التوقيع الرقمي وحجيته في الإثبات
في قانون المعاملات الاماراتي والاسباني

إعداد

د / فرحان نزال احميد المساعيد

استاذ القانون الدستوري والاداري
المشارك رئيس قسم القانون العام –
كلية القانون- جامعة ال البيت -
المملكة الاردنية الهاشمية

د/ سامر خليل شطناوي

استاذ القانون الدستوري االمساعد
محاضر متفرغ – كلية القانون-
جامعة ال البيت

المقدمة

تتميز الحكومة الإلكترونية بانها شكلا جديدا من اشكال الادارة الحديثة وليده التكنولوجيا الحديثة وتتمتع بإمكانية صنع تمازج وانخراط عبر الإنترنت. فالحكومة الإلكترونية مثل استخدام تكنولوجيا المعلومات والاتصالات في الإدارة العامة ، ويرتبط مع التغيير التنظيمي وجود مهارات جديدة للموظفين. الهدف من منها تحسين الخدمات العامة والعمليات الديمقراطية وتعزيز دعم السياسات العامة. وتمكن قانون المعاملات والتجارة الإلكترونية لإمارة دبي وصدر قانون المعاملات والتجارة الإلكترونية رقم (٢) لعام ٢٠٠٢ لإمارة دبي بهدف إحلال الوسائل التقنية الحديثة في المعاملات التجارية محل الوسائل التقليدية. وقد سبقه التوجيه الاوروبي رقم ٩٩. ١٩٩٣ بشان التوقيع الالكتروني لينظم المعاملات الالكترونية. وكذلك الجهود الدولية لذا من بين هذه الموضوعات موضوع التوقيع الرقمي الذي هو عبارة عن مجموعة من البيانات المرتبطة رسالة يضمن هوية الموقع وسلامة الرسالة. يهدف إلكترونيا لضمان هوية المواطن لجعل المعاملات الإلكترونية سلسلة وبسيطة. ولكن كل ذلك يتطلب من اجراءات للوصول إلى الخدمات التي تقدمها الحكومة الإلكترونية، اذ ينبغي أن يكون الفرد في حيازة شهادة مستخدم صادرة عن مقدم خدمات التصديق للسماح بالتوقيعات الالكترونية المتقدمة و المعترف بها من قبل الإدارة العامة. استفادت ١٢٠ جهة ومؤسسة من مشروع مطابقة البيانات في دولة الامارات العربية المتحدة من التوقيع الرقمي.

التوقيعات الرقمية تعتمد على الترميز غير المتناظر اي أننا امام مفهوم أعمق من التوقيع الالكتروني، ليس بالضرورة افتراض استخدام تكنولوجيات التشفير غير المتناظر . على الرغم من أن العديد من الكتاب يتحدث عادة عن التوقيع الإلكتروني أو التوقيع الرقمي على انهما سيان.وعلية سيقوم الباحثان ببيان ذلك في المباحث التالية:-

المبحث الاول

التوقيع الرقمي

يعتبر التوقيع الإلكتروني حديثا جدا بالمقارنة الى غيره من الموضوعات التكنولوجية، إذ تم ابتكاره على يد ديفي هيلمان[١]. فهو عبارة عن مجموعة من العمليات الحسابية التي يتم تطبيقها على وثيقة إلكترونية باستخدام شهادة رقمية ، والسماح لاستبدال التوقيع الخطي التقليدي. يتم ضمان هوية الموقع من وثيقة إلكترونية و سلامتها ، وهذا هو الذي لم يجر تغيير المحتوى منذ التوقيع عليه. وضعت لجنة الأمم المتحدة للتجارة الدولية (الاونسترال) القواعد الموحدة بشأن التوقيعات الالكترونية ، وقد ورد في القواعد الموحدة تعريف للتوقيع الالكترونى بأنه عبارة عن : بيانات في شكل الكترونى مدرجة في رسالة بيانات أو مضافة اليها أو مرتبطة بها منطقيا ، ويجوزأن تستخدم بتعيين هوية الموقع بالنسبة الى رسالة البيانات وبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات[٢]. ويعرف الاتحاد الأوروبي نوعين من التوقيع الالكترونى ووضع لكل منها تعريفا محددا هما:

---

(١) خوارزمية ديفي و هيلمان (DH) : وارزمية ديفي وهيلمان تعتبر أول خوارزمية ذات مفتاح عام وكانت ١٩٧٦م وتعتمد على خاصية نظام اللوغاريتم الصحيح في تصميم نظام للتشفير. أن صعوبة كسر هذه الخوارزمية حسب ما هو معروف الآن تعادل صعوبة حل مسالة اللوغاريتم الصحيح إلا إنها خوارزمية بطيئة لأنها تعتمد على كثير من عمليات الرفع إلى قوة ، لذلك ينصح باستعمالها لتشفير الرسائل القصيرة وخصوصا المفاتيح التي تستخدمها خوارزميات أخرى ويتم تبادلها بين الإطراف المتراسلة. انظر. د.أحمد عبد القادر صالح، المصادقة الالكترونية، اللجنة القومية للمصادقة الالكترونية، الخرطوم، ٢٠٠٩.

(٢) وثائق الاونسترال –الدورة السابعة.فيينا.لعام ٢٠٠٠. مذكرة في الامانة الجمعية العامة للأمم المتحدة.ص١٠.

١. التوقيع الالكتروني هو عبارة عن معلومات على شكل الكتروني متعلقة بمعلومات الكترونية أخرى ومرتبطة بها ارتباطا وثيقا، وتستخدم أداة للتوثيق.

٢. التوقيع الالكتروني المعزز هو عبارة عن توقيع الكتروني يشترط فيه أن يكون:

أ. مرتبطا ارتباطا فريدا من نوعه مع صاحب التوقيع .

ب. قادرا على تحديد صاحب التوقيع والتعرف عليه باستخدامه.

ج. تستخدم فيه وسائل يضمنفيها صاحبه السرية التامة.

د. مرتبطا مع المعلومات المحتواة في الرسالة حيث انه يكشف أى تغيير في المعلومات.

وقد ورد لدى المشرع الاماراتي اهتمامه وتبنيه التوقيع الالكتروني بوضع نصوص قانونية تحدد ماهيته حيث اصدر القانون الاتحادي رقم (١) لسنة ٢٠٠٦ بشأن المعاملات والتجارة الإلكترونية في المادة (١) معرفا التوقيع الالكتروني على انه: (توقيع مكون من حروف أو أرقام أو رموز أو صوت أو نظام معالجة ذي شكل الكتروني وملحق أو مرتبط منطقياً برسالة الكترونية وممهور بنية توثيق أو اعتماد تلك الرسالة).

وبين كذلك أداة التوقيع بنفس المادة موضحا اياها على انه: (جهاز أو معلومات الكترونية معدة بشكل مستقل أو بالاشتراك مع أجهزة ومعلومات الكترونية أخرى لوضع توقيع الكتروني لشخص معين، وتشمل هذه العمليات أية أنظمة أو أجهزة تنتج أو تلتقط معلومات معينة مثل رموز أو مناهج حسابية أو حروف أو أرقام أو مفاتيح خصوصية أو أرقام تعريف الشخصية أو خواص شخصية).

وللاهتمام الكبير في هذا المجال اصدرت كذلك منطقة دبي الحرة للتكنولوجيا الالكترونية والاعلام قانون رقم ١ لسنة ٢٠٠٠ بهدف تنظيم وجعل دبي مركزا للتكنولوجيا والتجارة والاعلام.

كما صدر ايضا قانون رقم ٥ لسنة ٢٠٠٢ بشأن المعاملات والتجارة الالكترونية وحدد مفهوما عاما للمعلومات الالكترونية والموقع والتوقيع ومزود الخدمات في المادة الثانية منه على ان: التوقيع الالكتروني المحمي هو التوقيع الالكتروني المستوفي لشروط المادة (١٨) من هذا القانون. بأن الموقع هو : (الشخص الطبيعي أو المعنوي الحائز لأداة توقيع الكتروني خاصة به ويقوم بالتوقيع أو يتم التوقيع بالنيابة عنه على الرسالة الالكترونية باستخدام هذه الأداة). وحدد واجبات الموقع في المادة ٢٢ اما في المادة الثامنة عرف شهادة المصادقة الالكترونية.

المطلب الاول

مفهوم التوقيع الرقمي

التوقيع الرقمي نوع من أنواع التوقيع الإلكتروني . ايضا التوقيع الرقمي يعتبر فئة جزئية من مجال التوقيع الإلكتروني. وكان في البداية قبولا للتعامل الالكتروني[١]،

(١) المادة ٦ التي اخذت بمبدأ القبول الالكتروني .1ليس في هذا القانون مايتطلب من شخص أن يستخدم أو يقبل معلومات بشكل إلكتروني ، إلا انه يجوز استنتاج موافقة الشخص من سلوكه الإيجابي. .2يجوز أن يتفق الأطراف الذين لهم علاقة بإنشاء أو إرسال أو استلام أو تخزين أو معالجة أية سجلات إلكترونية ، على التعاقد بصورة مغايرة لأي من الأحكام الواردة في الفصل الثاني حتى الفصل الرابع من هذا القانون .3. استثناءً من أحكام الفقرة (١) السابقة ، يجب أن يكون صريحاً قبول الحكومة بالتعامل الإلكتروني في المعاملات التي تكون طرفاً فيها.

وان شهادة المستخدم هي وثيقة الرقمية التي تحدد حاملها على الإنترنت والمعاملات والسلوك مع الحكومة وان تجري بأمان دون الحاجة للسفر و التأخير الذي لا لزوم له. فهو نظام يضمن أن يحدد هوية التواصل و الاتصالات من بعد وذلك إذا ما استخدمت لتوقيع بيانات بما يضمن أنه لم يتم تعديلها لا هي ولا هوية الموقع. فالتوقيع الرقمي علامة أمان إلكترونية يمكن إضافتها إلى الملفات. ويتيح إمكانية التحقق من ناشر الملف كما يساعد في التحقق من أن الملف لم يتم تغييره منذ تم توقيعه رقميًا(١).

عرف المشرع الاسباني التوقيع الرقمي في قانون التوقع الالكتروني ٢٠٠٣/٥٩ كمجموعة من البيانات الالكترونية المشتركة مع بيانات اخرى للتعرف على هوية الموقع(٢).

ويمكن القول بأن التوقيع الرقمي هو الوسيلة المادية لتوقيع المستندات إلكترونيا. ومثله مثل التوقيع اليدوي، فإن التوقيع الرقمي يثبت هوية صاحبه او حامله في العالم الإلكتروني وفي جميع التعاملات الإلكترونية. وهو كعملية الكترونية لتوقيع المستند الإلكتروني باستخدام الشهادة الرقمية، ويتم ذلك من خلال تشفير المختصر الحسابي الناتج من عملية دالة الاختزال للمستند الإلكتروني (Hash) باستخدام المفتاح الخاص. حيث تكمن أهمية التوقيع الرقمي في إثبات هوية الشخص وإثبات موافقته على ما تم التوقيع عليه، كما يضمن سلامة المستند الإلكتروني من أي تعديل بعد التوقيع الإلكتروني(٣).

---

(١) أ. محمد البقيرات. مديرية التشغيل والخدمات المعلوماتية. دائرة التوقيع الرقمي. الهيئة الوطنية لخدمات الشبكة

(2) Martínez Nadal, Comentarios a la ley de firma electrónica, Thomson Reuters, 2009, pág. 72.

(٣) المركز الوطني للتصديق الرقمي. وزارة الاتصالات وتقنية المعلومات. مجمع الملك عبدالعزيز للاتصالات – الرياض. المملكة العربية السعودية. http://www.ncdc.gov.sa/faqs

ايضا يمكن اعتبار التوقيع الرقمي المتجزء عن التوقيع الالكتروني او كصورة من صور التوقيع الالكتروني كنوع رقمي بحت فهو ليس ترقيم لتوقيع يدوي أو أخذ بصمة وترقيمها وإنما ينشئ رقميا ويظل رقميا[١] وهو سهل الاستخدام إذا ما تعلم الشخص استخدامه ولكنه من النوع المعقد هندسيا والآمن جداً ويضمن هذا النوع موثقية المستند وأن من أرسله هو فعلا صاحب التوقيع بلا شك. وكما يعتبر هذا النوع من التوقيعات التي يستحيل تزويرها أو تقليدها أو كسرها لانه أكثر الأنواع أمانا[٢].

كما ان التوقيع الرقمي هو عبارة عن جملة من البيانات تدرج بوسيلة إلكترونية على وثيقة إلكترونية وتربط بها، ويكون لها طابع متفرد يسمح بتحديد شخص الموقع ويميزه عن غيره وينسب إليه وثيقة إلكترونية بعينها. فالتوقيع الرقمي ليس صورة رقمية لتوقيع يدوي تتم بارسلها مذيلة بالرسالة عبر البريد الإلكتروني كما هو شائع بين المستخدمين، بل إن التوقيع الرقمي هو المزود والمؤكد باثبات وببرهان لهوية المرسل، وكما انه برهان على سلامة البيانات المرسلة[٣]. لانه عملية من عمليات توقيع الملفات الحاسوبية وهي مكافئة للتوقيع الورقي التقليدي. اذ يمكن بواسطة التوقيع الرقمي توقيع أي ملف وإرساله بواسطة البريد الإلكتروني. ويكون مستقبل هذا البريد متأكداً من الشخص الذي أرسل هذا الملف وذلك بالتحقق من صحة توقيعه الرقمي. ومن الجدير بالذكر ان اهتمام الحكومات الذكية كما في دولة الامارات العربية المتحدة استخدمته في اكثر من مجال من مجالات الحياة التكنولوجية. كما يمكن

(١) م. أشرف صلاح الدين، أساسيات التخزين الرقمي ، ورقة عمل غير منشورة مقدمة لندوة المفاهيم الأساسية للمعاملات القانونية والاقتصادية عبر الانترنت ، شرم الشيخ ، ٢٥ – ٢٩ ديسمبر ٢٠٠٥.

(2) Diffie, W., and Hellman, M. "Privacy and Authentication: An Introduction to Cryptography." Proceeding of the IEEE, March 1979.

(٣) د.أسامة أحمد شوقي المليجي، استخدام مستخرجات التقنيات العلمية الحديثة وأثره على قواعد الإثبات المدني، دار النهضة العربية، القاهرة، ٢٠٠٠. ص ٧٧,١١٠.

استخدام التوقيع الرقمي في توقيع العقود والشبكات وفي جميع معاملات الحكومة الإلكترونية تقوم بإرسال ملف موقع رقمياً إلى شخص اخر، وبتشفير الملف بمفتاح خاص ويرسل بالبريد الإلكتروني وعندما يستلم هذا الشخص الرسالة يحاول فك تشفيرها بواسطة مفتاح عام فإذا نجح في ذلك فهذا يعني أن الرسالة مشفّرة بمفتاح خاص فعلاً. وحتى يتم تبادل المفاتيح العامة بين الناس هناك مؤسسات موثوقة لديها بنية معطيات تحوي جميع مفاتيح المشتركين وتقوم بتخزين المفتاح العام واسم المستخدم ورقم جواز سفره وتاريخ تسجيل المفتاح ومدة صلاحيته. وتضع جميع هذه المعلومات في قالب واحد يطلق عليه شهادة رقمية. من هذه المؤسساتVeri Sign ، Global Sign.

اولا : خصائص التوقيع الرقمي

يرتبط التوقيع الرقمي ببعض المعايير المتعلقة بالأمن المعلوماتي، وسرية المعلومات التي يجب أن تكون محصورة بين المُرسِل والمُرسَل إليه. وسلامتها من حدوث أي تغيير أو تزوير فيها[١]، وأصالتها من خلال إمكانية التأكد من هوية المرسل أو المستقبل، وقدرة المتعاملين على إجبار الطرف الآخر على الاعتراف بصحة المعلومات المتبادلة.[٢]

ان التوقيع الرقمي لا يمكن تزويره لانه لا يعتمد على حركات اليد ولا يقوم به الانسان، وبما ان التوقيع الرقمي عبارة عن جزء صغير من البيانات المشفرة والموثوقة تنزل بالرسائل والمعاملات لصحة نسبتيا الى مصدرها، كما ان الأنظمة التي يعتمدها التوقيع الرقمي تراعي أعلى مضامين السلامة والأمن في نقله وتوزيعه.

(١) أ. أمين فرج يوسف. التوقيع الالكتروني. دار المطبوعات الجامعية. ٢٠٠٨ . ص ٧٢.

(٢) د.سعيد السيد قنديل، التوقيع الالكتروني. ماهيته، صوره، حجيته في الإثبات بين التداول والاقتباس. دار الجامعة الجديدة. الإسكندرية. الطبعة الثانية، ٢٠٠٦. ص ١٤٥.

علما ان المشرع الاماراتي لم بتطرق الى كلمة التشفير[١] في القانون رقم ٢ لسنة ٢٠٠٢ م الا انه اعطاها في اكثر من وصف باكثر من مادة قانونية مثل المادة رقم ٢ التي عرفت المعلومات الالكترونية بانها ذات خصائص الكترونية في شكل نصوص او رموز او اصوات او رسوم او صور....

من جهة اخرى المشرع الاسباني تطرق كلمة التشفير في المادة ٢٤ فقرة ١ من قانون التوقيع الالكتروني[٢]

ويصعب كشف عمليات التشفير التي يتم تبنيها عند إحداث التوقيع الرقمي، الذي هو ختم رقمي مشفر خاص بالشخص، يتم وضعه من قبل هيئات مخولة بإعطائه، تخضع كل من يطلبه إلى شروط محددة تُنظم من خلال ما يعرف بـ Public Key) Infrastructure (PKI. ويتم لهذه الغاية إنشاء مفتاحين، مفتاح خاص معروف من قبل صاحب التوقيع ليوقع على الوثائق، ومفتاح عام يستخدمه المستلم للتأكد من صحة الوثائق. ومن خلال هذا التوقيع المعتمد على المفتاحين المذكورين .اللذين يقومان بدور القفل والمفتاح. يتم تأمين التعامل بين الأطراف بحرية وسرية عاليتين.

ومع تزايد الاعتماد على التكنولوجيا في تبادل الوثائق وخاصة التجارية والمالية منها، تزداد الحاجة إلى وضع الخطط المتقنة الضامنة لسلامة هذه المبادلات. ولهذا، فقد جرت في بعض الدول إعادة تحليل المعايير المعمول بها من أجل التأقلم مع هذه المتغيرات، وتطوير القوانين المتعلقة بالتوقيع الرقمي، فحاز هذا الشكل من التوقيع على رضا الكثير من الحكومات وقبولها له، وطبق في بعض الدول، فيما لا تزال

(١) سند حسن سالم. التنظيم القانوني للتوقيع الالكتروني وحجيته في الاثبات المدني. دار النهضة العربية. ٢٠١٠م. ص ١٣٧.

(2) Ferrer Gomila, El problema temporal del sistema de certificados, RCE, Enero 2000, pág. 29.

تدرس دول أخرى إمكانات تطبيقه. ومهما يكن من أمر، فلا بد من أن يشهد التوقيع الرقمي في زمن قريب اعتماداً على صعيد العالم بأسره. شأنه في ذلك شأن معظم التطورات التكنولوجية التي اعتمدت بسرعة في بعض الأماكن، وببطء في أماكن أخرى، مما أدى إلى ظهور الفجوات ما بين السابقين واللاحقين.

إن للتوقيع الرقمي متطلبات معينة مسبقة له والتي بدونها يصبح هذا التوقيع بدون أي قيمة قانونية.(١)

المفتاح الخاص يجب أن يبقى سري وبالتالي فإنه إذا عرضه أحد الفرق فإن هذا الفريق يستطيع أن يصدر ويقلد أي توقيع.

إن على المستخدمين وعلى برامجهم أن تكون متبعة للبروتوكول بحرفيته. بهذه الأحوال يمكن من خلاله إثبات من إرسل الرسالة والتأكد من صحة مضمونها.

هي قواعد منظمة لاستخدام الشهادات الرقمية وتحتوي على ارشادات هامة لمستخدمي البنية التحتية للمفاتيح العامة، توضح ما للمستخدم وما عليه، وتتطرق لإلتزامات مراكز التصديق ومراكز التسجيل.

ومن الأمثلة الحية لهذه القواعد هو الضوابط الأمنية لأماكن تشغيل مراكز التصديق. ومنع استخدام معلومات الزبائن خارج النطاق المسموح به. كذلك استخدام بطاقة الأحوال المدنية لإثبات هوية الأفراد. ايضا عدم حفظ المفاتيح الخاصة للزبائن لدى مركز التصديق. واخيرا تحديد حجم مفاتيح التشفير المستخدمة.

(١) قيمة الخوارزميات: بعض مفاتيح الخوارزميات غير آمنة وقد تم إثبات خرق البعض منها. قيمة التنفيذ: تنفيذ وتطبيق خوارزميات مع أخطاء لن يؤدي إلى أي نتيجة

ثانيا: اطراف التوقيع الرقمي

نصت المادة السادسة من قانون الأونسيترال النموذجي الخاص بالتوقيعات الإلكترونية على انه: (حيثما يشترط القانون وجود توقيع من شخص، يعد ذلك الاشتراط مستوفى بالنسبة إلى رسالة البيانات إذا استخدم توقيعا إلكترونيا موثوقا به بالقدر المناسب للغرض الذي انشئت أو ابلغت من اجله رسالة البيانات في ضوء كل الظروف بما في ذلك أي اتفاق ذي صلة).

ونصت المادة الاولى من القانون الاتحادي الاماراتي ان: (الطرف المعتمد: الشخص الذي يتصرف معتمداً على توقيع الكتروني أو شهادة مصادقة الكترونياً)[1].

وكما بينت المادة (١٣) من نفس القانون على ان:

١. تعتبر الرسالة الإلكترونية صادرة عن المنشئ إذا كان هو الذي أصدرها بنفسه.

٢. في العلاقة بين المنشئ والمرسل إليه، تعتبر الرسالة الإلكترونية صادرة عن المنشئ إذا أرسلت:

أ. من شخص له صلاحية التصرف نيابة عن المنشئ فيما يتعلق بالرسالة الإلكترونية.

ب. من نظام معلومات مؤتمت ومبرمج للعمل تلقائياً من قبل المنشئ، أو نيابة عنه.

فمن هنا نجد ان العلاقة بين الاطراف محددة من قبل المشرع الاماراتي وان الاطراف هم المنشئ والمرسل اليه وهي علاقة محكومة بواجبات افرغها المشرع على الاطراف طالما ان المعاملات ذات طابع الكتروني).

(١) القانون الاتحادي رقم (١) لسنة ٢٠٠٦ بشأن المعاملات والتجارة الإلكترونية

فواجبات الموقع ذكرت في المادة (١٩) حيث بينت انه أولاً: يجب على الموقع:

١. عدم استخدام أداة توقيعه استخداماً غير قانوني.

٢. أن يمارس عناية معقولة لتفادي استخدام أداة توقيعه استخداماً غير مصرح به.

٣. أن يخطر الأشخاص المعنيين بدون تأخير غير مبرر، وذلك في حالة:

أ. علم الموقع بأن أداة توقيعه قد تعرضت لما يثير الشبهة في درجة أمانها.

ب. أو إذا تبين من دلالة الظروف المعروفة لديه ما يرجح أن تكون أداة التوقيع تعرضت لما يثير الشبهة فيها.

٤. أن يمارس عناية معقولة لضمان دقة واكتمال كل ما يقدمه من بيانات وتصريحات جوهرية ذات صلة بشهادة المصادقة الالكترونية طوال مدة سريانها، وذلك في الحالات التي تستلزم فيها أداة التوقيع استخدام هذه الشهادة.

ان الحصول على التوقيعات الإلكترونية (الشهادة الرقمية) الخاصة بالفرد بناء على طلب من العملاء[١] والتي تتم بواسطة الشخص نفسه[٢] يتم بعلاقة متبادلة من

(١) علي محمد أحمد أبو العز، التجارة الإلكترونية وأحكامها في الفقه الإسلامي. دار النفائس للنشر والتوزيع، الأردن. ٢٠٠٨ .ص ٣٢٤ . وتسمى أيضا شهادة المستخدم الفئة ٢ CA، هي الشهادة الإلكترونية التي تصدرها FNMT. RCM ربط المشترك الخاصة بك عن التحقق من البيانات التوقيع وتأكيد هويتها . في هذه الشهادات، المشترك قد يكون مجرد شخص طبيعي . Persona Física. También denominado Certificado de usuario Clase 2 CA, es la certificación electrónica expedida por la FNMT.RCM que vincula a su Suscriptor unos Datos de verificación de Firma y confirma su identidad. En estos Certificados, el Suscriptor sólo lo podrá ser una persona física.

(٢) محمود عبد االرحيم االشريفات، التراضي في تكوين العقد عبر الإنترنت، دار الثقافة. عمان، ٢٠٠٩. ص ٢٠٩.

خلال منظمة ذاتية الحكم لإدارة الاقتصاد والمكاتب الالكترونية[١] مثل OAGER الذي يسمح للمواطنين الوصول إلى مشاورات فورية كوسيلة مريحة وتكون المفاوضات من خلال شبكة الإنترنت توفر الجهد والوقت من تجنب الذهاب إلى مكاتب البلدية.

فعلى الرغم من أنه من الممكن اتخاذ خطوات متعددة دون التوقيعات الإلكترونية لتحقيق بعض من لهم (مع الأوراق شهادة رقمية) ، مطلوب التوقيع الالكتروني عن طريق الحصول على شهادة من الدرجة CA٢، FNMT الرقمية الصادرة عن دار سك النقود الوطنية و جرس ريال مدريد كازا دي لا مونيدا[٢]. فللاطراف علاقة مباشرة ببعضهم البعض حيث تكون على كافة المراحل من المطالبة بالشهادة الالكترونية الى لحظة استخدامها. فالمرحلة الاولى . تطبيق الشهادة الرقمية بدءا من معدات جهاز الكمبيوتر الخاص بالمستخدم ، اذ يجب على المواطن الوصول إلى المكتب مثل .فابريكا ناسيونال دي مونيدا ذ جرس. (FNMT) لما يسمى الفئة. CA٢ شهادة العضو صادر عن وكالة (الوطنية) فالإدارة العامة[٣] هذا هو التصديق الإلكترونية التي يصدرها FNMT. RCM ربط صاحبها (الحكومة ، والجسم، وكالة أو هيئة عامة) مع بعض

(١) د.رامي محمد علوان، التعبير عن الإرادة عن طريق الإنترنت، وإثبات التعاقد الإلكتروني، مجلة الحقوق، جامعة الكويت، العدد الرابع،،٢٠٠٢ .٢٤١ ص

(٢) في هذا القسم سوف تجد كل المعلومات المتعلقة بجمع وإدارة الشهادات الرقمية التي تقدمها فابريكا ناسيونال دي مونيدا ذ جرس . ريال مدريد كازا دي لا مونيدا.

Certificados Digitales qu'ofrece la Fábrica Nacional de Moneda y Timbre. Real Casa de la Moneda.

(3) Administración Pública. Es la certificación electrónica emitida por la FNMT.RCM que vincula a su Titular (la Administración, órgano, organismo o entidad pública) con unos Datos de verificación de Firma y confirma, de forma conjunta la identidad del Firmante junto con su puesto de trabajo, y al Titular del Certificado, que es el órgano donde el Firmante desarrolla su actividad.

توقيع بيانات التحقق و أكد معا هوية الموقع جنبا إلى جنب مع وظائفهم ، و حامل شهادة، وهو الجهاز التي تعمل فيها الموقع. اما المرحلة الثانية فهي الاعتماد لمدرج التعليمات البرمجية للتطبيق والتوثق من صلاحية الهوية عن طريق (مدير الاستخبارات الوطنية ، أو جواز السفر NIE). كما يجب أن يحضر أحد المكاتب المعتمدة المسجلة بالتحقق من هوية المواطن و تشرع في وضع اللمسات الأخيرة على العقد للحصول على خدمات التوقيع الإلكتروني مع الوكالة الوطنية (الوكالة المستقلة لإدارة الاقتصاد والإيرادات لديه مكتب الرقمية شهادات التسجيل)[١]. اما المرحلة ٣ . وبعد تحميل الشهادة بضع دقائق، يجب على المواطن مقدم الطلب الوصول إليها من جهاز الكمبيوتر الخاص به بتطبيقه إلى الوكالة الوطنية لتحميل الشهادة الرقمية. عند هذه النقطة، يمكن للمستخدم هنا استخدام التوقيع الإلكتروني الخاص به لإجراءات الاتصالات من بعد مع السلطات العامة وغيرها من المؤسسات[٢]. وبالمثل، يمكن عمل نسخة احتياطية من الشهادة عن طريق تصديرها إلى التخزين القابلة للإزالة. طرف ثالث محايد[٣].

(١) تقع في ميناء Espoz و رقم ١٦,١٨ (Pz. الحرية) ، الطابق الثاني ، مفتوح من الاثنين إلى الجمعة من الساعة ٨:٣٠ إلى ١٤ ساعة.

(٢) فمن الشهادة الإلكترونية التي تصدرها FNMT. RCM ربط المشترك الخاصة بالمستخدم عن بيانات التحقق من التوقيع وتأكيد هوية. المشترك قد يكون مجرد كيان قانوني . هذه الشهادة هي أيضا أن الهيئات العامة يجب أن تنطبق على علاقاتها مع وزارة الخزانة . .Persona Jurídica
Es la certificación electrónica expedida por la FNMT.RCM que vincula a su Suscriptor unos Datos de verificación de Firma y confirma su identidad. El Suscriptor sólo lo podrá ser una Persona jurídica. Este certificado es también el que deben solicitar los organismos públicos para sus relaciones con Hacienda.

(٣) فادي عماد الدين توكل، عقد التجارة الإلكترونية، منشورات الحلبي الحقوقية، بيروت، ٢٠١٠، ص١٥٤.

وهذا ما نلاحظه في المادة (٢١) من القانون الاتحادي الاماراتي اذ يحدد واجبات مزود خدمات التصديق وهو طرف من اطراف العلاقة بخصوص التوقيع الرقمي مع ضرورة التحقق من البيانات.

أولاً: يجب على مزود خدمات التصديق:

أ. أن يتصرف وفقاً للبيانات التي يقدمها بشأن ممارسته لنشاطه.

ب. أن يمارس عناية معقولة لضمان دقة واكتمال كل ما يقدمه من بيانات جوهرية ذات صلة بشهادة المصادقة الالكترونية أو مدرجة فيها طيلة سريانها.

ج. أن يوفر وسائل يكون من المعقول الوصول إليها وتمكن الطرف الذي يعتمد على خدماته من التأكد من الآتي:

١. هوية مزود خدمات التصديق.

٢. أن الشخص المعينة هويته في شهادة المصادقة الالكترونية، لديه السيطرة في الوقت المعني على أداة التوقيع المشار إليها في هذه الشهادة.

٣. الطريقة المستخدمة في تعيين هوية الموقع.

٤. وجود أية قيود على الغرض أو القيمة التي يجوز أن تستخدم من أجلها أداة التوقيع.

٥. ما إذا كانت أداة التوقيع صحيحة ولم تتعرض لما يثير الشبهة.

٦. ما إذا كان للموقع وسيلة لإعطاء إخطار بموجب هذا القانون.

٧. ما إذا كان هناك وسيلة مناسبة للإبلاغ عن إلغاء التوقيع.

د. أن يوفر وسيلة للموقعين تمكنهم من تقديم إخطار بأن أداة التوقيع قد تعرضت لما يثير الشبهة، وأن يضمن توافر خدمة إلغاء للتوقيع يمكن استخدامها في الوقت المناسب.

ه. أن يستخدم في أداء خدماته نظماً وإجراءات وموارد بشرية جديرة بالثقة.

و. أن يكون مرخصاً من مراقب خدمات التصديق إذا كان يعمل في الدولة.

ومن ناحية اخرى فان الاستخدام الحكومي للسجلات والتوقيعات الالكترونية يكون حسب المادة (٢٤) من القانون الاتحادي رقم (١) لسنة ٢٠٠٦ بشأن المعاملات والتجارة الإلكترونية اذ حدد الاعمال المنوطة بها

١. يجوز للجهات الحكومية في نطاق أداء الأعمال المنوطة بها بحكم القانون، ان تقوم بما يأتي:

أ. قبول ايداع أو تقديم المستندات أو انشائها أو الاحتفاظ بها في شكل سجلات الكترونية.

ب. اصدار أي اذن أو ترخيص أو قرار أو موافقة في شكل سجلات إلكترونية.

ج. قبول الرسوم أو أي مدفوعات اخرى في شكل الكتروني.

د. طرح العطاءات واستلام المناقصات المتعلقة بالمشتريات الحكومية بطريقة الكترونية.

٢. إذا قررت الحكومة تنفيذ أي من الاعمال المذكورة في الفقرة (١) من هذه المادة، فيجوز لها عندئذ ان تحدد:

أ. الطريقة أو الشكل الذي يتم بواسطته انشاء أو ايداع أو حفظ أو تقديم أو اصدار تلك السجلات الالكترونية.

ب. الطريقة والاسلوب والكيفية والاجراءات التي يتم بها طرح العطاءات واستلام المناقصات وانجاز المشتريات الحكومية.

ج. نوع التوقيع الالكتروني المطلوب بما في ذلك اشتراط ان يستخدم المرسل توقيعا رقميا أو توقيعا الكترونيا محميا آخر.

د. الطريقة والشكل اللذين يتم بهما تثبيت ذلك التوقيع على السجل الالكتروني والمعيار الذي يجب ان يستوفيه مزود خدمات التصديق الذي يقدم له المستند للحفظ والايداع.

ه. عمليات واجراءات الرقابة المناسبة للتأكد من سلامة وأمن وسرية السجلات الالكترونية او المدفوعات أو الرسوم.

و. اية خصائص او شروط او احكام اخرى مهددة حاليا لارسال المستندات الورقية، إذا كان ذلك مطلوبا فيما يتعلق بالسجلات الالكترونية الخاصة بالمدفوعات والرسوم.

المطلب الثاني
أهمية التوقيع الرقمي

تقوم عملية حماية التوقيع الإلكتروني على تشفير المعلومات[1] أي تحويلها إلى صيغة رياضية لمنع الأشخاص غير المرخص لهم من الاطلاع على المعلومات أو

(١) يرتبط التشفير بالتوقيع الإلكتروني ارتباطاً وثيقاً، فالتشفير هو التغيير في البيانات بحيث لا يتمكن من قرأتها الا شخص المستقبل وحده باستخدام مفتاح فك التشفير، وفي تقنية المفتاح العام يتوفر المفتاح ذاته لدى المرسل والمستقبل. انظر في ذلك، التوقيع الرقمي(حلول فعالة للمصادقة والتوثيق والآمان)الدكتور:كمال الدين يوسف يسن. ورقة علمية بحثية لعام ٢٠١٢.

فهمها. وتستخدم المفاتيح في تشفير المعلومة في محاولة لتحسين سير المعاملات الالكترونية والخدمة في الحكومة الالكترونية ايضا، تم إنشاء المواقع ذات الصلة سواء في دولة الامارات العربية المتحدة او في المملكة الاسبانية التي تهدف إلى تسهيل التفاعل مع المستخدمين والحكومات، وهذا كله بتزايد مضطرب في كلا الدولتين حيث ان الحاصلين على شهادات من موقع واحد (CERES) في اسبانيا حقق أكثر من ثلاثة ملايين مستخدم. وكما وجدت اليات معينة لتقديم الاقتراحات والنصائح و الآراء من خلال "المصدر المفتوح" أداة النظر في تعظيم الاستفادة من الموارد، وضعنا هذا الموقع الجديد الذي يحاول تجميعها وتحسينها[١]. بالإضافة إلى إصدار شهادات المستخدم الإلكترونية، ويقدم آلية التنسيق الإقليمية الحكومية وخدماتها شهادة الأعمال تضمن مبادئ المصداقية، النزاهة والسرية وعدم التنصل من الاتصالات عبر الشبكات المفتوحة.

اذ تكمن اهمية التوقيع الرقمي بانه يحدد الشخص بداية كحامل للتوقيع يتضمن معلومات صحيحة ومصداقية عالية وعدم المساس بها اذ نرى ان له فوائد عامة يمكن اجمالها بما يلي:

١. فالتوقيع الرقمي يثبت الشخص الذي وقع الوثيقة كما يحدد ذات الوثيقة التي تم توقيعها بشكل لا يحتمل التغيير[٢]. بمصداقية عالية، بالرغم من أن الرسائل تتضمن معلومات لكن هذه المعلومات قد تكون صحيحة وقد تكون خاطئة وبالتالي وجود التوقيع الرقمي لا يعني أن المعلومات الموجودة في الملف

(١) آلية التنسيق الإقليمية ، من خلال CERES قسم (شهادة التوقيع الرقمية الاسبانية) يقدم شهادة معترف بها من قبل الحكومة العامة الإلكترونية بشهادة من الدرجة الوطنية CA٢ .

(٢) أ. أمين فرج يوسف. التوقيع الالكتروني. دار المطبوعات الجامعية. ٢٠٠٨ . ص ٦٩.

صحيحة بشكل أكيد، «بمعنى أن التوقيع الرقمي يثبت صحة المرسل وليس صحة البيانات الموجودة بالرسالة».

أهمية هذه المصادقة تظهر جلياً في المستندات المالية، على سبيل المثال إذا قام فرع لبنك ببعث رسالة إلى الفرع الرئيسي يطلب فيها تغيير حساب معين، فإذا لم يتأكد الفرع الرئيسي أن مصدر مرسل الرسالة مصرح له بإصدار هذه المعلومات، فتغيير هذا الحساب يعتبر خطأً فادحاً.

٢. عامل الثقة والنزاهة: يمكن لباعث أو متلقي الرسالة أن يكون بحاجة للتأكد أو الثقة بأنه لم يتم المساس بالمعلومات خلال عملية الإرسال. وبما أن عملية التشفير تخفي مضمون الرسالة فإنه لا يمكن التغيير فيها، إذا كانت الرسالة موقعة رقمياً.

٣. ارتباط التوقيع الرقمي بختم التاريخ والتوقيت الصحيح:إن بروتوكولات التوقيع الرقمي لا تعطي تأكيداً واضحاً عن التاريخ والوقت الذي تم فيهما توقيع الملف. إن الموقع «قد أو لا» يضع ختم التاريخ على الملف أو يمكن أن يكون الملف نفسه متضمناً التاريخ، ولكن قارئ هذا الملف يمكن أن يشك بمصداقية وصحة هذا التاريخ.

وبالتالي فإن التوقيع الرقمي كالتوقيع المكتوب أي يستخدم للمصادقة على صحة مضمون الملف الموقع عليه والذي يسمى عادة الرسالة. ومن الممكن أن تكون هذه الرسالة على شكل بريد إلكتروني أو عقد معين أو حتى رسالة معقدة مرسلة ببروتوكول معين[١].

(١) م. عبدالملك رحال. مجلة رسالة الجامعة. http://rs.ksu.edu.sa/69418.html

المطلب الثالث

آلية عمل التوقيع الرقمي

بين القانون الاتحادي الاماراتي في المادة (١)[١] على ان: (المعاملة الالكترونية: أي تعامل أو عقد أو اتفاقية يتم إبرامها أو تنفيذها بشكل كلي أو جزئي بوساطة المراسلات الالكترونية). فهي اصلا تقوم على مراسلات الكترونية بين منشئ مرسل ومستقبل لدية الاهتمام بوضع توقيع له يشكل فائدة ذاتية شخصية او عامة. وكما ورد ايضا في المادة (١٢) الالية التي تتم من خلالها عمل التوقيع الرقمي بنصها حيث: (١. يجوز أن يتم التعاقد بين وسائط الكترونية مؤتمتة متضمنة نظامي معلومات الكترونية أو أكثر تكون معدة ومبرمجة مسبقاً للقيام بذلك، ويكون التعاقد صحيحاً ونافذاً ومنتجاً لآثاره القانونية حتى في حالة عدم التدخل الشخصي أو المباشر لأي شخص طبيعي في عملية إبرام العقد في هذه الأنظمة. ٢. يجوز أن يتم التعاقد بين نظام معلوماتي الكتروني مؤتمت بحوزة شخص طبيعي أو معنوي وبين شخص طبيعي آخر إذا كان الأخير يعلم أو من المفترض أن يعلم أن ذلك النظام سيتولى إبرام العقد أو تنفيذه تلقائياً).

نلاحظ ان المشرع الاماراتي لم يشترط بالتوقيع الالكتروني تعزيزه بشهادة مصادقة الكترونية[٢] . اذ تقوم الالية على الاجراءات المتبعة من قبل مركز التصديق لإصدار الشهادات الرقمية التي توضح الطرق الفنية والأمنية والإجرائية المتبعة

(١) القانون الاتحادي رقم (١) لسنة ٢٠٠٦ بشأن المعاملات والتجارة الإلكترونية.

(٢) د. علي هادي العبيدي.قواعد إسناد الرسالة الإلكترونية إالى المنشئ في قانون المعاملات والتجارة الإلكترونية الإماراتي. بحث منشور في مجلة الشريعة والقانون. السنة السلبعة والعشرون. العدد الرابع والخمسون. ٢٠١٣. ص ١٨٠ وما بعدها.

لإصدار الشهادة من قبل مركز التصديق. يستفيد منها المستخدم في تحديد الوثوق بمركز التصديق. تبين كذلك حقوق مستخدم الشهادة ومسؤولية المركز تجاهه[1].

اولا: عملية الحصول على شهادة رقمية وانشاء توقيع رقمي من خلال الموقع الإلكتروني

يتم انشاء التوقيع الإلكتروني باستخدام Microsoft Office وهذا المثال الذي يتم عادة وعن طريقه تطبيق انشاء توقيع إلكتروني وهو كمثال يتم التعال معه بشكل كبير، لذا وفي حال الانشاء نتبع الخطوت التالية:

١) فتح ملف الكتابة Word File ثم الذهاب بالمؤشر للمكان المراد وضع التوقيع فيه .

٢) الذهاب الى Insert Tab ثم اختيار Signature Lineثم الضغط بالسهم الموجود بالاسفل واختيار Microsoft Office Signature line

٣) سوف يظهر صندوق هنا يجب القيام بملئ البيانات الشخصية (الإسم،العنوان،الإيميل)

٤) من ثم القيام بالضغط على Right Click في علامة التوقيع على شكل X ثم اختيار الامر Sign...

٥) بعده القيام بملئ المتطلبات في الخيار الثاني.

٦) سوف يطلب الجهاز ان تدخل الاسم او صورة للتوقيع.

٧) وهنا تكون قد تمت عملية التوقيع الإلكتروني على الملف Word File.

(١) أ. محمد البقيرات. مديرية التشغيل والخدمات المعلوماتية. دائرة التوقيع الرقمي. الهيئة الوطنية لخدمات الشبكة.

٨) ولكن اذا اردنا إزالة التوقيع الإلكتروني نضع المؤشر التوقيع ثم نضغط Right click ثم نختار Remove Signature ثم نحذفه.

ثانيا: عملية التقدم للحصول على شهادة رقمية من خلال الموقع الإلكتروني في اسبانيا.

ان معالجة البيانات الشخصية التي تتطلب شهادة مقدمي الخدمات لتطوير الهيئات التجارية والإدارية على ممارسة المهام التي يمنحها هذا القانون ٢٠٠٣/٥٩ المؤرخ ١٩ كانون الأول على التوقيع الالكتروني. بان تخضع لأحكام القانون رقم ١٥ /١٩٩٩ المؤرخ ١٣ ديسمبر حماية البيانات الشخصية والقواعد المنفذة له. هناك خطوات للحصول على شهادة رقمية[١] يجب على مقدمي خدمات التصديق التي أنشئت في إسبانيا قبل نفاذ هذا القانون إبلاغ وزارة العلوم والتكنولوجيا بخصائص الخدمات المقدمة خلال شهر واحد من بدء نفاذه. وتنشر هذه المعلومات في عنوان إنترنت من تلك الوزارة من أجل إعطاء أقصى قدر من التعرض والمعرفة. فمن خلال شبكة الإنترنت تبدا بطلب شهادة التوقيع الالكتروني من الدخول الى موقع: http://www.cert.fnmt.es ومن ثم النقر على : الحصول على شهادة المستخدم. وتكون بالشكل التالي. انقر على : طلب الشهادة عبر الإنترنت. وهنا تدخل الى الجهة المختصة التي تعنى بالطلب ويمكنها استقباله بمستوى عال من الأمان، بحيث يتم استقبال كلمة مرور في كل مرة عند استخدام الشهادة. وهذا مهم جدا ، وخاصة إذا العديد من الناس يستخدمون نفس جهاز الكمبيوتر. ومن بعد يكون هناك رمز للمستخدم وطالب الشهادة التي سيتم طباعتها.

(١) هذه الشهادات الإلكترونية التي تم إصدارها من قبل مقدمي خدمات التصديق لا بد ان توافق القانون وهي طبقت بموجب قانون المرسوم الملكي ١٩٩٩/١٤ تاريخ ١٧ أيلول بشأن التوقيعات الالكترونية سارية المفعول.

هنا تقوم الجهة المختصة بإثبات الهوية[1]. فيجب أن يكون مقدم الطلب شهادة موجودة فعليا في مكتب الرقمية شهادة الاعتماد بذلك على الرقم (الجهة المختصة) و طلب رمز كما لاحظنا سابقا. فهي خطوة يتعين على مقدم الطلب التوقيع على استمارة الطلب للحصول على الترخيص وشروط استخدامه ، منها أنه سيتم إعطاء نسخة . وبعد دقائق قليلة بعد أداء شهادة الاعتماد التي يمكن تحميلها على نفس الكمبيوتر حيث تم إجراء الطلب. لإصدار شهادات العامة الإلكترونية، من مزودي خدمات التصديق بجمع البيانات الشخصية مباشرة والموافقة الصريحة مع التوقيع. سيكون مطلوبا من البيانات المطلوبة على وجه الحصر لإصدار وصيانة الشهادة الإلكترونية، وتوفير خدمات أخرى ذات صلة بالتوقيعات الإلكترونية، وعدم استخدامها لأغراض أخرى دون الحصول على موافقة صريحة من الدول الموقعة .

يلي ذلك تحميل ما تم ارساله من الجهة المختصة ثم ، بعدها الاعتماد الناجح. والخلاصة هي ان مواقع مختصة بالقانون الاسباني تعتمد شهادات التوقيع الالكتروني بالدخول الى موقع: http://www.cert.fnmt.es ثم النقر على : الحصول على شهادة المستخدم. ثم النقر على : حمل شهادة المستخدم الخاصة بك. ثم دخول المعلومات الخاصة بك بالإضافة إلى التعليمات البرمجية للتطبيق ترخيص لطلب الشهادة التي حصل عليها. ثم اخيرا النقر على تحميل (إذا سار كل شيء بشكل جيد) ، اما ان لم يكن جيدا فيتم الحصول على رسالة تشير الى خطأ (هو سيء لعدم اكتمال البيانات) وما عليك الا تحميل المعلومات الصائبة من جديد و سوف تضطر إلى إرسال مرة أخرى. وبعد ذلك ان تمت الخطوات بشكل صحيح، يظهر لك انه يمكنك الآن استخدام التوقيع الرقمي لاتخاذ الترتيبات اللازمة من خلال شبكة الإنترنت دون الحاجة

(1) Martínez Nadal, A., Comentarios a la ley de firma electrónica, Thomson Reuters, 2009, pág. 247.

للتحرك والتنقل بل يمكنك عمل كافة المتطلبات من منزلك. لذا فمن الضروري أن يكون لديك شهادة صالحة من المؤسسة الوطنية أو الهوية الإلكترونية الفردية.(١)

عند بطاقة ذات FNMT التشفير المعتمدة، و يجب أن يكون هناك قارئ بطاقة متوافقة ومطابقة للمعلومات و يجب أن يكون كل شيء بشكل صحيح تثبيت و تكوين ل جهاز الكمبيوتر الخاص بك و المتصفح ، اعتمادا على برامج التشغيل وإرشادات من الشركة المصنعة للبطاقة التشفير والقارئ المستخدمة.

وعلى كل الاحوال فان على مقدم خدمات التصديق المصدر للشهادة ان يوقع رقميا على شهادته اثناء فترة سريان الشهادة الاخرى المستخدمة في التحقق من صحة التوقيع الرقمي لانه شرط من شروط امكانية التحقق من صحته(٢).

---

(1) En cuanto a sistemas operativos, se requiere disponer de: Windows 2000 o superior (XP, Vista, indows 7) Linux 2.6 (Guadalinex 4 o superior, Ubuntu, etc.) Mac OS X 10.6.8 y superiores (Snow Leopard, Lion y Mountain Lion) En cuanto a navegadores web, se requiere:Internet Explorer 7 o superior. Firefox 3.0 o superior [Firefox].Google Chrome 4 o superior. Apple Safari 4.0 o superior. En cuanto a Java, se requiere disponer de JRE 1.5 o superior, aunque se recomienda el uso de JRE 1.7. Java debe estar habilitado para el navegador que vayamos a utilizar.Para poder visualizar correctamente el documento a firmar y los justificantes de firma deberá tener instalado algún software de visualización de documentos en formato PDF (por ejemplo, Adobe Reader).Advertencia para los usuarios de Firefox en entorno Windows: lgunas versiones de Java para Windows requieren para su ejecución en el momento de la firma, que en su sistema esté instalado un componente específico de Microsoft. De no tener instalado este componente, se presentará el problema de que la aplicación no mostrará al usuario el certificado con el que proceder a la firma electrónica. Puede descargar este componente desde: Entorno de ejecución de Visual C++.

(٢) أ. أمين فرج يوسف. التوقيع الالكتروني. دار المطبوعات الجامعية. ٢٠٠٨ . ص ١٠٦.

المطلب الرابع

ادراج التوقيع الرقمي في المستندات

بعد التثبت من صحة التوقيع الالكتروني المعين من قبل القادر على الوصول سوار من قبل الشخص المستخدم او من هيئة معينة للمفتاح العام وانه متطابقا مع مفتاح الموقع الخاص فان من الافضل التثبت من صحة التوقيع عن طريق شخص ثالث وهي جهة التصديق الالكتروني كما بينا سابقا. وهي التي تقوم باصدار شهادة بسجل الكتروني يذكر فيه المفتاح الشفري العام وهو موضوع الشهادة والتثبت من صحة التوقيع الالكتروني لجهة التصديق[1]. وقد عالج المشرع الاماراتي هذا في المادة ١ من القانون الاتحادي بوضع صيغة تحدد الوسيط الالكتروني المؤتمت: برنامج أو نظام الكتروني لوسيلة تقنية المعلومات تعمل تلقائياً بشكل مستقل، كلياً أو جزئياً، من دون إشراف من أي شخص طبيعي في الوقت الذي يتم فيه العمل أو الاستجابة له. ونجد كذلك الجهة المعتمدة باصدار الشهادة الالكترونية عن طريق مزود خدمات التصديق: أي شخص أو جهة معتمدة أو معترف بها تقوم بإصدار شهادات تصديق الكترونية أو أية خدمات أو مهمات متعلقة بها وبالتوقيعات الالكترونية والمنظمة بموجب أحكام هذا القانون. وكذلك وضح شهادة المصادقة الالكترونية: الشهادة التي يصدرها مزود خدمات التصديق يفيد فيها تأكيد هوية الشخص أو الجهة الحائزة على أداة توقيع معينة.

وبين القانون الاسباني انه يجب على مقدمي خدمات التصديق أن تسجل اسما مستعارا في طلب توقيع الشهادة الالكترونية بتحديد هويته الحقيقية والحفاظ على

(١) أ. أمين فرج يوسف. التوقيع الالكتروني. دار المطبوعات الجامعية. ٢٠٠٨ . ص ٦٩.

وثائق تثبت ذلك. فهي ملزمة لمقدمي خدمات التصديق على الكشف عن هوية الموقعين عندما تطلبها المحاكم فقط وذلك لممارسة المهام الموكلة للموظفين المعنيين كما هو منصوص عليها في المادة ١١,٢ من القانون الأساسي لحماية البيانات الشخصية[١].

فإن امكانية إرسال رسالة الإلكترونية بأمان تام إلى المتلقي دون أن تتعرض لاختراق أي طرف ثالث، منها على سبيل المثال تقنية تشفير الرسائل الإلكترونية وكذلك التوقيع الرقمي. ولكن استعمال مثل هذه التقنيات مع برامج البريد العادية يتم بشكل محدود؛ لأن توفير أعلى مستويات الأمان يتطلب دائماً الاعتماد على البرامج الإضافية . ومن أهم العمليات المرتبطة بالتوقيع الرقمي هناك التشفير.

والتشفير معروف منذ عصور قديمة واستخدم أساساً لغايات عسكرية. أما الآن فقد أصبح عملية معقدة جداً وبالغة السرية وذات ترميز معقد، يتم من خلالها إخفاء هوية البيانات من خلال اتباعها لخوارزمية ما. وهي بلا شك عملية أكثر تعقيداً من عملية الترميز التي هي مجرد تحويل من نظام إلى آخر.

كما نصت المادة ١٨ من القانون الاسباني ٢٠٠٣/٥٩ المؤرخ ١٩ كانون الأول على التوقيع الالكتروني[٢] (ان التزامات مقدمي خدمات التصديق بإصدار شهادات

---

(١) . الملدة ١٧ من القانون ٢٠٠٣/٥٩ المؤرخ ١٩ كانون الأول على التوقيع الالكتروني.

(2) Artículo 18 Obligaciones de los prestadores de servicios de certificación que expidan certificados electrónicos

Los prestadores de servicios de certificación que expidan certificados electrónicos deberán cumplir las siguientes obligaciones:

a) No almacenar ni copiar los datos de creación de firma de la persona a la que hayan prestado sus servicios.

b) Proporcionar al solicitante antes de la expedición del certificado la siguiente información mínima, que deberá transmitirse de forma gratuita, por escrito o por vía electrónica:

=

=

1.º Las obligaciones del firmante, la forma en que han de custodiarse los datos de creación de firma, el procedimiento que haya de seguirse para comunicar la pérdida o posible utilización indebida de dichos datos y determinados dispositivos de creación y de verificación de firma electrónica que sean compatibles con los datos de firma y con el certificado expedido.

2.º Los mecanismos para garantizar la fiabilidad de la firma electrónica de un documento a lo largo del tiempo.

3.º El método utilizado por el prestador para comprobar la identidad del firmante u otros datos que figuren en el certificado.

4.º Las condiciones precisas de utilización del certificado, sus posibles límites de uso y la forma en que el prestador garantiza su responsabilidad patrimonial.

5.º Las certificaciones que haya obtenido, en su caso, el prestador de servicios de certificación y los procedimientos aplicables para la resolución extrajudicial de los conflictos que pudieran surgir por el ejercicio de su actividad.

6.º Las demás informaciones contenidas en la declaración de prácticas de certificación.

La información citada anteriormente que sea relevante para terceros afectados por los certificados deberá estar disponible a instancia de éstos.

c) Mantener un directorio actualizado de certificados en el que se indicarán los certificados expedidos y si están vigentes o si su vigencia ha sido suspendida o extinguida. La integridad del directorio se protegerá mediante la utilización de los mecanismos de seguridad adecuados.

d) Garantizar la disponibilidad de un servicio de consulta sobre la vigencia de los certificados rápido y seguro. .

إلكترونية انه يجب على مقدمي خدمات التصديق إصدار شهادات إلكترونية تلبية المتطلبات التالية :

أ) عدم تخزين أو نسخ بيانات انشاء التوقيع من الشخص طالب الخدمة.

ب) تقديم الطلب من الشخص قبل إصدار الشهادة وان المعلومات تقدم مجانا ، من خلال الكتابة أو عن طريق الوسائل الإلكترونية وهي :

١ . التزامات الموقعين أدناه ، والطريقة التي لديهم عن سند معلق التسليم انشاء التوقيع البيانات، و الإجراءات الواجب اتباعها للإبلاغ عن فقدان أو احتمال إساءة استخدام هذه البيانات و إنشاء بعض الأجهزة والتحقق من التوقيع الإلكتروني كانت متوافقة مع توقيع البيانات و شهادة تم إصدارها.

٢. آليات ل ضمان موثوقية التوقيع الالكتروني مع مرور الوقت.

٣. الطريقة المستخدمة من قبل موفر الخدمة يتحقق من هوية الموقع أو غيرها من المعلومات الواردة في الشهادة.

٤. الظروف الدقيقة لاستخدام الشهادة، حدوده استخدام ممكن وموفر يضمن المسؤولية المالية.

٥. الشهادات التي تم الحصول عليها ، عند الاقتضاء ، و الخدمة، و إجراءات إصدار الشهادات المطبقة لتسوية النزاعات التي قد تنشأ عن ممارسة نشاطها.

٦ . المعلومات الأخرى الواردة في بيان ممارسات التصديق .

المعلومات الواردة هي ذات الصلة والموضوع يجب أن تكون لدى الطرف الثالث اذا تضرر من الشهادات.

ج) المحافظة على الشهادة كدليل يشير إذا كانت فاعلة أو إذا كان قد تم تعليق تطبيقها أو منتهية الصلاحية . وهي محمية كدليل باستخدام آليات أمنية مناسبة.

د) ضمان توافر خدمة التفاوض بشأن االصدار شهادات سريعة وآمنة.

اولا: أنظمة التشغيل

أما بالنسبة لأنظمة التشغيل ، يجب أن يكون المشترك: ويندوز ٢٠٠٠ أو أعلى (إكس بي، فيستا ، ويندوز ٧(لينكس ٢,٦ Guadalinex 4) أو أعلى، أوبونتو، الخ. (نظام التشغيل Mac OS X 10.6.8 و أعلى (سنو ليوبارد ، الأسد و اسد الجبل(كما يتطلب متصفحات الويب: Internet Explorer 7أو أعلى. فايرفوكس ٣,٠ أو أعلى [فايرفوكس. [جوجل كروم ٤ أو أعلى. أبل سفاري ٤,٠ أو أعلى. كما يتطلب جافا JRE وجود ١,٥ أو أعلى، على الرغم من أن استخدام JRE 1.7 مستحسن. يجب تفعيل جافا للمتصفح ليكون قابلا للاستخدام. ولرؤية وثيقة التوقيع وإثبات التوقيع يجب تثبيت بعض الوثائق عرض برامج) PDF على سبيل المثال ، برنامج أدوبي ريدر. (تحذير لمستخدمي فايرفوكس على بيئة ويندوز : بعض إصدارات ويندوز يتطلب جافا لتشغيلها في وقت التوقيع ، على النظام الخاص بك أن مكون محدد من Microsoft[1] مثبتة. لم يكن لدينا هذا المكون المثبتة، المشكلة التي لا تظهر تطبيق شهادة المستخدم التي تسير مع التوقيع الإلكتروني هو المقدمة. وتم إطلاق برنامج "LetterSigner" لتسهيل استخدام التوقيع الإلكتروني والتشجيع عليه، عبر جعل التوقيع باستخدام بطاقة الهوية أمراً ممكناً على المستندات الإلكترونية، سواء كان

(1)http://windows.microsoft.com/ar.xm/windows.live/mail.create.signature.

ذلك عبر برنامج "مايكروسوفت وورد" أو ضمن أنظمة أتمتة الإجراءات أو برامج إدارة المحتويات[1].

ففي الامارات العربية المتحدة، أطلقت شركة التقنية لحلول الأعمال، الخبيرة في مجال الخدمات الإلكترونية، بالتعاون مع شريكها البلجيكي "LetterGen"، برنامجاً للتوقيع الإلكتروني باستخدام بطاقة الهوية الصادرة عن هيئة الإمارات للهوية. ويأتي إطلاق البرنامج في ظل النجاح الذي حققته هيئة الإمارات للهوية في تطوير البنية التحتية لبطاقة الهوية الذكية وشمول التسجيل فيها وإصدارها لجميع سكان الدولة من مواطنين ومقيمين، بهدف توسيع استخدامها في جميع التعاملات سواء بغرض الحصول على المعلومات، أو الولوج إلى المواقع أو التوقيع الإلكتروني عبر جهاز قارىء بطاقة الهوية الإلكتروني.

ثانيا: إستخدام الشهادات الرقمية

١. البريد إلكتروني: تستخدم لتوقيع بريد إلكتروني وتشفيره ويتم التحقق من خلال عنوان البريد الإلكتروني

٢. موقع إلكتروني: تستخدم لتحقق من الموقع ويتم التحقق من خلال اسم النطاق في الشهادة

٣. توقيع وثيقة: تستخدم لتحقق من أن الوثيقة لم يتم التعديل عليها بعد أن تم توقيعها.

٤. شخصية : تستخدم في التبادل الإلكتروني ويتم التحقق من خلال اسم الشخص في الشهادة

(1)http://www.albayan.ae/across.the.uae/news.and.reports/2013.09.17.1.1961343

ومن الامثلة عليها في اسبانيا مثلا: بطاقة سيريس وهو جهاز إلكتروني صغير بحجم بطاقة الائتمان التي تحتوي على الذاكرة الإلكترونية بحيث يمكن استخدامها لتخزين الشهادات الالكترونية لضمان أمن من خلال آليات التشفير. مع وجود دليل التكوين الذي يوفر جميع الخطوات اللازمة لتثبيت LTC31 قارئ بطاقة USB على جهاز الكمبيوتر الخاص بالمستخدم و برامج إدارة المرتبطة للحصول على البطاقة. ندرج هنا الخطوات المتبعة وهي:

الخطوة ١ . وحدة تحكم قارئ البطاقة الذكية . :اذ تحتوي على تعليمات لتحميل برامج تشغيل ويندوز

الخطوة ٢ . بسيطة للتعامل مع بطاقة البرمجيات: اذ تحتوي على تعليمات لتحميل بطاقة البرمجيات

الخطوة ٣ . بطاقة دليل البرنامج: المستورد شهادة. تحدد نوع الشهادات ثم فتح البطاقة و رقم التعريف الشخصي التغيير

ثالثا: الاعتراف بالشهادات والتوقيعات الإلكترونية الأجنبية

اوردت المادة ٢٦:

١. لتقرير ما إذا كانت الشهادة أو التوقيع الإلكتروني نافذاً قانوناً ، لا يتعين إيلاء الاعتبار إلى المكان الذي صدرت فيه الشهادة أو التوقيع الإلكتروني، ولا إلى الاختصاص القضائي الذي يوجد فيه مقر عمل الجهة التي أصدرت الشهادة أو التوقيع الإلكتروني.

٢. يعتبر الشهادات التي يصدرها مزودو خدمات التصديق الأجانب ، كشهاداتصادرة من مزودي خدمات التصديق الذين يعملون بموجب هذا القانون ، إذا كانت ممارسات مزودي خدمات التصديق الأجانب ذات مستوى من الوثوق يوازي على

الأقل المستوى الذي تتطلبه المادة (٢٤) من مزودي خدمات التصديق العاملين بموجب هذا القانون، ومع الأخذ بالاعتبار المعايير الدولية المعترف بها.

٣. يجوز الاعتراف بالتوقيعات التيتستوفي شروط القوانين الخاصة بدولة أخرى ، واعتبارها في مستوى التوقيعات الصادرة وفقاً لأحكام هذا القانون ، إذا اشترطت قوانين الدولة الأخرى مستوى من الاعتماد على التوقيعات يوازي على الأقل المستوى الذي يشترطه هذا القانون لتلك التوقيعات.

٤. يتعين في موضوع الاعتراف المنصوص عليه في الفقرتين (٢) (٣) السابقتين، النظر إلى العوامل الواردة في الفقرة (٢) من المادة (٢٤) من هذا القانون.

٥. لتقرير ما إذا كان التوقيع الإلكتروني او الشهادة نافذة قانوناً ،يتعين ايلاء الاعتبار إلى أي اتفاق بين الطرفين حول المعاملة التي يستخدم فيها ذلك التوقيع أو الشهادة.

٦. على الرغم من أحكام الفقرتين (٢) ، (٣) السابقتين:

أ. يجوز للأطراف في المعاملات التجارية والمعاملات الأخرى أن يحددوا وجوب إستخدام مزودي خدمات تصديق معينين أو فئة معينة منهم أو فئة معينة من الشهادات فيما يتصل بالرسائل أو التوقيعات الإلكترونية المقدمة لهم

ب. وفي الحالات التي يتفق فيها الأطراف فيما بينهم على استخدام أنواع معينة من التوقيعات الإلكترونية أو الشهادات فإن ذلك الاتفاق يعتبر كافياً لأغراض الاعتراف المتبادل بين الاختصاصات القضائية المختلفة للدول ، شريطة ألا يكون مثل هذا الاتفاق غير مشروع وفقاً لأحكام القوانين المطبقة في الإمارة.

المبحث الثاني

حجية التوقيع الرقمي في الاثبات

اعتمدت التشريعات الجديدة مؤخراً من قبل الدول الأعضاء في الاتحاد الاوروبي ضمن ما يسمى قاعدة المسائل التشريعية المتعلقة بالتجارة الإلكترونية . فقد أقرت بالتوقيع الرقمي وأكدت على أهميته ومنحه قيمة قانونية مساوية للإمضاء الخطي أو للتوقيع الخطي، لذا فقد أصدرت اللجنة الأوروبية المعنية بالإشراف على تقنين هذا المشروع توجيها يتعلق بالإطار المشترك للتوقيع الرقمي هدفه ما يلي:

أولاً : منع الدول الأعضاء من رفض منح التوقيع الرقمي مفعولاً قانونيا لمجرد تنفيذه إلكترونيا.

ثانياً : ضمان حرية سير خدمات التصديق والمصادقات في قلب الاتحاد الأوروبي.

وبموجب هذا التوجيه تمنح المصادقات الصفة القانونية اللازمة إذا تضمنت البيانات: هوية مورد خدمة التصديق. اسم حامل اللقب titulaire وصلاحيته النوعية. توقيع نظام التحقيق. مدة الصلاحية. التوقيع الرقمي لمقدم خدمة المصادقة. الكود الذي يحدد هوية المصادقة.

في اسبانيا هناك قانون ٢٠٠٣/٥٩ بشأن التوقيع الإلكتروني، الذي يحدد ثلاثة أنواع من العلامات[1]:

(1) En España existe la Ley 59/2003, de Firma electrónica, que define tres tipos de firma: Simple. Datos que puedan ser usados para identificar al firmante (autenticidad) Avanzada. Además de identificar al firmante permite garantizar la integridad del documento y la integridad de la clave usada, utilizando para ello un DSCF (dispositivo seguro de =

بسيطة: البيانات التي يمكن أن تستخدم لتحديد الموقع (أصالة).

متقدمة: بالإضافة إلى التعرف على الموقع وثيقة يضمن سلامة ونزاهة الرئيسية المستخدمة، وذلك باستخدام DSCF (آمن جهاز إنشاء التوقيع، ومدير الاستخبارات الوطنية الإلكترونية). وتستخدم تقنيات PKI.

معترف بها. هو متقدمة ومحمية بموجب شهادة مؤهل (شهادة تمنح بعد التحقق حضور هوية الموقع) التوقيع. في بعض الأحيان وهذا ما يسمى توقيع المؤهلين عن طريق الترجمة المؤهلين لمصطلح الظهور في التوجيه الأوروبي بشأن التوقيعات الالكترونية.

المطلب الاول

حجية التوقيع الرقمي (التصديق الالكتروني).

نصت المادة ١٧/٤ مكرر من قانون الاثبات الاتحادي المعدل بالقانون الاتحادي رقم ٢٠٠٦/٣٦ على ان (للكتابة الالكترونية والمحررات الالكترونية والسجلات والمستندات الالكترونية ذات الحجية المقررة للكتابة والمحررات الرسمية والعرفية في

=

creación de firma, el DNI electrónico). Se emplean técnicas de PKI. Reconocida. Es la firma avanzada y amparada por un certificado reconocido (certificado que se otorga tras la verificación presencial de la identidad del firmante). En ocasiones, esta firma se denomina cualificada por traducción del término inglés qualified que parece en la Directiva Europea de Firma Electrónica.

احكام هذا القانون متى استوفت الشروط والاحكام المقررة في قانون المعاملات والتجارة الالكترونية).

لا يمكن تطبيق التوقيع الإلكتروني نهائياً الا في حالة وجود الشهادات الرقمية CA التي تصدر عن جهات التوثيق المرخص لها من قبل الجهات المسؤلة في الدولة لتشهد بأن التوقيع الإلكتروني صحيح وينسب الا من اصدره ويستوفي الشروط وتعرف الشهادات بال (Third.Party) اي الطرف الثالث بين المرسل والمستقبل ومن امثلة هذه الجهات عالمياً هنالك شركة Magenta Corporation في الولايات المتحدة والتي تعمل في مجال حماية المعلومات حيث اصدرت اداة التوقيع الإلكتروني(١).

ومن حيث تزوير التواقيع الرقمية .يمكن للمزور أن يختار توقيعاً عشوائياً ويستخدم إجراءات التأكد من صحته ليجد الرسالة التي تعود لهذا التوقيع. عند التطبيق لا يستخدم هذا النوع من الإمضاء مباشرة ولكن يتم تجزيء هذه الرسالة إولاً ثم التوقيع عليها، وبالتالي فإن هذا التجزئ ينتج مفتاح التجزئة (hash function) وبذلك فإنه لا يؤدي إلى فرق.

هناك أسباب معينة لتوقيع قسم من هذه الرسالة (hash) وليس الرسالة كلها:

١. فعاليته: يكون التوقيع أصغر باعتباره يكون لقسم محدد فقط وليس لكل الرسالة.
٢. تطابقه مع برامج أخرى مثل ال RSA.
٣. مصداقيته: بحال عدم استعمال مفتاح التجزئة فإنه يجب تقسيم النص الذي يتم التوقيع عليه إلى أجزاء صغيرة جداً وبالتالي فإنه يتعذر على متلقي الرسالة أن يفهم أويتلقى هذه الإجزاء.

(1) http://ar.wikipedia.org.

كما لا يمكن أن يتم لتوقيع على شهادة منتهية الصلاحية أو إلغاء تواقيع صحيحة . فلا بد ان تكون الشهادة صالحة ، وعليه يجب الحصول على شهادة جديدة.

اولا: التزامات جهات التوثيق الالكتروني:التوقيع الإلكتروني (الرقمي) يتم بواسطة برنامج كمبيوتر خاص لهذه الغاية وباستعماله فان الشخص يكون قد وقع على رسالته تماما كما يوقع ماديا (في عالم الأوراق والوثائق الورقية) ، ويستخدم التوقيع الرقمي على كافة الرسائل الإلكترونية والعقود الإلكترونية . وبينا ايضا ان التوقيع الالكتروني مرتبط جوهريا بالتشفير، وهناك عملية تغيير في البيانات، بحيث لا يكون قادر على قرأتها الا الشخص المستقبل وحده، باستخدام مفتاح فك التشفير. في تكنولوجيا المفتاح العام الذي يعمل على التشفير وفك التشفير والطريقة الاكثر شيوعا للتشفير هو وجود مفتاحين ، المفتاح الخاص الذي يتوفر فقط للشخص الذي انشأه و المفتاح العام وهو معروف للجميع وبامكان الجميع او أي شخص إرسال رسائل مشفرة ، ولكن لا يمكن أن يفك رمز الرسالة الا الشخص الذي لديه المفتاح الخاص[1] وهذا واضح في نص امادة من القانون الاتحادي الذي عرف المعاملات الالكترونية المؤتمتة: معاملات يتم إبرامها أو تنفيذها بشكل كلي أو جزئي بوساطة وسائل أو سجلات الكترونية، والتي لا تكون فيها هذه الأعمال أو السجلات خاضعة لأية متابعة أو مراجعة من قبل شخص طبيعي[2].

استخدام تقنية شفرة المفتاحين العام والخاص(بنية المفتاح المعلن) والتى تقوم على استخدام مفتاحين للتشفير احدهما عام والأخر خاص بالموقع وان تصدر الهيئة المفتاح الشفرى الجذرى الخاصة بالجهة المرخص لها وهو المفتاح التى ستستخدمه الجهة فى انشاء التوقيعات للافراد. وهو المعد للاطراف لقيام الثقة والاكثر امانا وبعدا

(١) أ. أمين فرج يوسف. التوقيع الالكتروني. دار المطبوعات الجامعية. ٢٠٠٨ . ص ٦٩ وما بعدها.
(٢) المادة رقم ١ من القانون الاتحادي رقم (١) لسنة ٢٠٠٦ بشأن المعاملات والتجارة الإلكترونية

عن الاحتيال والتزوير[١] وتكمن صعوبته بفضل التقدم التقني في استخدام نظام التشفير بمفتاحين[٢].

على ان يتوافر لدى طالب الترخيص نظام لتحديد تاريخ ووقت إصدار الشهادات ، وإيقافها ، وتعليقها ، وإعادة تشغيلها، وإلغائها. وكذلك نظام للتحقق من الأشخاص المصدر لهم شهادات التصديق الإلكتروني ، والتحقق من صفاتهم المميزة وبالمقابل أن يتوافر لدى المرخص المتخصصون من ذوى الخبرة الحاصلين على المؤهلات الضرورية ونظام حفظ بيانات إنشاء التوقيع الإلكتروني وشهادات التصديق الإلكتروني طوال المدة التي تحددها الهيئة فى الترخيص[٣].

ثانيا: واجبات الموقع: المادة ٢: ١. يجب على الموقع:

أ. أن يمارس عناية معقولة لتفادي استخدام أداة توقيعه استخداماً غير مأذون .

ب. أن يخطر الأشخاص المعنيين بدون تأخير غير مبرر ، وذلك في حالة:

١- معرفة الموقعبأن أداة توقيعه تعرضت لما يثير الشبهة في درجة أمانها.

٢- دلالة الظروف المعروفة لديه على احتمال كبير بأن تكون أداة التوقيع قد تعرضت لما يثير الشبهة فيها.

ج. أن يمارس عناية معقولة لضمان دقة واكتمال كل ما يقدمه من بيانات وتصريحات جوهرية ذات صلة بالشهادة طيلة فترة سريانها ، وذلك في الحالات التي تستلزم فيها أداة التوقيع استخدام شهادة .

---

(١) ايمان مأمون أحمد سليمان، إبرام العقد الإلكتروني وإثباته، دار الجامعة الجديدة للنشرالإسكندرية، ٢٠٠٨. ص ٣٣٨.

(٢) د. ممدوح محمد علي ميروك. مدى حجية التوقيع الالكتروني في الاثبات. دار النهضة العربية. ٢٠٠٩. ص ٤٨.

(٣) د.عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، الحماية الجنائية لنظام التجارة الإلكترونية. دار الفكر الجامعي. الاسكندرية، ٢٠٠٤، ص ١٨٦ - ١٨٧.

ثالثا: المسؤولية المدنية لجهات التوثيق:

اعتمد التوجيه الاروبي مبدأ عاما يجعل فيه نظام التوثيق بالتوقيع الالكتروني اختياريا. اي ان كل ما يصدر من تراخيص تحدد الحقوق والالتزامات الخاصة بتوريد خدمة التوثيق بواسطة هيئة عامة او خاصة واحترامها ومراقبتها فيما اذا كان مقدم الخدمة غير مؤهل. حيث اصدر التوجيه الاوروبي قانون رقم ٩٣ لسنة ١٩٩٩ الخاص بالتوقيعات الإلكترونية الذي يهدف إلى توحيد قوانين الدول الأعضاء في الاتحاد الأوروبي، بحيث يجب عليهم إدخال القواعد القانونية التي ينص عليها ذلك التوجية في قوانينها. مما يعني ضرورة اتخاذ الدول الاعضاء الاجراءات اللازمة لادماج احكام التوجية الاوروبي في نصوصها خلال مدة اقصاها ثمانية عشر شهرا من تاريخ نفاذ ذاك التوجيه على الدول الاعضاء ان تعمل على اصدار النصوص التشريعية اللازمة للسماح بالقيام باعتماد التوقيع بشكل عام ومنها التوقيع الرقمي موضوع بحثنا باصدار شهادات مستوفية الشروط من التوثق من التوقيع وشخصه صاحب التوقيع وارتباطه بالمحرر ايضا[١] وتأمينه ضد اي تعديل او تحريف فيه. كما يجب ان يكون مقدم التوثيق مؤهلا لاصدار شهادات التوثيق وهذا ما بيناه سابقا من توافر الشروط الكفيلة لتحقق الامان في التوقيع بمواصفات تم اعتمادها وبعيدا عن الاحتيال[٢]. دون اي اخلال وبدونها اي بوجود الاخلال يترتب على ذلك مسؤولية[٣]. في دولة الامارات العربية

(١) د. سامح عبد الواحد التهامى، التعاقد عبر الإنترنت (دراسة مقارنة)، دار الكتب القانونية، مصر، ٢٠٠٨، ص ٤٧٥.

(٢) إبراهيم الدسوقي أبو الليل، التوقيع الإلكتروني ومدى حجيته في الإثبات (دراسة مقارنة)، بحث منشور في مجلة الحقوق، جامعة الكويت ، ملحق العدد ٢٠٠٥، ص ١٢٥.

(٣) سند حسن سالم. التنظيم القانوني للتوقيع الالكتروني وحجيته في الاثبات المدني. دار النهضة العربية. ٢٠١٠م. ص ٨٨.

المتحدة يوجد ٢٨٠ ألف منشأة تستفيد من الخدمة وتعتمد إلزامية التوقيع الإلكتروني بوزارة العمل تضمن دقة المعاملات والمسؤولية القانونية[١].

رابعا: مراقب خدمات التصديق: المادة ٢٣ :

١. لأغراض هذا القانون يعين الرئيس بقرار يصدره ، مراقباً لخدمات التصديق وعلى وجه الخصوص لأغراض ترخيص وتصديق ومراقبة أنشطة مزودي خدمات التصديق والإشراف عليها ، وينشر هذا القرار في الجريدة الرسمية .

٢. يجوز للمراقب أن يفوض كتابة اياً من مسؤولياته بموجب هذا الفصل لمن يراه .

٣. يعتبر المراقب أو المفوض من قبله موظفاً عاماً .

٤. على المفوض أن يبرز عند ممارسته اياً من الصلاحيات المخولة له واستجابة لطلب الشخص الذي يتصرف تجاهه ، ما يثبت الصلاحية التي خوله إياها المراقب

المطلب الثاني
الاثبات في التوقيع الرقمي

احتلت الكتابة من بين الادلة القانونية منزلة متقدمة وتحديدا في المسائل المدنية والتصرفات العقدية ، اما الاوراق غير الموقعة ، فانها ليست حجة بوجه عام. القواعد العامة في الاثبات في النظام القانوني لا تقبل اية مستندات او محررات غير

(١) للاستفادة من تلك الخدمة، الحصول على بطاقة التوقيع الالكتروني، للمنشآت المسجلة لديها والبالغ عددها نحو ٢٨٠ ألفاً، بما يتيح لأصحابها إتمام إجراءات الإلغاء على مدار الساعة وطوال أيام الأسبوع. انظر جريدة دار الخليج – العدد ليوم السبت١٢نوفمبر٢٠١١

موقعة من منظمها ، ولا تقبل الاحتجاج بالسندات العادية . ما لم يقر الخصم بها . الا عن طريق ابرازها من قبل منظمها. ويمكن ان يكون التوقيع قرينة في الاثبات سواء اكان موثقا او غير موثق[١]. ولا شك ان مبدأ حرية الاثبات تتيح للقاضي حرية تقدير ما يعرض عليه من قرائن[٢]. ومع تطور الوسائل التقنية المعلوماتية وتبادل البيانات التي تتصل بالذمة المالية وغيرها، عن طريق الانترنت وامام مسائل الإثبات فيما انتجته الحواسيب والشبكات من مخرجات ، وبحث مدى حجية مستخرجات الحاسوب والبريد الإلكتروني وقواعد البيانات المخزنة داخل النظم وغيرها . واستخدام وسائل تقنية المعلومات لاجراء التصرفات القانونية وتبادل البيانات واجراء عمليات تتصل بالذمة المالية اثار ويثير العديد من الاشكالات حول مدى اعتراف القانون . واظهرت التقنية تحديات قانونية تستلزم التنظيم بالنسبة لعقود تقنية المعلومات.

لقد اتجهت النظم القانونية والقضائية والفقهية بوجه عام الى قبول وسائل الاثبات التي توفر من حيث طبيعتها موثوقية في اثبات الواقعة وصلاحية للدليل محل الاحتجاج ، وتحقق فوق ذلك وظيفتين :. امكان حفظ المعلومات لغايات المراجعة عند التنازع ، التوسط في الاثبات عن طريق جهات الموثوقية الوسيطة او سلطات الشهادات التعاقدية ، ومن هنا قبل نظام (سويفت) التقني لغايات الحوالات البنكية . وكذا نظامي شيبس وشابس ونحوهما كما بينا سابقا. والتحديد القانوني للرّسائل الإلكترونيةِ والتوقيع الالكتروني تم تنظيمه في القانون الاماراتي ام لا.

حاول المشرع الاماراتي مواكبة التقدم التكنولوجي وتقنين موضوعات التجارة والمعاملات الالكترونية بقانون رقم (٢) لسنة ٢٠٠٢ بشأن المعاملات والتجارة

(١) د.عادل رمضان الأبيوكي، التوقيع الإلكتروني في التشريعات الخليجية (دراسة مقارنة)، المكتب الجامعي الحديث.الإسكندرية، ٢٠٠٩، ص ٤٣.

(٢) د. عبد السميع عبد الوهاب ابو الخير. الوجيز في قانون الاثبات. ٢٠٠٥. ص ٢٦٠.

الالكترونية والقانون الاتحادي رقم ١ لسنة ٢٠٠٦ الخاص بالمعاملات والتجارة الالكترونية. ايضا من قانون الاثبات الاتحادي رقم ٣٦ لسنة ٢٠٠٦.

ان استخدام السندات والعقود الالكترونية التي تفرض تقنية التوقيع الالكتروني، حتّم تدخل التشريعات الدولية والوطنية لتنظيم هذه المفاهيم الحديثة وبيان شروطها وآثارها. نذكر من تلك التشريعات:

القانون النموذجي حول التجارة الالكترونية الصادر عن لجنة القانون التجاري الدولي لدى الأمم المتحدة بموجب القرار رقم ١٦٢/٥١ تاريخ ١٩٩٦/١/١٦، الذي أقرَّ بالقوة الثبوتية للسند والتوقيع الالكترونيين[١].

مع نظرة مستقبلية لهيئة الإمارات للهوية[٢] على تفعيل تطبيق التوقيع الرقمي عبر الهواتف الذكية مستقبلا، ليشكل إضافة نوعية على أمن ومصداقية التعاملات والإجراءات الإلكترونية في القطاعين الحكومي والخاص على مستوى الدولة، وبما يدعم مشروع «الحكومة الذكية». وتعزم ايضا على إطلاق تطبيقات ٢٠ خدمة خاصة

(١) هناك اهتمام عالمي بهذا المجال منها البرلمان الاروبي الذي عمل على اكثر من مرة باصدار التوجيهات مثل التوجيه الصادر عن البرلمان الأوروبي بتاريخ ١٩٩٩/١٢/١٣ حول التوقيع الالكتروني وايضا أقرَّ البرلمان الأوروبي توجيهاً آخر بتاريخ ٢٠٠٠/٦/٨ حول التجارة الالكترونية والتأكيد على الاهتمام بتوقيع العقود بالطرق الالكترونية. وكذلك نلاحظ قانون الأونيسترال النموذجي بشأن التوقيعات الالكترونية، الذي اعتمدته لجنة القانون التجاري الدولي لدى الأمم المتحدة في دورتها ال٣٤ بتاريخ ٢٠٠١/٧/٥، لتنظيم التوقيع الالكتروني في سياق العلاقات ذات الطابع التجاري. ويعتبر هذا القانون قانوناً استرشادياً في مجاله، لكنه لا يتضمن كل التفاصيل المتعلقة بالتوقيع الالكتروني، بل يفسح المجال لإصدار قوانين خاصة به. وقد اقرت عدة دول قوانين خاصة بتنظيم التجارة الالكترونية والسندات والتواقيع الالكترونية ومنها دولة الامارات العربية ومملكة اسبانيا.

(٢) وقعت محاكم دبي وهيئة الإمارات للهوية مذكرة تفاهم، للاستفادة من تطبيقات بطاقة الهوية "الذكية"، وبناء علاقات شراكة فعالة بين الجانبين، لتحقيق الأهداف الاستراتيجية المشتركة، وتبادل المعلومات، والدراسات ذات العلاقة باختصاصات عمل كل منهما، والتنسيق في تنفيذ المشاريع المشتركة، بهدف ضمان حسن التنفيذ وسرعة الإنجاز.

بها عبر الهواتف الذكية قبل نهاية العام الجاري ٢٠١٤، والتنسيق مع بعض المؤسسات المزودة للحلول المصرفية في الدولة، على إحلال بطاقة الهوية الصادرة عنها بشكل تجريبي خلال العام، محل بعض (البطاقات) المستخدمة في التعاملات البنكية على نطاق واسع في الإمارات، و التنسيق متواصل ايضا مع مصرف الإمارات المركزي لإحلال بطاقة الهوية محل الوثائق التعريفية الأخرى التي تطلبها بعض المؤسسات المصرفية حالياً كشرط لإنجاز تعاملات بنكية محددة. وتسعى كذلك على دمج عديد من البطاقات التعريفية التي تستخدمها بعض مؤسسات الدولة في بطاقة الهوية، ومن بينها بطاقة العمل، وذلك وفقاً لما أعلنت عنه وزارة العمل، ورخصة القيادة التي سيتم الاستغناء عنها خلال النصف الثاني من العام المقبل، والاستعاضة عنها بإضافة رمز السواقة على بطاقة الهوية. وتعمل على الربط الإلكتروني مع خمس جهات حكومية رئيسة مسؤولة عن الواقعات المدنية في الدولة وعلى أن يتم الانتهاء من الربط مع تسع جهات أخرى خلال النصف الأول من العام المقبل. لذا فان إتاحة خدمة (التوقيع الرقمي) على المعاملات الإلكترونية تعتبر واحدة من مقومات جاهزية دولة الإمارات من حيث البنية التحتية اللازمة للتحول نحو الاقتصاد الرقمي الآمن والموثوق، الذي من شأنه إضفاء مصداقية تامة على أي معاملة إلكترونية ستتم في الدولة عبر الفضاء الرقمي، بما يحمي مصالح جميع أطراف العلاقة من مؤسسات وأفراد، وبما يحافظ على مصداقية وصحة الوثائق المرفقة، بالاستفادة من الخصائص المتقدمة لبطاقة الهوية والشهادات الرقمية[١] المتوفرة في الشريحة الذكية[٢]. وهنالك إجراءات التوثيق

(١) وهي عبارة عن ملف رقمي صغير مكون من بعض الحروف والأرقام والرموز الإلكترونية تخزن في الشريحة الذكية في بطاقات الهوية التي تصدرها هيئة الإمارات للهوية، وتحتوي الشهادات الرقمية على بعض المعلومات الشخصية وتاريخ ورقم الشهادة ومصدرها .

(٢) هيئة الإمارات للهوية، الدكتور المهندس علي محمد الخوري . الهوية تطلق التوقيع الرقمي عبر الهواتف الذكية للعام المقبل ٢٠١٤. جريدة دار الخليج . الأحد ٢٤ نوفمبر ٢٠١٣.

المحكمة وهي الإجراءات التي تهدف الى التحقق من أن رسالة الكترونية قد صدرت من أو إلى شخص معين، والكشف عن أي خطأ أو تعديل في محتويات أو في إرسال أو تخزين رسالة الكترونية أو سجل الكتروني خلال فترة زمنية محددة ويشمل ذلك أي إجراء يستخدم مناهج حسابية أو رموزاً أو كلمات أو أرقاماً تعريفية أو تشفيراً أو إجراءات للرد أو لإقرار الاستلام وغيرها من وسائل إجراءات حماية المعلومات[١].

اولا: مبدأ ثبوت التوقيع في الكتابة:كما هو معلوم ان التوقيع عنصر ضروري للاثبات وهو الحجة القانونية للورقة المكتوبة، وبها الزامية القاضي[٢]. ولكن التوقيع الرقمي يختلف نوعا وشكلا عن التوقيع التقليدي فبه لا بد من تأمين البيانات والحفاظ عليها وعلى سريتها وخصوصيتها والحفاظ على خصوصية صاحب البيانات Privacy كمنطلق طبيعي للحفاظ على الإنجازات في العالم الرقمي، بدون هذه الضمانات سوف يضعُف وينهار، ولهذا فإن علم أمن البيانات والشبكات Data and Network Security يسعى لتأمين البيانات أينما كانت ويعمل على تأمين ستة خدمات رئيسية وهي الحفاظ على الخصوصية Confidentiality (privacy

(وتأكيد التوثيق بأن مرسل الرسالة موثوق به Authentication والحفاظ على البيانات سليمه لا تعدل ولا تمس Data Integrity والحفاظ على أن لا ينكر سواء الراسل أو المستقبل إرساله أو إستقباله للرسالة Non.repudiations والحفاظ على الأجهزة والبرامج تعمل خلال خط التوصيل Control Access وأخيرا القدرة على منع فقد أو سقوط أي من عناصر منظومة الإتصال بين الراسل و Availability المستقبل. [٣]

---

(١) القانون الاتحادي رقم (١) لسنة ٢٠٠٦ بشأن المعاملات والتجارة الإلكترونية المادة رقم ١.

(٢) د. محمد السعيد رشدي. حجية وسائل الاتصال الحديثة في الاثبات. مطبعة النسر الذهبي. ص ٤٦.

(٣) دسمير حامد عبد العزيز الجمال. التعاقد عبر تقنيات الاتصال الحديثة. دار النهضة العربية. ٢٠٠٦. ص١٩٩.؛ د. علي عبد العالي خشان الاسدي. حجية الرسائل الالكترونية.

في الامارات، أكدت وزارة العمل أن بطاقة التوقيع الإلكتروني تتيح لمالك المنشأة أو المفوض عنه بالتوقيع الإلكتروني، والاستغناء عن التوقيع الكتابي وتمكينه من التوقيع على معاملاته المقدمة لوزارة العمل إلكترونياً.

يكون لهذا التوقيع الحجية القانونية الكاملة في الإثبات وذلك باستخدام بطاقة ذكية ومؤمنة[1]، وهي أداة إلكترونية خاصة لصاحبها ومخزنة على شريحة تتضمن رقماً سرياً بحيث يتم التوقيع إلكترونياً على المعاملات، مع اشتراط استخدام البصمة والرقم السري معاً أو الرقم السري فقط حسب اختيار مالك المنشأة عند تقديمه طلب التوقيع الإلكتروني في الوزارة .

وأوضحت الوزارة أنه تم إعداد وتصميم بطاقة التوقيع الإلكتروني لتوقيع المعاملات إلكترونيا وإرفاق الوثائق المطلوبة دون الحاجة إلى القدوم للوزارة، وهذا النظام مربوط آليا بنظام وزارة العمل ليوفر على المراجعين عملية توقيع المعاملات .

وأشارت إلى أن خدمة التوقيع الإلكتروني تقدم التسهيلات للمخولين بالتوقيع في تشغيل نظام المعاملات الإلكترونية، بتوفير عدد من الخدمات تتمثل في تحديد الصلاحيات للمستخدمين الحاليين من خلال إدارة العضوية، كذلك توقيع معاملات جديدة أو رفضها أو وضع ملاحظات عليها، فضلا عن عرض المعاملات الموقعة، وعرض

(١) التوقيع الإلكتروني المحمي نجده في المادة ٢٠(١. يعامل التوقيع على أنه توقيع إلكتروني محمي إذا كان من الممكن التحقق من خلال تطبيق إجراءات توثيق محكمة ، منصوص عليها في هذا القانون أو معقولة تجارياً ومتفق عليها بين الطرفين ، من أن التوقيع الإلكتروني كان في الوقت الذي تم فيه : أ. ينفرد به الشخص الذي استخدمه . ب. ومن الممكن أن يثبت هوية ذلك الشخص . ج. وأن يكون تحت سيطرته التامة سواء بالنسبة لإنشائه أو وسيلة استعماله وقت التوقيع . د. ويرتبط بالرسالة الإلكترونية ذات الصلة به بطريقة توفر تأكيداً يعول عليه حول سلامة التوقيع ، بحيث إذا تم تغيير السجل الإلكتروني فإن التوقيع الإلكتروني يصبح غير محمي .٢. على الرغم من أحكام المادة (٢١) من هذا القانون وما لم يثبت العكس، يعتبر الاعتماد على التوقيع الإلكتروني المحمي معقولاً).

المعـاملات المرفوضـة، والمعـاملات التـي تـم وضـع ملاحظـات عليهـا، والمعـاملات الموقوفة من قبل الوزارة، وكذلك الاستعلام عن حالـة المعاملـة فـي النظـام، والاستعلام عن وضع المنشأة في الوزارة، والمعاملات غير المصرح بإجرائها في منشأة معينة .

وذكرت أنه يمكن لصاحب البطاقة تغيير إعدادات النظـام بالطريقـة التـي تناسبه، وتمتـاز هذه الخاصـية مـن النظـام بإعطـاء المـستخدم الفرصـة لجعل النظـام يتكيـف مـع طريقة عمله مثل تعديل بيانـات الاشتراك، أو إيقـاف بطاقـة التوقيـع وكذلك تغيير الرقم السري .

وأشارت إلى أن فريق إدارة النظـام يعمـل علـى بنـاء قاعدة معلومـات فـي النظـام لإجابـة المـستخدمين علـى أيـة أسـئلة حـول كيفيـة عمـل النظـام أو الاسـتعلام عـن أي استمارة لدى الوزارة، ولذا تم وضـع قسم "الأسئلة الأكثر شيوعا" والتـي مـن خلالهـا ستطلع على أسئلة المستخدمين الآخرين مستفيدا بذلك من الإجابات والتوضيحات[1].

المادة ١٨ مـن قـانون الاثبـات الامـاراتي تـنص علـى انـه : ١. يجوز للخصم في الحالات التالية أن يطلب الزام خصمة بتقديم أى محررات أو أوراق منتجة تكون تحت يده. أ . اذا كـان القانون يجيز مطالبته بتقديمه أو تسليمه. ب . اذا كـان المحرر مشتركـا بينه وبين خصمه ويعتبر المحرر مشتركـا على الاخص اذا كـان لمصلحة الخصمين أو كان مثبتا لالتزاماتهما وحقوقهما المتبادلة. ج . اذا أستند اليه خصمه في أي مرحلة من مراحل الدعوى. ٢. ويجب أن يبين في هذا لطلب ، وصاف المحرر وفحواه ، والواقعة التي يستدل بها عليه والدلائل والظروف المؤيدة الموجودة تحت يد الخصم ،ووجه الزام الخصم بتقديمه.

(١) خالد عبدالعزيز. يمتلك الحجية القانونية الكاملة في الإثبات. "العمل": بطاقة التوقيع الإلكتروني تسمح لمالك المنشأة أو المفوض عنه بالاستغناء عن التوقيع الكتابي. جريدة دار الخليج . الأحد ٦ ديسمبر ٢٠٠٩.

ثانيا: **ما يحول دون الحصول على دليل كتابي**: لا تعد الكتابة من الناحية القانونية دليلاً كاملاً في الاثبات إلا إذا كانت موقعة في صورة إمضاء أو ختم أو بصمة. ومع ان إنتشار الحاسب الآلي والإعتماد عليه في كافة مناحي الحياة بصورة شبه كلية أوجد طرق ووسائل حديثة في التعامل. مع إنتشار نظم معالجة المعلومات رقمياً في ادارات الدولة، الشركات، الادارات والبنوك لم يترك مجالاً للإجراءات اليدوية. وكانت النتيجة بالتالي ان أصبح التوقيع اليدوي عقبة من المستحيل تكيفها مع النظم الحديثة للادارة والمحاسبة وتم إستبداله بالتوقيع الالكتروني والعالم يستشرف عصر الحكومات الالكترونية. من هنا كان منشاؤه قانون القانون الاتحادي رقم (١) لسنة ٢٠٠٦ بشأن المعاملات والتجارة الإلكترونية.

وما يعني ان الاثبات يكون دائما عن طريق الكتابة وهذا هو المعتاد ولكن هناك ما يعني بوجود حائل يمنع من الحصول على الدليل الكتابي اي المانع سواء كان المادي منها من خلال ظروف لم تجعل لاحد من الحصول على الدليل الكتابي لاثبات التصرف القانون الذي تم عمله من كلاهما او من احدهما، او المعنوي الذي يكون بالنسبة لنا ليس ملموسا بل يرجع الى سلطة القاضي في حالات ما لاثبات التصرف من عدمه[١]. وكذلك بسبب الاستحالة التي ترجع الى ظروف خاصة سواء كانت شخصية او نسبية .

ولضمان الاثبات في علمية التفشير الخاصة بالتوقيع الالكتروني، فقد وجدت الحاجة إلى طرف ثالث يكون محل ثقة الأفراد، ويتمثل في هيئة مختصة يكون لها سلطة إنشاء وتوثيق التوقيع الالكتروني. هذا الطرف المحايد أو الهيئة المختصة أوجده قانون المعاملات الالكترونية لسنة ٢٠٠٧ وسماه اللجنة الوطنية للمصادقة الالكترونية.

(١) د. سند حسن سالم. التنظيم القانوني للتوقيع الالكتروني وحجيته في الاثبات المدني. دار النهضة العربية. ٢٠١٠م. ص ١٤٥.

التي كان لها الدور الأساسي والرئيسي في إضفاء المصداقية على منظومة التوقيع الالكتروني وذلك بإصدار شهادة المصادقة عنه. عليه فإن من أهم المهام التي تقوم به إدارات اللجنة القومية للمصادقة الالكترونية وذلك بكل الطرق الامنة[1].

الخاتمة والتوصيات :

١. الاستمرار في تفعيل التوقيع الرقمي الإلكتروني على كافة الدوائر في الدولة. ونشر الثقافة الالكترونية على مدى اكبر بايجاد محاضرين وخبراء متخصصين.

٢. تحقيق اكبر قدر بين الافراد والمؤسسات العامة والخاصة لتحقيق التكاملية والسرية والسرعة والثقة في انجاز المعاملات الالكترونية بسلاسة وسهولة .

٣. تعميم والزامية حصول كل مواطن ومقيم على ارض الامارات العربية المتحدة على توقيع رقمي إلكتروني مسجل وخاص به وموثق لدى الدولة. وكذلك وبالمقابل ان يكون لاي موسسة توقيعها الخاص بها.

٤. ومن ثم لا بد من سن القوانين المنظمة للعمليات الإلكترونية والوقاية من التزوير والاحتيال على استخدام التوقيع الالكتروني. وخلق ضمانات لمستخدمي التوقيع الالكتروني بحيث يعطي الحق للمستخدم بتغيير التوقيع الرقمي الإلكتروني لزيادة الأمن والحماية.

(١) د. سامح عبد الواحد التهامى، التعاقد عبر الإنترنت (دراسة مقارنة)، دار الكتب القانونية، مصر، ٢٠٠٨، ص ٤٧٥.

المراجع

المراجع العربية

- أ. أمين فرج يوسف. التوقيع الالكتروني. دار المطبوعات الجامعية. ٢٠٠٨
- د. ايمان مأمون أحمد سليمان، إبرام العقد الإلكتروني وإثباته، دار الجامعة الجديدة للنشر. الإسكندرية، ٢٠٠٨.
- د. سند حسن سالم. التنظيم القانوني للتوقيع الالكتروني وحجيته في الاثبات المدني. دار النهضة العربية. ٢٠١٠م.
- د. عبد السميع عبد الوهاب ابو الخير. الوجيز في قانون الاثبات. مكتبة وهبة. ٢٠٠٥.
- د. علي عبد العالي خشان الاسدي. حجية الرسائل الالكترونية. ٢٠١٠م
- د. علي محمد أحمد أبو العز، التجارة الإلكترونية وأحكامها في الفقه الإسلامي. دار النفائس للنشر والتوزيع، الأردن. ٢٠٠٨ .
- د. فادي عماد الدين توكل، عقد التجارة الإلكترونية، منشورات الحلبي الحقوقية، بيروت، ٢٠١٠
- د. محمد السعيد رشدي. حجية وسائل الاتصال الحديثة في الاثبات. مطبعة النسر الذهبي.
- د. محمود عبد االرحيم االشريفات، التراضي في تكوين العقد عبر الإنترنت، دار الثقافة. عمان، ٢٠٠٩.

- د.أسامة أحمد شوقي المليجي، استخدام مستخرجات التقنيات العلمية الحديثة وأثره على قواعد الإثبات المدني، دار النهضة العربية، القاهرة، ٢٠٠٠.
- د.حسن عبد الباسط جميعى.اثبات التصرفات القانونية التى يتم ابرامها عن طريق الانترنت. دار النهضة العربية. القاهرة.طبع ٢٠٠٠.
- د.سعيد السيد قنديل، التوقيع الالكتروني. ماهيته، صوره، حجيته في الإثبات بين التداول والاقتباس. دار الجامعة الجديدة. الإسكندرية. الطبعة الثانية، ٢٠٠٦.
- د.سليمان مرقص.الوافي في شرح القانون المدنى.الجزء الثانى –المجلد الأول.نظرية العقد.الطبعة الرابعة. سنة ١٩٨٧.
- د.عادل رمضان الأبيوكي، التوقيع الإلكتروني في التشريعات الخليجية (دراسة مقارنة)، المكتب الجامعي الحديث.الإسكندرية، ٢٠٠٩.
- د.عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، الحماية الجنائية لنظام التجارة الإلكترونية. دار الفكر الجامعي. الاسكندرية، ٢٠٠٤.
- د.عمر حسن المومنى. التوقيع الالكترونى وقانون التجارة الالكرونية. دار وائل للنشر. الطبعة الأولى. عمان. ٢٠٠٣ .
- د.مفلح القضاة. قانون البينات في المواد المدنية والتجارية. عمان. الطبعة١. دار الثقافة للنشر والتوزيع. ١٩٩٠.
- د. سمير حامد عبد العزيز الجمال. التعاقد عبر تقنيات الاتصال الحديثة. دار النهضة العربية. ٢٠٠٦. ص١٩٩.

المراجع الاسبانية

- Martínez Nadal، Comentarios a la ley de firma electrónica، Thomson Reuters، 2009.
- Diffie، W.، and Hellman، M. "Privacy and Authentication: An Introduction to Cryptography." Proceeding of the IEEE، March 1979.

الرسائل والبحوث والمجلات:

- د علي محمد الخوري . الهوية تطلق التوقيع الرقمي عبر الهواتف الذكية للعام المقبل ٢٠١٤. جريدة دار الخليج . الأحد٢٤ نوفمبر٢٠١٣.
- محمد البقيرات. مديرية التشغيل والخدمات المعلوماتية. دائرة التوقيع الرقمي. الهيئة الوطنية لخدمات الشبكة.
- http://windows.microsoft.com/ar.xm/windows.live/mail.create.signature
- http://www.albayan.ae/across.the.uae/news.and.reports/2013.09.17.1.1961343
- أشرف صلاح الدين، أساسيات التخزين الرقمي ، ورقة عمل غير منشورة مقدمة لندوة المفاهيم الأساسية للمعاملات القانونية والاقتصادية عبر الانترنت ، شرم الشيخ ، ٢٥ – ٢٩ ديسمبر ٢٠٠٥.
- جريدة دار الخليج – العدد ليوم السبت١٢نوفمبر٢٠١١.
- جريدة دار الخليج –الامارات. السبت١٣يوليو٢٠١٣.

- د. إبراهيم الدسوقي أبو الليل،التوقيع الإلكتروني ومدى حجيته في الإثبات (دراسة مقارنة)، بحث منشور في مجلة الحقوق، جامعة الكويت ، ملحق العدد ٢٠٠٥.
- د. أحمد شرف الدين،عقود التجارة الالكترونية. دروس دكتوراه كلية الحقوق. جامعة عين شمس. القاهرة. سنة ٢٠٠٠.
- د. خالد عبدالعزيز. يمتلك الحجية القانونية الكاملة في الإثبات. "العمل": بطاقة التوقيع الإلكتروني تسمح لمالك المنشأة أو المفوض عنه بالاستغناء عن التوقيع الكتابي. جريدة دار الخليج . الأحد ٦ ديسمبر ٢٠٠٩.
- د. رامي محمد علوان.التعبير عن الارادة عبر الانترنت. بحث مقدم الى نقابة المحاميين.عمان سنة ٢٠٠١،
- د. عايض المري. رسالة دكتوراه غير منشورة. جامعة القاهرة. كلية الحقوق. مدى حجية التكنولوجيا الحديثة في اثبات العقود التجارية. ٢٠٠٣.
- د. علي هادي العبيدي.قواعد إسناد الرسالة الإلكترونية إلى المنشئ قانون المعاملات والتجارة الإلكترونية الإمارات. بحث منشور في مجلة الشريعة والقانون. السنة السلبعة والعشرون. العدد الرابع والخمسون. ٢٠١٣.
- د.رامي محمد علوان،التعبير عن الإرادة عن طريق الإنترنت، وإثبات التعاقد الإلكتروني، مجلة الحقوق، جامعة الكويت، العدد الرابع،،٢٠٠٢ .
- م. عبدالملك رحال. مجلة رسالة الجامعة.

http://rs.ksu.edu.sa/69418.html

- مذكرة تفاهم بين محاكم دبي وهيئة الإمارات للهوية ، للاستفادة من تطبيقات بطاقة الهوية "الذكية". 02/01/2014.

http://wam.org.ae/ar/news/emirates/1395240171217.html

- المركز الوطني للتصديق الرقمي. وزارة الاتصالات وتقنية المعلومات. مجمع الملك عبدالعزيز للاتصالات – الرياض. المملكة العربية السعودية. http://www.ncdc.gov.sa/faqs
- وثائق الاونسترال –الدورة السابعة.فيينا.لعام ٢٠٠٠. مذكرة في الامانة الجمعية العامة للأمم المتحدة.

القوانين:

- قانون المعاملات الالكترونية الاماراتي. رقم (٥) لسنة ١٩٨٥م.
- قانون المعاملات والتجارة الالكترونية الاماراتي رقم (١) لسنة ٢٠٠٦م.
- القانون الالكتروني الاسباني 59/2003.
- قانون الأونيسترال النموذجي بشأن التوقيعات الالكترونية، الذي اعتمدته لجنة القانون التجاري الدولي لدى الأمم المتحدة في دورتها ال٣٤ بتاريخ ٧/٥/
- التوجيه الصادر عن البرلمان الأوروبي بتاريخ ١٩٩٩/١٢/١٣ حول التوقيع الالكتروني.
- التوجيه الصادر عن البرلمان الأوروبي بتاريخ ٢٠٠٠/٦/٨ حول التجارة الالكترونية .