

baumann.at – concepts & solutions

DI Dr. Christian Baumann

Mail: cbaumann@baumann.at

Web: <http://www.baumann.at>

Tel.: +43 (0) 664 43 24 243

Die elektronische Signatur - Security-Trend 2006?

Es gibt wohl kaum mehr eine Geldbörse, in der sich keine Chipkarte findet. Bankomatkarten sind ebenso mit Chips versehen wie die e-Card der Krankenkassen.

Die Chipkarten könnten für eine große Anzahl von „sicheren“ Anwendungen eingesetzt, neben dem e-Government-Bereich (Amtswege Online - Stichwort "Bürgerkarte") sind das beispielsweise:

- e-Mail: Eindeutige Identifikation des Absenders und Möglichkeit die Nachrichten zu verschlüsseln. Damit könnte das Problem Spam (unerwünschte e-Mails, teilweise mit Viren) drastisch entschärft werden.
- Sicheres Online-Banking: Das Problem „Phishing“ (Identitätsdiebstahl im Internet und Missbrauch der PIN/TAN für Online-Betrug) wäre gelöst.
- Login bei Internetanwendungen (Portale, Webshops etc.): Keine Vielzahl an unterschiedlichen Benutzer-/Passwortkombinationen mehr notwendig.
- Elektronische Zustellung (umgangssprachlich als „eingeschriebene e-Mail“ bezeichnet): Nachweisbare, rechtssichere Übermittlung von elektronischen Dokumenten im behördlichen, wirtschaftlichen und auch im privaten Bereich.
- Digitales Unterschreiben von Online-Formularen und Abschließen von rechtsgültigen Verträgen über das Internet.

Mit diesen und weiteren Anwendungen wären enorme Potentiale realisierbar. Neben der Erhöhung der Sicherheit könnte die Benutzerfreundlichkeit und das Vertrauen in Onlineanwendungen stark gesteigert werden. Für Unternehmen bieten sich durch die Rechtsgültigkeit von Internettransaktionen diverse Optimierungspotentiale. Einerseits bei (Online-) Geschäften mit dem Endkunden, andererseits auch im B2B-Bereich. Hier bietet beispielsweise die elektronische Rechnungslegung ein Einsparungspotential in der Höhe von mehreren hundert Millionen Euro pro Jahr.

Mit einer elektronischen Zustellung könnten zig Millionen Schriftstücke rechtssicher übermittelt werden (kein Druck, keine Kuvertierung, drastische Reduktion des Portos, keine Medienbrüche).

Alle technischen und rechtlichen Grundlagen (Signaturgesetz) sind seit einiger Zeit gegeben, sowohl in Österreich, als auch in anderen Ländern Europas.

Die Preisfrage lautet nun: Warum wird die elektronische Signatur derzeit noch kaum eingesetzt? Es handelt sich hier um das typische "Henne-Ei" Problem:

Die Verbreitung unter den potentiellen Anwendern - besonders im privaten Bereich - ist sehr gering, weil es noch viel zu wenige Anwendungen dafür gibt. Es gibt so wenige Anwendungen, weil die Verbreitung so gering ist und die Einbindung der Signaturfunktionen in Webportale, Online-Shops etc. nicht ganz trivial ist und entsprechende Kosten verursacht. Und das würde sich erst auszahlen, wenn es mehr Benutzer gäbe ...

Dass die elektronische Signatur heute im e-Governmentbereich nur vereinzelt eingesetzt wird, im privaten Bereich aber kaum, darf nicht verwundern. Jede neue Technologie erlebt eine „Anlaufphase“ vor dem „Boom“, was beispielsweise beim Fax und beim Handy zu beobachten war. Auch die Killerapplikationen des Internet (e-Mail und Web) haben mehrere Jahre benötigt, um eine breite öffentliche Akzeptanz und dadurch die enorme heutige Verbreitung zu erreichen.

Die elektronische Signatur wird kommen – daran zweifelt kein Experte. Auch Bill Gates sieht „die Zukunft des sicheren Internet im Einsatz von digitalen Zertifikaten und der elektronischen Signatur“.

Wie funktioniert die sichere elektronische Signatur?

Die Basis bildet ein „digitales Zertifikat“ (eine Art elektronischer Ausweis). Dieses Zertifikat wird – um maximale Sicherheit zu gewährleisten – nicht auf einem normalen Datenträger gespeichert, sondern auf einem sog. „Hardware-Token“, typischerweise einer Chipkarte. Der auf dem Chip integrierte Prozessor wickelt die notwendigen Verschlüsselungsfunktionen ab. Um eine elektronische Signatur zu erstellen, muss zusätzlich ein PIN-Code (i.d.R. am Chipkartenleser) eingegeben werden.

Für automatisierte Anwendungen wird die „Serversignatur“ verwendet, bei welcher die Funktionen in einem sicheren Hardwaremodul implementiert sind – eine PIN-Eingabe ist nicht erforderlich. Weiters existieren reine Softwarelösungen, die zwar keine Chipkarte und keinen Leser benötigen, aber nur eine niedrige Sicherheitsstufe bieten.

Was benötigt man dafür?

Um als Benutzer/in eine sichere elektronische Signatur einsetzen zu können, benötigt man ein sog. „qualifiziertes Zertifikat“ auf einer Chipkarte und einen Chipkartenleser. Das qualifizierte Zertifikat wird nach Vorlage eines Ausweises bei einer Zertifizierungsstelle erstellt, mit der (vom Benutzer frei wählbaren) PIN verschlüsselt und auf der Chipkarte gespeichert. Derzeit gibt es in Österreich mehrere Hundert solcher Zertifizierungsstellen. Chipkartenleser sind bei neuen PCs teilweise bereits eingebaut, externe Geräte sind im Handel erhältlich. Die nötige Signatursoftware ist frei verfügbar. Die Initialkosten betragen (je nach Zertifikat und Chipkartenleser) ca. € 15 bis € 40.

Als Chipkarte kann entweder eine bereits vorhandene Karte verwendet werden (Bankomatkarte, e-Card, zukünftig auch der Personalausweis) oder optional eine eigene Karte, die nur die Signaturfunktion beinhaltet (ca. € 30,-).

Auch die im e-Government verwendete „Bürgerkarte“ ist keine spezielle Karte sondern lediglich eine Zusatzfunktion, die auf einer vorhandenen signaturfähigen Karte aktiviert werden kann.

Digitale Zertifikate und elektronische Signatur, bis vor kurzem noch als „Geheimwissenschaft“ betrachtet, werden ziemlich bald genauso bekannt und einfach zu verwenden sein wie e-Mail oder das Web. Erste Ansätze dazu sind bereits erkennbar. So wurde z.B. in einem bekannten Magazin, das sich mit dem Thema „e-Medien“ beschäftigt, kürzlich ein mehrseitiger Artikel veröffentlicht, der die Thematik in allgemein verständlicher Form darlegt. Auch eine Elektronikhandelskette hat („nicht blöd“)

den Trend erkannt und bietet neben dem „Bürger-PC“ (Standard-PC plus Chipkartenleser) als Zertifizierungsstelle die „Aktivierung der digitalen Signatur binnen 10 Minuten“.

Das Jahr 2006:

Die elektronische Signatur ist eine der Basistechnologien für das e-Government, in diesem Bereich gehört Österreich zu den Vorreitern in Europa. Die österreichische Bundesregierung will diese Rolle weiterhin einnehmen und plant daher für 2006 eine groß angelegte Werbe-/PR-Kampagne um die Verbreitung der elektronischen Signatur massiv zu forcieren.

Alle Unternehmen die im Internet präsent sind bzw. Online-Geschäfte abwickeln sollten die dadurch möglichen Synergieeffekte nutzen und auf den (noch langsam) rollenden Zug aufspringen, um den Anschluss nicht zu verpassen.