التحكم في توثيق وسرية المعلومات الإلكترونية
على شبكات أتصالات الحكومة المصرية

قدمت شبكة المعلومات العالمية " الإنترنت " لمجتمعنا ما يمكن إنـــجازه في عصر المعلومات كما أن التزايد السريع أصبح سمة الطلب على الوصول للمعلومات وعلى التجارة الإلكترونية فضلا على أن الطلبات تتزايد من جميع عناصر المجتمع بما في ذلك البنوك ورجال الصناعة ومؤسسات تقديم الخدمات والحكومات المحلية والمؤسسات التعليمية.

التفاعلات اليومية في مجال الأعمال والمجالات الاجتماعية تتم من خلال المناقشات وجها لوجه والاتصالات التليفونية والمراسلات المكتوبة وكل من هذه الوسائل تتيح التعرف على الشخص أو الطرف الآخر من وجهه أو صوته أو توقيعه المكتوب وهذا التعرف هو ما يسمح بالثقة في الاتصال.

آلا أنه في عصر المعلومات سيتم إحلال هذه الأعمال الشخصية ببدائل مقابلة رقميـــة يمكن أن نعتمد عليها حيث ستتم الاتصالات في مجال الأعمال والمجالات الحكومية من خلال عمليات الإرسال الإلكتروني والتي ستفصل بين الرسالة وبين الشخص مما يؤدى إلى فقد الثقة التي كان مصدرها السلام باليد أو التوقيع على وثيقة.

وفى نفس الوقت فأن الاعتمـــاد المتزايد للحكومات ومكونات المجتمع على نظم المعلومات في هـذه البيئة الجديدة يعرض كلا من المواطنين ومؤسساتهم ومعلوماتهم لمخاطر لم يسبق لها مثيل.

كان يجب إضفاء خصائص معينة على نظم المعلومات والبنية الأساسية الشاملة للمعلومات ومن التجارة الإلكترونية بحيث يمكن التغلب على هذه المخاطر مع توفير السبل الموثوق فيها لتحديد المستخدمين.

يمكن لأنظمة الشفرات الحديثة أن تستجيب لهذه الاحتياجات إذ يمكن استخدامها للتوقيع رقميا على الاتصالات والمستندات الإلكترونية بحيث يثق المستلم في أن الرسالة التي استلمها ليس لها مصدر غير الراسل الحقيقي فضلا عن أن التشفير أداة هامـــة وحاسمة لحماية ســـرية الاتصالات السلكية والإلكترونية والبيانات المخزونة.

أدركت الحكومة الحاجة القومية الملحة لتشجيع عمليـــات تطوير وتبنى واستخدام المنتجـــات الشفرية الحديثة عالية السرية وتوفير تكنولوجيا التوقيع الالكتروني الرقمي التي تحقق المعايير القياسية العالمية وتتلاءم للاستخدام داخل المجتمع المصري.

كما أدركت الحكومة أن غياب البنية الأساسية لإدارة مفاتيح الشفرة داخل المجتمع المصري والحكومة يعوق استخدام التشفير وتوفير تكنولوجيا التوقيع الالكتروني الرقمي وبالتالي التجارة الإلكترونية المتوقعة .

كما أن حماية وسرية المعلومات المرسلة عبر شبكات الاتصال تعتبر من الأمور الهامة والحيوية لكثير من المؤسسات الحكومية والأنشطة الاقتصادية في هذه الأيام .

وأيضا أفراد الحكومة المصرية لا يمكنهم تشفير الرسائل والتوقيع الالكتروني عليها بدون مفاتيح شفرة وعلى ذلك أدركت الحكومة الحاجة لأساليب قياسية علمية تحقق السرية العالية لإنشاء المفاتيح من خلال برامج خاصة وتخزينها وتداولها بين المستخدمين .

وقد قامت وزارة المالية بتحديد النموذج الأمثل لتنفيذ البنية التحتية لشفرة المفاتيح العامة للتوقيع الالكتروني ووضع المعايير المنظمة لها، كما قامت الوزارة باختيار وتعين وتدريب الكوادر اللازمة للتجهيز والتشغيل.

إن الأفراد في واقع الأمر يعرفون الفرق بين أصول المستندات وصورها ومصداقية كثير من الوثائق القانونية والمالية وغيرها يعتمد وبصورة أساسية تماماً على وجود أو عدم وجود التوقيع الرسمي للشخص المسئول " التوقيع باليد " وعلى هذا فيجب أن نجد حلاً لهذه المشكلة المتعلقة باستبدال الرسائل والوثائق المكتوبة بالحبر وخط اليد بالرسائل والوثائق الموجودة والمخزنة على الحاسبات. ولعلنا نستطيع إدراك أن عملية استنباط بديل للتوقيعات اليدوية هي مشكلة صعبة، فالمطلوب أساساً هو عمل نظام عن طريقة تتمكن الجهة أو الفرد من إرسال رسالة موقعة إلى طرف أخر وبحيث تستوفى الشروط التالية:

١. يتمكن متلقي الرسالة من التحقق من هوية الراسل.

٢. لا يمكن للراسل أن يتنكر من هذه الرسالة فيما بعد.

والشرط الأول مطلوب على سبيل المثال في الأنظمة المالية ، فعندما يقوم الحاسب الشخصي لاحد العملاء بإرسال رسالة إلى الحاسب في البنك يأمره بشراء طن من الذهب ، فأن حاسب البنك يحتاج لأن يتأكد بأن هذا الحاسب الذي يعطى الأوامر يتبع الشركة التي لها حساب في البنك وينبغى أن تتحمل تكاليف الشراء، أما الشرط الثاني فهو مطلوب لحماية البنك ضد الاحتيال والخديعة، ولشرح ذلك نفترض أن البنك بعد أن أشترى طن الذهب، انخفض سعره وبشكل حاد ، وهنا قد يكون العميل غير أمين ويقاضى البنك مدعياً بأنه لم يقم بإصدار أية أوامر لشراء الذهب ، وعندما يقوم البنك بتقديم الرسالة في المحكمة فأن العميل ينكر أنه لم يقم بإرسالها. ولعله من المدهش حقاً أن علوم الشفرة التي يتم

استخدامها لضمان سرية المعلومات يمكن استخدامها أيضا لضمان تصديق أو مصداقية المستندات من خلال تكنولوجيا التوقيع الالكترونى الرقمى لسلطة التصديق الالكترونى الحكومية Gov-CA بوزارة المالية.

كما إن حماية وسرية المعلومات المرسلة عبر شبكات الاتصال تعتبر من الأمور الهامة والحيوية لكثير من المؤسسات الحكومية والأنشطة الاقتصادية في هذه الأيام وأن الزيادة المطردة في الاعتماد على شبكات الحاسبات وخصوصاً شبكة الإنترنت الدولية جعل من أداة التشفير لحماية المعلومات وأداة التوثيق للتأكد من مصدر المعلومات التي يتم استقبالها شئ في غاية الأهمية بحيث يصعب الاستغناء عنهما في مثل هذه البيئة الجديدة، و إن كثير من المؤسسات الحكومية والاقتصادية تهدف إلى حماية معلوماتها الحساسة ضد أي تهديد أو اختراق وبالتالى وقبل أدراك مواصفات نظام التأمين المناسب للاستخدام على شبكات الحكومة المصرية.. يجب علينا تحديد التهديدات الأساسية التي تتعرض لها الرسائل على هذه الشبكات والتي نستطيع أن نلخصها في النقاط الآتية:

١- التصنت والإطلاع على كامل المعلومات التي تحويها الرسائل المتبادلة عبر الشبكة .

٢- ممارسة الغش والخداع (إرسال رسائل مزيفة) بهدف الإرباك وتحطيم الثقة.

٣- حذف أو تعديل أو تأخير الرسائل وهى في طريقها إلى المستقبل الحقيقي.

٤- قيام الراسل الحقيقي من التنكر من أنه أرسل المعلومات التي تحويها رسائله بهدف التنصل من مسئولياته.

٥- مشكلة توزيع مفاتيح شفرة التوقيع الالكتروني على الشبكة.

وستقوم منظومة سلطة التصديق الالكتروني الحكومية بالتغلب على التهديدات السابقة من خلال استخدام تكنولوجيا بنية المفتاح العام المتكاملة عالية السرية في أنتاج شفرات التوقيع الالكتروني الحكومية والتى تحقق للحكومة المصرية نقاط القوة التى نستطيع تلخيصها فى النقاط التالية :

١. استخدام تشفير عالي السرية لحماية المعلومات من آي شخص غير مصرح له الإطلاع على هذه المعلومات .

٢. يستطيع الراسل إثبات نفسه لمستقبل الرسالة إثباتاً علمياً والتي من خلالها تتوفر الثقة الكاملة في المعلومات التي يتم استقبالها .

٣. يتأكد المستقبل من صحة وتمام محتويات الرسالة التي تم استقبالها وأنه لم يطرأ عليها أي تغيير أو تعديل أثناء رحلتها على شبكة الاتصال .

٤. **يتأكد و يثق المستقبل من أن الراسل لا يمكن له أن يتنكر من المعلومات التي تحويها رسائله. بمعنى آخر أن ما يتم استقباله من معلومات يكون إثبات رسمي موثق على الراسل بضمان الحكومة المصرية والقانون المصري وسلطة التصديق الالكتروني الحكومية .**

٥. **عدم القدرة على تزوير التوقيع الالكتروني لأحد الرسائل أى أن مايتم الحصول علية هو توقيع الكتروني رقمى غير قابل للتزوير .**

٦. **التأكد من التوقيت الفعلي لتشفير الرسالة والتي يتم الحصول علية من سلطة التصديق الالكتروني الحكومية لحظيا وقت التوقيع الالكتروني على الرسالة قبل إرسالها (البصمة الزمنية الموثقة).**