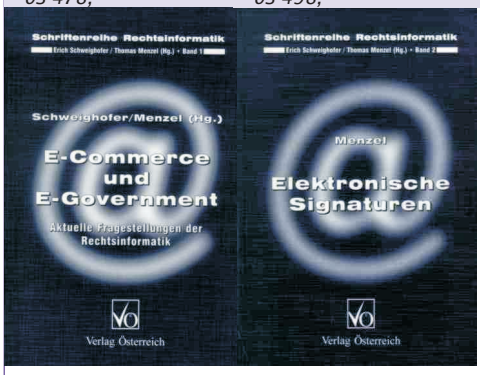
Schriftenreihe

Rechtsinformatik

Otto Cap

Band 1:
E-Commerce und E-Government,
Verlag Österreich,
ISBN 3-7046-1592-7,
230 Seiten, br.;
öS 478,-

Band 2:
Elektronische Signaturen,
Verlag Österreich,
ISBN 3-7046-1593-5,
265 Seiten, br.;
öS 498,-



Der - dem Juristen schon lang vertraute - Verlag Österreich (vormals Verlag der Österreichischen Staatsdruckerei) eröffnet mit den vorliegenden ersten beiden Bänden die neue Schriftenreihe "Rechtsinformatik". Auch für den Informationstechniker von Interesse ?

Ich möchte diese Frage - vor allem für jene, die sich mit dem Internet befassen - vorbehaltlos bejahen. Dieses weltweite Netz schafft nicht nur einen gemeinsamen Pool der Information, des Gesamtwissens der Menschheit, sondern ermöglicht es auch erstmals in der Geschichte, weltweit kommerziell zu kommunizieren, "im Fernverkehr" Geschäfte abzuschließen oder Dienstleistungen in Anspruch zu nehmen. Die historisch ganz unterschiedlich strukturierten Rechtsordnungen sind dem nur sehr bedingt gewachsen und müssen schleunigst dafür adaptiert werden, dass nicht mehr (nur) Papier und Tinte, sondern (auch) Bits und Bytes für das zustande Kommen von Verträgen verantwortlich sind.Nur eine fruchtbringende Rückkoppelung zwischen Informatik und Rechtswissenschaft wird dies erreichen können; der fachübergreifende Blick der Spezialisten beider Sparten ist gefordert!

Nach dieser Rechtfertigung für die Rezension einer vermeintlich nur für Juristen geeigneten Schriftenreihe in einer EDV-Zeitschrift nun zur Sache.

Der erste Band der Reihe "E-Commerce und E-Government" ist den Ergebnissen des 3. Internationalen Rechtsinformatik Kolloquiums im Februar dieses Jahres in Salzburg gewidmet. Referate zu den Sachgebieten Electronic Commerce, elektronische Signatur, E-Government, Elektronisches Publizieren, Wissensrepräsentation und Theorie der Rechtsinformatik spiegeln die Breite der Diskussion zu diesen Themen wider. Einige Referatstitel: Unerwünschte Direktwerbung per E-Mail (Spam), Das virtuelle Passamt, Amtshelfer Online, Elektronische Demokratie, Das Internet eine globale Agora. Wer sich für Trends und Perspektiven in diesen Bereichen und in der öffentlichen Verwaltung interessiert, erfährt exzellent den Stand der Dinge. Einen besonderen Schwerpunkt der Publikation sehe ich in den Beiträgen zum bevorstehenden Umbau der öffentlichen Verwaltung durch den Einsatz von Informationstechnologie. Ein hochkarätiges Kompendium zukunftsweisender Ansätze!

Unmittelbar praktischen Bedürfnissen dient der zweite Band der Reihe "Elektronische Signaturen". In handlichem Format und durchwegs flüssiger - trotzdem auch tiefschürfender - Darstellung werden dem Leser zunächst die informationstechnischen Grundlagen von Kryptographieverfahren und Anforderungen an ein sicheres Verschlüsselungssystem nahegebracht (natürlich nicht mit sämtlichen Details wie in einem informationstechnischen Spezialwerk, etwa dem in den PCNEWS 68 S. 76f. vorgestellten Werk “Kryptographie”, aber in allen wesentlichen Gesichtspunkten präzise dargestellt), um sodann den rechtlichen Hintergrund - die sogenannte Signaturrichtlinie der EU - und schließlich die österreichische Umsetzung im Signaturgesetz (in Kraft seit 1.1.2000) eingehend zu beleuchten.Dabei werden wirklich umfassend, ohne sich aber in einem "Paragraphengestrüpp" zu verlieren, also - soweit ich als Jurist dies beurteilen kann - auch für "rechtliche Laien" vollkommen verständlich, die wichtigen Begriffe einfaches und qualifiziertes Zertifikat, Zertifizierungsdiensteanbieter, Aufsichtsstelle und viele andere erläutert, aber auch besonders wichtige Themen wie die Rechtswirkungen elektronischer Signaturen, Haftungsregelungen, Anerkennung ausländischer Zertifikate und die Rechtssituation in anderen Ländern ausführlichst behandelt: Ein Werk, das allen empfohlen werden kann, die - ob geschäftlich, von der technischen oder der juristischen Seite her - eine profunde Information über elektronische Signaturen benötigen!

Woher kommt “SPAM” ?

Über die Ableitung dieser aus dem Amerikanischen kommenden Abkürzung kenne ich schon 3 Meinungen: so soll sie sich von einem Sketch aus Mountypython's Flying Circus ableiten, worin der Ausdruck "Spiced Pork And haM" etwa 20 mal vorkam und die Assoziation zu gehäuft auftretenden E-Mails herstellte; sie soll vom Erzeugnis der Lebensmittelfirma Hormel hergeleitet sein, deren Internetadresse lautet; schließlich wird die Ableitung von "Send Phenomenal Amounts of Mail" vertreten.

Und was scheint Ihnen am plausibelsten ?

Das Wesen einer Signatur

Digitale Signaturen sind keineswegs nur digitalisierte Versionen handschriftlicher Unterschriften; vielmehr handelt es sich um in einer bestimmten Weise versiegelte Nachrichten. Digitale Signaturen schließen nicht nur ein Dokument ab, sie sollen auch das unbemerkte bzw. unbefugte (etwa betrügerische) Einfügen von Textelementen verhindern. Digitale Signaturen sollen also Sicherheit über die Authentizität einer Nachricht, sowohl was Inhalt als auch Absender anlangt, bringen.Klar ist indes, das es bei einem Rechtsgeschäft über wenige Schilling geringerer Sicherheitsstandards (im Gesetz heißt dies "Sicherheitsstufen") bedarf als bei einem solchen, das in die Hunderttausende geht. Dementsprechend müssen auch unterschiedliche Standards zur sogenannten Zertifizierung eines Dokuments (Zertifikatsklassen) geschaffen werden (auch Kostenfrage!). Bei sogenannten symmetrischen Verschlüsselungsformen, bei welchen Sender und Empfänger denselben Schlüssel verwenden, muss dieser vor Beginn der Kommunikation auf sicheren Wegen zwischen den Partnern ausgetauscht werden. Als beste technische Erfordernisse dienen daher nach dem derzeitigen Stand der Technik sogenannte asymmetrische Verschlüsselungsverfahren(Schlüsselpaar bestehend aus einem sog. öffentlichen und einem privaten Schlüssel), wobei der Sender der Nachricht zur Sicherung der Vertraulichkeit mit seinem öffentlichen, zur Sicherung der Authentizität hingegen mit seinem privaten Schlüssel versiegelt und der Empfänger den jeweiligen Gegenschlüssel anwendet; wird beides benötigt, kommt eine Kombination von beiden zur Anwendung. Um das Verschlüsseln der gesamten Nachricht zu vermeiden, wird zusätzlich ein sogenannter Hash-Wert gebildet, der bei jeder neuerlichen Signatur vom Computer neu gebildet und verschlüsselt der Nachricht angefügt wird, sodass auch mittels Kopierens eines früheren Hashwertes keine Verfälschung des Textes möglich ist.

Die große Sicherheitslücke aller dieser Methoden liegt naturgemäß darin, dass der Inhaber eines bestimmten Schlüsselpaares zunächst einmal mit Sicherheit identifiziert und katalogisiert sein muss. Die Erlangung einer Authentifizierung unter Vorspiegelung einer falschen Identität muss verhindert werden.Diesem Bedürfnis dienen Zertifizierungstellen, im Gesetz Zertifizierungsdiensteanbieter genannt, die - soferne sie qualifizierte Zertifikate (für "sichere" elektronische Signaturen) vergeben wollen - einer staatlichen Aufsicht unterstellt sind und zu ihrer Zulassung besondere informations- und sicherheitstechnische Fachkenntnisse sowie kaufmännische Seriosität (Haftpflichtversicherung) nachweisen müssen.

otto.cap@utanet.at