Digitale Signatur

Digital unterschreiben: Hintergründe, Chancen und Risiken

Entgegen der gedämpften Stimmung rund um die sogenannte „New Economy“ gewinnt das Internet als **Handelsplattform** unvermindert an Bedeutung. Damit verbunden steigt der Bedarf nach sicheren und beweiskräftigen Verfahren für den elektronischen Schriftverkehr. Anbieter sowie Kunden erwarten bei online übermittelten **Bestellungen**, **Rechnungen** und **Verträgen** eine mit herkömmlichen Verfahren zumindest vergleichbare **Fälschungssicherheit** und **eindeutige Identität** des Gegenübers.

Vor allem bei den Nutzern bestehen immer noch weit verbreitete **Vorbehalte** gegenüber dem e-Commerce hinsichtlich **Datenmissbrauch** und unseriösen Geschäftspraktiken. Gemäß einer EMNID-Studie fürchten immerhin **75 Prozent** der dem e-Commerce aufgeschlossenen einen möglichen Missbrauch ihrer Daten. Von den Totalverweigerern nennen 70 Prozent **Sicherheitsbedenken** als Grund für Ihre Zögerlichkeit beim Online-Shopping.

Anbieter, die ihren Kunden eine sichere Übertragung sensibler Daten garantieren können, gewinnen **Vertrauen** und erhöhen ihre **Chancen**, in Zukunft **nachhaltig e-Commerce-Umsätze** und **Kundenbindungseffekte** zu erzielen.

Sind die heute verfügbaren rechtlichen Bestimmungen und technischen Verfahren wirklich geeignet, das Vertrauen der Anwender in den e-Commerce zu steigern? Lohnt sich deren teilweise kostspieliger Einsatz für Unternehmen?

Rechtliche Grundlagen für Sicherheit im e-Commerce sind gelegt

Die Rahmenbedingungen für Rechtssicherheit im e-Commerce hat die EU mit Ihrer **Signaturrichtlinie** geschaffen. Sie wurde in Deutschland mit Wirkung vom 22. Mai 2001 durch die Neufassung des **Signaturgesetzes** (SigG) in nationales Recht umgesetzt.

Rechtsverbindlich ist die digitale Unterschrift jedoch erst seit dem 1. August 2001 mit der Novellierung von rund 400 Rechtsvorschriften des **Zivilrechts**. Überall dort, wo die einfache Schriftform verlangt wird, muss bis auf wenige Ausnahmen die **digitale Signatur** daneben **als gleichwertig zugelassen** werden.

Digitale Signatur

Digital unterschreiben: Hintergründe, Chancen und Risiken

Technische Verfahren zur digitalen Signatur sind einsatzfähig!

Von einer **Zertifizierungsstelle**, deren technische Einheit ein sogenanntes **„Trust-Center“** ist, erhalten Nutzer auf Antrag und nach einer Identitätsprüfung ihr **Zertifikat**. Dieses wird auf eine **Signaturkomponente** (z.B. Chipkarte) übertragen.

Ein **privater elektronischer Schlüssel**, mit dem der rechtmäßige Besitzer die **digitale Unterschrift** für sein elektronisches Dokument (z.B. ein e-Mail) erzeugt, befindet sich auf einer separaten Signaturkomponente. Mit Hilfe des dazugehörigen **öffentlichen Schlüssels**, der beim Trust-Center öffentlich einsehbar archiviert ist (Public-Key-Infrastruktur), kann der Empfänger die Signatur **überprüfen**.

Die **Registrierungsstellen** (z.B: viele Industrie- und Handels-kammern) organisieren als Kooperationspartner die **kostenpflichtige Ausgabe der Chipkarten** z.T. in Verbindung mit Lesegeräten und Software.

Vorteile gegenüber dem klassischen Schriftverkehr?

Ungeachtet aller Bedenken hinsichtlich Sicherheit und Praktikabilität bietet das digitale Verfahren einen großen Vorteil: Zertifizierungsanbieter sind **haftpflichtig** für Schäden, die dadurch entstehen, dass sie die gesetzlichen Anforderungen schuldhaft verletzen oder ihre Signaturen und Einrichtungen schuldhaft versagen.

Tatsache ist, dass heute im Geschäftsalltag umfangreiche Lieferungen und Leistungen auf Grund von **Telefon und Faxaufträgen** ohne vergleichbare Prüfmechanismen ausgeführt werden. Selbst ein mit Kugelschreiber signiertes Dokument kann von jemand anderem stammen, als die Unterschrift glauben macht. Ein digital signierter Auftrag bietet **im Vergleich erweiterte Anspruchmöglichkeiten** für den Geschädigten.

Die gesetzlich anerkannte digitale Signatur bietet gegenüber klassischen Papier-Dokumenten eine technisch bedingt höhere **Fälschungssicherheit**. Der Absender einer Nachricht kann vom Empfänger unkompliziert und weitgehend **zweifelsfrei identifiziert** werden. Eventuelle **Manipulationen** der Nachricht auf dem Weg zu ihrem Empfänger werden **erkennbar**. Diese augenscheinlichen technischen Vorteile sind juristisch allerdings bisher nicht vollumfänglich nutzbar: als **Beweismittel** im Zivilprozess

ist das elektronische Dokument **nicht einer Urkunde entsprechend anerkannt**.

Hundertprozentig sichere Systeme gibt es nicht!

Nicht die Digitale Signatur ist unsicher, sondern die **Systeme**, auf denen die Verarbeitung stattfindet. Dazu Hajo Bickenbach von der Deutschen Post SignTrust: *„Bei bestimmungsgemäßem Gebrauch ist das Produkt sicher. Die Integrität des Systems muss vom Benutzer sichergestellt werden“*.

Den **„Schwarzen Peter“** hat demzufolge der Anwender selbst: Genau wie bei den etablierten Verfahren, z.B. bei der EC-Karte, handelt **grob fahrlässig** oder schuldhaft, wer seine Chipkarte und die Geheimnummer **anderen zugänglich** macht. Bei Missbrauch muss der **Kunde beweisen**, dass es einem anderen möglich war, seine Signatur zu fälschen und seine Ansprüche gegen das Trust-Center juristisch durchsetzen. Das reduziert hingegen für den e-Commerce Betreiber das Risiko beim Vertrauen auf die **Echtheit einer digital signierten Bestellung**.

Vom Durchbruch weit entfernt!

Angesichts der **gewaltigen Investitionen und Betriebskosten** der Trustcenter liegt es nicht zuletzt in deren Interesse, eine **starke Verbreitung** und Nutzung der digitalen Signatur zu erreichen. Von **zielgerichteten Aktivitäten** in Form von **Werbung** und **vertrauensbildenden** Maßnahmen ist derzeit aber nur wenig zu spüren. Zwar sind die **Kosten** im Bereich B2B weithin **vernachlässigbar**, aber im Bereich der Privatanwender ist fraglich, wie schnell die **Infrastruktur am heimischen PC** hinreichend verbreitet ist.

Die Verifizierung der "elektronischen Ausweise" ist und bleibt **technisch aufwendig**, die **Abfrage auf ungültig gewordene Signaturen umständlich**. Eine **Massennutzung** könnte nach Ansicht von Sicherheitsfachleuten die Trust-Center überfordern. Überdies sind die Schlüssel verschiedener Zertifizierungsstellen und die zugehörige Software **nicht untereinander kompatibel**. Im schlimmsten Fall brauchen die Anwender dann **für jeden Dienst eine separate Karte** von einem anderen Trust-Center.

Die Attraktivität des Verfahrens für Organisationen und Unternehmen ist derzeit noch dadurch eingeschränkt, dass es **keine**

Digital unterschreiben: Hintergründe, Chancen und Risiken

Gruppenzertifikate oder **Stellvertreterregelungen** gibt. Jede Signatur gehört untrennbar zu einer **natürlichen Person**. Ist diese aber gerade nicht verfügbar, lässt sich ein Dokument nicht signieren, wenn nicht auch **alle anderen** Personen im Unternehmen über **Zertifikate und die technische Infrastruktur** (Chipkartenleser und Software) verfügen.

Einsatz zur Zeit nur im B2B-Bereich empfehlenswert

Heute sind die Experten allgemein der Auffassung, dass im Verkehr unter **Geschäftspartnern Chancen** und Nutzenpotenziale für die Etablierung der digitalen Signatur bestehen. Im Bereich der **Privatanwender** hingegen bleibt dies fragwürdig, allein schon wegen der Fülle von Trust-Centern und der mangelnden Verbreitung von Kartenlesern nebst Anwenderprogrammen.

Nur für Geschäftsbeziehungen, bei denen beide Seiten **mehr Rechtssicherheit und vor allem Prozessoptimierung** in den Abläufen als Vorteil erkennen, wird man die Infrastrukturen schaffen und das Personal entsprechend schulen, um die Vorteile nutzen zu können. Für diesen Einsatzbereich stehen allerdings auch kostengünstigere Stand-alone-Lösungen verschiedener Anbieter zur Verfügung.

Sie haben weitere Fragen zum Thema Digitale Signatur, wie und wo sie schon heute **sinnvoll eingesetzt** werden kann und wie die **Risiken** auf ein **Minimum reduziert** werden können?

Unsere Berater stehen Ihnen gerne zu Ihrer Verfügung.

Ihr e-trend Team

e - t r e n d

Impressum

e-trends im Abo
Ausgabe 7
September 2001
ISSN 1618-5854

Verantwortlich
Hauke Peyn (Geschäftsführer)
Volker Liedtke (Geschäftsführer)

e-trend
Media Consulting GmbH
Herforder Str. 74
33602 Bielefeld
fon +49(521) 96751-0
fax +49(521) 96751-99

http://www.e-trend.de
e-Mail: newsletter@e-trend.de

Newsletter-Abo unter
http://www.e-trend.de/newsletter

Alle Angaben ohne Gewähr
© Copyright e-trend 2001