1.3 مقدمة:

المصادقة هامة لتوفير اتصال آمن . يجب أن يمكن المستخدمون من إثبات هويتهم لمن يتصلون بهم ويجب أن يتمكنوا من التحقق من هوية الآخرين. تعتبر مصادقة هوية على شبكة اتصال عملية معقدة لأن الجهات المتصلة لا تتطابق فعلياً عند الاتصال. يمكن أن يسمح هذا لشخص غير أخلاقي بأن يحتجز الرسائل أو ينتحل صفة شخص أو كيان آخر.

الشهادة الرقمية ورقة اعتماد توفر وسيلة للتحقق من الهوية. تستخدم الشهادات تقنيات التشفير من أجل حل مشكلة افتقاد الاتصال الفعلي بين المتصلين. يحد استخدام هذه التقنيات من احتمال احتجاز الرسائل، أو تغييرها، أو تزييفها من قبل شخص غير أخلاقي. تؤدي تقنيات التشفير هذه إلى جعل الشهادات صعبة التعديل. وهكذا، سيكون من الصعب على أي شخص انتحال صفة شخص آخر.

تتضمن البيانات الموجودة في الشهادة مفتاح التشفير العمومي من زوج المفاتيح الخاص والعمومي لصاحب الشهادة. يمكن التحقق من أن الرسالة الموقعة باستخدام المفتاح الخاص للمرسل مصدقة وذلك من قبل مستلم الرسالة وباستخدام المفتاح العمومي للمرسل. يمكن العثور على هذا المفتاح على نسخة من شهادة المرسل. إن التحقق من التوقيع باستخدام المفتاح العمومي من شهادة يثبت أنه قد تم إنشاء هذا التوقيع باستخدام المفتاح الخاص لصاحب الشهادة. إذا كان المرسل حذراً وأبقى المفتاح الخاص سرياً، يمكن أن يثق المتلقي بهوية مرسل الرسالة.

طورت شركة (Net Scape) بروتوكول الطبقات الأمنية لتأمين نقل آمن للمعلومات بين خادم الويب ومستعرضات الويب. ويعتمد هذا البروتوكول على خوارزمية المفتاح العام (Public key) والمفتاح الخاص (Private key) ، إذ يزود الخادم المستفيد بالمفاتيح العامة، وتستخدم هذه المفاتيح العامة في تشفير الرسائل المتَّجِهة إلى الخادم، ولا يمكن استخدم المفتاح العام لفك شفرة الرسالة التي شَفَّرها، إذ يتفرد المفتاح الخاص (لدى الخادم) بالقدرة على فك شفرة الرسالة التي شفَّرَها المفتاح العام.

ويستطيع المستفيد (Client) بالطريقة ذاتها إنشاء زوج من المفاتيح العامة /الخاصة لإرسال المعلومات إلى الخادم. وتمنع هذه الطريقة من ظهور مشاكل الاتصال مثل التجسس أو التنصت (eavesdropping) عند كشف المعلومات الحساسة (مثل : البيانات الشخصية، وأرقام بطاقات الإئتمان (Credit card)) ضمن أحد مواقع الويب.

ويساعد بروتوكول الطبقات الأمنية (SSL) في التحقق من المفتاح العام الذي أصدره الخادم، ويأكد من عدم تغيُّر المعلومات أثناء النقل، وذلك باستخدام الشهادات الرقمية (digital certificates) التي سنتحدث عنها ضمن هذا البحث.

2.3 الشهادات الرقمية (Digital Certificates) :

الشهادات الرقمية عبارة عن وثيقة إلكترونية تربط بكل موثوق مفتاح عام (Public key) بكيان معين (مستخدم (user)، حاسب (computer)، ...). بالتالي يمكن اعتبار الشهادات الرقمية (Digital Certificates) عباره عن حامل للمفتاح العام بالإضافة إلى بعض المعلومات المتعلقة بذلك الكيان والجهة الصادرة لتلك الشهادة الرقمية والتي تُدعى بهيئة أو سلطة الشهادات (Certificate Authority (CA)). [5]

1.2.3 مكونات الشهادات الرقمية (The contents of Digital Certificate):

إن قطاع التوحيد القياسي لإتحاد الإتصالات العالمي (The Telecommunication Standardization Sector of the International Telecommunication Union)

(ITU-T) قام بتعريف ونشر معيار يدعى بـ X.509 والذي يُعَرّف مكونات الشهادة الرقمية والمستخدم بواسطة البنى التحتية للمفتاح العام (PKIs) [14]. وهي كالتالي:

- المفتاح العام المتعلق بكيان معين (Public key for a particular entity) :

يعتبر أهم المكونات الأساسية للشهادة الرقمية.والذي يحسب طوله بالبت (bit) على سبيل المثال 512bit، 1024bit، 2048bit والذي يكون بنفس طول المفتاح الخاص (Private key) .

كلما كان الطول أكبر كلما كان يتمتع بأمان أعلى ولكن يلزمه معالجة أكبر أثناء التشفير وفك التشفير.

- إسم الجهة الصادرة (The issuer name (CA)) :

الذي يعتبر هاماً من أجل معرفة هوية الجهة الصادرة لتلك الشهادة أثناء التعامل مع تلك الشهادة.

- المدة المسموحة (فترة سريان مفعولها) (Validity period) :

حيث يمكن أن تنتهي تلك الشهادة بعد زمن معين .

- توقيع الجهة الصادرة (The signature of the issuer(CA)) :

الذي يعتبر هاماً وذلك لكي نضمن أن الشهادة قد أتت من الجهة التي نريدها نحن وليس من مكان آخر.

- رقم تسلسلي (Serial number) :

والذي تم تخصيصه من قبل الجهة الصادرة حيث يُعرّف الشهادة بشكل فريد.

- الإصدار (Version) :

والذي يعرف اصدار معيار الـX.509 حيث يوجد ثلاثة إصدارات هي:

- الإصدار الأول X.509v1
- الإصدار الثانيX.509v2
- الإصدار الثالث X.509v3 وهو المستخدم في النظام المقترح.

- خوارزمية التوقيع الرقمي (Signature algorithm):

وهي الخوارزمية التي استخدمتها الـ(CA) في حساب الـ(hash) عندما وقعت رقمياً الشهادة الرقمية، لأنه كما ذكر أعلاه تقوم الـ (CA) بالتوقيع رقمياً على كل شهادة أصدرتها [5].

2.2.3 أنواع الشهادات الرقمية:

يوجد عدد من أنواع الشهادات الرقمية منها:

1. شهادة بروتوكول طبقة المقابس الآمنة SSL :

بروتوكول SSL : يستخدم هذا البروتوكول بشكل واسع في الانترنت بالتحديد في الاتصالات التي يتم فيها تبادل المعلومات الحساسة. وهو عبارة عن مجموعة من القواعد التي تحكم عمليات تأكيد الخادم والعميل والاتصالات المشفرة بينهما.

يتطلب بروتوكول SSL شهادتين وهما:

- شهادة SSL للعملاء:

تأكيد العملاء وتستخدم لتعريف العميل من قبل الخادم بواسطة بروتوكول SSL . مثلا يقوم بنك بمنح عميل شهادة SSL للعميل وبذلك يتم التعرف على العميل من قبل خادمات البنك فيسمح له بالدخول إلى حسابه.

- شهادة SSL للخادمات:

تأكيد الخادمات وتستخدم لتعريف الخادمات من قبل العملاء باستخدام BG بروتوكول SSL .مثلا تدعم مواقع التجارة الإلكترونية تأكيد الخادم باستخدام العميل بحيث يقوم بتأسيس اتصال SSL مشفر والتأكد من أن العميل يقوم بالتعامل مع موقع ويب معرف، و أيضاً يضمن عدم كشف البيانات المرسلة عبر الشبكة.

2. شهادة بروتوكول الامتدادات الآمنة لبريد الانترنت متعددة الأغراض S/MIME:

هناك الكثير من برامج البريد الإلكتروني تدعم تشفير وتوقيع الرسائل باستخدام بروتوكول S/MIME . S/MIMEفعند الرغبة في استخدام هذا البروتوكول يجب أن يملك المرسل شهادة S/MIME .

بروتوكول S/MIME يقوم بتشفير الرسالة ولكن يجب استخدامه بحذر لأن المستقبل لو فقد مفتاحه الخاص ولم يقم بعمل نسخة احتياطية منه فإن الرسالة المستقبلة لن يفك تشفيرها أبداً [5].

2.2.4 استخدام نظام ال P12 :

عند تحميل وتنصيب الشهادة الرقمية ضمن مستعرض الإنترنت، يجب على المستخدم القيام بعملية تصدير (export) للشهادة وحفظها على قرص أو (Token) كما هو مستخدم في البحث على نحوٍ آمن، وذلك لاستخدامها في تنفيذ مهام عبر الحوسبة الشبكية. تكون الشهادة الرقمية المرسلة عادة بإحدى صيغتي- PEM (extension .pem) أو (extension .p12 or .pfx) PKCS12، [6].

3.3 حالات الشهادة الرقمية:

- شهادة سارية المفعول (صالحة) : هذا يعني أن الشهادة سارية المفعول وتستخدم فعلياً من أجل التحقق من التوقيع.
- شهادة منتهية الصلاحية : وهي شهادة قد إنتهت فترة صلاحيتها.
- شهادة مرفوضة : وتعني أن هذه الشهادة مدرجة في قائمة الشهادات المرفوضة.
- شهادة مؤرشفة : وتعني أن الشهادة قد أُصدرت مسبقاً من هيئة التوثيق ولم تعد تستخدم حالياً ضمن الخدمات المتقدمة من الجهة المصدرة للشهادة ولكنها موجودة ضمن قائمة الشهادات التي أصدرت من قبل هيئة التوثيق.
- الشهادة المُتوقفة : أي أن الشهادة مرفوضة لمدة محدودة حسب قائمة الشهادات المرفوضة.
- الشهادة المعدلة : أي أنه تم التعديل على بيانات مالك الشهادة مثل الإسم والعنوان وغيره ؛ من ثم أُصدرت شهادة أخرى لنفس الشخص بالمعلومات الجديدة المعدلة، أي أنه تم عمل تجديد للشهادة بالبيانات الجديدة [7].

4.3 سياسة الشهادات الرقمية:

هي مجموعة من المهام والمراحل والسياسات والقواعد التي تطبق في دورة حياة الشهادة منذ إصدارها وحتى إنتهاء فترة صلاحيتها أو إلغاءها، ومنها :

1.4.3 الإصدار :

وهي أول مرحلة وتشمل التأكد من بيانات الشخص أو المؤسسة وذلك قبل إصدار الشهادة، وتعتمد عملية التأكد على حسب نوع الشهادة المراد إصدارها، ففي الشهادات التي تصدر خصيصاً للمعاملات المالية يلزم التأكد من عدد من البيانات، وبعد التأكد من صِحة الهوية والبيانات يتم إرسال تلك البيانات إلى هيئة التوثيق والتي بدورها تقوم بعمل الشهادة.

الشكل (1.3) : إرسال طلب شهادة والرد عليه

2.4.3 الإلغاء :

تستطيع الجهة أو الشخص الذي يملك الشهادة أن يلغيها قبل تاريخ إنتهاءها إذا فقد المفتاح الخاص مثلاً أو لأي سبب آخر، ويتم إضافة الشهادة إلى قائمة الشهادات الملغاة.

3.4.3 الإنتهاء :

لكل شهادة تاريخ إنتهاء يكون مدرج ضمن بيانات الشهادة ولكن بموجب هذا التاريخ تصبح الشهادة غير صالحة للإستخدام ولابد من إصدار شهادة جديدة ويمكن أن تكون لها نفس بيانات الشهادة المنتهية.

4.4.3 التعطيل المؤقت :

يمكن لمالك الشهادة أن يعطل شهادته لفترة مؤقتة لا يحتاج في هذه الفترة لإستخدام الشهادة حتى لا تستغل من قبل أطراف أُخرى [7] .

5.3 متطلبات الشهادات الرقمية (digital certificate Requirements):

تبدأ عملية تصميم الـ (CA) بتعريف المتطلبات اللازمة من استخدام الشهادات الرقمية (digital certificates). بمعنى هل هناك ضرورة من أجل استخدام الشهادات الرقمية . سنذكر هنا بعض الحالات التي يلزمها شهادات رقمية:

- استخدام الشهادات الرقمية لعملية تصديق الحاسب (Computer Authentication) عند التعامل ببروتوكول الـ (IP) الآمن (IPSec). وذلك لأن هذا البروتوكول (IP Security) يؤمن الإتصال الآمن بين جهازين متصلين عبر الشبكة حيث يبدأ عملية تأسيس الإتصال بالتفاوض بين الجهازين فإذا كان شرط التفاوض هو تصديق كلا الحاسبين قبل الإتصال ، هذا يستوجب استخدام الشهادات الرقمية (Digital Certificates).
- استخدام الشهادات الرقمية لعملية تصديق المستخدم (User Authentication)عند استخدام البطاقات الذكية (Smart Cards) في عملية الولوج (Login) للحاسب. أحياناً أسم المستخدم وكلمة المرور(User name and password) تكون غير كافية من أجل ضمان عدم اختراق حاسب لأنه يمكن أن يتم سرقة الأسم وكلمة المرور بأي طريقة. البطاقات الذكية (smart card) تُجبر المستخدم والذي بالغالب يكون مدير (Administrator) بالأتصال الفيزيائي بذلك الحاسب وذلك من خلال تزويده بالبطاقة الذكية (smart card) أثناء عملية الولوج (Login) للحاسب. هذا يستلزم وجود كاتب بطاقات (card writer) عند الـ(CA) وذلك لكتابة معلومات الشخص في البطاقة الذكية وأيضاً قارئ بطاقات (Card Reader) على جهاز الحاسب الذي سيقرأ البطاقة الذكية عند عملية الولوج (Login) للحاسب.
- استخدام الشهادات الرقمية لتزويد السرية (confidentiality) من أجل المعطيات المخزنة في ملفات الحاسب عند استخدام نظام تشفير الملفات (Encrypting File System EFS). وذلك حتى لا يفك تشفير

المعطيات إلا الشخص الذي قام بتشفير المعطيات. مع العلم أنه هناك أمكانية لإعطاء شهادة لشخص معين والذي يسمى بوكيل إسترجاع المعطيات (Data Recovery Agent) يمكنه من خلالها فك تشفير أي معطيات مشفرة بواسطة أي شخص في شبكة ما والتي تعتمد في عملها على الشبكة من نوع نطاق (domain).

- استخدام الشهادات الرقمية لتجنب عدم اظهار هوية (No repudiation) الطرف الذي نتعامل معه وذلك باستخدام التوقيع الرقمي(Digital Signature). أحياناً بعض الأطراف التي يتم التعامل معها لا تظهر هويتها أو تخفيها . فإذا أردنا إجبار الطرف الذي نتعامل معه على إثبات هويته يجب أن يمتلك شهادة رقمية.
- استخدام الشهادات الرقمية لعملية سلامة المعطيات عند ارسالها (Data Integrity). تعتبر سلامة المعطيات أثناء عبورها عبر الشبكة إما شبكة داخلية أو عامة كالإنترنت أمر هام. باستخدام الشهادات الرقمية نستطيع تحقيق هذا الهدف.
- استخدام الشهادات الرقمية لعملية حماية الرسائل الإلكترونية (Secure Email) عند إرسالها . وذلك إن بروتوكولات البريد الإلكتروني (Internet e-mail protocols) تنقل الرسائل الإلكترونية بشكل واضح ((غير مشفر) Plain text) مما تجعلها سهلة للقراءة فيما إذا تم اعتراضها بأي طريقة أثناء انتقالها. باستخدام الشهادات الرقمية يمكننا أولاً تشفير نص الرسالة الإلكترونية بواسطة المفتاح العام (Public key) الخاص بالمستقبل ومن ثم توقيع الرسالة الإلكترونية رقمياً بواسطة المفتاح الخاص (Private key) الخاص بالمرسل .
- استخدام الشهادات الرقمية لعملية التصديق في الإنترنت (Internet Authentication) إما من أجل الزبائن (clients) أو من أجل مخدمات الويب (Web Servers) وذلك حتى يتمكن مخدم الويب (Web Servers) من معرفة هوية الزبائن المتصلة به. أيضاً حتي يتمكن الزبائن من التأكد من أنهم متصلين بالمخدم الصحيح وهذا ما يطلق عليه بمخدم الويب الآمن (Secure Web Server).
- استخدام الشهادات الرقمية لعملية التصديق في الشبكة اللاسلكية (Wireless Network Authentication)عند استخدامنا بروتوكول (802.1x) و ذلك لمعرفة هوية الشخص أو الكمبيوتر قبل اتصاله بالشبكة اللاسلكية.
- استخدم الشهادات الرقمية في حال أردت أمانٍ عالٍ (High Security)عند استخدامك الشبكات الإفتراضية الخاصة (Virtual Private Network (VPN)) وذلك من أجل عملية مصادقة مخدمات الـ (VPN Servers Authentication). [8]

6.3 التوقيع الإلكتروني:

هو عملية توقيع المستند الإلكتروني باستخدام الشهادة الرقمية، ويتم ذلك من خلال تشفير المختصر الحسابي الناتج من عملية دالة الاختزال (Hash Function) للمستند الإلكتروني باستخدام المفتاح الخاص. وتكمن 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.

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 [9].

1.6.3 خواص التوقيع الإلكتروني:

1. حماية المعلومات الحساسة بالتكامل مع البريد الإلكتروني.
2. التحقق من هوية المرسل ومصداقية الرسالة.
3. إسناد الصلاحية المناسبة لمستقبل الرسالة من: طباعة أو تعديل أو إعادة توجيه أو رد وغيرها.
4. تشفير الرسائل وعدم تمكين عرض الرسائل إلا من الأشخاص المرخص لهم ذلك [9].

2.6.3 مزايا استخدام التوقيع الإلكتروني:

1. إمكانية استخدامه كبديل للتوقيع التقليدى بالإضافة الى مسايرته لنظم المعلومات الحديثة.
2. يؤدى التوقيع الإلكتروني إلى رفع مستوى الأمن والخصوصية بالنسبة للمتعاملين على شبكة الإنترنت خاصة فى مجال التجارة الإلكترونية.
3. إمكانية تحديد هوية المرسل والمستقبل إلكترونياً والتأكد من مصداقية الأشخاص والمعلومات.
4. يساعد التوقيع الإلكتروني كل المؤسسات على حماية نفسها من عمليات التزييف وتزوير التوقيعات .

5. يسمح التوقيع الإلكتروني بعقد الصفقات عن بعد ودون حضور المتعاقدين وهو بذلك يساعد فى تنمية وضمان التجارة الإلكترونية [9].

3.6.3 فوائد التوقيع الإلكتروني:

1.3.6.3 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"

2.3.6.3 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.

3.3.6.3 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 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 [9].

4.6.3 متطلبات التوقيع الإلكتروني:

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.

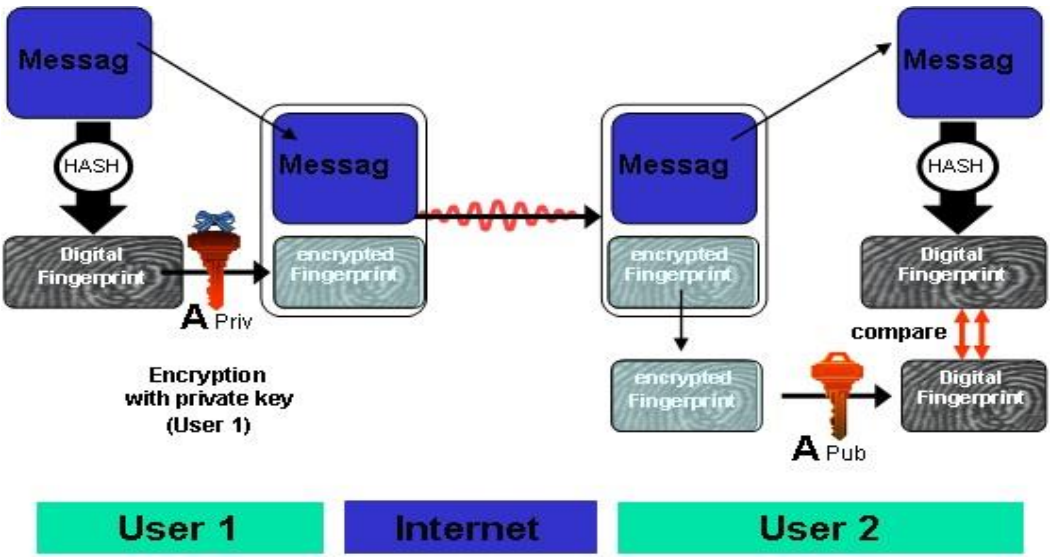
3. المفتاح الخاص يجب أن يبقى سري وبالتالي فإنه إذا عرضه أحد الفرق فإن هذا الفريق يستطيع أن يصدر ويقلد أي توقيع.
4. إن على المستخدمين وعلى برامجهم أن تكون متبعة للبروتوكول بحرفيته .بهذه الأحوال يمكن من خلاله إثبات من أرسل الرسالة والتأكد من صحة مضمونها [9].

5.6.3 كيفية عمل تقنية التوقيع الإلكتروني:

إن التوقيع الإلكتروني يحقق الموثوقية للمستند المرسل (Authenticity of Massage) ويقوم كذلك بالتحقق من هوية الشخص المرسل وحماية هوية المرسل من السرقة .

فعند إرسال مستند موقعاً بالتوقيع الإلكتروني بإستخدام برمجيات خاصة بذلك ، فإن محتوى المستند (البيانات) تتحول إلى شكل أرقام (Unique digital representation) وذلك هو ناتج دالة تسمى بالـ (Hash) وهي دالة رياضيهة بحته . وهذه هي المرحلة الأولى.

أما في المرحلة لثانية فيمر المستند من خلال دالة التوقيع (Signing Function) ويتم ذلك بواسطة المفتاح الخاص (Private Key) الذي يكون بحوزة المرسل فقط (مرسل الرسالة) أي صاحب التوقيع الإلكتروني الذي يستخدمه من خلال كلمة مرور أو رقم خاص بالمرسل وهنا يقوم المفتاح الخاص بتشفير نتائج دالة الـ (hash) ويقوم المفتاح العام (Public Key) بفك تشفيرها وهذه العملية تسمى بصمة التوقيع الإلكتروني (Digital (fingerprint) .



الشكل (2.3) : تقنية التوقيع الإلكتروني

مما سبق يتضح أن الرسالة النهائية تكون جاهزة للإرسال تتكون من :

- المستند .
- نتائج دالة الـ hash.
- دالة التوقيع بواسطة المفتاح الخاص .

هذه المكونات جميعها تنشئ التوقيع الإلكتروني؛ مع العلم أن التوقيع الإلكتروني لا يقوم بتشفير الرسالة ولكن يمكن استخدام نفس تقنية التشفير المستخدمة في التوقيع الإلكتروني في تشفير الرسالة نفسها .

يقوم مستلم الرسالة بإستخدام المفتاح العام الذي بحوزته ويكون معروفاً للجميع والذي يكون الخوارزمية الخاصة به في التوقيع الإلكتروني وفي نتائج دالة الـ (hash)، حيث أن برمجية التوقيع الإلكتروني تختبر فيما إذا كان التوقيع الإلكتروني قد تم إنشاؤه بإستخدام المفتاح الخاص الذي يقابله المفتاح العام الذي بحوزة مستقبل الرسالة الذي يعمل على التحقق من هوية المرسل ومن أن الرسالة مرسله فعلاً من الشخص المقصود [7].

7.3 التحقق من صحة التوقيع الرقمي بإستخدام خوارزمية البعثرة (Hash Function):

التحقق من صحة التوقيع الرقمي هو عملية تدقيق للتوقيع الرقمي بالرجوع إلى الرسالة الأصلية وإلى مفتاح عمومي معين، من أجل البتّ فيما إذا كان ذلك التوقيع الرقمي قد أنشئ لتلك الرسالة ذاتها باستخدام المفتاح الخصوصي المناظر للمفتاح العمومي المذكور في المرجع. ويتم التحقق من صحة التوقيع الرقمي بحوسبة نتيجة بعثرة جديدة للرسالة الأصلية بواسطة دالة البعثرة نفسها التي استُخدمت لإنشاء التوقيع الرقمي. ثم يدقق الشخص المتحقق، باستخدام المفتاح العمومي ونتيجة البعثرة الجديدة، فيما إذا كان التوقيع الرقمي قد أنشئ باستخدام المفتاح الخصوصي المناظر، وفيما إذا كانت نتيجة البعثرة المحوسبة مجددا تطابق نتيجة البعثرة الأصلية التي حُولت إلى التوقيع الرقمي أثناء عملية التوقيع.

إلى جانب عملية إنتاج أزواج المفاتيح توجد عملية أساسية أخرى يشار إليها عموما بعبارة "دالة البعثرة" (hash function) وتستخدم في إنشاء التوقيعات الرقمية وفي التحقق من صحتها. ودالة البعثرة عملية رياضية مبنية على خوارزمية تنشئ تمثيلا رقميا للرسالة أو شكلا مضغوطا من الرسالة، (كثيرا ما يشار إليهما بعبارة "خلاصة الرسالة" (message digest) أو "بصمة" الرسالة (message fingerprint)) تتخذ شكل "قيمة بعثرة" (hash value) أو "نتيجة بعثرة" (hash result) ذات طول موحد قياسيا يكون عادة أصغر كثيرا من الرسالة ولكن تنفرد به الرسالة جوهرياً. وأي تغيير يطرأ على الرسالة تترتب عليه دائما نتيجة بعثرة مختلفة عندما تستخدم دالة البعثرة نفسها. وفي حالة دالة بعثرة مأمونة، تعرف أحيانا باسم "دالة بعثرة ذات اتجاه واحد"، يستحيل عمليا اشتقاق الرسالة الأصلية عند معرفة قيمة البعثرة الخاصة بها. ومن المزايا الأساسية الأخرى لدالة البعثرة أنه يستحيل عمليا أيضا إيجاد شيء رقمي ثنائي (مختلف عن الشيء الذي اشتُقت منه الخلاصة أصلا) ينتج الخلاصة نفسها. ومن ثم، فإن دوالّ البعثرة تمكّن من تشغيل البرنامج الحاسوبي المعد لإنشاء التوقيعات الرقمية بمقادير من البيانات أصغر ويمكن التنبؤ بها بسهولة أكبر، كما تمكّن في الوقت نفسه من تحقيق ارتباط إثباتي قوي بمحتوى الرسالة الأصلية، والتوصل بذلك بفعالية إلى توفير ضمان على أن الرسالة لم يطرأ عليها أي تعديل منذ أن وُقّع عليها رقمياً.

قبل التوقيع على مستند أو على أي معلومات أخرى، يتعين على الموقّع أن يبين بدقة حدود ما يريد التوقيع عليه. ثم تحوسِب دالةُ بعثرة في البرنامج الحاسوبي لدى الموقّع نتيجةَ بعثرة تنفرد بها (بخصوص كل الأغراض العملية المقصودة) المعلوماتُ التي يراد التوقيع عليها. وعندئذ يحوّل البرنامجُ الحاسوبي لدى الموقّع نتيجةَ البعثرة إلى توقيع رقمي باستخدام المفتاح الخصوصي للموقّع. وبذلك يكون التوقيع الرقمي الناتج توقيعاً فريداً خاصاً بالمعلومات التي يجري التوقيع عليها وبالمفتاح الخصوصي المستخدم في إنشاء التوقيع الرقمي معاً. وفي العادة، يُلحق التوقيع الرقمي (أي ترميز نتيجة البعثرة المستخلصة من الرسالة بواسطة المفتاح الخصوصي لدى الموقّع) بالرسالة، ويُخزن أو يُنقل مع تلك الرسالة. غير أن من الممكن أيضا إرساله أو خزنه على أنه عنصر

بيانات منفصل، ما دام مرتبطاً بالرسالة المناظرة ارتباطاً يمكن التعويل عليه. ولأن التوقيع الرقمي هو توقيع فريد يخص رسالته دون سواها، فإنه غير قابل للعمل به إذا كان مفصولاً دوما عن الرسالة.

تختص برامجية التحقق بالتأكد من أن التوقيع الرقمي قد تم "التحقق" من صحته فيما يخص الترميز (أ) إذا كان المفتاح الخصوصي للموقّع قد استخدم للتوقيع على الرسالة رقمياً، ومعروف أن ذلك هو الذي يحدث إذا استُخدم المفتاح العمومي للموقّع في التحقق من صحة التوقيع لأن المفتاح العمومي للموقّع يقتصر على التحقق من صحة توقيع رقمي منشأ بواسطة المفتاح الخصوصي للموقّع؛ و(ب) إذا كانت الرسالة لم يطرأ عليها أي تحوير، ومعروف أن ذلك هو الذي يحدث إذا كانت نتيجة البعثرة التي حسبها المتحقق مطابقة لنتيجة البعثرة المستخرجة من التوقيع الرقمي أثناء عملية التحقق من صحته [7] .

9.3 الفرق بين الشهادة الرقمية والتوقيع الرقمي :

في التوقيع الرقمي لا يوجد به ضمان أن المفتاح العام يتبع لهذه المؤسسة بالفعل، فمثلاً تقوم جهة معينة بنشر مفتاح عام على أنها جهة أخرى فتستطيع هذه الجهة الحصول على كل الرسائل التي تُرسل لمالك المفتاح ويكون بذلك إنتحال شخصية، أي أن في التوقيع لا يوجد ربط بين الجهة المعينة والمفتاح العام لذلك ظهرت الشهادة الرقمية التي تربط بين الشخص أو الجهة المعينة ومفتاحه العام حيث تحتوي الشهادة على اسم صاحب الشهادة ومفتاحه العام موقعة من طرف آخر موثوق به يستطيع إثبات المفتاح العام لصاحبه [7].