الفصل التاسع

التوقيع الرقمي أو الإلكتروني

مقدمة :

يعتبر التوقيع' Signature' شرطاً أساسياً في توثيق اغلب المستندات سواء إن كانت في المراسلات العادية اليدوية أو المراسلات الإلكترونية بجميع أنواعها وحتى إن كانت محلية أو دولية، ومع ظهور التحديات الجديدة التي يواجهها الاقتصاد الرقمي والأمني وبشكل خاص نشوء الحكومات الإلكترونية وعدم توافر الضمانات الكافية التي تحمي المجتمع الذي يتعامل بالخصوص مع هذا النظام الإلكتروني والتعامل معه بكل ثقة وأمان أصبحت الحاجة إلى ظهور طريقة آمنة وسريعة وفعالة في عمليات تصديق الوثائق التي يتم تبادلها إلكترونيا على جميع المستويات بكل مراحلها و إضفاء الصفة القانونية عليها ومن ثم أرشفتها رقميا كل ذلك أدى لظهور ما يسمى بالتوقيع الرقمي.

وفي المقالة المشهورة " اتجاهات جديدة في علم التعمية " يقوم كل من ويتفلد ديفي ومارتن هيلمن بوصف أهمية التوقيع الرقمي بالرغم من أسفهما لم يؤكدا بشدة على وجود وكثرة استعمال هذا النوع من التواقيع. بعد ذلك قام كل من رونالد ريفاست وأدى شمير بابتكار خوارزميات الـ RSA ليستخدم للتوقيع الرقمي الأولي البرنامج الأول الذي تم توثيقه والإعلان عنه كان مع لوتس نوتس عام ١٩٨٩ والذي استخدم خوارزميات الـRSA، في الـRSA الأساسية يجب إجراء cryptographic hash function للرسالة ثم تطبيق الـ RSA التي تم ذكرها أعلاه. هذا النموذج يكون آمنا في ال oracle module. وقد تم تطوير التواقيع الرقمية بعد نموذج الـ RSA فظهرت نماذج مثل توقيع اللامبورت و توقيع ميركل ورابن .

تعريف التوقيع الإلكتروني Digital Signature :

- هو عبارة عن ملف رقمي صغير مكون من بعض الحروف والأرقام والرموز تصدر عن إحدى الجهات المتخصصة والمعترف بها حكوميا ودوليا ويطلق عليها الشهادة الرقمية Digital Certificate وتخزن فيها جميع معلومات الشخص وتاريخ ورقم الشهادة ومصدرها، وعادة يسلم مع هذه الشهادة مفتاحان احدهما عام والآخر خاص، أما المفتاح العام فهو الذي ينشر في الدليل لكل الناس والمفتاح الخاص هو توقيعك الرقمي[1]. وهناك

1 - أسامة الكسواني، التوقيع الإلكتروني، شبكة الإنترنت، ٢٠٠٧..

بعض التعريفات الأخرى كما عرفها ياسر العدل[1] على أن التوقيع الإلكتروني هو ما يوضع على محرر إلكتروني، شريحة إلكترونية، ويتخذ شكل حروف أو أرقام أو رموز أو إشارات غيرها ويكون له طابع متميز ومنفرد يسمح بتحديد شخص الموقع ويميزه عن غيره وهو هو نظام تشفير إلكتروني يعتمد على مفتاح خاص ومفتاح عام، وتنشأ المفاتيح بواسطة عمليات حسابية خاصة تضمن السرية. المفتاح الخاص عبارة عن أداة إلكترونية خاصة بصاحبها، ويستخدم في وضع التوقيع الإلكتروني على المحررات الإلكترونية ويتم الاحتفاظ على بطاقة ذكية مؤمنة، وهو مثل البصمة لا يتكرر مع أي شخص آخر، والبطاقة الذكية عبارة عن وسيط إلكتروني مؤمن يستخدم في عملية إنشاء وتثبيت التوقيع الإلكتروني على المحرر الإلكتروني وتحتوي على شريحة إلكترونية بها معالج إلكتروني وعناصر تخزين وبرمجيات للتشغيل. والمفتاح العام عبارة عن أداة إلكترونية توضع لدى شخص مستقبل الرسالة نفسه، ويتم إصداره من الجهة المصدرة للتوقيع الإلكتروني، ويستخدم المفتاح في التحقق من شخصية الموقع على المحرر الإلكتروني والتأكد من صحة وسلامة محتوى المحرر الإلكتروني الأصلي.

- وباختصار شديد يمكننا أن نعرف التوقيع الرقمي على انه طريقة اتصال مشفرة رقميا تعمل على توثيق المعاملات بشتى أنواعها والتي تتم عبر صفحات الإنترنت[2].
- وهناك بعض التعريفات الأخرى والتي توضح بأن التوقيع الإلكتروني يحتوي على على قيمة تدعى قيمة هاش (Hash Value) أو نتيجة هاش (Hash result) يتم احتسابها عن طريق وظيفة هاش، وهي خوارزمية تحول البيانات إلى قيمة فريدة (بصمة) تمثل هذه البيانات.وفي حال إجراء أي تعديل على تلك البيانات- مهما كان صغيراً- ستتغير هذه القيمة، مما يحتم إمكانية اكتشاف أي تغيرات تطرأ على البيانات (في حال محاولة تزوير الرسالة من قِبَل متطفلين)[3].

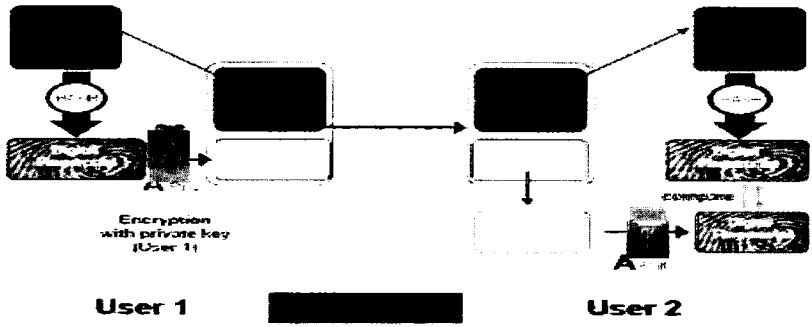
---

1 - ياسر العدل، كبسولة في التوقيع الإلكتروني، مجلة الحوار المتمدن، العدد ٢٧٨٤، ٢٠٠٩ شبكة الإنترنت.

2 - محمد نور الدين، التوقيع الرقمي، كلية الهندسة الكهربائية، ٢٠٠٨- ٢٠٠٩، ورقة عمل.

3 - رها القوتلي، التوقيع الرقمي، www.kantakji.com .

الرسم التالي يوضح سير العمل الأساسي لتوقيع رقمي تم إستخدامه لإرسال رسالة :



لقد عرّف قانون المعاملات الإلكترونية **رقم ٨٥ لسنة ٢٠٠١ الأردني** في المادة(٢) منه التوقيع الإلكتروني بأنه "عبارة عن البيانات التي تتخذ هيئة حروف أو أرقام أو رموز أو إشارات أو غيرها وتكون مدرجة بشكل إلكتروني أو رقمي أو ضوئي أو أي وسيلة أخرى مماثلة في رسالة معلومات أو مضافة عليها أو مرتبطة بها ولها طابع يسمح بتحديد هوية الشخص الذي وقعها ويميزه عن غيره من اجل توقيعه وبغرض الموافقة على مضمونه[1] وفي هذا المقام لا بد من التفريق بين التوقيع الإلكتروني والتوقيع الرقمي إذ إن التوقيع الإلكتروني يكون بأية صورة بما فيها الرسم الضوئي، في حين أن التوقيع الرقمي والذي يصنعه برنامج خاص هو مجموعة مزايا رقمية مأخوذة من حجم الرسالة المرسلة تنقل بشكل مشفر ويتبين من فك تشفيرها مدى صحة أو عدم صحة التوقيع أيضا عرف بأنه التوقيع المكون من حروف أو أرقام أو رموز أو صوت أو نظام معالجة ذي شكل إلكتروني وملحق أو مرتبط منطقيا برسالة إلكترونية وممهور بنية توثيق أو اعتماد تلك الرسالة بحيث يتم التوقيع الإلكتروني (الرقمي) بواسطة برنامج كمبيوتر خاص لهذه الغاية وباستعماله فإن الشخص يكون قد وقع على رسالته تماما كما يوقع ماديا (في عالم الأوراق والوثائق الورقية) ويستخدم التوقيع الرقمي على كافة الرسائل الإلكترونية والعقود الإلكترونية.

---

1 - قانون المعاملات الالكترونية رقم ٢٠٠١/٨٥، التشريعات الاردنية، المادة(٢)، الجريدة الرسمية، العدد٤٥٢٤، لعام ٢٠٠١.

أنواع التوقيعات الرقمية :

هناك نوعان من التوقيعات الرقمية الشائعة:

١- التوقيع المحمي: ' Key Based Signature ' : وهنا يتم تزويد الوثيقة الإلكترونية بتوقيع رقمي مشفر يقوم بتشخيص المستخدم 'الموقع ' الذي قام بالتوقيع ووقت التوقيع ومعلومات عن الشخص نفسه وهو عادة مميز لأصحاب التوقيع[١].

٢- التوقيع البيومتري ' Signature Biometric' : يقوم على أساس التحقق من شخصية المتعامل بالاعتماد على الصفات الجسمانية للأفراد مثل البصمة الشخصية، مسح العين البشرية، التعرف على الوجه البشري، خواص اليد، التحقق من نبرة الصوت والتوقيع الشخصي ويتم التأكد من شخصية المتعامل عن طريق إدخال المعلومات للحاسب أو الوسائل ألحديثه مثل التقاط صورة دقيقة لعين المستخدم أو صوته أو يده ويتم تخزينها بطريقة مشفرة في ذاكرة الحاسوب ليقوم بعد ذلك بالمطابقة ويواجه هذا النظام الكثير من المشاكل منها أن صورة التوقيع يتم وضعها على القرص الصلب للحاسوب ومن ثم يمكن مهاجمتها بالفيروسات أو نسخها بواسطة الطرق المستخدمة في القرصنة الإلكترونية. كذلك عدم إمكانية إستخدام هذه التقنية مع جميع الحاسبات المتوفرة، ويحتاج هذا النوع من التوقيع إلى استثمارات ضخمه لتمكين مستخدمي الشبكة الإلكترونية من إستخدام الخصائص الذاتية لشخص الموقع في التوقيع الإلكتروني[٢].

٣- التوقيع الرقمي أو الكودي : Digital Signature : وهو عبارة عن عدة أرقام يتم تركيبها لتكون في النهاية كودا يتم التوقيع به ويستخدم هذا في التعاملات البنكية والمراسلات الإلكترونية بين التجار أو بين الشركات وبعضها ، ومثال لذلك بطاقة الائتمان التي تحتوي على رقم سري لا يعرفه سوى العميل، ويعد هذا النوع وسيلة آمنه لتحديد هوية الشخص الذي قام بالتوقيع من خلال الحاسب الآلي[٣].

٤- التوقيع بالقلم الإلكتروني : Pen- Op : يقوم مرسل الرسالة بكتابة توقيعه الشخصي بإستخدام قلم إلكتروني خاص على شاشة الحاسب الآلي عن طريق برنامج معين ويقوم

---

1 - شبكة الإنترنت، التوقيع الإلكتروني، منتدى المحاسبين العرب، ٢٠٠٩.

2 - رها القوتلي، التوقيع الرقمي، www.kantakji.com .

3 - ياسر العدل، مرجع سبق ذكره.

هذا البرنامج بالتقاط التوقيع والتحقق من صحته، ولكن يحتاج هذا النظام إلى جهاز حاسب آلي بمواصفات خاصة ويستخدم هذا بواسطة أجهزة الأمن والمخابرات كوسيلة للتحقق من الشخصية، وهذا النوع أفضل من التوقيع اليدوي والذي يتم على شاشة جهاز الكمبيوتر أو على لوحة خاصة معدة لذلك باستعمال قلم خاص عند ظهور المحرر الإلكتروني على الشاشة وهذا النوع لا يتمتع بأي درجة من الآمان، كذلك لا يتضمن حجية في الإثبات[1].

أهم تطبيقات التوقيع الإلكتروني[2]:

- المعاملات التجارية الإلكترونية: وتشمل كل معاملة ذات طابع تجاري في مجالات التعامل المختلفة مثل البيع وغيرها من العقود والمعاملات التجارية القانونية الأخرى ومثل الاستيراد والتصدير وباقي التعاقدات وتذاكر السفر والفنادق والمطاعم والمعاملات المصرفية بكل أنواعها التي تتم في شكل محرر إلكتروني أو موقع توقيع إلكتروني:

١. المعاملات المدنية الإلكترونية : وتشمل كل معاملة إلكترونية سواء بالنظر إلى طرفيها أو إلى احد طرفيها والتي تخرج عن مفهوم المعاملات التجارية
٢. الحكومة الإلكترونية: وتشمل المعاملات الإدارية الحكومية وخدمات المواطنين بشكل عام ومنها التصاريح المختلفة والخدمات التي تقدمها الجمارك والضرائب ومصلحة الأحوال المدنية وكذلك ما يقدم للجهات الحكومية من طلبات
٣. الكروت الذكية : وهي عبارة عن وسيط إلكتروني مؤمن يستخدم في عملية إنشاء وتثبيت التوقيع الإلكتروني على المحرر الإلكتروني ويحتوي على شريحة إلكترونية بها معالج إلكتروني وعناصر تخزين وبرمجيات للتشغيل.

وظيفة التوقيع الرقمي:

يمكن من الوجهة القانونية اعتبار أن الوظائف الرئيسية للتوقيع الرقمي هي[3]:-

١- التوقيع الرقمي يثبت الشخص الذي وقع الوثيقة.

---

1 - يوسف المومني، التوقيع الإلكتروني، شبكة الإنترنت، ٢٠٠٨.

2 - رها القوتلي، التوقيع الرقمي، www.kantakji.com .

3 - أحلام الحمبرجي، بحث بعنوان حجية التوقيع الإلكتروني في الأردن، مؤسسة المناطق الحرة، ٢٠٠٨.

٢- يحدد التوقيع الرقمي الشئ (الوثيقة) التي تم توقيعها بشكل لا يحتمل التغيير.

الفرق بين التوقيع العادي والتوقيع الإلكتروني (الرقمي):

التوقيع الإلكتروني (الرقمي): عبارة عن جزء صغير مشفّر من بيانات يضاف إلى رسالة إلكترونية كالبريد الإلكتروني أو العقد الإلكتروني، وثمة خطر كبير في مفهوم التوقيع الرقمي حيث يظن البعض انه أرقام أو رموز أو صورة للتوقيع العادي وهو ليس كذلك، إذ لا تعد صورة التوقيع العادي بواسطة السكانر (الماسحة الضوئية) توقيعا إلكترونيا.

فالتوقيع الإلكتروني الرقمي على رسالة ما عبارة عن بيانات متجزأه من الرسالة ذاتها (جزء صغير من البيانات) يجري تشفيره وإرساله مع الرسالة، بحيث يتم التوثّق من صحة الرسالة من الشخص عند فك التشفير وانطباق محتوى التوقيع على الرسالة[1].

حجيّة التوقيع الإلكتروني وتأثير تقنية المعلومات على بعض العلاقات التعاقدية والإثبات[2]:

في بعض الأحوال يستلزم التشريع تقديم المعاملة إلى جهة معينة كوثيقة خطية محرر كما هو الحال ببوالص الشحن مثلا في حين تكون هذه الوثيقة أجريت بطريقة إلكترونية ومخزنة في نظم الكمبيوتر، أو كالكشوف المحاسبية التي تجري داخل النظام لكن يتعين تقديمها للقضاء كمستخرج ورقي.

ولقد قررت المادة (٦) من قانون المعاملات الإلكترونية الأردني أن طباعة المعاملة المجزّأة بواسطة وسائل إلكترونية من قبل المرسل إليه وتقديمها كمستخرج خطي يفي بالإلتزام الذي تقرره التشريعات الخاصة حين تتطلب تقديم المستند أو المعاملة بصورة خطية، لكن هذه السجلات تعتبر غير ملزمة للمرسل إليه إن عجز عن طباعتها أو تخزينها والاحتفاظ بها بسلوك صادر عن المرسل ذاته.

---

1 - مقالة بعنوان التحديات القانونية للتجارة الإلكترونية على الموقع الإلكتروني.

2 - أحلام الحمبرجي، مصدر سبق ذكره.

ولتوضيح هذه الفكرة فان المرسل قد يرسل رسالة معلومات إلى المرسل إليه بالبريد الإلكتروني، فان افترضنا إن تقنية الإرسال تمنع المرسل إليه من الاحتفاظ بالرسالة وتخزينها واسترجاعها ورقيا فان هذه الرسالة لا تكون ملزمة للمرسل إليه.

حجية التوقيع الإلكتروني:

لقد أكدت المادة (١٠) من قانون المعاملات الإلكترونية الأردني على أن التوقيع الإلكتروني على السجل الإلكتروني يفي بمتطلبات التشريع الذي يستوجب توقيعا على المستند أو نص على ترتيب اثر على خلوة من التوقيع، وهذا تكريس لمبدأ أن التوضيح الإلكتروني حقق المقصود من التوقيع الخطي، لكن إيفاء التوقيع الإلكتروني بهذه الوظيفة التي يحققها التوقيع العادي رهن بالثقة بصحة هذا التوقيع، فكيف ستحقق هذه الثقة[1].

إن الفقرة (ب) من ذات المادة أجابت على هذا التساؤل حين قررت أنه يتم إثبات صحة التوقيع الإلكتروني ونسبته إلى صاحبه إذا توافرت طريقة لتحديد هويته والدلالة على موافقته على المعلومات الواردة في السجل الإلكتروني الذي يحمل توقيعه إذا كانت تلك الطريقة، مما يعول عليها لهذه الغاية في ضوء الظروف المتعلقة بالمعاملة بما في ذلك اتفاق الأطراف على إستخدام تلك الطريقة ومن الطرق الشائعة في البيئة الرقمية (انضمام الشخص إلى نظامه الإلكتروني) ويقصد بها الانضمام إلى شبكة يديرها الغير تمنحه مصادقة على أن التوقيع الإلكتروني المستخدم فيه معتمد من قبلها لشخصه ونظامه وانه يستخدمه في تعاملاته الإلكترونية، ومن الطرق أيضا إثبات اشتمال نظام الكمبيوتر المستخدم في الإرسال على برمجيات التوقيع الإلكتروني مزودّة من منتجيها بحيث يسهل اللجوء إلى منتج البرنامج لتأكيد سلامة أو عدم سلامة التوقيع الإلكتروني محل الإستخدام.

ولقد بحثت العديد من المحاكم في النظم القانونية المقارنة حجية التوقيع الإلكتروني، وتباينت الاتجاهات بشأنها قبل أن يتم تطبيق حجيتها قانونا في عدد

1- قانون المعاملات الإلكترونية الأردني، ٢٠٠١.

من الدول أو الاستعداد التشريعي في عدد آخر تمهيدا لقبوله أو إقرار حجيته، ضمن شروط ومعايير معينة.

وقد اعتبر قانون المعاملات الإلكتروني الأردني إن السجل الإلكتروني أو العقد الإلكتروني أو الرسالة الإلكترونية أو التوقيع الإلكتروني منتجا للأثر القانوني ذاته المترتب على الوثائق والمستندات الخطية والتوقيع الخطي بموجب أحكام التشريعات النافذة من حيث إلزامها لإطرافها أو صلاحياتها في الإثبات ولا يجوز إغفال هذا الأثر، شريطة عدم تعارضها مع مواد القانون المعمول به وذلك حسب نص المادة (٧) من القانون نفسه[1].

وفي هذا المقام لا يمكن أن نتجاهل التعديل التشريعي في قانون البينات الأردني مؤخرا، فقد تناول القانون المعدّل لقانون البينات الأردني لسنة ٢٠٠١ حجية رسائل الفاكس والتلكس والبريد الإلكتروني وقوتها في الإثبات، واعتبر أن لها قوة الإسناد العادية في الإثبات ما لم يثبت من نُسب إليه إرسالها انه لم يقم بذلك أو لم يكلف احد بإرسالها، كما إن لرسائل التلكس بالرقم السري المتفق عليه بين المرسل والمرسل إليه حجة على كل منهما وتكون لمخرجات الحاسوب المصدقة أو الموثقة قوة الإسناد العاديّة من حيث الإثبات ما لم يثبت من نسبت إليه انه لم يستخرجها أو لم يكلّف احد باستخراجها.

وبذلك يكون المشّرع الأردني قد قطع شوطا في مجال التطور التشريعي بما يتناسب مع التطور العالمي وتطور التشريعات على المستوى العالمي بما سينعكس إيجابا على تشجيع الاستثمار ويكون نقطة جذب للمستثمرين الذين سيتمكنوا من إثبات أعمالهم في ظل قانون عصري يتواكب مع التطور.

ويتم إثبات صحة التوقيع الإلكتروني ونسبته إلى صاحبه إذا توافرت طريقة لتحديد هويته والدلالة على موافقته على المعلومات الواردة في السجل الإلكتروني الذي يحمل توقيعه إذا كانت تلك الطريقة مما يعول عليها لهذه الغاية في ضوء الظروف المتعلقة بالمعاملة بما في ذلك اتفاق الأطراف على إستخدام تلك الطريقة.

وقد اعتبرت المادة (١/٣٢) من الفصل السادس من قانون المعاملات المذكور

---

1 - قانون المعاملات الإلكتروني الأردني، مصدر سابق ذكره.

والخاص بتوثيق السجل والتوقيع الإلكتروني، أن التوقيع الإلكتروني يعتبر موثقا إذا اتصف بما يلي:

- ارتباطه بالشخص صاحب العلاقة وتميّزه بشكل فريد.
- كان كافيا للتعريف بشخص صاحبه
- تم إنشاؤه بوسائل خاصة بالشخص وتحت سيطرته
- ارتبط بالسجل الذي يتعلق به بصورة لا تسمح بإجراء تعديل على القيد بعد توقيعه دون إحداث تغيير في التوقيع.

لذلك فإن القانون الأردني يفترض أن التوقيع الإلكتروني والسجل الإلكتروني الموثق لم يتم تغييره أو تعديله منذ تاريخ إجراءات توثيقه وأنه صادر عن الشخص المنسوب إليه وأنه قد وضع من قبله للتدليل على موافقته على مضمون السند ما لم يثبت العكس.

وفي حالة عدم توثيق السجل الإلكتروني أو التوقيع الإلكتروني، فلا يعتمد بهما ولا يرتب أيا منهما أي حجية في القانون، ويعتبر السجل الإلكتروني أو أي جزء منه إذاً كان يحمل توقيعا إلكترونيا موثقا، سجلا موثقا بكامله أو فيما يتعلق بذلك بذلك الجزء حسب واقع الحال، إذاً تم التوقيع خلال مدة سريان شهادة توثيق معتمدة وتمت مطابقته مع رمز التعريف المبين في تلك الشهادة.

وفي حالة اعتماد شهادة التوثيق التي تبين رمز التعريف الإلكتروني: فقد عرف قانون المعاملات الإلكترونية الأردني في المادة (٢) منه شهادة التوثيق بأنها الشهادة التي تصدر عن جهة مرخصة أو معتمدة لإثبات نسبة توقيع إلكتروني إلى شخص معين استنادا إلى إجراءات توثيق معتمدة.

مزايا إستخدام التوقيع الإلكتروني[1]:

١. إمكانية إستخدامه كبديل للتوقيع التقليدي بالإضافة إلى مسايرته لنظم المعلومات الحديثة.

٢. يؤدي التوقيع الإلكتروني إلى رفع مستوى الأمن والخصوصية بالنسبة للمتعاملين على شبكة الإنترنت خاصة في مجال التجارة الإلكترونية.

---

1 - يوسف مومني، التوقيع الإلكتروني، منتدى شبكة قانوني الأردن، www.lawjo.net

٣. إمكانية تحديد هوية المرسل والمستقبل إلكترونيا والتأكد من مصداقية الأشخاص والمعلومات.

٤. يساعد التوقيع الإلكتروني كل المؤسسات على حماية نفسها من عمليات التزييف وتزوير التوقيعات

٥. يسمح التوقيع الإلكتروني بعقد الصفقات عن بعد ودون حضور المتعاقدين فبالتالي يساعد في تنمية وضمان التجارة الإلكترونية

متطلبات التوقيع الرقمي:

إن للتوقيع الرقمي متطلبات معينة مسبقة له والتي بدونها يصبح هذا التوقيع بدون أي قيمة قانونية هذه المتطلبات هي:

١. قيمة الخوارزميات: بعض مفاتيح الخوارزميات غير أمنة وقد تم إثبات خرق البعض منها.

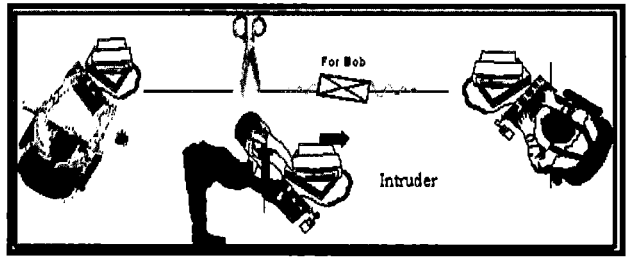
٢. قيمة التنفيذ : تنفيذ وتطبيق خوارزميات مع أخطاء لن يؤدي إلى أي نتيجة.

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

إن على المستخدمين وعلى برامجهم أن تكون ملتزمة بالبروتوكول المتفق عليه.

صفات التوقيع الإلكتروني[1]:

- توثيق الموقع : إن التوقيع يجب أن يبين أو يشير إلى الشخص الذي قام بتوقيع الوثيقة أو الرسالة أو السجل ويجب أن يكون من الصعب على شخص آخر القيام به بدون تفويض. الصورة التالية تظهر متسلل يزعم بكونه الطرف المرسل.



1 - شبكة الإنترنت، نبذة عن التوقيعات الرقمية.
www.e-signature.gov.eg/.../ElectronicSignature_Mechanizm_Arabic.doc

- توثيق الوثيقة :أي توقيع يجب أن يعرف عن الطرف الذي قام بتوقيعه بما يجعله غير ممكنا تزوير أو تغيير أي من المادة الموقعة أو التوقيع بدون انكشاف الحقيقة .

الهدف من التوقيع الإلكتروني:

الهدف يندرج تحت مضمون الأمن والسلامة الرقميين، وعند ثبوت صحتها فإنها بالطبع تحقق جميع الجوانب العملية والأهداف المرجوة منها ولعدة أهداف قانونية بحتة تبعد المتطفلين عن التلصص وسرقة البيانات وأهمها[1]:

١. توثيق التوقيع الإلكتروني للموقع

عند إنشاء الشهادة فإنه يتم إنشاء مفتاحين (عام وخاص)، وفي حالة إن كان المفتاحان مرتبطين بصاحب التوقيع الإلكتروني فإن كل وظيفة يقوم بها من إرسال الوثائق من عنده فإنها تكون خاصة به، وهنا لا يمكن القيام بعملية التزوير إلا في حالة واحدة وهي إن فقد صاحب التوقيع الإلكتروني المفتاح الخاص به أو تم تسريبه.

٢. ضمان توثيق الرسالة [2]"Hash Function":

عندما يقوم المستخدم بإنشاء رسالة مصاحبة لتوقيعه الإلكتروني فإنها عادة تكون مدمجة معها بعض الشفرات كوظيفة أساسية تسمى 'وظيفة الهاش' وتستخدم في بداية إنشاء التوقيع الإلكتروني والتأكد من صحته، أما الطريقة التي تعمل بها فإنها تقوم على أساس إنشاء تمثيل رقمي معين على شكل قيمة رقمية 'هاش' أو 'نتيجة الهاش' عادة تكون هذه القيمة أصغر من الرسالة وتوضع إما في بدايتها أو نهايتها وتكون مدمجة بها، وفي هذه الحالة إن تم التلاعب بتلك الرسالة فإنه على الفور تختلف قيمة 'الهاش' التي تم احتسابها منذ البداية عند إنشاء الرسالة، وحتى إن تم التعرف على قيمة 'الهاش' الثانية فإنه من الصعوبة تقفي أثر قيمة 'الهاش ' الأولية.

٣. الضمان[3]:

عند البدء في إنشاء التوقيع الإلكتروني بوساطة الهيئات المعتمدة فإنها بالطبع تتطلب ضمانا عاليا حسب المستويات والتراخيص الدولية والتي تتم عادة

---

1 - منتدى القانون العماني، التوقيع الإلكتروني، ٢٠١٠.

2 - عبد الغني الإدريسي، ماذا تعرف عن التوقيع الإلكتروني، شبكة الإنترنت، ٢٠٠٩.

3 - أسامة الكسواني، التوقيع الإلكتروني، شبكة الإنترنت، ٢٠٠٧.

بموافقة الموقع الإلكتروني، وهنا فإنها ومن دون شك تولد أعلى درجات السلامة الأمنية.

٤. توسيع التجارة الإلكترونية[1]:

إن انتشار التوقيع الإلكتروني له من المميزات الكبيرة التي من شأنها القيام بالتوسع في التجارة الإلكترونية وتأمين جميع معاملاتها على الصعيدين الدولي والمحلي، وحقيقة تذكر أن بعض الدول العربية باتت بالعمل في سن قوانين كثيرة تخص التوقيع الإلكتروني ومنهجيته ومدى الاستفادة منه في تأمين سرية المعلومات المرسلة مع عدم قدرة أحد على الاطلاع عليها أو تعديل جزء منها، والتي من شأنها أن تقضي على 'الواسطة' في بعض البلدان.

التوقيع الإلكتروني وتأثيره على الخدمات العامة[2]:

١. تحويل المعلومات الشخصية بصورة سرية ومضمونة لكل مواطن.
٢. يمكن الاعتماد اعتماداً كلياً على التوقيع الرقمي ضمن الإجراءات القانونية والقضائية في المنازعات بين الأشخاص والشركات الخاصة أو المؤسسات والهيئات الحكومية
٣. توفير الهوية الرقمية لكل مواطن.
٤. التوقيع باستخدام التوقيع الرقمي الإلكتروني على جميع المستندات ونماذج الطلبات والعقود وغيرها من الطلبات.
٥. التوفير في جميع إجراءات إرسال البيانات إلى المواطن والحصول على المعلومات منه (التوفير في الورق، الطلبات، الطباعة، الأحبار، الخ).
٦. توفير عامل الوقت الثمين للمواطن والموظف وفي هذه الحالة لن يضطر المواطن إلى أن يذهب بسيارته أو باستخدام وسائل النقل إلى الدوائر الحكومية والانتظار مطولا.

---

1 - عبد الغني الإدريسي، مرجع سبق ذكره.

2 - الخالد ٢٠٠٢، جوجل، www.ejabat.google.com

٧. خلق وعي رقمي وفكري للمواطن، وتطوير التعامل في الإنترنت وأثره على التجارة الإلكترونية

شهادات التصديق الإلكتروني Public Key Certificates :

للتثبت من صحة توقيع إلكتروني معين، على الطرف الذي يقوم بالتثبت من الصحة أن يكون قادرا على الوصول إلى مفتاح الموقع العام وأن يكون واثقا بأنه متطابق مع مفتاح الموقع الخاص. على أية حال فإن أي زوج من المفاتيح العامة والخاصة ليس له أي ارتباط جوهري أو فعلي بأي شخص . إنه ببساطة زوج من الأرقام . من الضروري وجود إستراتيجية مقنعة لكي يتم ربط شخص أو هيئة معينة بزوج المفاتيح.

إن الحل لهذا هو استخدام طرف ثالث واحد أو أكثر يكون موثوق به لكي يربط موقع معين مع مفتاح عام محدد . تلك الجهة الثالثة الموثوق بها يشار إليها بعبارة " جهة التصديق الإلكتروني "

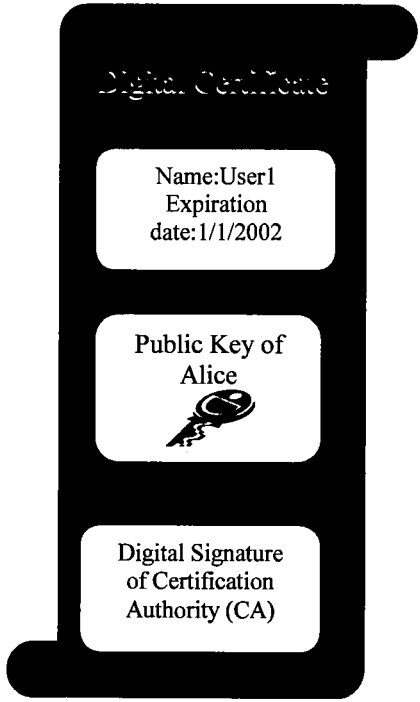
كيف يتم إنشاء ثقة رقمية ؟

كي يتم ربط زوج من المفاتيح بموقع محتمل تقوم " جهة التصديق الإلكتروني " بإصدار شهادة، سجل إلكتروني يذكر فيه المفتاح الشفرة العام على أنه " موضوع" الشهادة ويؤكد بأن الموقع المحتمل المعرف عنه في الشهادة يحمل المفتاح الخاص المقابل. يشار إلى الموقع المحتمل بعبارة " المشترك" . إن وظيفة الشهادة الرئيسية هي ربط زوج من المفاتيح مع مشترك معين. أي " مستلم " للشهادة يرغب في الاعتماد على والوثوق بتوقيع إلكتروني ينشئه المشترك المذكور في الشهادة (عندئذ يصبح المستلم هو الطرف المعتمد) بإمكانه استخدام المفتاح الشفرة العام المذكور في الشهادة للتثبت من صحة التوقيع الإلكتروني أي بأنه تم إنشائه بواسطة المفتاح الخاص المقابل. في حال نجحت عملية التثبت من الصحة فإن هذه السلسلة من الوقائع والمقدمات توفر الثقة والضمان بأن المفتاح الخاص المقابل محتفظ به من قبل المشترك المذكور أسمه في الشهادة وبأن التوقيع الإلكتروني قد تم إنشائه من قبل ذلك المشترك[1].

---

1 - شبكة الإنترنت، نبذة عن التوقيعات الرقمية.
www.e-signature.gov.eg/.../ElectronicSignature_Mechanizm_Arabic.doc

لتأكيد صحة كل من الرسالة والهوية في الشهادة تقوم جهة التصديق الإلكتروني بتوقيعها إلكترونيا. إن التوقيع الإلكتروني لجهة التصديق الإلكتروني على الشهادة يمكن التثبت من صحته باستخدام المفتاح الشفرى العام الخاص بجهة التصديق الإلكتروني والمذكور في شهادة أخرى من قبل جهة تصديق إلكتروني أخرى (والتي يمكن أن تكون على مستوى أعلى فيما يتعلق بالرتبة ولكن ذلك ليس بالضرورة) وتلك الشهادة الأخرى يمكن توثيقها بدورها بواسطة المفتاح الشفرى العام المذكور كذلك في شهادة أخرى وهكذا .. حتى يتثبت الشخص المعتمد على التوقيع الإلكتروني من صحته . في أي حال فإن جهة التصديق الإلكتروني المصدرة للشهادة يجب أن توقع إلكترونيا على شهادتها الخاصة بها خلال الفترة التشغيلية للشهادة الأخرى المستخدمة للتثبت من صحة التوقيع الإلكتروني لجهة التصديق الإلكتروني. الرسم التالي يوضح شكل شهادة التصديق الإلكتروني.



شهادة التصديق الإلكتروني

إن أي توقيع إلكتروني سواء تم إنشائه من قبل مشترك معين لتوثيق رسالة ما أو تم إنشائه من قبل جهة تصديق إلكتروني لتوثيق شهادتها (بالفعل رسالة متخصصة) يجب أن تكون مختومة زمنيا بشكل موثوق به وذلك كي يستطيع المتثبت من الصحة تحديد ما إذا كان التوقيع الإلكتروني قد تم إنشائه خلال الفترة التشغيلية (مدة الصلاحية) المذكورة في الرسالة .

كي يكون مفتاح عام وتعريفه مع مشترك معين متوفرين بسرعة وسهولة للإستخدام في التثبت من الصحة ، يمكن نشر شهادة في حافظة أو يتم توفيرهم من خلال أي طريقة أخرى . إن الحافظات هي عبارة عن قاعدة بيانات إلكترونية من الشهادات والمعلومات الأخرى المتوفرة للإسترجاع والإستخدام في التثبت من صحة التوقيعات الإلكترونية . يمكن القيام بالإسترجاع أوتوماتيكيا من خلال أمر برنامج التثبت من الصحة بأن يستفسر مباشرة من الحافظة للحصول على الشهادات المطلوبة .

لشهادة التصديق الإلكتروني المميزات التالية :

- تعتمد صحة التوقيعات الإلكترونية على صحة زوج المفاتيح الشفرية (العام والخاص).
- تستخدم الشهادات لضمان حصة زوج مفاتيح معين.
- إن الشهادة تربط مفتاح شفرى عام معين بهوية معينة (مثلا أسم شخص معين، أسم المضيف في الحاسب الآلي الخ).
- يمكن أن تتضمن الشهادة معلومات أخرى مثل تاريخ الإنتهاء.
- يتم توقيع الشهادة من قبل جهة التصديق الإلكتروني .