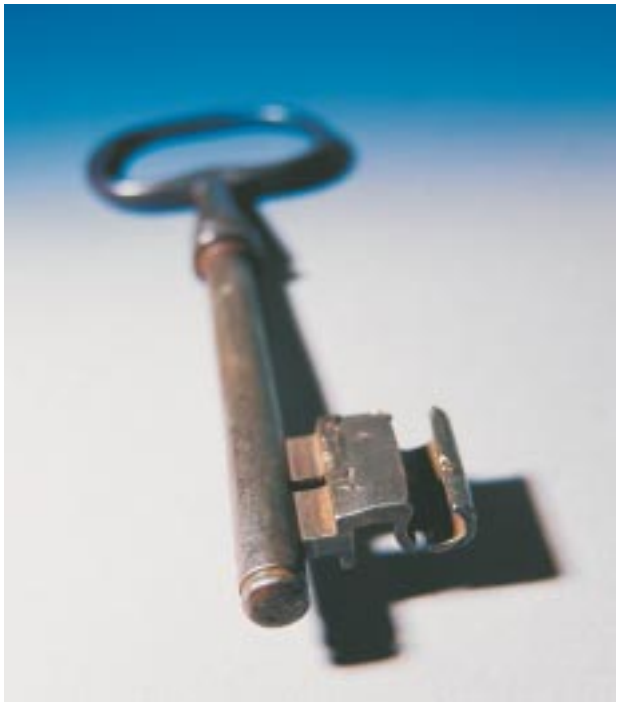
Elektronischer **Notar**

von Christoph Meinel und Lutz Gollan

Die Anwendungen im Bereich der elektronischen Unterschrift sind aufgrund fehlender Standards oft inkompatibel. Kann die Ausgabe digitaler Signaturen der Wirtschaft überlassen werden oder trägt der Staat hier die Verantwortung?

Die Verbreitung digitaler Signaturen erfordert neben der entsprechenden Technik auch vertrauenswürdige Infrastrukturen. Zur Gleichstellung der digitalen Signaturen mit den Handunterschriften verlangt der Gesetzgeber daher den Einsatz so genannter „qualifizierter Zertifikate". Diese – ebenfalls elektronischen – Urkunden bestätigen, dass ein öffentlicher Schlüssel einer bestimmten Person zuordenbar ist. Sie dürfen nur von nachweisbar zuverlässigen und sicheren Anbietern ausgegeben werden. Der Zertifizierungsdiensteanbieter oder ein mit ihm kooperierender Dritter fungiert hierzu als elektronischer Notar. Dieser firmiert unter dem Namen „Trust Center" und garantiert durch das elektronische, im Internet abrufbare Zertifikat, dass seine Registrierungsstellen die Identität des Schlüsselinhabers bei der Schlüsselvergabe überprüft haben, zum Beispiel anhand des Personalausweises oder Reisepasses. Gleichzeitig stellt er allen potenziellen Empfängern von Signaturen seiner Kunden deren öffentliche Schlüssel in einem sicheren, aber frei über das Internet zugänglichen Verzeichnis zum Abruf zur Verfügung.



Trust Center vergeben elektronische Schlüssel.

In der aktuellen Gesetzgebung der Europäischen Union und in der Folge der Bundesrepublik Deutschland (Signaturgesetz 2001) werden die digitalen Signaturen nunmehr als „qualifizierte elektronische Signaturen" umschrieben. Diese basieren auf den schon genannten qualifizierten Zertifikaten. Durch hohe Sicherheitsanforderungen sollen dabei deren Zuordnung zum Unterzeichner und ihre Fälschungssicherheit gewährleistet werden. Die privatwirtschaftlich organisierten Trust Center haben mit Betriebsaufnahme der hierfür zuständigen Regulierungsbehörde für Telekommunikation und Post (RegTP) nachzuweisen, dass sie den strengen Anforderungen des Gesetzes gerecht werden. Das Einhalten bestimmter Kompatibilitätsanforderungen zu anderen Anbietern wird dabei jedoch nicht geprüft. Auf Wunsch kann sich ein entsprechender Anbieter akkreditieren lassen, um so durch eine umfassende Prüfung eine Art Gütesiegel für geprüfte Sicherheit zu erhalten.

Die existierenden Anwendungen im Bereich der gesetzeskonformen digitalen Signaturen sind aufgrund fehlender verpflichtender Standards derzeit proprietär ausgestaltet und oft inkompatibel: In vielen Fällen

Web-Service

Ein Beispiel, wie digitales Signieren technisch funktioniert, findet sich auf der Webseite der Mozquito Technologies AG:

- www.mozquito.org/digsig01.html

können qualifizierte Signaturen, die mithilfe eines bestimmten Anbieters erstellt worden sind, nicht mit der Software und Hardware eines anderen Anbieters überprüft werden. Derzeit bieten (neben auf bestimmte Berufsgruppen beschränkten Anbietern) lediglich zwei von der RegTP akkreditierte Trust Center (Signtrust und Telesec) qualifizierte elektronische Signaturen für Jedermann an. Nur wenige Bürger besitzen jedoch ein entsprechendes Schlüsselpaar.

Dadurch ist der eigentliche Zweck, ein elektronisches, allgemein akzeptiertes Pendant zur Handunterschrift zu schaffen, bislang nicht erreicht. Die Folge ist bekannt: Nur zögerlich finden (gesetzeskonforme) digitale Signaturen Beachtung im Massenmarkt. Das Ziel der Europäischen Kommission, durch die entsprechende Richtlinie aus dem Jahr 1999 und deren nationale Umsetzung die „allgemeine Akzeptanz elektronischer Authentisierungsmethoden zu fördern“, ist offensichtlich bis heute nicht erreicht worden. Der Staat ist dazu berufen, die Wirtschaft zu fördern und das Verwaltungshandeln zu optimieren. Hierzu gehört auch die Beachtung der Kompatibilität der vom Staat empfohlenen Technologien. Die Unterstützung der Bevölkerung, diese Technologie zu nutzen, kann im Bereich der digitalen Signaturen offensichtlich nicht allein der Wirtschaft überlassen werden. Das Abwarten, bis die privaten elektronischen Notare einheitliche Techniken einsetzen und für die umfassende Akzeptanz der digitalen Signaturen sorgen, ist nicht länger zu vertreten. Ähnlich wie bei der Personalausweis- und Pass-Vergabe muss der Staat daher die Verantwortung für die flächendeckende Einrichtung von Trust Centern mittragen.

Die Versorgung der Bevölkerung und auch der Verwaltung durch den Staat mit den entsprechenden Infrastrukturen würde zwei Aspekte hervorheben: Zum einen würde der Staat neben seiner legislativen und exekutiven Verantwortung auch der gesellschaftlichen Aufgabe der Förderung gesetzlich vorgesehener Technologien nachkommen. Die demonstrative Bejahung der digitalen Signaturen seitens des Staates würde außerdem das Vertrauen der breiten Bevölkerung in die Technik fördern. Zum anderen könnten die Behörden vor Ort als Registrierungsstellen auftreten. Die Bürgernähe der heutigen Verwaltung auch in örtlicher Sicht würde so einen wesentlichen Teil der nötigen Infrastruktur – die umfassende räumliche Verfügbarkeit – kostengünstig liefern. Daneben ist zu beachten, dass auch der Staat selbst und seine ausführenden Organe mittelfristig digitale Signaturen einsetzen werden. Spätestens mit den entsprechenden gesetzlichen Änderungen im Verwaltungsrecht muss der Staat wissen, woher er seine Zertifikate bezieht. Wenn er selbst als elektronischer Notar auftritt, so sollte er seine Dienste auch dem Bürger zur Verfügung stellen. Die wesentlichen hoheitlichen Aufgaben muss der Staat selbst erledigen. Die Gewährleistung sicheren, rechtsverbindlichen Handels im Cyberspace ist eine hoheitliche Aufgabe.

Prof. Dr. Christoph Meinel lehrt Informatik an der Universität Trier und leitet das Institut für Telematik, Trier. Dr. Lutz Gollan ist wissenschaftlicher Mitarbeiter am Institut für Telematik.

Digitale Signatur

Digitale Signaturen basieren auf einem Zwei-Schlüssel-Verschlüsselungsverfahren. Jeder Unterzeichner hat zwei Schlüssel, von denen der eine nur ihm zugänglich bleibt (privater Schlüssel) und der andere bekannt gemacht wird (öffentlicher Schlüssel).

Der private Schlüssel, der später zum Unterschreiben eingesetzt wird, befindet sich auf einem sicheren und überall verfügbaren Medium wie einer Smart Card. Der Empfänger der elektronisch signierten Nachricht ruft den zur Überprüfung der digitalen Signatur notwendigen, passenden öffentlichen Schlüssel aus einem frei zugänglichen Verzeichnis ab. Die digitale Signatur selbst enthält einen elektronischen „Fingerabdruck“, den Hash-Wert der zu signierenden Nachricht. Dieser nach einem allgemein bekannten Verfahren berechnete Hash-Wert wird mit dem privaten Schlüssel des Unterzeichners verschlüsselt und der zu signierenden Nachricht angefügt. Der Empfänger erzeugt nun einerseits mit dem gleichen Verfahren wie der Absender den Hash-Wert der Nachricht, entschlüsselt andererseits mit dem allgemein verfügbaren öffentlichen Schlüssel des Unterzeichners die Signatur. Stimmen die Hash-Werte überein, so steht der Unterzeichner fest. Außerdem ist sichergestellt, dass die signierten Daten während ihres Transports nicht verändert wurden – andernfalls hätte der Empfänger einen anderen Hash-Wert berechnet als der Unterzeichner.