الأمم المتحدة
A/CN.9/630/Add.1
الجمعية العامة
Distr.: General
25 April 2007
Arabic
Original: English

لجنة الأمم المتحدة للقانون التجاري الدولي
الدورة الأربعون
فيينا، ٢٥ حزيران/يونيه – ١٢ تموز/يوليه ٢٠٠٧

الأعمال التي يمكن الاضطلاع بها مستقبلاً في مجال التجارة الإلكترونية

وثيقة مرجعية شاملة عن العناصر اللازمة لإنشاء إطار قانوني مؤات للتجارة الإلكترونية: نموذج فصل عن استخدام طرائق التوثيق والتوقيع الإلكترونية على الصعيد الدولي

مذكّرة من الأمانة*

إضافة

يحتوي مرفق هذه المذكّرة على جزء (الجزء الأول، الفصل الأول، القسمين باء وجيم) من نموذج فصل من وثيقة مرجعية شاملة، يتناول المسائل القانونية ذات الصلة باستخدام طرائق التوثيق والتوقيع الإلكترونية على الصعيد الدولي.

* تأخرت أمانة لجنة الأمم المتحدة للقانون التجاري الدولي في تقديم هذه الوثيقة بسبب نقص الموظفين.

250507 V.07-82778 (A)

المرفق

المحتويات

	الفقرات	الصفحة
باء- الطرائق الرئيسية في التوقيع والتوثيق الإلكترونيين	١	٣
١- التوقيعات الرقمية التي تعتمد على الترميز بالمفتاح العمومي	٢-٢٩	٣
٢- القياسات الحيوية	٣٠-٤٠	١٧
٣- كلمات السر والطرائق الهجينة	٤١-٤٢	٢٠
٤- التوقيعات المستنسخة بالمسح التصويري والأسماء المطبوعة	٤٣-٤٤	٢١
جيم- إدارة شؤون الهوية الإلكترونية	٤٥-٥٤	٢٢

الجزء الأول

طرائق التوقيع والتوثيق الإلكترونية

[...]

أولا- تعريف التوقيع والتوثيق الإلكترونيين وطرائقهما

[...]

باء- الطرائق الرئيسية في التوقيع والتوثيق الإلكترونيين

١- لأغراض هذه المناقشة، تُبحث أربع طرائق رئيسية للتوقيع والتوثيق وهي: التوقيع الرقمي؛ وطرائق القياس الحيوي؛ وكلمات السر والطرائق الهجينة؛ والتوقيعات المستنسخة بالمسح التصويري أو المطبوعة بالآلة.

١- التوقيعات الرقمية التي تعتمد على الترميز بالمفتاح العمومي

٢- "التوقيع الرقمي" هو الاسم الذي يُطلق على التطبيقات التكنولوجية التي تستخدم نظم الترميز غير المتناظرة، ويشار إليها أيضا بنظم الترميز بالمفتاح العمومي، من أجل كفالة موثوقية الرسائل الإلكترونية وضمان سلامة محتويات هذه الرسائل. ويظهر التوقيع الرقمي في طرائق مختلفة كثيرة، منها التوقيعات الرقمية بتقنية كشف التزوير والوقف الفوري، والتوقيع المعمَّى، والتوقيعات الرقمية التي لا يمكن إنكارها.

(أ) المفاهيم التقنية والمصطلحات

'١' الترميز

٣- تُنشأ التوقيعات الرقمية ويُتحقق من صحتها باستخدام الترميز، وهو فرع من الرياضيات التطبيقية يُعنى بتحويل الرسائل إلى صيغ شكليّة تبدو غير مفهومة ثم إعادتها إلى صيغتها الشكلية الأصلية. وتستخدم التوقيعات الرقمية ما يُعرف باسم الترميز بالمفتاح العمومي، الذي كثيرا ما يستند إلى استخدام دوالّ خوارزمية لإنتاج "مفتاحين" مختلفين ولكنهما مترابطان رياضيا (والمفاتيح هي أعداد ضخمة يُحصل عليها باستخدام سلسلة من

الصيغ الرياضية المطبقة على أعداد أولية).[1] ويُستخدم أحد هذين المفتاحين في إنشاء توقيع رقمي أو في تحويل بيانات إلى صيغة شكلية غير مفهومة في ظاهرها، ويستخدم المفتاح الثاني للتحقق من صحة توقيع رقمي أو إعادة رسالة البيانات إلى صيغتها الشكلية الأصلية.[2] وكثيرا ما يشار إلى أجهزة وبرامجيات الحاسوب التي تستخدم مثل هذين المفتاحين بعبارة جامعة هي "نظم ترميز" (cryptosystems) أو بعبارة أكثر تحديدا هي "نظم ترميز غير متناظرة" "asymmetric cryptosystems" حيث تعتمد على خوارزميات غير متناظرة.

'٢' مفاتيح الترميز العمومية والخصوصية

٤- يُستخدم مفتاح يكمل المفتاح الآخر للتوقيعات الرقمية يسمى "المفتاح الخصوصي"، وهو المفتاح الذي لا يستخدمه إلا الموقّع في إنشاء توقيع رقمي، وينبغي أن يُحافَظ على سرِّيته، في حين يكون "المفتاح العمومي" الآخر عادة معروفا على نطاق أوسع ويستخدمه طرف معوِّل في التحقق من صحة التوقيع الرقمي. ويمكن أن يُحفظ المفتاح الخصوصي على "بطاقة ذكية" أو أن يتاح الوصول إليه عن طريق رقم لتحديد الهوية الشخصية (PIN)، أو عن طريق أداة قياس حيوي لتحديد الهوية، وذلك مثلا عن طريق التعرّف على بصمة الإبهام. وإذا احتاج عدد كبير من الناس إلى التحقق من صحة التوقيع الرقمي للموقّع، فيجب إتاحة المفتاح العمومي لهم جميعا أو توزيعه عليهم، وذلك مثلا بإلحاق شهادات التصديق بالتوقيع أو بواسطة طرق أخرى تضمن ألا يحصل على الشهادات ذات الصلة إلا الأطراف المعوِّلة والأطراف التي عليها أن تتحقق من التوقيعات. وعلى الرغم من أن زوج المفاتيح مترابط رياضيا، فإنه إذا ما صُمّم ونُفّذ نظام ترميز لامتناظر بطريقة مأمونة أصبح في حكم المستحيل فعلا اشتقاق المفتاح

---

(1) جدير بالذكر مع ذلك أن مفهوم الترميز بالمفتاح العمومي، على النحو المبين هنا، لا يقتضي ضمنا بالضرورة استخدام الخوارزميات المبنية على الأعداد الأولية. ذلك أنه توجد في الوقت الراهن تقنيات رياضية مستخدمة أو قيد التطوير، يُذكر منها نظم الترميز التي تعتمد على المنحنيات الاهليلجية، والتي كثيرا ما يقال عنها إنها تتيح درجة عالية من الأمان من خلال استخدام مفاتيح مخفضة الطول بدرجة كبيرة.

(2) على حين أن استخدام الترميز هو أحد السمات الرئيسية للتوقيعات الرقمية، فإن كون التوقيع الرقمي لا يستخدم سوى لتوثيق رسالة تحتوي على معلومات مقدّمة في صيغة رقمية ينبغي ألا يُخلط بينه وبين الاستخدام الأعم للترميز لأغراض الحفاظ على السرية، الذي هو طريقة تستخدم لترميز الرسالة الإلكترونية بحيث لا يتمكن من قراءتها أحد غير منشئ الرسالة والمرسل إليه. وفي عدد من البلدان يقيد القانون استخدام الترميز لأغراض الحفاظ على السرية، وذلك لأسباب ذات صلة بالسياسة العامة المنطوية على اعتبارات تتعلق بالدفاع القومي. ومن جهة أخرى فإن استخدام الترميز لأغراض التوثيق بإنتاج توقيع رقمي لا يعني بالضرورة استخدام الترميز لإضفاء السرية على أي معلومات أثناء عملية الاتصال، وذلك نظرا لأن التوقيع الرقمي المرمَّز قد لا يكون سوى إضافة إلى رسالة غير مرمّزة.

الخصوصي انطلاقا من معرفة المفتاح العمومي. وأكثر الخوارزميات شيوعا في الترميز باستخدام المفتاح العمومي والمفتاح الخصوصي تستند إلى سمة هامة من سمات الأعداد الأولية الكبيرة: وهي أن تلك الأعداد إذ تُضرب معا لإنتاج عدد جديد تصبح معرفة أي عددين أوليين أنشآ ذلك العدد الجديد الأكبر عملية صعبة وتستغرق وقتا طويلا على وجه الخصوص.[3] وهكذا فعلى الرغم من أن كثيرا من الناس قد يعرفون المفتاح العمومي لموقّع معين ويستخدمونه في التحقق من صحة توقيعه، فإنهم لا يستطيعون أن يكتشفوا المفتاح الخصوصي للموقّع وأن يستخدموه في تزوير توقيعات رقمية.

'٣' دالة البعثرة

٥- إلى جانب عملية إنتاج أزواج المفاتيح توجد عملية أساسية أخرى يشار إليها عموما بعبارة "دالة البعثرة" (hash function) وتستخدم في إنشاء التوقيعات الرقمية وفي التحقق من صحتها. ودالة البعثرة عملية رياضية مبنية على خوارزمية تنشئ تمثيلا رقميا للرسالة أو شكلا مضغوطا من الرسالة، (كثيرا ما يشار إليهما بعبارة "خلاصة رسالة " (message digest) أو "بصمة" رسالة (message fingerprint)) تتخذ شكل "قيمة بعثرة" (hash value) أو "نتيجة بعثرة" (hash result) ذات طول موحد قياسيا يكون عادة أصغر كثيرا من الرسالة ولكن تنفرد به الرسالة جوهريا. وأي تغيير يطرأ على الرسالة تترتب عليه دائما نتيجة بعثرة مختلفة عندما تستخدم دالة البعثرة نفسها. وفي حالة دالة بعثرة مأمونة، تعرف أحيانا باسم "دالة بعثرة ذات اتجاه واحد"، يستحيل عمليا اشتقاق الرسالة الأصلية عند معرفة قيمة البعثرة الخاصة بها. ومن المزايا الأساسية لدالة البعثرة أنه يستحيل بالفعل أيضا إيجاد شيء رقمي ثنائي (مختلف عن الشيء الذي اشتُقت منه الخلاصة أصلا) ينتج الخلاصة نفسها. وعلى ذلك فإن دوالّ البعثرة تمكّن من تشغيل البرنامج الحاسوبي المعد لإنشاء التوقيعات الرقمية بمقادير من البيانات أصغر ويمكن التنبؤ بها بسهولة أكبر، وكذلك تمكّن في الوقت نفسه من تحقيق

(3) تشير بعض المعايير الموجودة إلى مفهوم "الاستحالة الحسابية (computational unfeasibility)" لوصف توقع عدم قابلية العملية للعكس، أي الأمل في استحالة اشتقاق المفتاح الخصوصي السري للمستعمل من المفتاح العمومي لذلك المستعمل. و'الاستحالة الحسابية' مفهوم نسبي يستند إلى قيمة البيانات المحمية، وتكلفة العمليات الحوسبيّة اللازمة لحمايتها، وطول الفترة التي تلزم حمايتها أثناءها، والتكلفة والوقت اللازمين للاعتداء على البيانات، مع تقدير كل هذه العوامل على ما هي عليه في الوقت الراهن وعلى ضوء التقدم التكنولوجي في المستقبل" (المبادئ التوجيهية للتوقيعات الرقمية، رابطة المحامين الأمريكيين: *Legal Infrastructure for Certification Authorities and Secure Electronic Commerce* (شيكاغو، رابطة المحامين الأمريكيين، ١ آب/أغسطس ١٩٩٦)، صفحة ٩، الحاشية ٢٣، متاح في الموقع الشبكي http://www.abanet.org/ scitech/ec/isc/dsgfree.html، الذي تم الدخول إليه في ٥ نيسان/أبريل ٢٠٠٧).

ارتباط إثباتي قوي بمحتوى الرسالة الأصلية، والتوصل بذلك بفعالية إلى توفير ضمان على أنه لم يطرأ على الرسالة أي تعديل منذ أن وُقّع عليها رقميا.

'٤' التوقيع الرقمي

٦- قبل التوقيع على مستند أو على أي معلومات أخرى، يتعين على الموقّع أن يبين بدقة حدود ما يريد التوقيع عليه. ثم تحوسب دالة بعثرة في البرنامج الحاسوبي لدى الموقّع نتيجة بعثرة تنفرد بها (بخصوص كل الأغراض العملية المقصودة) المعلومات التي يراد التوقيع عليها. وعندئذ يحوّل البرنامج الحاسوبي لدى الموقّع نتيجة البعثرة إلى توقيع رقمي باستخدام المفتاح الخصوصي للموقّع. وبذلك يكون التوقيع الرقمي الناتج توقيعا فريدا خاصا بالمعلومات التي يجري التوقيع عليها وبالمفتاح الخصوصي المستخدم في إنشاء التوقيع الرقمي معا. وفي الأحوال النمطية، يُلحق التوقيع الرقمي (أي ترميز نتيجة البعثرة المستخلصة من الرسالة بواسطة المفتاح الخصوصي لدى الموقّع) بالرسالة، ويُخزن أو يُنقل مع تلك الرسالة. غير أن من الممكن أيضا إرساله أو خزنه على أنه عنصر بيانات منفصل، ما دام مرتبطا بالرسالة المناظرة ارتباطا يمكن التعويل عليه. ولأن التوقيع الرقمي يكون فريدا يخص رسالته دون سواها، فإنه غير قابل للعمل به إذا كان مفصولا دوما عن الرسالة.

'٥' التحقق من صحة التوقيع الرقمي

٧- التحقق من صحة التوقيع الرقمي هو عملية تدقيق للتوقيع الرقمي بالرجوع إلى الرسالة الأصلية والى مفتاح عمومي معين، من أجل البتّ فيما إذا كان ذلك التوقيع الرقمي قد أنشئ لتلك الرسالة ذاتها باستخدام المفتاح الخصوصي المناظر للمفتاح العمومي المذكور في المرجع. ويتم التحقق من صحة التوقيع الرقمي بحوسبة نتيجة بعثرة جديدة للرسالة الأصلية بواسطة دالة البعثرة نفسها التي استُخدمت لإنشاء التوقيع الرقمي. ثم يدقق الشخص المتحقق، باستخدام المفتاح العمومي ونتيجة البعثرة الجديدة، فيما إذا كان التوقيع الرقمي قد أنشئ باستخدام المفتاح الخصوصي المناظر، وفيما إذا كانت نتيجة البعثرة المحوسبة مجددا تطابق نتيجة البعثرة الأصلية التي حُولت إلى التوقيع الرقمي أثناء عملية التوقيع.

٨- ومن شأن برنامج التحقق الحاسوبي أن يؤكد التوقيع الرقمي "المُحقق" من حيث صحته فيما يخص الترميز (أ) إذا كان المفتاح الخصوصي للموقّع قد استخدم للتوقيع على الرسالة رقميا، ومعروف أن ذلك هو الذي يحدث إذا استُخدم المفتاح العمومي للموقّع في التحقق من صحة التوقيع لأن المفتاح العمومي للموقّع يقتصر على التحقق من صحة توقيع

رقمي منشأ بواسطة المفتاح الخصوصي للموقّع؛ و(ب) إذا كانت الرسالة لم يطرأ عليها أي تحوير، ومعروف أن ذلك هو الذي يحدث إذا كانت نتيجة البعثرة المحوسبة بمعرفة المتحقق مطابقة لنتيجة البعثرة المستخرجة من التوقيع الرقمي أثناء عملية التحقق من صحته.

'٦' استخدام تكنولوجيا التوقيع الرقمي لأغراض أخرى

٩- كما ذكر أعلاه، فإن لتكنولوجيا التوقيع الرقمي استخداما أوسع نطاقا بكثير من "التوقيع" فحسب على الخطابات الإلكترونية بالطريقة نفسها التي تستخدم بها التوقيعات الخطية للتوقيع على المستندات (انظر الفقرة [...]). والواقع أن شهادات التصديق الموقّعة رقميا كثيرا ما تُستخدم "لتوثيق" وحدات خدمات التطبيقات (الخوادم) أو المواقع الشبكية، على سبيل المثال، لكي يضمن المستعملون أن وحدة خدمات التطبيقات أو الموقع الشبكي هو ذاته المدعى أنه المقصود، أو أنه تابع حقا إلى الشركة التي تدعي بأنها تدير وحدة الخدمات أو الموقع الشبكي. كما يمكن استخدام تكنولوجيا التوقيع الرقمي لغرض "توثيق" برامجيات الحاسوب، على سبيل المثال، من أجل ضمان موثوقية برامجية منزَّلة من موقع شبكي؛ أو لضمان استخدام خادوم تطبيقات معين لتكنولوجيا معتَرف على نطاق واسع بأنها توفر مستوى معينا من الأمان في الاتصال الشبكي، أو لغرض "توثيق" أي بيانات أخرى موزَّعة أو مخزَّنة رقميا.

(ب) مرافق المفاتيح العمومية ومقدّمو خدمات التصديق

١٠- للتحقق من صحة توقيع رقمي، يجب أن تتوافر للمتحقق سبل الوصول إلى المفتاح العمومي الخاص بالموقّع ويكون لديه ما يضمن له تناظره مع المفتاح الخصوصي للموقّع. غير أنه ليس لزوج من المفاتيح عمومي وخصوصي أي ارتباط جوهري بأي شخص معين؛ إذ إنه مجرد زوج من الأرقام. ومن الضروري توافر آلية إضافية للربط على نحو جدير بالتعويل عليه بين شخص معين أو هيئة معينة وزوج المفاتيح. وهذا مهم على نحو خاص، لأنه قد لا يكون هناك علاقة ثقة مسبقة بين الموقِّع ومتلقي الخطابات الموقّعة رقميا عبر وسائط الاتصالات الإلكترونية. ولهذا الغرض، يجب أن تتوافر لدى الأطراف المشمولة درجة من الثقة فيما يصدر من مفاتيح عمومية وخصوصية.

١١- وقد يتوافر مستوى الثقة المطلوب بين الأطراف الذين يثقون بعضهم ببعض، أو الذين يكونون قد تعاملوا فيما بينهم طوال فترة من الزمن، أو الذين يقيمون الاتصالات فيما بينهم ضمن نظم مغلقة، أو الذين يعملون ضمن مجموعة مغلقة، أو الذين لديهم القدرة على

إحكام معاملاتهم تعاقديا، كأن يكون بينهم مثلا اتفاق شراكة تجارية. أما في معاملة لا تشمل سوى طرفين، فإنه يمكن لكل منهما الاقتصار على إبلاغ الآخر (عبر قناة مأمونة نسبيا، مثل ساع خاص أو هاتف) بالمفتاح العمومي من زوج المفاتيح الذي سوف يستخدمه كل منهما. غير أنه قد لا يكون المستوى نفسه من الثقة متوافرا إذا كان الأطراف لا يتعاملون فيما بينهم إلا نادرا، أو يجرون اتصالاتهم بواسطة نظم مفتوحة (مثل الشبكة العالمية عبر الإنترنت)، أو لا يعملون ضمن مجموعة مغلقة، أو لم تكن لديهم اتفاقات شراكة تجارية أو قوانين أخرى تحكم ما بينهم من علاقات. علاوة على ذلك، ينبغي أن يوضع في الحسبان أنه إذا كانت هناك حاجة إلى تسوية المنازعات في المحكمة أو باللجوء إلى التحكيم، فإنه قد يكون من الصعب إثبات أن المالك الفعلي لمفتاح عمومي معين هو الذي أعطاه فعلا إلى المستلِم أو أنه لم يعطه إياه فعلا.

١٢- وقد يصدِر موقّع مرتقب بيانا عاما يذكر فيه أن التوقيعات التي يمكن التحقق من صحتها بمفتاح عمومي معين ينبغي أن تعامل على أنها ناشئة من الموقّع. ويخضع شكل ذلك البيان وفعاليته القانونية لقانون الدولة المشترعة. وعلى سبيل المثال، فإن قرينة إسناد توقيعات إلكترونية إلى موقّع معيّن يمكن إثباتها من خلال نشر ذلك البيان في مجلة رسمية أو في وثيقة تعترف السلطات العمومية بأنها "موثوقة". غير أن أطرافا أخرى قد لا تكون على استعداد لقبول البيان، وبخاصة في حال عدم وجود عقد سابق يُرسي عن يقين المفعول القانوني لذلك البيان المنشور. فالطرف الذي يعوّل على مثل ذلك البيان المنشور في نظام مفتوح ودون سند يدعمه، سيكون عرضة لمخاطرة كبيرة من جرّاء وضعه ثقته بعدم احتراز في شخص محتال، أو نتيجة لاضطراره إلى دحض إنكار زائف لتوقيع رقمي (وهي مسألة كثيرا ما يشار إليها في سياق "عدم التنصل من التوقيعات الرقمية") إذا تبين أن معاملة ما ليست في صالح الموقّع المزعوم.

١٣- ويتمثل أحد الحلول لبعض هذه المشاكل في استخدام واحد أو أكثر من الأطراف الثالثة في الربط بين موقّع محدد الهوية أو اسم الموقّع من جهة ومفتاح عمومي معيّن من جهة أخرى. ويشار إلى هذا الطرف الثالث عموما بعبارة "سلطة التصديق" أو "مقدّم خدمات التصديق" أو "مورِّد خدمات التصديق" في معظم المعايير التقنية والمبادئ التوجيهية (في قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية،[4] اختيرت عبارة "مقدّم خدمات التصديق"). وفي عدد من البلدان تُنظَّم سلطات التصديق هذه هرميا لتصبح كيانا يشار إليه في أحيان كثيرة بعبارة "مرفق مفاتيح عمومية". إذ إن سلطات التصديق ضمن مرفق للمفاتيح العمومية يمكن إنشاؤها في

(4) انظر الحاشية [...] [منشورات الأمم المتحدة، رقم المبيع A.02.V. 8].

بنية هرمية، حيث تقتصر وظيفة بعض سلطات التصديق على تصديق سلطات تصديق أخرى تقدِّم الخدمات مباشرة إلى المستعملين. وفي بنية كهذه، تكون بعض سلطات التصديق تابعة لسلطات تصديق أخرى. وفي بنى أخرى يمكن تصورها، قد تعمل جميع سلطات التصديق على قدم المساواة بعضها مع البعض الآخر. وفي أي مرفق كبير للمفاتيح العمومية، يُرجّح أن توجد سلطات تصديق تابعة وسلطات تصديق أعلى مستوى. وقد تشمل الحلول الأخرى المتبعة في هذا الخصوص، مثلا، اللجوء إلى شهادات التصديق التي تصدرها أطراف معوِّلة.

'١' مرفق المفاتيح العمومية

١٤- إن إنشاء مرفق مفاتيح عمومية هو وسيلة لتوفير الثقة: (أ) بأن المفتاح العمومي لمستعمِل ما لم يُعبث به وبأنه يناظر بالفعل المفتاح الخصوصي لذلك المستعمل؛ و(ب) بأن تقنيات الترميز المستخدمة هي تقنيات سليمة. وبغية توفير الثقة المبينة أعلاه، يمكن أن يقدّم مرفق المفاتيح العمومية عددا من الخدمات تشمل ما يلي: (أ) إدارة مفاتيح الترميز المستعملة لأغراض التوقيع الرقمي؛ و(ب) التصديق على أن مفتاحا عموميا معيّنا يناظر مفتاحا خصوصيا؛ و(ج) توفير مفاتيح للمستعملين النهائيين؛ و(د) نشر معلومات عن إلغاء المفاتيح العمومية أو شهادات التصديق؛ و(ه) إدارة الوسائل الرمزية الشخصية (كالبطاقات الذكية مثلا) التي يمكنها تحديد هوية المستعمل بمعلومات هوية شخصية فريدة، أو يمكنها أن تنتج وتخزن المفاتيح الخصوصية الخاصة بالأفراد؛ و(و) التدقيق في هوية المستعملين النهائيين وتزويدهم بالخدمات؛ و(ز) تقديم خدمات ختم الوقت؛ و(ح) إدارة مفاتيح الترميز المستخدمة لأغراض السرّية حيثما يكون استخدام هذه التقنية مأذونا به.

١٥- وقد يكون مرفق المفاتيح العمومية مستندا إلى مستويات هرمية مختلفة من السلطة. من أمثلة ذلك أن النماذج التي يجري النظر فيها في بلدان معيّنة لإنشاء مرافق مفاتيح عمومية ممكنة تشتمل على إحالات مرجعية إلى المستويات التالية: (أ) "سلطة رئيسية" (root authority) فريدة تصدّق على تكنولوجيا وممارسات جميع الأطراف المأذون لها بإصدار أزواج مفاتيح ترميز أو شهادات تصديق تتعلق باستخدام تلك الأزواج من المفاتيح؛ كما تسجل سلطات التصديق التابعة لها؛[(5)] و(ب) سلطات تصديق مختلفة في موضع أدنى من مرتبة السلطة "الرئيسية"، تصدّق على أن المفتاح العمومي لأحد المستعملين يناظر بالفعل المفتاح الخصوصي لذلك المستعمل (أي أنه لم يُعبث به)؛ و(ج) سلطات تسجيل محلية مختلفة على مستوى أدنى

(5) مسألة ما إذا كان ينبغي أن تكون لدى الحكومة القدرة التقنية على الاحتفاظ بالمفاتيح الخصوصية المستخدمة لأغراض السرية أو على إعادة إنشاء تلك المفاتيح هي مسألة يمكن تناولها على مستوى السلطة الرئيسية.

من مستوى سلطات التصديق، تتلقى الطلبات من المستعملين للحصول على أزواج مفاتيح الترميز أو على شهادات التصديق المتعلقة باستخدام تلك الأزواج من المفاتيح، وتشترط إثبات هوية المستعملين المحتملين وتدقق في تلك الهوية. وفي بلدان معيّنة، يُتوخى أن يقوم الكُتّاب العدول بدور سلطات التسجيل المحلية أو بمساندة تلك السلطات في مهمتها.

١٦- ويمكن توسيع نطاق مرافق المفاتيح العمومية المنظَّمة في بنية هرمية وذلك بإدماج "مجموعات" جديدة من هذه المرافق من خلال قيام "السلطة الرئيسية" الأصل بإنشاء علاقة ثقة مع "الكيان الرئيسي" للمجموعة الجديدة.(6) ويجوز إدماج السلطة الرئيسية للمجموعة الجديدة مباشرة في "الكيان الرئيسي" لمرفق المفاتيح العمومية المستقبِل، لتصبح بالتالي مقدّما لخدمات تصديق تابعا ضمن ذلك المرفق. كما يمكن للسلطة الرئيسية الأصل للمجموعة الجديدة أن تصبح مقدّما لخدمات تصديق تابعا لأحد مقدّمي خدمات التصديق التابعين ضمن المرفق القائم. ومن السمات الجذابة الأخرى للمرافق الهرمية للمفاتيح العمومية أنها تسهِّل تطوير مسارات التصديق لأنها تسير في اتجاه واحد فقط، أي من الشهادة الموجودة بحيازة المستعمل رجوعا إلى موضع جهة الثقة. إضافة إلى ذلك، فإن مسارات التصديق ضمن أي مرفق هرمي للمفاتيح العمومية قصيرة نسبيا، ويعلم مستعملو البنية الهرمية ضمنيا التطبيقات التي يجوز أن تُستعمل لها كل شهادة، بحسب مكانة مقدّم خدمات التصديق داخل البنية الهرمية. غير أن لهذه المرافق الهرمية الخاصة بالمفاتيح العمومية سلبياتها أيضا، ولا سيما السلبيات الناجمة عن التعويل على جهة ثقة وحيدة. فإذا ضعفت السلطة الرئيسية، ضعف مرفق المفاتيح العمومية بكامله. إضافة إلى ذلك، وجدت بعض البلدان أنه من الصعب اختيار كيان واحد ليكون سلطة رئيسية وفرض تلك البنية الهرمية على جميع مقدّمي خدمات التصديق الآخرين.(7)

١٧- أما ما يسمى بمرفق المفاتيح العمومية "المتشابك" فيعتبر بنية بديلة عن المرفق الهرمي. ففي إطار هذا النموذج، يرتبط مقدّمو خدمات التصديق بعلاقة بين الأقران. ويمكن لجميع مقدّمي خدمات التصديق في هذا النموذج أن يكونوا جهات ثقة. وعموما، سوف يثق المستعملون بمقدّمي خدمات التصديق الذين أصدروا شهادة التصديق. وسوف يصدر مقدّمو

(6) William T. Polk and Nelson E. Hastings, *Bridge Certification Authorities: Connecting B2B Public Key Infrastructures*, National Institute of Standards and Technology (أيلول/سبتمبر ٢٠٠٠)، منشور متاح على الموقع الشبكي http://csrc.nist.gov/pki/documents/B2B-article.pdf، الذي تم الدخول إليه في ٣٠ آذار/مارس ٢٠٠٧.

(7) يذكر Polk and Hastings (انظر الحاشية [٦]) أن في الولايات المتحدة الأمريكية، كان من الصعب جدا اختيار وكالة واحدة من وكالات الحكومة الفدرالية للاضطلاع بكامل السلطة على مرفق المفاتيح العمومية الفدرالية.

خدمات التصديق الشهادات بعضهم إلى بعض؛ ويبين زوج الشهادات علاقة الثقة المتبادلة بينهم. ويعني غياب الترتيب الهرمي في هذا النظام أن مقدّمي خدمات التصديق لا يستطيعون فرض شروط تحكم أنواع الشهادات التي يصدرها مقدّمون آخرون لخدمات التصديق. وإذا رغب مقدّم خدمات تصديق تقييد حدود الثقة المتاحة إلى مقدّمي خدمات تصديق آخرين، وجب عليه تحديد هذه القيود في الشهادات التي يصدرها لأقرانه.[8] غير أن شروط وقيود الاعتراف المتبادل قد تكون هدفا معقدا للغاية.

١٨- وهناك بنية بديلة ثالثة تستند إلى مقدّم خدمات تصديق يسمى مجازا "الجسر". وقد تكون هذه البنية مفيدة على نحو مخصوص إذ يمكن لمجموعات مرافق المفاتيح العمومية من خلالها أن تثق بشهادات كل منها. وعلى خلاف مقدّم خدمات التصديق في مرفق المفاتيح العمومية "المتشابك"، فإن مقدّم خدمات التصديق "الجسر" لا يصدر شهادات التصديق مباشرة إلى المستعملين. وليس المقصود أن يقوم مستعملو مرفق المفاتيح العمومية باستخدام مقدّم خدمات التصديق "الجسر" كجهة ثقة، كما هو الحال بالنسبة إلى مقدّم خدمات التصديق "الرئيسي". وعوضا عن ذلك، ينشئ مقدّم خدمات التصديق "الجسر" علاقة ثقة بين الأقران مع مختلف مجموعات المستعملين، وبالتالي يمكِّن المستعملين من الإبقاء على جهات الثقة الطبيعية الخاصة بهم ضمن كل مرفق من مرافق المفاتيح العمومية لديهم. وإذا ما نفّذت مجموعة من المستعملين تكوين مجال ثقة على شكل مرفق مفاتيح عمومية هرمي، فإن مقدّم خدمات التصديق "الجسر" سوف يقيم علاقة مع السلطة الرئيسية لذلك المرفق. غير أنه إذا نفّذت مجموعة المستعملين تكوين مجال ثقة من خلال إنشاء مرفق مفاتيح عمومية متشابك، فلن يحتاج مقدّم خدمات التصديق "الجسر" إلا إلى إرساء علاقة مع أحد مقدّمي خدمات التصديق التابعين لمرفق المفتاح العمومي، الذي يصبح عندئذ مقدّم خدمات التصديق "الرئيسي"داخل ذلك المرفق لغرض إرساء "جسر ثقة" لمرفق المفتاح العمومي الآخر. وبفضل "جسر الثقة" الذي يصل مرفقين أو أكثر من مرافق المفاتيح العمومية من خلال علاقتهما المشتركة مع مقدّم خدمات التصديق "الجسر" يتمكّن المستعملون من مجموعات المستعملين المختلفة من التفاعل فيما بينهم من خلال مقدّم خدمات التصديق "الجسر" بمستوى ثقة محدد.[9]

---

(8) Polk and Hastings, *Bridge Certification Authorities* … (انظر الحاشية [٥]).

(9) اختير في نهاية المطاف مقدّم خدمات التصديق "الجسر" كبنية لإقامة نظام مرفق المفاتيح العمومية للحكومة الفدرالية للولايات المتحدة (Polk and Hastings، انظر الحاشية [٦]). وكان ذلك أيضا هو النموذج المتبع لاستحداث نظام مرفق المفاتيح العمومية لحكومة اليابان.

'٢' مقدِّم خدمات التصديق

١٩- للربط بين زوج من المفاتيح وموقِّع مرتقب، يصدر مقدّم خدمات التصديق (أو سلطة التصديق) شهادة هي عبارة عن سجل إلكتروني يتضمن في قوائمه المفتاح العمومي إلى جانب اسم المكتتب في الشهادة، باعتباره "موضوع" الشهادة، وقد يؤكد أن الموقّع المرتقب المحددة هويته في الشهادة حائز على المفتاح الخصوصي المناظر. والوظيفة الرئيسية للشهادة هي ربط مفتاح عمومي بموقِّع معين. وبوسع "متلقي" الشهادة الراغب في التعويل على توقيع رقمي أنشأه الموقِّع المسمى في الشهادة أن يستعمل المفتاح العمومي المذكور في الشهادة للتحقق من أن التوقيع الرقمي أنشئ باستخدام المفتاح الخصوصي المناظر. فإذا صح هذا التحقق، يتوفّر مستوى من الضمان تقنيا بأن الموقِّع هو الذي أنشأ التوقيع الرقمي، وأن الجزء من الرسالة المستخدم في دالة البعثرة (وبالتالي رسالة البيانات المناظرة) لم يعدَّل منذ أن وقِّع عليها رقميا.

٢٠- ولتأكيد وثوقية الشهادة فيما يتعلق بمحتواها ومصدرها كليهما معا، يوقّع عليها مقدّم خدمات التصديق رقميا. ويمكن التحقق من صحة التوقيع الرقمي لمقدّم خدمات التصديق المصدِر على الشهادة باستخدام المفتاح العمومي الخاص بمقدّم خدمات التصديق المذكور في شهادة أخرى صادرة عن مقدّم خدمات تصديق آخر (قد يكون، ولكن ليس ذلك لازما، أعلى منه مستوى في الترتيب الهرمي)، ويمكن أن تُوثّق تلك الشهادة الأخرى بدورها باستخدام المفتاح العمومي المذكور في شهادة أخرى غير هذه وتلك، وهكذا دواليك إلى أن يطمئن بما فيه الكفاية الشخص المعوّل على التوقيع الرقمي إلى أصالة التوقيع. وكذلك يُعدّ تسجيل التوقيع الرقمي في شهادة تصديق صادرة عن مقدّم خدمات التصديق (يشار إليها أحيانا بعبارة "الشهادة الرئيسية") وسيلة أخرى للتحقق من التوقيع الرقمي.[(10)]

٢١- في كل من هذه الحالات، يجوز لمقدّم خدمات التصديق المصدر للشهادة أن يوقّع رقميا على شهادته هو أثناء فترة سريان الشهادة الأخرى المستخدمة في التحقق من صحة التوقيع الرقمي لمقدّم خدمات التصديق. وبموجب قوانين بعض الدول، قد يكون نشر المفتاح العمومي لمقدّم خدمات التصديق، أو بعض البيانات الخاصة بالشهادة الرئيسية (مثل "البصمة الرقمية")، في نشرة رسمية طريقة من طرق بناء الثقة في التوقيع الرقمي لمقدّم خدمات التصديق.

٢٢- والتوقيع الرقمي المناظر لرسالة ما، سواء أنشأه الموقِّع لتوثيق رسالة، أو أنشأه مقدّم خدمات تصديق لتوثيق شهادته، ينبغي عموما أن يُختم زمنيا على نحو يعوَّل عليه، وذلك لكي يتاح للشخص المتحقق أن يعرف قطعا ما إذا كان التوقيع الرقمي قد أنشئ أثناء "فترة

(10) الوثائق الرسمية للجمعية العامة، الدورة السادسة والخمسون، الملحق رقم ١٧ والتصويب (A/56/17 وCorr.3)، الفقرة ٢٧٩.

السريان" المذكورة في الشهادة، وأن يعرف، إذا اقتضت الحاجة، ما إذا كانت الشهادة صالحة (أي مثلا أنها غير مذكورة في قائمة من قوائم إلغاء الشهادات) في الوقت المعين، وهو شرط من شروط قابلية التحقق من صحة التوقيع الرقمي.

٢٣- ولتيسير التحقق من المفتاح العمومي ومن مناظرته لموقِّع معين، من الجائز نشر الشهادة في مستودع اتصال حاسوبي مباشر، أو إتاحة الاطلاع عليها بوسائل أخرى. ونموذجيا، تكون المستودعات قواعد بيانات للاتصال الحاسوبي المباشر تحوي معلومات عن الشهادات ومعلومات أخرى متاحة للاسترجاع والاستخدام في التحقق من صحة التوقيعات الرقمية.

٢٤- وربما يتبين، بعد صدور الشهادة، أنها لا يُعوّل عليها، كما يحدث في المواقف التي يدعي فيها موقِّع الشهادة لنفسه أمام مقدّم خدمات التصديق هوية غير هويته. وفي ظروف أخرى ربما يمكن التعويل على الشهادة حين صدورها، ولكنها قد تفقد صلاحيتها للتعويل عليها بعد ذلك. فإذا لحق بالمفتاح الخصوصي، "ما يثير الشبهة"، كأن يفقد الموقِّع سيطرته على المفتاح الخصوصي، فقد تفقد الشهادة جدارتها بالثقة أو تصبح غير جديرة بالتعويل عليها، وقد يعمد مقدّم خدمات التصديق (بناء على طلب الموقِّع أو حتى من دون موافقته، رهنا بالظروف) إلى تعليق الشهادة (بوقف فترة سريانها مؤقتا) أو إلى إلغائها (إبطالها بصفة دائمة). ويتوقع من مقدّم خدمات التصديق أن ينشر في الوقت المناسب إشعارا بالإلغاء أو التعليق أو يبلّغ ذلك إلى الأشخاص المستفسرين أو إلى الأشخاص الذين يعرف أنهم تلقوا توقيعا رقميا يمكن التحقق من صحته بالرجوع إلى الشهادة التي فقدت صلاحية التعويل عليها. وعلى نحو مماثل، ينبغي أيضا، حيثما انطبق الموقف، مراجعة شهادة مقدّم خدمات التصديق نفسه للتأكد من عدم إلغائها، وكذلك مراجعة الشهادات الصادرة للتحقق من توقيع سلطة ختم الوقت على أدوات ختم الوقت وعلى شهادات مقدّم خدمات التصديق الذي يصدر هذه الشهادات الخاصة بسلطات ختم الوقت.

٢٥- ويمكن أن يدير سلطات التصديق مقدّمو خدمات من القطاع الخاص أو جهات حكومية. ومن المتوخّى في بعض البلدان، لأسباب تتعلق بالسياسة العامة، أن تكون الهيئات الحكومية هي فحسب المأذونة بتشغيل سلطات التصديق. غير أن تقديم خدمات التصديق في معظم البلدان يكون إما مجالا متروكا بالكامل للقطاع الخاص، وإما يتعايش فيه مقدّمو خدمات التصديق التي تشغّلها الحكومات مع مقدّمي خدمات التصديق من القطاع الخاص. وتوجد أيضا نظم تصديق مقفلة، حيث تقوم مجموعات صغيرة بإيجاد مقدّم خدمات التصديق الخاص بها. وفي بعض البلدان يصدِر مقدّمو خدمات التصديق الحكومية الشهادات فقط لدعم التوقيعات الإلكترونية التي تستخدمها الإدارات العامة. وبصرف النظر عما إذا كانت سلطات التصديق تشغّلها هيئات حكومية أو يشغّلها مقدّمو خدمات من القطاع الخاص، وعما إذا كانت سلطات

التصديق ستحتاج أو لن تحتاج إلى الحصول على رخصة للعمل، يوجد نموذجيا أكثر من مقدّم خدمات تصديق عامل في مرفق المفاتيح العمومية. ومن دواعي الاهتمام الخاص ما يقام من علاقات بين سلطات التصديق المختلفة (انظر الفقرات [١٥]-[١٨] أعلاه).

٢٦- وقد يتعين على مقدّم خدمات التصديق، أو على السلطة الرئيسية، ضمان استيفاء المقتضيات المفروضة بموجب سياستهما العامة باستمرار. فقد يستند اختيار سلطات التصديق إلى عدد من العوامل، يُذكر منها قوة المفتاح العمومي المستخدم وهوية مستعمله، إلا أن الجدارة بالثقة التي يتمتع بها أي مقدّم خدمات تصديق قد تتوقف أيضا على إنفاذه معايير بشأن إصدار الشهادات ومدى إمكانية التعويل على تقييمه للبيانات التي يتلقاها من المستعملين الراغبين في الحصول على شهادات. ومما يتسم بأهمية بالغة نظام المسؤولية الذي ينطبق على أي مقدّم خدمات تصديق فيما يتعلق بامتثاله لمقتضيات السياسة العامة والأمان الصادرة عن السلطة الرئيسية أو عن مقدّم خدمات التصديق من مرتبة عليا، أو بامتثاله لأي مقتضيات أخرى منطبقة، وذلك على أساس مستمر. ومما يتسم بالأهمية نفسها، الالتزام بأن يتصرف مقدّم خدمات التصديق وفقا للتأكيدات التي يقدمها بخصوص سياساته العامة وممارساته، كما هو متوخى في الفقرة ١ (أ) من المادة ٩ من القانون النموذجي بشأن التوقيعات الإلكترونية.

(ج) مشاكل عملية في استخدام مرفق المفتاح العمومي

٢٧- على الرغم من المعرفة الواسعة في مجال تكنولوجيات التوقيع الرقمي والطريقة التي تعمل بها، فإن تنفيذ إنشاء مرافق المفاتيح العمومية ومخططات التوقيعات الرقمية، واجه عمليا بعض المشكلات التي أبقت مستوى استخدام التوقيعات الرقمية أدنى من التوقعات.

٢٨- والتوقيعات الرقمية تؤدي عملها جيدا كوسيلة للتحقق من التوقيعات التي تُنشأ خلال فترة صلاحية شهادة ما. غير أنه حالما تنتهي صلاحية الشهادة أو تُلغى، يفقد المفتاح العمومي المناظر صلاحيته، حتى وإن لم يكن هناك ما يثير الشبهة في زوج المفاتيح. وعليه، فإن مخطط مرفق المفتاح العمومي يتطلب نظاما لإدارة شؤون التواقيع الرقمية لضمان إتاحة التوقيع طوال الوقت اللازم. وتنجم الصعوبة الرئيسية عن احتمال أن تصبح السجلات الإلكترونية "الأصلية" (أي الأرقام الثنائية، أو "البتّات" (bits) التي يتكوّن منها الملف الحاسوبي الذي سُجِّلت عليه المعلومات)، بما في ذلك التوقيع الرقمي، غير مقروءة أو غير جديرة بالتعويل عليها مع مرور الوقت، وذلك أساسا بسبب تقادم البرامجية، أو المعدات أو كلتيهما. وفي الواقع قد يصبح التوقيع الرقمي غير مأمون، نتيجة التطورات العلمية في تحليل الترميز (الجفرة)، أو قد لا تتوافر برامجية التحقق من التوقيع طوال فترات طويلة من الزمن أو

قد لا يبقى المستند سليما.[11] وهذا يجعل الاحتفاظ بالتوقيعات الإلكترونية لفترة طويلة مسألة إشكالية عموما. ومع أن الاعتقاد ساد لفترة من الزمن بأن التوقيعات الرقمية أساسية لأغراض المحفوظات، فقد بينت التجربة أنها ليست محصنة من المخاطر على المدى الطويل. وبما أن أي تغيير في السجل بعد وقت إنشاء التوقيع سوف يتسبب في إخفاق التحقق من التوقيع، فإن عمليات إعادة التشكيل بما يحفظ السجل مقروءا في المستقبل (من قبيل "الانتقال" أو "التحويل") قد يؤثر على ديمومة التوقيع.[12] والحقيقة أن تصوّر استخدام التوقيعات الرقمية كان لتوفير الأمان في تبليغ المعلومات أكثر منه لحفظ المعلومات على مدى الزمن.[13] ولم تؤد المبادرات الرامية إلى تجاوز هذه المشكلة إلى حل دائم بعد.[14]

---

(11) Jean-François Blanchette, "Defining electronic authenticity: an interdisciplinary journey"، منشور متاح على الموقع الشبكي: http://polaris.gseis.ucla.edu/blanchette/papers/dsn.pdf، الذي تم الدخول إليه في ٥ نيسان/أبريل ٢٠٠٧ (ورقة منشورة في مجلد إضافي خاص 2004 International Conference on Dependable Systems and Networks (DSN 2004)، فلورنسا، إيطاليا، ٢٨ حزيران/يونيه – ١ تموز/يوليه ٢٠٠٤)، الصفحات ٢٢٨-٢٣٢.

(12) "في النهاية، كل ما يمكن الاحتفاظ به في السياق الإلكتروني هي البتات (bits). غير أنه كان واضحا لوقت طويل أن من الصعب جدا الاحتفاظ بمجموعة من البتات (bits) إلى ما لا نهاية. فمع مرور الزمن، تصبح مجموعة البتات غير مقروءة (للحاسوب وبالتالي للبشر) بسبب التقادم التكنولوجي لبرنامج التطبيق و/أو للأجهزة الحاسوبية (ومنها القارئ). ولم يتم حتى الآن دراسة مشكلة ديمومة التوقيعات الرقمية المستندة إلى مرافق المفاتيح العمومية على نحو جيد بسبب تعقيدها. ومع أن أدوات التوثيق التي كانت مستخدمة في الماضي، كالتوقيعات الخطية، والأختام، والطوابع، وبصمات الأصابع، الخ معرضة أيضا إلى إعادة تشكيل (مثل استخدام الميكروفيلم) بسبب تقادم الحامل الورقي، فإنها لا تصبح أبدا عديمة الفائدة بعد إعادة التشكيل. فهناك دوما نسخة واحدة على الأقل متاحة لمقارنتها بأدوات توثيق أصلية أخرى." Jos Dumortier and Sofie Van den Eynde, *Electronic Signatures and Trusted Archival Services*، الصفحة ٥ من منشور متاح على الموقع الشبكي: http://www.law.kuleuven. ac.be/icri/publications/172DLM2002.pdf? where=، الذي تم الدخول إليه في ٥ نيسان/أبريل ٢٠٠٧.

(13) في عام ١٩٩٩، أطلق أمناء محفوظات من بلدان مختلفة مشروع الأبحاث الدولية الخاصة بالسجلات ذات الحجية الدائمة في النظم الإلكترونية (InterPARES) الذي يهدف إلى "تطوير المعارف النظرية والمنهجية اللازمة لحفظ السجلات ذات الحجية المنشأة و/أو المحتفظ بها بالشكل الرقمي (انظر الموقع الشبكي: http://www.interpares.org/، الذي تم الدخول إلى الموقع في ٥ نيسان/أبريل ٢٠٠٧). وأشار مشروع تقرير فرقة العمل المعنية بالتحقق من الحجية، الذي كان جزءا من المرحلة الأولى من مشروع (InterPARES 1) التي انتهت في عام ٢٠٠١، إلى أن "التوقيعات الرقمية ومرافق المفاتيح العمومية هي أمثلة على التكنولوجيات التي تم تطويرها وتنفيذها كوسائل توثيق للسجلات الإلكترونية التي تُنقل **عبر الفضاء**. ومع أن حافظي السجلات والعاملين في مجال تكنولوجيا المعلومات يثقون في تكنولوجيات التوثيق لضمان حجية السجلات، لم يكن القصد من هذه التكنولوجيات هو ضمان حجية السجلات الإلكترونية **عبر الزمن** (الخط الغامق أضيف للتأكيد) وهي لا تمثل وسيلة قابلة للاستمرار في هذا المجال." متاح على الموقع الشبكي: http://www.interpares.org/documents/atf_draft_final_report.pdf الذي تم الدخول إليه في ٥ نيسان/أبريل ٢٠٠٧. التقرير النهائي عن (InterPARES 1) متاح على الموقع الشبكي http://www.interpares.org/book/

٢٩- وثمة مجال آخر قد تؤدي فيه التوقيعات الرقمية ومخططات مرافق المفاتيح العمومية إلى مشكلات عملية، وهو يتعلق بأمن البيانات وحماية الخصوصية (الحرمة) الشخصية. فعلى مقدّمي خدمات التصديق تأمين حفظ المفاتيح التي تُستخدم لتوقيع الشهادات التي يصدرونها لزبائنهم، وقد تتعرض لمحاولات خارجية للوصول إليها دون إذن (انظر أيضا الجزء الثاني،

---

index.htm. وتهدف مواصلة المرحلة الثانية من المشروع (InterPARES 2) إلى وضع وتحديد المفاهيم والمبادئ والمعايير والطرائق التي يمكن بها ضمان إنشاء سجلات دقيقة وموثوقة وصيانتها والحفاظ على السجلات الأصلية على المدى الطويل في سياق الأنشطة الفنية والعلمية والحكومية المنفذة بين عام ١٩٩٩ و٢٠٠١.

(14) على سبيل المثال، أُطلقت عام ١٩٩٩ المبادرة الأوروبية بشأن التوحيد القياسي للتوقيعات الإلكترونية (EESSI) من جانب مجلس معايير تكنولوجيا المعلومات والاتصالات، وهو فريق تعاون بين المنظمات المعنية بالتوحيد القياسي والأنشطة ذات الصلة في مجال تكنولوجيات المعلومات والاتصالات، أنشئ من أجل تنسيق أنشطة التوحيد القياسي بهدف دعم تنفيذ التوجيه الإداري الصادر عن الاتحاد الأوروبي بشأن التواقيع الإلكترونية (انظر الحاشية [...] [Official Journal of the European Communities, L 13/12]). وسعى اتحاد مؤسسات المبادرة الأوروبية بشأن التوحيد القياسي للتوقيعات الإلكترونية (وهو جهد للتوحيد القياسي يهدف إلى تحويل المقتضيات الواردة في التوجيه الإداري الأوروبي بشأن التوقيعات الإلكترونية إلى معايير قياسية أوروبية) إلى تلبية الحاجة إلى ضمان الاحتفاظ بالوثائق الموقعة من خلال تقنيات الترميز على المدى الطويل من خلال معياره الخاص "بنماذج تشكيل التوقيع الإلكتروني" (Electronic Signature Formats ES 201 733, ETSI, 2000). ويميز النموذج التشكيلي بين لحظتي التحقق من صحة التوقيع، وهما تحقق أولي وتحقق لاحق. ويحوي نموذج التحقق اللاحق جميع المعلومات التي يمكن استعمالها في عملية التحقق النهائي مثل معلومات الإلغاء، وأختام الوقت، والسياسات العامة بشأن التوقيع، الخ. وتُجمع هذه المعلومات في مرحلة التحقق الأولي. وكان التهديد الأمني لصحة التوقيع الذي ينتج عن تفسُّخ قوة الترميز من بين شواغل مصممي نماذج التوقيع الإلكتروني. ولتجنب التهديد الذي يمثله هذا التفسخ، يجدد ختم الوقت بانتظام على التوقيعات بحسب مقتضيات المبادرة، مع توفير خوارزميات توقيع وأحجام مفاتيح مناسبة لأحدث طرائق الترميز. وجرى تناول مشكلة عمر البرامجية في تقرير المبادرة لعام ٢٠٠٠، الذي عرَّف "خدمات المحفوظات الموثوقة"، وهو نوع جديد من الخدمات التجارية التي ستقدمها أجهزة مختصة ومهنيون في هذا المجال، بهدف ضمان حفظ الوثائق الموقعة بتقنية الترميز، على المدى الطويل. ويورد التقرير عددا من المقتضيات التقنية التي ينبغي أن توفرها خدمات المحفوظات الموثوقة ومنها "التوافق الارتجاعي" مع الأجهزة الحاسوبية والبرامجيات إما من خلال المحافظة على المعدات و/أو من خلال المضاهاة. (انظر "... Blanchette Defining electronic authenticity") (انظر الحاشية [١٢]). ويمكن الاطلاع على دراسة متابعة بشأن توصية المبادرة (EESSI) المتعلقة بخدمات المحفوظات الموثوقة، التي أجراها المركز المتعدد التخصصات للقانون وتكنولوجيا المعلومات والاتصالات في جامعة لوفن الكاثوليكية للتكنولوجيا، بلجيكا، (Interdisciplinary Centre for Law and ICT of the Catholic University of Leuven Technology)، والمعنونة *European Electronic Signature Standardization Initiative: Trusted Archival Services* (المرحلة ٣، التقرير النهائي، ٢٨ آب/أغسطس ٢٠٠٠) على الموقع الشبكي: http://www.law.kuleuven.ac.be/ icri/publications/91TAS-Report.pdf?where=، الذي تم الدخول إليه في ١٢ نيسان/أبريل ٢٠٠٧). وقد انتهت المبادرة في تشرين الأول/أكتوبر ٢٠٠٤. ولا يبدو أن نظم تنفيذ هذه التوصيات تعمل حاليا (انظر Dumortier and Van den Eynde، *Electronic Signatures and Trusted Archival Services*) (انظر الحاشية [١٣]).

الفقرات [...]-[...] أدناه). وبالإضافة إلى ذلك، يتعين على مقدّمي خدمات التصديق الحصول على سلسلة من البيانات الشخصية والمعلومات التجارية من الأشخاص الذين يتقدمون بطلب للحصول على شهادات التصديق. كما يتعين على مقدّم خدمات التصديق تخزين هذه المعلومات للرجوع إليها مستقبلا. كذلك يجب على مقدّمي خدمات التصديق اتخاذ التدابير اللازمة لضمان أن يكون الوصول إلى هذه المعلومات وفقا لقوانين حماية البيانات المعمول بها.[15] غير أن الوصول إلى المعلومات من دون إذن لا يزال يمثل تهديدا حقيقيا.

٢- القياسات الحيوية

٣٠- يُستخدم القياس الحيوي لتحديد شخصية فرد ما من خلال الميزات البدنية أو السلوكية الجوهرية الخاصة به. وتشمل الميزات التي يمكن استعمالها في القياسات الحيوية للتعرّف على الشخصية ما يلي: الحمض الخلوي الصبغي (حمض د. ن. أ.)، وبصمات الأصابع، وقزحية العين، وشبكية العين، وشكل وخطوط اليد أو الوجه، والمخطط الحراري للوجه، وشكل الأذن، والصوت، ورائحة الجسم، ونمط الأوعية الدموية، وخط الكتابة باليد، وطريقة المشي، وأنماط الطباعة.

٣١- ويشمل استخدام أدوات القياس الحيوي عادة أخذ عيّنة قياس حيوي لإحدى الميزات الحيوية (البيولوجية) الفردية للشخص. وتكون هذه العينة بالشكل الرقمي. ثُم تُستخرج بيانات القياس الحيوي من تلك العينة لإنشاء قالب حاسوبي مرجعي. وفي نهاية المطاف، تُقارن بيانات القياس الحيوي المخزَّنة في القالب الحاسوبي المرجعي مع البيانات

(15) انظر المبادئ التوجيهية لمنظمة التعاون والتنمية في الميدان الاقتصادي (OECD) بشأن حماية الخصوصية وتدفقات البيانات الشخصية عبر الحدود (باريس، ١٩٨٠)، متاحة على الموقع الشبكي: http://www.oecd.org/document/18/ 0,2340,en_2649_34255_1815186_1_1_1_1,00.html، الذي تم الدخول إليه في ٧ شباط/فبراير ٢٠٠٧؛ واتفاقية مجلس أوروبا لحماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية (مجلس أوروبا، مجموعة المعاهدات الأوروبية، رقم ١٠٨)، متاحة على الموقع الشبكي http://conventions.coe.int/Treaty/en/ Treaties/Html/108.htm، الذي تم الدخول إليه في ٧ شباط/فبراير ٢٠٠٧؛ ومبادئ الأمم المتحدة التوجيهية لتنظيم ملفات البيانات الشخصية المحوسبة (قرار الجمعية العامة ٤٥/٩٥)، متاحة على الموقع الشبكي: http://193.194.138.190/html/menu3/b/71.htm، الذي تم الدخول إليه في ٧ شباط/فبراير ٢٠٠٧؛ والتوجيه الإداري الصادر عن البرلمان الأوروبي والاتحاد الأوروبي ومجلس أوروبا 95/46/EC المؤرخ ٢٤ تشرين الأول/أكتوبر ١٩٩٥ بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية وبشأن حرّية حركة هذه البيانات (*Official Journal of the European Communities*, L 281, 23 November 1995)، متاحة على الموقع الشبكي: http://eur-lex.europa.eu/smartapi/cgi/sga_doc? smartapi!celexapi!prod!CELEXnumdoc&lg= EN&numdoc=31995L0046&model=guichett، الذي تم الدخول إليه في ٧ شباط/فبراير ٢٠٠٧.

المستخرَجة من المستعمِل النهائي لأغراض التحقق، وذلك لكي يتسنى تبيان ما إذا كان قد تم التعرف على الهوية أو التحقق منها أم لا.[16]

٣٢- وتستلزم طبيعة أدوات القياس الحيوي سمات بارزة فريدة لا بد من إيلائها الاعتبار الواجب. ولوجود تلك السمات البارزة، التي قد تختلف إلى حد ما عن الميزة المختارة كمرجع، تأثير كبير على مدى ملاءمة هذه التكنولوجيا للتطبيق المقصود.

٣٣- وهناك عدد من المخاطر تتعلق بتخزين بيانات القياس الحيوي، لأن أنماط القياس الحيوي غير قابلة للإلغاء عادة. وعندما يقع المساس بنظم القياس الحيوي بما يثير الشبهة، لا سبيل أمام المستعمل الشرعي سوى إلغاء بيانات تحديد الهوية والانتقال إلى مجموعة أخرى من بيانات تحديد الهوية لم تُمس بما يثير الشبهة. ولذلك، ثمة حاجة إلى قواعد خاصة لمنع إساءة استعمال قواعد بيانات القياس الحيوي.

٣٤- ولا يمكن أن تكون دقّة تقنيات القياس الحيوي مطلقة، لأن السمات البارزة البيولوجية تميل في جوهرها إلى التغير، وقد ينطوي أي قياس على انحراف ما. وفي هذا الخصوص، لا تعتبر القياسات الحيوية محدِّدات فريدة للهوية بل شبه فريدة. ولاستيعاب تلك التغيرات، يمكن التأثير في دقة القياسات الحيوية من خلال وضع حد أدنى لتواؤم القالب الحاسوبي المرجعي مع العينة المستخرَجة. غير أن وضع حد أدنى منخفض قد يميل باتجاه قبول زائف، بينما يميل تحديد حد أدنى مرتفع إلى حالات رفض زائف. ومع ذلك، قد تكون دقة التوثُّق التي توفرها القياسات الحيوية كافية في أغلب التطبيقات التجارية.

٣٥- إضافة إلى ذلك، فإن مسائل حماية البيانات وحقوق الإنسان تبرز فيما يتعلق بتخزين بيانات القياس الحيوي والكشف عنها. وقد لا تشير قوانين حماية البيانات[17] صراحة إلى القياسات الحيوية، ومع ذلك فهي تهدف إلى حماية البيانات الشخصية المتعلقة بالأشخاص الطبيعيين، والتي تُعتبر معالجتها في شكلها الخام وكقوالب حاسوبية مرجعية، عملية في صميم تكنولوجيا القياسات الحيوية.[18] علاوة على ذلك، قد تكون هناك حاجة إلى تدابير لحماية

(16) الرابطة الدولية للقياسات الحيوية (iAfB) والرابطة الدولية لأمن الحواسيب (ICSA)، قائمة مصطلحات القياسات الحيوية لعام ١٩٩٩، متاحة على الموقع الشبكي: (http://www.afb.org.uk/docs/glossary.htm)، الذي تم الدخول إليه في ٧ شباط/فبراير ٢٠٠٧.

(17) انظر الحاشية [١٥].

(18) Paul de Hert, "*Biometrics: Legal Issues and Implications* - background paper for the Institute for Prospective Technological Studies (European Communities, Directorate General Joint Research Centre, Institute for Prospective Technological ورقة معلومات خلفية من أجل المعهد التابع للمفوضية الأوروبية

المستهلكين من المخاطر المتأتية عن الاستخدام الخصوصي لبيانات القياسات الحيوية، وكذلك في حالة سرقة الهوية. وقد يشمل ذلك مجالات قانونية أخرى، بما في ذلك قانون العمل والصحة.[19]

٣٦- وقد تساعد الحلول التقنية على العناية ببعض الشواغل. فإن تخزين بيانات القياسات الحيوية مثلا على بطاقات ذكية أو الأمارات الرمزية قد يمنع الوصول إلى هذه البيانات من دون إذن، وهي حالة قد تحدث إذا كانت البيانات مخزنة في نظام حاسوبي مركزي. وبالإضافة إلى ذلك، تم تطوير مجموعة من أفضل الممارسات لتقليص المخاطر في مجالات مختلفة مثل: النطاق والقدرات؛ وحماية البيانات؛ وتحكُّم المستعمِل بالبيانات الشخصية، وإفشاء البيانات، وتدقيقها، والمساءلة بشأنها والإشراف عليها.[20]

٣٧- وعموما، يُنظر إلى أدوات القياس الحيوي على أنها وسيلة توفر مستوى عاليا من الأمان. ومع أنها ملائمة لطائفة من الاستعمالات، فإن نطاقها الرئيسي الحالي يتعلق بالتطبيقات الحكومية، وخصوصا تطبيقات إنفاذ القانون كالتطبيقات الخاصة بإجراءات الموافقة في دائرة الهجرة وتدابير مراقبة الدخول.

٣٨- كما تم تطوير تطبيقات تجارية، إذ باتت القياسات الحيوية تُستخدم كثيرا في سياق عملية توثيق تقوم على عاملين، فتستلزم توفير عنصر يكون ملازما للشخص الفرد (القياسات الحيوية) وعنصر يكون بعلم الشخص (عادة، كلمة سر أو رقم لتحديد الهوية الشخصية (PIN). إضافة إلى ذلك، تم تطوير تطبيقات لتخزين ومقارنة خصائص التوقيع الخطي لشخص ما. إذ تسجّل لوحة بيانية إلكترونية رقمية ضغط القلم ومدة عملية التوقيع. ثم تُخزَّن البيانات على شكل خوارزمية تُستخدم لمقارنتها بالتوقيعات في المستقبل. غير أنه على ضوء السمات الفطرية التي تميز القياسات الحيوية، يعرب أيضا عن التزام الحيطة إزاء أخطار الزيادة التدريجية وغير المراقبة فيما يتعلق باستخدامها في المعاملات التجارية المعتادة.

(2005، الصفحة ١٣، متاحة على الموقع الشبكي: http://cybersecurity.jrc.es/docs/LIBE%20Biometrics%20March%2005/LegalImplications_Paul_de_Hert.pdf.

(19) في كندا، على سبيل المثال، نوقش استعمال القياسات الحيوية فيما يتعلق بتطبيق قانون حماية المعلومات الشخصية والوثائق الإلكترونية (Personal Information Protection and Electronic Documents Act in the workplace) (2000, c. 5) في أماكن العمل (انظر *Turner v. TELUS Communications Inc.*, 2005 FC 1601, 29 November 2005 (Federal Court of Canada)).

(20) انظر، للحصول على مثال على أفضل الممارسات، International Biometric Group BioPrivacy Initiative, "Best practices for privacy-sympathetic biometric deployment"، متاحة على الموقع الشبكي: http://www.bioprivacy.org.

٣٩- وقد تبرز مشكلة في الإثبات إذا استُخدمت توقيعات القياسات الحيوية كبديل عن التوقيعات الخطية. فكما ذُكر آنفا، تتغير عوِلية الأدلة الإثباتية المستمدة من القياسات الحيوية بحسب اختلاف التكنولوجيات المستخدمة ونسبة القبول الزائف المختارة. وبالإضافة إلى ذلك، ثمة إمكانية للتلاعب ببيانات القياسات الحيوية المخزنة بالشكل الرقمي أو لتزييفها.

٤٠- ويمكن تطبيق اختبارات العول العامة بمقتضى قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية،[21] والقانون النموذجي بشأن التجارة الإلكترونية،[22] وكذلك بمقتضى اتفاقية الأمم المتحدة المتعلقة باستخدام الخطابات الإلكترونية في العقود الدولية،[23] وهي أحدث عهدا، بشأن استخدام توقيعات القياس الحيوي. وبغية ضمان التوحيد، قد يكون من المفيد أيضا وضع مبادئ توجيهية دولية بشأن استخدام طرائق القياس الحيوي وإدارتها.[24] ويتعين النظر بعناية فيما إذا كان وضع معايير قياسية من هذا القبيل سابقا لأوانه، نظرا إلى الحالة الراهنة لتطور تكنولوجيات القياس الحيوي، وفيما إذا كان من المحتمل أن تؤدي إلى إعاقة التطور المتواصل في هذه التكنولوجيات.

٣- كلمات السر والطرائق الهجينة

٤١- تُستخدم كلمات السر والرموز الاصطلاحية لضبط سبل الوصول إلى المعلومات أو الخدمات و"لتوقيع" الخطابات الإلكترونية. وفي الممارسة العملية يُلاحظ أن الاستخدام الثاني أقل شيوعا من الأول، بسبب المخاطرة المحتملة في المساس بالرمز عندما يرسل في رسائل غير مرمّزة. ومع ذلك، فإن كلمات السر والرموز هي الطريقة الأوسع استعمالا "للتوثيق" بغرض ضبط سبل الوصول إلى المعلومات والتحقق من الهوية في طائفة واسعة من المعاملات، بما في ذلك غالبية العمليات المصرفية عبر الإنترنت، والسحوبات النقدية من أجهزة الصرف الآلي والمعاملات الاستهلاكية التي تُجرى بواسطة بطاقات الائتمان.

---

(21) (انظر الحاشية [...]) [منشورات الأمم المتحدة، رقم المبيع A.02.V.8].

(22) (انظر الحاشية [...]) [منشورات الأمم المتحدة، رقم المبيع A.99.V.4].

(23) انتهت الأونسيترال من صوغ اتفاقية الأمم المتحدة المتعلقة باستخدام الخطابات الإلكترونية في العقود الدولية في دورتها الثامنة والثلاثين (فيينا، ٤-١٥ تموز/يوليه ٢٠٠٥) وأقرَّتها الجمعية العامة رسميا في ٢٣ تشرين الثاني/نوفمبر ٢٠٠٥ (مرفق قرار الجمعية العامة ٦٠/٢١)، وهي متاحة على الموقع الشبكي: http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html.

(24) يمكن مقارنتها بمعايير قابلية التعويل الواردة في دليل الاشتراع لقانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية. (انظر الحاشية [...]) (منشورات الأمم المتحدة، رقم المبيع A.02.V.8)، الفقرة ٧٥.

٤٢- وينبغي التسليم بإمكانية استخدام تكنولوجيات متعددة "لتوثيق" معاملة إلكترونية. ويمكن الاستعانة بعدة تكنولوجيات أو بعدة استخدامات لتكنولوجيا واحدة لإجراء معاملة واحدة. فعلى سبيل المثال، يمكن الجمع بين ديناميات التوقيع بغرض التوثيق وتقنيات الترميز لضمان سلامة الرسالة. وبدلا من ذلك، يمكن إرسال كلمات السر عبر الإنترنت باستخدام تقنيات الترميز (أي طبقة المقابس الآمنة في المتصفِّح SSL) لحمايتها، بالاقتران مع استخدام القياسات الحيوية لإطلاق توقيع رقمي (يعتمد على نظم الترميز غير المتناظرة) ينتج عند استلامه ما يسمى ببطاقة كيربيروس في نافذة خاصة على الشاشة (نظم الترميز المتناظرة). ولدى وضع الأطر القانونية والسياسة العامة للتعامل مع هذه التكنولوجيات، ينبغي إيلاء الاعتبار لدور التكنولوجيات المتعددة. ويتعين أن تكون الأطر القانونية والسياسة العامة للتوثيق الإلكتروني مرنة بما يكفي لتغطية نهوج التكنولوجيا الهجينة، لأن الأطر التي تركز على تكنولوجيات محددة يمكن أن تعيق استخدام التكنولوجيات المتعددة.[25] ومن شأن الأحكام المحايدة إلكترونيا أن تسهل قبول النهوج الهجينة في التكنولوجيا.

٤- التوقيعات المستنسخة بالمسح التصويري والأسماء المطبوعة

٤٣- يعود السبب الرئيسي لاهتمام المشرِّعين بالتجارة الإلكترونية في مجال القانون الخاص إلى القلق من أن التكنولوجيات الجديدة قد تؤثر في تطبيق قواعد القانون التي وُضِعت لوسائط أخرى. وغالبا ما أدى هذا الاهتمام بالتكنولوجيا، عمدا أو عن غير قصد، إلى التركيز على التكنولوجيات المتطورة التي تقدم مستوى أعلى من الأمان لطرائق التوثيق والتوقيع الإلكترونية. وغالبا ما يُهمل، في هذا السياق، أن عددا كبيرا جدا من الخطابات التجارية، إن لم يكن أكثرها، التي يجري تبادلها عبر العالم لا تُستخدم فيها تكنولوجيا محددة للتوثيق أو التوقيع.

٤٤- وفي الممارسات اليومية، كثيرا ما تكون الشركات في أنحاء مختلفة من العالم مقتنعة بتبادل الرسائل الإلكترونية من دون استخدام أي شكل من أشكال التوثيق أو التوقيع غير الاسم المطبوع، مع اسم وعنوان الأطراف في أسفل الخطابات. وفي بعض الأحيان، يكون

---

(25) مؤسسة أبحاث السياسات العامة بشأن المعلومات، تجميع الاستشارات بشأن تعليمات التوقيع، ٢٨ تشرين الأول/أكتوبر، والتي توفر تجميعا للردود على الاستشارات الخاصة بالتوجيه الإداري الصادر عن الاتحاد الأوروبي بشأن التوقيعات الإلكترونية، الذي أُعِدَّ بطلب من المفوضية الأوروبية، متاح على الموقع الشبكي: www.fipr.org/publications/sigdirecon.html، تم الدخول إليه في ١٢ نيسان/أبريل ٢٠٠٧. (Foundation for Information Policy Research, *Signature Directive Consultation Compilation)*

للخطاب شكل أكثر اتساما بالطابع الرسمي من خلال استخدام صور مأخوذة بطريقة التصوير البرقي أو مستنسخة بالمسح التصويري للتوقيعات الخطية، والتي لا تمثل بالطبع إلا نسخة بالشكل الرقمي للأصل الخطي. ولا تقدم الأسماء المطبوعة ولا التوقيعات المستنسخة بالمسح التصويري على الرسائل الإلكترونية غير المرمّزة مستوى عاليا من الأمان، ولا يمكنها على نحو مؤكد إثبات هوية منشئ الخطابات الإلكترونية التي تظهر فيها. ومع ذلك فإن الكيانات التجارية تختار بحرية استخدام هذه الأشكال من "التوثيق" بسبب سهولتها وملاءمتها في الخطابات وفعاليتها من حيث التكلفة. ومن المهم أن يضع المشرِّعون ومقرّرو السياسات العامة في اعتبارهم هذه الممارسات الواسعة الانتشار في الميدان التجاري لدى النظر في التنظيم الرقابي للتوثيق والتوقيع الإلكترونيين. ذلك أن فرض اشتراطات صارمة على التوثيق والتوقيع الإلكترونيين، وخصوصا فرض طريقة أو تكنولوجيا معينة، قد يلقي، دون قصد، بظلال من الشكوك على صحة وقابلية إنفاذ عدد كبير من المعاملات التي تُبرم يوميا من دون استخدام أي نوع معين من التوثيق أو التوقيع الإلكترونيين. وقد يشجع ذلك بدوره الأطراف التي تتصرف بسوء نية، على التهرّب من تبعات الالتزامات التي قبلتها عن طيب خاطر، وذلك من خلال التشكيك في قابلية التعويل على خطاباتها الإلكترونية. وليس من الواقعي أن يتوقع المرء أن يؤدي فرض مقتضيات ذات مستوى عال بدرجة ما على التوقيع والتصديق الإلكترونيين إلى قيام جميع الأطراف في نهاية المطاف باستخدامها يوميا وبصورة فعلية. وقد بينت الخبرة الحديثة في الطرائق المتطورة، كالتوقيعات الرقمية، أن الشواغل بشأن التكلفة ومدى التعقيد كثيرا ما تحدُّ من الاستخدام العملي لتقنيات التوثيق والتوقيع.

جيم- إدارة شؤون الهوية الإلكترونية*

٤٥- في العالم الإلكتروني، يستطيع الأشخاص الطبيعيون والاعتباريون الوصول إلى خدمات عدد من مقدّمي الخدمات الإلكترونية. وفي كل مرة يقوم شخص ما بتسجيل نفسه لدى مقدّم خدمات للحصول على هذه الخدمات يتم إنشاء "هوية" إلكترونية له. إضافة إلى ذلك، يمكن ربط هوية واحدة بعدد من الحسابات الخاصة بالخدمات الإلكترونية لكل تطبيق أو منصّة حاسوبية. ومن شأن تعدد الهويات والحسابات الخاصة بها أن يعيق إدارتها بالنسبة للمستعمِل ومقدّم الخدمات على حد سواء. ويمكن اجتناب هذه الصعوبات من خلال هوية إلكترونية واحدة لكل شخص.

* سيتم التوسع في هذا الفصل في النسخة النهائية من الوثيقة المرجعية الشاملة.

٤٦- ويقتضي التسجيل لدى مقدّم الخدمات وإنشاء هوية إلكترونية إقامة علاقة ثقة متبادلة بين الشخص ومقدّم الخدمات. ويتطلب إنشاء هوية إلكترونية واحدة تجميع تلك العلاقات الثنائية في إطار أوسع يمكن من خلاله إدارتها على نحو مشترك، وهو ما يشار إليه بإدارة شؤون الهوية. وقد تشمل المنافع التي يجنيها مقدّم الخدمات من هذه الإدارة تحسين تدابير الأمان، وتسهيل الامتثال للوائح التنظيم الرقابي وزيادة سرعة التنفيذ؛ أما المنافع التي يجنيها المستعمل فقد تشمل تيسير سبل الوصول إلى المعلومات.

٤٧- ويمكن وصف إدارة شؤون الهوية في سياق نهجين اثنين هما: الأنموذج التقليدي لدخول المستعمل (تسجيل الدخول)، الذي يعتمد على بطاقة ذكية وما يرتبط بها من بيانات يستخدمها الزبون للدخول إلى خدمة ما، وأنموذج خدمة يتسم بقدر أكبر من الابتكار ويستند إلى نظام يقدم خدمات شخصية الطابع مخصصة للمستعملين ولأدواتهم.

٤٨- ويركز نهج دخول المستعمل المتَّبع في إدارة شؤون الهوية على إدارة التوثّق من المستعمل، وحقوق الدخول، وقيود الدخول، ومواصفات الحساب، وكلمات السر وغير ذلك من الخصائص، في واحد أو أكثر من التطبيقات أو النظم. ويهدف إلى تسهيل ومراقبة الدخول إلى التطبيقات والموارد، كما يهدف في الوقت نفسه إلى حماية المعلومات الشخصية والتجارية السرية من المستعملين غير المأذون لهم.

٤٩- وأما في إطار نهج أنموذج الخدمة، فيصبح نطاق إدارة شؤون الهوية أوسع ليشمل جميع موارد الشركة المستخدَمة لتقديم الخدمات الشبكية المباشرة، ومنها المعدات ووحدات الخدمة والبوّابات والمحتويات والتطبيقات والمنتجات الشبكية، علاوة على وثائق الاعتماد الخاصة بالمستعمل، ودفاتر العناوين، والأفضليات والاستحقاقات. ومن الناحية العملية، يمكن أن يشمل هذا النطاق مثلا المعلومات المتعلقة بوسائل رقابة الآباء على المواقع، والمشاركة في برامج الولاء.

٥٠- وتُبذل جهود على المستويين التجاري والحكومي لتوسيع إدارة شؤون الهوية. غير أنه تجدر الإشارة إلى أن الخيارات في السياسة العامة قد تختلف اختلافا كبيرا بين مشهدي هذين المستويين. فالنهج الحكومي قد يكون موجها بقدر أكبر نحو تلبية احتياجات المواطنين على نحو أفضل، وبالتالي فقد يتم تصميمه بحيث يضمن التفاعل مع الأشخاص الطبيعيين. ومن ناحية أخرى، لا بد من أن تأخذ التطبيقات التجارية في الاعتبار تزايد استخدام الآلات المؤتمتة في المعاملات التجارية، وبالتالي فقد تعتمد خصائص ترمي إلى تلبية الاحتياجات المحددة لتلك الآلات.

٥١- وأما الصعوبات التي تتعلق بنظم إدارة شؤون الهوية فتشمل شواغل الخصوصية (الحرمة) الشخصية بسبب المخاطر المرتبطة بسوء استخدام العلامات الفريدة للتعرف على الهوية. إضافة إلى ذلك، قد تنشأ أيضا مسائل تتعلق بالفوارق بين الأنظمة القانونية السارية، وبخاصة ما يتعلق بإمكانية الحصول على تفويض سلطة للتصرّف بالنيابة عن شخص آخر. وقد اقتُرِحت حلول تستند إلى تعاون تجاري طوعي يقوم على ما يسمى بدائرة الثقة، حيث يُطلب إلى المشاركين التعويل على صحة ودقة المعلومات التي يقدمها إليهم أعضاء آخرين من الدائرة. غير أن هذا النهج قد لا يكون كافيا تماما لتنظيم جميع المسائل ذات الصلة، وقد يبقى بحاجة إلى اعتماد إطار قانوني له.[26] كما وُضعَت مبادئ توجيهية لتوفير المقتضيات القانونية بشأن التقيّد بدائرة من البنى التحتية الموثوقة.[27]

٥٢- أما فيما يتعلق بالصلاحية التقنية للعمل التبادلي، فقد أنشأ الاتحاد الدولي للاتصالات فريقا مختصا معنيا بإدارة شؤون الهوية "لتسهيل ومواصلة تطوير إطار عام لإدارة شؤون الهوية ووسائل اكتشاف الهويات المستقلة الموزعة ومجموعات الهويات وسبل التنفيذ."[28]

٥٣- ويجري أيضا تقديم حلول لإدارة شؤون الهوية في سياق بيئة الحكومة الإلكترونية. فعلى سبيل المثال، بدأ في سياق مبادرة "الاتحاد الأوروبي لعام ٢٠١٠ لمجتمع معلومات أوروبي من أجل النمو والعمالة"، الاضطلاع بدراسة بشأن إدارة شؤون الهوية في بيئة الحكومة الإلكترونية لتسهيل التقدم نحو نهج متسق في إدارة شؤون الهوية الإلكترونية في بيئة الحكومة الإلكترونية في الاتحاد الأوروبي، بالاستناد إلى الخبرات والمبادرات المتوافرة في دول الاتحاد الأوروبي.[29]

---

(26) انظر *Modinis Study on Identity Management in eGovernment*: تقرير حول مسألة إدارة شؤون الهوية *(Identity Management Issue Report)*، (European Commission, Directorate General Information Society and Media, June 2006)، الصفحات ٩-١٢، متاح على الموقع الشبكي:
https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/pub/Main/ProjectDocs/modinis.D3.9_Identity_Management_Issue_Interim_Report_II1.pdf.

(27) مشروع تحالف الحرية The Liberty Alliance Project (انظر www.projectliberty.org) وهو تحالف يضم أكثر من ١٥٠ شركة، ومنظمات غير ربحية ومنظمات حكومية من مختلف أنحاء العالم. ويلتزم الاتحاد بوضع معيار مفتوح لهوية شبكية في إطار نظام حكومي موحد يكون مناسبا لجميع الأجهزة الشبكية الموجودة حاليا والتي ستظهر قريبا. وتقدم هذه الهوية للشركات والحكومات والمستخدَمين والزبائن وسيلة أكثر ملاءمة وأكثر أمانا لضبط المعلومات الخاصة بالهوية في الاقتصاد الرقمي القائم حاليا، وهي مكوِّن رئيسي في تطوير استخدام التجارة الإلكترونية وخدمات البيانات الشخصية الطابع، وكذلك الخدمات الشبكية. والعضوية في التحالف مفتوحة لجميع المؤسسات التجارية وغير التجارية.

(28) انظر http://www.itu.int/ITU-T/studygroups/com17/fgidm/index.html.

(29) انظر https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi.

٥٤- وقد أخذ يتسع توزيع أدوات التوقيعات الإلكترونية، وغالبا على شكل بطاقات ذكية، في سياق المبادرات المعنية ببيئة الحكومة الإلكترونية. وبدأت عملية توزيع البطاقات الذكية على النطاق الوطني في كل من بلجيكا[30] وإستونيا، من بين أماكن أخرى. ونتيجة لتلك المبادرات، يتلقى عدد كبير جدا من المواطنين تلك الأدوات ومعها قدرات آمنة للتوقيع الإلكتروني بتكلفة قليلة. ومع أن الهدف الرئيسي من تلك المبادرات قد لا يكون تجاريا، فإن هذه الأدوات قد تستخدم كذلك في الميدان التجاري. كما أخذ يزداد التسليم بتقارب مجالي التطبيق كليهما.[31]

---

(30) انظر http://eid.belgium.be/en/navigation/12000/index.html.

(31) انظر، على سبيل المثال، *(2006 Korea Internet White Paper)* الورقة الكورية البيضاء الخاصة بالإنترنت لعام ٢٠٠٦، (سيول، الوكالة الوطنية لتطوير الإنترنت في كوريا، ٢٠٠٦، صفحة ٨١، في معرض الإشارة إلى الاستعمال المزدوج لقانون التوقيع الإلكتروني في جمهورية كوريا في تطبيقات الحكومة الإلكترونية والتجارة الإلكترونية، والمتاحة على الموقع الشبكي: http://www.ecommerce.or.kr/activities/documents_view.asp?bNo=642&Page=1.