## ورقة علمية بحثية بعنوان

# التوقيع الرقمي

## حلول فعالة للمصادقة والتوثيق والآمان


تأليف الدكتور

## كمال الدين يوسف يسن

2012م

## المقدمة

نسبة للإنتشار الواسع للتعاملات الإلكترونية، أصبح التحول من المعاملات الورقية إلى التعاملات الإلكترونية أكثر سهولة وأقل تعقيدا ولكن التحدي يكمن في تنفيذ هذه التعاملات من حيث المصادقة والتأمين، ويمكن النظر إلى تقنية التوقيع الرقمي كآلية للمحافظة على سلامة ونسبة الأمان في التعاملات الإلكترونية. وحيث إن الاعتماد على الإنترنت لتبادل المعلومات والتواصل في تزايد مستمر، فإن المخاوف الأمنية أصبحت أكثر أهمية، فالحاجة ماسة إلى الهوية الرقمية أو التوقيع الرقمي والذي سيعمل على تفعيل تعاملاتنا واتصالاتنا بطريقة أكثر جودة وبنسبة أمان عالية.

فمن الملاحظ أنه عند إجراء المعاملات إلكترونيا، لا يوجد طريقة يمكن من خلالها تأكيد هوية من قام بإرسال أو تسلم المعاملة، ومن هنا تأتي إمكانية استخدام التواقيع الرقمية للمصادقة الإلكترونية على مصدر الرسائل أو المعاملات، فالتوقيع الإلكتروني يؤكد الهوية الحقيقية للمرسل والأهم من ذلك يمكن استخدامه للحفاظ على سلامة البيانات، حيث إن تعديل الرسائل أو المعاملات بعد التوقيع أمر غير وارد مما يشكل أحد مصادر قوة وتميز التواقيع الإلكترونية كحل فعال للمصادقة والتوثيق.

وبالنظر لأهمية أمن وسلامة التعاملات الإلكترونية ومدى الضرر والحرج الذي قد تقع فيه العديد من القطاعات الحكومية والخاصة عند تعرض معاملاتها ووثائقها للقرصنة أو الاستخدام غير المسؤول فإن توافر التواقيع الرقمية بأسعار في متناول الجميع وبطريقة مناسبة للتطبيقات والأعمال كافة أصبح ضرورة، حيث إن هناك ضغطا مستمرا لحماية قطاع الأعمال بشكل عام من الأنشطة الوهمية وسوء الاستخدام، خاصة أن مستوى المخاطر هو نفسه بالنسبة لقطاعات الأعمال كافة بغض النظر عن حجم القطاع، وهذا الأمر يحتم ضرورة تطوير سلامة إجراءات التعاملات الإلكترونية لجميع القطاعات وتنفيذها بفعالية لتحقق مردودا اقتصاديا أعلى.

فمثلاً، الخدمات المصرفية الإلكترونية تتطلب نسبة أمان عالية حتى تتمكن من بناء ثقة العملاء عند استخدامهم

الخدمات الإلكترونية ولكن مع الأسف فإن حالات الاحتيال المصرفي في تزايد مستمر رغم أن العديد من البنوك قام بتطوير آلية الدخول للخدمات البنكية كتأكيد إدخال رقم سري يتم إرساله عبر الأجهزة المحمولة أو غيرها من الأجهزة، ولذلك فإن عددا كبيرا من البنوك العالمية توجه نحو تبني الآليات القائمة على التوقيع الإلكتروني أو الخواص البيومترية لزيادة نسبة الأمان في الوصول للتعاملات البنكية الإلكترونية.

كما أن استخدام التواقيع الإلكترونية سيساعد على الحد من الاعتماد على استخدام الورق في تعاملاتنا كافة وسيعمل في السياق نفسه نحو الجهود الرامية إلى تعزيز مفهوم البيئة الخضراء، فاستخدام التواقيع الإلكترونية له فوائد أخرى ستسهم إن شاء الله في تحمل المسؤولية المشتركة تجاه البيئة والمجتمع.

## تقنية التوقيع الرقمي:

يتم عن طريق صيغة رياضية خلق مفتاحين مختلفين ولكنهما مرتبطين رياضياً، المفتاح الخاص ( Private key) والمفتاح العام (Public key)، الأول والذي لا يعرفه سوى المرسل يستخدم لتشفير البيانات والثاني يستخدم لفك شيفرة الرسالة و يكون معروف لدى الشخص المستقبل أو لدى جهات موثوقة للوصول إليه في حال استدعت الحاجة.

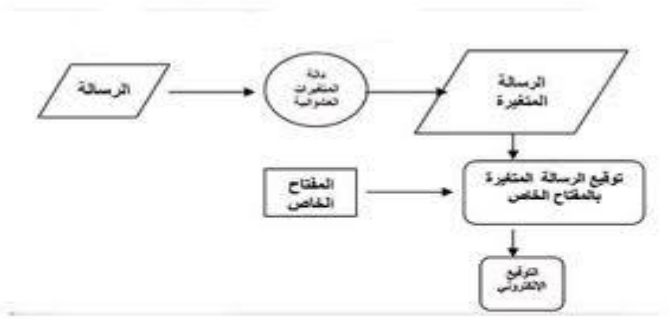
إذا أراد أحدهم ارسال ملف الكتروني موقع رقمياً، تقوم برمجيات خاصة موجودة لدى الموقّع بإنشاء قيمة هاش عن طريق تطبيق وظيفة هاش على البيانات الأصلية، ثم تشفيرتلك القيمة باستخدام المفتاح الخاص للمرسل، وأخيراً يُرفق التوقيع (قيمة هاش بعد التشفير) مع الرسالة. وللتحقق من صحة التوقيع، يستخدم المستقبل المفتاح العام الموافق للمفتاح الخاص للمرسل لفك شيفرة التوقيع، فإن نجحت عملية فك شيفرة التوقيع، فهذا يعني أن المرسل قد وقَّع الرسالة بالفعل، وكخطوة ثانية تقوم برمجيات المستقبل باحتساب نتيجة هاش جديدة للرسالة الأصلية بواسطة نفس وظيفة الهاش المستخدمة في خلق التوقيع الرقمي، فإن تطابقت قيمة هاش للتوقيع الذي

فكت شيفرته مع قيمة هاش التي تم احتسابها من قِبَل برمجيات المستقبل، فهذا يعني أن ملف الرسالة سليم ولم يتعرض لأي تخريب أثناء الارسال.

## خوارزميات التوقيع الرقمي

إن للتوقيع الرقمي ثلاث خوارزميات تمثل مراحل عملية التوقيع الرقمي وهي:-

1. إنتاج أو توليد المفتاح الخاص واختياره من مجموعة من المفاتيح وتتضمن المفتاح الخاص أو السري للمستخدم.
2. عميلة إنتاج التوقيع وإعطائه المفتاح الخاص.
3. التحقق من صحة المفتاح ثم قبوله أو رفضه.




**مراحل التوقيع الرقمي شكل رقم 1**

النتيجة العامة لهذه العملية تسمى التوقيع الرقمي.

إن التوقيع الرقمي يستخدم لخلق نوع من الأساس للمفتاح العام بحيث يكون هذا المفتاح للمستخدم مرتبط بوثيقة وهوية رقمية محددة تصدرها سلطة معينة، وبالتالي فإنه من خلال هذه العملية ترتبط بشكل وثيق معلومات

خاصة عن المستخدم (الاسم، العنوان، رقم الهاتف ..) بمفتاح عام فيصبح هذا المفتاح العام نوع من أنواع التعريف أو الهوية الخاصة للمستخدم.

التواقيع الرقمية تستخدم عادة لتنفيذ التواقيع الإلكترونية بينما العكس ليس صحيحاً لأن ليس كل التواقيع الإلكترونية تستخدم التواقيع الرقمية.

للتوقيع الرقمي في بعض البلدان مثل الولايات المتحدة والإتحاد الأوروبي أهمية قانونية. إن القوانين المتعلقة بالتوقيع الإلكتروني ليست واضحة بينما يتعلق بتعمية أو تشفير التوقيع الرقمي وبالتالي تبقى قانونية هذه التواقيع غير محددة وغير واضحة.

## مزايا استخدام التوقيع الرقمي:

- التأكد من وثوقية المرسل:

بفضل وجود زوج من المفاتيح،عام وخاص، لا يمكن تزوير التوقيع الرقمي إلا في حال معرفة المفتاح الخاص للمرسل.

- التأكد من وثوقية الرسالة:

مقارنة نتائج الهاش تؤكد ما إذا تم التلاعب بالرسالة بعد التوقيع أم حافظت على محتواها نفسه.

- الالتزام:

إن نتيجة وثوقية استخدام المفتاح الخاص عند انشاء توقيع رقمي من قِبَل المرسل يُلزمه بالاعتراف بمحتوى الرسالة ولا يدع له مجالاً للتنكر لها.

- المصداقية:

بالرغم من أن الرسائل تتضمن معلومات عن كيان أو محتوى الرسالة فإن في معظم الوقت لا تكون هذه المعلومات دقيقة، وبالتالي فإنه بالتوقيع الرقمي يمكن المصادقة على مصدر هذه الرسالة.

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.

- 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 فإن إي تغيير فيها سيشكك بمصداقية التوقيع.

- ارتباط التوقيع الرقمي بختم التاريه والتوقيت الصحيح:

إن بروتوكولات التوقيع الرقمي لا تعطي تأكيداً واضحاً عن التاريخ والوقت الذي تم فيهما توقيع الملف إن الموقع قد أو قد 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.

## سلطات المصادقة Certification authorities:

من أجل التأكد من وثوقية توقيع رقمي ما، علينا معرفة المفتاح العام لصاحب التوقيع، والتثبت من تطابقه مع المفتاح الخاص للمرسل.

إن الحل الأفضل في هذه الحالة (في حال عدم معرفتنا للمفتاح العام للجهة المرسلة) هو الاستعانة بطرف ثالث موثوق به، ليزودنا بالمفتاح العام لتلك الجهة مما يزيد من التأكد من صحة توقيعها الرقمي، ذلك الطرف يدعى سلطة المصادقة.

## أنواع الشهادات الرقمية

- **شهادات هيئة التوثيق:**

هذا النوع من الشهادات يصدر من هيئة التوثيق مباشرة وعادة ما يكون لحماية البريد الإلكتروني.

- **شهادات الخادم:**

هذا النوع من الشهادات يصدر من خادم الشبكة (web server) أو خادم البريد (mail server) للتأكد من أمان إرسال واستقبال البيانات.

- **شهادات ناشر البرامج:**

تستخدم للتأكد من أن البرامج الخاصة بناشر معين برامج آمنه .

(X.509) معيار الشهادة الرقمية

هو معيار عالمي أصدره اتحاد الاتصالات الدولي (ITU) لتوحيد شكل وبنية (format) الشهادة الرقمية. أكثر الشهادات الرقمية حاليا تتبع هذا المعيار .

الفرق بين التوقيع الرقمي والشهادة الرقمية:

في التوقيع الرقمي لا يوجد ضمان أن المفتاح العام هو لهذا الشخص بالفعل مثلا يستطيع خالد أن ينشئ له مفتاحين عام وخاص ثم ينشر مفتاحه العام على أساس أنه أحمد فلو أراد شخص أن يرسل رسالة سريه لأحمد سوف يشفرها باستخدام المفتاح العام الذي نشره خالد وبالتالي سوف يستطيع خالد فك تشفير الرسالة والاطلاع عليها . أي أنه في التوقيع الرقمي لا يوجد ربط بين الشخص بالفعل ومفتاحه العام لذلك ظهرت الشهادة الرقمية والتي تربط بين الشخص ومفتاحه العام حيث تحتوي الشهادة على صاحب الشهادة ومفتاحه العام وموقعه من طرف موثوق فيه يثبت ذلك.

## الشهادة الرقمية للتحقق من الهوية Authentication

لنفرض أن أحمد يريد أن يرسل رسالة لخالد لكي يثبت أحمد لخالد بأن المرسل هو بالفعل أحمد فانه سوف يوقع المختصر الحسابي (hash) بالمفتاح الخاص فيه ويرسل الرسالة الأصلية والمختصر الحسابي المشفر لخالد في الطرف الآخر يقوم خالد بفك تشفير المختصر الحسابي باستخدام المفتاح العام لأحمد الموجود في شهادته الرقمية والمتاحة كما ذكرت مسبقا على دليل عام (مخزن الشهادات الرقمية) ثم يقوم بإجراء نفس المختصر الحسابي الذي أجراه احمد على الرسالة بعد ذلك يقارن المختصرين الحسابيين إذا تطابقا فهذا يعني انه بالفعل المرسل هو أحمد. وبهذا ضمنت الشهادة الرقمية التحقق من الهوية. وتسمى العملية السابقة بالتوقيع الإلكتروني.

## الشهادة الرقمية لضمان السرية(Confidentiality)

لنفرض أن أحمد يريد أن يرسل لخالد رسالة سريه فلكي يضمن سريتها سوف يقوم بتشفير الرسالة بالمفتاح العام لأحمد ولن يفك التشفير إلا بالمفتاح الخاص لأحمد (حيث أن المفتاح العام والخاص مربوطة ببعضها أي انه إذا

شفرت رسالة بالمفتاح العام لشخص فانه لا يفك تشفير هذه الرسالة إلا بالمفتاح الخاص لنفس الشخص) وبهذا ضمنت السرية.

## إدارة الشهادات الرقمية

يستطيع الشخص أن يختار هيئة التوثيق (CA) التي يريد إصدار شهادته منها وبعد إصدار الشهادة يمكنه تنزيل و تخزين الشهادة والمفتاح العام (public key)على كمبيوتره. بالنسبة لهيئات التوثيق يوجد بعضها تأتي مع متصفح الانترنت في وقت تنزيله ويكون موثوق فيها( انظر صورة 2).


شكل رقم 2 هيئات التوثيق في متصفح الانترنت

## سياسة الشهادة الرقمية:Certificate Policy

هي مجموعة من القواعد والسياسات الإدارية والتي تطبق عند إدارة الشهادة الرقمية في جميع مراحل حياتها[3].

## دورة حياة الشهادات الرقمية:

هناك بعض الأحداث التي تؤثر على فعالية الشهادة الرقمية مثل إضافة جهاز (hardware) جديد على الكمبيوتر أو تحديث برنامج وغيره لذلك أصبح للشهادة الرقمية حالات تمر فيها منذ إصدارها.

- **الإصدار:**

وهي أول مرحلة وتشمل التأكد من هوية الشخص قبل الإصدار. ويعتمد التأكد على نوع الشهادة المصدرة ففي الشهادات الرقمية التي تصدر للبريد الالكتروني يتم التأكد من هوية الشخص بطلب إرسال رسالة من بريده الالكتروني فقط أما الشهادات الرقمية المستخدمة للعمليات المالية فتتطلب إجرآت اخرى للتأكد من الهوية . بعد التأكد من الهوية يتم إرسال الطلب لهيئة التوثيق وتوافق على إصدار الشهادة.

- **الإلغاء:**

يستطيع الشخص أن يلغي شهادته قبل تاريخ انتهائها عندما يفقد المفتاح الخاص بالشهادة أو ينتشر لأنه بعد انتشار المفتاح الخاص تبطل فعالية الشهادة وهي الثقة بالطرف الآخر.(Authentication) ويتم إضافة الشهادة الملغاة إلى قائمة الشهادات الملغاة.

- **الانتهاء:**

لكل شهادة تاريخ انتهاء بعد هذا التاريخ تصبح الشهادة غير صالحه للاستخدام ولابد من إصدار شهادة جديدة ويمكن أن تكون الشهادة الجديدة لها نفس المفتاح العام والخاص للشهادة المنتهية.

- **التعطيل المؤقت:**

يمكن للشخص أن يوقف أو يعطل استخدام الشهادة لفترة زمنية لا يحتاج فيها لاستخدام الشهادة حتى لا تستغل من قبل أشخاص آخرين.

## كيفية الحصول على الشهادة الرقمية المستخدمة لغرض حماية البريد المثالي:

1. اذهب إلى احد المواقع الإلكترونية التي تمنح الشهادات على سبيل المثال .comodo
2. قم بتعبئة البيانات المطلوبة ( الاسم الأول، الاسم الأخير، عنوان البريد الإلكتروني، البلد، الرقم السري لإلغاء الشهادة.

## شهادات المفتاح العام Public key certificates:

تقوم سلطة المصادقة باصدار شهادات يكون موضوعها المفتاح العام لجهة معينة أو شخص، يملك بالمقابل المفتاح الخاص، يمكن الحصول على تلك الشهادات مجاناً وعند الطلب.

يتخذ المشترك في شهادة المفتاح العام توقيع رقمي يمكنه الاعتماد عليه لتأمين رسائله التي تحتاج إلى وثوقية، وبإمكان ذلك المشترك أيضاً استخدام المفتاح العام المذكور في الشهادة للتأكد من صحة التوقيع الرقمي أي التأكد بأنه قد تم انشاءه من قِبَل المفتاح الخاص المقابل. ومن ثم تقوم سلطة المصادقة أيضاً بتوقيع الشهادة رقمياً لتأكيد وثوقيتها أكثر، الذي يمكن التأكد من صحته باستخدام المفتاح العام، الخاص بسلطة المصادقة، والمعرَّف في شهادة أخرى من قِبَل سلطة مصادقة أخرى (يمكن أن تكون على مستوى أعلى بالرتبة).

وتلك الشهادة الأخرى يمكن توثيقها بدورها بواسطة المفتاح العام، المعرَّف أيضاً في شهادة أخرى وهكذا...

إن هذه الهرمية بتسلسل سلطات المصادقة يمنحها مزيداً من الضمان والثقة.

إن استخدام التوقيع الرقمي يفتح لنا فرص واسعة في مجالات عديدة، مثل تبادل البضائع، طلب قروض، تفويض الخ... كل الأمور التي كانت تتطلب توقيع ورقي أصبح بالامكان ممارستها عبر الشبكة وأصبح اجراء الصفقات التجارية أسهل، أسرع، أكثر أماناً وأقل تكلفة.

## متطلبات التوقيع الرقمي

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

1. قيمة الخوارزميات: بعض مفاتيح الخوارزميات غير آمنة وقد تم إثبات خرق البعض منها.
2. قيمة التنفيذ: تنفيذ وتطبيق خوارزميات مع أخطاء لن يؤدي إلى أي نتيجة.
3. المفتاح الخاص يجب أن يبقى سري وبالتالي فإنه إذا عرضه أحد الفرق فإن هذا الفريق يستطيع أن يصدر ويقلد أي توقيع.

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

## مقارنة بين التوقيع الرقمي والتواقيع الأخري

يستخدم اليوم وعلى نطاق واسع أنماط متعددة من التواقيع ، أولها وأشهرها وأكثرها تداول التوقيع الحيوي أو التوقيع التقليدي العادي الذي يعتمد على حركات اليد وهو بهذا الشكل يعتبر مبرئي للزمة ومعتدماً ولدية طرق للتثبت منه واثبات مرجعيته لمصدره ، ومن مساوئ هذا النوع من التواقيع سهولة تقليدة وتزويرة .

كما يستخدم أيضاً مايعرف بالتوقيع الالكتروني وهو توقيع يعتمد بالأساس على التوقيع العادي ويتم إدخالة الى الوسائط الالكترونية عن طريق بعض وحدات الادخال مثل الماسحات الضوئية.

مقارنة التوقيع الرقمي بالتواقيع الاخرى تثبت تفوقا واضح له حيث ان التوقيع الرقمي لايمكن تزويرة لانه لا يعتمد على حركات اليد ولايقوم به الانسان ، التوقيع الرقمي عبارة عن جزء صغير من البيانات المشفرة والموثوقة تزيل به الرسائل والمعاملات لصحة نسبتها الى مصدرها، كما ان الأنظمة التي يعتمدها التوقيع الرقمي تراعي أعلى مضامين السلامة والأمن في نقله وتوزيعة .

بالاضافة الى ذلك فان التوقيع الرقمي بدأ يستخدم الأن وعلى نطاق واسع في كل المعاملات الالكترونية لما يشكله من إعتمادية وموثوقية وملائمة عالية مع البيئة الالكترونية والرقمية المتمثله في معاملات البنوك والتجارة الالكترونية والحكومة الالكترونية والمعاملات الشبيه.

## التوقيع الرقمي في التشريعات المقارنة

يعرف الفقه التوقيع الإلكتروني بأنه: "هو الذي يقوم على مجموعة من الإجراءات والوسائل الذي يتيح استخدامها عن طريق الرموز أو الأرقام إخراج رسالة إلكترونية تتضمن علامة مميزة لصاحب الرسالة المنقولة إلكترونياً يجرى تشفيرها باستخدام خوارزم المفاتيح واحد معلن والآخر خاص بصاحب الرسالة

وهناك تعريف آخر للتوقيع الإلكتروني وهو: مجموعة من الإجراءات التقنية التي تسمح بتحديد شخصية من تصدر عنه هذه الإجراءات وقبوله بمضمون التصرف الذي يصدر التوقيع بمناسبته. ولقد ركز التعريف الأول على الوسيلة التي يتم بها إنشاء التوقيع، كما أبرز النتيجة المترتبة على ذلك وهو إخراج رسالة إلكترونية تتضمن علامة مميزة لصاحب التوقيع الإلكتروني، كما ركز على التوقيع الرقمى وأنه أحد صور التوقيع الإلكتروني الذي يقوم على تشفير المفتاح العام والخاص، بينما لم يحدد التعريف الثاني صور التوقيع التي يمكن أن تكون توقيعاً إلكترونياً بل اكتفى بذكر أنها مجموعة من الإجراءات التقنية، وهو ما يجعل التعريف لا يقف في وجه أى تطور تقنى مستقبلى في صور التوقيع الإلكتروني. كما أبرز وظائف التوقيع الإلكتروني التي يجب أن تسعى إليها الإجراءات التقنية المعترف بها وهى تحديد هوية الموقّع والتعبير عن إرادته بالموافقة على مضمون السند الذي

وقع عليه.

ولقد تصدت أكثر من منظمة لتعريف التوقيع الإلكتروني من خلال قوانين التجارة الإلكترونية أو من خلال قوانين وضعت خصيصا للتوقيع الإلكتروني، ومن هذه المنظمات: لجنة الأمم المتحدة للتجارة الدولية المعروفة بالأونسترال وأيضا الاتحاد الأوروبي إحدى المنظمات الإقليمية .

## التوقيع الرقمي في قواعد الأونسترال

وضعت لجنة الأمم المتحدة للتجارة الألكترونية (الأونسترال) القواعد الموحدة بشأن التوقيعات الإلكترونية وهي :

.1عدم تحديد نوع الطريقة التي يتم بها استخدام التوقيع الإلكتروني، فاتحاً المجال لإيراد أية طريقة تراها الدول ملائمة من ترميز أو تكويد أو تشفير أو أية طريقة أخرى تكون مناسبة.

.2أن التعريف ركز على أن أية طريقة للتوقيع يجب أن تحقق وظائف التوقيع من تحديد لهوية الشخص الموقع والتعبير عن إرادته بالموافقة على مضمون رسالة البيانات، ومن المؤكد أن كل توقيع أيا كانت الطريقة المستخدمة في إنشائه يجب أن يحقق تلك الوظائف .

## التوقيع الرقمي في التشريعات الدولية

تم تعريف التوقيع الإلكتروني في القانون الأمريكي: في المادة 8/102 بأنه: "التوقيع الذي يصدر في شكل إلكتروني ويرتبط بسجل إلكتروني.

تعريف التوقيع الإلكتروني في قانون المعاملات الإلكترونية الموحد حيث عرف بأنه:" صوت أو رمز أو إجراء يقع في شكل إلكتروني يلحق (يرتبط منطقياً) بعقد أو سجل آخر (وثيقة) ينفذ أو يصدر من شخص بقصد التوقيع على السجل.

ويلاحظ أن التعريفات لم تشر بشكل مانع جامع لصور التوقيع الإلكتروني، بل أشارت إلى بعض صوره مثل

الأصوات أو الرموز، كما أن التعريفات لم تربط التوقيع بشكل مادى محدد بل أشارت إلى كونه مرتبطاً بسجل ارتباطاً منطقياً.

وتعرف القوانين الأمريكية السجل الإلكتروني بأنه: أي عقد أو أي سجل آخر جرى إنشاؤه أو إرساله أو استقباله أو تخزينه بالوسائل الإلكترونية.

## التوقيع الرقمي في توجيهات الاتحاد الاوروبي

يعرف الاتحاد الأوروبي نوعين من التوقيع الإلكتروني ووضع لكل نوع تعريفاً محدداً هما :

1.التوقيع الإلكتروني: معلومات على شكل إلكتروني متعلقة بمعلومات إلكترونية أخرى ومرتبطة بها ارتباطاً وثيقاً ويستخدم أداة للتوثيق.

2. التوقيع الإلكتروني المعزز: هو توقيع إلكتروني يشترط فيه أن يكون :

- مرتبطا إرتباطاً فريداً من نوعه مع صاحب التوقيع.
- قادراً على تحقيق تحديد صاحب التوقيع والتعرف عليه باستخدامه.
- تم إيجاده باستخدام وسائل يضمن فيها صاحبه السرية التامة.
- مرتبطاً مع المعلومات المحتواة في الرسالة حيث أنه يكشف أي تغيير في المعلومات .

## الحماية التكنولوجية للتوقيع الرقمي

تقوم عملية حماية التوقيع الإلكتروني على تشفير المعلومات أي تحويلها إلى صيغة رياضية لمنع الأشخاص غير المرخص لهم من الاطلاع على المعلومات أو فهمها. وتستخدم المفاتيح في تشفير المعلومة. وتعتمد قوة وفعالية التشفير على عاملين أساسيين هما: " الخوارزمية وطول المفاتيح مقدرا بالبت. وعملية فك التشفير تعنى إعادة تحويل البيانات إلى صيغتها الأصلية التي يمكن عن طريقها الإفصاح عن التوقيع الإلكترونيالمعتمد.

يرتبط التشفير بالتوقيع الإلكتروني ارتباطاً وثيقاً، فالتشفير هو التغيير في البيانات بحيث لا يتمكن من قراءتها

سوى الشخص المستقبل وحده باستخدام مفتاح فك التشفير، وفي تقنية المفتاح العام يتوفر المفتاح ذاته لدى المرسل والمستقبل، ويستخدم في عمليتى التشفير وفك التشفير، ومن هنا تتبين العلاقة بين التوقيع الإلكتروني والتشفير فالتوقيع الإلكتروني هو ختم إلكتروني مشفر يملك مفتاحه صاحب التوقيع.

إن تقنية التشفير تعطي قوة للوثيقة الإلكترونية المشفرة من جهة الحجية والقوة في الإثبات حيث تقوم بعض تقنيات كبرنامج Privacy Paarett good PPG بحماية البيانات وصعوبة فك وكسر الشفرة، وهذا يعطى الوثيقة الإلكترونية التي تم استخدام تقنية التشفير فيها قوة في الإثبات والنفى، فإن من المعمول عليه في اعتبار قوة الحجية وعدمها مدى ما يعترى هذه البينة من عوامل للتغيير والتحريف والتزوير، فإنه إذا ما كان القيام بذلك صعباً كان ذلك أقوى في اعتبار الحجية والعكس بالعكس.

## الحماية القانونية للتوقيع الرقمي

إن ازدهار المعاملات الإلكترونية متوقف على كم الضمانات التي تحوز عليها هذه المعاملات وخاصة لو أخذنا في الاعتبار أنها تتم آلياً أو إلكترونياً بين أشخاص لا يعرفون بعضهم البعض ولا يلتقون، فهي تجارة عن بعد أو بالأحرى معاملات وتعاملات عبر شبكة الإنترنت، الأمر الذي لا يستبعد فيه وقوع التزوير أو التلاعب في التوقيع الإلكتروني، من هنا كان من الضرورى الاهتمام بتوافر الضمانات اللازمة لإضفاء الثقة لدى المتعاملين بالتوقيع الإلكتروني فقد سعت كثير من التشريعات إلى اتخاذ وسائل تضمن ثقة المتعاملين مع وسائل الاتصال الجديدة، فهناك من اقترح ما يعرف بنظام (غير الثقة) بحيث يوجد مفتاحان: مفتاح عام ومفتاح خاص، ويحمل كل مفتاح علاقة رياضية غير مفهومة، ويبقى المفتاح الخاص مع المستخدم أو العميل بحيث لا يستعمله إلا هو، فإذا استعمله في أيه عملية قانونية وصدر منه توقيع يعدّ ذلك قرينة على أنه شخصيا استعمل المفتاح. ولمواجهة تقنيات القرصنة الإلكترونية ابتكر العلماء تقنيات متقدمة لأمن المعلومات المتبادلة على الخط ومنها سلاسل التشفير التي شهدت المزيد من التطور بما يضمن الأمان للمتخاطبين عبر الشبكات الإلكترونية بحيث لا

تنفك رموز رسائلهم وتعاقداتهم إلا من الجهة التي تمتلك المفتاح المزودة من قبلها. إلا أن التشفير هذا استلزم وضع قواعد تشريعية ومعايير محددة تضمن الاستفادة من الفوائد والإيجابيات وفي ذات الوقت تضمن إنسياب المعلومات والاتصالات. وتعرف عملية التشفير بأنها (تحويل المعلومات إلى صيغة غير مفهومة لمنع الأشخاص غير المرخص لهم من الاطلاع على المعلومات أو فهمها).

ويرتبط التشفير بالتوقيع الإلكتروني ارتباطاً وثيقاً، فالتشفير هو التغيير في البيانات بحيث لا يتمكن من قراءتها سوى الشخص المستقبل وحده، باستخدام مفتاح فك التشفير، وفي تقنية المفتاح العام يتوفر المفتاح ذاته لدى المرسل والمستقبل، ويستخدم في عمليتى التشفير وفك التشفير، ومن هنا تتبين العلاقة بين التوقيع الإلكتروني والتشفير فالتوقيع الإلكتروني هو ختم إلكتروني مشفر يملك مفتاحه صاحب الختم. إن تقنية التشفير تعطى قوة للوثيقة الإلكترونية المشفرة من جهة الحجية والقوة في الإثبات، ولذا فإن من المعول عليه في اعتبار قوة الحجية وعدمها مدى ما يعترى هذه البينة من عوامل التغيير والتحريف والتزوير، فإنه إذا كان إمكان القيام بذلك صعبا كان ذلك أقوى في اعتبار الحجية والعكس بالعكس.

# المراجع


## 1.المواقع الالكترونية

موقع الموسوعة الحرة 27/11/2012

http://kenanaonline.com/users/ahmedkordy/posts/323677

27/11/2012

http://coeia.edu.sa/index.php/ar/asuurance-awarness/articles/55-information-assurance-management-and-governance/940-digital-certificates.html

27/11/2012

## 2.المقالات

رها القوتلي

فهد الحربي