التوقيع الإلكتروني.

بكوش خميسي

مقدمة:

لقد لفت انتباهي و انا بصدد تفحص مختلف المقالات التي تم نشرها بالعدد صفر من هذه المجلة ذلك المقال الذي أعد من طرف زميلي المحترم الأستاذ خلفي عبد الرحمان تحت عنوان: " الإنترنت و القانون" و الذي تناول بموجبه مختلف العراقيل التي تواجه التنظيم القانوني لشبكة الانترنت، ومن بين تلك التي أشار إليها صاحب المقال العراقيل المتعلقة بالإثبات.

فلا شك أن التطور الحاصل في عالم الاتصالات في العشريتين الاخيرتين من القرن العشرين، واقصد تلك الثورة الناجمة عن طغيان وسائل الاتصال الحديثة المتمخضة أساسا عن دمج المعلومات بالاعلام الآلي، أدى الى ظهور تقنيات غاية في الحداثة - أذكر على سبيل المثال تلك المعروفة برسائل البيانات الإلكترونية [1] و التي سمحت بإجراء المبادلات و إبرام العقود مدنية كانت أو تجارية عن طريق وسائط إلكترونية دون اللجوء إلى استعمال الدعامات الورقية، الأمر الذي سمح بربح الوقت و اقتصار المسافات في آن واحد.

و إذا كان هذا النوع من التعامل يفرض بطبيعته معلوماتية كل مبادلة[2]، فإنه يؤدي إلى إلغاء كل إمكانية للحديث عن المستندات أو المحررات بالمفهوم التقليدي لهذين المصطلحين، إذ استبدلت هذه الأخيرة بدعائم إلكترونية.

غير أن تطور التجارة الإلكترونية بقي منذ بوادر نشأتها رهن وجود ضمانات كافية تسمح بتبادل الرسائل الالكترونية ودفع الثمن بطريقة آمنة. ولذلك فقد ساد التخوف من الخوض في غمار هذا النوع من التجارة الذي ظل بحكم العادات المتواترة في عالم التجارة و الذهنية السائدة لدى أغلب التجار تصرفا مجهول العواقب، إلا أن ابتدع التقنيون ما يعرف حاليا بالتوقيع الالكتروني، وهو الوسيلة التي أزالت التخوفات المذكورة أعلاه، باعتبار أن الضمانات المطلوبة صارت متوفرة في ظل هذه التقنية المتطورة، ذلك أنه صار من السهل عن طريق التوقيع الرقمي ضمان وحدة **intégrité** و أصالة **authenticité** وسرية **confidentialité** الرسالة الالكترونية.

و إذا كان الوضع على ما هو عليه أعلاه من الناحية العملية، فإنه من الناحية القانونية قد أحدث ثورة - إن صح التعبير - في مجال الإثبات، إذ أن القواعد القانونية التقليدية لم تعد بإمكانها التصدي للإشكالات القانونية التي أفرزتها هذه التقنية. ولذلك فإن مختلف الدول على اختلاف أنظمتها القانونية قد عكفت على تبني نصوص قانونية مستقلة تناولت بموجبها التوقيع الالكتروني أو عدلت القواعد القانونية التقليدية بحيث أدمجت نصوص جديدة على نحو أزال الإشكالات القانونية المترتبة عنه.3

أ أما على المستوى الدولي فإن لجنة الأمم المتحدة للقانون التجاري الدولي كانت السباقة في هذا الميدان، إذ أنها تبنت بتاريخ 2001/12/12 وبموجب قرارها المتخذ في الدورة السادسة والخمسون القانون النموذجي بشأن التوقيعات الإلكترونية4. وهو جملة من القواعد غير الملزمة يمكن للدول أعضاء منظمة الأمم المتحدة أن تسترشد بها لتبني قواعد قانونية داخلية حول التوقيع الإلكتروني وذلك في محاولة من اللجنة لتوحيد القانون التجاري الدولي.

ولذلك سأحاول في هذا المقال أن أتناول التوقيع الإلكتروني كتقنية حديثة لتوقيع الرسائل الإلكترونية. ونظرا لتشعب الموضوع فقد ارتأيت أن يقسم الموضوع إلى قسمين:

الأول يتضمن دراسة التوقيع الإلكتروني من الناحية التقنية فقط، والثاني يخصص للجانب القانوني الذي سيكون محل بحث في العدد القادم. - بحول الله -.

الجوانب التقنية المتعلقة بالتوقيع الإلكتروني

إن الحديث عن حجية التوقيع الإلكتروني في الاثبات والشروط اللازم توفرها فيه ليصلح لآداء الوظيفة المنوطة به، يستدعي باديء ذي بدء فهم التوقيع الإلكتروني من الناحية التقنية. و أقصد بذلك أن يفهم كيف يتم عمليا خلق توقيع إلكتروني، و كيف توقع رسالة الكترونية، و كيف يتحقق المرسل اليه من أن الرسالة التي تلقاها موقعة من طرف المرسل. ونظرا لان التوقيع الإلكتروني يحتاج لتدخل طرف ثالث غير المرسل و المرسل إليه يدعى مقدم خدمات التصديق[5]، فإن الأمر يستدعي بحث هيكلة هذا الطرف ووظيفته.

وأخيرا نختم الحديث عن الجانب التقني بموجز مبسط يبين كيفية استعمال التوقيع الإلكتروني.

أولا: المصطلحات المتعلقة بالتوقيع الإلكتروني:

- التشفير.
- المفتاح الخاص و المفتاح العام.
- وظيفة المراقب.
- خلق التوقيع الإلكتروني.
- تحقيق التوقيع الإلكتروني.

ثانيا: هيكلة مفاتيح التشفير وسلطات التوثيق.

ثالثا: ملخص الإجراءات التقنية لخلق التوقيع الإلكتروني.

أولا: المصطلحات المتعلقة بالتوقيع الإلكتروني:

توجد عمليا عدة تقنيات للتوقيع الإلكتروني. فهناك من التقنيات ما يسمح بتوقيع رسالة إلكترونية بموجب مفتاح واحد يستعمل في نفس الوقت من طرف المرسل لتشفير الرسالة وتوقيعها كما يستعمل نفس المفتاح من المرسل إليه لفك التشفير. وعلى ذلك ولضمان سرية الرسالة يتعين الإبقاء على المفتاح سريا بين الطرفين.

المشكل الذي تثيره هذه الطريقة يكمن في كيفية إرسال المفتاح للمرسل إليه بطريقة آمنة. بحيث أنه لا توجد قنوات آمنة بالقدر اللازم تسمح بتمكين المرسل إليه من المفتاح الأمر الذي يجعل فرص القرصنة المعلوماتية وتزوير المفتاح أو فك الرسالة كثيرة الوقوع6.

أما الطريقة الثانية فهي التي تعتمد على زوج من المفاتيح، الأول سري والثاني مفتاح عام وتسمى بطريقة التشفير التناظرية la cryptographie asymétrique وهي الطريقة الأكثر أمنا واستعمالا. وعلى هذا الأساس سأركز على شرح هذه الأخيرة دون الأولى.

إن وضع توقيع إلكتروني حيز التطبيق بموجب الطريقة الثانية يستند أساسا إلى مبدأين محوريين:

- مبدأ تقني يعتمد على مفاتيح تدعى بمفاتيح التشفير Les clés cryptographiques .
- مبدأ تنظيمي يستدعي تدخل طرف ثالث لتحقيق التوقيع يدعى سلطات التوثيق أو مقدم خدمات التصديق les prestataires de services de certification

1- المبدأ التقني:

إن الالمام بمسألة خلق التوقيع الإلكتروني يستدعي التطرق لمختلف المصطلحات الخاصة بالتوقيع الإلكتروني وهو ما نوضحه أدناه:

التشفير la cryptologie : إن خلق التوقيع الالكتروني من وجهة نظر تقنية يستند الى أنظمة معلوماتية تعرف بأنظمة التشفير التناظرية les cryptosystèmes asymétriques ، وهي عبارة عن أنظمة تستعمل كقاعدة محورية ما يعرف بالتشفير، وهو فرع من الرياضيات يعتمد على جملة من الوسائل والبرامج المعلوماتية لتحويل المعطيات من حالتها الأصلية الى مظهر غير واضح أو غير مقروء من قبل الغير، لكنه في نفس الوقت يسمح بإعادة هذا المظهر إلى حالته الأصلية من طرف صاحب المعطيات والمرسل إليه فقط، وذلك باستعمال لوغريتميات تعرف بالتناظرية des algorithmes asymétriques لخلق زوج من المفاتيح [7] une paire de clés . تتألف هذه المفاتيح من عدد من الأرقام قد يصل إلى 31 رقما أو أكثر. وللحصول على هذا الزوج من المفاتيح تستعمل اللوغريتميات المذكورة أعلاه وجملة من العمليات الحسابية التي تستند إلى الأعداد الأولية les nombres premiers بحيث يتم ضرب عددين أوليين مثلا 127 و 997 ليتم الحصول على عدد أكبر و هو 619126. وإذا كان من السهل انطلاقا من هذين العددين معرفة حاصل عملية الضرب بواسطة اللوغرتميات أعلاه، فإنه يستحيل مطلقا انطلاقا من العدد الأكبر أي من 619126 معرفة العددين الأوليين الذين استعملا أي 127 أو 997 [8].

وبتطبيق هذه النظرية الرياضية المعروفة بنظرية أولير le théorème d'EULER يكون المبدأ كالتالي:

يتم تشفير الرسالة وتوقيعها بواسطة المفتاح الخاص للسيد "أ" الذي نسميه المفتاح x . تتم مراقبة التوقيع بواسطة المفتاح العام للسيد "أ" الذي نسميه المفتاح y أنه يستحيل انطلاقا من المفتاح y معرفة المفتاح x لتقليد توقيع السيد " أ"[9]. وكما يقول التقنيون في الإعلام الآلي فإن تقليد مفتاح خاص مؤلف من 31 رقما يستدعي على الأقل إجراء احتمالات بعدد حبات رمل صحراء. ويزيد الأمر تعقيدا واستحالة إذا كان المفتاح عبارة عن ترقيم يصل الى 50 رقما، إذ لابد من إجراء ملايير من الاحتمالات للوصول إلى المفتاح الخاص في زمن معقول [10]

المفتاح الخاص والمفتاح العام: رأينا أعلاه وضع توقيع إلكتروني حيز التطبيق يحتاج إلى زوج من المفاتيح.

المقصود بتحقيق التوقيع الإلكتروني تلك العملية التي تمكن من التأكد من أن التوقيع الإلكتروني المستعمل بالرجوع إلى الرسالة الأصلية و المفتاح العام هو التوقيع الذي تم خلقه من اجل نفس الرسالة و بواسطة المفتاح الخاص المقابل للمفتاح العام. ثقنيا يتم تحقيق التوقيع من طرف المرسل اليه الذي يقوم بحساب نتيجة مراقبة الرسالة الاصلية من جديد بمعرفته الخاصة و ذلك باستعمال نفس وظيفة المراقبة التي استعملها المرسل. ثم باستعمال المفتاح العام و نتيجة المراقبة المتحصل عليها يتحقق المرسل اليه من أن التوقيع الالكتروني قد استعمل بواسطة نفس المفتاح الخاص المقابل للمفتاح العام للمرسل، و أن نتيجة المراقبة المتوصل اليها بعد الحساب الذي أجراه المرسل اليه نفسها تلك المستعملة في خلق التوقيع الالكتروني.

الأول مفتاح خاص يستعمل لخلق التوقيع الإلكتروني وتشفير الرسالة، و الثاني مفتاح عام يستعمل من طرف المرسل اليه لتحقيق - مظاهاة- التوقيع الإلكتروني.

وإذا كان المفتاح الخاص ينبغي أن يتسم بطابع السرية أي أن يحفظ بطريقة آمنة لدى المرسل موقع الرسالة الإلكترونية، فإن تحقيق التوقيع الإلكتروني يستدعي وضع المفتاح العام في متناول الجميع أو على الأقل في متناول الأشخاص الذين وجهت إليهم رسالة موقعة الكترونيا بالمفتاح الخاص . على هذا الأساس جرت العادة أن تنشر قائمة المفاتيح العامة للجمهور في فهارس رقمية معدة خصيصا لذلك من قبل مقدمي خدمات التصديق كما سنوضحه لاحقا[11] . وإذا كانت هناك علاقة وطيدة بين المفاتيحين كما شرحنا أعلاه باعتبار انهما خلقا باستعمال نفس اللوغاريتم الرياضي، فإن الأنظمة المعلوماتية المتاحة حاليا للتشفير تعدو كل امكانية للتعارف على المفتاح الخاص انطلاقا من المفتاح العام و هكذا اذا كان في امكان الجميع معرفة المفتاح العام لأي شخص بالاطلاع فقط على شهادة التصديق ، فانه يستحيل في وقت معقول التعرف على المفتاح الخاص المفتاح الخاص لهذا الشخص و من ثمة تقليد توقيعه الالكتروني.

وظيفة المراقبة : la fonction contrôle بالإضافة إلى المفاتيحين العام و الخاص يحتاج التوقيع الإلكتروني الى اجراء جوهري اخر وهو ما يعرف بوظيفة المراقبة هذا الإجراء يؤدي وظيفتين في ان واحد إذ أنه يدخل كإجراء لخلق التوقيع الالكتروني" وسنرى ادناه كيف يتحقق ذلك" ويستعمل من جهة ثانية لتحقيق التوقيع الإلكتروني. و المقصود بعملية المراقبة عملية رياضية

une équation mathématique تستند بدورها إلى لوغاريتم رياضي يؤدي تطبيقه على الرسالة الإلكترونية إلى خلق مختصر للرسالة يسمى تقنيا بالرسالة المختصرة **le message abrégé** أو بصمة الرسالة **l'empreinte**" هذه الرسالة المختصرة هي نتاج عملية المراقبة التي يجريها المرسل قبل توقيع الرسالة، وإذا كان برنامج التشفير المستعمل ناجعا فإن مختصر الرسالة لا يمكن إلا أن يكون وحيدا **"unique"** بحيث إذا طرأ أي تغيير على محتوى الرسالة فإن استعمال نفس وظيفة المراقبة بالاستناد إلى نفس اللوغاريتم سيؤدي لا محالة إلى نتيجة مراقبة مغايرة تماما، وبالتبعية رسالة مغايرة لتلك التي أجراها المرسل. وهكذا يمكن للمرسل إليه أن يتحقق أن الرسالة الموقعة لم يطرأ عليها أي تغيير[12] مع الملاحظة أن هذه الرسالة المختصرة التي هي نتاج عملية المراقبة تدمج مع الرسالة الأصلية لترسل في ان واحد.

كيفية خلق التوقيع الإلكتروني:

لخلق التوقيع الإلكتروني يقوم المرسل صاحب المفتاح الخاص أولا وقبل كل شيء بتحديد وحصر الرسالة الإلكترونية، ثم باستعمال وظيفة المراقبة المذكورة أعلاه يقوم بحساب نتيجة المراقبة أو الرسالة المختصرة، وهذا طبعا باستعمال النظام المعلوماتي المسمى أعلاه بنظام التشفير. ثم يقوم النظام المعلوماتي عن طريق استعمال نتيجة المراقبة و المفتاح الخاص معا بخلق التوقيع الإلكتروني، بحيث يكون التوقيع نتاج تحويل نتيجة المراقبة باستعمال المفتاح الخاص عن طريق اللوغريتمات الخاصة بالتشفير[13].

ويكون التوقيع الإلكتروني مخصصا فقط لهذه الرسالة و المفتاح الخاص، أو لعبارة أخرى فإن الرسالة الأصلية ورسالتها المختصرة و التوقيع الإلكتروني يكونون معا وحدة واحدة، بحيث يتدمج التوقيع بالرسالة الإلكترونية. إذا كان من الممكن فصل التوقيع عن الرسالة فهذا يعني ببساطة أن النظام المستعمل لخلق التوقيع الإلكتروني غير محدد[15] تحقيق "مظاهاة" التوقيع الإلكتروني. المقصود بتحقيق التوقيع الإلكتروني تلك العملية التي تمكن من التأكد من أن التوقيع الإلكتروني المستعمل بالرجوع إلى الرسالة الأصلية و المفتاح العام هو التوقيع الذي تم خلقه من أجل نفس الرسالة و بواسطة المفتاح الخاص المقابل للمفتاح العام.[16] تقنيا يتم تحقيق التوقيع من طرف المرسل اليه الذي يقوم بحساب نتيجة مراقبة الرسالة الأصلية من جديد بمعرفته الخاصة و ذلك باستعمال نفس وظيفة المراقبة التي استعملها المرسل (لأن الرسالة المرسلة تتضمن حتما نفس اللوغاريتم الذي استعمله المرسل لحساب نتيجة المراقبة) ثم باستعمال المفتاح العام و نتيجة المراقبة المتحصل عليها يتحقق المرسل اليه من أن التوقيع الإلكتروني قد استعمل بواسطة نفس المفتاح الخاص المقابل للمفتاح العام للمرسل، و أن نتيجة المراقبة المتوصل اليها بعد الحساب الذي اجراه المرسل اليه هي نفسها تلك المستعملة في خلق التوقيع الإلكتروني.[17]

ولكي تتحقق الغاية المرجوة من عملية المظاهاة لا بد من تحقق أمرين أساسين:

- أن المفتاح الخاص قد استعمل لخلق التوقيع الإلكتروني الموضوع على الرسالة الإلكترونية، وهذا الأمر لا يتحقق إلا إذا كان المفتاح العام لا يسمح إلا بمراقبة التوقيع الذي تم خلقه بالمفتاح الخاص المقابل.

- أن الرسالة الأصلية لم يطرأ عليها أي تغيير أو تحريف وهو الأمر الذي يتحقق إذا كانت نتيجة المراقبة المتوصل إليها من طرف المرسل إليه باستعمال نفس عملية المراقبة هي نفسها تلك التي استعملت لخلق التوقيع الإلكتروني.

ثانيا: هيكلة المفتاح العام ومقدمي خدمات التصديق:

رأينا أن تحقيق التوقيع الإلكتروني يحتاج إلى الحصول على المفتاح العام للموقع والتأكد من هذا المفتاح العام بقابل المفتاح الخاص الذي استعمل لخلق التوقيع الإلكتروني.

ولقد رأينا عند التطرق إلى شرح كيفية خلق المفتاحين أنه لا توجد من الناحية التقنية أي وسيلة ربط بين هذا الزوج من المفاتيح وشخص معين سواء كان طبيعيا أو معنويا، إذ أن الأمر يتعلق بمفتاحين دون إمكانية نسبتهما لشخص معين الأمر الذي يطرح التساؤل التالي: كيف يمكن تبادل المفاتيح العامة بطريقة آمنة؟ ثم كيف يمكن للمرسل إليه أن يعرف أن المفتاح العام هو ملك للشخص موقع الرسالة الإلكترونية؟ إن الإجابة على هذا التساؤل في ظل الأنظمة المغلقة بسيطة ولا تثير أي إشكال، إذ أن تبادل الرسائل الإلكترونية يتم بين الأشخاص المنخرطين في النظام فقط، ومن ثمة فإن النظام المغلق يسمح بتبادل المفاتيح بشكل آمن. كما أن الأنظمة المغلقة عادة ما تتحقق عند قبول الانخراط من هوية المنخرط وفي حالة منحت مفتاحا عاما فإنها تكن مسئولة عن أي خطأ.

غير أن الأمر ليس بهذه السهولة في ظل أنظمة الاتصال المفتوحة كالويب إذ أن النظام المفتوح معرض للقرصنة المعلوماتية الأمر الذي يصعب معه إرسال المفاتيح العامة دون أن تكون عرضة للتقليد أو القرصنة.

ولما كان الحال كذلك، فقد كان حتما على التقنيين إيجاد ميكانيزم يسمح أو لا بنسبة المفاتيح لشخص معين وثانيا إعلام الغير بالمفاتيح العامة وهو على يقين أن هذه المفاتيح لم تكن عرضة للتقليد ولذلك فقد وفر العمل الميداني حلا يمكن في تدخل طرف ثالث يكون محل ثقة تسند له مهمة نسبة المفتاح لشخص محدد، وهو الطرف الذي اصطلح عليه بمقدم خدمات التصديق

le prestataire de service de certification أو سلطات التوثيق.[18]

أ- هيكلة المفتاح العام: تتدو عملية تنظيم المفاتيح العامة و تأطيرها جد هامة و تحقق جملة من الأغراض يمكن أن نذكر منها:

ولكي تكتسب شهادة التصديق الحجية المنوطة بها أعلاه، يجب ان تكون ممهورة بالتوقيع الإلكتروني للسلطة مصدرة الشهادة. هذا التوقيع يمكن أن يكون محل تحقيق عن طريق مراقبة المفتاح العام للسلطة مصدرة الشهادة و ذلك عن طريق شهادة تصدرها سلطة توثيق أخرى، و بدورها هذه الأخيرة يمكن أن تكون محل تحقيق بنفس الطريقة، و هكذا يمكن للشخص المرسل اليه أن يتحقق في كل مرة من التوقيع بتحقيق التوقيع الالكتروني لكل سلطة مصدرة لشهادة التصديق.

- ضمان عدم وقوع المفتاح العام محل تقليد أو تحريف.
- ضمان مقابلة المفتاح العام للمفتاح الخاص الذي كان وسيلة للتوقيع.
- ضمان سلامة التقنيات المستعملة للترقيم.

و في سبيل تحقيق هذه الأغراض يقدم متعهدي خدمات التصديق جملة من الخدمات منها:

- تبادل المفاتيح العامة بين المستعملين.
- نشر فهرس الكتروني بقائمة المفاتيح العامة.
- نشر شهادات التصديق التي تبين أن المفتاح العام منسوب لشخص معين أو أنه يقابل مفتاحه الخاص.
- تحقيق هوية أصحاب المفاتيح العامة[19].

ولكي تؤدي هذه الجهات مهمتها فإن الأنظمة المعتمدة في الدول الأوروبية، أمريكا على سبيل الخصوص تنتم هيكلتها طبقا لقاعدة التبعية التدرجية على النحو التالي:

/1 جهة تصديق مركزية وحيدة، تكون مهمتها المصادقة على التكنولوجيات التي تسمح باستعمال المفاتيح العامة و الخاصة، وكذا تصديق عمل مقدمي خدمات التصديق الأقل منها درجة.

ب/ جهات تصديق جهوية، تكون مهمتها ضمان نسبة المفتاح العام للشخص صاحب المفتاح الخاص المستعمل من الموقع.

ج/ جهات توثيقية محلية تعمل تحت وصاية الجهات الجهوية، تكون مهمتها منح المستعملين الأزواج من المفاتيح الكريبتوغرافية وكذا شهادات التصديق المتعلقة بكل زوج من المفاتيح وذلك بعد التأكد التام من هوية مقتني هذه المفاتيح[20].

يبقى أن نشير أن تنظيم مقدمي خدمات التصديق يختلف من دولة إلى أخرى. فقد تسند مهمة تقديم الخدمات المشار إليها أعلاه إلى مؤسسة عمومية أو جهة إدارية معينة، كما قد تسند إلى الخواص بعد الحصول على رخصة بذلك. كما تختلف كذلك الخدمات التي تقدمها، فقد تسند لها مهمة منح المفاتيح أو الأنظمة المعلوماتية المستعملة لخلق المفاتيح، وقد تسند لها المهمة الثانية فقط وينقى للمستعملين صلاحية خلق المفاتيح ويقتصر دور هذه الجهات هنا على تسيير المفاتيح العامة وإصدار شهادات التصديق.

2- مقدمي خدمات التصديق:

لكي تحقق الجهات الخاصة بالتصديق مهمة نسبة المفتاح العام لشخص معين تقوم بإصدار شهادات تسجيل إلكترونية تعرف بشهادات التصديق "تعرض ضمن فهرس إلكتروني". تتضمن هذه الشهادات بالتحديد المفتاح العام وهوية الشخص حائز هذا المفتاح وأن هذا الشخص هو صاحب المفتاح الخاص المقابل للمفتاح العام.[21]

وهكذا يكون لكل مستعمل يريد تحقيق توقيع إلكتروني ما، أن يلجأ لشهادة التصديق ويستعمل المفتاح العام المذكور بها ليتأكد أن التوقيع استعمل بواسطة المفتاح الخاص المقابل.

ولكي تكتسب شهادة التصديق الحجية المنوطة بها أعلاه، يجب أن تكون مصحوبة بالتوقيع الإلكتروني للسلطة مصدرة الشهادة. هذا التوقيع يمكن أن يكون محل تحقيق عن طريق مراقبة المفتاح العام للسلطة مصدرة الشهادة و ذلك عن طريق شهادة تصدرها سلطة توثيق أخرى. و يدورها هذه الأخيرة يمكن أن تكون محل تحقيق بنفس الطريقة، و هكذا يمكن للشخص المرسل اليه أن يتحقق في كل مرة من التوقيع بتحقيق التوقيع الإلكتروني لكل سلطة مصدرة لشهادة التصديق، بحيث أنه كلما تعددت سلطات التوثيق زادت مصداقية التوقيع لا سيما اذا كانت السلطات مخولة باصدار الشهادات سلطات عمومية تخضع لمبدأ التدرج كما ذكر أعلاه.

و ينبغي الاشارة في هذا الصدد أن التوقيع الالكتروني الذي يوضع على الرسالة الالكترونية او حتى على شهادة التصديق يجب أن يكون مؤرخا، و العلة في ذلك هو التحقق من أن التوقيع قد تم خلقه و استعماله أثناء فترة صلاحية شهادة التصديق (الأمر الذي يفرض في حالة الخطأ تحديد المسؤولية المدنية او الجزائية كما سنراه لاحقا)[23].

و قد تشترط الجهات المخولة بالاصدار شهادات التصديق قبل منح المفاتيح و الشهادة تقديم مبلغ كفالة و يتصور ذلك في حالة تقديم مقتني المفاتيح لهوية خاطئة أو مزورة. وإذا تبين أن صاحب المفتاح الخاص قد فقد السيطرة عليه تقوم سلطات التوثيق مباشرة "بموافقة المعني أو دونها" بإلغاء شهادة التصديق ويتعين بالتبعية في هذه الحالة نشر هذا الإلغاء بنفس الطرق[24].

ثالثا :ملخص إجراءات استعمال التوقيع الالكتروني:

مكن تلخيص إجراءات خلق و استعمال التوقيع الإلكتروني كالتالي:

1 - يقدم الشخص الذي يريد تبادل رسائل إلكترونية موقعة إلى جهة مقدمة خدمات التصديق من أجل الحصول على زوج من المفاتيح.

2- يقوم المرسل بإعداد الرسالة الإلكترونية المراد إرسالها في شكل بريد إلكتروني. 3- يقوم المرسل بإعداد ملخص الرسالة الإلكترونية المعدة وذلك باستعمال عملية حسابية بواسطة لوغاريتم رياضي، ثم يقوم بواسطة نفس النظام المعلوماتي بإجراء عملية المراقبة لتحويل ملخص الرسالة الى نتيجة مراقبة وباستعمال هذه النتيجة و المفتاح الخاص يتم خلق التوقيع الإلكتروني.

4- يقوم المرسل بواسطة لوغاريتم موجود بالنظام المعلوماتي يربط التوقيع الإلكتروني بالرسالة الأصلية و الرسالة المختصرة.

5- يقوم المرسل عبر البريد الإلكتروني بإرسال الرسالة الموقعة

6- فور تلقي المرسل إليه هذه الرسالة، يقوم بإجراء تحقيق التوقيع الإلكتروني، بحيث يطلع على فهرس الشهادات التي يصدرها مقدم خدمات التصديق وباستعمال المفتاح العام المذكور بالشهادة المتعلقة بالمرسل موقع الرسالة الإلكترونية، يتأكد أن الرسالة موقعة بواسطة المفتاح الخاص للمرسل

7- للتحقق من أن الرسالة الأصلية لم تقع محل تحريف أو تغيير، يقوم المرسل إليه بإعداد ملخص الرسالة الأصلية من جديد وحساب نتيجة المراقبة باستعمال نفس اللوغاريتم، وإذا توصل إلى نفس النتيجة فهذا معناه أن الرسالة لم تتغير.

بكوش خميسي
محامي بمنظمة سطيف
ماجيستير في القانون الخاص

الهوامش

1- تقابل هذه الترجمة باللغة الفرنسية de échange électronic données informatisées وباللغة الانجليزية data interchange المختصرة إلى "EDI" ويقصد بها تبادل بيانات تجارية من حاسوب إلى اخر على شكل رسائل إلكترونية قياسية بالاستعانة بوساطة شبكات الإرسال.

2- أقصد بمصطلح معلوماتية المبادلات نقلها من طابعها المادي إلى طابع إلكتروني.

3-V.à Titre d'example:

-En France,la loi n°230/2000 du 13 mars2000 portant adaptation du droit de la preuve aux téchnologies et relative à la signature électronique
Www.legifrance.gouv.fr/jorf_nor.ow?numjo=JUSX9900020L

- En Belgique,la loi du 20 octobre2000 portant l'introduction de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire,In la signature électronique.
Www.awt.be/web/fic/index/aspx?pagfic.fr.j00.000.000.

- En province de l'Ontario,la loi du 16 octobre2000 sur le commerce électronique, citée par diane bellavance et autre, la signature électronique et la gestion documentaire.

4- V .l'integralité de la loi type sur les signatures électroniques, www.uncitral.org/stable/res5680-a.pdf.

5- انظر أدناه

6- V. Jean michel, la signature électronique, ça marche, combien ça coute, à quoi sert, www.yolin.net/signature.html#oc8:
La sécurité sur le net, la cryptologie: la signature électronique, www.securnet.free/fr/annexe/fc67_mono.html

7- signature électronique: cryptologie et signature:enjeux et concepts, www.awt.be/web/services/imp/index.aspx?page-fic.fr.j00.015.001.

8-Valérie Sédallian.Preuve et signature électronique,juriscom.Net,revue du droit des téchnologie de l'information. www.juriscom.net/miniev/ithoumyre.php:
CNUDCI, groupe de travail sur le commerce électronique, trente-et-unième session,New-York,18-28 février 1997, planification des travaux à venir en matière de commerce électronique: signatures électronique,tiérs authentificateurs et questions juridique connexes.
Www.uncitral.org/workinggroups/wg_ec/ml-ec-becdocs/wp.71.f.pdf,p.8,9

9- Jean Michel, op.cit,p.3,4

10- Ibid

11- CNUDCI,op.cit,p.16.

12- CNUDCI,op.cit,p.11.

13-Ibid.

14- Cryptographie et signature électronique:enjeux et concepts,op.cit

15- CNUDCI,ibid.

16- Ibid.

17- CNUDCI,op.cit,p.11,12.

18- Valérie Sédallian,op.cit,p.05

19- Frédéric Mascré,la signature électronique, www.mascre.heguy.com/htm/fr/contract.htmCNUDCI,op.cit,p.13.

20- Ibid, p.14

21-Signature électronique et liste des autorisés de certification reconnue,www.achatpublic.com
Thierry Lévy-Abégnoli,Signature électronique:la renaissance des infrastructures à clés publiques,www.zdnet.fr/techupdate/securite/talkback.htm

22- CNUDCI,op.cit,p.16

23- Signature électronique, certificat numérique, www.awt.be/web/services/imp/index.aspx?page-fic.fr.j00.015.001, op.cit.

24- CNUDCI,ibid.