د. فهد بن عبد الله الحويماني

البنية التحتية للمفاتح العامة (*)

تقوم مدينة الملك عبدالعزيز للعلوم والتقنية حالياً بإنشاء ما يعرف بالبنية التحتية للمفاتح العامة (Public-Key Infrastructure - PKI) ، لما لها من أهمية بالغة في دعم نشاطات القطاعين العام والخاص في المملكة، حيث أنها تعد القاعدة التي تنطلق منها التجارة الإلكترونية، وتقوم عليها الحكومة الإلكترونية، وهي البنية التي تمكّن المتعاملين عن طريق شبكة الإنترنت بمختلف فئاتهم بإجراء مختلف العمليات الإلكترونية بموثوقية وسلامة تامة.

أدى الإنتشار السريع للإنترنت والتوسع في استخدامها في شتى المجالات، إلى ضرورة التعامل الآمن معها لإيجاد قدر كبير من السرية والموثوقية . وهناك ما يعرف بالشبكات الإفتراضية الخاصة (Virtual Private Networks) ، والتي تستفيد من انتشار شبكة الإنترنت وانخفاض تكلفة الارتباط عن طريقها لتمنح المنشأة إمكانية إنشاء شبكتها الخاصة بإستخدام خطوط الإنترنت ذات التكلفة المتدنية. إلا أن من يستخدم هذه الشبكات الإفتراضية بحاجة إلى طريقة تضمن سرية وموثوقية البيانات المتبادلة بواسطتها.

ويمكن معرفة مفهوم البنية التحتية للمفاتح العامة من خلال الإجابة على بعض الأسئلة، منها ما يلي:

١ـ كيف يمكن لشخصين التراسل فيما بينهما بعيداً عن أعين المتطفلين والعابثين؟

٢ـ كيف يستطيع من يستقبل رسالة إلكترونية التأكد من أن المرسل هو الشخص المتوقع وليس بشخص آخر قد إنتحل شخصيته؟

٣ـ كيف يستطيع المصرف التأكد من أن الشخص الذي يود الدخول إلى حسابه الشخصي هو في الواقع الشخص نفسه صاحب الحساب؟ أو كيف لإدارة المرور التأكد من أن من يطلب تجديد رخصة القيادة هو بالفعل صاحب الرخصة؟ أو كيف لمدرسة أو جامعة التأكد من أن الشخص الذي يود الدخول إلى سجلاته الدراسية هو الطالب المعني وليس شخص آخر غيره؟

٤ـ كيف يستطيع من يود الدخول إلى موقع على الإنترنت (كالموقع الخاص بالمصرف أو بإدارة المرور أو بالجامعة) التأكد من أن الموقع الذي لديه هو الموقع المعني وليس بموقع تم إنشاؤه للاحتيال على المستخدمين؟

٥ـ كيف يستطيع وسيط الأسهم منع زبون من إنكار قيامه بإدخال طلب الشراء لعدد من الأسهم، عندما يكون الزبون بالفعل قد أدخل الأمر لشراء الأسهم؟

٦ـ ماذا لو أن الزبون (بعد سقوط سعر السهم الذي إشتراه) أنكر إدخال أمر الشراء لعدد ١٠٠ ألف سهم، وإدعى أن الأمر كان لشراء ١٠٠ سهم فقط، هل يستطيع الوسيط إثبات عكس ذلك؟

٧ـ كيف يمكن لطرفين التوقيع على عقد تجاري فيما بينهما عن طريق الإنترنت، بدون الحاجة لوجودهما معاً في نفس المكان؟

٨ـ كيف يمكن للمرسل التأكد من إستلام المرسل إليه للرسالة؟ وكيف يلزمه قانونياً بذلك؟ وكيف للمرسَل إليه إثبات قيام المرسل بإرسال الرسالة؟

وظائف البنية التحتية للمفاتح

تنحصر وظائف البنية التحتية للمفاتح العامة فيما يلي:

* **سرية المعلومات:** وتكمن في تمكين المتعاملين من تبادل المعلومات فيما بينهم، بحيث لا يمكن للآخرين معرفة طبيعة تلك المعلومات.
* **التثبت من هوية المتعاملين:** وذلك بمعرفة كل من المرسل والمستقبل لهوية الآخر بشكل قاطع.
* **سلامة المعلومة:** وذلك لإكتشاف أية محاولة لتغيير محتوى المعلومة، أو حذف جزء منها أو الاضافة إليها أو تعديلها بعد إرسالها من قبل المرسل.
* **التوقيع الإلكتروني :** وتعني موافقة الشخص على وثيقة ما، وذلك بالتوقيع عليها، ومقدرة المستلم من التحقق من صحة التوقيع.

(*) مفاتيح هي خطأ شائع لكلمة مفاتح التي وردت هكذا في القرآن الكريم ﴿وَعِندَهُ مَفَاتِحُ الْغَيْبِ..﴾ [الأنعام: ٥٩]

*منح الصلاحية : وذلك لتحديد نطاق الصلاحية الممنوحة للشخص المفوض بعمل ما، بحيث تختلف هذه الصلاحية حسب هوية الشخص.

التشفير والمفاتح العامة

التشفير هو طريقة لنقل أو تخزين البيانات الإلكترونية بحيث لا يمكن لغير الشخص المعني قراءتها أو الاستفادة منها. ومن أبسط الأمثلة على التشفير هو قيام المرسل بتغيير ترتيب أحرف الرسالة بحيث يستبدل حرف (A) بحرف (B) وحرف (B) بحرف (C) وهكذا، بينما يقوم مستقبل الرسالة بإعادة الرسالة لصورتها الأصلية بإستبدال حرف (B) بحرف (A) وحرف (C) بحرف (B) إلخ. وفي هذه الحالة يمكننا القول بأن المفتاح (key) المستخدم للتشفير هو استبدال الأحرف بالطريقة التي قام بها المرسل أعلاه، وأن المفتاح المستخدم لفك التشفير هو عكس هذه الطريقة. وقد تطور علم التشفير إلى أن وصل إلى درجة متقدمة، بحيث أصبح من شبه المستحيل إكتشاف المفتاح المستخدم في التشفير حتى لو أن شخصاً أمضى آلاف السنين محاولاً القيام بذلك ومستخدماً أسرع وأحدث الحاسبات الآلية.

تم إكتشاف طريقة التشفير بواسطة المفتاح العام قبل حوالي ٢٥ عاماً، وهي تعد ثورة عظيمة في علم التشفير حيث تعتمد على مفتاحين مختلفين تجمعهما علاقة رياضية معينة، بحيث لا يمكن فتح ما يتم تشفيره بأحد هذه المفاتح إلا بواسطة المفتاح الآخر. ويحتفظ الشخص المتعامل بطريقة المفاتح العامة بالمفتاح الخاص (private key) في مكان آمن لا يطلّع عليه أي شخص آخر ولكن يقوم بنشر المفتاح الآخر، المعروف بالمفتاح العام(public key) على الملأ، أو على الأقل لمن يريد التعامل معه. ويمكن للشخص إيصال مفتاحه العام للآخرين بأي طريقة يشاء سواءً عن طريق البريد الإلكتروني، أو بعرضه في أحد أدلة المفاتح العامة. ولا يتطلب ذلك أي طريقة سرية، حيث إن الهدف من المفتاح العام هو للاستخدام العلني من قبل الآخرين. فعند حصول شخص ما على المفتاح العام لشخص آخر، فإن بإمكانه إرسال رسالة مشفرة لذلك الشخص، الذي يقوم بفك التشفير عن الرسالة بإستخدام مفتاحه الخاص. ولكي يقوم الشخصان بالتشفير فيما بينهما فعلى كل واحد منهما الحصول على المفتاح العام للشخص الآخر، بالإضافة إلى إحتفاظ كل واحد منهما بمفتاحه الخاص، شكل (١).

● مثال تشبيهي

كما هو معلوم فإن البيانات الإلكترونية بجميع أشكالها ـ من كتابات نصية وصور ثابتة ومتحركة وتسجيلات صوتية وغيرها ـ تتحول في نهاية الأمر إلى سلسلة من الشحنات الكهربائية التي يعبّر عنها بالأرقام صفر و واحد. فعلى سبيل المثال: تتحول كلمة علي (ALI) عند تخزينها في الحاسب أو نقلها عبر شبكة الحاسب، كما هو متبع في نظام (ASCII)، إلى الأرقام التالية:

حرف (A) يتحول إلى: 01000001 ويساوي الرقم ٦٥

حرف (L) يتحول إلى: 0100 1100 ويساوي الرقم ٧٦

حرف (I) يتحول إلى: 0100 1001 ويساوي الرقم ٧٣

فتظهر كلمة (ALI) في الحاسب وعلى الإنترنت كما يلي:

010000010100110001001001

لنفرض أن شخصاً يود إرسال كلمة (ALI)عبر الإنترنت لصديقه علي، فإن عليه أولاً الحصول على المفتاح العام لعلي، ليستخدمه في تشفير الكلمة. لنفرض أن الطريقة التي يعمل بها ذلك المفتاح العام عند التشفير هي أن يقوم بضرب كل حرف بالرقم ٢، أي كما يلي:

* حرف A= 01000001 يتحول بعد الضرب في ٢ إلى 10000010، وهو عبارة عن الحرف الفرنسي (é).

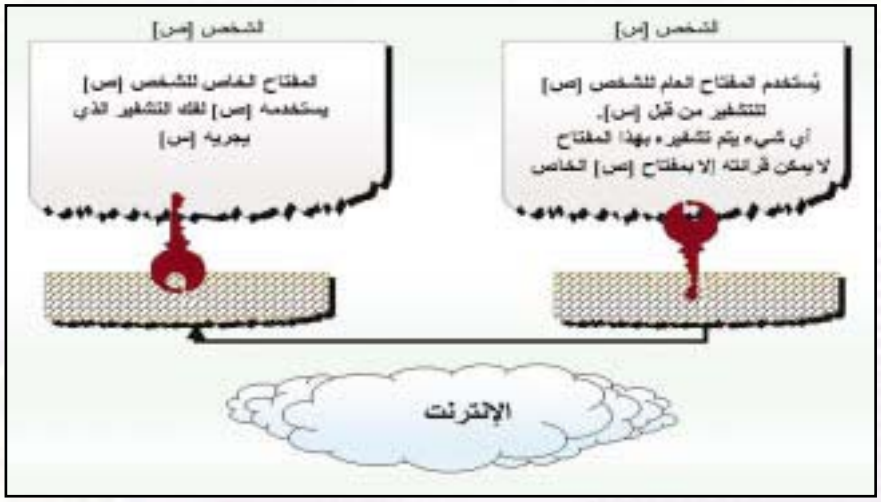
*حرف L = 0100 1100 يتحول بعد الضرب في ٢ إلى 10011000، وهو عبارة عن علامة (–).

* حرف I = 0100 1001 يتحول بعد الضرب في ٢ إلى 10010010، وهو عبارة عن أحد الحروف الأجنبية (?).

فيتم نقل الكلمة المراد إرسالها على أنها (é_ ?)، والتي لا يمكن لأحد أن يعرف أنها تعني كلمة (ALI) ما لم يعلم بأن المفتاح المستخدم لفك الشفرة هو القسمة على الرقم ٢. وهناك طرق رياضية متقدمة تعتمد على مفاهيم رياضية معقدة تعتمد في مجملها بعدم إمكانية عكس العملية للحصول على النص الأصلي، والتي جعلت من السهولة فك التشفير في المثال السابق.

التشفير وسلامة المحتوى

نظراً لبطء عملية التشفير بواسطة المفاتح العامة فإنها لا تستعمل ـ غالباً ـ في تشفير البيانات، ولكن تستخدم فقط للتوقيع الإلكتروني والتثبت من هوية المتعاملين، إضافة إلى استخدامها في تمرير مفتاح التشفير التقليدي ـ يتميز بسرعة التشفير عن طريقه ـ قبل البدء بعملية التراسل، فعلى سبيل المثال لكي يستطيع



● شكل (١) طريقة إرسال رسالة مشفرة.

الشخص (س) إرسال وثيقة مشفرة للشخص (ص)، شكل (١)، ولكي يضمن سلامة المحتوى من العبث والتغيير، فإن عليه إتباع الخطوات التالية:

١ـ الحصول على المفتاح العام للشخص (ص).

٢ـ إختيار مفتاح تشفير تقليدي بطريقة آلية عشوائية عن طريق برنامج التشفير في جهاز (س)

٣ـ القيام بتشفير ذلك المفتاح التقليدي بإستخدام المفتاح العام لـ (ص)، بحيث لا يستطيع أحد قراءته عدا (ص) وإرساله إلى (ص).

٤ـ إرسال الوثيقة مشفرة إلى (ص)، الذي يستطيع بدوره قراءتها بواسطة مفتاح التشفير التقليدي الذي حصل عليه من (س).

لاحظ أن الشخصين (س) و (ص) لم يسبق لهما أن إلتقيا وجهاً لوجه، وإلا لربما تبادلا مفاتحهما العامة، ولم يعد هناك حاجة للتأكد من هوية الآخر، بل إنه من الممكن أن يتفقا على مفتاح التشفير التقليدي، ولا يكون هناك حاجة للبنية التحتية للمفاتح العامة (PKI) على الاطلاق، حيث أن الهدف الجوهري من المفاتح العامة هو التحقق من هوية الأطراف المعنية، وليس التشفير بحد ذاته، ومع ذلك فإنها تمكّن المتعاملين من تغيير مفاتح التشفير التقليدية متى شاؤوا ـ منعاً لاكتشافه من قبل الآخرين ـ وذلك بتشفيرها بواسطة المفتاح العام للشخص الآخر. بقي علينا الإجابة على الأسئلة التالية فيما يخص قيام (س)بإرسال رسالة مشفرة لـ (ص).

السؤال: كيف يقوم (س) بالحصول على المفتاح العام للشخص (ص) ؟

الإجابة: هناك جهات معينة تقدم خدمة إصدار الشهادات الرقمية تعرف بهيئات الشهادات الرقمية (Certification Authority) وهي التي تقوم بالمصادقة على إرتباط المفتاح العام بالشخص. فيمكن لـ (س) البحث في أدلة المفاتح التي تحتفظ بالمفاتح العامة للأشخاص والتأكد من صحة المفتاح عن طريق هيئة التصديق.

السؤال: كيف يضمن كل من (س) و (ص) سلامة البيانات من التغيير والعبث؟

الإجابة: لاحظ أن كل ما يقوم به (ص) هو مجرد فك التشفير عن الوثيقة التي تصله من (س)، ولا يعرف إن كان قد حصل لها تغيير أو حذف وهي في طريقها إليه. ويتمثل الحل هنا في إجراء عملية مختصر حسابي (Hashing) أو (Checksum) وهي عملية رياضية معينة تُجرى على محتوى الوثيقة، يتم فيها تحويل قيمة بيانات الوثيقة إلى عدد محدود ـ وليكن مكوناً من ٤٠ رقماً ـ يرفق مع الوثيقة المرسلة. ومعلوم في علم الرياضيات استحالة تطابق المختصر الحسابي لوثيقتين إلا إذا كانت كل وثيقة مطابقة للأخرى. وعند وصول الوثيقة إلى (ص) فإنه يقوم بإجراء العملية الحسابية نفسها على البيانات، ليخرج بعدد مكون من ٤٠ رقماً. فإذا تطابق الرقمان دل ذلك على أنه لم يحدث أي تغيير للوثيقة المستلمة. ولضمان عدم قيام شخص آخر بتغيير محتوى الوثيقة، وإجراء المختصر الحسابي الخاص بها وإرفاقه معها، يجب على (س) القيام بتشفير المختصر الحسابي بواسطة المفتاح العام لـ (ص) قبل إرسال الوثيقة.

السؤال: كيف يتحقق (ص)من أن المرسل هو في الواقع (س)؟

الإجابة: لا يكفي هنا أن يتم التراسل بسرية تامة وبسلامة تامة للمحتوى إذا كان (ص) لا يعلم بشكل قاطع أن الوثيقة فعلاً وصلته من (ص). الحل هنا أن يقوم (س) بالتوقيع على البيانات بواسطة مفتاحه الخاص، ويقوم (ص) بالتحقق من التوقيع بالحصول على المفتاح العام لـ (س) وإجراء العملية الحسابية اللازمة للتأكد من أن المفتاحين هما للشخص ذاته، كما سوف نرى في شرح طبيعة التوقيع الإلكتروني.

● مثال لاستخدام المفاتح العامة خلال الإنترنت

من أكثر استخدامات البنية التحتية للمفاتح العامة مانراه في مواقع التجارة الإلكترونية، ومواقع إجراء العمليات المصرفية من خلال الإنترنت. لكي يثق العميل بموقع المصرف على الإنترنت، فإنه بحاجة إلى جهة رسمية تؤكد بأن الموقع الذي يوشك الدخول إليه هو بالفعل الموقع الخاص بالمصرف، ويتم ذلك بمطابقة التوقيع الظاهر في الشهادة الرقمية الخاصة بالموقع بتوقيع هيئة التصديق المعروفة لدى العميل.

إن الذي يتم عادة هو أن يقوم المصرف بالحصول على مايعرف بشهادة موقع (Server certificate)، لاستخدامها في بروتوكول نقل البيانات المعروف بـ (SSL)، ويحصل المصرف على هذه الشهادة عن طريق إحدى هيئات التصديق المعروفة أو عن طريق هيئة تصديق خاصة به. كل ما تمنحه هذه الشهادة هو الإقرار بأن المصرف الفلاني هو المالك الفعلي للمفتاح العام المرفق بالشهادة، وأن المفتاح الخاص (المرتبط بذلك المفتاح العام) موجود لدى المصرف. عندما يقوم العميل بتوجيه متصفح الإنترنت إلى موقع المصرف، فإن جهاز المصرف يقوم بإرسال شهادة الموقع إلى جهاز العميل، الذي يقوم بالبحث في الشهادات المعروفة لديه عن هوية هيئة التصديق التي قامت بالتوقيع على شهادة المصرف. في حالة وجود شهادة لتلك الهيئة، يقوم المتصفح بمطابقة توقيع الهيئة التي أصدرت شهادة المصرف بتوقيع الهيئة المتوفر لديه.حيث يدل تطابق التوقيعين، على أن هيئة التصديق المعروفة لدى عميل المصرف (في جهازه) قد قامت بالتوقيع، أي المصادقة، على شهادة المصرف. أما إذا كانت شهادة هيئة التصديق التي صادقت على شهادة المصرف غير معروفة لدى متصفح العميل، فإن المتصفح يبرز رسالة على الشاشة لاطلاع العميل بذلك يدعوه لاتخاذ القرار المناسب، إما إعتماد تلك الهيئة على مسؤوليته أو رفض الاتصال ومحاولة التأكد من صحة الموقع.

● شكل (٢) مثال لشهادة وهمية.

لاحظ أن شهادة المصرف وُجدت لكي يثق العميل في المصَرف، ولكن هناك كذلك حاجة لأن يثق المصرف بالعميل، وذلك بحصول العميل على شهادة عميل (Client certificate)، ليتأكد المصرف من هويته بمقارنة توقيع الهيئة التي أصدرت شهادة العميل بتواقيع الهيئات المعروفة لدى المصرف. وعلى الرغم من ذلك، فإن الكثير من العمليات الإلكترونية حالياً لا تشترط حصول العميل على شهادة، ربما لعدم شيوع الشهادات الرقمية بين المستخدمين، الأمر الذي سوف يتغير حتماً في الفترات القادمة.

● الشهادة الرقمية

يوجد في المملكة هيئات تصديق خاصة، قائمة أو تحت الانشاء، منها هيئات التصديق التابعة لكل من مؤسسة النقد العربي السعودي، وشركة الزيت (ARAMCO)، وشركة الاتصالات السعودية، ومن المتوقع أن ينشأ هيئات تصديق أخرى في المستقبل القريب.

تقوم هيئات التصديق بالإقرار بأن الشخص المدون إسمه في الشهادة هو المالك الفعلي للمفتاح العام الظاهر في الشهادة، وأنه المالك الفعلي للمفتاح الخاص المصاحب لذلك المفتاح العام. ويوضح شكل (٢) مثال لشهادة وهمية تبين إسم صاحب الشهادة، ومفتاحه العام، والرقم التسلسلي للشهادة، وتاريخ سريان مفعولها، وكذلك إسم هيئة التصديق المانحة للشهادة وتوقيعها عليها. حيث يعد توقيع الهيئة على الشهادة بواسطة المفتاح الخاص بها عملية تشفير للمختصر الحسابي، وتعتمد موثوقية الشهادة الرقمية على ما يلي:

- الطريقة التي تعمل بها هيئة التصديق لإثبات هوية المستخدم.
- أسلوب العمل والأنظمة التشغيلية لدى هيئة التصديق.
- الخوارزميات الفنية المستخدمة في عملية التشفير وإثبات الهوية.
- الإطار القانوني الذي تعمل به هيئة التصديق و مدى إلتزامها به.

● شكل (٣) مثال لشكل التوقيع الإلكتروني.

- مدى محافظة الشخص على المفتاح الخاص به.

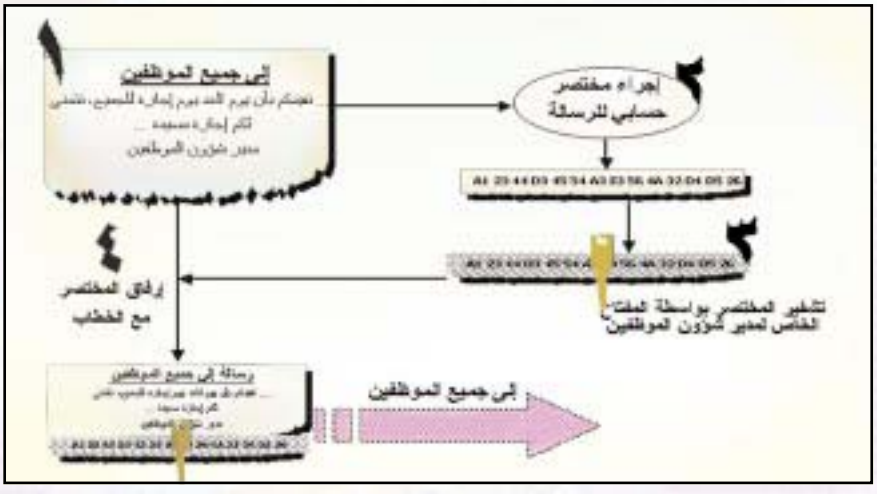
وتعد البطاقة الذكية (Smart card) من أفضل الطرق للمحافظة على المفتاح الخاص، حيث أنها لا تسمح بخروج المفتاح من البطاقة، بل إن عملية إنشاء المفتاح ذاته تتم داخل البطاقة وليس في جهاز المستخدم ولا في جهاز هيئة التصديق.

التوقيع الإلكتروني

التوقيع الإلكتروني عبارة عن إجراء يقوم به المرسل لربط هويته بالوثيقة الموقع عليها، وبحيث يمكن لمستلم الوثيقة التحقق من صحة التوقيع. ولا يعني التوقيع الإلكتروني الإمضاء المعروف الذي يتم غالباً على الورق، بل هو عبارة عن نص قصير يضاف إلى أول أو آخر الوثيقة، وقد يكون مفصولاً عنها تماماً، كأن يرسل في ملف مستقل. يبين الشكل (٣) مثالاً لشكل التوقيع الإلكتروني عند ظهوره على الشاشة.

يختلف التوقيع الإلكتروني عن التوقيع على الورق في كونه يؤكد هوية المرسل بشكل قاطع ويمنع حدوث أي تغيير أو عبث في الوثيقة الموقع عليها، وذلك بشرط أن تتم العملية بكاملها حسب قواعد وأسس البنية التحتية للمفاتح العامة، أو ما يعادلها من تقنيات أخرى. والتوقيع الذي تتوفر فيه هذه الشروط يسمى التوقيع الرقمي وليس التوقيع الإلكتروني. ويعد التوقيع اليدوي على الورق قابل للتزييف بسهولة رغم إختلاف التوقيع من شخص لآخر وصعوبته، كما إن عملية التحقق من صحته التوقيع اليدوي غير عملية، لإعتمادها على مهارة الشخص الذي يقوم بمطابقة التوقيع، أو على معرفته السابقة بالشخص الموقع. كذلك فإن الوثيقة الموقعة يدوياً قابلة للتغيير والعبث، وفي كثير من الأحيان يأتي التوقيع اليدوي في نهاية وثيقة مكونة من عدة صفحات من السهل قيام عابث بتغيير بعض صفحاتها دون أن يلحظ أحد ذلك، وعليه ـ بإختصار ـ فإن التوقيع الإلكتروني يتجنب جميع المشاكل الناتجة عن التوقيع اليدوي متى ما تم إحداثه بطريقة صحيحة.

* **كيفية عمل التوقيع**، عندما يود مدير شؤون الموظفين إرسال إعلان لجميع الموظفين عن موعد الإجازة، فإن الحاجة في هذه الحالة ليست للتشفير ولكن فقط للتأكد من أن الإعلان صادر بالفعل منه. وهنا يفترض بأن جميع الموظفين لديهم المفتاح العام لمدير شؤون الموظفين،وتتم



● شكل (٤) كيفية عمل التوقيع الإلكتروني.

العملية، شكل(٤) كالتالي:

١ـ يقوم المدير بإعداد الإعلان.

٢ـ يقوم الجهاز لديه بإجراء العملية الرياضية التي تضمن سلامة المحتوى (راجع شرح الطريقة أعلاه) ليستخرج المختصر الحسابي الخاص بتلك الوثيقة.

٣ـ يقوم الجهاز بتشفير المختصر الحسابي بإستخدام المفتاح الخاص لمدير شؤون الموظفين، وذلك لمنع قيام شخص آخر بتغيير الإعلان وإعادة حساب المختصر الحسابي وإرفاقه مع الإعلان.

٤ـ يتم إرفاق المختصر الحسابي مع الوثيقة ويرسل الملف الناتج إلى جميع الموظفين عن طريق البريد الإلكتروني.

عند إستلام أحد الموظفين للإعلان، يقوم جهازه بالتأكد من صحة التوقيع وذلك بإجراء الخطوات الظاهرة في الشكل (٥).

١ـ استلام الإعلان المرفق به التوقيع.

٢ـ إجراء المختصر الحسابي للوثيقة بإستخدام العملية الرياضية نفسها التي تمت في جهاز مدير شؤون الموظفين

٣ـ يقوم الجهاز بإستخدام المفتاح العام لمدير شؤون الموظفين لفك التشفير عن المختصر الحسابي المرفق بالإعلان، تؤكد هذه الخطوة بأن المرسل هو بالفعل مدير شؤون الموظفين، ولكنها لا تضمن سلامة نص الإعلان من العبث أو التغيير في الطريق

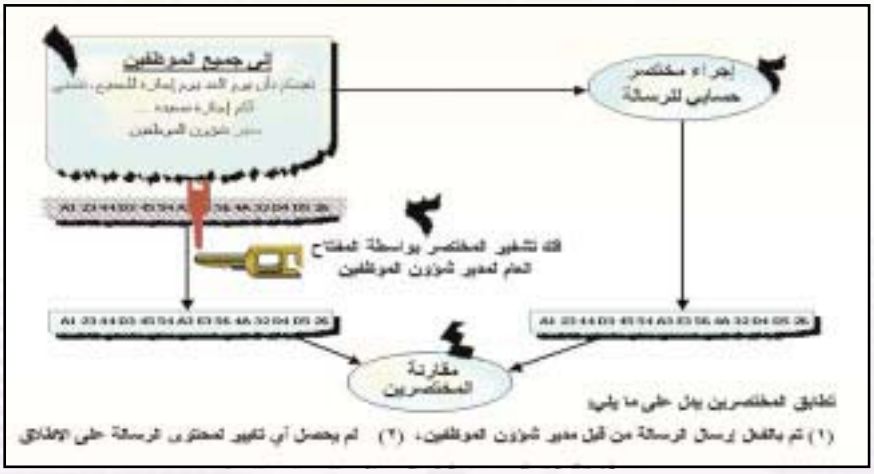
٤ـ مقارنة الرقمين (من الخطوتين ٢ و ٣)، للتأكد من عدم وجود تغير أو عبث للنص أثناء الطريق

أنظمة وقوانين المفاتح العامة

من أهم أنظمة وقوانين المفاتح العامة ما يلي:

● نظام الشهادات الرقمية

نظام الشهادات الرقمية (Certification Policy) عبارة عن مجموعة من الشروط والارشادات التي تبين لمستخدم الشهادة مدى ملائمة الشهادة الرقمية الصادرة من هيئة التصديق لاحتياجاته ومدى الموثوقية المصاحبة لها، وكذلك تحديد الاستخدامات المشروعة وغير المشروعة لها، ويبين هذا



● شكل (٥) مطابقة التوقيع من قبل المستلم.

النظام إلتزامات هيئات التصديق والتي تشمل ما يلي:

ـ إصدار الشهادات وإلغائها.

ـ إثبات هوية المستخدم قبل الإصدار.

ـ تخزين ونشر الشهادات الصادرة والشهادات الملغاة.

ـ الطرق الواجب إتباعها عند إصدار الشهادات للتأكد من سلامة الإجراءات المتبعة.

يجب على الجهة الراغبة في إصدار شهادات رقمية الإلتزام بجميع الشروط الواردة في هذا النظام، والتي من أهمها ضرورة إصدار ما يعرف باللوائح الإجرائية الإصدار الشهادات الرقمية (Certification Practice Statement)، والتي عن طريقها يستطيع المستخدم معرفة الطرق الفنية والأمنية والإجرائية المتبعة لإصدار الشهادة من قبل هيئة التصديق، وكذلك كامل حقوقه ومسؤوليته الناتجة عن استخدامها.

كما يتطرق النظام لدور مراكز التسجيل (Registration Authorities) للمساعدة بالتثبت من هوية المستخدم ومتابعة إجراءات الإصدار والإلغاء وما إلى ذلك، ويجب أن لا يشمل دور مراكز التسجيل إصدار الشهادات، حيث يقتصر ذلك على هيئات التصديق فقط.

وفيما يخص المستخدم فهناك شروط عليه الإلتزام بها، منها:

ـ التقيد باللوائح الإجرائية لإصدار الشهادات الرقمية.

ـ المحافظة على مفتاحه الخاص.

ـ إشعار هيئة التصديق في حالة فقدانه، أو إكتشافه من قبل الآخرين.

ـ معرفة ما له وما عليه فيما يخص حقوقه ومسؤولياته.

وبإختصار يمكن القول بأن نظام الشهادات الرقمية هو عبارة عن الدليل الكامل لجميع المتعاملين به يمكن الرجوع إليه عند حاجة المستخدم للحصول على شهادة، أو عند حاجة هيئة التصديق لمعرفة إلتزاماتها تجاه الآخرين، أو قبل قيام شخص بمطابقة توقيع شخص آخر، أو عند حاجة الجهات التجارية والحكومية معرفة ما يمكنهم الإستناد إليه عند قيامهم بالتعامل الإلكتروني.

● قانون الأونسترال(UNCITRAL) النموذجي للتجارة الإلكترونية

رأت الجمعية العامة للأمم المتحدة التي أنشأت لجنة الأمم المتحدة للقانون التجاري الدولي في عام ١٩٦٦م، أن هناك حاجة لإعداد قانون عام للتجارة الإلكترونية يستخدم كمثال يحتذى به من قبل دول العالم الراغبة في الأخذ بالطرق الإلكترونية في المعاملات التجارية. وحسب هذا القانون النموذجي فإنه يجب الإعتراف القانوني بالمعلومات المرسلة بشكل إلكتروني ومعاملتها تماماً كما تعامل العمليات التجارية على الورق. فمتى ما كان هناك نظام يشترط وجود وثيقة ما بشكل مكتوب، فإن وجود هذه المعلومة بشكل

إلكتروني يفي بالغرض. وكذلك فيما يخص التوقيع وإبراز النسخة الأصلية من عقد أو خطاب أو فاتورة، وما إلى ذلك، فإن من الممكن لها أن تتم بطريقة إلكترونية. ويؤكد هذا القانون النموذجي على قانونية العقود الإلكترونية وضرورة إعتراف الأطراف بجميع أنواع البيانات التي تتم بشكل إلكتروني.

يقدم القانون النموذجي مثالاً لتطبيق القانون على تجارة البضائع التي تشتمل على:

- اتفاقيات نقل البضائع وطبيعتها وعددها.
- فواتير الاستلام والمطالبة بالتسليم والإذن بالإفراج عن البضائع.
- تسليم البضائع إلى شخص معين أو جهة معينة.
- أي ضوابط أخرى تستخدم في هذا المجال.

● قانون الأونسترال(UNCITRAL) النموذجي للتواقيع الإلكترونية

قامت منظمة الأونسترال في عام ٢٠٠١م بإصدار القانون النموذجي للتواقيع الإلكترونية، ليكون مكملاً لقانون التجارة الإلكترونية وقاعدة أساسية له. يختص هذا القانون بمنح التوقيع الإلكتروني المعتمد الصبغة القانونية اللازمة لمساواته بالتوقيع اليدوي. ويعد التوقيع الإلكتروني معتمداً إذا تم الإقرار به من قبل جهة رسمية مخولة بذلك، والتي قد تحدد بعض الشروط اللازم توافرها في التوقيع الإلكتروني ليكون صحيحاً ومعتمداً، منها مايلي:

١- يجب أن يرتبط التوقيع بشكل قاطع بالشخص أو الجهة التي قامت به.

٢- يجب أن يكون التوقيع تحت سيطرة الشخص الذي قام بالتوقيع وقت حدوثه.

٣- يجب أن تكون هناك قدرة على إكتشاف أي تغيير أو عبث يطرأ على التوقيع الإلكتروني أوالوثيقة الموقع عليها.

ويتطرق القانون كذلك لبعض الأنظمة والشروط اللازم توفرها في من يقوم بتقديم خدمة التواقيع الرقمية (كهيئات التصديق)، وقوانين أخرى تخص مسؤولية المتعاملين بالتواقيع الإلكترونية ضماناً لحفظ حقوقهم القانونية.

واقع المفاتح العامة في المملكة

صدر في ١٤١٩/١٠/٢٧هـ أمر سامي بتشكيل لجنة دائمة للتجارة الإلكترونية كانت **مدينة الملك عبد العزيز للعلوم والتقنية** عضواً فيها، ثم تم رفع مستوى التمثيل في هذه اللجنة إلى مستوى الوكلاء المختصين بأمر سامي بتاريخ ١٤٢١/٩/١٠هـ، وقامت اللجنة بإختيار **مدينة الملك عبد العزيز** لتتولى مهمة إنشاء وتشغيل المركز الوطني لتصديق الشهادات الرقمية بتاريخ ١٤٢٢/١/١٠هـ، وتمت الموافقة السامية على ذلك بتاريخ ١٤٢٢/٥/١٧هـ.

يتمثل دور **المدينة** في تأسيس وتشغيل المركز الوطني لتصديق الشهادات الرقمية - المعروف بـ (Root CA) - وتحديد متطلبات هيئات التصديق، وتحديد الأنظمة واللوائح الخاصة بالتواقيع الإلكترونية، إلى جانب تحديد متطلبات أمن المعلومات والخصوصية، وإنشاء لجنة عليا لإدارة البنية التحتية ومراجعة الأنظمة والقرارات المتعلقة بالبنية التحتية والتنسيق فيما بين هيئات التصديق.

● وظيفة المركز الوطني

يلعب المركز الوطني لتصديق الشهادات الرقمية (Root CA) - وغيره من الهيئات الخاصة والشبيهة به مثل هيئة التصديق التابعة لمؤسسة النقد العربي السعودي، وهيئة التصديق التابعة لشركة الزيت (ARAMCO)، شركة الاتصالات السعودية - وأي هيئات تصديق عامة للأفراد والجهات الحكومية والتعليمية وغيرها- دوراً هاماً في عملية الثقة بين المتعاملين.

ويعد وجود المركز الوطني في غاية الأهمية للأسباب التالية:-

١- واجهت العديد من الدول التي لم تقم بإنشاء هيئة عليا للتصديق صعوبات كبيرة فيما يخص قانونية التعاملات التي تتم في غياب جهة رسمية، مثل: مدى المسؤولية التي تتحملها هيئات التصديق، وسلامة الإجراءات المتبعة في إصدار الشهادات الرقمية، وحقوق المستخدمين وخصوصيتهم، وغيرها من الأمور.

٢- لكي يتم التعامل الإلكتروني بموثوقية تامة فمن الواجب أن يكون هناك جهة عليا تقوم بالمصادقة على هيئات التصديق نفسها. كيف يمكن لجهة خارجية، على سبيل المثال، مطابقة توقيع شخص حصل على شهادته الرقمية من هيئة تصديق سعودية ليس بينها وبين الجهة الخارجية أي علاقة؟ وعلى أي أساس يمكن لتلك الجهة الخارجية الوثوق من سلامة إجراءات منح الشهادة الرقمية التي تقوم بها هيئة التصديق هذه؟

٣- إن وجود هيئة عليا للتصديق من شأنه أن يساعد على التوافق والتطابق الفني والإداري للأعمال التي تقوم بها هيئات التصديق، الأمر الذي يضفي جواً من التناسق والتلاؤم فيما بينها، ويساعد في عملية توافق الشهادات الصادرة من هيئات التصديق المختلفة. كما إن بامكان الهيئة العليا فرض مواصفات ومقاييس عامة تلتزم بها جميع الأطراف المعنية لتحقيق الصالح العام.

من جانب آخر هناك بعض المفاهيم الخاطئة التي يجب تصحيحها فيما يخص دور المركز الوطني للتصديق ودوره في الأمن والخصوصية:، منها:

١- لا يقوم المركز الوطني بالاحتفاظ بالمفاتح الخاصة (Private keys) للأفراد ولا لهيئات التصديق، حيث إن عمله الحقيقي لا يتطلب التعامل مع المفاتح الخاصة، بل إنه يقوم فقط بالمصادقة على كون المفتاح العام للشخص أو الجهة ملكاً لذلك الشخص أو تلك الجهة.

٢- لا يقوم المركز الوطني بإصدار المفاتح الخاصة سواء للأفراد أو هيئات التصديق، ولذا فإنها لا تمر عن طريق المركز على الاطلاق.

٣- لا يستطيع المركز الوطني فك التشفير عن أي بيانات مشفرة من جهة أخرى، لكونه لا يملك المفاتح اللازمة لفك التشفير. غير أن هناك حالات يمكن من خلالها فك التشفير من قبل جهة أخرى، وذلك بإستخدام طريقة الحفظ لدى جهة مختصة، والتي تعرف بطريقة (Escrow)، حيث يقوم الشخص أو هيئة التصديق طواعية بحفظ المفتاح الخاص به لدى تلك الجهة، أو السماح للجهة بالحصول على