نحو إطار عام لتطبيق استخدام منظومة التوقيع الالكتروني في مؤسسات المعلومات

دراسة للإطار التقني والتنظيمي والبنية التحتية

د. أحمد فرج أحمد

قسم دراسات المعلومات كلية علوم الحاسب والمعلومات

جامعة الإمام محمد بن سعود الإسلامية

المستخلص

تركز هذه الدراسة على عدة محاور من أبرزها استعراض المفاهيم الأساسية والأهداف والتحديات المتعلقة بمنظومة التوقيع الالكتروني، إلى جانب دوره البارز الذي يؤديه في سبيل تأمين أنظمة المعلومات الخاصة بمؤسسات المعلومات، وما يمكن أن يحققه لرفع معدل الوثوق في المعاملات والإجراءات الالكترونية من خلال الخصوصية ووحدة البيانات واستقامتها وعدم القدرة على إنكار القيام بالمعاملات والتحقق من هوية المستخدم. كما تتناول الدراسة الإطار التقني والتنظيمي للتوقيع الالكتروني وهو ما يطلق عليه البنية التحتية للمفاتيح العامة PKI وما تتضمنه من الشهادات الالكترونية سواء كانت شخصية أو خاصة بأجهزة الخوادم وسبل إنشاء واستخدام وحفظ هذه الشهادات والوسائط التي تختزن من خلالها. كما تتعلق هذه الدراسة بإنماط الكتابة المشفرة من خلال التشفير التماثلي وغير التماثلي والتشفير من خلال المفتاح العام والمفتاح الخاص، إلى غير من المحاور التي تلعب دور جوهري في سبيل تبني تطبيق إطار عام لاستخدام منظومة التوقيع الالكتروني في مؤسسات المعلومات

الكلمات الدالة

التوقيع الالكتروني ، الإدارة الالكترونية ، الشهادات الالكترونية ، سياسة التشفير ، أنظمة المعلومات ، سلطة التصديق ، سلطة التسجيل

1. مقدمة

لجأت العديد من مؤسسات المعلومات والمراكز البحثية في الدول المتقدمة إلى تبني إجراءات لمواجهة الاحتياجات المتنامية المتعلقة بتطوير وميكنة الإجراءات والخدمات المقدمة، إلى جانب الرغبة المتزايدة في تأمين أنظمة المعلومات لتحقيق مستويات أفضل من الكفاءة والفاعلية.

ويجب أن يرتكز استخدام تطبيقات تكنولوجيا المعلومات والاتصال على أربعة مبادئ تتمثل في: البساطة والتأمين والخصوصية وأخيراً تطبيق مبدأ العمل وفق سمات واهتمامات المستخدمين.

وتكمن إحدى الأهداف الأساسية للمرحلة الراهنة والمتعلقة بتطوير الإدارة الالكترونية في الانتقال من المعالجة العشوائية (وفيها يكون المستخدم مجهول أو غير معروف) إلى معالجة تعتمد على التعرف على هوية المستخدم (شخص أو مؤسسة). وكما يقتضي تطوير الإدارة الالكترونية الالتزام بقواعد الخصوصية وحماية البيانات في مناخ من الثقة، مما يستوجب على كل من المؤسسات ومجتمع المستفيدين ضرورة تبني آليات تعمل على تأمين والمحافظة على خصوصية البيانات والمعلومات التي يتم نقلها بشكل الكتروني من خلال منظومة شبكات المعلومات سواء كانت داخلية "tenartnI" أو عبر الشبكة العالمية "tenretnI".

وجدير بالذكر انه نتيجة لتعقد التقنيات المتعلقة بتأمين نظم المعلومات الآلية، ظل استخدامها -لفترة ليست بالقصيرة- مقتصراً على المتخصصين في تقنيات الحاسبات الآلية، ولكنه من الآن فصاعداً، قد أصبح أمراً أساسياً أن يتأقلم مستخدمي هذه التقنيات مع التحديات والمتطلبات المختلفة سواء كانت تقنية أو قانونية أو متعلقة بحقوق الوصول إلى المعلومات.

وتكمن الإشكالية الأساسية في دراسة مثل هذا الموضوع، في ضرورة أن يتم النظر إليه من خلال زوايا متعددة سواء كانت وظيفية وتقنية فنية وقانونية، وتتعلق هذه الدراسة بمحاولة تصور إطار عام لتطبيق استخدام التوقيع الالكتروني في مؤسسات المعلومات والمراكز البحثية، مع المشاركة بسلسلة من المقترحات التي من شأنها إتاحة الفرصة أمام نشر هذه التقنية المتطورة، مع التركيز على أن الممارسات والتطبيقات المتعلقة باستخدام التوقيع الالكتروني في مؤسسات المعلومات والمراكز البحثية المختلفة.

وتستعرض الدراسة أساليب نشر منظومة التوقيع الالكتروني في مؤسسات ومراكز المعلومات وإداراتها المختلفة، الأمر الذي له تأثيرات مباشرة على الأبعاد التقنية والتنظيمية والقانونية للتطبيقات المستخدمة.

2. التوقيع الالكتروني: مفاهيم أساسية

1.2. مفهوم التوقيع الالكتروني

عرفت المنظمة الدولية للتوحيد القياسي ISO (International Organization for Standardization) التوقيع الالكتروني بأنه تحويل مشفر لوحدة البيانات بحيث يسمح للشخص المرسل إليه الرسالة إمكانية تحديد مصدرها ومدى استقامة ووحدة البيانات من خلال حمايتها من أي تزوير أو تزييف (ISO 7 498-2).

ويمكن ملاحظة أن هذا التعريف يغطي مبدأين أساسيين من مبادئ التوقيع الالكتروني وهما التحقق أو التوثيق من ناحية ووحدة واستقامة البيانات من ناحية أخرى.

وهذا الاتجاه الوظيفي تم استكماله بتعريف أخر يركز على الجانب القانوني، حيث يعطي صفة أو صيغة رسمية لهذا التوقيع.

وينبغي التأكيد على أن مفهوم التوقيع الالكتروني يختلف كلياتاً عن التوقيع المرقمن (الذي يعتبر صورة في شكل الكتروني من التوقيع الخطي التقليدي والذي يتم الحصول عليه من خلال أجهزة الماسحات الضوئية Scanners) والذي ليست له أي قيمة أو سند قانوني فيما يختص بتأمين أنظمة المعلومات.

2.2. أهداف استخدام التوقيع الالكتروني

يزيد إتاحة أنظمة المعلومات في متناول مستخدمين متباعدين جغرافياً من معدل ضعف تأمينها، وبناء عليه أصبح من الضروري ضمان خصوصية وسرية البيانات التي يتم تبادلها والتحقق من هوية المستخدمين قبل منحهم التصاريح التي تُمكنهم من الوصول إلى المصادر المتاحة.

وتستهدف منظومة التوقيع الالكتروني توفير مستوى من التأمين، لضمان قدر من الثقة لمختلف العناصر المشاركة في عملية التبادل الالكتروني والحفظ والاختزان الطويل الأمد للبيانات الالكترونية. وبفضل هذا المناخ، يمكن أن يصل معدل الثقة في التوقيع الالكتروني إلى مستوى متطابق تماماً مع المعدل الذي يمكن تحقيقه من خلال المستندات الورقية. وحتى يتم منح صفة قانونية للتوقيع الالكتروني، يجب ضمان جودته وصلاحيته من خلال مستويين هما:

- مستوى تقني: ويتمثل في منع أي استخدام احتيالي أو تزويري للتوقيع
- مستوى قانوني: يتمثل في إعطاء صفة أو صبغة قانونية قاطعة للتوقيع الالكتروني

وهذا الأمر لا يتعلق فقط بضرورة ضمان خصوصية البيانات المرسلة من خلال تقنيات التشفير والترميز ولكن أيضاً ضرورة ضمان باقي مستويات وخدمات التأمين والتي تتمثل في وحدة البيانات واستقامتها وعدم التنصل أو (عدم القدرة على الإنكار) والتحقق أو التوثيق أو (التعرف على المستخدم)، وبفضل الإطار التقني والقانوني الذي يمكن استخدامه يمكن للتوقيع الالكتروني تأدية كافة هذه الخدمات.

3.2. التحديات المرتبطة بالتوقيع الالكتروني

1.3.2. تأمين أنظمة المعلومات

من المعروف أن البناء الهيكلي لشبكة الانترنت العالمية "Internet" لم يتم تصوره منذ البداية لتلبية الاحتياجات التي تستلزم إجراءات تأمينية فعالة، حيث يمثل (DNS (Domain Name Server إحدى آليات التراسل عبر شبكة الانترنت، والذي لا يمكن اعتباره حتى وقتنا الراهن وسيلة مؤمنة. إلى جانب ظواهر الهجوم بالفيروسات الحديثة على البيانات والمعلومات المتاحة في مواقع الشبكة العنكبوتية (الويب)، وبروز تقنيات "Spam" والتي تعمل على إرسال الكثير من الرسائل الالكترونية غير المرغوبة، كما أصبح من السهل نسبياً التعدي على الهوية من خلال منظومة البريد الالكتروني، وخاصة اقتناص الرسائل البريدية التي تخص شخص معين وإمكانية العبث في محتوياتها والتعديل فيها، والولوج بشكل احتيالي إلى مواقع غير مصرح لغير المشتركين فيها الدخول والإطلاع على محتوياتها.

وبناء على تلك الإشكاليات، يكمن الهدف الرئيسي من وراء تطبيقات للتوقيع الالكتروني ليس فقط في إتاحة مجموعة من التقنيات الحديثة، ولكن أيضاً توفير مناخ من الثقة على مجمل المعاملات التي تتم عبر شبكات المعلومات.

ويعتبر تأمين التبادل الالكتروني عبر أنظمة المعلومات المختلفة من المسائل الحيوية والتي تمثل مجالا خصباً لمجموعات من الدراسات والتطبيقات على المستوى الدولي، حيث أطلقت المفوضية الأوربية "European Commission" من خلال برنامج "أوربا الالكترونية" "E- Europe" جدول زمني لتطبيق وتعميم استخدام الإدارة الالكترونية والذي أنتهي رسمياً مع نهاية عام 2005.

ومن اجل إنشاء وتدعيم "ثقافة تأمين المعلومات" والتنسيق بين أعمال ومهام المؤسسات الأوربية، تم إنشاء وكالة أوربية في نوفمبر من عام 2003 تحت تسمية" وكالة الشبكة الأوروبية وأمن المعلومات" European) Network and Information Security Agency، ENISA)[1].

وبناء عليه أصبحت سياسة تأمين أنظمة المعلومات عامل استراتيجي له أولوية قصوى على مستوى الدول ومؤسساتها المعلوماتية.

وفي دولة فرنسا على سبيل المثال يمكن التمثيل بخطة "RE/SO 2007 " (من أجل جمهورية رقميه في عصر مجتمع المعلومات) والتي قدمها رئيس الوزراء الفرنسي في 12 نوفمبر من عام 2002، بهدف دعم منظومة ايمقرلا ةيروهملجة. والتي أكد فيها رئيس الوزراء الفرنسي ضرورة إقامة الشروط المتعلقة بضمان الثقة عند التبادل الالكتروني. ويمثل القانون الخاص بالاقتصاد الرقمي (التجارة الالكترونية) أحد المحاور الرئيسية لهذه الخطة.

2.3.2. الإطار العام للثقة في المعاملات الالكترونية

وتطالب كل من منظمة التعاون والتنمية الاقتصادية OECD[2] والاتحاد الأوربي في العديد من التقارير المتعلقة بالإدارة الالكترونية ضرورة الالتزام بأربعة وظائف أو مستويات أساسية لضمان تامين أنظمة المعلومات والإدارة الالكترونية وهي:

1. الخصوصية Confidentiality

ويقصد بالخصوصية، أن عملية الولوج إلى المعلومات المتاحة في شكل الكتروني تقتصر فقط على الأطراف المشاركة في الاتصال (الأشخاص، والتطبيقات، والبرمجيات، والأجهزة)، وتستند الخصوصية على مبدأ التشفير الذي يمكن إجرائه على البيانات والمعلومات.

2. وحدة البيانات واستقامتها Integrity

يؤدى الالتزام بوحدة البيانات واستقامتها إلى ضمان أن المعلومات المتبادلة لم يتم التدخل فيها أو تعديلها وذلك في الفترة ما بين إرسالها من جانب المرسل واستقبالها بواسطة المرسل إليه. وجدير بالذكر أنه بدون الاستناد إلى تطبيقات التوقيع الالكتروني، من العسير اكتشاف أي تعديلات أو تغييرات تطرأ على مستند أو نص معين. ويجب في بعض الحالات، ضمان هذه الاستقامة طوال الفترة التي يتم فيها الاحتفاظ بالبيانات والمعلومات. كما أن عملية أرشفة مستند معين والتوقيع الخاص به يجب أن يكون مؤمناً بهدف تفادي أي تعديلات يمكن أن تطرأ عليه فيما بعد.

3. عدم التنصل (عدم القدرة على الإنكار) Non-Repudiation

المقصود بعدم التنصل أو عدم النكران، أنه لا يمكن لأي طرف من الأطراف المشاركة في عملية التراسل إنكار القيام بالمعاملة أو الإجراء، ولضمان عدم النكران لابد أن تتوافر إمكانية التتبع المستمر للمعاملة التي يتم القيام بها، وبالتالي معارضة أي رفض لها من خلال الإثبات الحاسم بالقيام بها. ويتعلق هذا الأمر باستخدام مجموعة متنوعة من آليات التوقيع الالكتروني منها منظومة تأكيد الإرسال والاستقبال والاستناد إلى تقنية تعمل على ضمان الحصول على تاريخ ووقت إجراء المعاملة، وهذه التقنية يطلق عليها "time-stamping" أو العمل على أرشفة المعاملة والتوقيع المرتبط بها.

4. التحقق (التعرف على المستخدم) Authentication

ويكمن الهدف من وراء التحقق أو التوثيق إلى التأكد من أن هوية المستخدم -سواء كانت (أسم مستعار، أو حقيقي، أو عنوان IP...)- تكون هوية متعارف عليها.

ويتوافر أساليب أساسية يمكن الاستعانة بها من أجل التعرف على المستخدم ومنها:

1. التحقق والتوثيق من خلال تقنيات التعرف على أسم المستخدم وكلمة السر خاصته.
2. إمكانية التحقق أو التوثيق من خلال امتلاك وسيط مادي يستخدم في عملية التحقق مثل (البطاقات الذكية، وبطاقات USB)

ويؤدى الربط بين الأسلوبين (الوسيط المادي إلى جانب كلمة السر) إلى رفع معدل التأمين، وذلك لأنه يضمن أن مستخدم الوسيط المادي هو صاحبه ومالكه الشرعي، وهو ما يطلق عليه التحقق الفعال أو تحقق ذو عاملين.

ويعتبر التحقق أمر أساسي في استخدام التطبيقات والخدمات المتاحة عن بُعد، ويمثل اختيار أسلوب التحقق الذي يسمح بإمكانية الوصول إلى مختلف تطبيقات نظام المعلومات، من المسائل الجوهرية المرتبطة بسياسات التأمين. كما ترتبط عملية الميكنة المستمرة للخدمات (داخل المؤسسة أو خارجها) بتقديمها وفقاً للسمات الشخصية لمجتمع المستفيدين، وبناء عليه فإن عملية الميكنة تقع في قلب نظام المعلومات المسئول عن إدارة الهويات الالكترونية والصلاحيات المرتبطة التي تجعل من الأهمية إمكانية التفاعل والعمل المتبادل بين الأنظمة، وفي نفس الوقت التأكيد على سهولة الاستخدام من جانب المستخدم النهائي.

3. الإطار التقني والتنظيمي للتوقيع الالكتروني (البنية التحتية للمفاتيح العامة PKI)

تتضمن تكنولوجيا "البنية التحتية للمفاتيح العامة".(Public Key Infrastructure) "PKI"، على كل من الإطار التنظيمي والبنية التقنية للتوقيع الالكتروني، ويكمن التحدي الرئيسي للتقنيات المستخدمة في إطار "PKI" في تغطية مجمل خدمات الخصوصية ووحدة البيانات واستقامتها وعدم النكران إلى جانب التحقق (التوثيق)، وبناء علية يمكن اعتبار "PKI" على أنه بناء تقني وإداري معاً.

وعادة ما يستند "PKI" على الإطار التالي:

- شهادة الكترونية تكون بمثابة تصريح مرور الكتروني (Passport)
- عملية التشفير وتتضمن على مفتاحين أحدهما عام والأخر خاص

ويتم استخدام هذه التقنيات في إطار مقنن يتمثل في:

- جهاتٌ محددة تتضمن سلطة التصديق و سلطة التسجيل
- سياسة التصديق

ويتم استخدام "PKI" وفقاً للأتي:

- الخدمات المتاحة: وهي التوقيع، والتشفير، والأرشفة، والحصول على تاريخ وتوقيت إجراء المعاملة "time-stamping".
- محيط التغطية: الاستخدام داخل الجهة أو موجه إلى الجمهور الخارجي.
- أسلوب التصنيع: يتم القيام به في داخل أو خارج الجهة.

1.3. مخطط البناء العام (التخطيط العام) PKI

يمكن أن تستند البنية التحتية للمفاتيح العامة "PKI" –في حال استخدام شبكة مفتوحة كشبكة الانترنت –على برتوكولات اتصال مختلفة، والتي تهدف إلى تأمين عمليات تبادل البيانات والمعلومات، ومن الممكن إرسال البيانات والمعلومات من خلال الاعتماد على تقنيات متخصصة في التشفير، وذلك عبر قناة مؤمنة باستخدام تقنيات (Virtual Private Network) VPN أو من خلال قناة اتصال (Hyper Text Transfer Protocol) مؤمنة عبر برتوكول SSL HTTPS.

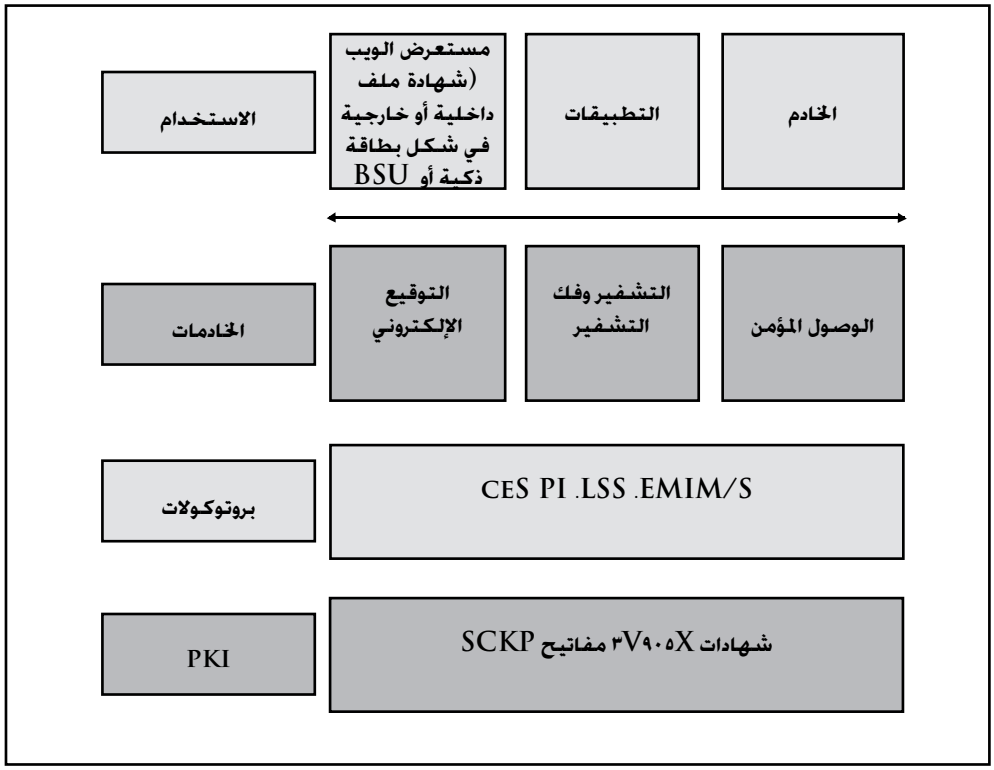
وتتوافر لدى "PKI" إمكانية الإمداد بشهادات أو تراخيص الكترونية، والسماح باستخدام تطبيقات التشفير التي تجرى على البيانات والمعلومات، وبالتالي ضمان خصوصية الرسائل البريدية الالكترونية عن طريق تشفيرها إلى جانب الاستعانة بشهادات الكترونية وامتدادات معدة خصيصاً لهذا الغرض في إطار برتوكولات البريد الالكتروني (S/MIME).

وتهدف "PKI" إلى إتاحة في متناول المستخدمين النهائيين ثلاثة فئات عريضة من الخدمات هي:

- التوقيع الالكتروني: من أجل ضمان التحقق من أصحاب الرسائل ووحدة واستقامة البيانات
- التشفير: ويهدف إلى تحقيق خصوصية البيانات والمعلومات
- التحكم في الوصول إلى البيانات والتطبيقات: وتستهدف تأمين أنظمة المعلومات.

وهناك خدمات تكميلية أخرى يمكن إضافتها مثل الأرشفة والحصول على تاريخ مؤكد في وقت إجراء المعاملة.

مخطط البناء التقني لـPKI



2.3. الشهادات الالكترونية

يتم عادة إعداد الشهادات الالكترونية في إطار البنية التحتية للمفاتيح العامة "PKI"، والتي تعتبر معادلة لبطاقات الهوية التقليدية أو تصريح المرور (Passport)، حيث أنها تستند إلى نفس المبادئ التي يمكن من خلالها إثبات هوية شخص أو وحدة (قسم) داخل مؤسسة ما. وتتضمن الشهادة الالكترونية -مثل بطاقة الهوية- معلومات تتعلق بصاحبها مثل (الاسم، واللقب، والعنوان، والتوقيع، والصلاحية...). ومن الضروري كذلك توافر إمكانية ضمان أن الشهادة ليست مزيفة وأنه تم اعتماد إصدارها من خلال سلطة أو هيئة مصرح لها بإصدار مثل هذه الشهادات، فمن المعروف أن تصريح المرور (Passport) يتم إصداره عبر مصلحة السفر والهجرة والجنسية، وبطاقات الهوية تقوم بإصدارها مصلحة السجل المدني، أما الشهادات الالكترونية

فتقوم بإصدارها جهة لها سلطات تحرير مثل هذه الشهادات. وتربط الشهادات بهوية المستخدم سواء كان شخص فيزيائي أو معنوي "هيئة" بزوج من المفاتيح (أحداها عام والأخر خاص) والتي تستخدم لتشفير وتوقيع المعلومات المتاحة في شكل الكتروني، وتسمح هذه الشهادات الالكترونية للمستخدمين والمؤسسات بإمكانية تأمين المعاملات المهنية والشخصية والتي يتم القيام بها عبر شبكات المعلومات.

ويمكن تمييز نوعين أساسيين من الشهادات الالكترونية هما الشهادة المتعلقة بالتشفير والشهادة الخاصة بالتوقيع، كما أن هناك العديد من الشهادات الحديثة التي يمكن أن تسمح في السنوات القليلة القادمة بإمكانية الانتقال من الإدارة المبسطة للهويات إلى إدارة أكثر تهيئة للوظائف والخدمات المتاحة وحقوق الوصول المرتبطة، ومن خصائص هذه الشهادات سماحها بإدارة الحقوق التقنية التي يمتلكها الأشخاص في نظام المعلومات، وهذه الفئة ليست متاحة بعد في الأسواق (حتى وقت إعداد هذه الدراسة) وبالتالي فإن المسألة المتعلقة بصفتها القانونية لم يتم البت فيها بعد.

وتجدر الإشارة إلى أن التقنيات المستخدمة في إطار "PKI" ليست ثابتة حيث أنها في تطور مستمر، ويوصي تقرير حول التوقيع الالكتروني صادر عن المفوضية الأوربية بضرورة تتبع التطورات التقنية وخاصة المعتمدة على تقنيات التأمين والمحافظة على الخصوصية.

1.2.3. الشهادات الشخصية وشهادات الخوادم

يتم عادة استخدام الشهادات الالكترونية بواسطة شخص فيزيائي أو معنوي، ويمكن التمييز بين شهادات الخوادم (Servers) والشهادات الشخصية. وتسمح شهادة الخادم بإمكانية التأكد من الجهاز الخادم الذي يتصل به المستخدم هو المطلوب الوصول إليه، وبالتالي يتحقق المستخدم بشكل مؤكد من خادم الجهة والذي يرغب من خلاله في تبادل البيانات المحمية بالتشفير، والتي تتم عادة عبر برتوكول "SSL" وهو البرتوكول الأكثر شيوعاً في بيئة الشبكة العنكبوتية، وهذا الأسلوب هو الأكثر استخداماً على شبكة الانترنت مع غالبية المعاملات التجارية. وعادة ما تستخدم الشهادات المتعلقة بسلطة تجارية تتمتع بالثقة في عمليات الدفع على الخط المباشر مثل (شراء تذاكر الطيران أو دفع الفواتير المختلفة....)، أو من خلال المعاملات البنكية مثل (الإطلاع على الرصيد والتعرف على أخر المعاملات التي تم القيام بها، وتحويل المال على الخط المباشر إلى حساب بنكي...)، وهذه الشهادات تكون مفهرسة ومرتبة من خلال مستعرض الويب المستخدم.

وعادة ما تتم عملية تشفير البيانات والمعلومات المتداولة من خلال منظومة شبكات الاتصال كما هو الحال في (البطاقة البنكية على سبيل المثال) بشكل غير مرئي (ملاحظ) من جانب المستخدم، حيث أنه من خلال شاشة مستعرض الويب المستخدم، عادة ما تتواجد أيقونة في شكل قفل مغلق، تبين للمستخدم أن العملية التي يقوم بها في الوقت الراهن تعتبر مؤمنة.

ويمكن وضع مستوي إضافي من التأمين موضع التنفيذ يتمثل في فرض ضرورة التعرف على هوية المستخدم القائم بالاتصال. ويجهز كل من جهاز الخادم "Server" والمستخدم بشهادة تصديق تخص كل طرف على حدا، وعند إجراء الاتصال، يطلب جهاز الخادم من المستخدم المتصل به التعريف بنفسه من خلال شهادة التصديق التي تخصه.

2.2.3. إنشاء الشهادات

تعتمد القيمة القانونية للشهادة على مدى دقة إجراءات التحكم التي تقوم بها السلطة التي تأخذ على عاتقها مسئولية إنشائها، ويمكن التمييز بين ثلاث مرتبات (فئات) للشهادات وذلك وفقاً لمستوى التحكم الذي يتم إجرائه:

المرتبة الأولى: يمكن الحصول على الشهادات التابعة لهذه الفئة عبر الخط المباشر، وهي لا تحتاج على فحص للهوية، والتحقق الوحيد يكون على البريد الالكتروني للمستخدم، وتتجرد هذه الفئة من الصفة القانونية، ويقتصر استخدامها على المستخدمين الراغبين في تشفير رسائلهم المتبادلة عبر شبكة الانترنت.

المرتبة الثانية: وفيها تخضع المعلومات مثل (عنوان السكن، والبريد الالكتروني.....) التي يتم الحصول عليها من خلال طالب الشهادة –وهو في هذه الحالة شخص فيزيائي فقط– إلى الفحص والتحقق من جانب السلطة المسئولة عن إصدار الشهادة، ويمكن أن يستند التحقق من الهوية على دليل خاص يحصر كافة العاملين والوكلاء المتعلقين بالمؤسسة مثل (Lightweight Directory Access Protocol) (LDAP).

المرتبة الثالثة: التحقق وفحص المعلومات المزودة من خلال طالب الشهادة (سواء كان فيزيائي أو معنوي)، يكون وجهاً لوجه، ويمكن أن يتم هذا التحكم في الهوية سواء من خلال السلطة أو الهيئة المسئولة عن الشهادة أو من خلال التفويض لسلطة التسجيل المتواجدة بالقرب من طالب الشهادة مثل أماكن العمل.....

3.2.3. استخدام الشهادات

يمكن أن تستخدم الشهادات في توقيع المستندات والرسائل والنصوص وتشفيرها إلى جانب التحكم في الوصول إلى التطبيقات المختلفة.

ويوضح الجدول التالي الخدمات التي تقدمها الشهادات واستخداماتها المختلفة:

الخدمة التأمينية	استخدام الشهادة
الخصوصية	تسمح الشهادات بتشفير وفك تشفير الرسائل
الاكتمال (وحدة البيانات)	توفر الشهادات إمكانية توقيع الرسائل، وضمان أن الرسالة المرسلة لم يحدث بها أي تلف أو تدخل في محتوياتها.
التحقق (التعرف على المستخدم)	يسمح استخدام الشهادات بتحديد هوية الشخص المرسل (فيزيائي أو معنوي) والتحكم في عملية الوصول إلى التطبيقات ومواقع الانترنت والشبكات الداخلية "stenartnI"...
عدم القدرة على النكران (عدم التنصل)	تسمح الشهادة بالتعرف على المشاركين في عملية تبادل المعلومات سواء كانوا (جهاز خادم، أو تطبيقات أو أشخاص)، كما أن المرسل لا يمكن إنكار إرسال الرسالة وكذلك المستقبل لا يمكنه إنكار استقبال الرسالة.

4.2.3. حفظ الشهادات وقائمة الإلغاءات

عادة ما تختزن وتحفظ الشهادات داخل أدلة من نوع LDAP (Lightweight Directory Access Protocol)، ويمكن الإطلاع على هذه الأدلة على الخط المباشر من أجل التعرف على المفاتيح العامة المتاحة داخل الشهادات، ويجب أن تكون الأدلة في مأمن من أي استعمال غير مرغوب، وذلك حتى يمكن تفادى تزوير الشهادة أو استخدام مفتاح عام مزيف.

ويمكن إلغاء الشهادة في أي وقت، وهذا التصرف من شأنه إلغاء كفالة سلطة التصديق على شهادة معينة، وذلك قبل نهاية فترة صلاحيتها. ويجب أن يتمكن أطراف الاتصال من الإطلاع المستمر على قائمة الشهادات الملغاة (Certificate Revocation List) CRL حتى يمكن تفادى استعمال الشهادات المنتهية الصلاحية.

وهناك تقنيات تعتمد على برتوكول (Online Certificate Status Protocol) OCSP والتي تسمح بتبسيط آليات التحديث المستمر لهذه القائمة. وجدير بالذكر أن إدارة قائمة الإلغاءات عبر التحديث المستمر لها وأساليب الإطلاع عليها تمثل تحدى استراتيجي تواجهه المؤسسة. كما تعتبر مسألة تحديث وإتاحة مثل هذه القوائم إحدى النقاط الحساسة المتعلقة بالبنية التحتية للمفاتيح العامة PKI. ويختلف حدث إلغاء الشهادة عن التجديد والذي يتمثل في إصدار شهادة جديدة لحاملها. وهذا الحدث يتم القيام به نتيجة لطلب من حامل الشهادة يعبر فيه عن رغبته في التجديد أو يتم بشكل تلقائي في نهاية فترة صلاحية الشهادة، وعادة ما تتراوح فترة صلاحية الشهادة من عام إلى ثلاثة أعوام. ويعتبر نشر الشهادات وقائمة الإلغاءات إحدى خدمات نشر "PKI". ويمكن القيام بعملية النشر والإعلان من خلال الاستعانة بعدة وسائل منها الدليل الالكتروني (الذي يمكن الوصول إليه عبر شبكة الانترنت العالمية أو من خلال الشبكة الداخلية)....

5.2.3. المعايير والمقاييس

تستند شهادات التوقيع والتشفير على مجموعة من التقنيات المعيارية الدولية، والشكل المتعارف عليه في الوقت الراهن للشهادات هو X509v3 (RFC2459)[3] ويهدف الاعتراف على المستوى الدولي بهذا المعيار و(Request for Comment) RFC المرتبطة، إلى السماح باستخدام بطاقات هوية الكترونية من جانب التطبيقات وبين الأقسام والوحدات المختلفة.

وعادة ما تأخذ الشهادة شكل ملف صغير الحجم نسبياً، يتضمن على أقل تقدير المعلومات التالية:

- أسم الهيئة المسئولة عن سلطة التصديق وهي التي تقوم بتحرير الشهادة
- الاسم واللقب المتعلقين بحامل الشهادة
- الجهة التابع لها المستخدم
- القسم الذي يعمل به المستخدم
- عنوان البريد الالكتروني الخاص بالمستخدم
- المفتاح الخاص المتعلق بالمستخدم
- تواريخ صلاحية الشهادة
- معلومات أخرى اختيارية مثل: طبيعة ومجال استخدام الشهادة مثل (التوقيع، والتشفير، والتحكم في الوصول.....)
- توقيع سلطة التصديق

6.2.3. وسائط حفظ الشهادات

يمكن حفظ الشهادة التي تأخذ شكل ملف بأساليب مختلفة، سواء بشكل مباشر من خلال التحميل على جهاز العميل وتسمى في هذه الحالة (شهادة برنامج)، أو حفظها على وسيط فيزيائي مثل مفتاح USB أو في شكل بطاقة ذكية.

شهادة برنامج: يقتضي استخدام شهادة من خلال جهاز العميل ضرورة تحميل برنامج معين للعمل مع كافة مستعرضات الويب المستخدمة (Internet explorer، ...Netscape، Firefox)، وهذه العملية يمكن أن تكون معقدة خاصة في حالة المستعرضات غير المتجانسة، حيث قد تحتاج كل إصدارة منها إلى عمليات ضبط أو إعداد من أجل تنصيب شهادة جديدة.

شهادة على مفتاح USB: تعتبر من التقنيات المنتشرة الاستخدام، وفي هذه الحالة يتعلق الأمر بمفتاح مشفر، يستخدم عادة مع برنامج يعمل كواجهة للتطبيق، ويتميز هذا الوسيط بسهولة استخدامه والحركة به، وتوافقه مع غالبية الحاسبات الآلية الحديثة المزودة بمنافذ USB.

شهادة البطاقة الذكية: يقتضي استخدام هذه البطاقات ضرورة تجهيز كل جهاز عمل"Work station" ببرنامج قارئ "Reader" لهذه البطاقة، ويرتبط كذلك ببرنامج عمل يستخدم كواجهة. ومن الضروري أن يتمكن هذا الوسيط من إجراء عملية الاتصال بطريقة بسيطة، وأن يكون قابل للنقل بشكل مريح دون أن يؤدى ذلك إلى تحمل تكلفة إضافية.

وتجدر الإشارة إلى أن الأسواق الأوربية سيطر عليها استخدام البطاقات الذكية، كما أن اختيار البطاقة الذكية كوسيط لإجراء المعاملات في محيط مؤسسات المعلومات قد فرض نفسه في المشروعات المتعلقة ببطاقات الهوية على سبيل المثال.

ومن أهم معايير اختيار الوسائط الفيزيائية:

- تكلفة الاقتناء
- تكلفة التشغيل
- تبسيط الإدارة
- تبسيط النشر والإتاحة
- قابلية وسيط التخزين للنقل والحركة

ويستعرض الجدول التالي وسائط تخزين الشهادات وأهم المميزات والعيوب المرتبطة بها ومستوى التأمين المتعلق:

الوسيط المختزنة عليه الشهادة	المميزات	العيوب	مستوى التامين
برنامج	البرنامج يتم تحميله بشكل مباشر على جهاز العمل الخاص بالمستخدم.	– عملية التحميل تختلف من برنامج مستعرض إلى مستعرض أخر – عدم التوافق بين بعض أنظمة التشغيل مثل (caM، أو xuniL...)، وإمكانية الاختلاف بين الإصدارات المتعددة لنظام التشغيل الواحد. – قدرة الوسيط على الحركة والانتقال تعتمد على جهاز المستخدم الذي يتم من خلاله أداء العمل.	متوسط
BSU	– القدرة على الحركة والانتقال – تيسير الاستخدام – منافذ BSU متاحة في كافة الحاسبات الآلية الحديثة	هذا الوسيط ما زال غير واسع الاستخدام من جانب المستخدمين غير المتخصصين في علوم الحاسبات الآلية.	فعال مع استخدام كلمة السر.
البطاقة	– وسيط معروف لمستخدمي (البطاقات البنكية على سبيل المثال) – وسيط يمكن تهيئته وفق سمات واهتمامات المستخدمين – وسيط عادة ما يستخدم في غالبية المشروعات	– ضرورة تحميل برنامج قارئ – تكلفة التجهيزات مرتفعة	فعال مع استخدام كلمة السر.

3.3. الكتابة المشفرة للمفتاح العام

تستند شهادات التوقيع الالكتروني على تقنيات التشفير للمفاتيح غير المتماثلة (اللامتناظرة)، وتسمح الشهادة الالكترونية بإنشاء رابطة بين المفتاح العام من ناحية والبيانات الدالة على الهوية من ناحية أخرى، الأمر الذي من نتائجه المباشرة تفادى استخدام أي شخص لمفتاح بهدف انتحال هوية شخص أخر.
وتعتبر مفاتيح التشفير أساس أنظمة التشفير الحالية، ويضمن امتداد وطول المفاتيح [4] والأسلوب المتبع في إنشائها إلى حد كبير تأمين أنظمة التشفير أو الترميز. ويستند عامل الثقة على الافتراض بأن عملية التشفير المستخدمة لا يمكن كسرها (فكها) في وقت قصير خاصة مع الإمكانيات والتقنيات المتاحة في منظومة الحاسبات الآلية. وهناك منهجان في الكتابة المشفرة غالباً ما يتم الاستناد إلى استخدام أحدهما وهما:
أولاً المنهج المعتمد على المفتاح التماثلي (التناظري) والذي يستند إلى مفتاح وأحد خاص فقط
ثانياً المنهج غير التماثلي (اللامتناظر) والذي تم إنشائه في عام 1976 والذي يعتمد على نظام ثنائي للمفاتيح أحداها عام والأخر خاص.

1.3.3. التشفير التماثلي (التناظري)

يستند الإجراء التناظري على مفتاح سرى وأحد فريد (لا نظير له) يستخدم في كل من معاملات التشفير وفك التشفير، وبالتالي يجب في هذه الحالة مشاركة الكود السري المرتبط بالمفتاح الخاص بين

المستخدمين ممثلي طرفي الاتصال (المرسل والمستقبل). وهذا القصور المرتبط بمشاركة الكود بين المتصلين عن بُعد، يمكن تخفيفه من خلال سرعة تنفيذ إجراءات التشفير وفك التشفير بين الحاسبات الآلية. ويمكن استخدام هذا النوع من المفاتيح مع برتوكول SSL(5) على سبيل المثال، وبذلك فهو يتعلق بمفتاح يتم استخدامه في فترة الاتصال. ولا يستخدم هذا المسلك في التشفير في منظومة التوقيع الالكتروني لوجود مخاطر نتيجة اعتماده على مفتاح واحد فقط، حيث من الممكن التقاطه أثناء عملية التراسل (الاتصال) من جانب أشخاص غير مرغوبين.

2.3.3. التشفير غير التماثلي (اللامتناظر)

وفيه تستند منظومة التوقيع الالكتروني على نظام للتشفير أكثر أماناً ولكنه أكثر تعقيداً، حيث يعتمد التشفير غير التماثلي على إصدار مفتاحين متكاملين ومرتبطين بشكل مُحكم، وهما مفتاح خاص (معروف فقط من جانب المالك الشرعي للشهادة) ومفتاح عام (معروف للمستخدمين الذين يتم معهم إجراء التراسل).

وتسمح هذه المفاتيح بإمكانية التوقيع الالكتروني وتشفير النصوص بهدف ضمان الخصوصية والتأمين، ويمكن لهاتين العملتين أن يرتبطوا معاً في أثناء تبادل المعلومات التي تستلزم مستوى رفيع من التأمين والخصوصية.

وغالباً ما يتم تطبيق التشفير من خلال مفتاح خاص وأخر عام في إطار العمل البنكي (البنوك)، حيث ينفذ مستخدم البطاقة البنكية (مثل فيزا كارت)، -دون أن يشعر- عملية تشفير غير تماثلي وذلك عند إجراء معاملة مالية -على سبيل المثال- بواسطة بطاقته من خلال إحدى الطرفيات المتصلة بشبكة بنكية، حيث يقوم المستخدم بالتصديق على هويته من خلال الكود الشخصي السري الخاص به، والتوقيع الخاص المتاح على البطاقة (المفتاح العام) وذلك لضمان التأكد من أن مستخدم البطاقة هو نفسه المالك الشرعي لها، وتتم هذه الإجراءات على الخط المباشر دون أن يلاحظ المستخدم مستوى التعقيد المتعلق بها.

وفي حالة تشفير المعلومات مباشرة على شبكة الانترنت العالمية، يكون مستوى الشفافية متماثل بالنسبة للمستخدم، حيث أن هذه العملية لا يشعر بها المستخدم وبالتالي، بمجرد الضغط بالفارة (الماوس) على الأيقونة المناسبة يتم السماح له بتوقيع وتشفير المعلومات الخاصة به. وعملية التشفير والتوقيع تتم من خلال عدة مراحل تحدث بين صاحب (مرسل) المستند والجهة المرسل إليها بطريقة شفافة أي بدون أن يشعر بها الأطراف المشاركة في عملية التراسل.

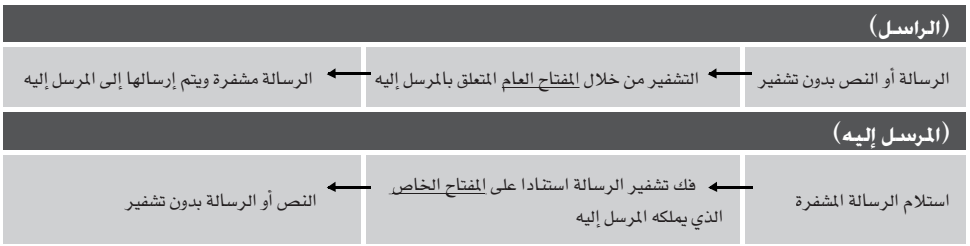
3.3.3. التشفير من خلال المفتاح العام

يستخدم أي شخص راغب في إرسال رسالة مشفرة المفتاح العام للشخص المرسل إليه وذلك من أجل تشفير محتوى رسالته، وبناء عليه فإن المفتاح الخاص المرتبط بالمفتاح العام (الذي تم استخدمه في تشفير الرسالة) هو بمفردة القادر على فك تشفير هذه الرسالة، والشخص المرسل إليه وهو المالك الشرعي للمفتاح الخاص هو الذي في مقدوره فك تشفير محتوى الرسالة.

والمسائل المرتبطة بالتأمين والقوانين المتعلقة بهذا المفتاح الخاص عادة ما توضع عند طرف أخر

يحظى بالثقة، والذي يمكنه إذا دعت الحاجة إمكانية إعادة اتصال مفتاح التشفير، مثل في حالة فقده على سبيل المثال.

شكل توضيحي لإجراءات التشفير



4.3.3. التوقيع الالكتروني من خلال المفتاح الخاص

كما سبقت الإشارة إلى أن التوقيع الالكتروني يجب أن يسمح بإمكانية التحقق من المرسل والتأكيد على وحدة واكتمال الرسالة المرسلة، وضمان مثل هذه الوظيفة يمكن أن يتم من خلال المفتاح الخاص، الذي يكون في مثل هذه الحالة، محفوظ مع مالكة الشرعي فقط، وفي حالة فقدانه يجب إنشاء وتحرير شهادة توقيع جديدة.

ويرتكز التوقيع الالكتروني على وظيفة تسمي (hachage) والتي تتألف من إنشاء "بصمة أو ختم أو علامة" قد تكون في شكل صورة مصغرة أو مبسطة للمستند، والتي تسمح بضمان عدم حدوث أي تعديل في المستند إلى جانب تطبيق تشفير غير تماثلي.

شكل توضيحي لإجراء التوقيع

وجدير بالذكر أن التطابق الحاسم للمستند الموقع والعلامتين يمثل الإثبات على:

- اكتمال ووحدة الرسالة قد تم الالتزام بها: حيث أن المستند لم يطرأ عليه أي تعديل، كما يؤخذ بعين الاعتبار أن العلامة (الوشم) الأصلية متطابقة تماماً مع العلامة المتعلقة بالمستند المرسل.
- الخصوصية: تتم المحافظة على خصوصية البيانات والمعلومات أثناء التبادل من خلال الاستعانة بتطبيقات التشفير مثل برتوكولات التبادل المؤمن أو تشفير الرسالة نفسها.

- عدم النكران (عدم التنصل): وهي تضمن أن المرسل لا يمكنه إنكار إرسال رسالته، كما أن المرسل إليه لا يمكنه نكران استلام الرسالة.
- التحقق أو التوثيق: يمكن أن يتم التحقق من التوقيع على الرسالة من خلال استخدام المفتاح الخاص، كما إنه في حالة تشفير محتوى الرسالة، فمن الممكن كذلك ضمان التحقق من المرسل إليه.

4.3. الأطراف المشاركة في البنية التحتية للمفاتيح العامة PKI.

يفترض تطبيق البنية التحتية للمفاتيح العامة (Public Key Infrastructure) PKI ضرورة تداخل مجموعة من الأطراف ويضطلع كل طرف بأداء وظيفة محددة، وأهم هذه الأطراف هي:

السلطة الإدارية: وهي الهيئة التي تأخذ على عاتقها مسئولية القيام بالمهام المتعلقة بالتأمين، والتي تضاف إلى مجموعة الوظائف المتعلقة بالإدارة، وتتمتع السلطة الإدارية بسلطة اتخاذ القرارات فيما يتعلق "PKI".

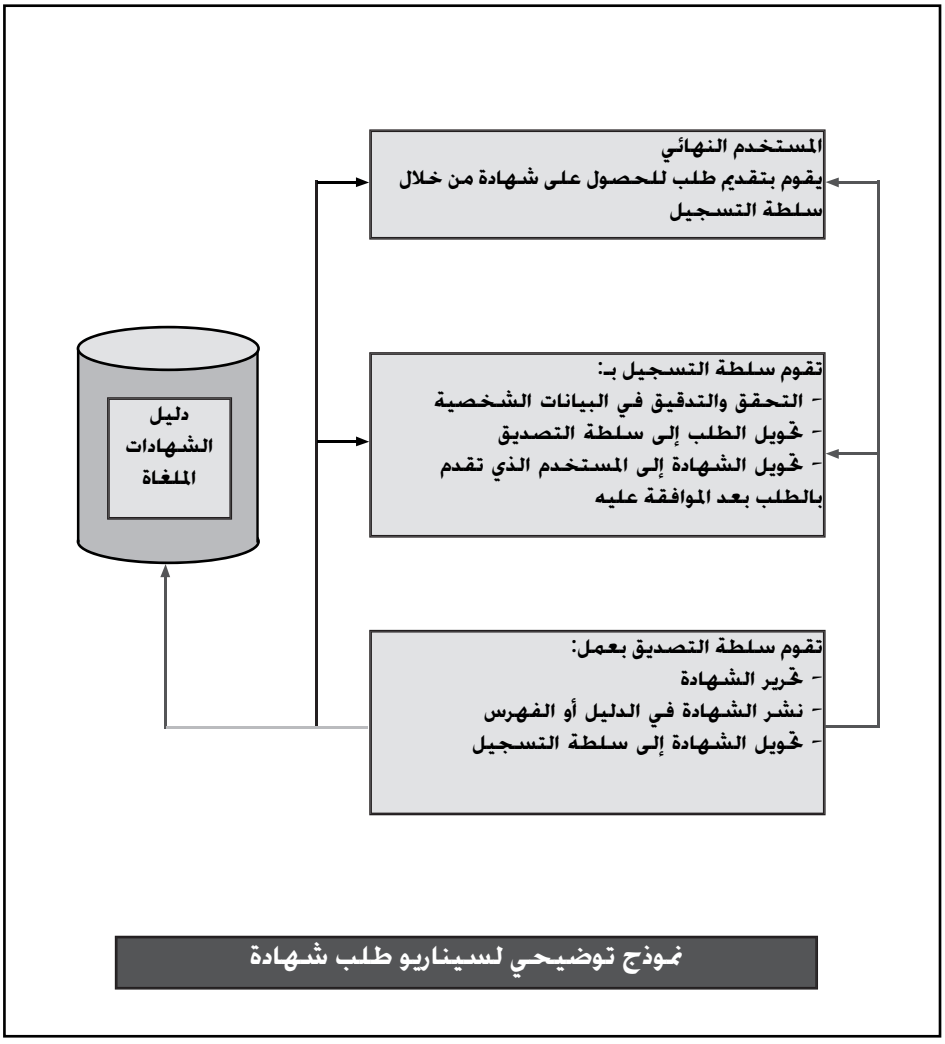
سلطة التصديق: تقوم هذه السلطة بإنشاء المفاتيح وتحرير الشهادة المرتبطة بها، وتوقيعها مع المفتاح الخاص المتعلق بها، الأمر الذي من شأنه ضمان شهادة صحيحة. وعملية التسليم تقع مسئوليتها الفنية والقانونية على عائق هذه السلطة. كما تقوم بإدارة قائمة الشهادات الملغاة، واختزان المفتاح العام المتعلق بالمستخدمين المرتبطين بها، ويمكنها كذلك أن تفوض في التحقق من هوية طالبي الحصول على شهادات إلى جهة قريبة من المستخدمين يطلق عليها "سلطة التسجيل". ومن الممكن تسليم الشهادة على الخط المباشر، وهنا يتم تحميلها مباشرة على الحاسب الآلي الخاص بالمستخدم، كما يمكن أن تكون الشهادة محملة على قرص مليزر أو قرص ممغنط أو "USB" أو على بطاقة ذكية، ويتم تسليمها "وجهاً لوجه" للمستخدم. كما يمكن أن تشير الهيئة المسئولة عن التوثيق والتصديق على الشهادة إلى هيئة التوثيق الأصلية والتي تعتبر مرجع يتضمن كافة سلطات التصديق الأخرى.

سلطة التسجيل: تعمل على استقبال طلبات الحصول على شهادات، وتقوم بعملية الجمع والتحكم في بيانات الهوية الضرورية، حيث تستقبل طلبات الشهادات وتدقق في هوية الطالبين وذلك قبل توجيه هذه الطلبات إلى سلطة التصديق، ويمكن أن يقع على عائق هذه السلطة مسئولية إرسال الشهادة إلى طالبيها، وهي تعتبر مكون اختياري من مكونات "PKI".

مسئول التشغيل: وهو المسئول عن التشغيل وعمل الاعدادات وعمليات الضبط اللازمة والصيانة التقنية لمكونات "PKI"، كما يضمن إدارة النظام والشبكة داخل هذه المكونات.

المستخدم النهائي: وقد يكون شخص فيزيائي أو معنوي (هيئة) أو مكون مادي (تطبيقات، أجهزة خوادم "Servers"....) وهو يحتفظ بشهادة ذات مفتاح عام تم تسلمها من خلال سلطة التصديق أو سلطة التسجيل. وعندما يتقدم المستخدم بطلب للحصول على شهادة يطلق عليه "طالب الشهادة"، ويطلق عليه "حامل الشهادة" في الوقت الذي يحصل فيه على الشهادة.

نموذج توضيحي لسيناريو طلب شهادة



نموذج توضيحي لسيناريو طلب شهادة

5.3. سياسة التصديق

تضطلع سياسة التصديق أو التوثيق بوصف كافة القواعد التي تحكم الإجراءات التي يتم القيام بها، بداية من طلب الحصول على شهادة وصولاً بتحرير وتسليم الشهادة واستخدامها وإدارتها. وتختلف إدارة الشهادات وبالتالي سياسة التصديق وفقاً لطبيعة ومستوى الحماية المطلوب تطبيقها على المعلومات التي يتم معالجاتها. ويمكن تصنيف سياسات التوثيق إلى ثلاثة مستويات من المعلومات وهي معلومات ليست حساسة، وحساسة، وشديدة الحساسية، ووفقاً لحاجتين هما التحقق والتوثيق من ناحية والخصوصية من ناحية أخرى.

ومن الضروري أن تقوم سلطة التصديق بتحرير سياسة التصديق في شكل مستند يتضمن ممارسات التصديق التي توضع موضع التنفيذ، وذلك من أجل إصدار وإدارة الشهادات، ويجب أن يحظى هذا المستند بالقبول والتصديق من جانب لجنة التوجيه والإرشاد مثل سياسة التصديق.

وبالتالي تقوم سياسة التصديق بوصف كافة الأبعاد الفنية والتكنولوجية والتنظيمية المتعلقة بشهادة معينة، وذلك بهدف ضمان مستوى مناسب من الثقة. وأحد الأبعاد المركزية لهذه السياسة يتعلق بمستوى الحماية المطبق على المفاتيح الخاصة.

وتعيين سياسة للتصديق، يمكن أن يسمح لوحدتين أو قسمين أو جهتين بعمل معايير مشتركة تضمن إمكانية التفاعل والتعرف المتبادل على الشهادات والعمل المشترك على "PKI" الخاص بهم.

6.3. خدمات إضافية

يمكن أن تتيح "PKI" سلسلة من الخدمات التكميلية لمنظومة التوقيع الالكتروني منها تقنية يطلق عليها time-stamping، إلى جانب خدمة الأرشفة.

1.6.3. تسجيل الوقت time-stamping

يكمن الهدف الرئيسي من جهاز خادم "time-stamping" في إمكانية تسجيل الوقت والتاريخ الذي يتم فيه إجراء المعاملة على المستند الالكتروني وذلك بشكل لا يمكن تزويره.

وتتوافر العديد من التطبيقات التجارية التي تتضمن إمكانية السماح بإيداع موجز للمستندات الموقعة، وذلك في حال عدم رغبة الجهة المعتمدة في تبادل المستند الأصلي نفسه، والتي تحتفظ ببصمته مع تاريخ ووقت الإيداع. ويكمن الدور المنوط بجهاز خادم "time-stamping" في تسجيل على المستند الالكتروني تاريخ مؤكد لا يمكن تعديله أو تزويره، وذلك من خلال خادم واحد فريد ولا نظير له.

وهذه الوظيفة لا غنى عنها في ميكنة الإجراءات التي تختص بالإحالة إلى تاريخ محدد مثل تاريخ (الرد على عروض معينة مثل المناقصات، تاريخ الإقرارات الضريبية...)

2.6.3. الأرشفة

تمثل أرشفة التوقيع الالكتروني جانب هام في سلسلة تحقيق الخصوصية والثقة، ومن الضرورى الاحتفاظ بالتوقيع الالكتروني لغايات وأهداف إدارية وإثبات حقوق المستخدمين. وتقتضي بعض حالات الخلاف ضرورة إجراء فحص لعدة سنوات راجعة للتعرف على الصلاحية القانونية ومدى سريان فاعلية توقيع معين.

وتواجه الأرشفة على المدى الطويل تحدى تكنولوجي يتمثل في مواجهة التطور التقني المستمر، حيث من الضروري في كثير من الأحيان أرشفة مجموعات كبيرة من البيانات والمعلومات المتعلقة بالتصديق والتوثيق، وتتنوع الفترة القانونية لأرشفة المستندات (من 5 إلى 35 عامً فأكثر) وذلك وفقاً لطبيعتها، وبالإضافة إلى ذلك يجب الاعتناء بحماية واستمرارية التوقيع الالكتروني، وذلك من خلال ضمان نقله –تحويله– على وسائط تخزين أكثر حداثة في حال حدوث تطور تكنولوجي هام.

وعلى الرغم من قيام العديد من المؤسسات بجهود في مجال المعايير والمقاييس الأرشيفية والتي تتعلق على باكتمال ووحدة البيانات وصلاحية المستندات التي يتم أرشفتها، فالأرشيف الالكتروني لا يحظى دائماً باتفاق جميع الآراء من بين متلقي خدمة التصديق.

ويجب أن يتم دراسة احتياجات الأرشفة بدقة من (حجم البيانات، فترة الحفظ والاختزان)، وذلك بهدف تخفيض التكاليف، فعلى سبيل المثال يتم الاحتفاظ بالإقرارات الضريبية في فرنسا لمدة خمس سنوات، ويتم قصر المعلومات التي يتم أرشفتها على البيانات المتعلقة بالإقرار فقط، الأمر الذي من شأنه السماح بخفض وتقليل حجم البيانات التي يتم أرشفتها. وهذه الأرشفة يتم استكمالها بأداة تسمح في حالة الضرورة بإعادة تشكيل الاستمارة بالشكل الذي وقعة وقام بملئه القائم بالإقرار.

7.3. أسلوب إدارة البنية التحتية للمفاتيح العامة PKI

يعتبر"PKI" ليغشتو ڤيبطة أمر معقد، حيث يتطلب كفاءات وقدرات تكنولوجيه عالية إلى جانب تنظيم وبناء يتسم بالهيكلية. وهناك عادة خياران للجهات سواء كان بناء وتطوير "PKI" داخلي (أي داخل الجهة) بشكل كامل أو جزئي والخيار الأخر يتعلق بتبني تطوير PKI من الخارج بشكل كامل (أي خارج الجهة)

1.7.3. البناء الداخلي (الاستدخال)

يمكن أن يلبى اختيار تبنى وتطوير "PKI" داخل الجهة بعض الاحتياجات المتعلقة بتأمين نظام المعلومات إلى جانب نشاطات البحث العلمي.

وإذا كان محيط "PKI" يتقيد فقط بالنشاطات الممارسة داخل الجهة، فإنها (الجهة) تحتاج إلى تنظيم داخلي معياري. ويفرض هذا الاتجاه تحديات تتعلق بكيفية اختيار التنظيم الهيكلي والكفاءات التكنولوجية والقانونية اللازمة.

وبناء عليه يمكن تحقيق عملية استدخال "PKI" بشكل كامل من خلال الاستعانة بمجموعات داخلية من المتخصصين الذين يعكفون على تطوير برمجيات الصيانة الخاصة بـ"PKI". كما يمكن أن تتم عملية الاستدخال بشكل جزئي من خلال اللجوء إلى "PKI" من خلال العروض التجارية سواء كانت تجهيزات مادية أو برمجيات، ويمكن الاستعانة بمضيف خارجي يحظى بالثقة والأمان (مضيفو PKI).

ويستخدم هذا النمط من جانب المركز الوطني الفرنسي للبحوث العلمية "CNRS" والذي يشرع على تطوير برنامج "PKI" خاص به. ومن الأمثلة الأخرى، ما تقوم به وزارة التعليم الوطني الفرنسية، حيث تعمل على وضع موضع التنفيذ "PKI" خاص بها، مستهدفة من وراء ذلك تحرير ومن ثم تسليم شهادات (تصاريح) داخلية إلى جميع الهيئة العاملة بها، كما تبنت وزارة الزراعة الفرنسية تطبيق نفس الاتجاه.

وبمجرد تدشين وتنصيب "PKI" داخل جهة ما، من الضروري أخذ كافة التدابير لضمان التشغيل الجيد، وخاصة تلك المتعلقة بصيانة التجهيزات المادية والبرمجيات، إلى جانب توافر الإمكانيات اللازمة لإدارة البنية التحتية تقنياً من خلال إدارة ما يطرأ من تطورات والإشراف والتخزين والتامين، وأخيراً تمثل عملية استخدام الشهادات من جانب المستخدمين ومطوري التطبيقات أمراً لا غنى عنه وذلك لتوثيق "PKI".

وأصبحت عملية اختيار تأمين النظام من خلال مراقبين عملية أساسية، وذلك لأن سياسة التأمين الخاصة بجهة ما تتضح ملامحها من خلال "PKI" المستخدم والذي تم اختياره أو تطويره.

2.7.3. اللجوء الخارجي من خلال الجهات المعتمدة

يتم في هذه الحالة إدارة المفاتيح المرتبطة بالشهادات من خلال طرف يحظى بالثقة يطلق عليه بشكل عام شريك في خدمة التصديق. وتحتفظ هنا الجهة بمسئوليتها نحو تحميل الشهادات في نظام المعلومات الخاص بها. وتتفاوت التكاليف المرتبطة بهذا الاتجاه وفقاً للبنية المطلوبة من حيث مستوى التأمين والإتاحة ومستوى جودة الخدمات وطبيعتها إلى جانب أعداد المستخدمين المتوقع.

وعادة ما يتم تحديد نمط إدارة الشهادات من (تسجيل، إلغاء، تجديد) في ضوء سياسة التصديق التي تتبعها الجهة، الأمر الذي يمكن أن ينبثق عنه تكاليف إضافية وذلك إذا كانت تلزم سلطة التسجيل ضرورة التعرف على هوية المستخدم وجهاً لوجه من أجل تحرير ومن ثم تسليم الشهادة.

ونلاحظ أن الحاجة إلى تقديم خدمات الأرشفة والتوقيع المؤمن وتسجيل الوقت والتاريخ التي يتم فيه إجراء المعاملة في غالبية الجهات ما زالت مقتصرة على فئات محددة من المستخدمين كذلك مقيدة ببعض الإجراءات الإدارية التي يمكن أن تتم عن بُعد.

ويعتمد الاختيار بين استدخال "PKI" داخل الجهة سواء بشكل كلى أو جزئي أو اللجوء الخارجي إلى "PKI" من خلال جهات معتمدة تحظى بالقبول، على المهارات والكفاءات المتاحة داخل الجهة والمتخصصة في تقنيات "PKI" والمحيط الخاص بها من خدمات وعدد المستخدمين..... بالإضافة إلى مدى تنوع وتعدد احتياجات ميكنة الإجراءات المتعلقة بالإدارات، حيث من الممكن أن يقود ذلك إلى الاستعانة بأكثر من "PKI" والتي يمكن أن تغطى بيئات ومحاور مختلفة واستخدام داخل الجهة وخارجها.

4. الخاتمة

يقع تطوير مؤسسات المعلومات في الوقت الراهن في مفترق طرق، حيث تتألف المرحلة الحالية من استغلال لكافة الخبرات والتجارب المكتسبة، واستشراف تصور لخدمات جديدة معدة وفقاً للسمات الشخصية ومقدمة عبر منظومة شبكات المعلومات والاتصالات، والتي تعطى مرونة في أسلوب العمل. ويمكن إتاحة الخدمات المتاحة عبر الخط المباشر، والمتأقلمة مع مختلف فئات العاملين من خلال نشر إدارة الهوية الالكترونية المتعلقة بالعاملين، ويلعب "PKI" دور جوهري في بناء مثل هذه الشهادة الالكترونية.

ويجب أن يستند انتشار مثل هذه التكنولوجيات على استخدامات محددة للخدمات المميكنة. ويسمح تطبيق التوقيع الالكتروني في إطار التطبيقات المهنية المتنوعة بإمكانية التطبيق المتنامي والقابل للبقاء لهذه التقنية. وذلك يكون له تأثير مباشر على نظام المعلومات المستخدم، حيث أن الشهادات يمكن أن ينتشر استخدامها على مجموعات واسعة من التطبيقات وخدمات الشبكة العنكبوتية وكذلك على مجموعات من العاملين والوكلاء.

وهذا الاتجاه المتنامي، والذي يعتمد على إجراءات إدارية الكترونية، تؤدي إلى التعايش بين العديد من "PKI"، وبالتالي يتم تحرير وتوزيع العديد من الشهادات المختلفة على المستخدمين، وحينما يتعلق الأمر بالإجراءات الإدارية التي تدير المعاملات خارج المركز أو الجهة مع وجود تحدى يرتبط بإدارة الهوية والإثبات أو إدارة الإجراءات الداخلية.

وتهيئة وإعداد البنية التحتية للمفاتيح العامة من أجل التوقيع الالكتروني، يمكن اعتباره مرحلة لا غنى عنها للإجابة على استفسارات ترتبط جميعها بالتطبيقات التي يمكن الوصول إليها عبر الشبكة العالمية مثل تأمين التبادل والمعاملات، والتعرف على هوية المستخدمين، وتوقيع المستندات، والخصوصية ووحدة البيانات واكتمالها، وتسجيل تواريخ وأوقات المعاملات إلى جانب حفظ وتخزين المستندات الالكترونية، وذلك من شأنه إتاحة خدمات أخرى يمكن استخدامها من خلال أدوات إضافية مثل: أدلة إدارة الهوية الالكترونية، وأدلة إدارة الحقوق، وشهادات التشفير، والأرشفة، وتقنيات تسجيل أوقات وتواريخ المعاملة الالكترونية.

المراجع

دراسات وتقارير

1. Document de travail sur les plates-formes informatiques de confiance. Commission
européenne, Groupe de travail protection des données. 23 janvier 2004.
http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2004/wpdocs04_fr.htm

2. L'administration électronique au CNRS : recommandations pour la mise en œuvre de téléprocédures. Laurence LOMME. CNRS, Secrétariat général, Bureau de pilotage et de coordination. Décembre 2003.

La signature électronique. Julien ESNAULT. Mémoire de DESS de droit du .*3* multimédia et de l'informatique. 2003-2004 http://www.signelec.com/content/download/memoire/memoire_la_signature_electronique_%20julien_esnault.PDF

Mettre en œuvre les téléprocédures dans la juridiction administrative. Thierry .*4* SOMA. Novembre 2003. http://www.conseil-etat.fr/ce/rappor/intro__teleproced.htm

Rapport du groupe de travail sur les cartes d'achat et la dématérialisation des .5 factures. Mission économie numérique, Ministère de l'économie, des finances et de l'industrie. Mai 2003. http://www.men.minefi.gouv.fr/webmen/informations/pdf/rapportv218303.pdf

6. Rapport 2003 du groupe de travail 7 de la Mission pour l'économie numérique : dématérialisation de l'achat public. Mission économie numérique, Ministère de l'économie, des finances et de l'industrie. Octobre 2003.
http://www.men.minefi.gouv.fr/webmen/groupetravail/g7/rapport2003.pdf

Rapport sur le projet de loi de finances pour 2004. Bernard CARAYON. 22 octobre .*7* 2003 http://www.assemblee-nationale.fr/12/budget/plf2004/b1110-36.asp

8. Recommandations pour la gestion de l'authentification-autorisation-SSO (AAS). Ministère de la jeunesse, de l'éducation nationale et de la recherche. 10 septembre 2003 http://www.educnet.education.fr/chrgt/AAS-V10.pdf

9. Sécurité juridique des téléprocédures Mission économie numérique, Ministère de l'économie, des finances et de l'industrie: rapport final. 2002
http://www.men.minefi.gouv.fr/webmen/groupetravail/g6/rapportfinal.pdf

10. Situation de l'achat électronique public en France et en Europe. Mission économie numérique, Ministère de l'économie, des finances et de l'industrie. Juin 2003.
http://www.men.minefi.gouv.fr/webmen/groupetravail/g7/rapport72.pdf

11. The Legal and Market Aspects of Electronic Signatures. Study for the European Commission DG Information society. European Commission. October 2003.
http://europa.eu.int/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf

دوريات ومقالات

Authentification par certificats : l'importance du gestionnaire de profils. Roland .*1* Dirlewanger. CNRS. Novembre 2003. http://2003.jres.org/actes/paper.128.pdf

2. Construire une architecture PKI. Réseaux & Télécoms. AGIR du n°196.
http://www.reseaux-telecoms.com/articles_btree/DP_196/Article_view

3. De l'authentification à la biométrie. Joseph ILLAND ; Caline VILLACRES ; Philippe WOLF Sécurité informatique. N° 46, Octobre 2003.
http://www.cnrs.fr/Infosecu/num46-sansFond.pdf

4. FAQ IGC/A v1.1. Direction centrale de la sécurité des systèmes d'information, Secrétariat général de la défense nationale. 2002.
http://www.adae.pm.gouv.fr/upload/documents/20030306_IGC_FAQv1_1.pdf

Faut-il brûler vos certificats ? Serge AUMONT. Comité réseau des universités .*5* (CRU). Novembre 2003. http://2003.jres.org/ACTES/8_infrastructures_gestion_cle/paper.21.pdf

6. La facturation électronique, ou la révolution tranquille de la signature électronique par l'administration fiscale. Isabelle RENARD. Octobre 2003.
http://solutions.journaldunet.com/0310/031008_juridique.shtml

Le cadre juridique de la certification. Blandine POIDEVIN. Avocat au Barreau de .*7* Lille. http://www.juriscom.net/pro/2/ce20020901.pdf

Le Livre Blanc : Architecture de Systèmes d'Information. Octo Technologies. .*8* Novembre 2002. http://www.octo.com/fr/techno/wp_archi.html

9. Le régime de l'acte administratif face à l'électronique. Gérard MARCOU. Communication au Colloque Université Paris 1 ; Conseil d'Etat, *L'administration électronique au service des citoyens*, 21 et 22 janvier 2002.
Liste de liens sur les certificats électroniques. Comité réseau des universités (CRU). http://www.cru.fr/igc/

10. Signature électronique. Direction centrale de la sécurité des systèmes d'information, Secrétariat général de la défense nationale. Avril 2003.
www.ssi.gouv.fr/fr/sigelec/sigmemento.pdf

11. Signature électronique : comment s'y retrouver entre les textes européens et français? Isabelle RENARD. Mars 2002.
http://www.journaldunet.com/juridique/juridique020305.shtml

Textes de loi relatifs à la signature électronique. Florent GUILLEUX. Comité .*12* réseau des universités (CRU). 2003. https://pki.cru.fr/signature_electronique.pdf

Plan stratégique pour l'administration électronique (PSAE) pour la période .13 2004-2007. ADAE. http://www.adae.gouv.fr/adele/

Plan REpublique numérique dans la SOciété de l'information (RESO), présenté .*14* par le Premier ministre. 12 novembre 2002 http://www.internet.gouv.fr/rubrique.php3?id_rubrique=61

15. Politique de Référencement Intersectorielle - PRI - v1. ADAE ; Septembre 2003.
http://www.adae.gouv.fr/article.php3?id_article=220&var_recherche=PRI

16. Contrat d'action pluriannuel CNRS-Etat 2002-2005. 21 mars 2005
http://www2.cnrs.fr/sites/band/fichier/3f1d5636c99a3.htm

17. Systèmes d'information : schéma directeur 2001-2006. CNRS, Secrétariat général, Direction des systèmes d'information. Avril 2001.

الهوامش

(1) Brussels, 20th November 2003 Commission welcomes agreement of Council and Parliament to set up the European Network and Information Security Agency http://europa.eu/rapid/pressReleasesAction.do?reference=IP/03/1577&format=HTML&aged=٠&language=en&guiLanguage=en

(2) لمزيد من المعلومات يمكن الاتصال بالموقع التالي http://www.oecd.org

(3) لمزيد من المعلومات يمكن الإطلاع على الرابط التالي: http://www.ietf.org/rfc/rfc2459.txt

(4) في إطار التشريع الفرنسي على سبيل المثال يبلغ 1024 Bits فيما يتعلق بالمفاتيح غير المتماثلة (اللاتناظرية) و128 Bits للمفاتيح المتناظرة أو المتماثلة.

(5) SSL : Secure Socket Layer:
برتوكول يسمح بتشفير البيانات المرسلة من خلال مستعرضات الويب، وقد من تطويره من خلال مؤسسة Netscape