حياتك.. أسرارها في مفتاح

تعد المفاتيح العامة إحدى ركائز التعامل الإلكتروني وتحد من استخدام الخطابات الورقية بفضل التوقيع الإلكتروني.

• الرياض: فتحي سمير

أكد د.فهد الحويماني، رئيس المركز الوطني للتصديق الرقمي، أن بنية المفاتيح العامة تعد أهم الركائز الأساسية في تطبيق الحكومة الإلكترونية، بفضل البيئة الآمنة التي توفرها في مختلف التعاملات والمراسلات، والموثوقية العالية للتشفير الذي يحمي الرسائل من المتطفلين.

والمفتاح العام هو مفتاح تشفير رقمي لكل شخص لديه شهادة رقمية، حيث يدرج هذا المفتاح داخل الشهادة الرقمية التي تحتوي كذلك على مُعرف معين للشخص «مثل بريده الإلكتروني أو اسمه أو رقم سجله المدني»، ويصادق على هذه الشهادة الرقمية من قبل مركز تصديق رسمي. لذا فإن الشهادة الرقمية تستخدم لتوجيه اتصال مشفر لصاحب الشهادة حسب المُعرف الظاهر في الشهادة. فإذا أردت إرسال بريد إلكتروني مشفر لشخص ما، تقوم بجلب الشهادة الرقمية لصاحب البريد الإلكتروني ومن ثم استخدام المفتاح العام المخزن فيها لتشفير الرسالة الموجهة إلى الشخص.

أما المفتاح الخاص فهو المفتاح المقابل للمفتاح العام، لكنه غير معلن، ولا يمكن الاطلاع عليه، كونه مخزنًا في بطاقة ذكية في حوزة المستخدم أو في قطعة فلاش في جيبه، ويستخدم لفك التشفير عن الرسالة الموجهة لصاحب المفتاح. إضافة إلى ذلك فإن المفتاح الخاص يستخدم لإجراء التوقيع الإلكتروني لرسالة أو وثيقة، ومن ثم يتم التحقق من صحة التوقيع باستخدام المفتاح العام للشخص. أي أنك تقوم بكتابة رسالتك الإلكترونية، ثم تستخدم مفتاحك الخاص لتشفير الرسالة التي بالتالي لا يمكن فك تشفيرها إلا بوساطة المفتاح العام التابع لك. وبما أن مفتاحك العام مصادق عليه من مركز تصديق معتمد، فبالإمكان التأكد «أو مطابقة التوقيع» من أنك أنت من قام بإرسال الرسالة.

وما يعرف بالبنية التحتية للمفاتيح العامة هو عبارة عن منظومة أمنية متكاملة لتوفير بيئة مناسبة للتعامل الآمن عبر شبكات الحاسب الآلي باستخدام الشهادة الرقمية، أي أن هذه البنية عبارة عن نظام متكامل لإدارة مفاتيح التشفير والتوقيع من خلال الشهادة الرقمية.

بدايات وتطور

بدأت فكرة المفاتيح العامة في منتصف السبعينيات، وأعدت في حينه ثورة كبيرة في عالم التشفير، حيث أصبح بالإمكان، ولأول مرة، قيام جهتين بتبادل مفتاح سري فيما بينهما من خلال شبكة مفتوحة ودون معرفتهما المسبقة. ولم يبدأ التطبيق الفعلي لهذه التقنية إلا في التسعينيات، حيث بدأت مواقع الإنترنت تستخدم الشهادات الرقمية لإثبات هوية الموقع الإلكتروني، ولتمكين الموقع من تبادل المفتاح السري مع متصفح الإنترنت لزائر الموقع «كمواقع البنوك والمحال التجارية».

بعد ذلك بدأت تقنية المفاتيح العامة بالانتشار، وقامت بعض الجهات الحكومية في المملكة وبعض الشركات الكبرى «مثل شركة أرامكو وشركة الاتصالات السعودية» بتجربة هذه التقنية قبل عدة سنوات، وبدأت وزارة الاتصالات وتقنية المعلومات ببناء القواعد الأساسية لهذه الخدمة والتي تشتمل إلى جانب التجهيزات الفنية والإنشائية، إصدار نظام للتعاملات الإلكترونية لضبط التعاملات والتوقيعات الإلكترونية وتنظيمها وتوفير إطار نظامي لها بما يؤدي إلى تحقيق ما يلي:

د. فهد الحويماني
مدير المركز الوطني للتصديق الرقمي

- إرساء قواعد نظامية موحدة لاستخدام التعاملات والتوقيعات الإلكترونية، وتسهيل تطبيقها في القطاعين العام والخاص، بوساطة سجلات إلكترونية يعول عليها.
- إضفاء الثقة في صحة التعاملات والتوقيعات والسجلات الإلكترونية وسلامتها.
- تيسير استخدام التعاملات والتوقيعات الإلكترونية على الصعيدين المحلي والدولي، للاستفادة منها في جميع المجالات، كالإجراءات الحكومية، والتجارة، والطب، والتعليم، والدفع المالي الإلكتروني.
- إزالة العوائق أمام استخدام التعاملات والتوقيعات الإلكترونية.
- منع إساءة الاستخدام والاحتيال في التعاملات والتوقيعات الإلكترونية.

المركز الوطني للتصديق الرقمي

تم إنشاء المركز الوطني للتصديق الرقمي بناء على توصية من اللجنة الدائمة للتجارة الإلكترونية، وتمت الموافقة السامية بموجب الأمر السامي رقم٧/ب/٩٣٧٨، ومن ثم نصت المادة السادسة عشرة من نظام التعاملات الإلكترونية الصادر بتاريخ ١٤٢٨/٣/٨هـ على أن ينشأ المركز الوطني للتصديق الرقمي في وزارة الاتصالات وتقنية المعلومات.

ويتمثل دور المركز الوطني للتصديق الرقمي في المصادقة على مراكز التصديق المنتشرة في قطاعات الدولة والقطاع الخاص وإضفاء صبغة قانونية لها ولتعاملاتها، وذلك من خلال إصدار الأنظمة والسياسات الخاصة بالشهادة الرقمية وإجراءات التصديق الرقمي، وكذلك التحقق من سلامة الإجراءات المتبعة في إصدار الشهادات الرقمية وحقوق المستخدمين وخصوصيتهم. كما أن وجود المركز الوطني يغني عن الاعتماد على عمليات التصديق المتبادل (Cross Certification) التي تعد بالغة التعقيد وتحتاج إلى تنسيق متواصل بين الجهات المصدرة للشهادات الرقمية.

تحديات

مر إنشاء المركز الوطني للتصديق الرقمي بعدة مراحل، ولكل مرحلة أهدافها وتحدياتها، فالمرحلة الأولى كانت إعداد الاستراتيجية العامة للبنية التحتية للمفاتيح العامة في المملكة، وكان الاهتمام فيها منصبًا على إعداد خطة استراتيجية منسجمة مع آخر ما توصلت إليه التقنية في هذا المجال، والاطلاع على بعض التجارب السابقة والنادرة آنذاك لدى بعض الدول المتقدمة، ورسم الأهداف الاستراتيجية

للمشروع وربطها بالمشاريع والمبادرات التنموية الأخرى ذات الأهمية نفسها في المملكة على مستوى إيجاد بيئة تعاملات إلكترونية آمنة مثل مشاريع الحكومة الإلكترونية وغيرها، وذلك لتحقيق التكامل المطلوب للخدمات، وقد تزامنت تلك المرحلة مع العمل على إيجاد بيئة نظامية وتشريعية فاعلة، حيث تم إحداث التعديلات اللازمة في بعض الأنظمة واللوائح النظامية على مستوى المملكة، وذلك بإعداد نظام التعاملات الإلكترونية المتضمن لنظام التواقيع الإلكترونية وإقراره من مجلس الوزراء، وإعداد نظام خاص للجرائم الإلكترونية وإقراره كذلك مع اللوائح التفصيلية المصاحبة لجميع الأنظمة، ويأتي التحدي هنا بإعداد نظام جديد وما يصاحبه من عمليات الدراسة والبحث والاستشارة وتكوين لجان العمل للمراجعة والاعتماد.

وجاءت بعد ذلك مراحل إعداد المواصفات الفنية والأمنية لمركز البيانات الذي يستضيف هذه البنية والتأكد من توافق مواصفات البناء مع المواصفات والمقاييس المعمول بها عالميًا، حيث تضمن ذلك الاستعانة بعدد من بيوت الخبرة العالمية، كما أن مرحلة إعداد المواصفات الفنية للتقنية أو المنتج الذي سيستخدم لإدارة البنية التحتية للمفاتيح العامة تعد من أعقد مراحل المشروع وتطلبت المرحلة ضرورة ضمان استقطاب منتج ذي مواصفات فنية وأمنية عالية ويتسم بالمرونة والاعتمادية العالية وقابلية تطويع المنتج النهائي أو الشهادة الرقمية المصدرة منه للتوافق مع عدد كبير من البرامج وأنظمة التشغيل المنتشرة. وقد تطلب ذلك عمل الدراسات والبحوث اللازمة للعديد من المواصفات والمقاييس العالمية الحديثة المستخدمة في هذه البنية مثل البحث عن خوارزميات التشفير المستخدمة، ومدى صلاحياتها ونجاعتها في تحمل محاولات الكسر والاختراق.

أما المرحلة الأخيرة والمهمة في عمر المشروع فهي مرحلة طرح وتقديم الخدمة «إصدار الشهادات الرقمية»، وتبرز تحديات هذه المرحلة في تقديم الخدمة بالشكل المناسب الذي يضمن فاعلية وسهولة تقديم الخدمة لمختلف قطاعات المستفيدين في المملكة من أفراد ومنظمات حكومية وتجارية وفق النموذج البنيوي الخاص بالمركز، وخلق فرص استثمار لدعم المنتج كإدراج شركات القطاع الخاص لتسويق خدمات الشهادات الرقمية وتقديمها بشكل عصري وجذاب مع الحفاظ على مستويات عالية من الموثوقية والمصداقية والأمان المصاحبة لهذه البنية عادة، وذلك من خلال فرض إجراءات وسياسات أمنية صارمة على مقدمي الخدمة.

الحكومة الإلكترونية

تعد بنية المفاتيح العامة هي إحدى ركائز التعامل الإلكتروني وعلى أساسها تقوم الحكومة الإلكترونية، وتقوم بأداء عدد من الوظائف منها:

- 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 بعضًا 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.

لذا فهي تستخدم في التحقق من هويات المستخدمين عند الدخول إلى أنظمة الحاسب والإنترنت، والحد من الخطابات الورقية في التعاملات الإلكترونية، وذلك بتفعيل التوقيع الإلكتروني، ومنع المتطفلين والعابثين من الاطلاع على وثائق الآخرين وتعاملاتهم من خلال آلية التشفير المتوافرة في بنية المفاتيح العامة والمفاتيح السرية، ويستفاد منها بشكل عام في جميع الأنظمة الإلكترونية كالحكومة الإلكترونية والتعليم عن بعد والطب الاتصالي والتجارة الإلكترونية وغيرها.

علاقات دولية

وحول علاقة المركز بالمنظمات والجهات الدولية الأخرى، أوضح د.فهد الحويماني أن المركز الوطني يعمل وفقًا لعدد من المواصفات العالمية في هذا المجال، معظمها صادر من قبل الاتحاد الدولي للاتصالات وفريق المواصفات التابع لمنظمة الإنترنت (IETF)، وكذلك المنظمة الأوروبية لمواصفات الاتصالات، وغيرها. كذلك هناك لقاءات تنسيقية وتوعوية تتم مع بعض المنظمات الإقليمية مثل منظمة «الإسكوا» المعنية بتطوير الاتصالات وتقنية المعلومات في المنطقة، وكذلك المنظمة العربية لتكنولوجيات الاتصال التابعة لجامعة الدول العربية، التي بادرت مؤخرًا بإطلاق المنتدى العربي للبنية التحتية للمفاتيح العامة.

وعن مدى إمكانية استفادة مختلف الجهات والأشخاص من تقنيات المفاتيح العامة، أصدر المركز مؤخرًا عددًا من الشهادات الرقمية من نوع SSL Certificates وذلك من خلال مقدم خدمة الشهادات الرقمية الخاص بالمركز الوطني للتصديق الرقمي، وبإمكان بقية الجهات الحكومية الراغبة في الحصول على شهادات رقمية لاستخدام موظفيها بغرض التشفير والتوقيع الرقمي، التقدم لدى المركز لإنهاء كل إجراءات الحصول على رخصة مقدم خدمة شهادات رقمية بغرض الحصول على برنامج التسجيل الخاص بالشهادات الرقمية كي يتمكنوا من استخدامه داخل جهاتهم لإصدار الشهادات المرغوب فيها لموظفيهم، أما بالنسبة للقطاع الخاص والأفراد، فإن المركز بصدد طرح تقديم خدمة الشهادات الرقمية من خلال مراكز تسجيل تجارية، حيث يجري التنسيق حاليًا بين المركز وعدة جهات تجارية بهدف معرفة المتطلبات الرئيسة لتقديم الخدمة بهذا الشكل ورسم نموذج بنيوي كامل قبل إطلاق الخدمة تجاريًا، ويشمل ذلك قيام المركز بنشر مفاهيم البنية التحتية للمفاتيح العامة وفوائدها من خلال تنظيم ندوات وورش عمل ومحاضرات إضافة إلى عزم المركز طرح وثيقة طلب مرئيات العموم في الصحف المحلية للاستفادة من الآراء والأفكار من جميع الفئات المستهدفة حول تقديم هذه الخدمة تجاريًا.

خطط مستقبلية

وكشف رئيس المركز الوطني للتصديق الرقمي عن الخطط التي يجري العمل عليها في الفترة الحالية، ومن ضمنها العمل مع أحد أكبر بيوت الخبرة في مجال أمن المعلومات لنيل الاعتراف العالمي بشهادة مركز التصديق الجذري، وهو المركز الأعلى سلطة ضمن هيكل المركز الوطني، ويتم ذلك من خلال إخضاع المركز وكل موارده من أجهزة وبرامج وسياسات وإجراءات تشغيل إلى عمليات مراجعة وتدقيق وتقييم وتحسين سنوي مستمر، وسيكون هذا الاعتراف على مستوى التطبيقات العالمية المشهورة من برامج تصفح الإنترنت وكل التطبيقات الأخرى التي تعتمد عمليات الثقة والتصديق فيها على الاعتراف بشهادات مراكز التصديق الرئيسة التي أصدرت شهادات المستخدمين، إضافة إلى ذلك يأمل المركز أن يشارك القطاع الخاص والمؤسسات البرمجية الكبرى والمتوسطة الأجنبية منها أو المحلية في الإسهام في إنجاح استخدام الشهادات الرقمية على مستوى التطبيقات، وهذا من أهم عوامل نجاح تطبيق البنية التحتية للمفاتيح العامة، وذلك عن طريق الاهتمام بإنتاج التطبيقات والبرامج المتوافقة مع استخدام الشهادات الرقمية في عمليات التوقيع الرقمي والمطابقة والتصديق، وإعطاء الصلاحيات كي يسهم ذلك في تعزيز استخدام الشهادات الرقمية، ما سيؤثر بشكل ملحوظ في مستوى الأمان والسرية على التعاملات الإلكترونية من خلال هذه التطبيقات المختلفة.

تسهم في إرساء القواعد لاستخدام التعاملات الإلكترونية، وتسهيل تطبيقها في القطاعين العام والخاص

تقديم خدمة الشهادات الرقمية من خلال مراكز تسجيل تجارية للقطاع الخاص والأفراد قريبًا

ندوة المفاتيح العامة فرصة مهمة للتعرف على بنية المفاتيح العامة والاستثمار فيها