البنية التحتية للمفاتيح العامة

مقدمة

المركز الوطني للتصديق الرقمي

برنامج الحكومة الإلكترونية

وزارة الاتصالات وتقنية المعلومات

المملكة العربية السعودية

ربيع أول ١٤٢٦ هـ

المحتويات

ملخص تنفيذي

تشكل البنية التحتية للمفاتيح العامة منظومة أمنية متكاملة لإدارة المفاتيح الرقمية المستخدمة في الحفاظ على سرية المعلومات، والتثبت من هوية المتعاملين، والحفاظ على سلامة البيانات من العبث والتغيير، والقيام بإجراء التوقيعات الإلكترونية.

ولتحقيق الاستفادة المثلى من التطبيقات والخدمات المتعددة للبنية التحتية للمفاتيح العامة (Public-Key Infrastructure-PKI)، ولبناء بنية أمنية متينة ومتطورة، يجب أن تكون هناك دراسة دقيقة لاحتياجات القطاعين العام والخاص في المملكة من خدمات البنية التحتية للمفاتيح العامة. وتعتبر هذه البنية القاعدة الأساسية التي تُبنى عليها الأعمال الإلكترونية، كالحكومة الإلكترونية والتجارة الإلكترونية، وغيرها من التطبيقات الإلكترونية الشبكية، إذ تمكّن هذه البنية الأمنية المتعاملين عن طريق شبكة الإنترنت من إجراء الأعمال والعمليات الإلكترونية بأمن وموثوقية وسلامة عالية.

هناك عدد من القضايا والأمور ذات العلاقة بهذه البنية الأمنية بحاجة إلى البحث والتحليل ومن ثم اتخاذ قرارات أساسية بشأنها، وهي ذات أثر كبير على طريقة تقديم الخدمة وإصدار الشهادات الرقمية وإدارتها والاستفادة من التوقيعات الإلكترونية وتشفير البيانات وغيرها من الخدمات. وتصب جميع تلك القرارات الإستراتيجية المطلوبة في المحاور التالية:

- **الأهداف ومتطلبات الاستخدام**: ما الأهداف العامة للبنية التحتية؟ وما شروط تحقيق هذه الأهداف؟ على سبيل المثال، إن كانت هناك حاجة للتحقق القاطع من هوية المستخدم، أو ما يعرف بـ (Strong Authentication)، فيجب تطبيق أساليب معينة كالبصمة وغيرها لتحقيق ذلك.

- **الهيكل**: ما العناصر المكونة للبنية التحتية؟ وكيف يتم الارتباط بينها؟

- **النطاق**: ما المجالات التي تغطيها البنية التحتية للمفاتيح العامة؟ وكم عدد الجهات المشمولة بها؟ وما مدى التغطية الجغرافية؟ وما فئات المستخدمين لها؟

- **المرجعية والمسؤولية**: من الجهة أو الجهات التي تتولى الإشراف على الهيكل وتنفيذ المشاريع المتعلقة به؟ ومن الجهات المسئولة عن تحقيق مجالات النطاق السابق ذكره؟

- **الأنموذج والتمويل:** ما الطريقة المناسبة لتمويل مشاريع البنية التحتية لضمان استمرارية بقائها وتشغيلها؟ ومن يتولى تكاليف الإنشاء الأولية؟

- **الأنظمة:** ما الأنظمة والقواعد والشروط والضوابط اللازمة لإدارة البنية التحتية وبث الثقة في نفوس المتعاملين والعدل بين المتعاملين وإنصافهم؟

من القرارات الإستراتيجية المرتبطة بهذه المحاور ما يلي:

١) هل تقوم كل جهة حكومية، حسب حاجتها، بتولي عملية تقديم خدمة المفاتيح العامة لموظفيها ومن يتعامل معها؟ أم تتولى جهة واحدة (حكومية أو غير حكومية) هذه المهمة وتقوم بتقديم الخدمة لجميع الجهات الحكومية؟ ومن تكون تلك الجهة؟

٢) من يتولى عملية تسجيل الشهادات والتحقق من هوية صاحب الشهادة عند التسجيل؟ هل الجهة المستفيدة أم الجهة المقدمة للخدمة؟

٣) هل تقوم كل جهة حكومية مستفيدة بإنشاء مركز تسجيل خاص بها؟

٤) كيف يتم التحقق من هوية صاحب الشهادة؟ وما الضوابط المتبعة في سبيل تحقيق ذلك؟

٥) هل هناك فئات مختلفة للشهادة الرقمية حسب طبيعة استخدامها؟ وما هذه الفئات؟

٦) هل يفتح المجال لعدد كبير من مراكز التصديق التجارية والحكومية والخاصة، أم يكتفى بعدد محدود حسب ضوابط وإجراءات ترخيص معينة؟

٧) كيف تتم معاملة مراكز التصديق الخاصة، القائم منها وما سيتم إقامته، من حيث قدرتها على إصدار الشهادات الرقمية؟ وما نوع الشهادات التي تصدرها؟ وهل تتم المصادقة على جميع هذه المراكز أو بعضها من قبل المركز الأم؟

٨) من يقوم بعملية المراقبة والتدقيق على هذه المراكز؟ هل تقوم بها جهة مستقلة مفوضة بذلك؟ أم تقوم بها هيئة الاتصالات وتقنية المعلومات؟ أم يقوم بها المركز الأم؟

٩) من يقوم باستخراج المفتاح الخاص لصاحب الشهادة؟ هل صاحب الشهادة نفسه أم مركز التصديق؟ وكيف يحفظ هذا المفتاح الخاص لضمان سلامة البنية الأمنية وبث الثقة فيها؟ وأين يحفظ؟

١٠) ما متطلبات حفظ الشهادات الرقمية بحيث تكون متوافرة بشكل فوري وعلى مدى ٢٤ ساعة؟

١١) كيف يمكن الحصول على الشهادات القديمة من أجل مطابقة توقيع قديم مضى عليه سنوات عديدة؟

١٢) ما طبيعة العلاقة بين مراكز التصديق الإقليمية والدولية؟ ومن يتولى تنسيق أعمال هذه العلاقة؟

تطرح هذه الوثيقة تلك القضايا وتحاول الإجابة عن بعضها، وتترك بقية الحلول والمقترحات للنقاشات والمباحثات اللاحقة.

لمزيد من المعلومات عن البنية التحتية للمفاتيح العامة

يمكن الاتصال بالمركز الوطني للتصديق الرقمي

برنامج الحكومة الإلكترونية - وزارة الاتصالات وتقنية المعلومات:

د. فهد عبد الله الحويماني

هاتف: 2131-452-1-966+

فاكس: 2064-452-1-966+

fhoymany@mcit.gov.sa

مقدمة

هناك حاجة ملحة للتعامل الآمن عن طريق شبكة الإنترنت لاسيما في ظل الانتشار السريع للإنترنت والتوسع في استخدامها في شتى المجالات. فالإنترنت تستخدم حالياً للتراسل والتخاطب بين عامة الناس، ولإجراء الصفقات التجارية المختلفة، علاوة على استخداماتها المتعددة في المنشآت الحكومية والعسكرية والتي تحتاج إلى قدر كبير من السرية والموثوقية حسب طبيعة عملها. وهناك ما يعرف بالشبكات الافتراضية الخاصة (Virtual Private Networks) والتي تستفيد من انتشار شبكة الإنترنت وانخفاض تكلفة الارتباط عن طريقها لتمنح المنشأة إمكانية إنشاء شبكتها الخاصة باستخدام خطوط الإنترنت ذات التكلفة المتدنية، مع ضمان سرية وموثوقية البيانات المتبادلة بوساطة هذه الشبكة العامة.

وهناك عدد من القضايا الهامة التي تمس المتعاملين عن طريق الإنترنت، والتي تبين من خلال البحوث والتجارب العالمية في السنوات الماضية أن تقنية البنية التحتية للمفاتيح العامة تقدم أفضل الحلول لهذه المشكلات. ومن هذه القضايا ما يلي:

- كيف يمكن لشخصين التراسل فيما بينهما بعيداً عن أعين المتطفلين والعابثين؟
- كيف يستطيع من يستقبل رسالة إلكترونية التأكد من أن المرسل هو الشخص المتوقع وليس بشخص آخر قد انتحل شخصيته؟
- كيف يستطيع المصرف التأكد من أن الشخص الذي يود الدخول إلى حسابه الشخصي هو في الواقع صاحب الحساب وليس بشخص آخر؟ أو كيف لإدارة المرور التأكد من أن من يطلب تجديد رخصة القيادة هو بالفعل صاحب الرخصة؟ أو كيف لمدرسة أو جامعة التأكد من أن من يود الدخول إلى سجلاته الدراسية هو الطالب المعني وليس بشخص آخر غيره؟
- كيف يستطيع من يود الدخول إلى موقع على الإنترنت (كالموقع الخاص بالمصرف أو بإدارة المرور أو بالجامعة) التأكد من أن الموقع الذي سيدخله هو الموقع المعني وليس بموقع تم إنشاؤه للاحتيال على المستخدمين؟
- كيف يستطيع وسيط الأسهم منع زبون من إنكار قيامه بإدخال طلب الشراء لعدد من الأسهم، عندما يكون الزبون بالفعل قد أدخل الأمر لشراء الأسهم؟
- ماذا لو أنكر الزبون إدخال أمر الشراء بعد سقوط سعر السهم الذي اشتراه لعدد ١٠٠ ألف سهم، وادعى أن الأمر كان لشراء ١٠٠ سهم فقط؟ هل يستطيع الوسيط إثبات عكس ذلك؟
- كيف يمكن لطرفين التوقيع على عقد تجاري فيما بينهما عن طريق الإنترنت،

بدون الحاجة لتواجدهما معاً في المكان نفسه؟

- كيف يمكن للمرسل التأكد من استلام المرسل إليه للرسالة؟ وكيف يلزمه قانونياً بذلك؟ وكيف للمرسَل إليه إثبات قيام المرسل بإرسال الرسالة؟

إن الأجوبة عن جميع تلك الأسئلة نجدها فيما يعرف بالبنية التحتية للمفاتيح العامة، والتي تشكل منظومة متكاملة لإدارة المفاتيح الرقمية المستخدمة في أمن المعلومات وسريتها وسلامتها، وتقوم بأداء عدد من الوظائف منها ما يلي:

- سرية المعلومات Confidentiality: وتعني تمكين المتعاملين من تبادل المعلومات فيما بينهم بحيث لا يمكن للآخرين معرفة طبيعة تلك المعلومات.
- التثبت من الهوية Authentication: وتعني تمكين المتعاملين من معرفة هوية بعضهم البعض بشكل قاطع.
- سلامة البيانات Data Integrity: وتعني اكتشاف أي تغيير في شكل البيانات أو محتواها، أو القيام بحذف جزء منها أو الإضافة إليها أو تعديلها بعد الإرسال.
- التوقيع الإلكتروني Electronic Signature: وتعني قدرة المستخدم على إجراء عملية التوقيع بصيغة إلكترونية وقدرة المستلم على التحقق من صحة هذا التوقيع.
- منح الصلاحية Authorization: تحديد نطاق الصلاحية الممنوحة للشخص المفوض بعمل ما، بحيث تختلف هذه الصلاحية حسب هوية الشخص.

راجع الملحق (أ) للتعرف على المفاهيم الخاصة بالبنية التحتية للمفاتيح العامة.

دور وزارة الاتصالات وتقنية المعلومات

يتمثل دور وزارة الاتصالات وتقنية المعلومات في البنية التحتية للمفاتيح العامة من خلال برنامج الحكومة الإلكترونية (يسّر) فيما يلي:

- **اقتراح الأنموذج الأنسب للبنية التحتية للمفاتيح العامة ووضع الأطر المنظمة لها.**

- **تجهيز وتشغيل المركز الخاص ببنية المفاتيح العامة، المسمى المركز الوطني للتصديق الرقمي.**
- **اقتراح الأنظمة والسياسات والاستراتيجيات اللازمة لها.**
- نشر التوعية بأهمية بنية المفاتيح العامة والتثقيف بها والتدريب عليها.

تطبيقات الشهادة الرقمية

في دراسة استخدام الشهادة الرقمية في المملكة يمكن لنا تصور عدد من التطبيقات المهمة التي قد تجد القبول السريع والانتشار، ومنها ما يلي:

البريد الإلكتروني الآمن

يتيح البريد الإلكتروني الآمن للمستخدمين، سواءً في المنازل أو في العمل، تشفير الرسائل الإلكترونية منعاً لقراءتها من قبل المتطفلين والعابثين، وتتم العملية بقيام المرسل بتشفير الرسالة بواسطة المفتاح العام للمرسل إليه، ويقوم المرسل إليه بعد وصول الرسالة بفتحها بوساطة مفتاحه الخاص. ولضمان الموثوقية والسرية فإن المرسل يحتاج إلى الحصول على الشهادة الرقمية الرسمية للمرسل إليه والتي يجب أن تكون صادرة من مركز تصديق يعمل بطريقة نظامية، ويتّبع إجراءات دقيقة في عملية إصدار الشهادة.

وبالنسبة لمستلم الرسالة، فيستطيع التحقق من مصدر الرسالة (التأكد من أن المرسل هو بالفعل الشخص الظاهر اسمه في البريد الإلكتروني) بالقيام بمطابقة التوقيع الإلكتروني للمرسل كما يظهر في الرسالة، وذلك بجلب الشهادة الرقمية الرسمية للمرسل وإجراء عملية المطابقة.

مواقع الإنترنت الآمنة

تستخدم الشهادة الرقمية بكثرة في مواقع الإنترنت، خصوصاً تلك المعنية بالتجارة الإلكترونية. في هذه الحالة تقوم الجهة المقدمة للخدمة الإلكترونية بالحصول على شهادة موقع لاستخدامها مع بروتوكول[1] SSL وتسمى هذه الشهادة بـ SSL Server Certificate، وتحتوي على اسم الجهة واسم النطاق الخاص بالموقع Domain

[1] SSL: Secure Socket Layer

Name، إلى جانب المفتاح العام للموقع. تكمن الفائدة من هذه الشهادة في أنها تتيح للزائر معرفة هوية الموقع، وتسمح بتشفير البيانات الصادرة عن الموقع والواردة إليه.

وقد يجد هذا الاستخدام قبولاً كبيراً في تطبيقات الحكومة الإلكترونية المنتظرة، وفي جعل مواقع التعليم عن بُعد ومواقع الطب الاتصالي أكثر أمناً وأماناً. إلا أن هناك عدداً من التحديات تجعل هذه العملية عرضة للتلاعب والتضليل إن لم تتم مراعاة عدد من الضوابط والإجراءات من قبل جميع الأطراف المعنية (المستخدم، والجهة صاحبة الموقع، ومركز التسجيل، ومركز التصديق) كما سنرى لاحقاً عند مناقشة قضية التحقق من الهوية.

التوقيع الإلكتروني

إن من أهم معوقات التحول من المكتب الورقي إلى المكتب اللاورقي (paperless office) عدم القدرة على تضمين التوقيع في الوثائق والخطابات والنماذج وغيرها، الأمر الذي يمكن تحقيقه بسهولة من خلال تقنية التوقيع الإلكتروني.

استخدامات أخرى

هناك استخدامات أخرى كثيرة لتقنية البنية التحتية للمفاتيح العامة من المتوقع أن تحظى باهتمام المستخدمين مع مرور الوقت ومنها ما يلي:

- التوقيع على البرامج الحاسوبية، بحيث يتمكن المستخدم من معرفة الجهة التي أصدرت البرنامج منعاً لانتشار الفيروسات أو استخدام برامج مقلدة أو رديئة المستوى.

- وضع الختم الزمني للمراسلات والوثائق، وهي طريقة يتم من خلالها إضافة الوقت الفعلي الرسمي الذي تمت فيه العملية الإلكترونية، ويستخدم لأغراض الإثبات القانوني لوقت حدوث عمل ما. وتتم عملية إضافة الختم الزمني من قبل جهة مستقلة مختصة بهذه المهمة.

- تصديق الخطابات التي تحتاج إلى مصادقة من جهة معينة، كما هو متبع في الطرق التقليدية كالحصول على مصادقة عمدة الحي، أو رئيس مركز الشرطة، والتي من الممكن أن تتم بشكل إلكتروني كامل.

- تحديد الصلاحيات بوساطة التوقيع الإلكتروني للجهة المانحة للصلاحية. على سبيل المثال، للدخول في مزاد إلكتروني يشترط وجود مركز رئيسي في مدينة معينة

للجهة المشاركة في المزاد يمكن في هذه الحالة قيام الجهة بالحصول على توقيع إلكتروني من الغرفة التجارية المعنية.

- التراسل الموثوق والآمن فيما بين أجهزة وخوادم الحاسبات من خلال إصدار شهادة رقمية لكل جهاز مع مقدرة الجهاز على إجراء التوقيع الإلكتروني الخاص به.

التحديات والمعوقات

على الرغم من القبول الكبير لتقنية البنية التحتية للمفاتيح العامة وقدرتها على الاستجابة للمتطلبات الأمنية المختلفة كالتحقق من الهوية والتشفير والتوقيع الإلكتروني، إلا أنها لم تحقق للدول والجهات التي قامت بتطبيقها النجاح المأمول على أرض الواقع، إذ لم تحظ بالقبول الواسع بين جموع المستخدمين ولا التنوع المطلوب في الاستخدام. ويستثنى من ذلك بالطبع الاستخدام الناجح والمنتشر للتقنية في مجال شهادات المواقع الآمنة وتشفير الاتصال مع المستخدمين بوساطة تقنية SSL.

لذا فإن من الضروري أن نتعرف على طبيعة تلك التحديات وأسباب المعوقات لكي نتمكن من تفاديها مبكراً والعمل على حلها عاجلاً.

من هذه التحديات والمعوقات التي برزت من خلال تجارب الدول في السنوات الماضية، واتضحت على سبيل المثال في تقارير مكتب المحاسبة العامة[2] في الولايات المتحدة الأمريكية ما يلي:

- ضعف الأنظمة الخاصة ببنية المفاتيح العامة، بل وعدم وجودها في بعض الحالات.
- التكلفة العالية لمشاريع بنية المفاتيح العامة، وعدم وجود أنموذج مناسب للتمويل الذاتي.
- صعوبة دمج تقنية بنية المفاتيح العامة مع البرامج الأخرى، وصعوبة تشغيلها في بيئات مختلفة، على سبيل المثال وجد صعوبات بالغة في تبادل المعلومات بين أدلة المفاتيح العاملة حسب بروتوكول LDAP وبروتوكول X.500.
- ضعف التوعية والتدريب يشكلان معوقاً من أهم المعوقات في سبيل استخدام التقنية وقبولها وانتشارها بين المستخدمين.

[2] GAO: General Accountability Office: http://www.gao.gov

وفي دراسة حديثة عن أبرز التحديات والمعوقات التي تواجه البنية التحتية للمفاتيح العامة[3] تبين أن أهم ثلاثة معوقات هي:

(١) عدم وجود دعم للبنية التحتية للمفاتيح العامة في البرامج.

(٢) التكلفة المرتفعة جداً.

(٣) وجود صعوبة بالغة في فهم التقنية واستخداماتها.

قرارات إستراتيجية

نظراً لأهمية البنية التحتية للمفاتيح العامة على المستوى الوطني لكونها تمس حياة المواطن والمقيم وتأثيرها البالغ في مجال التعاملات الإلكترونية كالتجارة الإلكترونية والحكومة الإلكترونية، ونظراً لكون الجانب الأمني للتعامل من خلال الإنترنت يأخذ دائماً أهمية خاصة لدى المتعاملين، ويقع في دائرة اهتمام مقدمي الخدمات والتطبيقات، سنقوم هنا باستعراض أهم عناصر هذه البنية الأمنية وتحديد النقاط الواجب مراعاتها واتخاذ القرارات الإستراتيجية بشأنها من البداية. وسنتجنب قدر الإمكان التوصية بخيار معين أو طريقة معينة، ونترك ذلك للنقاشات والدراسات التي سيقوم بها المختصون في الوزارة والجهات المعنية الأخرى.

الهيكل العام

هناك عدة أساليب وأطر عامة لكيفية نشر خدمة بنية المفاتيح العامة في البلاد، إذ نجد بعض الدول كالولايات المتحدة الأمريكية تقدّم الخدمة فيها عن طريق مراكز تصديق مستقلة ترتبط فيما بينها حسب اتفاقيات مصادقة بينية تبرم بين كل جهتين على حدة. وفي الأعوام الأخيرة تم إنشاء ما يعرف بالجسر الفيدرالي الذي يعتبر جهة مركزية مخولة بعملية المصادقة البينية.

أما طريقة المركز الأم Root CA، التي يقوم فيها المركز الأم بالمصادقة على شهادات مراكز التصديق التي تندرج تحته، فإنه يتلافى كثيراً من السلبيات، وينظم عملية تقديم الخدمة بشكل أفضل.

تقدر التكلفة الإجمالية لمشاريع بنية المفاتيح العامة الحكومية في الولايات المتحدة الأمريكية بأكثر من بليون دولار[4]، ويتم صرف ٣,٥٠ مليون دولار سنوياً

[3] "Identifying and Overcoming Obstacles to PKI Deployment and Usage", Stephen R. Hanna Sun Microsystems, Inc., Jean Pawluk Inovant, Inernet2 publication: http://www.internet2.org

في إدارة الجسر الفيدرالي وفي نشاطات هيئة وضع السياسات والأنظمة لبنية المفاتيح العامة. وقد كان عدد مشاريع بنية المفاتيح العاملة ٣٥ مشروعاً فقط من بين ٨٩ مشروعاً ومبادرة، وبلغ عدد الشهادات الرقمية التي تم إصدارها في الولايات المتحدة الأمريكية حتى مايو ٢٠٠٣م حوالي ٣,٥٠ مليون شهادة، من ١٢ مليون شهادة مستهدفة في السنوات القادمة.

ولتحقيق الاستفادة المثلى من البنية التحتية للمفاتيح العامة، وتلافي بعض الصعوبات، يجب أن نقوم بالإجابة عن عدد من الأسئلة ذات العلاقة بالهيكل العام للبنية ونطاق الاستخدام، منها ما يلي:

- من مستخدمو الشهادة الرقمية المتوقعون؟ وما التطبيقات المتوقعة التي تتطلب استخدام الشهادات الرقمية؟

- هل تقوم كل جهة حكومية، حسب حاجتها، بتولي عملية تقديم خدمة المفاتيح العامة لموظفيها والمتعاملين معها؟ أم تتولى جهة واحدة (حكومية أو غير حكومية) هذه المهمة وتقوم بتقديم الخدمة لجميع الجهات الحكومية؟ وما هذه الجهة؟

- في حالة قيام جهة بتقديم خدمة المفاتيح العامة للجهات الحكومية، من يتولى عملية تسجيل الشهادات والتحقق من هوية صاحب الشهادة عند التسجيل؟ هل الجهة المستفيدة أم الجهة المقدمة للخدمة؟ وهل تقوم كل جهة حكومية مستفيدة بإنشاء مركز تسجيل خاص بها؟ أم يكون هناك مركز تسجيل مركزي لجميع الجهات الحكومية؟ وكيف يتم الاتصال بين الجهة المستفيدة وجهة التسجيل والجهة المقدمة للخدمة؟ هل يكون هناك ارتباط إلكتروني فيما بين هذه الجهات؟ أم يتم إرسال طلبات تسجيل الشهادات بالطرق التقليدية؟ في أي جهة من الجهات الثلاث (الجهة المستفيدة، أو في مركز التسجيل، أو في مركز التصديق) يتم إدخال بيانات الشهادة في البطاقة الذكية؟

- هل يفتح المجال لعدد كبير من مراكز التصديق، التجارية والحكومية والخاصة، أم يكتفى بعدد محدود حسب ضوابط وإجراءات ترخيص معينة؟

- كيف تتم معاملة مراكز التصديق الخاصة، القائم منها والآتي، من حيث قدرتها على إصدار الشهادات الرقمية؟ وما نوع الشهادات التي تصدرها، وهل تتم المصادقة على جميع هذه المراكز من قبل المركز الأم؟

[4] "Status of Federal Public Key Infrastructure Activities at Major Federal Departments and Agencies", United States General Accounting Office, Dec. 2003.

- في حالة وجود أكثر من مركز تصديق، من يقوم بعملية المراقبة والتدقيق على هذه المراكز؟ هل تقوم بها جهة مستقلة مفوضة بذلك؟ أم تقوم بها هيئة الاتصالات وتقنية المعلومات؟ أم يقوم بها المركز الأم؟

فئات الشهادة الرقمية

من الممكن تقسيم الشهادة الرقمية إلى نوعين رئيسيين: (١) شهادة تشفير، و (٢) شهادة هوية. تستعمل شهادة التشفير في أغراض تشفير البيانات والمراسلات لحفظها بشكل سري وآمن أثناء التعاملات الإلكترونية. أما شهادة الهوية الرقمية فهي عبارة عن هوية إلكترونية صادرة من جهة معينة للتعريف بحامل الشهادة والإقرار بأنه الشخص المعني الواردة مواصفاته في الوثيقة، وبناءً على ذلك فهو مخول بما تمنحه الوثيقة من صلاحيات. على سبيل المثال، تعتبر بطاقة الأحوال المدنية وثيقة هوية لأنها تقر بأن الشخص الوارد اسمه في البطاقة سعودي الجنسية وإن اسمه الكامل ورقم بطاقته كما هو ظاهر في البطاقة، وتبعاً لذلك فهو يتمتع بالصلاحيات الممنوحة للمواطن السعودي. كذلك فإن بطاقة الصراف الآلي وبطاقة مراجعة المستشفى وغيرها من البطاقات عبارة عن إقرار بأن الاسم الظاهر في البطاقة له الحق في التمتع بالصلاحيات والميزات التي تمنحها هذه البطاقة. وبما أن هذه البطاقة عبارة عن شهادة هوية فإنها تستخدم كذلك في إجراء التوقيع الإلكتروني حسب ضوابط فنية ونظامية سوف نتطرق إليها لاحقاً.

ويجب التذكير بأن الهوية الإلكترونية تمنح لغير الأفراد كالمؤسسات والشركات والجهات الحكومية، وتمنح علاوة على ذلك لفئتين رئيسيتين:

١) **مراكز التصديق ومراكز التسجيل**، حيث تقوم جهة أخرى (كمركز التصديق الأم) بإصدار شهادة هوية إلكترونية لهذه المراكز ليتمكن المستخدمون من التحقق من صحة الشهادات الصادرة عن طريق هذه الجهات.

٢) **الأنظمة البرمجية**، وفيها يتم منح شهادة رقمية لنظام برمجي يعمل من خلال جهاز حاسب آلي لتتمكن بقية الأطراف المستفيدة من هذا النظام من معرفة هوية النظام.

وكما تختلف متطلبات إصدار الهوية التقليدية في إجراءاتها وشروط الحصول عليها، كذلك فإن متطلبات الشهادة الرقمية تختلف حسب نوعها. فقد يكون هناك نوع من الشهادات الرقمية يتطلب إصداره التحقق الكامل والتثبت بشكل قاطع من هوية صاحب الشهادة وأهليته للحصول عليها، كما قد يتم في عملية إصدار بطاقة أحوال مدنية إلكترونية على سبيل المثال. وهناك نوع آخر من الشهادات الرقمية يتطلب قدراً قليلاً من الشروط. على سبيل المثال، قد لا يتطلب الدخول إلى أحد المنتديات أكثر من شهادة رقمية مبنية فقط على التحقق من صحة البريد الإلكتروني للشخص.

لذا فقد يكون من المناسب اختيار عدد محدود من فئات الشهادة الرقمية يتناسب مع طبيعة الاستخدامات المفترضة للشهادة والأخذ في الاعتبار مدى المخاطر والعواقب والخسائر التي قد تنتج في حالة سوء استخدام هذه الشهادة. على سبيل المثال، قد تكون هناك ثلاث فئات رئيسية للشهادة الرقمية كما يلي:

أ. **شهادة من فئة (أ):** تكون هذه الشهادة عالية الموثوقية، ويتطلب إصدارها التحقق الكامل من هوية صاحبها بالحضور الشخصي لدى مركز التسجيل أو التصديق، وقد يستلزم الأمر أخذ بصمة صاحب الشهادة أو أي علامة بيولوجية له. وتستخدم هذه الشهادة لأغراض التحقق من الهوية في بعض التطبيقات الحكومية والتجارية المهمة، كإصدار جواز السفر أو تجديده.

ب. **شهادة من فئة (ب):** تكون هذه الشهادة متوسطة الموثوقية، وتبعاً لذلك تقل شروط وضوابط إصدارها عن الفئة (أ)، وقد تستخدم لأغراض التجارة الإلكترونية أو الحكومة الإلكترونية متوسطة الخطورة. على سبيل المثال، قد تستخدم هذه الشهادة في بعض التطبيقات الحكومية التي من خلالها يستطيع المستخدم الحصول على معلومات شخصية خاصة به أو إجراء عملية معينة لا تعتبر ذات خطورة عالية فيما لو كان هناك سوء استخدام لها.

ج. **شهادة من فئة (ج):** هذه الشهادة عبارة عن وسيلة تعريف إلكترونية قليلة الخطورة ولا يتطلب استخراجها أي نوع من التحقق من هوية صاحبها، وتستخدم في التطبيقات ذات الخطورة المتدنية. على سبيل المثال، لمنح المستخدم مساحة تخزينية صغيرة في موقع حكومي إلكتروني، أو في تعامل تجاري محدود، فيكتفى بهذا النوع من الشهادات.

كمثال على فئات الشهادات الرقمية المستخدمة في دول أخرى نجد أن الحكومة الفدرالية في الولايات المتحدة الأمريكية قد أقرت أربعة مستويات للشهادة الرقمية كما يلي[5]:

١) المستوى الأول: يكون مستوى الثقة في هوية صاحب الشهادة ضعيفاً أو معدوماً تماماً.

٢) المستوى الثاني: يكون مستوى الثقة في هوية صاحب الشهادة متوسطاً.

٣) المستوى الثالث: يكون مستوى الثقة في هوية صاحب الشهادة عالياً.

٤) المستوى الرابع: يكون مستوى الثقة في هوية صاحب الشهادة عالياً جداً.

[5] "E-Authentication Guidance for Federal Agencies", EXECUTIVE OFFICE OF THE PRESIDENT: OFFICE OF MANAGEMENT AND BUDGET, WASHINGTON, D.C. December 16, 2003

لذا فإن شركة فري ساين (Verisign) المختصة ببيع الشهادات الرقمية تقوم بتصنيف شهاداتها إلى ثلاث فئات رئيسية حسب متطلبات الاستخدام[6].

التحقق من الهوية

يجب التفريق بين مفهومين مهمين: (١) الهوية (Identification) و (٢) التحقق من الهوية (Authentication). بالنسبة للهوية فكما ذكرنا إنها مجرد وثيقة تثبت أن الشخص المذكور فيها هو صاحب الهوية وله الصلاحيات والحقوق التي تخوله بها. فإذا كانت الهوية صادرة من جهة رسمية أو أنها تحتوي على توقيع جهة ذات موثوقية عالية ومصداقية جيدة فإن الهوية تعتبر سليمة وجديرة بالتصديق. ولكن هذه الهوية بحد ذاتها لا تثبت أن حامل الهوية أو الذي يريد التصرف بها هو بالفعل صاحبها. هنا يأتي دور التحقق من الهوية الذي من خلاله تتم عملية التحري والتقصي للتأكد من علاقة الهوية بحاملها، قبل الإصدار وقبل كل استخدام. وفي الحالات التقليدية يتم التحقق من الهوية بمطابقة وجه الشخص بالصورة المثبتة في الهوية أو بقيام الشخص بالإدلاء برمز سري معين. ولكن يجب أن تراعى الجوانب العملية عند التحقق من الهوية إذ من غير العملي أن يبذل جهد كبير في التحقق من هوية صاحب الشهادة عند الإصدار إذا كانت الشهادة لن تستخدم في معاملات ذات طابع سري أو حساس.

التحقق القوي من الهوية

يجب على الجهات التي تقوم بعملية التسجيل للحصول على الشهادات الرقمية، سواءً أكانت مراكز تسجيل حكومية أم تجارية، مراعاة عدد من الضوابط والإجراءات للتحقق من شخصية الجهة الاعتبارية أو الطبيعية. وينطبق ذلك بالأخص في حالة الشهادات من فئة (أ) و فئة (ب) وذلك للتأكد من أن الاسم المراد تدوينه في الشهادة هو بالفعل الاسم الحقيقي والقانوني لصاحب الشهادة، وبالتالي بث الثقة في نفوس المستخدمين.

لمنح شهادة رقمية لموقع تجاري على الإنترنت، يجب على مركز التسجيل التحقق من ثلاثة ضوابط رئيسية[7] وهي:

١) التحقق من أن اسم النطاق الذي سيظهر في الشهادة هو ملك للجهة المتقدمة والتي سيتم ربط اسمها باسم النطاق في الشهادة، وقد يتطلب ذلك الحصول على خطاب رسمي من الجهة المانحة لاسم النطاق، سواءً أكانت داخل المملكة أم خارجها.

[6] http://www.verisign.com
[7] "Digital Certificates, Authentication, and Trust on the Internet", KPMG Whitepaper, 2002.

هذا الإجراء يمنع قيام جهة بتسجيل اسم نطاق جهة أخرى في شهادة رقمية لها، وبالتالي تضليل زائر الموقع الذي يقوم تشفير بياناته مستخدماً المفتاح العام الوارد في الشهادة، وتقوم الجهة المزيفة بفك التشفير عنها باستخدام المفتاح الخاص الذي بحوزتها.

٢) التحقق من الوجود القانوني للجهة طالبة الشهادة، وقد يتم ذلك بالحصول على صورة من السجل التجاري للجهة أو خطاب رسمي من جهة حكومية معينة، كالوزارة المشرفة على تلك الجهة.

هذا الإجراء يمنع انتشار المواقع الوهمية التي لا توجد بشكل قانوني على أرض الواقع، وتهدف في الغالب إلى تضليل المستخدمين والاحتيال عليهم.

٣) التحقق من أن الشخص المتقدم للحصول على الشهادة مخول رسمياً من قبل الجهة صاحبة الشهادة لاستخراج الشهادة باسمها واستلامها.

هذا الإجراء يمنع قيام أي شخص باستخراج شهادة رقمية لجهة دون إذن أو علم منها، وبالتالي الاستفادة من الشهادة في أعمال غير مشروعة.

المفتاح الخاص

إن أهم جزئية بيانات في منظومة البنية التحتية للمفاتيح العامة هي المفتاح الخاص لصاحب الشهادة[٨] الذي يجب أن يحفظ بشكل سري لدى صاحبه، ويجب ألا يطّلع عليه أحد. وتزداد أهمية المحافظة على المفتاح الخاص كلما اتجهنا إلى أعلى الهيكل، أي أن سرية المفتاح الخاص للمركز الأم تستحوذ على أقصى درجات الأهمية والسرية العالية، ويأتي بعد ذلك في درجات الأهمية المفتاح الخاص لمركز التصديق، ومن ثم المفتاح الخاص لمركز التسجيل، وأخيراً المفتاح الخاص للفرد أو المنشأة، وهكذا. وهذا ما يفسر ضرورة اتخاذ إجراءات أمنية صارمة ودقيقة لمراكز التصديق وبالأخص المركز الأم.

استخراج المفتاح الخاص

من يقوم باستخراج المفتاح الخاص لصاحب الشهادة؟ هل يقوم بذلك صاحب الشهادة بنفسه من خلال جهازه الخاص، ومن ثم يقوم بطلب المصادقة على مفتاحه العام (المرتبط بهذا المفتاح الخاص) من مركز تصديق معتمد؟ أم أن مركز التصديق يقوم باستخراج المفتاحين نيابة عن صاحب الشهادة؟ هنا يجب الانتباه إلى أن قيام الشخص باستخراج مفتاحه الخاص يأتي بدافع المحافظة عليه ومنع أياً كان من الإطلاع عليه. ولكن هناك مشكلتان رئيسيتان تنتجان عند قيام الشخص باستخراج المفتاح الخاص بنفسه:

[8] لا يقصد هنا "المفتاح الخاص بصاحب الشهادة"، بل "المفتاح الخاص لصاحب الشهادة" أي المفتاح الخاص المملوك من قبل صاحب الشهادة، مثله مثل المفتاح العام لصاحب الشهادة.

١) قد لا تتوافر لدى الشخص البنية الفنية المناسبة من الناحية الأمنية والتقنية لاستخراج المفتاح الخاص بالشكل المطلوب، وبالتالي يصبح هذا الشخص عرضة لمخاطر أمنية عديدة.

٢) في حالة المفتاح الخاص لشهادة التشفير، قد ترى جهة العمل ضرورة حفظ المفتاح الخاص بموظفيها لديها، وذلك من أجل فك التشفير عن الوثائق والمراسلات عند تعذر وجود الموظف أو في حالة فقدانه للمفتاح الخاص.

حفظ المفتاح الخاص

نظراً لأهمية المفتاح الخاص، سواء المفتاح الخاص للأفراد أو مراكز التصديق أو مراكز التسجيل، فإن من الضروري أن يحفظ هذا المفتاح بطريقة آمنة، وقد يكون ذلك حسب الضوابط التالية:

١) بالنسبة للأفراد، يحفظ المفتاح في بطاقة ذكية معدة لهذا الغرض، يتم تخزين المفتاح فيها أثناء عملية الإصدار من جهاز استخراج المفاتيح لدى مركز التصديق. وفي بعض البطاقات الذكية يمكن استخدام المفتاح الخاص مع بقائه داخل البطاقة طوال الوقت، أي أن بإمكان الشخص إدخال بطاقته في الجهاز وإجراء توقيعه الإلكتروني بتمرير الوثيقة داخل البطاقة وإخراجها موقعة مع بقاء المفتاح الخاص في مكانه طوال العملية.

٢) بالنسبة لمراكز التصديق، فيحفظ المفتاح الخاص في بيئة أمنية خاصة، ولا يسمح باستخدامه إلا حسب ضوابط محددة وإجراءات صارمة من قبل عدد معين من الأشخاص، بحيث يُشترط تواجد شخصين أو ثلاثة أثناء عملية استخدام المفتاح.

حفظ الشهادات الرقمية وأرشفتها وتحديثها

نظراً لأهمية توافر الشهادة الرقمية بشكل فوري وعلى مدى ٢٤ ساعة، فإن من الضروري وضع الشهادات الرقمية في قاعدة معلومات خاصة يمكن الوصول إليها بيسر وسهولة باستخدام أنظمة قياسية معروفة، وذلك ليتمكن المعتمد على الشهادة من التحقق من الأمور التالية:

١) مطابقة توقيع صاحب الشهادة بالحصول على الشهادة المعتمدة وما تحتوي عليه من معلومات، بما في ذلك المفتاح العام للشخص.

٢) إرسال رسالة مشفرة لشخص معين عن طريق الشهادة المعتمدة له.

٣) التأكد من سريان مفعول الشهادة وأنه لم يتم إلغاؤها لسبب أو لأخر.

٤) وغالباً يستخدم نظام LDAP لطلب الشهادة الرقمية من قاعدة المعلومات المتوفرة لدى مركز التصديق، وتستخدم أنظمة OCSP[9]، SCVP[10]، و XKMS[11]. للتحقق من سريان مفعول الشهادة وصحتها.

ولكن ماذا عن الشهادات القديمة، كيف يمكن الحصول عليها؟ كيف يمكن مطابقة توقيع إلكتروني في وثيقة إلكترونية تم توقيعها قبل عدة سنوات؟ كما هو معروف فإن عملية مطابقة التوقيع تتم من خلال المفتاح العام لصاحب التوقيع الذي يوجد في شهادته الرقمية. ولكن من الممكن أن تنتهي صلاحية الشهادة ولا توجد في أي مكان، ومن الممكن أن يعلن مركز التصديق التجاري إفلاسه وتختفي جميع الشهادات الصادرة عن طريقه! لذا فمن الضروري أن تكون هناك آلية معينة لحفظ الشهادات الرقمية على المدى الطويل، والذي قد تمتد مدته إلى عشرات السنين، في قواعد معلومات خاصة من خلالها يمكن طلب الشهادة والحصول عليها بطريقة سريعة وآمنة. كما يجب أن تتوافر في نظام الأرشفة القدرة على تعقب التواقيع من شهادة لأخرى، حيث قد يكون من الضروري أحياناً طلب شهادة شخص لمطابقة التوقيع، ومن ثم طلب شهادة مركز التصديق الذي أصدر الشهادة لمطابقة توقيعه عليها، وهكذا.

متطلبات الأمن والتشغيل لمراكز التصديق

هناك عدد من المتطلبات والتجهيزات الفنية والإدارية والنظامية الواجب توافرها في بنية المفاتيح العامة لكي تتم عملية التشغيل بشكل سليم وآمن. فمن حيث التجهيزات الفنية فغالباً يتكون مركز التصديق الرقمي من عدد من الأجهزة والخوادم (servers) كأجهزة إصدار الشهادات والتوقيع عليها والتي تحتوي على محركات التشفير عالية السرية، وكذلك محركات استخراج الأرقام العشوائية. وهناك أجهزة أخرى تختص بإدارة قواعد المعلومات، وأجهزة تعمل كخوادم تطبيقات (Application Servers) وكخوادم لخدمة الويب، إلى جانب أنظمة الحفظ والأرشفة، وأنظمة حماية الشبكة من الاختراقات والفيروسات، كأنظمة الجدران النارية (Firewall)، وأنظمة التحكم في الأجهزة والشبكة. ويجب أن تكون هناك آلية متكاملة لإعادة تشغيل المركز في حالة وقوع كارثة أو خلل كبير ومن الممكن أن يتم ذلك عن طريق حفظ نسخة من الأجهزة والبرمجيات في مكان آخر.

أما بالنسبة لبقية التجهيزات الإدارية والتنظيمية التي يجب على مركز التصديق القيام بها لإرساء أسس الأمن والموثوقية وإضفاء المصداقية في طريقة عمل المركز والإجراءات المتبعة فيه، فمنها ما يلي:

[9] OCSP: Online Certificate Status Protocol
[10] SCVP: Simple Certificate Validation Protocol
[11] XKMS: XML Key Management Specification

- **سياسة الشهادة الرقمية** Certificate Policy: تحدد هذه السياسة مدى الثقة الممكن افتراضها في الشهادات الصادرة من مركز التصديق، والأوجه المشروعة لاستخدامها إلى جانب تبيانها لالتزامات مركز التصديق تجاه الأطراف المستفيدة وحقوق المستخدمين.

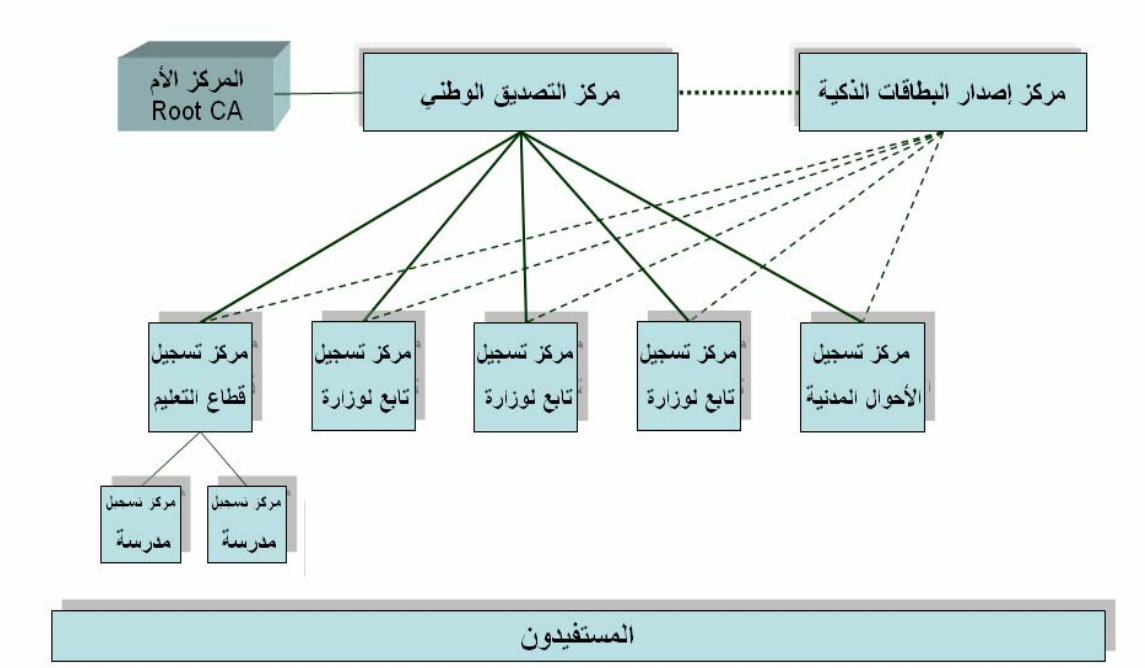
- **إجراءات التصديق الرقمي** Certification Practice Statement: يستطيع المستخدم معرفة الطرق الفنية والأمنية والإجرائية المتبعة لإصدار الشهادة من قبل مركز التصديق عن طريق تلك الإجراءات، وهي عبارة عن اللائحة التنفيذية لسياسة الشهادة الرقمية.

- **البيئة التشغيلية**: هي عبارة عن وثيقة تبيّن الطرق المتبعة من قبل مركز التصديق للقيام بمهامه، وتشمل إعداد الأنظمة وقواعد التشغيل وتحديثها باستمرار، والإجراءات الأمنية المكانية والبيئية وتلك المعنية بالأفراد، إلى جانب إدارة أنظمة الدخول والخروج والحفظ والأرشفة والتطوير والصيانة، وغيرها.

- **إدارة المفاتيح والشهادات**: نظراً لكون مفاتيح التشفير تقع في صلب عمل مركز التصديق، فيجب أن يتولى عملية إدارة مفاتيح التشفير من الألف إلى الياء، وتشمل استخراج المفاتيح وحفظها وأرشفتها وتوزيعها على المستفيدين واستعادتها في حالة فقدانها، أو إلغائها. ويقوم المركز كذلك بإدارة الشهادات الرقمية من وقت صدورها مروراً بنشرها واستخدامها وحفظها حتى تجديدها أو إلغائها وإتلافها.

الهيكل المقترح

يبين الشكل أدناه الهيكل الجديد المقترح لتقديم خدمة البنية التحتية للمفاتيح العامة في المملكة، والذي من خلاله نرى أن هناك عملية فصل للجانب الفني عن الجانب الإداري بحيث يقوم المركز الوطني للتصديق الرقمي بتولي الجوانب الفنية كإصدار مفاتيح التشفير وإدراجها في الشهادة الرقمية وفي البطاقة الذكية، وتترك الجوانب الإدارية المتعلقة باستيفاء متطلبات إصدار الشهادة كالتحقق من هوية صاحب الشهادة وأحقية الحصول على الشهادة لمراكز التسجيل في كل جهة. وبذلك تتخلص الجهات الحكومية (وربما غير الحكومية) من المصاعب الفنية والأمنية والتكاليف المرتبطة بهذه العملية والتركيز على أعمالهم الأساسية.



ويقوم بالإشراف على تنظيم خدمة البنية التحتية للمفاتيح العامة ووضع السياسات والقواعد المنظمة لها لجنة عليا مكونة من عدد من الجهات الحكومية وغير الحكومية.

خاتمة

تم في هذه الوثيقة إعطاء مقدمة مختصرة عن موضوع البنية التحتية للمفاتيح العامة واستخدامها في المملكة، وتم التركيز على أبرز الجوانب ذات العلاقة بالهيكل العام للبنية والقرارات الإستراتيجية اللازمة.

بقي أن نقول إن هناك من ينتقد الطريقة التي تتم بها المصادقة على الشهادات في البنية التحتية للمفاتيح العامة، حيث يشير هؤلاء إلى ضعف الموثوقية في عملية التحقق التي تقوم بها مراكز التصديق أو مراكز التسجيل في إثبات هوية طالب الشهادة، وصعوبة منح الثقة في تلك المراكز. كما إن هناك من يشكك في مدى السرية والأمن في الأجهزة التي تقوم بمطابقة التواقيع، أو تلك المستخدمة في حفظ المفاتيح الخاصة. وهناك من يشكك في الحاجة إلى تلك البنية التحتية برمتها، مشيراً إلى أن أكثر العمليات الإلكترونية تتم باتفاقات مسبقة بين أطراف معروفة لبعضها البعض، وليست هناك حاجة من قيام أطراف مجهولة لبعضها البعض بإنجاز معاملات تتطلب الأمن والسرية والالتزام بتبعيات مالية وقانونية! إلا أن الكثير في نهاية الأمر يعتقد بأن الإنترنت قد أوجدت أجواءً جديدة وفتحت فرصاً كثيرة تتطلب بنية تحتية آمنة كتلك المتوافرة عن طريق تقنية الـ PKI، كما إن الكثير مما ذكر من مصاعب يمكن حلها عن طريق إرساء القواعد القانونية اللازمة، ووضع الأسس والأطر التنظيمية اللازمة لضمان سلامة التعامل الإلكتروني والثقة به.

ختاماً، ندعو جميع المهتمين والمختصين ممن لديهم آراء أو مقترحات حول ما ورد في هذه الوثيقة إرسالها إلينا حسب العنوان الموضح في الصفحة رقم ٧.

ملحق (أ): البنية التحتية للمفاتيح العامة

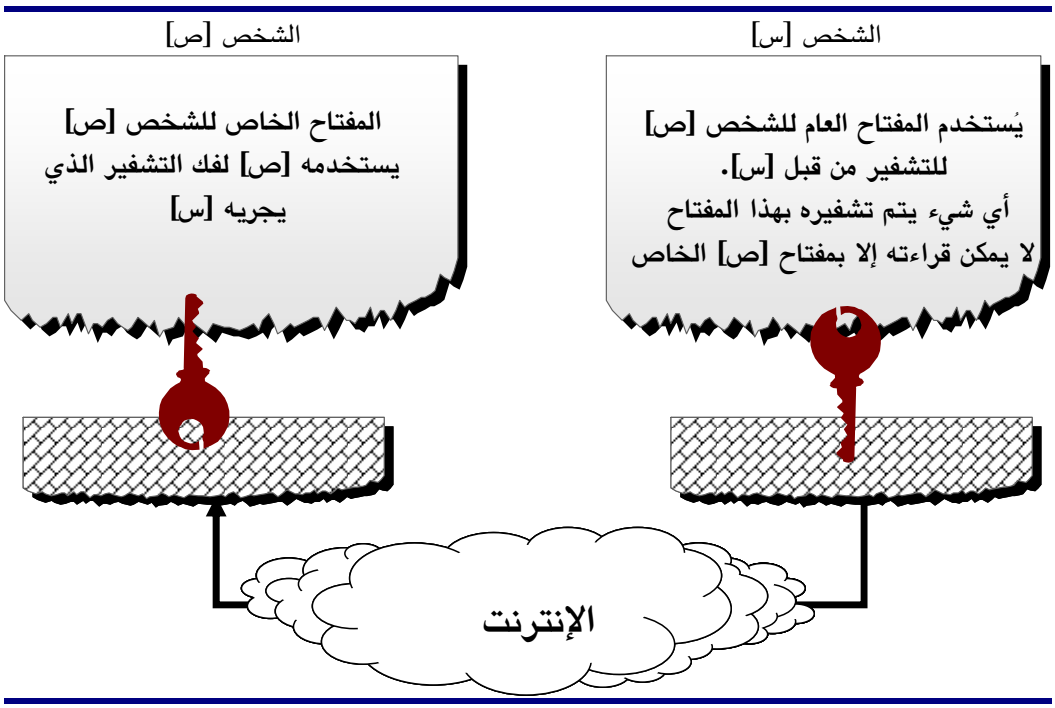
- تعريف -

التشفير والمفاتيح العامة

التشفير عبارة عن طريقة لنقل البيانات الإلكترونية أو تخزينها بحيث لا يمكن لغير الشخص المخول قراءتها أو الاستفادة منها بأي شكل كان. وأبسط مثال للتشفير هو قيام المرسل بتغيير ترتيب أحرف الرسالة بحيث يستبدل حرف A بحرف B وحرف B بحرف C وهكذا، ويقوم مستقبل الرسالة بإعادة الرسالة لصورتها الأصلية باستبدال حرف B بحرف A وحرف C بحرف B إلخ. في هذه الحالة يمكننا القول إن المفتاح (key) المستخدم للتشفير هو استبدال الأحرف بالطريقة التي قام بها المرسل أعلاه، وأن المفتاح المستخدم لفك التشفير هو عكس هذه الطريقة. ولقد تطور علم التشفير إلى أن وصل إلى درجة متقدمة بحيث أصبح اكتشاف المفتاح المستخدم في التشفير شبه مستحيل حتى لو أن شخصاً أمضى آلاف السنين محاولاً القيام بذلك ومستخدماً أسرع الحاسبات الآلية وأحدثها.

التشفير بواسطة المفتاح العام

تم اكتشاف طريقة التشفير بوساطة المفتاح العام قبل حوالي ٢٥ عاماً والتي تعتبر ثورة عظيمة في علم التشفير. تعتمد هذه الطريقة على مفتاحين مختلفين تجمعهما علاقة رياضية معينة، بحيث لا يمكن فتح ما يتم تشفيره بأحد هذه المفاتيح إلا بوساطة المفتاح الآخر. يحتفظ الشخص المتعامل بطريقة المفاتيح العامة بأحد هذه المفاتيح، وهو المفتاح الخاص (Private key)، ويقوم بحفظه لديه في مكان آمن، ولا يطلع عليه أي شخص آخر. ويقوم 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 - عن طريق البريد الإلكتروني، أو بعرضه في أحد أدلة المفاتيح العامة، على سبيل المثال. 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 إلى ذلك الشخص، الذي يقوم بفك التشفير عن الرسالة باستخدام مفتاحه الخاص. ولكي يقوم الشخصان بالتشفير فيما بينهما فعلى كل منهما الحصول على المفتاح العام للآخر، بالإضافة إلى احتفاظ كل واحد منهما بمفتاحه الخاص، أنظر الشكل رقم ١.



الشكل رقم ١: قيام [س] بتشفير رسالة لـ[ص] باستخدام المفتاح العام لـ[ص]

مثال تشبيهي

كما هو معروف فإن البيانات الإلكترونية بجميع أشكالها من كتابات نصية وصور ثابتة ومتحركة وتسجيلات صوتية وغيرها، تتحول في نهاية الأمر إلى سلسلة من الشحنات الكهربائية التي يعبّر عنها بالأرقام صفر و واحد. على 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: ٠١٠٠٠٠٠١ ويساوي الرقم ٦٥
- حرف L يتحول إلى: ٠١٠٠١١٠٠ ويساوي الرقم ٧٦
- حرف I يتحول إلى: ٠١٠٠١٠٠١ ويساوي الرقم ٧٣

فتظهر كلمة ALI في الحاسب وعلى الإنترنت كما يلي: ٠١٠٠٠٠٠١٠١٠٠١١٠٠٠١٠٠١٠٠١

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

- حرف A يتحول بعد الضرب في ٢ إلى ١٠٠٠٠٠١٠ = ١٣٠، وهو عبارة عن الحرف الفرنسي (é).
- حرف L يتحول بعد الضرب في ٢ إلى ١٠٠١١٠٠٠= ١٥٢، وهو عبارة عن علامة (_).
- حرف I يتحول بعد الضرب في ٢ إلى ١٠٠١٠٠١٠= ١٤٦، وهو عبارة عن الحرف الأجنبي (Æ).

فيتم نقل الكلمة المراد إرسالها على أنها Æ_é، والتي لا يمكن لأحد أن يعرف أنها تعني كلمة ALI ما لم يعلم أن المفتاح المستخدم لفك الشفرة هو القسمة على الرقم ٢، وهو المفتاح الخاص الموجود لدى المرسل إليه فقط ولا يعرفه أحد سواه. وغني عن القول، إن التشفير في هذا المثال مبسط جداً ولا يستعمل بهذه الطريقة على الإطلاق، بل إن هناك طرق رياضية متقدمة تعتمد على مفاهيم رياضية معقدة للحصول على أفضل حيلة تعمل بها هذه المفاتيح، وتعتمد تلك الطرق في مجملها على عدم إمكانية عكس العملية للحصول على النص الأصلي، والتي جعلت من السهولة فك التشفير في المثال السابق، وذلك بعكس العملية التي تم بها التشفير (من الضرب إلى القسمة).

التشفير بواسطة المفتاح السري

نظراً لبطء عملية التشفير بوساطة المفاتيح العامة، فإن المفاتيح العامة لا تستعمل غالباً في تشفير البيانات، بل تستخدم فقط في عملية التوقيع الإلكتروني والتثبت من هوية المتراسلين، وفي عملية تمرير مفتاح التشفير التقليدي قبل البدء في عملية التراسل. ويسمى مفتاح التشفير التقليدي أحياناً بالمفتاح السري (Secret Key) ويتميز بأن التشفير عن طريقه يتم بسرعة عالية، لذا يفضل عادة استخدامه في تشفير المراسلات والملفات الإلكترونية بدلاً من المفتاح العام. على سبيل المثال، لكي يستطيع الشخص [س] إرسال وثيقة مشفرة إلى شخص [ص] (كما في الشكل السابق رقم ١)، فإن عليه إتباع الخطوات التالية:

١) الحصول على المفتاح العام للشخص [ص].

٢) اختيار مفتاح تشفير تقليدي، الأمر الذي يتم بطريقة آلية عشوائية عن طريق برنامج التشفير في جهاز [س].

٣) القيام بتشفير ذلك المفتاح التقليدي باستخدام المفتاح العام لـ [ص]، بحيث لا يستطيع أحد قراءته عدا [ص]، وإرساله إلى [ص].

٤) إرسال الوثيقة مشفرة إلى [ص]، الذي يستطيع بدوره قراءتها بوساطة مفتاح التشفير التقليدي الذي حصل عليه من [س] سابقاً.

لاحظ لو أن الشخصين [س] و [ص] قد سبق لهما أن التقيا وجهاً لوجه لربما تبادلا مفتاحيهما العامين ولم يعد هناك حاجة ليتأكد كل منهما من هوية الآخر! بل إن من الممكن أن يتفقا على مفتاح التشفير التقليدي ولا يكون هناك حاجة للبنية التحتية للمفاتيح العامة على الإطلاق. ولكن ذلك بالطبع ليس عملياً ولا يتفق مع الهدف الأساس من إيجاد العمليات الإلكترونية التي تتيح إمكانية التواصل والتراسل وإتمام الصفقات والعمليات الإلكترونية المختلفة عن بُعد دون الحاجة إلى التعامل المباشر بين الأطراف. إن الهدف الجوهري للمفاتيح العامة هو التحقق من هوية الأطراف المعنية، وتوفير بيئة اتصال آمنة، وليس التشفير بحد ذاته. وبوساطة البنية التحتية يمكن القيام بتغيير مفتاح التشفير التقليدي عدة مرات (منعاً لاكتشافه من قبل الآخرين)، وذلك بتشفيره بوساطة المفتاح العام للشخص الآخر في كل مرة.

التحقق من الهوية

كيف يقوم [س] بالحصول على المفتاح العام للشخص [ص]؟

ذكرنا قبل قليل أن على [س] الحصول على المفتاح العام لـ [ص] ليتمكن من تشفير البيانات الموجهة إليه، فكيف يحصل [س] على هذا المفتاح؟ هناك جهات معينة تقدم خدمة إصدار الشهادات الرقمية، وتعرف هذه الجهات بمراكز التصديق الرقمي Certification Authorities (CA)، ويتلخص دورها الأساسي في أنها تقوم بالمصادقة على علاقة المفتاح العام بالشخص صاحب الشهادة الرقمية. والذي يحصل غالباً أن يتقدم الشخص إلى مركز التصديق ويقدم ما يثبت هويته ثم تتم المصادقة على أن الشخص الفلاني هو صاحب المفتاح العام الفلاني. فيمكن لـ[س] البحث في أحد أدلة المفاتيح المختصة بجمع المفاتيح العامة للمتعاملين وعرضها على الإنترنت، ومن ثم الحصول على المفتاح العام للشخص [ص]. وللتأكد من صحة تلك العلاقة يقوم [س] بالتحقق من صحة التوقيع الظاهر في الشهادة بأنه توقيع خاص بمركز تصديق معتمد، كما سنرى بعد قليل.

سلامة المحتوى

كيف يضمن كل من [س] و [ص] سلامة البيانات من التغيير والعبث؟

لاحظ أن كل ما يقوم به [ص] هو مجرد فك التشفير عن الوثيقة التي تصله من [س]، ولكنه لا يعرف إن كان قد حصل لها تغيير أو عبث وهي في طريقها إليه! الحل هنا أن يتم إجراء عملية مختصر حسابي للوثيقة قبل إرسالها، تسمى تلك العملية بطريقة

Hashing، أو Checksum. الفكرة هنا أنه بالإمكان إجراء عملية رياضية معينة على محتوى الوثيقة بحيث يتم تحويل قيمة بيانات الوثيقة (التي كما علمنا أنها مجرد سلسلة من صفر و واحد) إلى عدد محدود، وليكن مكوناً من أربعين رقماً، ويرفق ذلك الرقم مع الوثيقة المرسلة. ومن المعروف في علم الرياضيات أنه من الصعب جداً (بل إنه من شبه المستحيل) أن يتطابق المختصر الحسابي، المبني على أحد الطرق القياسية المصممة لهذا الغرض، 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 أربعين 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 مع الوثيقة، فإنه فيجب على [س] القيام بتشفير المختصر الحسابي بوساطة المفتاح العام لـ [ص]، قبل إرسال الوثيقة.

التحقق من هوية المرسل

كيف يتحقق [ص] من أن المرسل هو بالفعل [س]؟

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

استخدام المفاتيح العامة في الإنترنت

من أكثر استخدامات البنية التحتية للمفاتيح العامة شيوعاً ما نراه في مواقع التجارة الإلكترونية ومواقع إجراء العمليات المصرفية من خلال الإنترنت. فلكي يثق العميل بموقع المصرف على الإنترنت، فإنه بحاجة إلى جهة رسمية تصادق على أن الموقع المراد الدخول إليه هو بالفعل الموقع الخاص بالمصرف، ويتم ذلك بمطابقة التوقيع الظاهر في الشهادة الرقمية الخاصة بالموقع بتوقيع مركز التصديق المعروف لدى العميل.

إن الذي يتم عادة هو أن يقوم المصرف بالحصول على ما يعرف بشهادة موقع (Server Certificate)، لاستخدامها في بروتوكول نقل البيانات المعروف بـ SSL، ويحصل المصرف على هذه الشهادة عن طريق أحد مراكز التصديق أو عن طريق مركز التصديق الخاص به. كل ما تمنحه هذه الشهادة هو الإقرار بأن المصرف الفلاني هو المالك الفعلي للمفتاح العام المرفق بالشهادة، وإن 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، والذي يقوم بالبحث في

الشهادات المعروفة لديه عن هوية مركز التصديق الذي قام بالتوقيع على شهادة المصرف. في حالة وجود شهادة لذلك المركز، يقوم المتصفح بمطابقة توقيع المركز الذي أصدر شهادة المصرف بتوقيع المركز المتوفر لديه. يدل تطابق التوقيعين على أن مركز التصديق المعروف لدى عميل المصرف (في جهازه) قد قام بالتوقيع، أي المصادقة، على شهادة المصرف. أما إذا كانت شهادة المركز الذي صادق على شهادة المصرف غير معروفة لدى متصفح العميل، فإن المتصفح يبرز رسالة على الشاشة لإطلاع العميل بذلك ويدعوه إلى اتخاذ القرار المناسب: إما اعتماد ذلك المركز على مسؤوليته أو رفض الاتصال ومحاولة التأكد من صحة الموقع.

لاحظ أن شهادة المصرف وُجدت لكي يثق العميل في المصرف، ولكن هناك كذلك حاجة لأن يثق المصرف بالعميل، الأمر الذي يتم عن طريق حصول العميل على شهادة مستخدم (Client Certificate)، من خلالها يستطيع المصرف التأكد من هوية العميل بمقارنة توقيع المركز الذي أصدر شهادة العميل بتواقيع مراكز التصديق المعروفة لدى المصرف، ومنها يستطيع التحقق من صحة هوية العميل. 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 سيتغير حتماً في الفترات القادمة حفاظاً على حقوق المتعاملين ومنعاً للاحتيال وانتحال شخصية الغير.

الشهادة الرقمية Digital Certificate

توجد في المملكة مراكز تصديق خاصة، بعضها قائم والبعض الآخر تحت الإنشاء، منها مراكز التصديق التابعة لكل من مؤسسة النقد العربي السعودي، وشركة أرامكو السعودية، وشركة الاتصالات السعودية، ومن المتوقع أن تنشأ مراكز تصديق أخرى في المستقبل القريب.

إن ما تقوم به مراكز التصديق هو الإقرار بأن الشخص المدون اسمه في الشهادة هو المالك الفعلي للمفتاح العام الظاهر في الشهادة، وإنه المالك الفعلي للمفتاح الخاص المصاحب لذلك المفتاح العام. تبين الشهادة الظاهرة في الشكل رقم ٢ اسم صاحب الشهادة، ومفتاحه العام، والرقم التسلسلي للشهادة، وتاريخ سريان مفعولها، وكذلك اسم مركز التصديق المانح للشهادة وتوقيعه عليها. إن توقيع المركز على الشهادة هو عبارة عن عملية تشفير للمختصر الحسابي للشهادة بوساطة المفتاح الخاص للمركز.

تعتمد موثوقية الشهادة الرقمية على ما يلي:

- الطريقة التي يعمل بها مركز التصديق لإثبات هوية المستخدم.
- أسلوب العمل والأنظمة التشغيلية لدى مركز التصديق.

- الخوارزميات الفنية المستخدمة في عملية التشفير وإثبات الهوية.
- الإطار القانوني الذي يعمل به مركز التصديق ومدى التزام المركز بذلك.
- مدى محافظة الشخص على المفتاح الخاص به.

الشكل رقم ٢: مثال لمحتوى الشهادة الرقمية

وبالنسبة للنقطة الأخيرة هذه، فتعد البطاقة الذكية (Smart Card) من أفضل الطرق للمحافظة على المفتاح الخاص، والتي في بعض أشكالها لا تسمح بخروج المفتاح من البطاقة، بل إن عملية إنشاء المفتاح ذاته يمكن أن تتم داخل البطاقة وليس في جهاز المستخدم ولا في جهاز مركز التصديق.

بقي الإشارة إلى أن مركز التصديق يقوم بإعداد قائمة مهمة تسمى سجل الشهادات الملغاة (Certificate Revocation List – CRL)، والتي تحتوي على أرقام الشهادات التي تم إلغاؤها من قبل المركز، إما لأن صلاحيتها قد انتهت أو أن مستخدم الشهادة فقد مفتاحه الخاص، أو غيرها من الأسباب التي تمنع استخدام الشهادة بشكل نظامي. ويقوم جهاز المستخدم بمراجعة هذه القائمة قبل اعتماد أي شهادة رقمية لشخص أو جهة.

التوقيع الإلكتروني Electronic Signature

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

الشكل رقم ٣: ظهور التوقيع الإلكتروني في أسفل الرسالة

يختلف التوقيع الإلكتروني عن التوقيع على الورق في أنه 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 للمفاتيح العامة، أو ما يعادلها من تقنيات أخرى. إن التوقيع على الورق قابل للتزييف بسهولة كما هو معروف، على الرغم من تفاوت شكل التوقيع من شخص إلى آخر. كما إن عملية التحقق من صحة التوقيع اليدوي غير عملية وتعتمد بشكل كبير على مهارة الشخص الذي يقوم بمطابقة التوقيع أو على معرفته السابقة بالشخص الموقع، وفي أحيان كثيرة لا تتم مطابقة التوقيع على الإطلاق! كذلك فإن الوثيقة الموقعة يدوياً قابلة للتغيير والعبث، وفي كثير من الأحيان يأتي التوقيع اليدوي في نهاية وثيقة مكونة من عدة صفحات، فيكون من السهل على أي عابث القيام بتغيير بعض صفحاتها دون أن يلحظ أحد ذلك. باختصار، نقول إن التوقيع الإلكتروني يتجنب جميع المشاكل الناتجة عن التوقيع اليدوي متى ما تم إحداثه بطريقة صحيحة.

ويوضح الشكل رقم ٤ كيفية عمل التوقيع الإلكتروني حيث إن مدير شؤون الموظفين يود إرسال إعلان إلى جميع الموظفين لإعلامهم عن موعد يوم إجازة خاصة للموظفين.

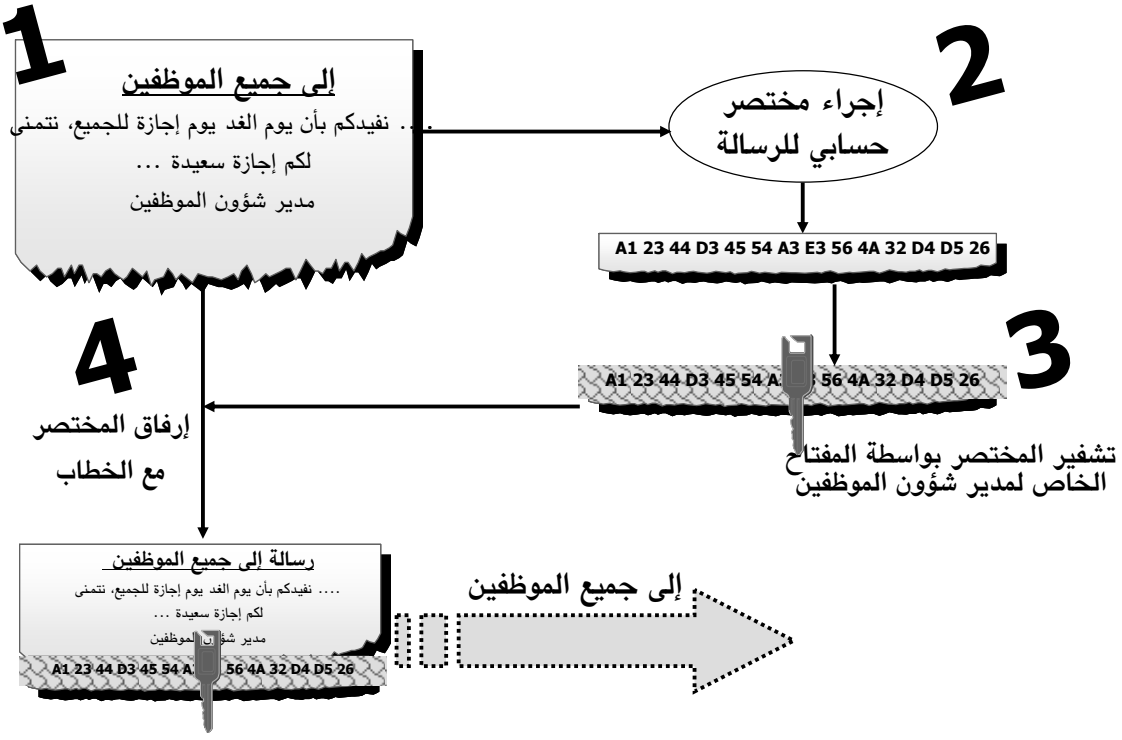
لاحظ أن المطلوب في هذه الحالة ليس تشفير الإعلان، الذي لا يعتبر سري بحد ذاته، بل إن المطلوب فقط التأكد من أن الإعلان صادر بالفعل من مدير شؤون الموظفين[12]. هنا نفترض أن جميع الموظفين لديهم المفتاح العام لمدير شؤون الموظفين، ونرى أن عملية التحقق من صحة توقيعه تتم حسب الخطوات التالية ووفقاً للأرقام الموضحة في الشكل:

١) قيام المدير بإعداد الإعلان.

٢) قيام جهاز المدير بإجراء العملية الحسابية التي تضمن سلامة المحتوى (راجع شرح الطريقة السابقة) لاستخراج المختصر الحسابي الخاص بتلك الوثيقة.

٣) قيام جهاز المدير بتشفير المختصر الحسابي باستخدام مفتاح المدير الخاص وذلك منعاً لقيام شخص آخر بتغيير الإعلان وإعادة حساب المختصر الحسابي وإرفاقه مع الإعلان.

٤) إرفاق المختصر الحسابي مع الوثيقة وإرسال الملف الناتج إلى جميع الموظفين عن طريق البريد الإلكتروني.



الشكل رقم ٤: توقيع الرسالة من قبل المرسل (مدير شؤون الموظفين)

[12] بالطبع هناك من الموظفين من سيفرح بالإجازة ويأخذ بها دون الحاجة إلى التحقق من صحة التوقيع، ولكن هذا موضوع آخر!

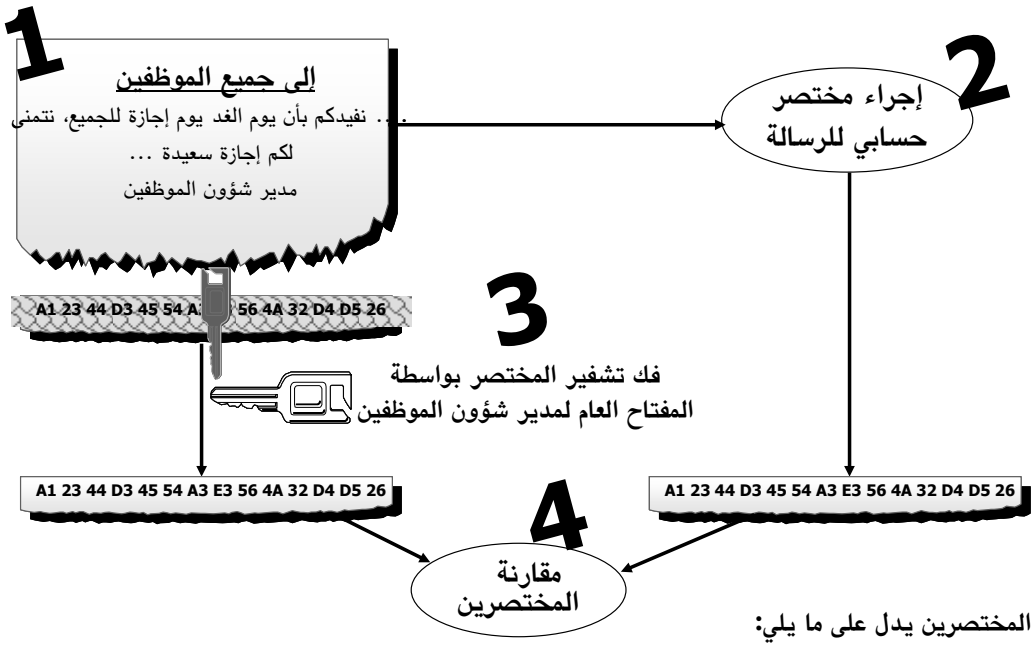
عند استلام أحد الموظفين للإعلان (أنظر الشكل رقم ٥)، يقوم جهازه بالتأكد من صحة التوقيع وذلك بإتباع الخطوات التالية.

١) استلام الإعلان من قبل أحد الموظفين.

٢) قيام الجهاز بإجراء المختصر الحسابي للوثيقة باستخدام العملية الرياضية نفسها التي تمت في جهاز المدير لاستخراج المختصر الحسابي الخاص بالرسالة.

٣) استخدام المفتاح العام للمدير لفك التشفير عن المختصر الحسابي واستخراج المختصر الحسابي الأصلي الذي تم إرساله من قبل المدير. هذه الخطوة تؤكد أن المرسل هو بالفعل مدير شؤون الموظفين، ولكنها لا تضمن سلامة نص الإعلان من العبث أو التغيير أثناء الطريق، بل إن ذلك يتم في الخطوة التالية.

٤) مقارنة الرقمين (من الخطوتين ٢ و ٣)، لإثبات أن الرسالة جاءت بالفعل من المدير ولم يحدث عليها أي تغيير.



تطابق المختصرين يدل على ما يلي:

(1) تم بالفعل إرسال الرسالة من قبل مدير شؤون الموظفين، (2) لم يحصل أي تغيير لمحتوى الرسالة على الاطلاق

الشكل رقم ٥: مطابقة التوقيع من قبل المستخدم (أحد الموظفين)

الأنظمة والقوانين

لكي تكون هناك بنية تحتية قوية ومتكاملة للمفاتيح العامة، يجب أن تراعى جوانب تنظيمية وتشريعية عديدة، منها قواعد ترخيص مراكز التصديق والقوانين المنظمة لإصدار الشهادات والعمل بها، إلى جانب الأنظمة الأخرى، كنظام التجارة الإلكترونية ونظام

التواقيع الإلكترونية. فيما يلي نستعرض أهم هذه الأنظمة والقوانين لإعطاء القارئ فكرة عنها وما يترتب عليها من أمور.

سياسة الشهادة الرقمية Certificate Policy

تحتاج البنية التحتية للمفاتيح العامة إلى وجود قواعد شاملة لتنظيم عملية إصدار الشهادات الرقمية من قبل مراكز التصديق. تعرف هذه القواعد بسياسة الشهادة الرقمية وهي عبارة عن مجموعة من الشروط والإرشادات التي تبيّن للمستخدم مدى ملائمة الشهادة الرقمية الصادرة من مركز التصديق لاحتياجاته، ومدى الموثوقية المصاحبة لها، إلى جانب تحديد الاستخدامات المشروعة وغير المشروعة للشهادات الرقمية. وتبيّن هذه القواعد التزامات مراكز التصديق التي تشمل إصدار الشهادات وإلغائها، وإثبات هوية المستخدم قبل الإصدار، وتخزين الشهادات الصادرة والشهادات الملغاة ونشرها، وكذلك الطرق الواجب إتباعها عند إصدار الشهادات للتأكد من سلامة الإجراءات المتبعة. لذا يجب على الجهة الراغبة في إصدار شهادات رقمية الالتزام بجميع الشروط الواردة في هذه السياسة ومن أهمها ضرورة إصدار ما يعرف بإجراءات التصديق الرقمي Certification Practice Statement، التي يستطيع المستخدم عن طريقها معرفة الطرق الفنية والأمنية والإجرائية المتبعة لإصدار الشهادة من قبل مركز التصديق، وكذلك معرفة كامل حقوقه ومسؤوليته الناتجة عن استخدام الشهادة الرقمية.

وتتطرق سياسة الشهادة الرقمية كذلك إلى دور مراكز التسجيل (Registration Authorities) في عملية المساعدة على إصدار الشهادات، وذلك بالتثبت من هوية المستخدم، ومتابعة إجراءات الإصدار والإلغاء، وما إلى ذلك. ولا تقوم مراكز التسجيل بإصدار الشهادات الرقمية، حيث يقتصر ذلك على مراكز التصديق فقط. وفيما يخص المستخدم فهناك شروط يجب عليه الالتزام بها، ومنها ضرورة التقيد بإجراءات التصديق الرقمي الصادرة من مركز التصديق، المحافظة على مفتاحه الخاص وإشعار مركز التصديق في حالة فقدانه، أو اكتشافه من قبل الآخرين، ومعرفة ما له وما عليه فيما يخص حقوقه ومسؤولياته.

باختصار، يمكننا القول أن سياسة الشهادة الرقمية وما يصدر بموجبها من لوائح إجرائية هي عبارة عن الدليل الكامل لجميع المتعاملين بالشهادات الرقمية، الذي يمكن الرجوع إليه عند حاجة المستخدم للحصول على شهادة، أو عند حاجة مركز التصديق لمعرفة التزاماته تجاه الآخرين، أو عند حاجة شخص لمطابقة توقيع شخص آخر. ومن خلال سياسة الشهادة الرقمية يمكن للجهات التجارية والحكومية معرفة ما يمكنهم الاستناد 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 الاعتراف 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 اعتراف الأطراف بجميع أنواع البيانات التي تتم بشكل إلكتروني.

يقدم القانون النموذجي مثالاً لتطبيق القانون على تجارة البضائع التي تشتمل على اتفاقيات بشأن نقل البضائع وطبيعتها وعددها، وكذلك فواتير الاستلام والمطالبة بالتسليم والإذن بالإفراج عن البضائع، وتسليمها إلى شخص معين أو جهة معينة، وما إلى ذلك من الضوابط التي 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. ويعتبر 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، ومن بينها ما يلي:

- يجب أن يرتبط التوقيع بشكل قاطع بالشخص الذي قام بالتوقيع وليس بشخص آخر غيره، فعندما يشير التوقيع إلى أنه يخص فلان ابن فلان، أو أنه توقيع جهة معينة، أو أنه توقيع باسم جهاز أو برنامج حاسوبي، فيجب أن يكون التوقيع بالفعل لذلك الشخص أو الجهة أو الجهاز.

- يجب أن يكون التوقيع تحت سيطرة الشخص الذي قام به وقت إجراء التوقيع، وليس تحت سيطرة أي شخص آخر.

- يجب أن تكون هناك القدرة على اكتشاف أي تغيير أو عبث يطرأ على التوقيع الإلكتروني بعد إحداثه، والمقدرة على اكتشاف أي تغيير أو عبث بالوثيقة الموقعة نفسها.

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

تقوم المملكة العربية السعودية حالياً بسن قوانين وأنظمة مشابهة لما تم التطرق إليه من قوانين وأنظمة، مراعية بذلك طبيعة التعاملات في المملكة وخصوصية الفرد السعودي، والتقيد بالشريعة الإسلامية. ولعل أهم هذه القوانين ما صدر مؤخراً على شكل مشروع لنظام التعاملات الإلكترونية، الذي يجمع عدة أنظمة في نظام واحد ويعتبر تطوراً مهماً في هذا المجال. فهذا النظام المنتظر يقوم بإرساء قواعد التعاملات الإلكترونية بجميع أشكالها من تجارة إلكترونية وحكومة إلكترونية وصحة إلكترونية وغيرها ويحتوي النظام على قواعد منظمة للتواقيع الإلكترونية وتشريعات خاصة بمقدمي خدمات التصديق الرقمي.

ملحق (ب) : المفاتيح العامة في المملكة العربية السعودية

تاريخ وهيكل

القرارات ذات العلاقة

يمكن تلخيص القرارات والأوامر السامية التي صدرت في السنوات الماضية والتي بناءً عليها بدأ العمل على عدة أصعدة في مجالات التجارة الإلكترونية والحكومة الإلكترونية والبنى التحتية المختلفة فيما يلي:

- الأمر السامي رقم ١٤٧٧٣/٥/ر، وتاريخ ١٤١٩/١٠/٢٧هـ، والقاضي بتشكيل لجنة دائمة للتجارة الإلكترونية بعضوية عدد من الجهات ورئاسة وزارة التجارة.

- الأمر السامي رقم ١١٤٢٧، وتاريخ ١٤٢١/٩/١٠هـ، القاضي برفع مستوى التمثيل في اللجنة الدائمة للتجارة الإلكترونية إلى مستوى الوكلاء المختصين.

- قرار اللجنة الدائمة للتجارة الإلكترونية بتاريخ ١٤٢٢/١/١٠هـ الذي أناط مهمة إنشاء وتشغيل المركز الوطني للتصديق الرقمي لمدينة الملك عبد العزيز، وتمت الموافقة السامية على ذلك بتاريخ ١٤٢٢/٥/١٧هـ بالأمر السامي رقم ٧/ب/٩٣٧٨.

- قرار مجلس الوزراء رقم ١٣٣، وتاريخ ١٤٢٤/٥/٢١هـ، والذي حددت فيه مهام وزارة الاتصالات وتقنية المعلومات وتنظيم عملها.

- خطاب رئيس ديوان رئاسة مجلس الوزراء رقم ٧/ب/٤٦٤٠٤ وتاريخ ١٤٢٤/٩/٢٨هـ القاضي بتغيير مسمى اللجنة الدائمة للتجارة الإلكترونية إلى اللجنة الدائمة للتعاملات الإلكترونية.

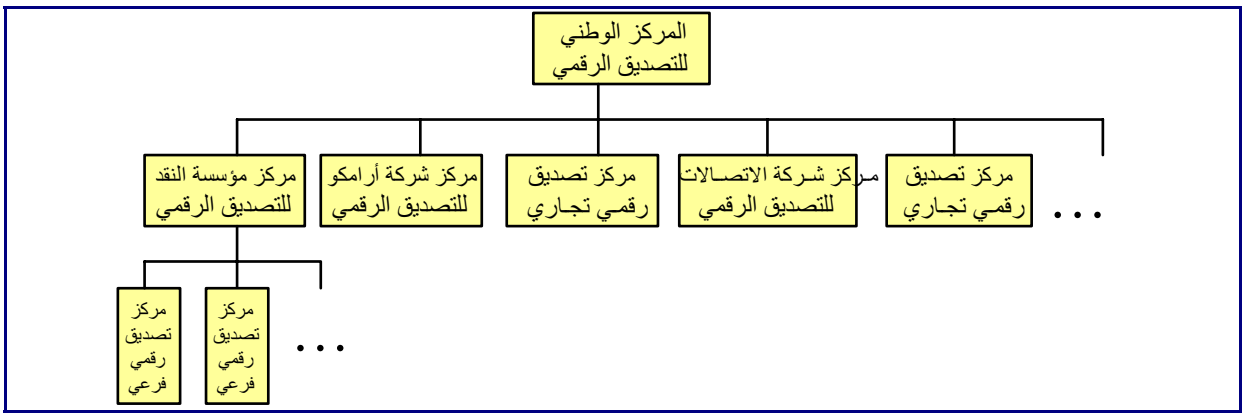
- خطاب رئيس ديوان رئاسة مجلس الوزراء رقم ٧/ب/٤٦٤٠٤، وتاريخ ١٤٢٤/٩/٢٨هـ، القاضي بالموافقة على نقل اختصاصات اللجنة الدائمة للتجارة الإلكترونية من وزارة التجارة والصناعة إلى هيئة الاتصالات وتقنية المعلومات.

- الأمر السامي رقم ٧/ب/٣٣١٨١، وتاريخ ١٤٢٤/٧/١٠هـ، المتضمن وضع خطة لتقديم الخدمات والمعاملات الحكومية إلكترونياً من قبل وزارة الاتصالات وتقنية المعلومات.

- القرار رقم ٧/ب/٢١٣٤٦، وتاريخ ١٤٢٤/٥/٦هـ، القاضي بإحالة مشروع نظام التعاملات الإلكترونية إلى وزارة الاتصالات وتقنية المعلومات بصفة عاجلة وإعداد مشروع نظام جديد.

وقد تمثل دور مدينة الملك عبد العزيز في حينها بتأسيس وتشغيل المركز الوطني للتصديق الرقمي، المعروف بـ Root CA، وتحديد متطلبات مراكز 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 مراكز التصديق.

يبين الشكل رقم ٦ الهيكل العام المقترح في حينه لمراكز التصديق في المملكة وارتباطها بالمركز الوطني.



الشكل رقم ٦: الهيكل العام لمراكز التصديق (مقترح)

وظيفة المركز الوطني للتصديق الرقمي Root CA

ما الفائدة من وجود المركز الوطني للتصديق في حال وجود عدد من مراكز التصديق الخاصة، كمركز التصديق التابع لمؤسسة النقد العربي السعودي، ومركز التصديق التابع لشركة أرامكو السعودية وذلك الخاص بشركة الاتصالات السعودية؟ ما الدور الذي يلعبه المركز الوطني للتصديق في دعم الثقة بين المتعاملين؟

إن وجود المركز الوطني للتصديق في غاية الأهمية وذلك للأسباب التالية:

- واجهت العديد من الدول التي لم تقم بإنشاء مركز وطني للتصديق صعوبات كبيرة فيما يخص قانونية التعاملات التي تتم في غياب جهة رسمية، كمدى المسؤولية التي تتحملها مراكز التصديق، وسلامة الإجراءات المتبعة في إصدار الشهادات الرقمية، وحقوق المستخدمين وخصوصيتهم، وغيرها من الأمور. كما إن عدم وجود مركز وطني للتصديق يؤدي إلى الاعتماد على عمليات التصديق المتبادل (Cross Certification) بين مراكز التصديق والذي يعتبر بالغ التعقيد.

- لكي يتم التعامل الإلكتروني بموثوقية تامة فمن الواجب أن يكون هناك جهة عليا تقوم بالمصادقة على مراكز التصديق نفسها. كيف يمكن لجهة خارجية (أو داخلية)، على سبيل المثال، مطابقة توقيع شخص حصل على شهادته الرقمية من مركز للتصديق غير معروف لديها؟ وعلى أي أساس يمكن لتلك الجهة الثقة في سلامة إجراءات منح الشهادة الرقمية التي يقوم بها مركز التصديق هذا؟ إن دور المركز الوطني يتمثل في المصادقة على مراكز التصديق وما يصدر منها من شهادات، بحيث تكون هناك جهة واحدة للدولة يمكن عن طريقها التأكد من صحة المفاتيح العامة للمستخدمين.

- إن وجود مركز وطني للتصديق من شأنه أن يساعد على التوافق والتطابق الفني والإداري للأعمال التي تقوم بها مراكز التصديق، الأمر الذي يضفي جواً من التناسق والتلاؤم فيما بين تلك الجهات، ويساعد في عملية توافق الشهادات الصادرة من مراكز التصديق المختلفة. كما إن بإمكان المركز الوطني فرض مواصفات ومقاييس عامة تلتزم بها جميع الأطراف المعنية لتحقيق الصالح العام.

هنا يجب تصحيح بعض المفاهيم الخاطئة فيما يخص دور المركز الوطني للتصديق ودوره في الأمن والخصوصية:

- لا يقوم المركز الوطني بالاحتفاظ بالمفاتيح الخاصة (Private Keys) للأفراد ولا لمراكز التصديق، حيث إن عمله الحقيقي لا يتطلب التعامل مع المفاتيح الخاصة، بل إنه يقوم فقط بالمصادقة – المباشرة أو غير المباشرة - على كون المفتاح العام للشخص أو الجهة ملكاً لذلك الشخص أو تلك الجهة.

- لا يقوم المركز الوطني بإصدار المفاتيح الخاصة سواء للأفراد أو مراكز التصديق، لذا فإن المفاتيح الخاصة لا تمر عن طريق المركز على الإطلاق.

- لا يستطيع المركز الوطني فك التشفير عن أي بيانات مشفرة من جهة أخرى، لكونه لا يملك المفاتيح اللازمة لفك التشفير. هناك حالات يمكن من خلالها فك التشفير من قبل جهة أخرى، وذلك باستخدام طريقة الحفظ لدى جهة مختصة، والتي تعرف بطريقة Escrow، حيث يقوم الشخص أو مركز التصديق طواعية بحفظ المفتاح الخاص به لدى تلك الجهة، أو السماح للجهة بالحصول على المفتاح بطريقة أو بأخرى، وذلك لاسترجاعه في حال فقدان المفتاح الذي بحوزته. إلا أن ذلك يتم حسب رغبة المستخدم وموافقته على ذلك.

- لا يتطلب إصدار الشهادات الرقمية ربط المركز الوطني بشبكة حاسب آلي، أو ربطه عن طريق الإنترنت، عدا قاعدة المعلومات المستخدمة في التحقق من التواقيع الإلكترونية ومعرفة الشهادات الملغاة فيجب أن تكون متاحة على الإنترنت بشكل دائم. ولكن هذه القاعدة ليس بالضرورة أن تتواجد في مقر المركز، بل يمكن أن تدار من قبل مزود خدمة مختص أو أن توضع في أي مكان مستقل بعيداً عن أجهزة إصدار الشهادات. تذكّر بأن حاجة المستخدم لخدمات المركز الوطني تكمن في الحاجة إلى الحصول على المفتاح العام للمركز لاستخدامه في التحقق من صحة الشهادات الرقمية الصادرة من مراكز التصديق المعترف بها من قبل المركز. وبإمكان المستخدم الحصول على المفتاح العام للمركز من المركز نفسه أو من قبل جهة يثق بها، أو بأي طريقة تقليدية، كأن يستلمه المستخدم بوساطة قرص مرن، أو يطلبه بالبريد العادي، أو يجده في إحدى الصحف المحلية.

مصطلحات

1	البنية التحتية للمفاتيح العامة	Public Key Infrastructure
2	مركز التصديق الرقمي	Certification Authority (CA)
3	المركز الوطني للتصديق الرقمي	National Root CA
4	سياسة الشهادة الرقمية	Certificate Policy
5	إجراءات التصديق الرقمي	Certification Practice Statement
6	مركز تسجيل الشهادات الرقمية	Registration Authority
7	التحقق من صحة الشهادة الرقمية	Certificate Verification
8	سجل الشهادات الملغاة	Certificate Revocation List
9	بروتوكول التحقق المباشر من وضع الشهادة	Online Certificate Status Protocol (OCSP)
10	التوقيع الرقمي	Digital Signature
11	التوقيع الإلكتروني	Electronic Signature
12	الهوية	Identification
13	التحقق من الهوية	Authentication
14	عدم الإنكار	Non-repudiation
15	السرية	Confidentiality
16	الخصوصية	Privacy
17	التشفير	Encryption
18	فك التشفير	Decryption
19	التصديق المتبادل	Cross Certification

مراجع

1. William Stallings, Cryptography and Network Security, Principles and Practice, second edition, Prentice Hall, 1999
2. Kapil Raina, PKI Security Solutions for the Enterprise, Wiley Publishing Inc, 2003.
3. General Accounting Office (USA), E-Authentication Handbook for Federal Government Agencies, July 2004. http://www.cio.gov/eauthentication
4. General Accounting Office (USA), Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology, Feb. 2001, http://www.gao.gov/
5. United Nations, UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001.
6. United Nations, UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996.
7. U.S. General Services Administration, GOVERNMENT SMART CARD HANDBOOK, Feb. 2004,