو تعبير عام ينصر ف إلي كل صور التوقيع التي تتخذ شكل اسم أو حروف أو ارقام قد تأخذ شكل صور متعددة وقد تتم بعدة طرق . وهو قد يكون، كما هو الحال في التوقيع المكتوب باليد، في شكل بعض الحروف أو الرموز التي ترتبط وتجمع منطقيا مع سجل أو مستند الكتروني لإضفاء الحجية عليه. ولكن مثل هذا التوقيع، سواء أكان مكتوبا باليد أو الإكترونيا، يقبل حصول التزوير أو التحريف ، و هوالأمر الأسهل بالنسبة للتوقيع الإلكتروني .
لذا كان الحل لضمان صحة ونسبة التوقيع الإلكتروني للموقع أو الراسل هو إيجاد وسيلة أكثر أمننا تمثلت في صورة التوقيع الإلكتروني الرقمي. لذا كان مركز اهتمام التشريعات المتعلقة بالتوقيع الإلكتروني ينصب علي كل من السجل أو القيد الإلكتروني والتوقيعات الإلكترونية التي تجري وترسل وتحفظ الكترونيا. وأصبح يشار عموما إلي تلك التوقيعات بتعبيرين : هما التوقيعات الإلكترونية أو التوقيعات الرقمية . ومن ثم يتعين تعريف هذين المصطلحين. ورغم الإختلاف بينهما. ولما كان التوقيع الإلكتروني الرقمي يقبل أن يتشكل ويأخذ جل صور التوقيع الإلكتروني الأخرى لذا استخدم تعبير التوقيع الرقمي كبديل عن تعبير التوقيع الإلكتروني بصفة عامة رغم التباين والفروق بينهما.
وقد عرفته المادة الثانية من القانون النموذجي للتوقيع الإلكتروني الذي وضعته منظمة الأمم المتحدة لجنة القانون التجاري الدولي- - الأونيسترال - علي أنه: "ولأغراض هذا القانون يقصد بالتعبيرات التالية المعاني المذكورة قرين كل منها (أ)- "توقيع الكتروني": يعني بيانات في شكل الكتروني مدرجة في رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقيا، يجوز أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات، ولبيان موافقة الموقع علي المعلومات الواردة في رسالة البيانات.
هذا وتعرف ذات المادة من ذات القانون النموذجي للتوقيع النموذج كل من رسالة البيانات والموقع علي النحو التالي :"رسالة بيانات" تعني معلومات يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها بوسائل الإلكترونية أو ضوئية أو بوسائل مشابه ، بما في ذلك ، علي سبيل المثال لا الحصر ، التبادل الإلكتروني للبيانات أو البريد الإلكتروني أو البرق أو التلكس أو النسخ البرقي ." والموقع "يعني شخصا حائزا علي بيانات إنشاء توقيع ويتصرف إما بالأصالة عن نفسه وإما بالنيابة عن الشخص الذي يمثله ".
وبلاحظ أن تسميات الرسالة تتعدد في الفقه والتشريعات علي الرغم من وحدة المضمون .ودلالتها تتسع لتشمل السجل الإلكتروني electronic record.الذي يعد أحد تطبيقات رسالة المعلومات .
وفي هذا المجال نجد أن القانون الماليزي الصادر عام 1997 تحت مسمي التوقيع الرقمي digital signature bill والمكون من ثماني أجزاء ، بعد أن عالج منظومة تولي شهادات التوثيق والساطات المعنية بها في الأجزاء الأربعة الأوي منه ، يعالج في الجزء الخامس المنظم لأحكام استخدام التوقيعات الرقمية وما يتعلق به ، يقرر في المادة 62 منه :" 1- حيثما توجد قاعدة قانونية تتطلب توقيعا أو تشترط نتائج معينة تترتب عن تخلف التوقيع ، هذه القاعدة تستوفي بوجود التوقيع الرقمي عندما :1- يكون هذا التوقيع محققا بالرجوع إلي مفتاح اعام وارد في شهادة صحيحة صادرة من مفوضة بإصدارها .ب)- أن يكون هذا التوقيع وضع من الموقع بقصد التوقيع علي الرسالة .ج) ألا يكون لمتلقي الرسالة علم أو لم يلاحظ أن الموقع : 1 -خرق واجب عليه كموق.2- أو أن أنه لم يحافظ

ويأمن المفتاح الخاص المستخدم في التوقيع الرقمي علي نحو منضبط . 2-رغما من أي قانون مكتوب مخالف يكون : أ) المستند الموقع بالتوقيع الرقمي وفقا لهذا القانون ملزما قانونا كمستند موقعا بخط اليد أو بصمة الإبهام أو أي علامة أخري .ب) والتوقيع الرقمي المنشأ وفقا لهذا القانون يفترض أنه توقيع ملزم قانونا . 3- ولا يوجد في هذا التشريع ما يمنع من اعتبار أي رمز كتوقيع سليما وصحيحا ملزما قانونا ." وتنص المادة 63 من ذات القانون علي أنه 1)- ما لم ينص علي خلاف ذلك بالقانون أو العقد ، يتحمل متلقي التوقيع الرقمي مسئولية كون هذا التوقيع مزورا ، إذا كان ، في ظل الظروف المحيطة به ، الإعتماد عليه غير معقول (-2 . علي امتلقي الراسلة عندما يقرر عدم الإعماد علي التوقيع وفقا لهذا القسم أن يخطر الوقع بعزمة علي ذلك ومبررات هذا التقرير." هذا وتنص المادة 64 منه علي أن ": المستنتد الموقع رقميا يعتبر مستندا مكتوبا باليد وتعد الراسلة صحيحة ونافذة وفعالة كما لوكانت مكتوبة علي ورق إذا".....":

وقد عرفت المادة 2 من قانون المعاملات الإلكترونية الأردني التوقيع الإلكتروني بأنه :" البيانات التي تتخذ هيئة حروف أو أرقام أو رموز أو إشارات أو غيرها ونكون مدرجة بشكل الكتروني أو رقمي أو ضوئي أو أي وسيلة أخري مماثلة في رسالة معلومات أو مضافة عليها أو رمتبطة بها ولها طابع يسمح بتحديد هوية الشخص الي وقعها ويميزها غن غيره من أجل توقيعه وبغرض الموافقة علي مضمونة ."كما عرفته المادة الأولي من القانون البحراني لقانون التجارة الإلكترونية بأنه :" معلومات في شكل الكتروني تكون موجودة في سجل الكتروني أو مثبتة أو مقترنة به منطقيا ويمكن للموقع استعاملها لإثبات هويته ."وقد عرفت المادة الأولي من القانون المصري رقم 15 لسنة 2004 بتنظيم التوقيع الإلكتروني بأنه :" ما يوضع علي محرر الكتروني ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها ويكون له طابع منفرد يسمح بتحديد شخص الموقع ويميزه عن غيره ." وقد عرفته المادة 2 من القانون النموذجي بشأن التوقيعات الإلكترونية الذي وضعته لجنة الأمم المتحدة للقانون التجاري الدولي بأنه : يعني البيانات في شكل الإلكتروني مدرجة في رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقيا ، ويجوز أن تستخدم لتعين هوية الموقع بالنسبة إلي رسالة البانات ، ولبيان موافقته علي المعلومات الواردة في رسالة البيانات"

التعريفات التي تبنتها تشرييعات الولايات بالولايات المتحدة الأمريكية.نشير إلي التعريفات التالية:

(an "electronic or digital method of identification that is executed or adopted by a person with the intent to be bound by or to authenticate a record)

("Electronic signature means any letters, characters, or symbols, manifested by electronic or similar means, executed or adopted by a party with an intent to authenticate a writing).(Any symbol executed or adopted, or any security procedure employed or adopted, using electronic means or otherwise, by or on behalf of a person with intent to authenticate a record.");(("An electronic identifier, created by computer, executed or adopted by the party using it with the intent to authenticate a writing).(("Any word, group of letters, name, including a trader-assumed name, mark, characters or symbols made manually, by device, by machine, or manifested by electronic or similar means, executed or adopted by a party with the intent to authenticate a writing.).(Electronic signature means a digital signature, executed or adopted by a party with an intent to authenticate a writing."); ("[Any of the following attached to or associated with an electronic record by an individual to authenticate the record: (a) a code consisting of a combination of letters, numbers, characters, or symbols that is adopted or executed by an individual as that individual's electronic signature; (b) a computer-generated signature code created for an individual; (c) an electronic image of an individual's handwritten signature created by using a pen computer." ("[Any letters, characters or symbols, manifested by electronic or similar means, executed or adopted by a party with an intent to authenticate a writing.") ("[Any identifier or authentication technique attached to or logically associated with an electronic record that is intended by the party using it to have the same force and effect as a manual signature) ("[An electronic identifier, created by a computer, intended by the party using it to have the same force and effect as the use of a manual signature.");" An electronic identifier, created by a computer, intended by the party using it to have the same force and effect as the use of a manual signature."); ("[Any combination of words, letters, symbols or characters that is attached to or logically associated with an electronic record and used by a person for the purpose of authenticating a document that has been created).

وعرفته المادة 2 من القانون الفيدرالي السويسري الخاصة بتقديم لخدمات الشهادات في مجال التوقيع الإلكتروني الصادر بتاريه 19 من ديسمبر عام 2004 بأنه:" في مفهوم هذا التشريع ، المعطيات الإلكترونية مجتمعة أو مرتبطة منطقيا بمعطيات الأكترونية أخري وتستخدم في التحقق من مصداقيته . و هو في التعريف الأكثر تطورا هو التوقيع الإلكتروني الذي يفي بالمتطلبات التالية : 1- أن يرتبط فقط بصاحبه -2. يسمح بالتعرف علي الموقع.3- أن يكون قد أنشأ بوسائل يحفظها الموقع تحت رقابتة المنفردة.4- يرتبط بالمعطيات التي يتعلق بها بحيث أن كل تغيير لاحق عليها يمكن اكتشافه. أما التوقيع الإلكتروني الموصوف فهو التوقيع الإلكتروني المتقدم والقائم علي تأمين إنشائه بالمفهوم الوارد بالمادة 6 فقرة 1و2 وهو بناء علي شهادة مكيفة بأنها صحيحة وقت لحظة إنشائه.

a-signature électronique : donnes l'electroniques jointes ou liées logiquement `a d"autre données electroniques et qui sevent ` a verifier leur authenticité; b- signature elelctronique avancée: La signature electronique qui satisfait aux exigences suivantes: 1- être liée uniquement au titulaire.2- permettre d'identifier le titulaire.3-être crée par des moyens que le titulaire peut garder sous son contrôle exclisif,4-être liée aux données auxquelles ell se rapporte de telle sorte que toute modification ultérieure des données soit détectable. C- signature électronique qualifiée: singature électronique

avancée fondée sur un dispositif sécurisé de céation de signature au sens de l'art6.al ,1,2 et sur un cerificat qualifié valable au moment de sa création ;

وفي قانون الصين الخاص بالتوقيعات الإلكترونية الصادر بتاريه 28 من أغسطس من عام 2004 تنص المادة الثانية منه علي أن :

All references to an electronic signature in this law are to electronic data that is contained in or attached to a data message and used to identify the signatory and indicate its endorsement of the contents of such data message.

وتنص المادة 13 من ذات القانون علي أنه التوقيع الإلكتروني يعتبر معولا عليه إذا استوفي الشروط التالية -1 : عند وقت انشاء رسالة المعلومات ، المعلومات المستخدمة للتوقيع تكون ملكا للموقع الإلكتروني.2- عند وقت التوقيع يكون انشاء التوقيع الإلكتروني تحت القابة المنفردة للموقع الإلكتروني.3- أي تغيير في التوقيع الإلكتروي بعد التوقيع ممكن ملاحظته . 4 -وأن يكون أي تغيير في مضمون وشكل معلومات الرسالة ، بعد التوقيع عليها ، يمكن ملاحظته . وللأطراف أن يستخدمو التوقيع الإلكتروني وفقا للشروط المتفق عليها فيما بينه للتعويل عليه .

وفي الجزء الأول من القرار الخاص بالتعاملات الإلكترونية التجارية لهونج كونج الصادر تحت رقم 1 لسنة 2000 ordonnace)) no.1 of 2000يعرف التوقيع الرقمي وذلك بعد أن عرف التشفير القائم علي الترميز المنفرد) asymmetric cryptosystem وهو النظام القادر علي توليد مفتاح آمن مكونا من مفتاح خاص للإنشاء التوقيع الإلكتروني ومفتاح عام للتحقق علي التوقيع الرقمي) بأنه ، بالنسبة إلي السجل الإلكتروني ، التوقيع الإلكتروني للموقع والمستخدم لنظام التشفير المذكور, ودالة hash fuction والتي يمكن التحقق بواسطتها من.....-2.....-1:

وتعرف المادة الأولي من القانون الفيدرالي النمساوي التوقيع الإلكتروني علي النحو التالي مميزا بين التوقيع الإلكتروني والتوقيع الإلكتروني الآمن علي النحو التالي":

Definitions

§ 2. The following definitions shall apply for the purposes of the present federal law:

1. Electronic signature: electronic data attached to or logically linked with other electronic data which serve to authenticate, that is establishing the identity of the signatory.

2. Signatory: a natural person to whom the signature creation data and the corresponding signature verification data have been allocated and who creates an electronic signature either on his own or on a third party's behalf, or a certification service provider who uses certificates to provide certification services.

3. Secure electronic signature: an electronic signature which

a) is allocated solely to the signatory,

b) allows the signatory to be identified,

c) is created using devices under the signatory's sole control;

d) is linked with the data to which it refers to in a way which allows any subsequent change to the data to be identified and

e) is based on a qualified certificate and is created using technical components and procedures which comply with the security requirements of the present federal law and the orders issued on the basis thereof.

4. Signature creation data: unique data such a codes or private signature keys which are used by the signatory to create an electronic signature.

5. Signature creation device: configured software or hardware which is used to implement the signature creation data.

6. Signature verification data: data such as codes or public signature keys which are used to verify an electronic signature.

7. Signature verification device: configured Software or hardware which is used to process the signature verification data.

8. Certificate: electronic confirmation in which signature verification data are linked to a specific person whose identity is certified.

9. Qualified certificate: a certificate containing the information referred to in § 5 and issued by a certification Service provider which meets the requirements of § 7,

10. Certification service provider: a natural or juristic person or some other legally capable Institution which issues certificates or provides other signature and certification services.

11. Signature and certification services: the provision of signature products and procedures, the issuing, renewal and administration of certificates, the provision of directory-, revocation-, registration-, time stamping-, computing- and consultancy- services in connection with electronic signatures.

12. Time stamp: electronically signed confirmation from a certification service provider that specific electronic data were submitted at a specific time.
13. Signature product: hardware or software or the specific components thereof used to create and verify electronic signatures or used by a certification service provider to provide signature or certification services.
14. Compromise: breach of security measures or security technique so that the level of security set up by the certification service provider no longer applies.

ويبدو أن هذا التعريف يتماثل مع التعريف الذي أورده التوجيه الصادر من مجلس الإتحاد الأوروبي تحت رقم 93 لسنة 1999 والذي علي دول الإتحاد العمل توقيع تشريعاتها الداخلية وفقا له وبما يحقق الأغراض المستهدفه به . حيث تنص المادة الأولي منه علي أن":

Definitions
For the purpose of this Directive:
1. 'electronic signature' means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication;
2. 'advanced electronic signature' means an electronic signature which meets the following requirements:
(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using means that the signatory can maintain under his sole control; and
(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;
3. 'signatory' means a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents;
4. 'signature-creation data' means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature;
5. 'signature-creation device' means configured software or hardware used to implement the signature-creation data;
6. 'secure-signature-creation device' means a signature-creation

ويلاحظ علي هذا التعريف أنه يميز بين التعريف العام للتوقيع الإلكتروني والتوقيع المتقدم أو المؤمن وهذا المنهج هو استنته تشريعات دول من دول الإتحاد.

فتعرف المادة الثانية من القانون الفيدرالي الألماني التوقيع الإلكتروني بأنه

:" § 2 Definitions(1) A digital signature within the meaning of this law is a seal on digital data created with a private signature key, which seal allows, by use of the associated public key marked with a signature key certificate of a certifier or of the Authority under § 3, the owner of the signature key and the unforged character of the data to be ascertained.

وقد عرفته المادة الأولي من القرار اللائحي الفرنسي الصادر لتحقيق حجية التوقيع الإلكتروني

Décret pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique
NOR:JUSC0120141D version consolidée au 19 avril 2002 - version JO initiale .
Article 1- Au sens du présent décret, on entend par :
1. Signature électronique : une donnée qui résulte de l'usage d'un procédé répondant aux conditions définies à la première phrase du second alinéa de l'article 1316-4 du code civil ;
2. Signature électronique sécurisée : une signature électronique qui satisfait, en outre, aux exigences suivantes :
- être propre au signataire ;
- être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;
- garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable.

حيث تعرف هذه المادة التوقيع الإلكرتوني بأنه معطاة تنتج عن استخدام طريقة تحقق الشروط المحددة في الجملة الأولي من الفقرة الثانية من المادة 1316-4 من الكود المدني . و أما التوقيع الإلكتروني المؤمن فهو توقيع الإلكتروني يفي فضلا عما يحقق التحقيق الإلكتروني المتطلبات التالية :1- أن يكون خاصا بالموقع -2 أن ينشأ بواسطة وسائل بمكن للموقع الحفاظ عليها تحت سيطرته المنفردة 3- يضمن مع ما هو مرتبط به رابطة تمكن من اكتشاف أي تعديلات لاحقة علي االمحرر".

كما يذهب التشريع الدانمركي Bill on Electronic Signatures - Bill No. L 229May 29 2000

إلي ذات التعريفات والتفرقة حيث ينص في المادة الأولي منه علي أن":

Part 2:Definitions

3. For the purposes of this Act:

1) "Electronic signature" shall be understood to mean data in electronic form that are attached to other electronic data by means of a signature-creation device and that are used to check that such data originate from the person indicated as signatory and that the data have not been changed.

2) "Advanced electronic signature" shall be understood to mean an electronic signature that:

(a) is uniquely linked to the signatory

(b) makes it possible to identify the signatory

(c) is created by means controlled only by the signatory, and that

(d) is linked to the data to which it relates in such a manner that any subsequent change made in the data is detectable.

أما القانون الفديرالي الألماني فينتهج ذات النج و يأخذ بالتفرقة بين التعريف العام للتوقيع الإلكتتروني والتفقيع الإلكتروني المؤمن أوالمتطور وأخيرا التوقيع الإلكتروني الموصوف حيث ينص علي:

Section 2: Definition of Terms

For the purposes of this Law

1. "Electronic signatures" shall be data in electronic form that are attached to other electronic data or logically linked to them and used for authentication;

2. "Advanced electronic signatures" shall be electronic signatures as in 1. above that :

a) are exclusively assigned to the owner of the signature code

b) enable the owner of the signature code to be identified

c) are produced with means which the owner of the signature code can keep under his sole control and

d) are so linked to the data to which they refer that any subsequent alteration of such data may be detected;

3. "Qualified electronic signatures" shall be electronic signatures as in 2. above that

a) are based on a qualified certificate valid at the time of their creation and

b) have been produced with a secure signature-creation device;

من هذه التعريفات يبين أن العناصر التي يتكون منها التعريف تتمثل فيما يلي:

-1أن التوقيع الإلكتروني إما أن يدرج في رسالة بيانات أو يرتبط أو يضاف إليها.

-2أن تكون الراسلة إلكترونية وأن يتم التوقيع بواسطة إلكتورنية.

-3أن يقصد منه تحقيق أمرين أساسيين : هما تحديد هوية الموقع وموافقتة علي الملعومات الواردة في رسالة البيانات . وعلي وجه العموم أن يحقق ثلاث وظائف أساسية تتمثل إضاف الحجية ، والدلالة عن وحدة وتكامل المستند الإلكتروني الرضي بمحتواه .

authentication ,integrity , non-repudiation

-ويمكن تلخيص بيان متطلبات تحقيق الثقة والإطمئنان في التوقيع الإلكتروني والرسالة:

يلاحظ ما يلي :

-1أن التوقيع الإلكتروني الرقمي حتي يؤدي دورة المطلوب يتعين أن يتبع ذلك ايجاد تنظيم قانوني وعلمي وأمني يحيط بإستخدام الرسائل الإلكترونية والتوقيع الإلكتروني الرقمي .و ويلاحظ أن التوقيع الإلكتروني الرقمي لا يتحقق فقط عن طريقة المفتاح المصح عنه ولكن هناك طرق أخرى أيضا تتبع لتأمين استخدام التوقيع الإلكتروني وعلي الجهة المختصة التي لها اصدار شهادات التصديق أن تختار الطريقة المثلي بشرط تحقق الضمانات التي يتطلبها المشرع بهدف تحقيق الغايات المرجوة من استخدام القيود الإلكترونية والتوقيع الإلكتروني و من ثم تشجيع التعامل عبر الرسائل الإلكترونية والتجارة الإلكترونية .

وقد رأينا التمييز بين التعريف العام للتوقيع الإلكتروني والتوقيع الإلكتروني المؤمن والتوقيع الإلكتروني الرقمي .

-2ولذلك نسوف نري أن التشريعات المعنية بالتوقيع الإلكتروني، حسبما سوف نعرض له، تتضمن بجانب إضفاء الحجية القانونية علي التوقيع الإلكتروني في الإثبات ، جانبا آخر، ينظم الجهات المعنية بإصدار شهادات التصديق وعلاقتها بكل من أطراف الرسالة الإلكترونية ومتطلبات السماح لها بالقيام بتلك الوظيفة والرقابة عليها. وتتطرق تلك التشريعات إلي بيان البيانات التي يجب أن تتضمنها لتلك الشهادات وبيان أنواعها والشروط الواجب توافرها فيها وما يتعلق كل نوع منها من ضمان. ومن جانب آخر، مدي مسئولية تلك الجهات المختصة بإصدارها عما يصدر عنها من الشهادات وسلطات الجهات الرقابية التي ترخص لتلك الجهات في العمل في هذا المجال .وبيان الجزاءات التي يمكن أن توقع والقرارات التي قد تتخذ في حالة مخالفة تلك الجهات لما هي ملتزمة به. فالتصديق يعني :

Authenticity is concerned with the source or origin of a communication. Who sent the message? Is it genuine or a forgery ?A party entering into an online transaction in reliance on an electronic message must be confident of that message That party must retain records of all relevant communications pertaining to the transaction and keep those records in such a way that the party can show that the records are authentic.

وقد عرفت المادة الثانية من القانون النموذجي المشار إليه الشهادة بأنها :" --تعني بيانات أو سجلا آخر يؤكد الارتباط بين الموقع وبيانات إنشاء التوقيع".

بينما يعني اكتمال المستند ووحدته أنه غير محرف أو منقوص:

Integrity is concerned with the accuracy and completeness of the communication. Is the document the recipient received the same as the document that the sender sent Is it complete? Has the document been altered either in transmission or storage

وكما تعني بأحوال صلاحية تلك الشهادات ، تعني بأحوال وقفها أو انقضاء صلاحيتها من جانب آخر. وإذ كان التشفير أداة لحماية الخصوصية في التعامل بين أطرافه أو بين أطراف الرسالة الإلكترونية، فإن المشرع قد يعني من جانب آخر، ببيان أحوال الخروج عن قاعد احترام الخصوصية عندما تتوافر حالة من الحالات التي تقتضي فيها المصلحة العامة ذلك. أن التعريفات تختلف في منهجها وفي موقفها من الحواسيب والتراسل الإلكتروني ووسائله. وقد يستخدم تعبير التوقيع الإلكتروني ولكن المشرع لا يحدد له معني ولا يعرفه .

-3أن هناك أربع متطلبات يتعين توافرها في تنظيم التعامل الإلكتروني والتوقيع الإلكتروني يجدر أن يتحلي بها هذا النظام ويؤديها :1- أن يكون مخصصاأو مفرد للشخص الذي يستخدمه بمعني ألا يكون لأكثر من شخص واحد استخدامه.2- قابلا للتحقق منه بحيث يمكن منه التعرف علي شخص الموقع. 3-وأن يكون تحت السيطرة الكلية والمنفردة للموقع. 4- أن يكون مرتبطا بمضمون الرسالة ومحتواها أو يمكن اعتباره منطقيا كذلك بحيث يمكن اكتشاف التحريف فيها للمعول عليها إذا حصل بعد التوقيع.

(d) Linkage to the Data Signed - The final requirement is that the signature must be linked to the data being signed in a manner such that if the data is altered after the signature is made, the fact of such alteration is disclosed to persons relying on the electronic record . This requirement is critical for a secure signature, because otherwise the electronic signature of one person could be altered to look like the electronic signature of another, or an electronic signature could be simply excised from one electronic record and pasted onto another.

اختلاف منهج التشريعات ::

لا يقتصر الخلاف بين التشريعات علي مجرد الإختلاف قي تعريف التوقيع الإلكتروني وإنما قد يكون الإختلاف في الأمور التالية :

-1فمنها ما يترك متاحا جميع طرق التوقيع الإلكتروني ومنها ما يتتطلب أن يكون التوقيع الإلكترونى رقميا .

-2وقد تختلف التشريعات فيما يصرح فيه بإستخدام التوقيع الإلكتروني من تعاملات أو مجالات . فمنها ما يقصر هذا الطريق علي أنواع معينة من التعاملات دون غيرها . ومنها ما يستعبد من نطاق استخدامها مجلات معينة أو تعاملات معينة لا يجوز فيها إستخدام الطريق الإلكتروني والتوقيع الإلكتروني . وهناك من التشريعات ما قصر نطاق استخدامها علي التعامل بين الجهات الحكومية أو التي يكون أحد أطرافها جهة حكومية . نذكر أمثلة منها علي سبيل المثال في الحاشية.مثال ذلك المادة 1 من القانون النموذجي المشار إليه والتي تنص علي أن يطبق هذا القانون حيثما تستخد توقيعات الكترونية في سياق "أنشطة تجارية" وهولا يلغي أي قاعدة قانونية يكون القصد منها حماية المستهلك ."وعلي سبيل المثال القانون الفيدرالي للولايات المتحدة الأمريكية الخاص بالتوقيع الإلكتروني في مجال الجارة العالمي والقومي الصادر عام 2000 تحت رقم 761 من السينات ورقم 1714 من مجلس النواب والموقع من من الرئيس كلينتون .الذي يستخرج من أحكامه كل ماهومحققا لحماية المستهلك وأنه ليس هناك التزاما علي أحد بأن يقبل استخدام أو يقبل السجلات الإلكترونية أة التوقيعات الإلكترونية . وأنه إذا كان الإخطار للمستهلك يجب أن يكون بالكتابة فإن المقابل الإلكتروني له يفي بهذا المطلب متي قبل المستهلك قبول البديل الإلكتروني وأثبت مكنته ولوج المعلومة بواسطة الشكل الإلكتروني. وهذا القانون لا يطبق في إنشاء أو تنفيذ الوصايا وشهادات منح الثقة .وكذلك في التبني والطلاق والأمور الأخري المتعلقة بمسائل الأسرة .كذلك بالنسبة لكل اخطار الغاء أو انتهاء الإنتفاع بالخدمات أو البدل عنها . أوللإسترداد أو نزع الحيازة أو انهاء الرهون. هذا ويتضمن هذا القانون بجانب الحكام الخاصة بالتوقيع الإلكتروني التي تسري اعتبارا من 10/1 /2000 هناك الأحكام الخاصة بالمحافظة علي السجلات الإلكترونية التي تسري اعتبارا من 1 متري من عام 2001.

-3وقد يري المشرع اصدار قانون منظم للتوقيع الإلكتروني، وقد يري الإكتفاء بتعديل قواعد الإثبات المقررة في القانون المدني كما حدث في فرنسا ويتبع ذلك بإصدار لقرارات إدارية تتناول التفصيل . والقانون االمنظم قد يكتفي بتقرير حجية التوقيع والسجل أو الراسلة الإلكترونية وبعض الأسس ويترك التفاصيل واختيار التقنيات للائحة التنفيذية لهذا القانون ، وقد يذهب المشرع لوضع التفصيلات والضوابط الخاصة بالموضوع ومتطلبات تحقق هذه الحجية في القانون كتنظيم شامل متضمنا جميع الموضوعات التي يتعين توافرها من أجل تحقيق الغاية من تقرير الحجية القانون للتوقيع والمستند الإلكتروني.

-4مما سبق يمكن استخلاص الخصائص التالية للتوقيع الإلكتروني : 1-أنه يرد علي وسيط الكتروني بوسيلة إلكترونية .2- يرتبط برسالة إلكترونية.3- بهدف إلي تحقيق الأغراض والوظائف التي يحققها التوقيع المكتوب باليد فهو البديل له من حيث الحجية والغرض في البيئة الإلكترونية وعلي الأخص بيان هوية الموقع من جانب واقرار موافقته علي مضمون المحرر الإلكتروني من جانب آخر مع العمل علي تحقيق الوظائف الأخري للتوقيع علي المحررات المكتوبة باليد .4- يتعين فيه ، وفقا إلي أغلبية التشريعات المعنية به ، توافرشروط معينة تستهدف الوثوق به و الإطمئنان له وتحقيق أغراضه التي من غيرها لايكون مقبولا في الإثبات . وبذلك يتعين التفرقة بين تقرير الحجية في الإثبات ومتطلبات تحققها بالنسبة للتوقيع الإلكتروني والسجل أو رسالة البايانت الإلكترونية.

-صور التوقيع الإلكتروني:

إذا كان التوقيع الإلكتروني قد يأخذ أحد الأشكال آنفة الذكر فإن طرق تنفيذه تتعدد صورها كما تتعدد التقنيات الفنية في تحقيق متطلباته .فتتعدد الطرق التكنولوجية المستخدمة في التوقيعات الإلكرتونية والتي قد تأخذ مثلا صورة التوقيعات الرقمية التي تعتمد نظم الترميز غير المتناظرة أو أدوات القايس الأحيائي التي نمكن من تحديد هوية الأفراد عن طريق سماتهم البدنية ، سواء عن طريق اليد أو شكل والجه أو قراءة بصمات الأصابع أو التعرف علي الصوت أو فحص شبكية العين إلخ (وكذلك نظم الترميز المتناظرة وكذلك أرقام الهوية الشخصية(pins) ، واستخدام أمارات لرموز كوسيلة للتحقق من الرسائل عن طريق ما يسمي بطاقات "ذكية" أو أي أداة

أخري يحتفظ بها الموقع ، وكذلك الصيغ الرقمية للتوقيعات الخطية وكذلك النقر مربع الموبفقة." ok-box "
فالتوقيع الإلكتروني قد يتم بواسطة الوسيط الإلكتروني وهو أداة أو أدوات أو أنظمة إنشاء التوقيع الإلكتروني والتي قد تأخذ أحد الصور التالية : لمسح الضوئي ، كما قد يتم بواسطة بالتوقيع باليد بواسطة قلم الكتروني ، وقد يتم بواسطة إدخال كود Pin code ، كما قد يتم بواسطة الضغط علي مربع يفيد القبول ، وأخيرا ، قد يتم بإتخاذ أسلوب التوقيع الإلكتروني الرقمي .PKI الذي يتعين تحقيقه علي النحو آنف الذكر.
وأيا كانت الصورة التي يتخذها التوقيع فإنه لضمان صحتة ونسبته إلي الموقع يلجأ إلي التشفير عن طريق استخدام Algorithm الأمر الذي تتعدد التقينات المستخدمة فيه ولكل من المتخصصين فيه طريقته وهو يمك بمرحلتين: مرحلة التشفير و مرحلة فكه . وقد سبق وقد ألمحنا بأن التشريعات قد تقف موقفا حياديا بالنسبة للتقنيات والتكنولوجيات المتوافرة لتحقيق التشفير وتأمين التعامل بالراسئل والتوقيع الإلكتروني وقد تذهب تشريعات منها إلي تبني صراحة أسلوب تكنولوجيا التوقيع الإلكتروني الرقمي .

حجيه القانونية التوقيع الإلكترونية

يتعين التمييز بين تقرير الحجية ومتطلبات التعويل علي التوقيع الإلكتروني أو بعبارة أخري متطلبات تحقق الحجية القانونية للتوقيع الإلكتروني.
-تقرير الحجية القانونية للتوقيع الإلكتروني :
قبل البدء فيما تثيره هذه الحجية القانونية للتوقيع الإلكرتوني نجد أن الغاية من دراسته هو التوصل بالتوقيع الإلكتروني والرسالة الإلكترونية ، إلي تحقيق ذات الحجية القانونية المقرر للتوقيع بخط اليد والستند المحرر علي الوق . وثم فهذه الدراسة يبتطلب الرجوع إلي قواعد الإثبات والتي يعني بها كأصل عام القانون المدني وقواعد الإثبات منه بصفة خاصة .
تثير الحجية القانونية للتوقيع الإلكتروني النقاط التالية : ماهيتها ، مدي هذه الحجية أو نطاق اعمالها ، ومتطلبات تحققها . ويلاحظ في هذا المجال أن الأصل في الإثبات هو الرجوع إلي قواعد الكود المدني في الإثبات . لذا نجد أن المشرع في كثير من الدول قد عدل في تلك القواعد ومع ذلك اضطر إلي تكملتها بالوائح المستقلة أو التنفيذية التي تضمنت قواعد تحقيق متطلبات هذه الحجية . بينما في دول أخري ، ذهبت إلي اصدار تشريعاتها المقررة لتلك الحجية بموجب تلك التشريعات . وقد يتضمن التشريع تفصيل أو أسس معالجة متطلبات تحققها أو قد يترك هذا للوائح التنفيذية . وهو في هذا الشأن قد يتخذ موقفا محايدا بالنسبة للتقنيات المستخدمة في هذا الشأن أوقد يتخذ موقفا بالنسبة لما يتبناة منها في هذا الخصوص.
هذا ومن جانب أخر ، قد تخرج بعض التشريعات الخاصة بالتوقيع الإلكترونية والتعامل الإلكتروني من نطاق تطبيقها أنواعا من التصرفات القانونية أو يقصر تطبيقها علي مجالا أو مجالات معينة وقد يعطي الأطراف الحق في سلوك التعامل الإلكتروني أو اتفاق علي عدم اتباعه أو الإتفاق علي أمور معينة عند اتباعه . وسف نظهر أثله علي ذلك فيما بعد .
و رغم رغبة التشريعات المختلفة في إضفاء الحجية علي التوقيعات الإلكترونية والرسائل الإلكترونية فإنها مع ذلك تأخذ ذلك بحذرها وتختلف في منهجها من حيث الشروط الواجب توافرها في إضفائها وبيان مجال إستخدامها. وكذلك في التنظيمات الخاصة بالتوثيق والتفاصيل . بحيث يتعين اجراء المقارنة فيما بينها والعمل علي توحيد الدعامات الرئيسية المهيأة للأخذ بهذا التنظيم بثقة وإطمئنان وذلك مع الأخذ بمبدأ الحيدة بين التقنيات التكنولوجية المتاحة لتحقيق شروط احجية التوقيع والمحرر الإلكتروني .
-القانون النموذجي للتوقيع الإلكتروني الصادر من الأونيسترال:
)لجنة القانون التجاري الدولي بمنظمة الأمم المتحدة(
وكان قد عرض علي لجنة القانون التجاري الدولي في منظمة الأمم المتحدة Un commission on international trade law (UNCITRAL)في اجتماعها رقم 18 عام 1985 تقريرا بعنوان القيمة القانونية لسجلات الحاسابت أو قيودها (a/cn.9/265)
وتبين لها أن في التجارة الإلكترونية وفي العلاقة بين حاسوب وآخر لا يوجد عائق قانوني في التعامل عن طريقهما أكثر من تطلب أن يكون التعامل بموجب مستندات ورقية مكتوبة باليد وموقعة باليد وأن القواعد السارية في التعاملات الدولية القائمة علي الإستخدام الورقي من شأنه إعاقة التعامل الإلكتروني عبر الحواسيب ويعوق تهيئة البيانات آليا. لذا صدر هذا القانون النموذجي للتوقيع الإلكتروني الذي أقرته الجمعية العامة لمنظمة الأمم المتحدة من إثني عشر مادة تتناول الموضوعات التالية:1- مجال التطبيق .2- تعريفات .3- المعاملة المتساوية لتكنلوجيات التوقيع .4- التفسير.5- تعديل الإتفاق .6- الإذعان لمتطلبات التوقيع .7 -تحقيق ما تقرره المادة السادسة لمتطلبات التوقيع .8_ مسلك الموقع .9- مسلك مقدم خدة الشهادة .10- الثقة .11- مسلك الطرف المعول عليه .12- الإعتراف بالشهادات والتوقيعات الإلكترونية الأجنبية .
ويلاحظ أن هذا القانون يراعي ما هو مقرر لمصلحة المستهلك ويضعها في اعتباره ولا يجعل من أحكامه ما يعلو علي ماهو مقرر لمصلحة المستهلك . وبعد اعتماد قانون الأونسترال النموذجي بشأن التجارة الإلكرتونية قررت لجنة القانون التجاري الدولي التابعة لمنظمة الأمم المتحدة ا في دورتها التاسعة عشر عام 1996 بعد اعتماد نموذجي للتجارة الكترونية صدر عام 1996 . إلي تكوين فريق عمل عكف علي وضع قانون نمدذجي للتوقيع الإلكتروني أسفر عن صدور قانون نموذجي للتوقيع الإلكتروني عام 2001. صدر له مرشدا لإعماله عام 2001.
و في عام 2005 أقرت الجمعية العامة لمنظمة الأمم المتحدة / مشروع اتفاقية استخدام المراسلات الإلكترونية في العقود الدولية.
وتنص المادة الأول منه علي أن : يطبق هذا القانون حيثما تستخدم توقيعات الكترونية في سياق انشطة تجارية وهو لا يلغي أي قاعدة قانونية يكون القصد منها حماية المستهلكين(المادة 1). وتنص المادة الثانية منه علي أنه: "ولأغراض هذا القانون يقصد بالتعبيرات التالية المعاني المذكورة قرين كل منها) أ)- "توقيع الكتروني": يعني بيانات في شكل الكتروني مدرجة في رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقيا، يجوز أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات، ولبيان موافقة الموقع علي المعلومات الواردة في رسالة البيانات .ب)- شهادة: تعني رسالة بيانات أو سجلا آخر يؤكدان الارتباط بين الموقع وبيانات انشاء التوقيع. ج) رسالة بيانات : تعني معلومات يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها بوسائل الكترونية أو ضوئية أو بوسائل مشابهة بما في ذلك، علي سبيل المثال لا الحصر، التبادل الإلكتروني للبيانات أو البريد الألكتروني أو البرق أو التلكس أو النسخ البرقي. (د) "موقع": يعني

شخصا حائزا علي بيانات إنشاء توقيع ويتصرف إما بالأصالة عن نفسه وإما بالنيابة عن الشخص الذي يمثله. هـ) "مزود خدمات تصديق" يعني شخصا يصدر الشهادات ويجوز أن يقدم خدمات أخرى ذات صلة بالتوقيعات الالكترونية. و) طرف معول عليه: يعني شخصا يجوز أن يتصرف استنادا إلي شهادة أو إلي توقيع الكتروني. وتنص المادة الثالثة منه والخاصة بالمعاملة المتكافئة لتكنولوجيات التوقيع(أو الحيدة بين التقنيات): "على أنه لا يطبق أي من أحكام هذا القانون، بإستثناء المادة 5، بما يشكل استبعادا أو تقييدا أو حرمانا من مفعول قانون لأي طريقة لإنشاء توقيع الكتروني تفي بالاشتراطات المشار إليها في الفقرة (أ) من المادة 6 أو تفي علي أي نحو آخر بمقتضيات القانون المطبق. وتنص المادة 4 الخاصة بالتفسير على أنه: "وفي تفسير هذا القانون يولي الاعتبار في تفسيره لمصدره الدولي وللحاجة إلي تشجيع توحيد تطبيقه ومراعاة حسن النية .وفي المسائل المتعلقة بالأمور التي يحكمها هذا القانون ولا يسويها صراحة تسوية وفقا للمبادئ العامة التي يستند إليها هذا القانون. (وبناء علي ذلك يتعين بيان تلك المبادئ والرجوع إليها) . وتنص المادة (5)علي أنه: يجوز الاتفاق علي الخروج علي أحكام هذا القانون أو تغيير مفعولها، ما لم يكن من شأن ذلك الاتفاق أن يكون غير صحيح أو غير ساري المفعول بمقتضي القانون المطبق.

والمادة (6) من القانون النموذجي للتوقيع الإلكتروني تنص علي أنه": حيثما يتطلب القانون أن تكون المعلومات مكتوبة باليد سواء أكان ذلك التزاما أو يترتب علي تخلفة نتائج قانونية، فإن هذا المطلب يعد محققا في رسالة المعلومات الإلكترونية إذا كانت تلك المعلومات الواردة بها قابلة للحصول عليها واستخراجها لإستعمالها فيما بعد. ويلاحظ أن تعبير رسالة المعلومات data message وفقا للمادة الثانية من ذات القانون تعني: المعلومات المتولدة أو المرسلة أو الواصلة أو المخزنة بواسطة الكترونيةأو بصريةأو ماشابه ذلك من وسائل .منها ،علي سبيل المثال وليس الحصر ، تبادل البيانات الكترونيا والبريد الإلكتروني و التلجراف والتلكس وتليكوبى . Electronic data interchange (EDI), electronic mail, telegram , telex or telecopy.

وينص البند 2 من ذات المادة علي أنه :" تطبق الفقرة (1) سواء أكان الاشتراط المشار إليه فيها في شكل التزام أم كان القانون يكتفي بالنص علي تبعات تترتب علي عدم وجود توقيع .أما البند3 من ذات المادة فينص علي أن يتعتبر التوقيع الإلكتروني قابلا للتعويل عليها لغرض الوفاء بالإشتراط المشار إليه في الفقرة _1 (إذا :أ) كانت بيانات انشاء التوقيع مرتبطة ، في السياق الذي تستخدم فيه ، بالموقع دون أي شخص آخر .(ب) كانت بيانات إنشاء التوقيع خاضعة ، وقت التوقيع ، لسيطرة الموقع دون أي شخص آخر .(ج) كان أي تغيير في التوقيع الإلكتروني ، يجري بعد حدوث التوقيع ، قابلا للإكتشاف .(د) كان الغرض من اشتراط التوقيع قانونا هو تأكيد سلامة المعلومات اليت يتعلق بها التوقيع وكان أي تغيير يجري في تلك المعلومات بعد التوقيع قابلا للإكتشاف".

وقد نصت الفقرة1 من المادة (7) من القانون النموذجي للتجارة الإلكترونية الصادر من منظمة الأمم المتحدة لجنة القانون التجاري الدولي عام 1996 على أنه: حيثما يتطلب القانون توقيع شخص، هذا المطلب يتحقق بالنسبة للرسالة الإلكترونية المتعلق بها إذا استعملت طريقة من شأنها التعريف بهذا الشخص والدلالة عن موافقته علي للمعلومات الواردة بها وإذا كانت الطريقة المستخدمة موثوقا بها وكانت مناسبة للغرض الذي من أجله تولدت أو أرسلت الرسالة في ضوء الظروف وبما فيها الإتفاق المتعلق بها. ونصت الفقرة الثانية منها: علي أن حكم الفقرة الأول يبطبق سواء أكان مطلب التوقيع هو الإلتزام بالتوقيع أو أن القانون يرتب نتائج علي عدم التوقيع .

ويلاحظ أن المادة 7 من قانون الأونستيرال النموذجي للتجارة الإلكترونية تستند إلي الاعتراف بوظائف التوقيع في بيئة ورقية ولدي اعداد قانون الأونستيرال النومذجي بشأن التجارة الإلكترونية ، ناقش الفريق العامل الوظائف التالية التي تؤديها التوقيعات الخطية عادة : تحديد هوية الشخص ،توفير ما يؤكد يقينا مشاركة ذلك الشخص بعينه في عملية التوقيع والربط بين ذلك الشخص ومضمون المستند ز ولوحظ بالإضافة غلي ذلك أن التوقيع يمكن أن يؤدي مجموعة متنوعة من الوظائف حسب طبيعة المستند الذي يحمل التوقيع . فعلي سبيل المثال : يمكن أن يكون التوقيع شاهدا علي نية الطرف الإلتزام بمضمون العقد الموقع عليه، وعلي نية الشخص الإقرار بتحريحه النص وعلي نيته تأييد مضمون المستند . وإذ أنه لا يمكن في البيئة الإلكترونية التمييز بين الرسالة الأصلية ونسخة منها / عندما لا تحمل الرسالة أي توقيع خطي ولا تكون مدونة علي ورق . كما أن امكانية الغش كبيرة نظرا لسهولة اعتراض المعلومات المتوافرة في شكل الكتروني وتغييرها دون اكتشاف ذلك ونظرا للسرعة التي بمكن بها تجهيز معاملات متعددة . لذا لإن الغرض من التقنيات المختلفة المتوافرة في الأسواف أو مازالت قيد التطوير ، وهو اتاحة الوسائل الفنية اليت يمكن بها أو يؤدي ، بيئة الكترونية ، بعض أو حميع الوظائف التي يتحدد أنها من خصائص التوقيعات الخطية . ويمكن أن يشار إلي هذه التقنيات بصورة عامة بعبارة " توقيعات الإلكترونية"

ورغم العلاقة الوثيقة بين بقانون التوقيع الإلكتروني النموذجي و القانون النموذجي للتجارة الإلكترونية بحيث بحث ما إذا كانت قانون النموذجي للتجارة الإلكرتونية يشمل التوقيع الإلكتروني في صيغة موسعة أم يفرد له قانون نموذجي مستقل إنتهت لمناقشة إلي تخصيص قانون نموذجي مستقل للتوقيع الإلكتروني حتي يكون نبراسا للدول . ويلاحظ أ، القانون إذ صدر صدر متسقا مع قانون الأنستيرال النموذجي بشأن التجارة الإلكترونية . فقد نقلت إلي القانون النموذجي للتوقيع الإلكتروني الأحكام العامة في القانون الأخير- بشأن التجارة الإلكترونية- و هذه هي التي تتعلق بنطاق التطبيق (المادة 1 (ومن المادة 2 تعريفات رسالة بيانات ومنشئ رسالة البيانات والمرسل إليه ، وكذلك الكادة 3 الخاصة بالتفسير ،و الرابعة الخاصة بالتغيير بالإتفاق ، والمادة 7 الخاصة بالتوقيع.

والقانون النموذجي التوقيع الإلكتروني يستند علي القانون النموذجي للتجارة الإلكترونية لأنه يقصد منه أن يجسد علي الخصوص ما يلي:

مبدأ الحياد بين الوسائط ، اتباع نهج يستوجب عدم التمييز تجاه استعمال النظائر الوظيفية للمفاهيم والممارسات الورقية التقليدية ، الإعتماد الواسع النطاق علي علي حرية الأطراف . أن يستخدم هذا القانون معايير دنيا في بيئة " مفتوحة " أي حيث يتصل الأطراف فيما بينهم الكترونيا دونما اتفاق مسبق ، وكذلك عند الإقتضاء كأحكام تعاقدية نموذجية أو كقواعد مفترضة احتياطيا في بيئة " مغلقة " أي حيث يكون يكون الأطراف ملزمين بقواعد وإجراءات تعاقدية موجوة مسبقا ينبغي اتباعها في الإتصال بالوسائل الإلكترونية .

ا حدي سمات هذا القانون الرئيسية هي اضافة مزيد من اليقين إلي تطبيق المعيار المرن الوارد بالمادة (7) من قانون الأونسيترال النموذجي بشأن التجارة الإكلكرتونية . والتي يجري نصها علي النحو التالي:

(1)"عندما يشترط القانون وجود توقيع من شخص يستوفي ذلك الشرط بالنسبة إلي رسالة البيانات إ ذا:

أ) استخدمت طريقة لتعيين هوية ذلك الشخص والتدليل علي موافقة ذلك الشخص علي المعلومات الواردة في رسالة البيانات و

ب) كانت تلك الطريقة جديرة بالتعويل عليها بالقدر المناسب للغرض الذي أنشئت أو أبلغت من أجله راسلة البيانات في ضوء كل الظروف ، بما في ذلك أي اتفاق متصل بالأمر.
(2)تسري الفقرة (1) سواء إ تخذ الشرط المنصوص عليه فيها شكل الترام أم اكتفي في القانون بمجرد النص علي العواقب اليت تترتب علي عدم وجود توقيع.
(3لا تسري أحكام هذه المادة علي مايلي".....:
يلاحظ أنه عند اعداد القانون النموذجي الجديد للتوقيع الإلكترونية ، أبدي رأي مفاده أن الإشارة الواردة في نص المادة 6 من هذا القانون إلي المادة 7 من قانون الأونستيرال النموذجي بشأن التجارة الإلكرتونية ينبغي أن تفسر بأنها تقصر نطاق القانون النموذجي الجديد علي الحوال التي يستخدم فيها توقيع الكتروني لتلبية شرط قانوني إلزامي يقضي بأن مستندات معينة ينبغي أن يوقع عليها لأغراض تبيان صلاحيتها. وذهب ذلك الرأي إلي أن نطاق القانون النموذجي الجديد بالغ الضيق ، بالنظر إلي أن القانون في معظم الدول لا يحتوي إلا علي شروط قليلة للغاية بشأن المستندات التي تستخدم في المعاملات التجارية .
وردا علي ذلك ، اتفق عموما علي أن ذلك التفسير لمشروع المادة 6) والمادة 7 من قانون الأونستيرال النموذجي للتجارة الإلكترونية) يتنافي مع تفسير عبارة " القانون" الذي إعتندته اللجنة في الفقرة 68 من دليل تشريع قانون الأونستيرال النموذجي بشأن التجارة الإلكترونية والذي ينص علي أنه " ينبغي أن تفهم الكلمة " القانون" ..... علي أنها لا تشمل القانون التشريعي أ، القانون التنظيمي فحسب ، بل تشمل أيضا القانون القضائي المنشأ والقوانين الإجرائية الأخري".
والواقع أن كل من المادتين واسع بصفة خاصة لأن معظم المستندات في سياق المعاملات التجارية يحتمل أو تواجهها ، في الممارسة العملية الشروط الواردة في قانون الإثبات كتابة.
هذا ويلاحظ أن كل من المادتين 6و7 من هذا القانون.....
وتنص المادة 8 من ذات القانون والخاصة بسلوك الموقع 1- حيثما أمكن استخدام بيانات إنشاء توقيع ذي مفعول قانوني يتعين علي كل موقع، (أ) أن يولي قدرا معقولا من العناية لاجتناب استخدام بيانات إنشاء توقيعه استخداما غير مأذون به. (ب) أن يبادر، دون تأخير لا مسوغ له ، غلي استخدام الوسائل التي يوفرها مقدم خدمات التصديق بمقتضي المادة (9) من هذا القانون، أو خلافا لذلك، إلي بذل جهود معقولة لإشعار أي شخص يجوز للموقع أن يتوقع منه علي وجه معقول أن يعول علي التوقيع الإلكتروني أو أن يقدم خدمات تأييد للتوقيع الإلكتروني، وذلك في حالة: 1- معرفة الموقع بأن بيانات إنشاء التوقيع تعرضت لما يثر الشبهة أو2-) كون الظروف المعروفة لدى الموقع تؤدي إلي نشوء احتمال قوي بتعرض بيانات إنشاء التوقيع لما يثير الشبهة ..ج) أن يولي قدرا معقولا من العناية في حال استخدام شهادة لتأييد التوقيع الإلكتروني، لضمان دقة واكتمال كل ما يقدمه الموقع من تأكيدات مادية ذات صلة بالشهادة طيلة دورة سريانها، أو يتوخى إدراجها في الشهادة. 2- يتحمل الموقع التبعات القانونية لتخلفه عن الوفاء بإشتراطات الفقرة 1.

وفي المادة "9" ينص علي التزامات مقدم خدمات التصديق، والتي تكون في حقيقة الأمر جانبا جوهريا في تنظيم الجهات المعنية بإصدار الشهادات وواجباتها. حيث تنص هذه المادة على ما يلي:
-1حيثما يوفر مقدم خدمات التصديق خدمات لتأييد توقيع الكتروني يجوز استخدامه لإعطاء مفعول قانوني بصفته توقيعا ، يتعين علي مقدم خدمات الفتصديق المشار إليه :
أ (أن يتصرف وفقا للتأكيدات التي يقدمها بخصوص سياساته وومارساته"
ب) أن يولي قدرا معقولا من العناية لضمان دقة واكتمال كل ما يفدمه من تأكيدات جوهرية ذات صلة بالشهادة طيلة دورة سريانها ، أو مدرجة في الشهادة.
ج) أن يوفر وسائل يكون الوصول إليها متيسرا بقدر معقول وتمكن الطرف المّعول من التأكد من الشهادة ممايلي:
-1هوية مقدم خدمات التصديق ،
-2أن الموقع المعينة هويته في الشهادة كان يتحكم في بيانات إنشاء التوقيع في وقت إصدار الشهادة ،
-3أن بيانات إنشاء التوقيع كانت صحيحة في وقت إصدارة الشهادة أو قبله ،
د) أن يوفر وسائل يكون الوصول إليها متيسرا بقدر معقول وتمكن الطرف المّعول من التأكد ، عند الإقتضاء ، من الشهادة أو من سواها مما يلي:
-1الطريقة المستخدة في تعيين هوية الموّقع ،
-2وجود أو تقييد علي الغرض أو القيمة التي يجوز أن تستخدم من أجلها بيانات إنشاء التوقيع أو أن تستخدم من أجلها الشهادة ،
-3أن بيانات إنشاء التوقيع صحيحة ولم تتعرض لما يثير الشبهه،
-4وجود أي تقييد علي نطاق أو مدي المسئولية اليت اشترطها مقدم خدمات التصديق.
-5ما إذا كانت هناك وسائل متاحة للموقع لتقديم إشعار بمقتضي الفقرة 1(ب) من المادة 8 من هذا القانون.
-6ما إذا كانت تتاح خدمة إلغاء آنية،
هه) أن يوفر ، حيثما تقدم الخدمات بمقتضي الفقرة الفرعية) د "5"، وسيلة للموقع لتقديم إشعار بمقتضي الفقرة (ي) من المادة 8 من هذا القانون ، وأن يضمن ، حيثما تقدم الخدمات بمقتضي الفقرة الفرعية (د) "6" إتاخدمة إغاء آنية ،
و) أن يستخدم في أداء خدماته نظما وإجراءات وموارد بشرية جديرة بالثقة,
-2يتحمل مقدم خدمات التصديق التبعات القانونية لتخلفه عن الوفاء بلإشتراطات الفقرة "1 ."

وتعني المادة "10" من ذات النظام بالجدارة بالثقة ولعل هذا الجانب يلقي الضوء علي كيفية تقدير الجهات العاملة في مجال إصدار شهادات التصديق وكيفية تقييمها من حيث مؤشر الثقة فيها. حيث تنص هذه المادة على أنه "لأغراض الفقرة) "1 و) من المادة 9 من هذا القانون يجوز / لدى تقرير ما إذا كانت أي نظم وإجراءات وموارد بشرية يستخدمها مقدم خدمات التصديق جديرة بالثقة أو لدي تقرير مدي جدارتها بالثقة، إيلاء الاعتبار للعوامل التالية: (أ) الموارد المالية والبشرية، بما في ذلك توافر الموجودات، (ب) جودة نوعية نظم المعدات والبرمجيات، (ج) إجراءات تجهيز الشهادات وطلبات الحصول على الشهادات والاحتفاظ بالسجلات.(د) إتاحة

المعلومات للموقعين المعنية هويتهم في الشهادات وللأطراف المعولة المحتملة، (هـ) انتظام ومدى مراجعة الحسابات من جانب هيئة مستقلة، (و) وجود إعلان من الجولة أو من هيئة اعتماد أو من مقدم خدمات التصديق بخصوص الامتثال لما يبق ذكره أو بخصوص وجوده. (ز) أي عامل آخر ذي صلة". ويعني القانون من جانب آخر بسلوك الطرف المعول حيث تنص المادة 11 منه علي أن: "يتحمل الطرف المعول التبعات القانونية الناجمة عن خلفه عن: (أ) اتخاذ خطوات معقولة للتحقق من قابلية التعويل علي التوقيع الإلكتروني، أو (ب) اتخاذ خطوات معقولة، إذا كان التوقيع الإلكتروني مؤيدا بشهادة لأجل: التحقق من صلاحية الشهادة أو وقفها أو إلغائها، 2- مراعاة وجود أي تقييد بخصوص الشهادة."

وتنص المادة 12 من ذات القانون علي الإعتراف بالشهادات والتوقيعات الألكترونية الأجنبية حيث تنص على أنه: 1- لدي تقرير ما إذا كانت الشهادة أو التوقيع الإلكتروني ساري المفعول قانونا أو مدى كونهما كذلك لا يولي أي اعتبار لما يلي: (أ) الموضع الجغرافي الذي تصدر فيه الشهادة أو ينشأ أو يستخدم فيه التوقيع الإلكتروني. (ب) الموضع الجغرافي لمكان عمل المصدر أو الموقع." 2- يكون للشهادة التي تصدر خارج الدولة المشترعة المفعول القانوني نفسه في الدولة المشترعة الذي للشهادة التي تصدر في الدولة المشترعة إذا كانت تتيح مستوى مكافئا جوهريا من قابلية التعويل. 3- يكون التوقيع الإلكتروني الذي ينشأ أو يستخدم خارج الدولة المشترعة المفعول القانوني نفسه في الدولة المشترعة الذي للتوقيع الإلكتروني الذي ينشأ أو يستخدم في الدولة المشترعة إذا كان يتيح مستوي مكافئا جوهريا من قابلية التويل. 4- لدي تقرير ما إذا كانت الشهادة أو التوقيع الإلكتروني يتيحان مستوى مكافئا جوهريا من قابلية التعويل لأغراض الفقرة 2 أو الفقرة 3 ، يولي الاعتبار للمعايير الدولية المعترف بها ولأي عوامل أخرى ذات صلة. 5- إذا اتفقت الأطراف فيما بينها على الرغم من ما ورد في الفقرات 2و3و4 ، علي استخدام أنواع معينة من التوقيعات الإلكترنية أو الشهادات، تعين الاعتراف بذلك الاتفاق بإعتباره كافيا لأغراض الاعتراف عبر الحدود، ما لم يكن من شأن ذلك الإتفاق أن يكون غير صحيح أو غير ساري المفعول بمقتضي القانون المطبق.
ولعل ما يستوقفنا من أحكام هذا القانون هو تعريف التوقيع الإلكتروني والمادة (6). وضرورة تحقق قابلية التوقيع الإلكتروني للتعويل عليه وأن يكون ذلك متسقا مع المعايير الدولية المعترف بها. فليس كل توقيع الكتروني يعد محققا لأحكام تلك المادة ، ولكن يتعين توافر الشروط الأربعة الواردة بالبند 3 من المادة 6 علي النحو آنف الذكر. ولكن حتى تتحقق تلك البنود، الأمر يتطلب منظومة من التنظيمات المصاحب لعملية التوقيع الإلكتروني. تتمثل في التزامات كل من الموقع ،و مصدر الشهادات ،وكذلك سلوك الطرف المعول. فكل من تلك الآطراف عليه الإلتزام بقدر من المسئوليات حتي يتحقق الأمان والثقة في التعامل والتوقيع الإلكتروني. بدون تلك الواجبات لا يتحقق الغرض المنشود.

وقد تناول المرشد في بيانه أغراض وأصل هذا النظام وذهب الى أن هذا النظام هو أداة للتنسيق بين التشريعات المختلفة المعنية بذات الموضوع، مع بيان الملاحظات العامة على التوقيع الإلكتروني: من حيث وظائفة والمقارنة بين التوقيعات الرقمية والتوقيعات الإلكرتونية الأخرى، ثم السمات الرئيسية لهذا القانون. وأخيرا المساعدة المتاحة من اللجنة في صياغة المشروعات .فالغرض من هذا القانون هو وضع أحكاما موحدة تكون القواعد الرئيسية لظاهرة التعامل الإلكتروني وإستخدام التوقيعات الإلكترونية حيث تكون هناك الرغبة في التناسق والقدرة علي التفعيل المشترك بين الدول where legal harmony as well as technical .
. interoperability is desirableفالإذعان لمتطلبات المادة السادسة من هذا النومذج والتي تذهب إلي انه حيثما يتطلب القانون توقيع شخص ما هذا المطلب يتحقق بالنسبة للبيانات إذا كان التوقيع الإلكتروني استخدم كتوقيع يعتمد عليه.
ويلاحظ أن القانون النموذجي يشكل خطوة جديدة في سلسلة من الصكوك الدولية التي اعتمدتها الأونسترال وهي إما تركز علي تحديد احتياجات التجارة الإلكترونية وإما أعدت مع مراعاة وسائل الإتصال الحديثة .

ويضاف إلي أحكام القانون النموذجي للتوقيع الإلكتروني وكذلك التجارة الإلكترونية ما خلصت إليه الجنة من مشروع اتفاقية دولية خاصة بالرسائل الإلكترونية المتعلقة بالإتفاقات التي تتم بين أطراف موجودة في دول مختلفة. نتوقف عند بعض نصوصها علي النحو التالي:حيث تحدد نطاق سريان أحكامها الذي ينصرف إلي الرسائل المتعلقة بتكوين أو أداء عقد أطراف المعاملة التجارية فيه موجودين في دول مختلفة.ويستبعد من سريانها أنواعا من العقود والمعاملات.وتعرف الرسائل، والرسائل الإلكترونية، ورسالة المعلومات، وماتنص عليه المادة4 منها.
إذا كان القصد من القانون النموذجي الجديد للتوقيع الإلكرتوني هاعتباره مكملا لقانون الأونستيرال النموذجي بشأن التجارة الإلكترونية ، غير أن هذا القانون بصفته اطارا لا يضع جميع القواعد والأنظمة التي قد تلزم (علي الترتيبات التعاقدية بين المستعملين) لتنفيذ تلك التقنيات في الدولة المشرعة . فلا يقصد من القانون النموذجي أن يتناول كل جانب من جوانب استعمال التوقيعات الإلكترونية.
بناء عليه قد ترغب الدولة المشترعة في اصدار لوائح تنظيمية تتضمن تفاصيل للإجراءات التي ينص عليها القانون النموذجي .
ويلاحظ أن تقنيات التوقيع الإلكرتوني التي يتناولها القانن النموذجي يمكن أن تثير إلي جانب المسائل الإجرائية التي قد يلزم التصدي لها لدي تنفيذ الوائح التنظيمية التقنية ، مسائل قانونية معينة لاتكون الإجابات عليها موجودة بالضرورة في القانون النوذجي بل في نصوص قانونية أخري ، قد يكون من تلك النصوص القانونية الأخري مثلا القوانين الإدارية وقوانين العقود وقوانين الضرر.
-القانون المصري الجديد رقم 15 لسنة 2004 :
يتكون هذا االقانون من ثلاثين مادة ، كما تتكون لائحتة التنفيذية من 24 مادة فضلا عن مادتي الإصدار . من جماع أحكام نصوص هذا القانون يبين أنه أخذ بما ذهب إلية القانون النموذجي للتوقيع الإلكتروني في مجمله وفي متطلبات التوقيع الإلكتروني . وقد اختط المشرع المصري منهج جديد يتفق مع التطور ومقتضيات التعامل بواسطة الرسائل الإلكترونية والتوقيع الإلكتروني ومضفيا الحجية سواء علي التوقيع الإلكتروني والكتابة الإلكترونية علي أن يستوفي التوقيع الإلكتروني الشروط والواردة بهذا القانون ولائحته.
و تنص المادة 14 منه القانون المصري الجديد رقم 15 لسنة 2004 علي أنه : للتوقيع الإلكتروني ، في نطاق المعاملات المدنية والتجارية والإدارية ، ذات الحجية المقررة للتوقيعات في أحكام قانون الإثبات في المواد المدنية والتجارية ، إذا روعي في انشائه واتمامه الشروط المنصوص عليها في هذا القانون والضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية لهذا القانون ." وتنص المادة

15 من ذات القانون علي أنه :" للكتابة الإلكترونية وللمحررات الإلكترونية ، في نطاق المعملات المدنية والتجارية والإدارية ، ذات الحجية المقررة للكتابة والمحررات الرسمية والعرفية في أحكام قانون الإثبات في المواد المدنية والتجارية ، متي استوفت الشروط المنصوص عليها في هذا القانون وفقا للضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية لهذا القانون ". وتنص المادة 16 من ذات القانون علي أن :" الصورة المنسوخة علي الورق من المحرر اللإلكتروني الرسمي حجة علي الكافة بالقدر الذي تكون فيها مطابقة لأصل هذا المحرر ، وذلك ما دام المحرر الإلكتروني الرسمي والتوقيع الإلكتروني موجودين علي الدعامة الإلكترونية ." كما تنص المادة 17 من ذات القانون علي أن :" تسري في شأن صحة المحررات الإلكترونية الرسمية والعرفية والتوقيع الإلكرتوني والكتابة الإلكترونية ، فيما لم يرد بشأنه نص في هذا القانون أو في لائحته التنفيذية الأحكام المنصوص عليها في قانون الإثبات في المواد المدنية والتجارية ".

من ذلك يبين أن المشرع المصري أضفي الحجية القانوني المقررة للتوقيعات في أحكام قانون الإثبات في المواد المدنية والتجارية علي التوقيع الإلكتروني وذلك في المعملات المدنية والتجارية وهو بذلك يكون قد توسع في هذا نطاق من حيث المعاملات التي تنصرف إليها هذه الحجية إلا أنه حددها من جانب آخر من حيث النطاق في حدود الحجية المقررة للتوقيعات في المواد المدنية والتجارية وعلق سريان هذه الحجية علي أن يراعي في انشائه واتمامه الشروط المنصوص عليها في هذا القانون والضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية لهذا القانون.

ومن ناحية ثانية فيما يتعلق بالكتابة و المحررات الإلكترونية فقد قرر لها أيضا ذات الحجية المقررة للكتابة والمحررات الرسمية والعرفية في أحكام قانون الإثبات في المواد المدنية والتجارية ، متي استوفت الشروط المنصوص عليها في هذا القانون وفقا للضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية لهذا القانون. وهو بذلك جمع بين المحررات الرسمية والعرفية وأكد أن المحرر الإلكتروني الرسمي له ذات الحجية للمحرر الرسمي اليدوي متي استوفت الشروط المنصوص عليها في هذا القانون وفقا للضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية لهذا القانون . بل أضفي علي الصورة المنسوخة علي الورق من المحرر اللإلكتروني الرسمي حجية علي الكافة بالقدر الذي تكون فيها مطابقة لأصل هذا المحرر ، وذلك ما دام المحرر الإلكتروني الرسمي والتوقيع الإلكتروني موجودين علي الدعامة الإلكترونية ، والقانون المصري يتسق في إضفاء الحجية للمحرر الرسمي مع المشرع الفرنسي جعل المحرر الإلكتروني الرسمي وهو من يتدخل موظفا عاما مختصا بما له من سلطة قانونية واختصاص في اضفاء الرسمية عليه بموجب القانون . وعلي سبيل المثال الموثقون.

أما فيما يتعلق بصحة الكتابة والمحررات والتوقيع الإلكتروني فقد جعل المشرع المصري أحكام هذا القانون هي الأصل ، وفيما لم يرد بشأنه نص في هذا القانون أو في لائحته التنفيذية يرجع إلي الأحكام المنصوص عليها في قانون الإثبات في المواد المدنية والتجارية ." والمشرع بذلك يربط بين قانون التوقيع الإلكتروني وأحكام مواد الإثبات في المعملات المدنيو التجارية علي النحو المذكور وفي الحدود المقررة لذلك.

والمشرع المصري في ذكره الحجية المقررة للمحررات الرسمية العرفية يكون مختلفا مع كثير من التشريعات التي لا تضفي تلك الحجية بنوعيها بل تكتفي بذكر الحجية المقرر للمحررات المكتوبة باليد دون هذا التفصيل . والمشرع المصري علي هذا النحو أخذ بمنهج المشرع الفرنسي الذي عني بتقرير هذه الحجية للمحرر الإلكرتوني الرسمي والمحرر الإلكتروني العرفي .

ورد ت بالقانون المصري للتوقيع الإلكتروني عدة مواد التي يظهر منها مكونات المنظومة والإطار الذي وضعه المشرع المصري كمتطلبات لتحقق حجية التوقيع الإلكتروني والسجلا ت الإلكترونية:

فالمادة 1 من هذا القانون تنص علي أن " فى تطبيق أحكام هذا القانون يقصد بالمصطلحات الآتية المعانى المبينة قرين كل منها:

)أ) 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.

)ب) المحرر الالكترونى:

رسالة بيانات تتضمن معلومات تنشأ أو تدمج ، أو تخزن ، أو ترسل أو تستقبل كليا أو جزئيا بوسيلة الكترونية ، أو رقمية ، أو ضوئية ، أو بأية وسيلة أخرى مشابهة.

)ج) التوقيع الالكترونى:

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

)د) الوسيط الالكترونى:

أداة أو أدوات أو أنظمة إنشاء التوقيع الالكترونى.

)هـ) الموقع : الشخص الحائز على بيانات إنشاء التوقيع ويوقع عن نفسه أو عمن ينيبه أو يمثله قانونا (و (شهادة التصديق الاليكترونى : الشهادة التى تصدر من الجهة المرخص لها بالتصديق وتثبت الارتباط بين الموقع وبيانات إنشاء التوقيع . (ز) الهيئة : هيئة تنمية صناعة تكنولوجيا المعلومات .(ح) الوزارة المختصة : الوزارة المختصة بشئون الاتصالات والمعلومات.

)ط) الوزير المختص : الوزير المختص بشئون الاتصالات والمعلومات.

وتنص م2)تنشأ هيئة عامة تسمى " هيئة تنمية صناعة تكنولوجيا المعلومات " تكون لها الشخصية الاعتبارية العامة وتتبع الوزير المختص ، ويكون مقرها الرئيسى محافظة الجيزة ، ولها إنشاء فروع فى جميع أنحاء جمهورية مصر العربية.

كما تنص م3) تهدف الهيئة إلى تحقيق الأغراض الآتية:

)أ) تشجيع وتنمية صناعة تكنولوجيا المعلومات والاتصالات.

)ب) نقل التكنولوجيا المتقدمة للمعلومات وتحقيق الاستفادة منها.

)ج) زيادة فرص تصدير خدمات الاتصالات وتكنولوجيا المعلومات ومنتجاتها.

)د (الإسهام فى تطوير وتنمية الجهات العاملة فى مجال تكنولوجيا المعلومات والاتصالات.

)هـ) توجيه وتشجيع وتنمية الاستثمار فى مجال صناعة تكنولوجيا المعلومات والاتصالات.
)و) رعاية المصالح المشتركة لأنشطة تكنولوجيا المعلومات.
)ز (دعم البحوث والدراسات فى مجال تكنولوجيا المعلومات والاتصالات وتشجيع الاستفادة بنتائجها
)ح) تشجيع ودعم المشروعات الصغيرة والمتوسطة فى مجال استخدام وتوظيف آليات المعاملات الالكترونية.
)ط) تنظيم نشاط خدمات التوقيع الالكترونى وغيرها من الأنشطة فى مجال المعاملات الالكترونية وصناعة تكنولوجيا المعلومات.
وتنص م4) علي أن :" تباشر الهيئة الاختصاصات اللازمة لتحقيق أغراضها ولها على الأخص ما يأتى:
)أ) إصدار وتجديد التراخيص اللازمة لمزاولة أنشطة خدمات التوقيع الالكترونى وغيرها من الأنشطة فى مجال المعاملات الالكترونية وصناعة تكنولوجيا المعلومات ، وذلك وفقا لأحكام القوانين واللوائح المنظمة لها.
)ب) تحديد معايير منظومة التوقيع الالكترونى بما يؤدى إلى ضبط مواصفاتها الفنية.
)ج) تلقى الشكاوى المتعلقة بأنشطة التوقيع الالكترونى والمعاملات الالكترونية وتكنولوجيا المعلومات واتخاذ ما يلزم فى شأنها.
)د) تقييم الجهات العاملة فى مجال أنشطة تكنولوجيا المعلومات وتحديد مستوياتها الفنية بحسب نتائج هذا التقييم.
)هـ (تقديم المشورة الفنية بشأن المنازعات التى تنشأ بين الأطراف المعنية بأنشطة التوقيع الالكترونى والمعاملات الالكترونية وتكنولوجيا المعلومات.
)و) تقديم المشورة الفنية إلى الجهات العاملة فى مجال أنشطة تكنولوجيا المعلومات ، وتدريب العاملين فيها.
)ز) إقامة المعارض والمؤتمرات والندوات المتخصصة فى مجال تكنولوجيا المعلومات والاتصالات داخليا وخارجيا.
)ح) إنشاء الشركات التى تساعد على تنمية صناعة تكنولوجيا المعلومات والاتصالات ، أو المساهمة فيها.
)ط) إيداع وقيد وتسجيل النسخ الأصلية لبرامج الحاسب الآلى وقواعد البيانات ، التى تتقدم بها الجهات أو الأفراد الناشرون والطابعون والمنتجون لها للمحافظة على حقوق الملكية الفكرية وغيرها من الحقوق.
وتنص المادة 18 - يتمتع التوقيع الالكترونى والكتابة الالكترونية والمحررات الالكترونية بالحجية فى الإثبات إذا ما توافرت فيها الشروط الآتية:
)أ) أرتباط التوقيع الالكترونى بالموقع وحده دون غيره.
)ب) سيطرة الموقع وحده دون غيره على الوسيط الالكترونى.
)ج) إمكانية كشف أى تعديل أو تبديل فى بيانات المحرر الالكترونى أو التوقيع الالكترونى.
وتحدد اللائحة التنفيذية لهذا القانون الضوابط الفنية والتقنية اللازمة لذلك.
وتنص المادة 19 من ذات القانون علي أنه :" لا تجوز مزاولة نشاط إصدار شهادات التصديق الالكترونى إلا بترخيص من الهيئة ، وذلك نظير مقابل يحدده مجلس إدارتها وفقا للإجراءات والقواعد والضمانات التى تقررها اللائحة التنفيذية لهذا القانون ودون التقيد بأحكام القانون رقم 129 لسنة 1947 بالتزامات المرافق العامة ، ومع مراعاة ما يأتى:
)أ (أن يتم اختيار المرخص له فى إطار من المنافسة والعلانية.
)ب) أن يحدد مجلس إدارة الهيئة مدة الترخيص بحيث لاتزيد على تسعة وتسعين عاما.
)ج) أن تحدد وسائل الإشراف والمتابعة الفنية والمالية التى تكفل حسن سير المرفق بانتظام وأطراد.
ولا يجوز التوقف عن مزاولة النشاط المرخص به أو الاندماج فى جهة أخرى أو التنازل عن الترخيص للغير إلا بعد الحصول على موافقة كتابية مسبقة من الهيئة.
وتنص المادة –20- تحدد اللائحة التنفيذية لهذا القانون البيانات التى يجب أن تشتمل عليها شهادة التصديق الالكترونى.
كما تنص المادة –21--بيانات التوقيع الإلكتروني والوسائط الالكترونية والمعلومات التى تقدم إلى الجهة المرخص لها بإصدار شهادات التصديق الالكترونى سرية ، ولايجوز لمن قدمت إليه أو اتصل بها بحكم عمله إفشاؤها للغير أو استخدامها فى غير الغرض الذى قدمت من أجله.

وتنص المادة --22– تختص الهيئة باعتماد–جهات الأجنبية المختصة بإصدار شهادات التصديق الالكترونى ، وذلك نظير المقابل الذى يحدده مجلس إدارة الهيئة ، وفى هذه الحالة تكون للشهادات التى تصدرها تلك الجهات ذات الحجية فى الإثبات المقررة لما تصدره نظيراتها فى الداخل من شهادات نظيرة ، وذلك كله وفقا للقواعد والإجراءات والضمانات التى تقررها اللائحة التنفيذية لهذا القانون.
وتنص المادة 26 --مع عدم الإخلال بأحكا–المادة (23) من هذا القانون ، يكون للهيئة إذا خالف المرخص له بإصدار شهادات تصديق إلكترونى شروط الترخيص أو خالف أيا من أحكام المادة (19) من هذا القانون ، أن تلغى الترخيص ، كما يكون لها أن توقف سريانه حتى إزالة أسباب المخالفة ، وذلك كله وفقا للقواعد والإجراءات التى تحددها اللائحة التنفيذية لهذا القانون.
وتنص المادة-- 27 مع عدم الإخلال بأحكا–المادة (23) من هذا القانون ، يكون للهيئة إذا خالف المرخص له بإصدار شهادات تصديق إلكترونى شروط الترخيص أو خالف أيا من أحكام المادة (19) من هذا القانون ، أن تلغى الترخيص ، كما يكون لها أن توقف سريانه حتى إزالة أسباب المخالفة ، وذلك كله وفقا للقواعد والإجراءات التى تحددها اللائحة التنفيذية لهذا القانون .
ويلاحظ أن المشرع المصري ترك تحديد تفصيلات مكونات المنظومة واختيار التقنيات التكنولوجية اللازمة لتحقيق أهداف تلك المنظومة التي تحقق الحجية القانونية للتوقيع الإلكتروني إلي اللائحة التنفيذية لهذا القانون التي صدرت بموجب قرار وزير الاتصالات رقم 109 لسنة 2005.
فتنص المادة 2 من قرار وزير الاتصالات وتكنولوجيا المعلومات رقم 109 لسنة 2005 الصادر باللائحة التنفيذية للقانون رقم 15 لسنة 2004 علي ما يلي:
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 ، 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 علما تاما بمضمون المحرر الإلكترونى قبل توقيعه له".
وتنص المادة 3 من ذات القرارتنص علي أن":
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 وفقا 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 لاتقل عن 2048 حرف إلكترونى. (bit)
)ج) أن تكون أجهزة التأمين الإلكترونى (Hardware Security Modules) المستخدمة معتمدة طبقا 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 ، وفقا للمعايير الفنية والتقنية المبينة فى الفقرة (ج) 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 أيضا 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.
وتنص المادة 4 من ذات القرار علي أن :" لمجلس إدارة الهيئة أن يضع نظم وقواعد أخرى لمنظومة تكوين بيانات إنشاء التوقيع الإلكترونى لمواكبة التطورات التقنية والتكنولوجية".
كما تنص المادة 5 من ذات القرار علي أن "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 طبقا للمادة (2) ، ومتضمنة الضوابط الفنية والتقنية والنظم والقواعد المبينة فى المادتين (3 ، 4.)
وتعتبر المنظومة بعد منح الترخيص وطوال مدة نفاذ مفعولة ، مؤمنة وفعالة مالم يثبت العكس".
وتنص المادة 6 من القرار علي أن:" 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".
وتذهب المادة 7 من ذات القرار إلي أن: "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.
)ج) سهولة العلم بشخص الموقع ، سواء فى حالة استخدام أسمه الأصلى أم استخدامه لاسم مستعار أم أسم شهرة.
ويجوز للهيئة أن تعهد للغير بتقديم هذه الخدمة تحت إشرافها ، وفى جميع الأحوال تصدر الهيئة شهادة فحص التوقيع الإلكترونى . "
وتنص المادة 8 من هذا القرار علي أن :" 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 متاحا 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 منشىء هذه الكتابة أو تلك المحررات ، أو لسيطرة المعنى بها.
)ب) أن يكون متاحا فنيا تحديد مصدر إنشاء الكتابة الإلكترونية أو المحررات الإلكترونية الرسمية أو العرفية ودرجة سيطرة منشئها على هذا المصدر وعلى الوسائط 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 ." وتنص المادة 9 من القرار علي أن ": يتحقق من الناحية الفنية والتقنية ، أرتباط التوقيع الإلكترونى بالموقع وحده دون غيره متى استند هذا التوقيع إلى منظومة تكوين بيانات إنشاء توقيع إلكترونى مؤمنة على النحو الوارد فى المواد (2 ، 3 ، 4) من هذه اللائحة ، وتوافرت إحدى الحالتين الآتيتين:
)أ) أن يكون هذا التوقيع مرتبطا بشهادة تصديق إلكترونى ، معتمدة ونافذة المفعول صادرة من جهة تصديق إلكترونى مرخص لها أو معتمدة.
)ب) أن يتم التحقق من صحة التوقيع الإلكترونى طبقا للمادة (7) من هذه اللائحة ." وأخيرا تنص المادة 10 من ذات القرار علي أن :" 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".
والمشرع المصري في منهجة المذكور يخالف القانون النموذجي الصادرمن منظمة الأمم المتحدة – لجنة القانون التجاري الدولي – المشار إليه في تلك الأمور حيث يطبق هذا القانون حيثما تستخدم توقيعات الكترونية في سياق أنشطة تجارية وهو لا يلغي أي قاعدة قانونية يكون القصد منها حماية المستهلكين كما تجيز المادة (5) منه الإتفاق علي الخروج علي أحكام هذا االقانون أو تغيير مفعولها ،

ما لم يكن من شأن ذلك الاتفاق أن يكون غير صحيح أو غير ساري المفعول بمقتضي القانون المطبق .هذا ويؤخذ في تفسير مصطلح تجاري بالتفسير الواسع بحيث يشمل المسائل الناشئة عن جميع العلاقات ذات الطابع التجاري سواء أكانت تعاقدية أم غير تعاقدية .
ويلاحظ أن القانون سنجابور ينتهج ذات النهج في تحديد نطاق سريان قانون التوقيع الإلكتروني حيث يخرج من نطاقه موضوعات معينة يجب فيها التعامل الورقي والتوقيع باليد .
كماأنه يبين، من جانب آخر، أنه لم يضع ولم ينظم الإستثناءات التي قد تخرج عن نطاق تطبيق أحكام هذا القانون علي النحو الوارد في قوانين أخري منها القانون الفديرالي للولايات المتحدة الأمريكية أو القانون النموذجي الصادر من منظمة الأمم المتحدة . كما أنه لم يتطرق بالتفصيل إلي التنظيم المطلوب لإضفاء الحجية القانونية للتوقيع والمحررات الإلكترونية في أحكامه كما ذهب إلي ذلك القانون الماليزي الخاص بالتوقيع الإلكتروني الصادر في عام 1997 والذي عني فضلا عن تنظيم جهات اصدار الشهادات وكل ما يتعلق بها والجهات الرقابية والمودع لدهم والمحتفظ طرفهم بالمفاتيح العامة وكذلك المعنيين بالتخزين وتأمين حفظ المراسلات.

-منهج المشرع الفرنسي:

في هذا المقام نذكر نص القانون المدني الخاصة بالإثبات حيث تنص المادة 1316 من القانون المدني الفرنسي الخاص بالإثبات والمواد المكرر لها علي ما يلي:
الدليل المقروءأو الدليل بالكتابة ينبع من حروف وأرقام أو من كل علامات أو رموز أخري لها دلالة مفهومة أيا كان الوسيط الذي تكون عليه أو أيا كانت صور إرسالهأو بعثه". هذا وتنص المادة (1316.1) علي أنه الكتابة المتخذة شكل الكتروني معترف لها بذات الحجية في الإثبات التي للكتابة المدرجة علي الورق .بشرط أمكان بيانها للشخص الصادر عنه وأن تنشأ وتحفظ في أحوال من طبيعها ضمان إ تكمالها أو وحدتها ." وتنص المادة 3- 1316 علي أن: الكتابة علي وسيط االكتروني لها ذات القوة في الإثبات كالكتابة علي االورق .
هذا وتنص المادة 4-1316 علي ما يلي": :
Article 1316-4 :(inséré par Loi nº 2000-230 du 13 mars 2000 art. 4 Journal Officiel du 14 mars 2000)
La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte. Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat.
حيث تذهب هذه المادة إلي أن التوقيع الضروري لإكتمال العمل القانوني يعرف الموقع . ويظهر رضاء الطراف الموقع عن الإلتزامات المتولدة عنه وعندما يوضع من قبل موظف عام فهو يضفي امصداقية هذا التصرف، وعندما يكون العمل الكترونيا يكون ،مع استخدام طريقة التعرف الضامنة لاتصاله بالعمل . ومصداقية هذا العمل تظل سارية حتي وجود الدليل العكسي ، متي كان التوقيع الإلكتروني منشأ ، وهوية الموقع مؤكدة واكتمال االعمل مضمونة بتحقق الشروط التي حددها القرار الصادر من مجلس الدولة.
Article 1317:(Loi nº 2000-230 du 13 mars 2000 art. 1 et art. 2 Journal Officiel du 14 mars 2000) :"
L'acte authentique est celui qui a été reçu par officiers publics ayant le droit d'instrumenter dans le lieu où l'acte a été rédigé, et avec les solennités requises.
Il peut être dressé sur support électronique s'il est établi et conservé dans des conditions fixées par décret en Conseil d'Etat.
Article 1318 :"(Loi nº 2000-230 du 13 mars 2000 art. 1 Journal Officiel du 14 mars 2000):" L'acte qui n'est point authentique par l'incompétence ou l'incapacité de l'officier, ou par un défaut de forme, vaut comme écriture privée, s'il a été signé des parties".Article 1319:"(Loi nº 2000-230 du 13 mars 2000 art. 1 Journal Officiel du 14 mars 2000) L'acte authentique fait pleine foi de la convention qu'il renferme entre les parties contractantes et leurs héritiers ou ayants cause.
Néanmoins, en cas de de plaintes en faux principal, l'exécution de l'acte argué de faux sera suspendue par la mise en accusation ; et, en cas d'inscription de faux faite incidemment, les tribunaux pourront, suivant les circonstances, suspendre provisoirement l'exécution de l'acte.Article 1320:"(Loi nº 2000-230 du 13 mars 2000 art. 1 Journal Officiel du 14 mars 2000):" L'acte, soit authentique, soit sous seing privé, fait foi entre les parties, même de ce qui n'y est exprimé qu'en termes énonciatifs, pourvu que l'énonciation ait un rapport
هذا بعد أن يضع القاعدة العامة في شأن الحجية القانونية للتوقيع والمحرر الإلكتروني في المواد 1316 ومكرراتها والمادة 1317 و1318 نجد أنه يقرر ذات الحجية لهما في نطاق ومجال العقود.
Section 3 : De l'envoi ou de la remise d'un écrit par voie électronique
Article 1369-7-(inséré par Ordonnance nº 2005-674 du 16 juin 2005 art. 1 IV Journal Officiel du 17 juin 2005)
Une lettre simple relative à la conclusion ou à l'exécution d'un contrat peut être envoyée par courrier électronique.
L'apposition de la date d'expédition résulte d'un procédé électronique dont la fiabilité est présumée,

jusqu'à preuve contraire, lorsqu'il satisfait à des exigences fixées par décret en Conseil d'Etat.
Article 1369-8-(inséré par Ordonnance nº 2005-674 du 16 juin 2005 art. 1 IV Journal Officiel du 17 juin 2005)
Une lettre recommandée relative à la conclusion ou à l'exécution d'un contrat peut être envoyée par courrier électronique à condition que ce courrier soit acheminé par un tiers selon un procédé permettant d'identifier le tiers, de désigner l'expéditeur, de garantir l'identité du destinataire et d'établir si la lettre a été remise ou non au destinataire.
Le contenu de cette lettre, au choix de l'expéditeur, peut être imprimé par le tiers sur papier pour être distribué au destinataire ou peut être adressé à celui-ci par voie électronique. Dans ce dernier cas, si le destinataire n'est pas un professionnel, il doit avoir demandé l'envoi par ce moyen ou en avoir accepté l'usage au cours d'échanges antérieurs.
Lorsque l'apposition de la date d'expédition ou de réception résulte d'un procédé électronique, la fiabilité de celui-ci est présumée, jusqu'à preuve contraire, s'il satisfait à des exigences fixées par un décret en Conseil d'Etat.
Un avis de réception peut être adressé à l'expéditeur par voie électronique ou par tout autre dispositif lui permettant de le conserver.
Les modalités d'application du présent article sont fixées par décret en Conseil d'Etat.

-منهج القانون الماليزي:
فمنهج المشرع الماليزي فيما يتعلق بالتوقيع والكتابة الإلكترونية على النحو التالي: " حيثما يتطلب القانون توقيع أو ينص علي نتائج معينة علي تخلفه فإن هذه القاعدة تتحقق بالتوقيع الرقمي ،(ولا يوجد في هذا القانون ما يمنع من اعتبار أي رمز توقيعا تحت أي قانون مطبق)، إذا كان التوقيع الرقمي تتوافر فيه مايلي :1- تم التحقق منه بالرجوع إلي المفتاح العام-2. كان وضعه من قبل الموقع بقصد التوقيع علي الرسالة 3-أن المستلم للرسالة ليس عنده علم أو اخطار بأن الموقع انتهك واجبا بإعتباره موقعاأو انه لايملك الحق في المفتاح الخاص.
حيث ينص هذا القانون في صلبه علي ما يلي:
Satisfaction of signature requirements
(1) Where a rule of law requires a signature or provides for certain consequences in the absence of a signature, that rule shall be satisfied by a digital signature where
(a) that digital signature is verified by reference to the public key listed in a valid certificate issued by a licensed certification authority;
(b) that digital signature was affixed by the signer with the intention of signing the message; and
(c) the recipient has no knowledge or notice that the signer(i) has breached a duty as a subscriber; or
(ii) does not rightfully hold the private key used to affix the digital signature.
(2) Notwithstanding any written law to the contrary-
(a) a document signed with a digital signature in accordance with this Act shall be as legally binding as a document signed with a handwritten signature, an affixed thumb-print or any other mark; and (b) a digital signature created in accordance with this Act shall be deemed to be a legally binding signature.
(3) Nothing in this Act shall preclude any symbol from being valid as a signature under any other applicable law.
63. Unreliable digital signatures
(1) Unless otherwise provided by law or contract, the recipient of a digital signature assumes the risk that a digital signature is forged, if reliance on the digital signature is not reasonable under the circumstances.
(2) Where the recipient determines not to rely on a digital signature under this section, the recipient shall promptly notify the signer of its determination not to rely on a digital signature and the grounds for that determination.
64. Digitally signed document deemed to be written document
(1) A message shall be as valid, enforceable and effective as if it had been written on paper if (a) it bears in its entirety a digital signature; and (b) that digital signature is verified by the public key listed in a certificate which(i) was issued by a licensed certification authority; and (ii) was valid at the time the digital signature was created.
(2) Nothing in this Act shall preclude any message, document or record from being considered written or in writing under any other applicable law.
65. Digitally signed document deemed to be original document.

A copy of a digitally signed message shall be as valid, enforceable and effective as the original of the message unless it is evident that the signer designated an instance of the digitally signed message to be a unique original, in which case only that instance constitutes the valid, enforceable and effective message.

مما سبق يبين أن تقرير الحجية القانونية للمحرر الإلكتروني والتوقيع الإلكتروني في الإثبات لا يكفي لوحده بل يتعين لتحقيق هذه الحجية تحقق المنظومة التي يتحقق بها تأمين الأمور السابق بيانها والإطمئنان علي توافرها بما يحقق الوظائف المقصودة .

-التشريع الفديرالي للولايات المتحدة الأمريكية:

ومن الطبيعي أن تأخذ الولايات المكونة للولايات المتحدة الأمريكية سبق المبادرة إذ تبنت كل منها تشريعها الخاص بها وأصدرته. و لكن الأمر كان أيضا محلا لعناية المشرع الفديرالي حيث أصدر في2 فبراير من عام 1998 قانون التوقيع الإلكتروني والتصديق الإلكتروني bill of digital signature and electronic authentification law لتعدل من أحكام قانون البنك الصادر the bank protection act 1968 وtd عام 1996 صدر تشريع . Utah digital signature act كما وقع الرئيس كلينتون في عام 2000 القانون الذي تم الموافقة عليه من كل من مجلس السينات (تحت رقم 761)و من مجلس النواب (تحت رقم 1714) القانون الفديرالي

للتجارة العالمية والوطنية .

The Millennium Digital Commerce Act of 2000 makes it legal to utilize digital technology to sign checks, credit and loan applications and many other legally binding documents.

وقد تظافرت الجهود في الجهات المعنية في الولايات المتحدة الأمريكية علي العمل علي تحقيق متطلبات الثقة والحجية للتوقيع الإلكتروني والسجل والرسالة الإلكترونية (أنظر الملحق في بيان تلك التشريعات). من ذلك جمعية المحامين الأمريكية the American bar associationحيث وضعت مخطط إرشادي لإستخدام التوقيع والرسائل الإلكترونية.

وهذا القانون ،وقد استهدف في المقام الأول حماية المستهلك ، يقرر الحجية القانونية للتوقيع والسجل أو المحرر الإلكتروني في الحدود التالية و التي يتحدد نطاق تطبيقه الموضوعي علي العمليات التجارية و بالنسبة لتلك العمليات فيما يتم منها بين الدويلات وبالنسبة التجارة الأجنبية مع الخارج يتطلب لسريان أحكامه علي رضاء المستهلك وإن كان لا ينكر أُر القانوني أو صحة التوقيع الإلكتروني أو المستنج الإلكتروني علي كونه متخذا هذا الشكل:

SEC. 101. GENERAL RULE OF VALIDITY.

(a) IN GENERAL- Notwithstanding any statute, regulation, or other rule of law (other than this title and title II), with respect to any transaction in or affecting interstate or foreign commerce--

(1) a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and

(2) a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.

علي الوجه العموم رغما عن أي نظام أو تنظيم أو أي قاعدة قانونية أخري غير البابين 1و2 من هذا القانون بالنسبة إلي لأي معاملة فيما بين الدويلات أو لها تأثير بالتجارة الخارجية التوقيع أو العقد أو أي سجل مرتبطا بهذه المعاملة لا يحجد أثره القانوني وصحتة أو قوته الإلزامية لمجرد أن شكله الإلكترونيا. 2- و أن ينكر علي هذا العقد أثره القانوني وصحته أو قوته الإلزامية لمجرد إ ستخدام التوقيع الإلكتروني أو السجل الإلكتروني في شكله.

(b) PRESERVATION OF RIGHTS AND OBLIGATIONS- This title does not--

(1) limit, alter, or otherwise affect any requirement imposed by a statute, regulation, or rule of law relating to the rights and obligations of persons under such statute, regulation, or rule of law other than a requirement that contracts or other records be written, signed, or in non electronic form; or

(2) require any person to agree to use or accept electronic records or electronic signatures, other than a governmental agency with respect to a record other than a contract to which it is a party.

(c) CONSUMER DISCLOSURES-

بالرغم من البند(أ) إذا تطلب تشريع أو لائحة أو أي قاعدة قانونية أخري أن تكون المعلومات المتعلقة بالتعامل أو التعاملات بين الدويلات أو التجارة الخارجية مقد مة أو متاحة للمستهلك بالكتابة ، فإن استخدام السجل الإلكرتوني لتقديم تلك المعلومات كما لوكانت مقدمة بالكتابة وذلك إذا تحقق التالي:

(1) CONSENT TO ELECTRONIC RECORDS- Notwithstanding subsection (a), if a statute, regulation, or other rule of law requires that information relating to a transaction or transactions in or affecting interstate or foreign commerce be provided or made available to a consumer in writing, the use of an electronic record to provide or make available (whichever is required) such information satisfies the requirement that such information be in writing if—المستهلك ارتضي استخدام المستند الإلكتروني ولم

يسحب رضاؤه .

(A) the consumer has affirmatively consented to such use and has not withdrawn such consent;

(B) the consumer, prior to consenting, is provided with a clear and conspicuous statement--

(i) informing the consumer of (I) any right or option of the consumer to have the record provided or made available on paper or in nonelectronic form, and (II) the right of the consumer to withdraw the consent to have the record provided or made available in an electronic form and of any conditions, consequences (which may include termination of the parties' relationship), or fees in the event of such withdrawal;

(ii) informing the consumer of whether the consent applies (I) only to the particular transaction which gave rise to the obligation to provide the record, or (II) to identified categories of records that may be provided or made available during the course of the parties' relationship;

(iii) describing the procedures the consumer must use to withdraw consent as provided in clause (i) and to update information needed to contact the consumer electronically; and

(iv) informing the consumer (I) how, after the consent, the consumer may, upon request, obtain a paper copy of an electronic record, and (II) whether any fee will be charged for such copy;

(C) the consumer--

(i) prior to consenting, is provided with a statement of the hardware and software requirements for access to and retention of the electronic records; and

(ii) consents electronically, or confirms his or her consent electronically, in a manner that reasonably demonstrates that the consumer can access information in the electronic form that will be used to provide the information that is the subject of the consent; and

(D) after the consent of a consumer in accordance with subparagraph (A), if a change in the hardware or software requirements needed to access or retain electronic records creates a material risk that the consumer will not be able to access or retain a subsequent electronic record that was the subject of the consent, the person providing the electronic record--

(i) provides the consumer with a statement of (I) the revised hardware and software requirements for access to and retention of the electronic records, and (II) the right to withdraw consent without the imposition of any fees for such withdrawal and without the imposition of any condition or consequence that was not disclosed under subparagraph (B)(i); and

(ii) again complies with subparagraph (C).

(3) EFFECT OF FAILURE TO OBTAIN ELECTRONIC CONSENT OR CONFIRMATION OF CONSENT- The legal effectiveness, validity, or enforceability of any contract executed by a consumer shall not be denied solely because of the failure to obtain electronic consent or confirmation of consent by that consumer in accordance with paragraph (1)(C)(ii).

:"يجب ألا تنكر الصحة و الفاعلية القانونية للعقد المنفذ من المستهلك وقوته الإلزامية ، لمجرد الإخفاق في الحصول علي رضاء الإلكتروني للمستهلك أو تأكيده وفقا البراجراف 1 فقرة ج بند "ii

(4) PROSPECTIVE EFFECT- Withdrawal of consent by a consumer shall not affect the legal effectiveness, validity, or enforceability of electronic records provided or made available to that consumer in accordance with paragraph (1) prior to implementation of the consumer's withdrawal of consent. A consumer's withdrawal of consent shall be effective within a reasonable period of time after receipt of the withdrawal by the provider of the record. Failure to comply with paragraph (1)(D) may, at the election of the consumer, be treated as a withdrawal of consent for purposes of this paragraph.

(5) PRIOR CONSENT- This subsection does not apply to any records that are provided or made available to a consumer who has consented prior to the effective date of this title to receive such records in electronic form as permitted by any statute, regulation, or other rule of law.

(6) ORAL COMMUNICATIONS- An oral communication or a recording of an oral communication shall not qualify as an electronic record for purposes of this subsection except as otherwise provided under applicable law.

-التوجيه الصادر من مجلس الاتحاد الأوروبي:

إذا ما نظرنا إلي الاتحاد الأوروبي نجد أن المجلس الأوروبي أصدرالتوجيه التالي ،بصدد التوقيع الإلكتروني

13/12 EN Official Journal of the European Communities 19. 1. 2000.DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999on a Community framework for electronic signatures THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THEEUROPEAN UNION, ,

فبعد أن عدد مبررات إصدار هذا التوجيه المكون من خمسة عشر مادة مواد وأربع ملاحق. يهمنا منها في هذا المقام ما نصت عليه المادة الخامسة منه المتعلقة بالأثار القانونية المترتبة علي التوقيع الإلكتروني ، و المادة السادسة منه التي نصت علي المسئولية التي تترتب علي شهادات التصديق أو التوثيق التي يعتمد عليها المتعاملين علي النحو التالي: هذا وقد أعملت دول الإتحاد هذا التوجيه في تشريعاتها الداخلية بما يحققه .نعرض لهذا التوجيه ثم بيان كيفية تطبيقة في تشريعات الدول الأوروبية.

و يقرر البند 1 المادة 5 من التوجيه الأوروبي الصادر من مجلس الإتحاد الأوروبي الحجية القانوني للتوقيع الإلكتروني :حيث ينص البند 1 من المادة 5 من التوجيه علي أنه يجب علي الدول أن تؤكد أن التوقيعات الإلكتروني المتطورة التي تستند علي شهادة موصوفة والتي يتم إشائها بواسطة أدة توقيع آمنة ، تفي بتحقيق المتطلبات القانونية لإرتباط التوقيع الإلكتروني بالبيانات المتخذة شكل الإلكتروني ، بذات الطريقة التي يحققها التوقيع بخط اليد بالنسبة للبيانات الواردة علي الورق
ويقررالبند (2) من المادة 5 من هذا التوجيه إلتزام الدول بتأكيد أن التوقيع الإلكتروني المتطور والمنشأ بأدة تأمين انشاء التوقيع و الذي يؤيد ه شهادة موصوفة ، لايحجد فاعليته القانونية أوالإعتراف به كدليل في المرافعات القانونية تأسيسا علي أنه متخذا شكلا اإلكترونيا أو أنه غير مستند علي شهادة غير موصوفة أو انه لايستند علي شهادة موصوفة صادرة من مقدم معتمد لتقديم اصدار تلك الشهادت أو انه علي ينشأ بأداة مؤمنة لإنشاء توقيع مؤمن .

-التشريع الدنماركي :
ونجد اعمالا للتفرقة التي تقررها المادة 5 من التوجيه الأوروبي أنه في المادة 13 من قانون التوقيع الإلكتروني الدانماركي . تنص المادة 13 مه ما يلي:
الأحكام القانونية التي بمقتضاها الرسا ئل الإلكترونية يجب أن تتضمن توقيع هذه حتي يكون لها القيمة القانونية يتعين أن تكون الرسالة متضمنة توقيع الإلكتروني متطور يعتمد علي شهادة وأن ينشأ التوقيع بأ داة مؤمنة . ومع ذلك في حالة الرسائل الإلكترونية الصادرة أو الواردة من سلطات عامة هذه الشروط لا تطبق إلأ إذا كانت التشريعات أو الأحكام التي تتبع في هذا الشأن لا تنص علي خلاف ذلك .
وتنص المادة 5 من هذا التشريع علي أن التوقيع الإلكتروني لا يمنع من أثره القانوني أو لا يستطاع رفضه كدليل إثبات أمام القضاء لمجرد أنه فقط : وارد بطريقة إلكترونية أو أنه لا يستند عي شهادة موصوفة أو أنه لا يستند علس شهادة موصوفة صادرة من مقدم خدمة الشهادات معتمد أو لأنه لم ينشأ بأداة مؤمنة لإنشاء التوقيع الإلكتروني.

-والتشريع الفديرالي النمساوي ينص AUSTRIAN Federal Electronic Signature Law :

Purpose and definitions

Purpose and scope

§ 1.(1) The present federal law sets out the legal framework governing the creation and use of electronic signatures and the provision of signature and certification services.

القانون الفديرالي يضع الإطار القانوني الحاكم لإنشاء واستعمال التوقيعات الإلكترونية والتوقيع وخدمات الشهادات.

(2) The present federal law shall apply in closed systems, insofar as the parties within the system have so agreed, and in open electronic transactions with courts and other authorities unless a law stipulates otherwise.يطبق هذا القانون سواء في النظم المغلقة بين الأطراف كما يطبق علي المعاملات الإلكترونية المفتوحة أمام المحاكم والسلطات الأخري مالم ينص القانون علي غير ذلك

Definitions

§ 2. The following definitions shall apply for the purposes of the present federal law:

1. Electronic signature: electronic data attached to or logically linked with other electronic data which serve to authenticate, that is establishing the identity of the signatory.

2. Signatory: a natural person to whom the signature creation data and the corresponding signature verification data have been allocated and who creates an electronic signature either on his own or on a third party's behalf, or a certification service provider who uses certificates to provide certification services.

3. Secure electronic signature: an electronic signature which

a) is allocated solely to the signatory,

b) allows the signatory to be identified,

c) is created using devices under the signatory's sole control;

d) is linked with the data to which it refers to in a way which allows any subsequent change to the data to be identified and

e) is based on a qualified certificate and is created using technical components and procedures which comply with the security requirements of the present federal law and the orders issued on the basis thereof.

4. Signature creation data: unique data such a codes or private signature keys which are used by the signatory to create an electronic signature.
5. Signature creation device: configured software or hardware which is used to implement the signature creation data.
6. Signature verification data: data such as codes or public signature keys which are used to verify an electronic signature.
7. Signature verification device: configured Software or hardware which is used to process the signature verification data.
8. Certificate: electronic confirmation in which signature verification data are linked to a specific person whose identity is certified.
9. Qualified certificate: a certificate containing the information referred to in § 5 and issued by a certification Service provider which meets the requirements of § 7,

10. Certification service provider: a natural or juristic person or some other legally capable Institution which issues certificates or provides other signature and certification services.
11. Signature and certification services: the provision of signature products and procedures, the issuing, renewal and administration of certificates, the provision of directory-, revocation-, registration-, time stamping-, computing- and consultancy- services in connection with electronic signatures.
12. Time stamp: electronically signed confirmation from a certification service provider that specific electronic data were submitted at a specific time.
13. Signature product: hardware or software or the specific components thereof used to create and verify electronic signatures or used by a certification service provider to provide signature or certification services.
14. Compromise: breach of security measures or security technique so that the level of security set up by the certification service provider no longer applies.

SECTION 2 .Relevancy in law of electronic signatures
General legal effects

SECTION 2
Relevancy in law of electronic signatures
General legal effects
§ 3. (1) Signature procedures with different levels of security and different classes of certificates can be used for legal or commercial transactions.
(2) The legal effects of an electronic signature and its use as evidence cannot therefore be excluded merely by reason of the fact that the electronic signature is only available in electronic form, is not based on a qualified certificate or on a qualified certificate issued by an accredited certification service provider or was not created using the technical components and procedures as defined in § 18.
Specific legal effects
§ 4. (1) A secure electronic signature meets the legal requirement for a hand-written signature especially the requirement for the written form as defined in § 886 of the Austrian Civil Code unless a different definitions laid down by law or by an agreement between the parties.
(2) A secure electronic signature does not have the legal effects of the written form as defined in § 886 of the Austrian Civil Code in the case of:
1. legal transactions under family and inheritance law which require the written form or a stricter formal requirement;
2. other declarations of intent or legal transactions which require official certification, judicial or notarial authentication or a notarial deed in order to be valid;
3. declarations of intent, legal transactions or petitions which require official certification, judicial or notarial authentication or a notarial deed in order to be entered in the land register, companies register or other official register or
4. declarations of guarantee (§ 1346 para. 2 of the Austrian Civil Code).
(3) The provisions of § 294 of the Code of Civil Procedure governing the presumption of authenticity of the content of a signed private deed shall apply to electronic documents bearing a secure electronic

signature.
(4) The legal effects of paragraphs 1 and 3 shall not apply if it is proven that the security requirements of the present federal law and the orders issued on the basis thereof have not been complied with or the precautions taken in order to comply with the said security requirements have been compromised.

-القانون البلجيكي
إذا انتقلنا إلي القانون البجيكيMINISTERE DES AFFAIRES ECONOMIQUES
[2001/11298] F. 2001 — 2699 9 JUILLET 2001. —Loi fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification .ALBERT II, Roi des Belges,
نجد أنه ينص علي أحكام ممثالة تقترب من القانون الفديرالي النمساوي في شأن تقرير حجية التوقيع الإلكتروني وذلك علي النحو التالي:
Définitions
Art. 2. La présente loi transpose les dispositions de la directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques.
Pour l'application de la présente loi et de ses arrêtés d'exécution, on entend par :
يلاحظ أن التشريع البلجيكي يميز بين في تعريف للتوقيع الإلكتروني بين تعريف عام لهذا التوقيع ، و التعريف بالتوقيع المتطور.
ويذهب إلي بيان المقصود بالتعبيرات التي تتضافر في تحقيق منظمة تحقيق التوقيع الإلكتروني والثقة في التعامل الإلكتروني . وبين الماة (3) منه ما يتضمنه هذا القانون من أحكام أولها : تلك التي تضع الإطار القانوني للتوقيع الإلكتروني وتحدد النظام القانوني الذي يحكم العمليات التي تتم من جانب مقدمي خدمة شهادات التصديق والقواعد التي علي تلك الجهات احترامها وكذلك الحائزين عليها دون الإخلال بالأحكام القانونية المتعلقة بالنيابة القانونية عن الأشخاص المعنوية .كما يقيم نظام للتفويض إرادي .

1° « signature électronique » : une donnée sous forme électronique jointe ou liée logiquement à d'autres données électroniques et servant de méthode d'authentification;
التوقيع الإلكتروني هو معطاه تحت شكل الكتروني متصلة أو مرتبطة منطقيا بمعطيات الإلكترونية أخري تستخد م كطريقة للتصديق. ا

2° « signature électronique avancée » : une donnée électronique, jointe ou liée logiquement à d'autres données électroniques, servant de méthode d'authentification et satisfaisant aux exigences suivantes :
a) être liée uniquement au signataire;
b) permettre l'identification du signataire;
c) être créée par des moyens que le signataire puisse garder sous son contrôle exclusif;
d) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectée;
3° « certificat » : une attestation électronique qui lie des données afférentes à la vérification de signature à une personne physique ou morale et confirme l'identité de cette personne;
4° « certificat qualifié » : un certificat qui satisfait aux exigences visées à l'annexe I de la présente loi et qui est fourni par un prestataire de service de certification satisfaisant aux exigences visées à l'annexe II de la présente loi;
5° « titulaire de certificat » : une personne physique ou morale à laquelle un prestataire de service de certification a délivré un certificat;
6° « données afférentes à la création de signature » : des données uniques, telles que des codes ou des clés cryptographiques privées, que le signataire utilise pour créer une signature électronique avancée;
7° « dispositif sécurisé de création de signature » : un dispositif logiciel ou matériel configuré pour mettre en application les données afférentes à la création de signature qui satisfait aux exigences de l'annexe III de la présente loi;
8° « données afférentes à la vérification de signature » : des données, telles que des codes ou des clés cryptographiques publiques, qui sont utilisées pour vérifier une signature électronique avancée;
9° « dispositif de vérification de signature » : un dispositif logiciel ou matériel configuré pour mettre en application les données afférentes à la vérification de signature;
10° « prestataire de service de certification » : toute personne physique ou morale qui délivre et gère des certificats ou fournit d'autres services liés aux signatures électroniques;

11° « produit de signature électronique » : tout produit matériel ou logiciel, ou élément spécifique de ce produit, destiné à être utilisé par un prestataire de service de certification pour la fourniture de services de signature électronique ou pour la création ou la vérification de

signatures électroniques;
12° « Administration » : l'administration du ministère des Affaires économiques qui est chargée des tâches relatives à l'accréditation et au contrôle des prestataires de service de certification délivrant des certificats qualifiés et établis en Belgique;
13° « entité » : organisme qui démontre sa compétence sur base d'un certificat délivré par le système belge d'accréditation conformément à la loi du 20 juillet 1990 concernant l'accréditation des organismes de certification et de contrôle, ainsi que des laboratoires d'essais, ou par un organisme équivalent établi dans l'Espace économique européen.
Section 2. — Champ d'application
Art. 3. La présente loi fixe certaines règles relatives au cadre juridique pour les signatures electroniques et définit le régime juridique applicable aux opérations effectuées par les prestataires de service de certification ainsi que les règles à respecter par ces derniers et les titulaires de certificats sans préjudice des dispositions légales concernant les règles de représentations des personnes morales. La présente loi instaure également un régime d'accréditation volontaire.
CHAPITRE III. — Principes généraux
Art. 4. § 1e . A défaut de dispositions légales contraires, nul ne peut être contraint de poser un acte juridique par voie électronique.
§ 2. Nul prestataire de service de certification ne peut être contraint de demander une autorisation préalable pour exercer ses activités. Néanmoins, les prestataires de service de certification délivrant des certificats qualifiés établis en Belgique doivent communiquer les informations suivantes à l'Administration, soit dans le mois suivant la publication de la présente loi, soit avant le début de leurs activités :— leur nom;— l'adresse géographique où ils sont établis;— les coordonnées permettant de les contacter rapidement, y compris leur adresse de courrier électronique; — le cas échéant, leur titre professionnel et leurs références et leurs numéros d'identification (registre de commerce, T.V.A.); — la preuve qu'une assurance a été souscrite en vue de couvrir leurs obligations visées à l'article 14. L'Administration leur délivre un récépissé dans les cinq jours ouvrables suivant la réception de leur communication.
§ 3. Le Roi peut, par arrêté délibéré en Conseil des Ministres, soumettre l'usage des signatures électroniques dans le secteur public à des exigences supplémentaires éventuelles. Ces exigences doivent être objectives, transparentes, proportionnées et non discriminatoires et ne s'appliquer qu'aux caractéristiques spécifiques de l'application concernée.
Ces exigences ne peuvent pas constituer un obstacle aux services transfrontaliers pour les citoyens.
§ 4. Sans préjudice des articles 1323 et suivants du Code civil, une signature électronique avancée réalisée sur la base d'un certificat qualifié et conçue au moyen d'un dispositif sécurisé de création de signature électronique, est assimilée à une signature manuscrite, qu'elle soit réalisée par une personne physique ou morale.
§ 5. Une signature électronique ne peut être privée de son efficacité juridique et ne peut être refusée comme preuve en justice au seul motif :
— que la signature se présente sous forme électronique, ou
— qu'elle ne repose pas sur un certificat qualifié, ou
— qu'elle ne repose pas sur un certificat qualifié délivré par un prestataire accrédité de service de certification, ou qu'elle n'est pas créée par un dispositif sécurisé de création de signature
— Art. 5. § 1er . Sans préjudice de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, un prestataire de service de certification qui délivre des certificats à l'intention du public ne peut recueillir des données personnelles que directement auprès de la personne concernée ou avec le consentement explicite de celle-ci et uniquement dans la mesure où cela est nécessaire à la délivrance et à la conservation du certificat. Les données ne peuvent être recueillies ni traitées à d'autres fins sans le consentement explicite de la personne intéressée.
— § 2. Lorsque le titulaire du certificat utilise un pseudonyme et lorsque les nécessités de l'instruction l'exigent, le prestataire de service de certification ayant délivré le certificat est tenu de communiquer toute donnée relative à l'identité du titulaire dans les circonstances et selon les conditions prévues par les articles 90ter à 90decies du Code d'instruction criminelle.

-قانون التوقيع الإلكتروني في الصين :
-وإذا نظرنا إلي تشريع الصادر من بتاريخ 28 أغسطس عام 2004 تحت رقمdecree No.18
والمكون من خمس أبواب تتضمن خمسة وثلاثين مادة ، والصادر بقصد تنظيم التوقيعات الإلكترونية وإقامة صحتها وأثرها القانوني وحماية الحقوق والمصالح المشروعة للأطراف . تشير المادة الاثنية من الباب الأول منه إلي أنه كل إشارة إلي التوقيع الإلكتروني في هذا القانون تكون بمعني البيانات الإلكترونية الواردة أو المرتبطة ببيانات رسالة ومستخدمة لتحقق من الموقع والتي تدل علي موافقته علي محتويات هذه الرسالة . وقد عني الباب الأول منه بالأحكام العامة والتي تتضمن بيان الغرض من هذا القانون ونطاق تطبيقه وبيان ارتباط الإشارة إلي التوقيع الإلكتروني بالبيانات الواردة في رسائل البيانات أو المرتبطة بها منطقيا بقصد التعرف علي الموقع والدلالة علي موافقته علي محتويات الراسلة .ويتناول في الباب الثاني منه بيانات الرسالة data messages ، وفي الباب الثالث يتناول التوقيع الإلكتروني والشهادات بحيث يضع تنظيما للجهات المتولية اصدارها وما يصدر عنها في المواد من 16 حتي 26 ، ويعني الباب الرابع بالمسئولية القانونية للموقع وكذلك مصدر الشهادة بصفته طرف ثالث ، وأخيرا الباب الخامس يضع أحكام تكميلية . ويلاحظ أن المادة 24 من هذا القانون تضع التزاما علي مقدم خدمة الشهادات بالإحتفاظ بالمعلومات الواردة بالراسئل الصادر عنها الشهادات لمدة خمس سنوات تالية لميعاد انتهاء صلاحية شهادة التوقيع الإلكتروني .
تنص المادة 4 من هذا القانون علي أن :" رسائل البيانات ذات المحتوي الممكن عرضه في شكل ملموس ويمكن استعادته وقراءته وإستخدامه في أي وقت تتنفق مع القوانين واللوائح الخاص بالموضوعات المتخذه شكل الكتابة باليد . وتنص المادة (5) من ذات التشريع علي أن رسالة البيانات تعتبر موفية لمتطلبات القوانين واللوائح الخاصة بالمستنتد الأصلي إ ذا -1 ": كان محتواها ممكن فعلا عرضه ويمكن استرجاعه أو الرجوع إليها واستخدامها في أي وقت و2- وكان من الممكن الإعتماد عليها في المحافظة علي وحدة واكتمال محتوياتها دون تعديل من وقت الإنتهاء منها . ومع ذلك إضافة الإعتماد علي بيانات الرسالة أو التعديلات في هيئتها الناتجة خلال تبادلها ، حفظها أو عرضها لا تؤثر علي اكتمال هذه الراسلة .

2- It can reliably maintain the integrity of its contents without modification from the time of its finalization. However, the addition of an endorsement on daqta message ,or chages in the format of a data message arosing during data exchange , storage ,or display , shall not affect the integrity of such message ."

وتنص المادة 7 من ذات القانون علي أن :" استخدام رسالة البيانات كدليل إثبات لايرفض لمجرد الإستناد علي أن إشائها أو ارسالها ، استلامها أو تخزينها في شكل الكتروني أو بصري ، ممغنط أو أي شكل آخر . لذا تنص المادة 8 من ذات القانون علي :" أنه عند يحث مصداقية رسالة البيانات كدليل اثبات ، العوامل التالية يتعين أخذها في الإعتبار : 1- مدي الإعتماد علي طريقة انشاء وتخزين و ارسال الراسلة .2- مدي الإعتماد علي طريقة.طريقة المحافظة علي قحدة واكتمال محتواها.3 -مدي الإعتماد علي طريقة طريقة التحقق من الراسل .4- والعوامل الأخري التصلة.
وتعد الرساة مرسلة من الراسل ، وفقا للمادة (9) منذات القانون إذا -1 -الراسل صرح بإرسالها 2- كانت أرسل أتوماتكيا من نظام معلوماته و3- المتلقي تحقق من رسالة البيانات مستخدما الطريقة المتفق عليها من الراسل والتي تؤدي إلي تأكيد الإرسال . وحيث يتفق الأطارف علي خلاف ذلك بالنسبة للإمور السابق ذكرها في البراجراف الأول هذا الإتفاق هو الذي يطبق".
هذا نجد أن المادة 14 منه تنص علي :" أن التوقيع الإلكتروني المعول عليه يجب أن يكون له ذات الصحة والأثر القانوني كالتوقيع بخط اليد المكتوب أو الختم الوضوع.
هذا وتنص المادة 13 من ذات القانون والسابقة علي هذه المادة علي أن :" يكون التوقيع الإلكتروني معولا عليه إذا : 1- أن يكون عند وقت إشائه البايات المتعلقة بالتوقيع في مكلية الموقع الإلكتروني .2- عند وقت انشاء التوقيع ، تكون بيانات التوقيع الإلكتروني محكومة فقط من جانب بالموقع الإلكرتروني .3- أي تغيير في التوقيع الإلكتروني بعد التوقيع يمكن ملاحظةه .4- أي تغيير في مضمون وشكل بيانات الرسالة بعد التوقيع يمكن ملاحظته . زالأطراف يمكن لهم استخدام التوقيعات الإلكترونية التي تتفق مع شروط المسئولية المتفق عليها فثيما بينهم .
ويلاحظ أن المادة الثالثة منه الواردة في الباب الأول من ذها القانون تنص علي أطراف العقد أوالمستند أو المحرر المستخدم في القانون المدني قد يتفقوا علي استخدام أو علي لألا يستخدموا التوقيعات الإلكترونية ورسائل البيانات الإلكترونية . وإذا اتفق الطرفان علي استخدام التوقيع االإلكتروني فإنها لا ينكري الصحة القانونية لهذه المستندات تأسيسا علي مجرد أن هذه المستتندات إتخذت شكل أو لأن التوقيع الإلكتروني استخدم . وهذا البراجراف ينطبق علي المستندات المتعلقة ب 1- العلاقات الشخصية مثل الزواج والتبني والتوارث .2- تحويل الحقوق والمصالح في المكلية العقارية مثل الأرض والمباني .3- 3- ايقاف الإمداد بالخدمات العامة مثل المياة والحرارة و الغاز والكهرباء .4- الظروف الأخري المحددة في القوانين واللوائح التي لا يتناسب معها المستندات الإلكترونية .

-قانون التوقيع الإلكتروني في سنجابور :
صدر تشريع المعملات الإلكترونية تحت رقم 25 عام 1998 لتأمين واستخدام التعاملات الإلكترونية والموضوعات المتربطة بها ولأن يجري التعديلات في تفسير الباب الأول من القانون الصادر عام 1997 وتشريع الإثبات الباب 97 المراجع عام 1997 .ويهدف هذا القانون إلي الإعتراف القانوني بالتوقيعات الإلكترونية والرقمية وعمل إطار قانوني لإقامة بنية المفتاح العام وإعطاء دعم قانوني للسجلات والملفات والمستندات المتخذة شكلا الإلكترونيا .وكذلك تمكين التنظيمات والمؤسسات وفطاعات الحكومة من قبول التطلبقات الإلكترونية وفي المقابل السماح لها بأن تصدر أذون وتراخيص الإلكترونية.ومن حيث أن الشبكات الوسيطة تلعب دورا هاما في إقامة البنية الأساسية فإن هذا التشريع يهدف إيضاح مسئولية مقدمي خدمات تلك الشبكات التي تقوم كطرف ثالث للتصديق علي الراسئل الإلكترونية . وفي المحصلة الإخيرة يهدف هذا التشريع لتسهيل التعاملات في التجارة الإلكترونية . وذلك علي الأخص بتسهيل الإتصال الإلكتروني وتقليل قدر المستطاع من أعمال التزوير وزيادة ثقة الجمهور في التعامل الإلكتروني.
تنص المادة 6 من هذا القانون علي أنه :" لاتلافي أي شك وفإنه من المعلن أن المعلومات يجب ألا ينكر عنها ا لأثر القانوني ، الصحة أو الإلزمام لمجرد التأسيس علي أنها متخذه شكل سجل الإلكتروني . وتنص المادة 7 التالية علي أنه:" حيثما تتطلب قاعدة من القانون

أن تكون المعلومات مكتوبة باليد أو تقدم في صورة مكتوبة أو تنص هلي بعض النتائج عند تخلفها ، فإن السجل الإلكتروني يفي بمتطلبات هذه القاعدة إذا كانت المعلومات الواردة به قابل للتوصل إليها يحث يمكن استعمالها في الرجوع إليها فيما بعد.
تنص المادة 8 منه علي أنه :"1- حيث تتطلب قاعدة من القانون توقيعا أو تشترط نتائج معينة عن عدم توقيع المستند التوقيع الإلكتروني يفي هذه القاعدة . 2 -والتوقيع الإلكتروني يمكن إثباته بأي طريقة وبما فيها بيان وجود إجراءات ضرورية للطرف المتعاقد ، لكي يسير في التعامل ،أن ينتفذ رمز أو اجراء آمن من ل التحقق من أن المستند لهذا الموقع ." بموجب هذا النص تتقرر الحجية القانونية للتوقيع الإلكتروني.
هذا وتنص المادة (4) منه علي الجزئين 2 و4 من هذا القانون لا يطبقا علي أي قاعدة قانونية تتطلب الكتابة أو التوقيع باليد وذلك في الموضوعات التالية : 1-عمل أو تنفيذ وصية .2- أ د وا ت قابلة للتفاوض.3-إقامة ،أداء أو الزام الخروج ،اعلان ، عن وصية ، 3- أي عقد لبيع أو أحكام متعلقة بالمكلية العقارية ، أو أي مصلحة في مثل هذه المكلية .4- نقل ملكية عقارية أو احالة أي مصلحة متعلقة بهذه الملكية .5- المستندات الألقاب . 2- ويجوز للوزير بموجب أمر منه تعديل الأحكام الواردة في البد 1 بالإضافة أو الحذف أو التعديل في أي تصنيف للتعاملات أو الموضوعات . 0 الجزء 2 متعلق بالسجلات والتوقيعات الإلكترونية الجزء الرابع متعلق بالعقود الإلكترونية 9 حيث تنص المادة 11 الواردة به علي أن":

PART IV :ELECTRONIC CONTRACTS

Formation and validity

11. —(1) For the avoidance of doubt, it is declared that in the context of the formation of contracts, unless otherwise agreed by the parties, an offer and the acceptance of an offer may he expressed by means of electronic records.

(2) Where an electronic record is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that an electronic record was used for that purpose.

Effectiveness between parties

12. As between the originator and the addressee of an electronic record, a declaration of intent or -- other statement shall not be denied legal effect, validity or enforceability solely on the ground that it is in the form of an electronic record.

Attribution

13. —(1) An electronic record is that of the originator if it was sent by the originator himself.

(2) As between the originator and the addressee, an electronic record is deemed to be that of the originator if it was sent

(a) by a person who had the authority to act on behalf of the originator in respect of that electronic record; or

(b) by an information system programmed by or on behalf of the originator to operate automatically

(3) As between the originator and the addressee, an addressee is entitled to regard an electronic record as being that of the originator and to act on that assumption if:

(a) in order to ascertain whether the electronic record was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or

(b) the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify electronic records as its own.

(4) Subsection (3) shall not apply

(a) from the time when the addressee has both received notice from the originator that the electronic record is not that of the originator, and had reasonable time to act accordingly;

(b) in a case within subsection (3)(b), at any time when the addressee knew or ought to have known, had it exercised reasonable care or used any agreed procedure, that the electronic record was not that of the originator; or

(c) ifl in all the circumstances of the case, it is unconscionable for the addressee to regard the electronic record as that of the originator or to act on that assumption.

(5) Where an electronic record is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee, the addressee is entitled to regard the electronic record received as being what the originator intended to send, and to act on that assumption.

(6) The addressee is not so entitled when the addressee knew or should have known, had the addressee exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the electronic record as received.

(7) The addressee is entitled to regard each electronic record received as a separate electronic record and to act on that assumption, except to the extent that the addressee duplicates another electronic record and the addressee knew or should have known, had the addressee exercised reasonable care or used any agreed procedure, that the electronic record was a duplicate.

(8) Nothing in this section shall affect the law of agency or the law on the formation of contracts.

Commentary.

PART V : SECURE ELECTRONIC RECORDS AND SIGNATUIUrS

Secure electronic record

16. —(1) If a prescribed security procedure or a commercially reasonable security procedure agreed to by the parties involved has been properly applied to an electronic record to verify that the electronic record has not been altered since a specified point in time, such record shall be treated as a secure electronic record from such specified point in time to the time of verification.

(2) For the purposes of this section and section 17, whether a security procedure is commercially reasonable shall be determined having regard to the purposes of the procedure and the commercial circumstances at the time the procedure was used, including —

(a) the nature of the transaction;

(b) the sophistication of the parties;

(c) the volume of similar transactions engaged in by either or all parties;

(d) the availability of alternatives offered to but rejected by any party;

(e) the cost of alternative procedures; and

(f) the procedures in general use for similar types of transactions.

Secure electronic signature

17. It through the application of a prescribed security procedure or a commercially reasonable security procedure agreed to by the parties involved, it can be verified that an electronic signature was, at the time it was made

(a) unique to the person using it;

(b) capable of identifying such person;

(c) created in a manner or using a means under the sole control of the person using it; and

(d) linked to the electronic record to which it relates in a manner such that if the record was changed the electronic signature would be invalidated.

Presumptions relating to secure electronic records and signatures

18. —(1) In any proceedings involving a secure electronic record. it shall be presumed, unless evidence to the contrary is adduced, that the secure electronic record has not been altered since the specific point in time to which the secure status relates.

(2) In any proceedings involving a secure electronic signature, it shall be presumed, unless evidence to the contrary is adduced, that

(a) the secure electronic signature is the signature of the person to whom it correlates; and

(b) the secure electronic signature was affixed by that person with the intention of signing or approving the electronic record.

(3) In the absence of a secure electronic record or a secure electronic signature, nothing in this Pan shall create any presumption relating to the authenticity and integrity of the electronic record or an electronic signature.

(4) For the purposes of this section

“secure electronic record” means an electronic record treated as a secure electronic record by virtue of section 16 or 19;

“secure electronic signature” means an electronic signature treated as a secure electronic signature byvirtue of section 17 or2O.

an electronic record signed with a secure electronic signature can presume that based on the secure electronic signature, the sender is the originator of the electronic record, and he cannot easily repudiate his signature on the electronic record.

In the absence of the use of such security procedures, no such presumptions will arise for electronic records and electronic signatures.

PART VI :EFFECT OF DIGITAL SIGNATURES

Secure electronic record with digital signature

19. The portion of an electronic record that is signed with a digital signature shall be treated as a secure electronic record if the digital signature is a secure electronic signature by virtue of section 20.

Secure digital signature

20. When any portion of an electronic record is signed with a digital signature, the digital signature shall be treated as a secure electronic signature with respect to such portion of the record, if—

(a) the digital signature was created during the operational period of a valid certificate and is verified by reference to the public key listed in such certificate; and

(b) the certificate is considered trustworthy, in that it is an accurate binding of a public key to a person s identity because —

(i) the certificate was issued by a licensed certification authority operating in compliance with the regulations made under section 42

(ii) the certificate was issued by a certification authority outside Singapore recognised for this purpose by the Controller pursuant to regulations made under section 43;

(iii) the certificate was issued by a department or ministry of the Government, an organ of State or a statutory corporation approved by the Minister to act as a certification authority on such conditions as he may by regulations impose or specify; or (iv) the parties have expressly agreed between themselves (sender and recipient) to use digital signatures as a security procedure, and the digital signature was properly verified by reference to the sender's public key.

التشريع الماليزي Digital signature bill 1997

تقترب صياغة هذا التشريع في المادة 62 منه من الصياغة التي أخذ بها تشريع سنجابور حيث تنص هذه المادة علي ما يلي : حيث ينص علي أنه حيثما توجد قاعدة من القانون تتطلب توقيع أو اشترط نتائج معينة تترتب عن تخلفه فإن هذه القاعدة تستوفي بالتوقيع الرقمي حيث تتوافر الشروط التالية :

.

PART V: EFFECT OF DIGITAL SIGNATURE

62. Satisfaction of signature requirements

(I) Where a rule of law requires a signature or provides for certain consequences in the absence of a signature, that rule shall be satisfied by a digital signature where-

(a) that digital signature is verified by reference to the public key listed in a valid certificate issued by a licensed certification authority;

(b) that digital signature was affixed by the signer with the intention of signing the message; and

(c) the recipient has no knowledge or notice that the signer¬

(i) has breached a duty as a subscriber; or

(ii) does not rightfully hold the private key used to affix the digital signature.

(2) Notwithstanding any written law to the contrary-

(a) a document signed with a digital signature in accordance with this Act shall be as legally binding as a document signed with a handwritten signature, an affixed thumb-print or any other mark; and

(b) a digital signature created in accordance with this Act shall be deemed to be a legally binding signature.

(3) Nothing in this Act shall preclude any symbol from being valid as a signature under any other applicable law.

63. Unreliable digital signatures

(I) Unless otherwise provided by law or contract, the recipient of a digital signature assumes the risk that a digital signature is forged, if reliance on the digital signature is not reasonable under the circumstances.

(2) Where the recipient determines not to rely on a digital signature under this section, the recipient shall promptly noti1~ the signer of its determination not to rely on a digital signature and the grounds for that determination.

64 Digitally signed document deemed to be written document
(1) A message shall be as valid , enforceable and effective as if it had been written on paper if :
a) it bears in its entirety a digital signature ; and b) that digital signature is verified bu public key listed in a certificate which :
(i) was issued be a licensed certification authority ; and
(ii) was valid at the time the digital signature was created.

(2) Nothing in this Act shall preclude any message, document or record from being considered written or in writing under any other applicable law.

65. Digitally signed document deemed to be original document.

A copy of a digitally signed message shall be as valid, enforceable and effective as the original of the message unless it is evident that the signer designated an instance of the digitally signed message to be a unique original, in which case only that instance constitutes the valid, enforceable and effective message.

66. Authentication of digital signatures

A certificate issued by a licensed certification authority shall be an acknowledgement of a digital signature verified by reference to the public key listed in the certificate, regardless of whether words of an express acknowledgement appear with the digital signature and regardless of whether the signer physically appeared before the licensed certification authority when the digital signature was created, if that digital signature is-
(a) verifiable by that certificate; and (b) affixed when that certificate was valid.

67. Presumptions in adjudicating disputes

In adjudicating a dispute involving a digital signature, a court shall presume-
(a) that a certificate digitally signed by a licensed certification authority and¬
(i) published in a recognised repository; or
(ii) made available by the issuing licensed certification authority or by the subscriber listed in the certificate, is issued by the licensed certification authority which digitally signed it and is accepted by the subscriber listed in it;

(b) that the information listed in a valid certificate and confirmed by a licensed certification authority issuing the certificate is accurate;
(c) where a digital signature is verified by the public key listed in a valid certificate issued by a licensed certification authority¬
(i) that digital signature is the digital signature of the subscriber listed in that certificate;
(ii) that digital signature was affixed by that subscriber with the intention of signing the message; and
(iii) the recipient of that digital signature has no knowledge or notice that the signer-

(A) has breached a duty as a subscriber; or
(B) does not rightfully hold the private key used to affix the digital signature; and

(d) that a digital signature was created before it was time-stamped by a recognised date/time stamp service utilising a trustworthy system.

-القانون الفديرالي الهندي للتجارة الإلكترونية الصادر في 10/19 1998 /

متطلبات تحقق المنظومة

من العرض السابق يبين أن التوقيع الإلكتروني والمحرر الإلكتروني يمر بمرحلتين : الأولي : تتعلق بإنشاء التوقيع وتوفير التأمين اللازم لذلك المرحلة الثانية: مرحلة التحقق من صدور التوقيع والمحرر من الموقع الراسل وذلك عند تلقي المرسل إلأيه الملعومات أو المحرر الإلكتروني.
غير أنه حتي تتحقق الحجية القانونية للتوقيع والمحرر الإلكتروني ويكون له ذات الحجية التي للتوقيع المكتوب بخط اليد والمحرر الورقي المحرر باليد يتعين توافر عدة شروط سواء أكان التشريع يأخذ بالتوقيع الإلكتروني المتطور أو الموصوف أو التوقيع الإلكتروني الرقمي .وأيا كان أيا منها أو كانت التقنية التكنولوجية المستخدمة في توفير التأمين للرسالة والتوقيع الإلكرتوني . هذا ومرحلة التحقق قد تطلب اشتراك طرف ثالث عن الراسل والمرسل إليه يضطلع بمهمة اصدار الشهادات المصدقة التي تفيد صودر التوقيعالإلكتروني من الموقع وأته هو الموقع وأن الراسلة كاملة متكاملة صادرة عنه ومنسوبة إليه ومن ثم يمكن بهذا التعرف عن هوية الموقع ونسبة الرالية والتوقيع له.
وحتي يمكن تبسيط عرض القواعد والإحكام المؤدية لماسبق والمحقق للغاية المرجوة يمكن تقسيمها إلي المجموعات التالية:
-1الأحكام المتعلقة بالموقع وتأمين أداته في إرسال الرسالة والتوقيع الإلكتروني الموقع به .2- أحكام متعلقة بإنشاء التوقيع وتأمين الرسالة و يتصل ذلك تأمين خدمات الإتصالات .3- تتعلق بالمرسل إليه وما عليه ومتي يعول علي التوقيع الإلكتروني ومتي لا يعول عليه . 4- أحكام تتعلق بالتحقق من نسبة التوقيع والمحرر للموقع، والتصديق علي ذلك من طرف ثالث ومن ثم تتعلق بمقدمي خدمات إصدار تلك الشهادات (الجهات التي تعطي الترخيص بمزاولة هذا النشاط ، الشروط الواجب توافرها في الجهات المرخص لها بإصدار الشهادات ومؤهلاتها ومؤهلات العاملين بها ، الشهات التي تصدر عنها – أنواعها والبيانات التي ترد بها وشكلها ،مكنة الغائها ، مدي حجيتها ، إيقاف الشهادات – علاقة الجهات المذكورة بالصادر لصالحهم الشهادات والعقود التي تبرم بينهما وما يجب أن تتضمنه من بيانات والمسئولية المترتبة علي تلك الجهات وعلي من صدرت لهم تلك الشهادات ، علاقة تلك الجهات بالجهات الأجنبية التي تمارس ذات النشاط . واجبات تلك الجهات علي التحفظ وتأمين المعلومات التي لديها .وتأمين أجهزتها والعاملين لديها وعدم افشاء الأسرار والمعلومات والمفاتيح المستخدمة . 5- أحكام تتعلق بالإحتفاظ وتخزين البيانات ومدد الاختفاظ بها واسترجاعها والتمسك بها أمام الجهات المعنية .6- أحكام تتعلق بالجهات الرقابية التي ترخص لمقدمي خدمات الشهادات -(تحديدها مؤهلاتها ووظائفها وبيان أحوال رفض اعطاء الترخيص وآثاره وانتهاؤه وإلغائه وإعادة الترخيص وتجديده ومكنات الرقابة والتدخل لكشف المعلومات إذا لزم الأمر وكانت هناك مقتض قانوني) 7- أحكام تتعلق بالتقنيات التكنولوجية التي يستخدمها مقدمي خدمة شهادات التصديق و الجهات الرقابية. هنا يثور نظم التشفير وكيفية عمل نظام المفتاح الخاص والمفتاح العام والدالة أو الدوا ل الحسابية Algorithm التي تستخدم في التشفير. encryptosystem asymmetric or symmetric
وفي هذا المقام نكتفي بالإشار إلي أحكام القرار الوزاري رقم 109 لسنة 2005 قرار وزير المالية رقم 1742 لسنة 2004 .علي النحو التالي:
وزارة الاتصالات وتكنولوجيا المعلومات
قرار رقم 109 لسنة 2005
بتاريخ 2005/5/15
بإصدار اللائحة التنفيذية لقانون التوقثع الإلكترونى
وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات

وزير الاتصالات وتكنولوجيا المعلومات
بعد الإطلاع على ادستور:
وعلى القانون المدنى:
وعلى قانون التجارة:
وعلى القانون رقم 13 لسنة 1968 بشأن المرافعات المدنية والتجارية.
وعلى القانون رقم 25 لسنة 1968 بشأن الإثبات فى المواد المدنية والتجارية.
وعلى القانون رقم 82 لسنة 2002 بشأن حسابة حقوق الملكية الفكرية.
وعلى القانون رقم 10 لسنة 2003 بشان تنظيم الاتصالات.
وعلى قانون رقم 15 لسنة 2004 بتنظيم التوقيع الإلكترونى وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات.
وعلى قرار رئيس الجمهورية رقم 201 لسنة 2004 بتشكيل الوزارة:
قـــــرار:
)المادة الأولى(
يعمل بأحكام اللائحة التنفيذية للقانون رقم 15 لسنة 2004 بتنظيم التوقيع الإلكترونى وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات

المرفقة.
)المادة الثانية(
ينشر هذا القرار فى الوقائع المصرية. ويعمل به من اليوم التالى لتاريخ النشر.

وزير الاتصالات وتكنولوجيا المعلومات
دكتور / طارق كامل

المـادة 1
فى تطبيق أحكام هذه اللائحة يقصد بالمصطلحات الآتية المعانى المبينة قرين كل منها:
-1التوقيع 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.
-2الكتابة الإلكترونية:
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.
-3المحرر الإلكترونى :
رسالة بيانات تتضمن معلومات تنشأ ، أو تدمج ، أو تخزن ، أو ترسل ، أو تستقبل ، كليا أو جزئيا ، بوسيلة إلكترونية أو رقمية ، أو ضوئية ، أو بأية وسيلة أخرى مشابهة.
-4الوسيط الإلكترونى:
أداة أو أدوات أو أنظمة إنشاء التوقيع الإلكترونى.
-5الموقع:
الشخص الحائز على بيانات إنشاء التوقيع ويوقع عن نفسه أو عمن ينيبه أو يمثله قانونا.
-6جهات التصديق الإلكترونى:
الجهات المرخص لها بإصدار شهادة التصديق الإلكترونى وتقديم خدمات تتعلق بالتوقيع الإلكترونى.
-7شهادة التصديق الإلكترونى:
الشهادة التى تصدر من الجهة المرخص لها بالتصديق وتثبت الارتباط بين الموقع وبيانات إنشاء التوقيع.
-8بيانات إنشاء التوقيع الإلكترونى:
عناصر متفردة خاصة بالموقع وتميزه عن غيره ، ومنها على الأخص مفاتيح الشفرة الخاصة به ، والتى تستخدم فى إنشاء التوقيع الإلكترونى.
-9التشفير:
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.
-10تقنية 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 يحتفظ به الشخص ويحفظه على درجة عالية من السرية.
-11المفتاح 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.

-12المفتاح 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.
-13المفتاح الشفرى الجذرى:
أداة إلكترونية تنشأ بواسطة عملية حسابية خاصة وتستخدمها جهات التصديق الإلكترونى لإنشاء شهادات التصديق الإلكترونى وبيانات إنشاء التوقيع الإلكترونى.
-14الدعامة الإلكترونية:
وسيط مادى لحفظ وتداول الكتابة الإلكترونية ، ومنها الأقراص المدمجة أو الأقراص الضوئية أو الأقراص الممغنطة أو الذاكرة الإلكترونية أو أى وسيط آخر مماثل.
-15البطاقة 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.
-16الحاسب الآلى:
جهاز إلكترونى قادر على تخزين ومعالجة وتحليل واسترجاع البيانات والمعلومات بطريقة إلكترونية.

-17برنامج 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.
-18منظومة 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.
-19منظومة إنشاء التوقيع الإلكترونى:
مجموعة عناصر مترابطة ومتكاملة ، تحتوى على وسائط إلكترونية وبرامج حاسب آلى ويتم بواسطتها التوقيع الكترونيا على المحرر الإلكترونى وذلك باستخدام بيانات إنشاء التوقيع الإلكترونى وشهادة التصديق الإلكترونى ، كما يتم بواسطتها وضع وتثبيت المحرر الموقع إلكترونيا على دعامة إلكترونية.
-20شهادة فحص بيانات إنشاء التوقيع الإلكترونى:
شهادة تصدرها الهيئة بنتيجة الفحص والتحقق من صحة بيانات إنشاء التوقيع الإلكترونى.
-21شهادة فحص التوقيع الإلكترونى:
شهادة تصدرها الهيئة بنتيجة فحصها لصحة وسلامة التوقيع الإلكترونى.

-22شهادة 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.
-23الهيئة:
هيئة تنمية صناعة تكنولوجيا المعلومات.
-24الوزارة المختصة:
الوزارة المختصة بشئون الاتصالات وتكنولوجيا المعلومات.
– 25الوزير المختص:
الوزير المختص بشئون الاتصالات وتكنولوجيا المعلومات.
-26القانون:
قانون رقم 15 لسنة 2004 بتنظيم التوقيع الإلكترونى وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات.
المادة 2
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 ، 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 علما تاما بمضمون المحرر الإلكترونى قبل توقيعه له.
المادة3
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 وفقا للمعاييرالفنية 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 لاتقل عن 2048 حرف إلكترونى.(bit)
)ج) أن تكون أجهزة التأمين الإلكترونى (Hardware Security Modules) المستخدمة معتمدة طبقا 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 ، وفقا للمعايير الفنية والتقنية المبينة فى الفقرة (ج) 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 أيضا 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.
المادة4
لمجلس إدارة الهيئة أن يضع نظم وقواعد أخرى لمنظومة تكوين بيانات إنشاء التوقيع الإلكترونى لمواكبة التطورات التقنية والتكنولوجية.
المادة 5

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 طبقا للمادة (2) ، ومتضمنة الضوابط الفنية والتقنية والنظم والقواعد المبينة فى المادتين (3) ، (4).
وتعتبر المنظومة بعد منح الترخيص وطوال مدة نفاذ مفعولة ، مؤمنة وفعالة مالم يثبت العكس.

المادة 6

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.

المادة 7

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.
)ج) سهولة العلم بشخص الموقع ، سواء فى حالة استخدام أسمه الأصلى أم استخدامه لاسم مستعار أم أسم شهرة.
ويجوز للهيئة أن تعهد للغير بتقديم هذه الخدمة تحت إشرافها ، وفى جميع الأحوال تصدر الهيئة شهادة فحص التوقيع الإلكترونى.

المادة 8

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 متاحا 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 منشىء هذه الكتابة أو تلك المحررات ، أو لسيطرة المعنى بها.
)ب) أن يكون متاحا فنيا تحديد مصدر إنشاء الكتابة الإلكترونية أو المحررات الإلكترونية الرسمية أو العرفية ودرجة سيطرة منشئها على هذا المصدر وعلى الوسائط 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.

المادة9

يتحقق من الناحية الفنية والتقنية ، أرتباط التوقيع الإلكترونى بالموقع وحده دون غيره متى استند هذا التوقيع إلى منظومة تكوين بيانات إنشاء توقيع إلكترونى مؤمنة على النحو الوارد فى المواد (2 ، 3 ، 4) من هذه اللائحة ، وتوافرت إحدى الحالتين الآتيتين:
)أ) أن يكون هذا التوقيع مرتبطا بشهادة تصديق إلكترونى ، معتمدة ونافذة المفعول صادرة من جهة تصديق إلكترونى مرخص لها أو معتمدة.
)ب) أن يتم التحقق من صحة التوقيع الإلكترونى طبقا للمادة (7) من هذه اللائحة.

المادة10

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.

المادة 11

مع عدم الإخلال بما هو منصوص عليه فى المواد (2 ، 3 ، 4) 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.

المادة 12

يجب أن يتوافر لدى طالب الحصول على الترخيص بإصدار شهادات التصديق الإلكترونى المتطلبات التالية:
)أ) نظام تأمين للمعلومات وحماية البيانات وخصوصيتها بمستوى حماية لايقل عن المستوى المذكور فى المعايير والقواعد المشار إليها فى الفقرة (د) من الملحق الفنى والتقنى للائحة.
)ب) دليل إرشادى يتضمن ما يلى:
-1إصدار شهادات التصديق الإلكترونى.
-2إدارة المفاتيح الشفرية.
-3إدارة الأعمال الداخلية.
-4إدارة التأمين والكوارث.
وذلك وفقا للمعايير الفنية والتقنية المذكورة فى الفقرة (هـ) من الملحق الفنى والتقنى للائحة.
)ج) منظومة تكوين بيانات إنشاء التوقيع الإلكترونى مؤمنة وفقا للضوابط الفنية والتقنية المنصوص عليها فى المواد (2 ، 3 ، (4من 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 بناء على طلب من الموقع وبموجب عقد مستقل يتم إبرامه بين المرخص له والموقع ووفقا 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:
-1العبث ببيانات الشهادة أو انتهاء مدة صلاحيتها.
-2سرقة أو فقد المفتاح الشفرى الخاص أو البطاقة الذكية ، أو عند الشك فى حدوث ذلك.
-3عدم التزام الشخص المصدر له شهادة التصديق الإلكترونى ببنود العقد المبرم مع المرخص له.
ويكون نظام إيقاف الشهادات وفقا 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.

المادة 13
فى جميع الأحوال يلتزم المرخص له بعدم إبرام أى عقد مع العملاء إلا بعد اعتماد نموذج هذا العقد من الهيئة طبقا للقواعد والضوابط التى يضعها مجلس إدارة الهيئة فى هذا الشأن لضمان حقوق ذوى الشأن.
المادة 14
على طالب الترخص بإصدار شهادات التصديق الإلكترونى أن يقدم الضمانات والتأمينات التى يحددها مجلس إدارة الهيئة لتغطية أى أضرار أو أخطار تتعلق بذوى الشأن ، وذلك فى حالة إنهاء الترخيص لأى سبب ، أو لتغطية أى إخلال من جانبه لالتزاماته الواردة فى الترخيص.
المادة 15
تتبع الإجراءات الآتية للحصول على الترخيص بإصدار شهادات التصديق الإلكترونى:
)أ) التقدم بالطلب على النماذج التى تعدها الهيئة فى هذا الشأن مصحوبا بالبيانات والمستندات الدالة على توافر الشروط والأحكام المنصوص عليها فى المواد
3) ، 4 ، 12 ، (14من هذه اللائحة.
)ب) تقوم الهيئة بعد تسلمها لكافة المستندات والبيانات المطلوبة ، وفقا للبند (أ) من طالب الترخيص بفحصها والتأكد من سلامتها ، وتبت الهيئة فى طلب الحصول على الترخيص خلال مدة لا تتجاوز ستين يوما من تاريخ استيفاء طالب الترخيص لجميع ما تطلبه الهيئة منه ، مالم تخطر الهيئة طالب الترخيص بمد هذه المدة ، وفى حالة انقضاء هذه المدة دون إصدار الترخيص يعتبر الطلب مرفوضا.
)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 طبقا للإجراءات والقواعد والضمانات المنصوص عليها فى القانون وفى هذه اللائحة ، وما يقره مجلس إدارة الهيئة من قواعد فى هذا الشأن.
المادة 16
تقوم الهيئة بالتفتيش على الجهات المرخص لها للتحقق من مدى التزامها بالترخيص.
المادة17
يحدد فى الترخيص التزامات المرخص له وفقا للقانون وهذه اللائحة والقرارات الصادرة من مجلس إدارة الهيئة فى هذا الشأن.
المادة 18
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.
المادة 19
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.

المادة 20
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:
-1ما يفيد صلاحية هذه الشهادة للاستخدام فى التوقيع الإلكترونى.
-2موضوع الترخيص الصادر للمرخص له ، موضحا فيه نطاقه ورقمه وتاريخ إصداره وفترة سريانه.
-3اسم وعنوان الجهة المصدرة للشهادة ومقرها الرئيسى وكيانها القانونى والدولة التابعة لها إن وجدت.
-4اسم الموقع الأصلى أو اسمه المستعار أو اسم شهرته ، وذلك فى حالة استخدامه لأحدهما.
-5صفة الموقع.

-6المفتاح الشفرى العام لحائز الشهادة المناظر للمفتاح الشفرى الخاص به.
-7تاريخ بدء صلاحية الشهادة وتاريخ انتهائها.
-8رقم مسلسل للشهادة.
-9التوقيع الإلكترونى لجهة إصدار الشهادة.
-10عنوان الموقع الإلكترونى (Web Site) المخصص لقائمة الشهادات الموقوفة أو الملغاة.
ويجوز أن تشتمل الشهادة على أى من البيانات الآتية عند الحاجة:
-1مايفيد اختصاص الموقع والغرض الذى تستخدم فيه الشهادة
-2حد قيمة التعاملات المسموح بها بالشهادة.
-3مجالات استخدام الشهادة.

المادة 21

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.
)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 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 اتفاقا 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 لاتجاوز ستين يوما من تاريخ استيفاء الجهة الأجنبية لكل ما تطلبه الهيئة . وفى حالة انقضاء هذه المدة دون إصدار الاعتماد يعتبر الطلب مرفوضا 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 دائما ، بقرار مسبب ، الحق فى إلغاء الاعتماد أو وقفه.

المادة 22

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

المادة 23

مع عدم الإخلال بالعقوبات المنصوص عليها فى المادة (23 (من القانون ، يلتزم المرخص له بجميع أحكام الترخيص الصادر له من الهيئة ، وفى حالة مخالفة المرخص لأى منها أو توقفه عن مزاولة النشاط المرخص ، أو اندماج منشأته فى جهة أخرى ، أو تنازله عن الترخيص للغير ، دون الحصول على موافقة كتابية مسبقة من الهيئة على أى من هذه الأفعال المشار إليها ، يجوز للهيئة ، بقرار مسبب ، عندئذ إلغاء الترخيص أو وقفه لحين التدارك أو التصحيح.
ويجوز للهيئة فى حالتى الإلغاء أو الوقف أن تتخذ التدابير المناسبة فى هذا الشأن لحماية حقوق ذوى الشأن.

المادة 24

مع عدم الإخلال بأحكام القانون ، يلتزم كل من يباشر نشاط شهادات التصديق الإلكترونى قبل العمل بالقانون ، أن يوفق أوضاعه مع القانون ، بأن يتقدم بطلب خلال شهرين من تاريخ صدور هذه اللائحة ، على النموذج الذى تعده الهيئة لذلك ، مصحوبا 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 وفقا لما تقدم ، مزاولا لهذا النشاط بدون ترخيص ، ويحق للهيئة فى هذه الحالة اتخاذ ما يلزم لوقف النشاط.

وزارة المالية
قرار رقم 1742 لسنة 2004

وزير المالية
بعد الاطلاع على القانون المدنى:
وعلى قانون الإثبات فى المواد المدنية والتجارية.
وعلى قانون الهيئات العامة الصادر بالقانون رقم 61 لسنة.1963
وعلى القانون رقم 53 لسنة 1973 بشأن الموازنة العامة للدولة.
وعلى قانون نظام العاملين المدنيين بالدولة رقم 47 لسنة 1978.
وعلى القانون رقم 127 لسنة 1981 بشأن المحاسبة الحكومية.

وعلى القانون رقم 15 لسنة 2004 بشأن التوقيع الإلكترونى.

قــرار

المادة الأولى

يعتد فى جميع التعاملات والتصرفات القانونية المقررة بموجب أحكام قانون الموازنة العامة للدولة وقانون المحاسبة الحكومية بنماذج الميزانية والموازنات أو الاستمارات أو الدفاتر الحكومية المعدة بواسطة الحاسب الآلى وكذلك مخرجات الحاسب الآلى المستخدمة بالوحدات الحسابية أو الواردة من الوحدات الإدارية الميكنة آلياً والمدون بها البيانات المتطلبة بالوثائق المالية الحكومية وذلك بعد إقرارها من وزير المالية أو كانت مماثلة لتلك التي تم تصميمها من خلال برنامج الحكومة الإلكترونية بوزارة المالية للتنمية الإدارية وحازت على موافقة وزارة المالية.

المادة الثانية

تعتبر مخرجات الحاسب الآلى المعتمدة باستخدام الآليات الخاصة بالتوقيع الإلكترونى والقواعد المنظمة لاستخدامه مخرجات رسمية معتمدة اعتماداً قانونياً حسب قانون التوقيع الإلكترونى ويعتمد تداولها بصفة رسمية.

المادة الثالثة

يتعين على مديرى الوحدات الحسابية تحت إشراف المراقبين الماليين بالوزارات والهيئات ومديرى المديريات المالية بالمحافظات ومديرى عموم الحسابات بالأجهزة المستقلة والرئاسية اعتماد مخرجات الحاسب الآلى المستخدمة بالوحدات الحسابية وتجميعها وأرشفتها بما يضمن سهولة الرجوع إليها وعليهم التأكد من أن نظام الميكنة المعتمد يتضمن الضوابط الآلية التي تحول دون إجراء أى تغيير فى بيانات المخرجات أو التلاعب فيها بعد ذلك.

المادة الرابعة

ينشر هذا القرار فى الوقائع المصرية، ويعمل به من تاريخ نشره.

صدر فى5/12/2004

وزير المالية

دكتور/ يوسف بطرس غالى