الفصل السادس

التوقيع الإلكتروني[1] E-Signature

لقد بدأت عصر التعاملات الإلكترونية بالظهور والانتشار مؤخراً بعد الاعتراف بالتوقيع الإلكتروني قانونياً وبدأت الخطوات العلمية لتعميم استخدامها لتكون أداة التعاملات المستقبلية بين الناس حيث أنها تسهل عليهم أعمالهم ومهماتهم ولقد حصل قطاع الأعمال الإلكترونية على دعم كبير ودفعة قوية من قبل الحكومة الأمريكية خاصة بعد اعتماد الكونجرس الأمريكي لعدة قرارات وتشريعها هامة خاصة بالتوقيع الإلكتروني لإضفاء الشرعية والصفة القانونية لها ليكون كالتوقيع اليدوي تماماً في التعاملات المالية والتجارية فتعالوا معنا نتعرف عليه وعلى فائدته وكيفية عمله.

ما هو التوقيع الإلكتروني؟

لا يوجد تعريف بسيط للتوقيع الإلكتروني **Digital Signature ولكن في حال وجود مثل هذا التعريف فإنه يمكن أن يكون مشابهاً للتعريف التالي: طريقة اتصال مشفرة تعمل على توثيق المعاملات التي تتم عبر الإنترنت.**

بشكل أساسي فإن الفكرة الكامنة وراء التوقيعات الإلكترونية هي نفسها كما في التوقيع المكتوب بخط اليد. إنك تستخدمه للتصديق أو لتوثيق الحقيقة بأنك وعدت بشيء ما ولا تستطيع التراجع عنه فيما بعد. إن التوقيع الإلكتروني لا يتضمن القيام بتوقيع شيء ما باستخدام القلم والورقة وبعد ذلك إرساله عبر الإنترنت ولكنه مثل التوقيع على الورق يلتصق بهوية الموقع على معاملة ما.

يجب أن يكون للتوقيع بشكل عام الصفات المميزة التالية :

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 متسللاً يزعم بكونه الطرف المرسل.

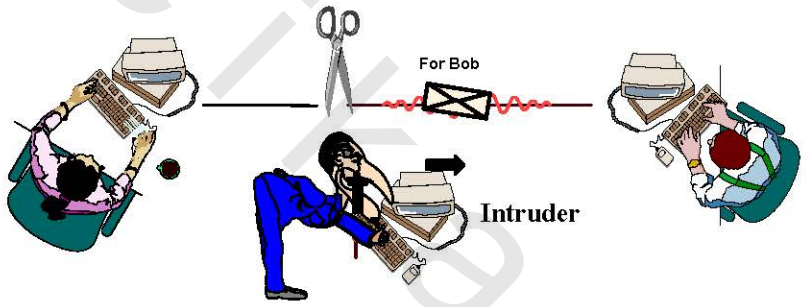
---

[1] www.egovs.com 2005

بأنك وعدت بشيء ما ولا تستطيع التراجع عنه فيما بعد. إن التوقيع الإلكتروني لا يتضمن القيام بتوقيع شيء ما باستخدام القلم والورقة وبعد ذلك إرساله عبر الإنترنت ولكنه مثل التوقيع على الورق يلتصق بهوية الموقع على معاملة ما.

يجب أن يكون للتوقيع بشكل عام الصفات المميزة التالية :

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 متسللاً يزعم بكونه الطرف المرسل.



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

- **ماهية التوقيع الرقمي (Digital Signature)**

يُستَخدَم التوقيع الرقمي للتأكد من أن الرسالة قد جاءت من مصدرها دون تعرضها لأي تغيير أثناء عملية النقل. ويمكن للمرسِل استخدام المفتاح الخاص لتوقيع الوثيقة إلكترونياً. أما في طرف المستقبل، فيتم التحقّق من صحة التوقيع عن طريق استخدام المفتاح العام المناسب.

- **عملية توقيع رقمي تقليدية**

وباستخدام التوقيع الرقمي، يتم تأمين سلامة الرسالة والتحقّق من صحتها.

ومن فوائد هذا التوقيع أيضاً أنه يمنع المرسِل من التنكّر للمعلومات التي أرسلها. ومن الممكن اعتماد طريقة أخرى تتلخّص في الدمج بين **مفهومي البصمة الإلكترونية للرسالة والمفتاح العام**، وهذه الطريقة أكثر أمناً من العملية النموذجية التقليدية. ويتم أولاً تمويه الرسالة لإنشاء بصمة إلكترونية لها، ثم تُشفَّر البصمة الإلكترونية باستخدام المفتاح الخاص للمالك، مما ينتج عنه توقيع رقمي يُلحَق بالوثيقة المُرسَلة. وللتحقُّق من صحة التوقيع، يستخدم المستقبِل المفتاحَ العام المناسب لفك شيفرة التوقيع، فإن نجحت عملية فك شيفرة التوقيع (بإعادتها إلى ناتج اقتران التمويه)، فهذا يعني أن المرسِل قد وقّع الوثيقة بالفعل، إذ إن أي تغيير يحصل على هذه الوثيقة الموقّعة (مهما كان صغيراً)، يتسبب في فشل عملية التحقُّق. وتقوم برمجيات المستقبِل بعد ذلك بتمويه محتوى الوثيقة لينتج عن ذلك بصمة إلكترونية للرسالة، فإن تطابقت القيمة المموّهة للتوقيع الذي فُكَّت شيفرته مع القيمة المموّهة للوثيقة، فهذا يعني أن الملف سليم ولم يتعرض لأي تغيير أثناء النقل.

- **خوارزميات البصمة الإلكترونية للرسالة (MD2, MD4, MD5)**

طوّر رونالد رايفست- Ronald Rivest- خوارزميات MD2 و MD4 و MD5 الخاصة بالبصمة الإلكترونية للرسالة. وهذه الخوارزميات هي اقترانات تمويه يُمكن تطبيقها على التواقيع الرقمية. وبدأ ظهور هذه الخوارزميات عام ١٩٨٩ بخوارزمية MD2، ثم تلتها خوارزمية [MD4 MD4] عام ١٩٩٠، ثم خوارزمية MD5 عام ١٩٩١. ويُولِّد كل من هذه الخوارزميات بصمة إلكترونية للرسالة بطول ١٢٨ بت. ورغم وجود تشابه كبير بين MD4 و MD5، إلا إن خوارزمية MD2 تختلف عنهما. ومن ناحية أخرى، فإن خوارزمية MD2 هي أبطأ هذه الخوارزميات، على حين أن خوارزمية MD4 هي أسرعها. أما أكثر هذه الخوارزميات أماناً فهي MD5؛ وهي تستند أساساً إلى خوارزمية MD4 مُضافاً إليها بعض خصائص الأمان الأكثر إحكاماً. ويمكن تطبيق خوارزمية MD2 بوساطة أجهزة كمبيوتر ذات ٨ بت (٨- computers bit)، بينما يلزم أجهزة كمبيوتر ذات ٣٢ بت لتطبيق خوارزميتي MD4 و MD5.

التوقيع الإلكتروني:

هو ملف رقمي صغير (شهادة رقمية) تصدر عن أحد الهيئات المتخصصة والمستقلة والمعترف بها من الحكومة تماماً مثل كتابة العدل وفي هذا الملف يتم تخزين اسمك وبعض المعلومات المهمة الأخرى مثل رقم التسلسل وتاريخ انتهاء الشهادة ومصدرها، وهي تحتوي عند تسليمها لك على مفتاحين(المفتاح العام والمفتاح الخاص) ويعتبر المفتاح الخاص هو توقيعك الإلكتروني الذي يميزك عن بقية الناس أما المفتاح العام فيتم نشرة في الدليل وهو متاح للعامة من الناس.

الحاجة لها وأهميتها:

كما تعلمون أن مشكلة الأمن والخصوصية على شبكة الإنترنت تشغل حيزاً كبيراً من اهتمام المسؤولين كما تثير قلق الكثير من الناس مما يسبب نوعاً من انعدام الثقة بهذه الشبكة ولذلك تم اللجوء إلى تكنولوجيا التوقيع الإلكتروني حتى يتم الرفع من مستوى الأمن والخصوصية للمتعاملين مع الشبكة ويتم ذلك بقدر قدرة هذه التكنولوجيا على الحفاظ على سرية المعلومات أو الرسالة المرسلة وعدم قدرة أي شخص آخر على الاطلاع أو تعديل أو تحريف الرسالة، كما يمكنها أن تحدد شخصية وهوية المرسل والمستقبل إلكترونياً والتأكد من مصداقية هذه الشخصيات مما يسمح لها بكشف أي متحايل أو متلاعب، فمثلاً لو كنت تأجراً أو رجل أعمال في السعودية وتريد عقد صفقة مع زميل لك في أمريكا أو اليابان وتنتظر منه معلومات حساسة ومهمة لاتخاذ القرار عن طريق البريد الإلكتروني فكيف تعرف أو تتأكد بأن هذه الرسالة فعلاً من ذلك الشخص فعلاً؟ وكيف تتأكد من أن المعلومات هي نفس المعلومات الأصلية ولم يتم العبث بها من قبل شخص آخر على الشبكة؟ وكيف تتأكد من سرية هذه المعلومات وعدم اطلاع أي أحد من المنافسين على هذه المعلومات؟ ولذلك فإن الحل الوحيد هو استخدام التوقيع الإلكتروني.

كيف تعمل تقنية التوقيع الإلكتروني:

التشفير بواسطة مفتاح الشفرة العام **Public Key Cryptography** (شفرة تستخدم مفتاحين متناظرين أحدهما سري ويحفظه مستلم البيانات والآخر عمومي)

يتم انشاء التوقيعات وكذلك التثبت من صحتها من خلال التشفير وهو فرع من الرياضيات التطبيقية المختصة بتحويل الرسائل إلى أشكال تبدو وكأنها لا يمكن فهمها وإعادتها مرة أخرى كما كانت. تستخدم التوقيعات الإلكترونية ما يعرف بنظام شفرة المفتاح الشفرى العام والذي يستخدم منهجاً معيناً مستعيناً بمفتاحين مختلفين ولكنهما مرتبطين حسابياً، واحد لإنشاء التوقيع الإلكتروني أو لتحويل البيانات إلى أشكال تبدو وكأنها لا يمكن فهمها والمفتاح الآخر للتثبت من صحة التوقيع الإلكتروني أو لإعادة الرسالة إلى شكلها الأصلي. تدعى أجهزة وبرامج الحاسب الآلي التي تستخدم مثل هذين المفتاحين عادة " نظام التشفير اللا تماثلي **asymmetric**".

إن المفاتيح التكميلية في نظام الشفرة اللاتماثلية للتوقيعات الإلكترونية تدعى عشوائياً المفتاح الخاص والذي يعرفه فقط الموقع ويستخدم لإنشاء التوقيع الإلكتروني ومفتاح الشفرة العام والمعروف عادة على نطاق أوسع ويستخدم من قبل شخص موثوق به للتثبت من صحة التوقيع الإلكتروني. في حال استدعت الظروف أن أكثر من جهة بحاجة للتثبت من صحة التوقيع الإلكتروني فإن مفتاح الشفرة العام يجب أن يكون متوفراً لتلك الجهات أو يوزع عليهم جميعاً أو ربما يتم نشره في ملف للاتصال المباشر حيث من الممكن الوصول إليه بسهولة. بالرغم من أن كلا المفتاحين مرتبطان ببعضها رياضياً فإنه في حال تم تصميم نظام الشفرة اللا تماثلي وتم تطبيقه بشكل آمن فإنه حسابياً لا يمكن التوصل إلى معرفة المفتاح الخاص من خلال معرفة المفتاح الشفرى العام. وبهذا فإنه بالرغم من أن العديد من الأشخاص يمكن أن يكونوا على علم بالمفتاح الشفرى العام لموقع ما ويستخدمونه للتثبت من صحة توقيعات موقع معين إلا أنهم لا يستطيعون اكتشاف المفتاح الخاص لذلك الموقع واستخدامه في تزوير توقيعاته الإلكترونية.

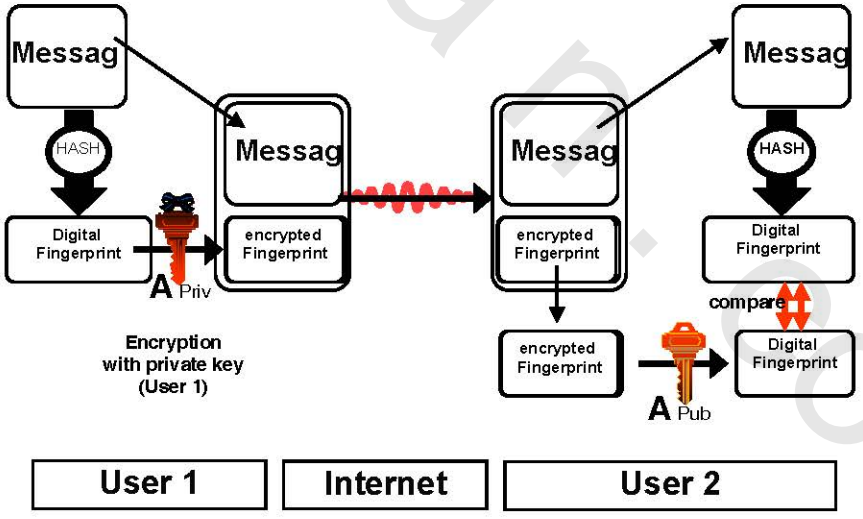
وظيفة الـ هاش Hash Function

عملية رئيسية وأساسية أخرى تدعى " وظيفة الـ هاش " وهي تستخدم في كلا عمليتي إنشاء التوقيع الإلكتروني والتثبت من صحته. إن وظيفة هاش هي عبارة عن

منهج يعمل على إنشاء تمثيل رقمي معين أو بصمة إصبع على شكل قيمة " هاش" أو " نتيجة هاش" بطول مقياسي يكون عادة أصغر من الرسالة ولكنه مقترن بالرسالة ومحصور بها. أي تغيير في الرسالة ينتج عنه نتيجة هاش مختلفة عند استخدام وظيفة الـ هاش نفسها. في حالة وظيفة الـ هاش الآمنة والتي تدعى أحياناً " وظيفة الـ هاش الأحادية الاتجاه" فإنه من الناحية الحسابية لا يمكن التوصل إلى الرسالة الأصلية من خلال معرفة قيمة الـ هاش الخاصة بها. لذلك فإن وظائف الـ هاش تتيح للبرمجيات إنشاء توقيعات إلكترونية للعمل على كمية أصغر يمكن التنبؤ بها من البيانات وفي نفس الوقت ما زالت توفر تلازماً قوياً وواضحاً مع محتويات الرسالة الأصلية وبهذا تعمل على توفير الضمان الفعال والتأكيد بأنه لم يتم إجراء أي تعديل على الرسالة منذ أن تم توقيعها إلكترونياً.

تدفق أو سير العمل

الرسم التالي يوضح سير العمل الأساسي لتوقيع إلكتروني تم استخدامه لإرسال رسالة :



كما يتضح من الرسم أعلاه فإن استخدام التوقيعات الإلكترونية عادة

يتضمن عمليتين، واحدة يتم إنجازها من قبل الموقع والأخرى من قبل مستلم التوقيع الإلكتروني:

إنشاء التوقيع الإلكتروني يستخدم نتيجة هاش يتم اشتقاقها من الرسالة وتكون مقتصرة على كل من الرسالة الموقعة ومفتاح خاص معين. بغرض أن تكون نتيجة الـ هاش آمنة ومحكمة يجب أن لا يكون هناك إمكانية أو احتمال ضئيل فقط بأن نفس التوقيع الإلكتروني يمكن إنشاؤه من خلال تركيبة أي رسالة أخرى أو مفتاح خاص آخر.

التثبت من صحة التوقيع الإلكتروني: وهي عملية التأكد من التوقيع الإلكتروني من خلال الرجوع إلى الرسالة الأصلية وإلى مفتاح عام معين وبهذا يتم تحديد ما إذا كان التوقيع الإلكتروني قد تم إنشاؤه لتلك الرسالة باستخدام المفتاح الخاص المقابل للمفتاح العام المشار إليه.

لتوقيع وثيقة معينة أو أي معلومات معينة، على الموقع أولاً أن يعين بدقة الحدود لما يراد توقيعه. إن المعلومات التي تم تعيينها أو تحديدها كي يتم توقيعها تدعى "الرسالة" في هذه الإرشادات. بعد ذلك تقوم وظيفة هاش معينة في برنامج الموقع باحتساب نتيجة الـ هاش المقتصرة (لكافة الأغراض العملية) على الرسالة. بعد ذلك يقوم برنامج الموقع بتحويل نتيجة الـ هاش إلى توقيع إلكتروني باستخدام المفتاح الخاص للموقع. إن التوقيع الإلكتروني الناجم عن ذلك هو مقتصر على كل من الرسالة والمفتاح الخاص المستخدم في إنشائه. أي أن لكل رسالة موقعة إلكترونياً يكون التوقيع المنشأ هو توقيع فريد.

نموذجياً يكون التوقيع الإلكتروني (نتيجة هاش للرسالة موقعة إلكترونياً) مرتبطاً ومرفقاً برسالته ويخزن أو يرسل مع رسالته. على أية حال يمكن أن يرسل أو يخزن أو يحفظ كعنصر بيانات منفصل طالما أنه يحافظ على ارتباط موثوق به مع رسالته. بما أن التوقيع الإلكتروني مقتصر وينحصر في رسالته فإنه لن يكون له أي فائدة أو نفع عندما يتم فصله كلياً عن رسالته.

يتم التثبت من صحة التوقيع الإلكتروني من خلال احتساب نتيجة هاش جديدة للرسالة الأصلية بواسطة نفس وظيفة الـ هاش المستخدمة في إنشاء التوقيع الإلكتروني. بعد ذلك وباستخدام مفتاح الشفرة العام ونتيجة هاش الجديدة يقوم الطرف الذي يعمل على التثبت من الصحة بالتأكد من ١) ما إذا كان قد تم إنشاء التوقيع الإلكتروني باستخدام المفتاح الخاص المقابل و ٢) ما إذا كانت نتيجة الـ هاش التي تم احتسابها مؤخراً مطابقة لنتيجة الـ هاش الأصلية والتي تم تحويلها إلى توقيع إلكتروني خلال عملية التوقيع. إن برامج التثبت من الصحة سوف تؤكد "صحة" التوقيع الإلكتروني في حال : ١) كان قد تم استخدام مفتاح الموقع الخاص لتوقيع الرسالة إلكترونياً وهذا ما سيكون الحال عليه لو أنه تم استخدام مفتاح الموقع العام للتثبت من صحة التوقيع لأن مفتاح الشفرة العام الخاص بالموقع سوف يثبت فقط صحة توقيع إلكتروني تم إنشائه بواسطة مفتاح الموقع الخاص. و ٢) بأن الرسالة لم يتم تغييرها وهذا يكون في حال كانت نتيجة الـ هاش التي تم احتسابها من قبل المتثبت من الصحة مشابهة ومطابقة لنتيجة الـ هاش المستخرجة من التوقيع الإلكتروني خلال عملية التثبت من الصحة.

❖ الأهداف العامة والأغراض من استخدام التوقيع الإلكتروني:

إن عمليات إنشاء التوقيع الإلكتروني والتثبت من صحته تحقق التأثيرات الجوهرية المرجوة من التوقيع لعدة أغراض قانونية :

توثيق الموقع : في حال كان هناك زوج من المفاتيح واحد عام والآخر خاص وكانا مرتبطين بموقع معين ومحدد فإن التوقيع الإلكتروني ينسب ويعزو الرسالة إلى الموقع. لا يمكن تزوير التوقيع الإلكتروني ما لم يفقد الموقع السيطرة على المفتاح الخاص (تعرض المفتاح الخاص للخطر) كأن يقوم بإفشائه أو يفقد الوسط أو الوسيلة المحتفظ به فيها مثل البطاقة الذكية.

توثيق الرسالة : كذلك فإن التوقيع الإلكتروني يعمل على تحديد هوية الرسالة الموقعة بثقة ودقة ويقين أكثر من التوقيعات على الورق. إن عملية التثبت من الصحة تكشف أي تلاعب حيث أن مقارنة نتائج الـ هاش (واحدة يتم إعدادها

عند التوقيع والأخرى عند التثبت من الصحة) تبين ما إذا كانت الرسالة هي نفسها عندما تم توقيعها.

عمل إيجابي : إن انشاء توقيع إلكتروني يتطلب من الموقع أن يستخدم مفتاح الموقع الخاص وهذا العمل بإمكانه أن ينجز الوظيفة الرئيسية في تنبيه الموقع إلى حقيقة أن الموقع يقوم باستكمال معاملة لها عواقب ونتائج قانونية.

الفعالية : إن عمليات إنشاء التوقيع الإلكتروني والتثبت من صحته تتطلب مستوى عالياً من الضمان بأن التوقيع الإلكتروني هو للموقع بدون تكلف أو رياء. مقارنة مع الأساليب الورقية مثل بطاقات نموذج اعتماد التوقيع والتي هي أساليب مملة و تستغرق الكثير من الجهد بحيث أنه نادراً ما يتم استخدامها بالواقع – فإن التوقيعات الإلكترونية تعطي وتولد درجة ضمان أعلى بدون أن تضيف كثيراً على الموارد المطلوبة للمعالجة.

❖ شهادات التصديق الإلكتروني Public Key Certificates

للتثبت من صحة توقيع إلكتروني معين، على الطرف الذي يقوم بالتثبت من الصحة أن يكون قادراً على الوصول إلى مفتاح الموقع العام وأن يكون واثقاً 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 استراتيجية 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 موقعاً معيناً 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 الشفرى 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 الشفرى 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 اسمه في الشهادة وبأن التوقيع الإلكتروني قد تم إنشاؤه من قبل ذلك المشترك.

لتأكيد صحة كل من الرسالة والهوية في الشهادة تقوم جهة التصديق الإلكتروني بتوقيعها إلكترونياً. إن التوقيع الإلكتروني لجهة التصديق الإلكتروني على الشهادة يمكن التثبت من صحته باستخدام مفتاح الشفرة 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 مفتاح الشفرة العام المذكور كذلك في شهادة أخرى وهكذا.. حتى يتثبت الشخص المعتمد على التوقيع الإلكتروني من صحته. في كل حالة فإن جهة التصديق الإلكتروني المصدرة للشهادة يجب أن توقع إلكترونياً 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.

إن أي توقيع إلكتروني سواء تم إنشاؤه من قبل مشترك معين لتوثيق رسالة ما أو تم إنشاؤه من قبل جهة تصديق إلكتروني لتوثيق شهادتها (بالفعل رسالة متخصصة) يجب أن تكون مختومة زمنياً 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 للاستخدام في التثبت من الصحة، يمكن نشر شهادة في حافظة أو يتم توفيرها من خلال أي طريقة أخرى. إن الحافظات هي عبارة عن قاعدة بيانات إلكترونية من الشهادات والمعلومات الأخرى المتوفرة للاسترجاع والاستخدام في التثبت من صحة التوقيعات الإلكترونية. يمكن القيام بالاسترجاع أوتوماتيكياً من خلال أمر

برنـامج التثبـت مـن الـصحة بـأن يستفـسر مباشـرة مـن الحافظـة للحـصول علـى 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 الشفرة العام معين بهوية معينة (مثلاً اسم شخص معين، اسم المضيف في الحاسب الآلي.....إلخ)
- يمكن أن تتضمن الشهادة معلومات أخرى مثل تاريخ الإنتهاء.
- يتم توقيع الشهادة من قبل جهة التصديق الإلكتروني.

❖ **بنية المفتاح المعلن PKI Infrastructure**

إن بنية المفتاح المعلن هى كامل كرة الشمع التي تتضمن مفاتيح شفرية ونظام إدارة شهادات. إن بنية المفتاح المعلن تتيح إجراء المعاملات بطريقة آمنة بالإضافة إلى أنها تتيح تبادل المعلومات الخاصة بين الأطراف الذين يمكن أن يكونوا على معرفة ببعضهم البعض أو يمكن أن يكونوا غرباء عن بعضهم البعض. إن بنية المفتاح المعلن توفر الخصوصية واستقامة وتوثيق وعدم الرفض عند التقدم بطلب ومعاملات التجارة الإلكترونية.

تركيبات مفتاح الشفرة العام

- تعمل على توليد وتوزيع أزواج المفاتيح الخاصة / العامة
- تنشر المفاتيح العامة مع هوية المستخدم على شكل شهادة في دليل مفتوح
- توفر الثقة بأن تبقى المفاتيح الخاصة آمنة ومصانة ومأمونة
- مفاتيح عامة معينة مرتبطة فعلياً بمفاتيح خاصة معينة
- حامل زوج المفاتيح الشفرية العامة/ الخاصة هو من يدعي أن يكون.

إن تركيبة المفتاح الشفرى العام تتكون من واحد أو أكثر من الأنظمة الموثوق بها والمعروفة بـ جهات التصديق الإلكتروني وهذه السلطات منظمة في هيكل هرمي شبيه بالشجرة حيث يتم وضع مفتاح الشفرة العام والتعريف فيما يتعلق بكل عميل في شهادة رقمية وتقوم جهة التصديق الإلكتروني بالتوقيع إلكترونياً على كل شهادة وتجعل الشهادات متوفرة مجاناً وبحرية من خلال نشرها في فهارس أو دليل يمكن الوصول إليه من قبل العامة. أي عميل في بنية المفتاح المعلن يمكنه الوصول إلى مفتاح الشفرة العام لأي مستخدم آخر والتثبت من صحته باستخدام مفتاح الشفرة العام الخاص بجهة التصديق الإلكتروني للتثبت من صحة توقيع جهة التصديق الالكتروني على الشهادة. إن جهة التصديق الإلكتروني التي هي على رأس التسلسل الهرمي توقع شهادات جهات التصديق الإلكتروني التابعة لها أو التي تأتي في مرتبة أدنى منها وجهات التصديق الإلكتروني تلك توقع شهادات جهات التصديق الإلكتروني التي يكون ترتيبها أدنى منها وهكذا. هذا النظام يشكل سلسلة من الثقة في أي نظام جهة تصديق إلكتروني موزع.

❖ **كيفية الحصول على توقيعك الإلكتروني:**

يمكنك التقدم إلى إحدى الهيئات المتخصصة في إصدار هذه الشهادات ومن أشهرها **Verisifn and Digital Signature Trust** وذلك مقابل مبلغ معين من المال سنوياً وتتم مراجعة الأوراق والمستندات ومطابقة الهوية بواسطة جواز السفر أو رخص القيادة وتصعب الإجراءات أو تسهل تبعاً للغرض من استخدامها حيث يتطلب منك الحضور شخصياً في بعض الحالات وفي بعض الحالات يكفي إرسال بالفاكس أو البريد.

❖ **كيفية عمل هذه التكنولوجيا:**

أولاً: يتم التقدم إلى الهيئة المتخصصة بإصدار الشهادات.

ثانياً: يتم إصدار الشهادة ومعها المفتاح العام والخاص للمستخدم الجديد.

ثالثاً: عندما ترسل الرسالة الإلكترونية تقوم أنت بتشفير الرسالة باستخدام المفتاح العام التابع للمستقبل أو المفتاح الخاص بك في كلتا الحالتين يتم إرفاق

توقيعك الإلكتروني داخل الرسالة.

رابعاً: يقوم البرنامج الخاص بالمستقبل بإرسال نسخة من التوقيع الإلكتروني إلى الهيئة التي أصدرت الشهادة للتأكد من صحة التوقيع.

خامساً: تقوم أجهزة الكمبيوتر المتخصصة في الهيئة بمراجعة قاعدة البيانات الخاص بها ويتم التعرف على صحة التوقيع وتعاد النتيجة والمعلومات الخاصة بالشهادة إلى الأجهزة الخاصة بالهيئة مرة أخرى.

سادساً: يتم إرسال المعلومات والنتيجة إلى المستقبل مرة أخرى ليتأكد من صحة وسلامة الرسالة.

سابعاً: يقوم بقراءة الرسالة وذلك باستخدام مفتاحه الخاص إذا كان التشفير قد تم على أساس رقمه العام أو بواسطة الرقم العام للمرسل إذا تم التشفير بواسطة الرقم الخاص للمرسل، ومن ثم يجيب على المرسل باستخدام نفس الطريقة وهكذا تتكرر العملية.

❖ **حقائق عن التوقيع الإلكتروني:**

هو ليس كما يعتقد البعض بأنه ما هو إلا توقيعك باليد ولكنه مصور رقمياً ولو كان كذلك لأصبح بإمكان أي شخص أن يصور أي توقيع ويدعى بأنه صاحب التوقيع. هو شهادة رقمية تصدر عن إحدى الهيئات المستقلة تميز كل مستخدم يمكن أن يستخدمه في إرسال أي وثيقة أو عقد تجاري أو تعهد أو إقرار. وتعتبر قانونية في القانون الأمريكي الآن و قريباً في عدة دول أخرى الوثائق والعقود التجارية المذيلة بالتوقيع الإلكتروني ولا تحتاج إلى مصادقة من كاتب عدل أو أي جهة أخرى لأنها صادرة أساساً من جهة معترف بها. لا تستطيع استخدامها الآن في التوقيع على القضايا المدنية كالطلاق أو الزواج ولا يعتد بها حالياً في أوراق الاعتراف في قضايا الإجرام أو إصدار الأحكام.

❖ **تجربة مصر حول قانون تنظيم التوقيع الإلكتروني:**

وفى إطار توجه مصر نحو تنمية صناعة تكنولوجيا المعلومات والاتصالات ومبادرة مجتمع المعلومات المصري، وتحقيقاً لهذا كله كان فى أوائل عام ٢٠٠٤

صدور قانون بتنظيم التوقيع الإلكتروني بمواده التى تكفل توفير بيئة مناسبة لعمل تنظيم كامل ومحكم للتوقيع الإلكتروني ولانتشاره بين كافة قطاعات الدولة من حكومة وأفراد عاديين دون افتئات على الحقوق المشروعة للمتعاملين فى هذا المجال، وفي مظلة الأمان القانوني.

ويمكن تلخيص أهم ملامح قانون تنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات فيما يلي:

إضفاء حجية الإثبات القانونية للكتابة الإلكترونية وللتوقيع الإلكتروني فى نطاق المعاملات المدنية والتجارية والإدارية، ليكون لهما نفس الحجية القانونية فى الإثبات للكتابة العادية وللتوقيع العادي المنصوص عليها فى قانون الإثبات فى المواد المدنية والتجارية.

إنشاء ما يسمى بالمحرر الإلكتروني وتعريفه وإعطاؤه نفس مفهوم المحرر الكتابي سواء من جواز اعتباره محرراً إلكترونياً عرفياً أو محرراً إلكترونياً رسمياً وفقاً لمفهوم المحررات العربية والرسمية الموجودة في قانون الإثبات في المواد المدنية والتجارية.

اتساع نطاق تطبيق التوقيع الإلكترونيوفقاً لهذا المشروع بقانون يشمل جميع المعاملات التييجوز إتمامها إلكترونياً وهيالمعاملات المدنية والتجارية والإدارية بشرط أن تكون موقعة إلكترونياً وفقاً للشروط والضوابط التي وضعها مشروع القانون ولائحته التنفيذية.

حرص القانون على إلزام الجهات التي ستقدم خدمات التصديق الإلكتروني أو الخدمات المتعلقة بالتوقيعات الإلكترونية بالحصول على التراخيص اللازمة لهذا النشاط من جهة حكومية تابعة لوزير الاتصالات والمعلومات، وبما يضمن توافر الثقة والرقابة اللازمة لصحة وسلامة المعاملات الإلكترونية.

أنشأ القانون هيئة عامة تسمى هيئة تنمية صناعة تكنولوجيا المعلومات تكون لها شخصية اعتبارية عامة وتتبع وزير الاتصالات والمعلومات تختص أساساً بإصدار التراخيص اللازمة لمزاولة نشاط خدمات التوقيع الإلكتروني وغيرها من الأنشطة

الأخرى في مجال المعاملات الإلكترونية وتكنولوجيا المعلومات. كما أعطى القانون لهذه الهيئة الحق في إدارة وتنظيم قطاع المعاملات الإلكترونية بصفة عامة بل وفي رقابة المرخص لهم بالعمل في هذا القطاع واتخاذ الإجراءات اللازمة نحو ضمان حسن سير هذا القطاع بما يتفق مع الصالح العام وسياسة الدولة في هذا الشأن.

ركز القانون على وضع المبادئ والشروط العامة الأساسية لتنظيم التوقيع الإلكتروني وترك أمر الشروط والضوابط التفصيلية لأحكام هذا التنظيم للائحة التنفيذية للقانون، وذلك لما لهذه الشروط من أبعاد فنية وتقنية دقيقة يتعذر وضعها في متن مشروع القانون.

كما أن لوجود هذه الضوابط الفنية داخل اللائحة التنفيذية ضرورة أخرى وهي سهولة تعديلها إذا اقتضى الأمر ذلك، حيث أن تلك الضوابط تكون عرضة للتغيير نظراً للتطور التقني (التكنولوجي) السريع والمستمر في مجال تكنولوجيا المعلومات والاتصالات. وفي هذه الحالة سيتم التعديل بقرار يصدر بذلك من وزير الاتصالات والمعلومات مع مراعاة حقوق المتعاملين في هذا المجال.

تعامل القانون مع بعض الجرائم التي من الممكن أن تقع في مجال المعاملات الإلكترونية وتحديداً على التوقيع الإلكتروني والمحرر الإلكتروني وما يرتبط بهما، وذلك تحقيقاً لمبدأ الردع العام والخاص في هذا المجال، وبقصد دعم الثقة في التوقيع الإلكتروني وفي المحرر الإلكتروني وتشجيع التعامل بهما دون تخوف من أي فعل إجرامي.

إن إتاحة استخدام التوقيع الإلكتروني تدعم التحول إلى عالم لا ورقي، يأمن فيه كل متعامل على أمواله ومصالحه. كما أن التوسع في استخدام التوقيع الإلكتروني يرفع كفاءة العمل الإداري ويساعد على الارتقاء بمستوى أداء الخدمات الحكومية بما يتفق مع إيقاع العصر، ومن شأنه أن يضيف إلى المزايا التنافسية التي تتمتع بها مصر في ظل النظام التجاري العالمي الجديد والذي أصبحت المعاملات الإلكترونية سمة من سماته وعلامة دالة عليه.

بقي أن نعلم أن أهم مجالات تطبيقات التوقيع الإلكتروني هي الحكومة الإلكترونية: حيث تشمل المعاملات الإدارية الحكومية وخدمات المواطنين بشكل عام ومنها التصاريح المختلفة والخدمات التي تقدمها الجمارك والضرائب ومصلحة الأحوال المدنية، وكذلك ما يقدم إلى الجهات الحكومية من طلبات والتي من الممكن ووفقا لهذا المشروع أن تتم عن طريق المحررات الإلكترونية التي تصدرها الجهات المشار إليها ويتم توقيعها من قبل الموظفين العموميين في هذه الجهات مما يضفي على تلك المحررات الإلكترونية الحكومية صفة المحررات الرسمية بسبب قيام الموظف العام للتوقيع عليها إلكترونياً. ويستهدف هذا كله رفع كفاءة العمل الإداري، والارتقاء بمستوى أداء الخدمات الحكومية بما يتفق مع إيقاع العصر.