




Management und Wissen


Digitale Signatur


Akkreditierung ohne Zukunft?

Rund ein Jahr nach dem neuen Signaturgesetz hat Ende Mai 2002 einer der ganz großen Anbieter qualifizierter elektronischer Signaturen aufgegeben. Die KES hat Konkurrenz, Anwender, Forschung und Politik gefragt, wie es wohl weitergehen wird mit der digitalen Signatur.

Die Deutsche Post Signtrust wird im Zuge der Neustrukturierung des Konzerns aufgelöst, meldete die Deutsche Post Ende Mai. Mit der elektronischen Signatur habe man als einer der führenden Anbieter auf diesem Markt die rechtsverbindliche Kommunikation im Internet vorangetrieben. Die allgemeine Marktsituation erlaube jedoch keine Fortsetzung des Geschäfts: "Die Zeit für eine solche Technologie ist noch nicht reif. Unsere Pläne für die Geschäftsentwicklung waren unter den gegebenen Bedingungen nicht einzuhalten. Als börsennotierter Konzern müssen wir immer den Wertbeitrag eines jeden Geschäfts im Auge behalten", äußerte Dr. Clemens Beckmann, Geschäftsführer der eBusiness GmbH der  [Deutschen Post](#) in einer Pressemitteilung.

Als die KES vor einem Jahr nach Erwartungen an das neue Signaturgesetz (SigG) gefragt hat, waren die Antworten überwiegend positiv (vgl. KES 2001/3, S. 6). Viele favorisierten die höchste Qualitätsstufe, qualifizierte Signaturen mit Anbieterakkreditierung: als einzig zukunftssicher (GI), Bekenntnis zur Haftung (DATEV) oder transparente, echte Sicherheit (Signtrust). Das Ende der abwartenden Haltung wurde prognostiziert (Telesec). Das Jahr hat zwar – auch große – Pilotprojekte in geschlossenen Benutzergruppen gebracht, aber keinen breiten Durchbruch (s. a. S. 14). Das Aus bei Signtrust hat unserer neuerlichen Stimmensammlung nun ein dunkles Vorzeichen beschert.

Johannes Feulner, CEO der  [fun communications GmbH](#), befindet sich ebenfalls auf dem geordneten (Teil-)Rückzug: "Bis zur flächendeckenden Verbreitung der digitalen Signatur ist es noch ein weiter Weg. Nicht nur müssen Karten und Lesegeräte erst in großer Stückzahl in den Markt gebracht werden, eine zweite Hürde ist die Realisierung eines effizienten Workflows für die Bearbeitung von Online-Formularen in den Behörden. Wir haben erkannt, dass für uns als Lösungsanbieter kurz- und mittelfristig mit der Digitalen Signatur kein nennenswerter Umsatz zu generieren ist und uns deshalb dazu entschlossen, die Vermarktung unserer Signaturkomponente fun eContractor nicht weiter zu verfolgen."

Ernüchterung zeigt sich auch bei Stefan Engel-Flehsig, CEO der  [Radicchio](#)-Initiative für drahtlosen E-Commerce: "Die aktuelle Entwicklung könnte Deutschland seine Rolle als europäischer Vorreiter für digitale Signaturen kosten. Obwohl die deutsche Signaturgesetzgebung große Beachtung fand, hat sie ihr eigentliches Ziel verfehlt, einen

Markt für sicheren E-Commerce zu etablieren." Signtrust sei übrigens in Europa nicht der erste Anbieter, der das Handtuch wirft: Schon letztes Jahr hätte das Schweizer Unternehmen Swisskey, später dann Interclear in Großbritannien dicht gemacht. "Andere könnten in Kürze folgen", befürchtet Engel-Flehsig.

Probleme sieht Engel-Flehsig weder in fehlender Expertise, Technologie, Gesetzgebung noch Standardisierung: "Womöglich waren einfach unsere Erwartungen zu hoch. Vielleicht haben wir die Fähigkeiten des Marktes überschätzt, den Graben zwischen technischen Möglichkeiten und alltäglicher Realität zu überwinden. Nach dem Hype ist jetzt Realismus eingekehrt und wir müssen einsehen, dass wir uns noch immer in der Pilotphase der 'Early Adopters' befinden. Zumindest lässt das Raum für Hoffnungen."

Nicht die letzte Schließung...

Eine längere Durststrecke und weitere Konsolidierung bei Trustcentern erwartet die Information Risk Management Group von [KPMG Deutschland](#): "Der Mittelstand und der Endverbraucher werden auf das nächste Jahrzehnt betrachtet von der – nach wie vor – hohen Komplexität der gesetzlichen Anforderungen und unterschiedlichen Signaturtypen 'verschont' bleiben, was aber auch dazu führt, dass sich deutschlandweit höchstens ein bis zwei akkreditierte Zertifizierungsstellen halten werden, da ohne entsprechende Nachfrage für diese Dienstleistung keinerlei Gewinn zu erwirtschaften ist", so Brad Chapman. "Wir sind der Meinung, dass sich die digitale Signatur nur im automatisierten B2B-Bereich bei großen Unternehmen durchsetzen wird, aber erst, wenn SAP und Co. diese Funktionalität implementiert haben."

Für die [Giesecke & Devrient GmbH](#) äußerte Andrea Bockholt Verständnis für Rückzieher: "In Deutschland gibt es de facto die qualifizierte Signatur nur mit Anbieterakkreditierung. Der Markt fragt Lösungen auf diesem Sicherheitsniveau aber nicht in dem Umfang nach, den ein Dienstleister zur Refinanzierung benötigt. Was wir jetzt brauchen, ist eine Lösung auf hohem Sicherheitsniveau, die den Ansprüchen der Kunden genügt, bezahlbar ist und vom Staat anerkannt wird. Nur so kann sich die digitale Signatur in Deutschland endlich durchsetzen."


Dr. Johann Bizer, Assistent am Institut für öffentliches Recht der Universität Frankfurt/Main, sieht ganz schwarz für die Hochsicherheitszertifikate: "Akkreditierte Signaturen sind praktisch tot. Grund sind aber nicht die Anbieter, sondern die potenziellen Kunden – sie brauchen akkreditierte Signaturen nicht." Im B2C verschlechtere ein Kunde durch die Beweisvermutung einer qualifizierten Signatur auf eigene Kosten seine Situation – er verschafft im Wesentlichen seinem Vertragspartner ein Beweismittel gegen sich selbst (vgl. [DuD - Datenschutz und Datensicherheit](#), 2002/5, S. 276). Und: "Der B2B-Bereich kommt unter definierten Rahmenbedingungen auch ohne akkreditierte Signaturen wunderbar aus. Rettung verspricht auch keine elektronische Rechnung für den Vorsteuerabzug. Eher werden kleine und mittlere Unternehmen Sammelrechnungen per Papier verschicken als ihre gesamten Prozesse auf akkreditierte Signaturen einzurichten. Die Zukunft gehört fortgeschrittenen Signaturen in geschlossenen Benutzergruppen."


Auf fortgeschrittene Signaturen von TC Trustcenter setzt derzeit auch die Deutsche Bank 24 bei einem [Pilotprojekt einer multifunktionalen Bankkarte \(Websign 24+\)](#). Aktuell schrieb [TC Trustcenter](#) in einer Pressemitteilung: "Viele sind überrascht über den Ausstieg der Deutschen Post World Net aus dem Zukunftsgeschäft mit der digitalen Signatur." TC TrustCenter habe bereits im letzten Jahr eine breit angelegte empirische Studie durchgeführt

und darin die Marktentwicklung analysiert und prognostiziert: "Diese ist exakt deckungsgleich mit der aktuellen Entwicklung."


Erfolgreiche Projekte zeigten einen großen Markt für Signaturen im Unternehmensbereich (B2E und B2B). Jedoch: "Die digitale Signaturkarte für 'jedermann und jede Anwendung' (B2C) war in der Vergangenheit oftmals mehr publicity- und medienwirksamer Wunschgedanke als pragmatisch mit breitem Anwendungsnutzen versehen. Aber auch in diesem mittelfristig attraktiven Anwendungsfeld sind die Voraussetzungen geschaffen und werden die Nutzenpotenziale deutlich. Treiber sind die Finanzdienstleister, Bund, Länder und Kommunen, das Gesundheitswesen sowie die Telekommunikationsindustrie. Die flächendeckende Verbreitung wird sich über die nächsten drei Jahre erstrecken", so die Zukunftsaussichten laut TC Trustcenter.

Kompatibilität ist Trumpf


Bedenken angesichts der aktuellen Marktlage äußert Rainer Gerling, Datenschutzbeauftragter der  [Max-Planck-Gesellschaft \(MPG\)](#): "Solange jeder Anbieter von Signaturlösungen sein eigenes inkompatibles Süppchen kocht, ist es für den Anwender wenig attraktiv einzusteigen. Erst uneingeschränkte Kompatibilität kann eine Marktdurchdringung bringen. Die MPG verzichtet bisher auf gesetzeskonforme Signaturlösungen und setzt bei Signaturen und Verschlüsselung bei E-Mail PGP/GnuPG ein."

Auch Andrea Muth von  [TeleCash](#) sieht offene Standards, eine Beschränkung auf wenige, untereinander kompatible Trustcenter und die Abkehr von Insellösungen als Erfolgsfaktoren der digitalen Signatur. Sie werde "erst dann erfolgreich sein, wenn der Nutzen des Verbrauchers die Zugangshürden (Beschaffung, Kosten) übersteigt und das Zertifikat multifunktional eingesetzt werden kann." Als mögliche Multiplikatoren könnten Kreditinstitute fungieren.

Qualitätssicherung beibehalten

"Akkreditierte Trustcenter haben ihre Existenzberechtigung. Sie sind technologisch sehr gut und vergleichbar mit dem TÜV für unsere Autos: Verglichen mit anderen Ländern, sind deutsche Autos sicherer. Die stetige Prüfung zahlt sich auf unseren Straßen aus. Auch das Internet braucht eine solche professionelle Ordnung", meint Ismet Koyun, Geschäftsführer von  [KOBIL Systems](#). "Deutschland hat die digitale Signatur ins Leben gerufen. Da es eine deutsche/europäische Strategie ist und keine amerikanische, traut man dem zukünftigem Erfolg jedoch nicht."

Dennoch stelle sich die Frage, ob man mit der qualifizierten Signatur ohne Anbieterakkreditierung nicht die bessere Wahl treffe: mit den gleichen technischen Komponenten, aber ohne teure Zulassungsverfahren. "Nicht jeder Mitarbeiter einer Firma hat Zeichnungsbefugnis, aber der Zugriff auf sensitive Daten muss überall geschützt sein", gibt Koyun zu bedenken.

"Der Aufbau von Infrastrukturen für die Digitale Signatur benötigt Zeit und verursacht erheblichen Aufwand. Ob oder wann sich diese Investitionen rechnen, ist für die Anbieter in diesem neuen Markt kaum abzuschätzen. Grund hierfür ist unter anderem, dass der Nutzen einer Signatur-Anwendung häufig nicht oder zumindest nicht *nur* beim Inhaber der Karte liegt. Daher müssen meines Erachtens diejenigen Modelle überdacht werden, bei denen die Kosten für die Signaturkarte ausschließlich vom Anwender zu tragen sind", gibt der 

[Bundesbeauftragte für den Datenschutz](#), Dr. Joachim Jacob, zu bedenken, und: "Weiter sollte der Anwendungsbereich – und damit der Markt – des Signaturgesetzes genauer eingegrenzt werden. So sehr ich auch den Einsatz sicherer Systeme fordere: Nicht jeder Zahlungsvorgang im Internet benötigt eine qualifizierte digitale Signatur."

Ähnliche Bedenken äußert Prof. Dr. Helmut Reimer vom [TeleTrusT Deutschland e.V.](#): "TeleTrusT hat bereits im November 1998 darauf hingewiesen, dass theoretisch begründete Forderungen nach höchster Sicherheit und die darauf gerichtete gesetzliche Regulierung marktgerechte Anwendungen der Digitalen Signatur nicht stimulieren." Geschäftsprozesse benötigen angemessene Sicherheit, ihre Anforderungen seien genauso individuell wie die Prozesse selbst. "Meist ist es im Leben eben nicht so, dass sich die an einem Geschäftsprozess Beteiligten überhaupt nicht kennen und die Sicherheit deshalb allein an einer Hochsicherheits-Signatur zu verankern ist. Die Geschäftswelt ist, wie sie ist – nicht wie Sicherheits-Theoretiker sie sich wünschen mögen."

Auf nicht-qualifizierten Zertifikaten beruhende Signaturen würden behördlicherseits (RegTP) zumindest indirekt a priori mit einer Unsicherheitsvermutung belegt und damit diskreditiert. TeleTrusT sieht zwei Alternativen, um mittelfristig Signaturanwendungen zu verbreiten: "Entweder orientiert sich die Regulierungsbehörde für Telekommunikation und Post (RegTP) darauf, die Flexibilität und Anwendungsorientierung von Zertifizierungsdiensteanbietern zu akzeptieren und zu fördern; was bedeutet, dass ihre Aufsichtsfunktion gegenüber angezeigten Dienstleistern wichtiger wird als ihre Rolle als Wurzelinstanz für akkreditierte Anbieter. Oder die öffentliche Hand beteiligt sich maßgeblich an den durch das Signaturgesetz geforderten Infrastrukturaufwendungen, indem zum Beispiel Personaldokumente mit Signaturfunktion eingeführt werden."

Auch nach Ansicht des [Instituts für Telematik, Trier](#) zeigt der Ausstieg der Deutschen Post Signtrust, dass "der Staat das Thema Sicherheitsinfrastruktur fürs Internet nicht kommerziellen Anbietern überlassen darf". Prof. Christoph Meinel, Direktor des Forschungs- und Entwicklungszentrums, befürchtet, dass die Durchsetzung der digitalen Signatur in Deutschland "nun noch stärker in die Sackgasse" geraten werde und forderte den Staat auf, "endlich seine hoheitliche Aufgabe wahrzunehmen, um im digitalen Zeitalter die Sicherheitsinfrastruktur für den immer bedeutender werdenden elektronischen Handel zu garantieren". Meinel zog einen Vergleich mit der Sicherheit, die amtliche Personalausweise und Pässe bieten.

Quelle: Studie "Zertifizierungsdienste-Anbieter in Deutschland",
 Institut für Telematik (www.ti.fhg.de/publikationen/studien_und_bucher/)

Stand: März
 2002

* einziger Anbieter eines ausschließlichen Zeitstempeldienstes ist Authentidate (www.authentidate.de)

	Telesec	Medizon	TC Trustcenter	D-Trust
Eigenes Trustcenter	ja	nein (Signtrust)	ja	ja
Komponente zur Schlüsselerzeugung	Schlüsselgenerator TC-SG Deutsche Telekom	Schlüsselgenerator KG-DPAG Deutsche Post	Smart Card StARCOS, Giesecke & Devrient (G&D)	Smart Card MICARDO Public, Orga ("D-TRUST-CARD")
Schlüsselspeicherung und Signatur-Erstellung	PKS-Card, Deutsche Telekom	SEA-Card, Deutsche Post	Smart Card StARCOS, G&D	Smart Card MICARDO Public, Orga
Systemvoraussetzung	MS Windows 95/NT4	MS Windows 9x,/NT4/2000	MS Windows 98/NT/2000	MS Windows 9x/NT/2000
Darstellung zu signierender Daten	TCrypt-SigG, Deutsche Telekom	Plug-in eTrust Mail für MS Outlook, Lotus Notes R5	SecSigner, Sec- Commerce	ID2/Smarttrust Personal i. V. m. MS Outlook
Überprüfung signierter Daten	TCrypt-SigG, Deutsche Telekom	Plug-In Signtrust eTrust Mail für MS Outlook, Lotus Notes R5	SecSigner, Sec- Commerce	ID2/Smarttrust Personal i. V. m. MS Outlook
Empfänger-Voraussetzung	wie Signierender	wie Signierender	wie Signierender	S/MIME- fähiger E-Mail Client und Root-Zertifikat
Sicherer Verzeichnis-Dienst	ÖVTC- Verzeichnis- Dienst, Deutsche Telekom	DIR-DPAG, Deutsche Post	TC-DIR, TC Trustcenter	OCSP- Responder, Secunet
Zeitstempeldienst*	(für PKS-Nutzer)	TSS Timeproof	k. A.	k. A.
Kosten	Chipkarte einschließlich Attribut-Zertifikat: €27,35 jährlich: €49,83	Chipkarte inkl. Gebühr für ein Jahr: €150,- jährlich: €75,-	k. A.	Chipkarte inkl. Gebühr für 3 Jahre: €49,-
Internet-Adresse	www.telesec.de	www.medizon.de	www.trustcenter.de	www.d-trust.de

Zertifizierungsdiensteanbieter, die nach dem deutschen Signaturgesetz als Trust Center ("Elektronischer Notar") arbeiten dürfen und keine eingeschränkten Kundenkreise haben. Hinzu kommen als Anbieter für Notare, Rechtsanwälte und Steuerberater die DATEV, die Bundesnotarkammer sowie verschiedene örtliche Rechtsanwalts- und Steuerberaterkammern.

Parole "Durchhalten!"

Die Regierung scheint indes beim bisherigen Modell bleiben zu wollen. Regina Wierig antwortete als Pressesprecherin des [Bundeministeriums für Wirtschaft und Technologie](#): "Die Bundesregierung hat mit dem Kabinettsbeschluss vom 16. Januar 2002 ein deutliches Bekenntnis zum breiten Einsatz elektronischer Signaturen bei E-Government-Dienstleistungen abgegeben. Hierbei sollen die qualifizierten elektronischen Signaturen überall dort zum Einsatz kommen, wo dies nach Rechtsvorschriften erforderlich ist oder, zum Beispiel aus Gründen der Beweissicherheit, geboten erscheint. Die Bundesregierung begrüßt hierbei ausdrücklich, dass Zertifizierungsdiensteanbieter auf Basis der freiwilligen Akkreditierung Signaturprodukte und Dienstleistungen anbieten, die einem hohen Sicherheitsstandard entsprechen"

Keinen Grund für Unruhe sieht Judith Balfanz, Leiterin Marketing bei der [AuthentiDate International AG](#): "Wir – als akkreditierter Anbieter – halten es in erster Linie für wichtig den Markt nicht unnötigerweise zu verunsichern. Es gibt nach wie vor noch mehrere akkreditierte Anbieter, sodass das Ausscheiden eines Einzelnen nicht überbewertet werden sollte." Im Übrigen verwies Balfanz auf bestehende Lösungen zur SigG-konformen Rechnungsstellung (E-Billing). Es habe sich gezeigt, "dass Unternehmen insbesondere im Bereich E-Billing außerordentlich hohe Einsparpotenziale innerhalb kürzester Zeit realisieren können. Dies wird allein durch qualifizierte Signaturen möglich. Diese können bei Einsatz geeigneter, bereits verfügbarer Technik, die Kosten der Wirtschaft senken – nicht erhöhen. Entsprechende ROI-Betrachtungen haben wir bereits durchgeführt."

Die Bundesdruckerei-Tochter [D-TRUST GmbH](#) fokussiert ebenfalls weiter auf qualifizierte elektronische Signaturen: "Wir richten unser Engagement jetzt noch stärker auf den Bereich öffentliche Verwaltung", so die D-TRUST-Geschäftsführer Norbert Frauböse und Achim von Berg. Auch sie führen zudem positive Beispiele an, beispielsweise den digitalen Dienstausweis für Bundesbehörden (vgl. S. 39), eine Bürgerkarte für Bremerhaven, Ulm und Passau sowie ein Projekt beim Europäischen Patentamt, über das derzeit 700 Patentanwälte neue Patente mittels D-TRUST-Signatur online anmelden.

Peter Willig, Leiter der Öffentlichkeitsarbeit der [DATEV eG](#) schrieb: "Die DATEV forciert nach wie vor die digitale Signatur für den elektronischen Rechts- und Geschäftsverkehr. Sie ist überzeugt, dass auf diese Weise eine sichere Infrastruktur für E-Business und E-Government geschaffen wird." Die teilweise pessimistischen Einschätzungen zur zögerlichen Verbreitung der digitalen Signatur teile man deshalb nicht, sondern sei im Gegenteil "der Auffassung, dass der elektronische Rechtsverkehr dann eine breite Nutzung findet, wenn passende Anwendungsfelder für den Einsatz gegeben sind." Bei Steuerberatern, Rechtsanwälten und Wirtschaftsprüfern seien diese bereits heute vorhanden. Die DATEV arbeite an weiteren Szenarien, etwa bei elektronischen Rechnungen.