Jürgen Ecker

DIE DIGITALEN UNTERSCHRIFTEN VON MORGEN

Digitale Unterschriften auf digitalen Dokumenten können „echte“ Unterschriften ersetzen. Und mehr. Neue Ideen machen digitale Unterschriften noch flexibler.

Foto: privat

DI DR. Jürgen Ecker lehrt Daten- und Kommunikationssicherheit am Studiengang „Computer- und Mediensicherheit“ in Hagenberg.

Herkömmliche Unterschriften erfüllen viele Zwecke.

Wahrung der Integrität: Ein unterschriebenes Dokument kann nachträglich nicht mehr geändert werden, insbesondere ist es schwer eine Unterschrift auf ein anderes Dokument zu übertragen.

Sicherstellung der Authentizität: Die Unterschrift unter die mit Kreditkarte bezahlte Rechnung überzeugt den Händler davon, dass tatsächlich der Besitzer der Karte vor ihm steht.

Garantie der Unleugbarkeit: Die Unterschrift unter einen Vertrag bindet den Unterschreibenden an die Vereinbarungen im Vertrag. Er kann im Nachhinein nicht behaupten, den Vertrag nicht gelesen zu haben.

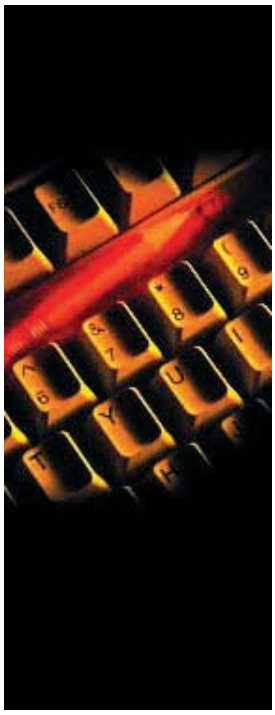
Eine digitale Signatur soll alle diese Funktionen einer herkömmlichen Unterschrift übernehmen können. Das ist schwierig. Elektronische Dokumente können kopiert und verändert werden, ohne dass dies bemerkt wird, ein Problem mit dem sich zurzeit vor allem die Musikindustrie herumschlägt.

Public-key Kryptographie und digitale Signaturen

Bei Public-key-Verschlüsselungssystemen ist der Schlüssel, der zur Verschlüsselung benötigt wird, nicht geheim, sondern öffentlich verfügbar. Lediglich der Schlüssel zum Entschlüsseln ist geheim und nur dem Empfänger bekannt. Dreht man nun einfach die Richtung um und benutzt den geheimen Schlüssel zum Verschlüsseln, so erhält man eine verschlüsselte Nachricht, die von jedermann mit Hilfe des öffentlichen Schlüssels entschlüsselt werden kann. Diese Nachricht taugt als Unterschrift, weil nur der Besitzer des geheimen Schlüssels sie erzeugen konnte. Die öffentlichen Schlüssel, die zur Überprüfung der Signatur benötigt werden, die Verifikationsschlüssel können dabei in einer frei zugänglichen Datenbank verwaltet werden, lediglich die Signaturschlüssel müssen geheim gehalten werden. Solche Signatursysteme können Integrität, Authentizität und Unleugbarkeit garantieren.

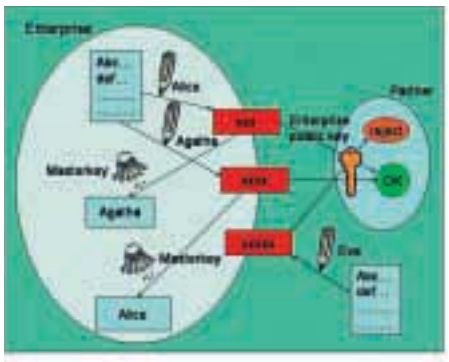
Gruppensignaturen

In großen Unternehmen oder Institutionen sind Zuständigkeiten und Berechtigungen oft über verschiedene Abteilungen und Personen verteilt. Soll nun ein Dokument für einen Geschäftspartner digital signiert werden, so stellt sich ein Problem:



Wenn jeder Mitarbeiter seinen eigenen Signaturschlüssel besitzt, so muss der Geschäftspartner die Verifikationsschlüssel aller Mitarbeiter des Unternehmens kennen, um gegebenenfalls die Unterschrift verifizieren zu können. Damit erhalten Außenstehende aber unter Umständen wertvolle Informationen, wer im Unternehmen welche Aufgaben und Berechtigungen besitzt; Wissen das Unternehmen nicht gerne weitergeben.

Alternativ dazu kann jeder Mitarbeiter den gleichen Signaturschlüssel verwenden. Dann braucht der Geschäftspartner nur einen Verifikationsschlüssel, um die Unterschrift zu überprüfen. Wenn aber Haftungsfragen auftreten, lässt sich nicht mehr feststellen, welcher Mitarbeiter unterschrieben hat.



Gruppensignaturen sollen dieses Problem lösen. Jeder Mitarbeiter besitzt einen eigenen Signaturschlüssel. Der Partner braucht jedoch nur einen Verifikationsschlüssel, den des Unternehmens. Unternehmensintern lässt sich jedoch gegebenenfalls feststellen, mit welchem der geheimen Schlüssel unterschrieben wurde.

Auf dem Gebiet der Gruppensignaturen wird erst seit den neunziger Jahren geforscht. Softwarelösungen für Unternehmen gibt es bislang aber noch nicht. In einer der ersten Bakkalaureatsarbeiten, die im Studiengang Computer- und Mediensicherheit geschrieben werden, widmet sich Ulrich Zehl dem Thema Gruppensignaturen und untersucht, welche Lösungen auch tatsächlich umsetzbar sind.