Das virtuelle Paßamt

Doris Hummer

Bindergasse 3/6
A-1090 Wien
h8550767@obelix.wu-wien.ac.at

Schlagworte: Trust Center, Zertifizierungsdiensteanbieter, Zertifikat, Asymmetrische Kryptographie, Sicherheit, Zertifikatsklassen

Abstract: In fünf österreichischen IT-Betrieben werden zurzeit sogenannte Trust Center eingerichtet, die ähnliche Funktionen ausüben wie staatliche Behörden. Sie geben Zertifikate aus, die als Personalausweise im Cyberspace garantieren, daß der Inhaber der ist, der er vorgibt zu sein.

1. Einleitung

Die Zutrittsbestimmungen für das Rechenzentrum des Trust Centers von Global Sign ähneln denen eines Tresors. Videokameras überwachen den Eingangsbereich. Wenn Reparaturen oder Wartungsarbeiten fällig sind, dürfen zwei Leute mit Spezialausbildung den Raum mit zwei getrennten Zugangsberechtigungen betreten. Immer nur zwei Personen gemeinsam, denn Vertrauen ist gut, Kontrolle ist besser. Auch *Heinz Buczolich*, Projektleiter von *A-Trust* bestätigt diesen Standard: „Wir werden wahrscheinlich ein ähnliches Sicherheitskonzept für unsere Räumlichkeiten verwenden." *Dieter Kronegger*, Projektleiter für das zentrale Trust Center für alle anderen Trust Center bei der *Telekom Control*: „Wir verwahren die Daten in einer mit Drähten umwickelten Box auf, die sich selbst zerstört, wenn jemand versucht, sie zu öffnen."

Die echte Bedrohung für die Sicherheit lauert freilich nicht am physischen Ort der Verwahrung des Schlüssels. Hacker-Attacken sind es, die es abzuwehren gilt. Laut Signaturgesetz müssen die Sicherheitsstandards dem „Stand der Technik" entsprechen. In der Praxis heißt das, daß die Server beispielsweise mit denselben Firewall-Produkten, die in einem großen Industriebetrieb üblich sind, abgesichert werden. Viele davon orientieren sich am deutschen BSI Grundschutzhandbuch als Sicherheitsstandard.

2. Karten kommen über staatliche und kommerzielle Großprojekte unters Volk

Ein Betrieb kann die technische Infrastruktur von der Telekom Control überprüfen lassen und so als Trust Center zugelassen werden. Während es in Österreich mehrere Anbieter von sogenannten „nicht qualifizierten Signaturen" gibt, arbeiten drei Unternehmen zurzeit fieberhaft an der Realisierung der sicheren qualifizierten Signatur, der vor Gericht volle Beweiskraft zukommt. Die Datakom, A-Trust, ein Start-Up-Unternehmen der Bankenbranche, und Global Sign, ein Ableger eines belgischen Anbieters, wollen alle innerhalb der nächsten Monate mit einer sicheren Signatur auf den Markt kommen. Die Datakom will ab dem Wintersemester 2000 alle Studenten der Wiener Wirtschaftsuniversität mit Signaturkarten ausrüsten, die den bisherigen Studentenausweis ersetzen und die Studenten darüberhinaus bei allen Gelegenheiten im Internet, wie etwa Einkäufen und Behördenwege, eindeutig und rechtsverbindlich ausweisen. Ein zweiter großer Schub an Signaturkarten wird durch die A-Trust GmbH auf den Markt gebracht werden. Das Projekt A-Trust wurde von den österreichischen Banken ins Leben gerufen und soll die Transaktionsnummern-Listen (TAN) ersetzen, die Bankkunden derzeit etwa für den Kauf von Wertpapieren benötigen. Online-Banking, eines der e-Commerce-Produkte, das die größte Akzeptanz bei der österreichischen Bevölkerung findet, wird ab Herbst mit einer Signaturkarte erleichtert. *Heinz Buczolich*, Projektleiter von A-Trust, rechnet mit 35.000 ausgegebenen Karten bis zum Jahresende 2000. Insgesamt wird die Karte innerhalb der nächsten vier bis fünf Jahre an rund 300.000 Österreicher gehen. Der dritte Anbieter, Global Sign, hat über seine in ganz Europa tätigen Schwestergesellschaften vor allem bei der Ausstattung von Kommunen Erfahrungen sammeln können. In Deutschland stattet die Schwesterfirma Regiomarkt gerade die 90.000 Einwohner von Esslingen mit Unterschriftskarten aus. In Österreich will Global-Sign-Chef *Gerald Stickler* demnächst das Geschäft mit Städten und Gemeinden anbahnen.

3. Zertifikat im Browser

Die Sinnhaftigkeit der sicheren Signaturkarten nach dem neuen Gesetz ist indes in der IT-Branche nicht unumstritten. *Hans Zeger*, Geschäftsführer der Arge Daten, die ebenfalls als Trust Center zugelassen ist, sieht dafür „noch keinen Markt". Die Verbreitung des Internet sei noch zu gering. Sein Unternehmen bietet daher lediglich nicht qualifizierte Zertifi-

kate an, wie sie auch von den oben genannten Firmen und der Generali-Versicherung vertrieben werden. „Die Beweiskraft der nicht qualifizierten Zertifikate ist nicht automatisch gegeben. Sie hängt von der Prüfung durch einen gerichtlich beeideten Sachverständigen ab," erklärt *Michael Brauchl*, Leiter der Gruppe E-Commerce bei der Generali. Dementsprechend kann man mit der hauseigenen elektronischen Signatur auf der Web-Site der Versicherung auch keine einzige Polizze abschließen. Nicht qualifizierte Signaturen liegen im Regelfall nicht auf einer Karte, sondern sind direkt im Web-Browser abgespeichert.

Das Generali-Produkt umfaßt neben der Beglaubigung elektronischer Unterschriften auch ein Versicherungspaket. Durch die Haftpflichtversicherung sind Schadenersatzansprüche gedeckt, die durch eine Transaktion im Internet entstehen. Mit bis zu 450.000 Schilling springt die Generali für den Vertragsnehmer in die Bresche, wenn er mit der digitalen Signatur einen Personen-, Sach- oder Vermögensschaden irgendwo in der Welt verursacht. Eine Rechtsschutzversicherung und eine Mißbrauchsversicherung sind ebenfalls enthalten. *Michael Brauchl*: „Sollte ein Vertragsnehmer versehentlich jemanden durch eine verseuchte e-Mail mit einem Virus infizieren, zahlt die Versicherung. Dasselbe gilt, wenn sich ein Hacker Zugang zum Zertifikat des Versicherten verschafft." Zweitausend dieser versicherten Zertifikate sind momentan laut Generali im Umlauf. Laut Angaben von *Herbert Tischler*, Produktmanager von a-sign bei der Datakom hat sie in Österreich ebenfalls bereits rund dreitausend Kunden mit nicht qualifizierten Zertifikaten.

4. Kryptographie nach dem Stand der Technik: asymetrisches Verschlüsselungsverfahren

Für die sichere Signatur ist eine Chipkarte erforderlich. Sie spielt eine wichtige Rolle im asymetrischen Verschlüsselungsverfahren, dem „Stand der Technik" in der Kryptographie. Auf dem Karten-Chip wird der private Schlüssel generiert, das Gegenstück zum öffentlichen Schlüssel. Während der öffentliche Schlüssel – nomen est omen – im Internet öffentlich aus einem Verzeichnis des Trust Centers abrufbar ist, darf der private Schlüssel die Karte des Besitzers nie und nimmer verlassen. So will es das Signaturgesetz. Die Benutzung der Karte ist zusätzlich mit einem PIN-Code gesichert. Public und Private Key stehen zueinander in einer besonderen mathematischen Beziehung. Dabei ist es extrem unwahrscheinlich, daß ein Schlüssel aus dem anderen errechnet werden kann. Die dafür notwendigen Rechnerkapazitäten sind nicht realisierbar.

Bei der Übermittlung der digitalen Signatur wird aus der unterzeichneten Mitteilung mithilfe der mathematischen Hash-Funktion ein Code errechnet. Dieser wird mit dem Private Key verschlüsselt. Dieses „Hash-Wert" des Dokuments ist einzigartig. Die unverschlüsselte Botschaft wird zusammen mit dem HashWert versendet. Wird sie verändert, so paßt der öffentliche Schlüssel nicht mehr und es ist klar, daß das Dokument gefälscht wurde. Wenn die Botschaft intakt ist, kann über den Hash-Wert der Absender bestätigt werden.

Voraussetzung für den Anwender der digitalen Signatur sind ein PC mit Internet-Zugang sowie ein Kartenleser mit dazugehöriger Software. Die meisten Anbieter planen, die Signaturkarten in einem Paket mit dem Kartenlesegerät auszugeben.

5. Zertifikatsklassen und -typen

Die meisten Anbieter offerieren verschiedene Zertifikatsklassen. Beginnend mit einer light-Version, einer kostenlosen, nicht qualifizierten Signatur, die nach einigen Wochen abläuft erstreckt sich das Spektrum bis hin zum Klasse-3 – oder Premium-Zertifikat, für das der User sich in einer lokalen Registrierungsstelle persönlich ausweisen muß. Abgesehen von Personen kann man auch Server oder Programme zertifizieren lassen.