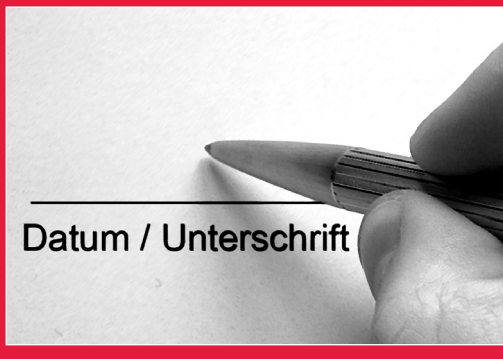
Was bringt die **elektronische Signatur** der Kartensicherheit?



Von Rüdiger Mock-Hecker, Uwe Saliger und Michael Welschenbach

Die Anonymität im Internet verursacht Sicherheitsprobleme. Sie verunsichern den Kunden und gefährden die Kunde-Bank-Beziehung. Als Lösung schlagen die Autoren Bankkarten mit digitalem Zertifikat vor, aus denen elektronische Signaturen erzeugt werden können. Der Kunde kann sich damit im Netz eindeutig identifizieren und endlich auch rechtsverbindliche Unterschriften leisten. Manko daran: Der Benutzer benötigt für alle Anwendungen ein Kartenlesegerät mit der Möglichkeit zur Pin-Eingabe, das er an seinen PC anschließen kann. Aber vielleicht muss er nicht alles alleine kaufen… Red.

Das Internet ist im beruflichen und privaten Alltag als Medium für die Informationssuche sowie zum schnellen Austausch von Mitteilungen und unterschiedlichen elektronischen Dokumenten mittlerweile unverzichtbar geworden.

Die elektronische Signatur macht dabei nicht nur die E-Mail-Kommunikation sicherer und ermöglicht den Behördengang per Mausklick: In die Vielzahl der Signaturanwendungen reiht sich künftig auch das Online-Banking als der wohl wichtigste und meist genutzte Anwendungsfall ein. Alles, was sich ins Netz stellen oder via E-Mail versenden lässt, spart Geld, Zeit und Wege – Kommunikationspartner kommen miteinander in Kontakt, ohne sich persönlich kennen lernen zu müssen.

Phishing, Pharming, Datenklau

Doch gerade an diesem Punkt hat das weltweite Datennetz auch seine größte Schwachstelle. Wie kann man seinem Gegenüber trauen, wenn man ihm nie begegnet ist und auch nicht einmal weiß, ob er tatsächlich der ist, für den er sich ausgibt?

Stichworte Phishing, Pharming, Datenklau: Angesichts solcher Gefahrenpotenziale beschleicht jeden Internetnutzer ein mulmiges Gefühl, wenn er auf einer Webseite seine persönlichen Daten eingibt oder eine Bezahlung tätigt und anschließend auf die Lieferung der bestellten Ware hofft. Es stellt sich die Frage: „Welche Absichten verfolgt der andere, versteckt hinter seiner Anonymität?"

Zu den Autoren

Dr. Rüdiger Mock-Hecker ist Leiter Geschäftssparte Kartensysteme, Deutscher Sparkassenverlag, Stuttgart. **Uwe Saliger** ist Berater Software-Entwicklung und **Michael Welschenbach** ist Bereichsleiter IT bei der SRC Security Research & Consulting GmbH, Bonn.

Dabei ist die Lösung dieses Problems einfach: Digitale Zertifikate, also Identitätsbescheinigungen und damit digitale Ausweise, die von autorisierter Stelle (Certification Authority, CA) ausgegeben werden, beenden den Status der virtuellen Namenlosigkeit.

Ein digitales Zertifikat enthält unter anderem den Namen seines Besitzers, den Namen der ausstellenden Behörde und einen Gültigkeitszeitraum. Mit diesem Zertifikat können elektronische Signaturen erzeugt werden. Diese identifizieren sowohl den Absender als auch das unterzeichnete Dokument und stellen somit Authentizität und Integrität sicher. Der Inhalt eines elektronisch signierten Dokumentes kann nicht unbemerkt verändert werden.

Rechtsverbindliche Unterzeichnung möglich

Dieses Verfahren ermöglicht neue, zukunftsweisende Funktionen.

- Elektronische Dokumente können rechtsverbindlich unterzeichnet und anschließend archiviert werden.

- In der privaten und geschäftlichen Kommunikation können E-Mails nicht nur verschlüsselt, sondern obendrein signiert übermittelt und elektronische Dienstleistungen nun auch über das Internet genutzt werden.

Als Beispiel sind virtuelle Behördengänge zu nennen, die über das Internet getätigt werden können.

Mit Zertifikaten kann also die Anonymität des Internets für bestimmte Anwendungszwecke aufgehoben werden. Dafür müssen die Internetnutzer lediglich mit Zertifikaten ausgestattet werden. Seit Ende 2005 bieten deshalb schon viele Sparkassen ihren Kunden zusätzlich zu den Bank- und Bezahlfunktionen der Sparkassen-Card die elektronische Signaturfunktion an.

Diese Verbindung der elektronischen Signatur mit einer Bankkarte ist neu. Damit die Sparkassen-Card, die in nahezu jeder zweiten bundesdeutschen Brieftasche steckt und fast täglich zum Einsatz kommt, nicht ausgetauscht werden muss, haben der Deutsche Sparkassenverlag (DSV) und die SRC Security Research & Consulting GmbH eine gemeinsame Lösung konzipiert. Mit ihr lassen sich zirka vier Millionen bereits ausgegebene Karten nachträglich zu jedem beliebigen Zeitpunkt mit einem Zertifikat ausstatten.

Zertifikat als Download

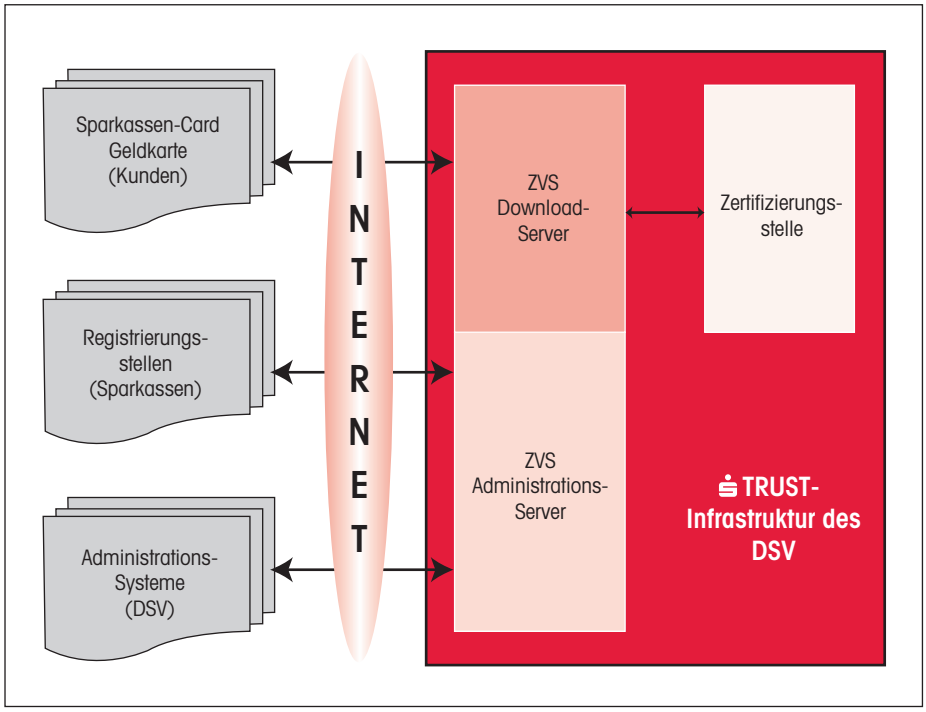
Sparkassenkunden, die bereits im Besitz einer für die Signatur vorbereiteten Sparkassen-Card (oder einer kontounabhängigen Geldkarte) sind, halten sozusagen eine „Signaturkarte auf Abruf" in ihren Händen.

Doch wie lassen sich die Zertifikate auf die bereits ausgegebenen Zahlungsverkehrskarten laden?

Zentraler Bestandteil der webbasierten, sicheren Downloadlösung stellt das so genannte Zertifikatsverwaltungssystem (ZVS) dar, das eigens vom DSV in Zusammenarbeit mit SRC entwickelt wurde.

Das ZVS ermöglicht Instituten in ihrer Funktion als Registrierungsstellen, Zertifikate auszugeben, zu verwalten und gegebenenfalls auch wieder zu sperren (siehe Abbildung 1). Dabei berücksichtigt das ZVS nicht nur die komplizierten technischen Anforderungen, sondern auch eine Fülle von organisatorischen Regelungen: Die Abrechnung gegenüber Registrierungsstellen (Sparkassen-Institute) und Kunden, den automatischen E-Mail-Versand zum Beispiel beim bevorstehenden Ablauf eines Zertifikats sowie die Verwaltung von Gültigkeiten und Kartensperrlisten.

Abbildung 1: Anbindung der Zertifikatsverwaltung an die Außenwelt



Insgesamt wurde so ein effizienter und kostengünstiger Prozess gestaltet, der mit allen Vorgaben des Signaturgesetzes (SigG) vereinbar ist. Dabei sind die Abläufe für Kunden und Registrierungsstellen simpel und überschaubar.

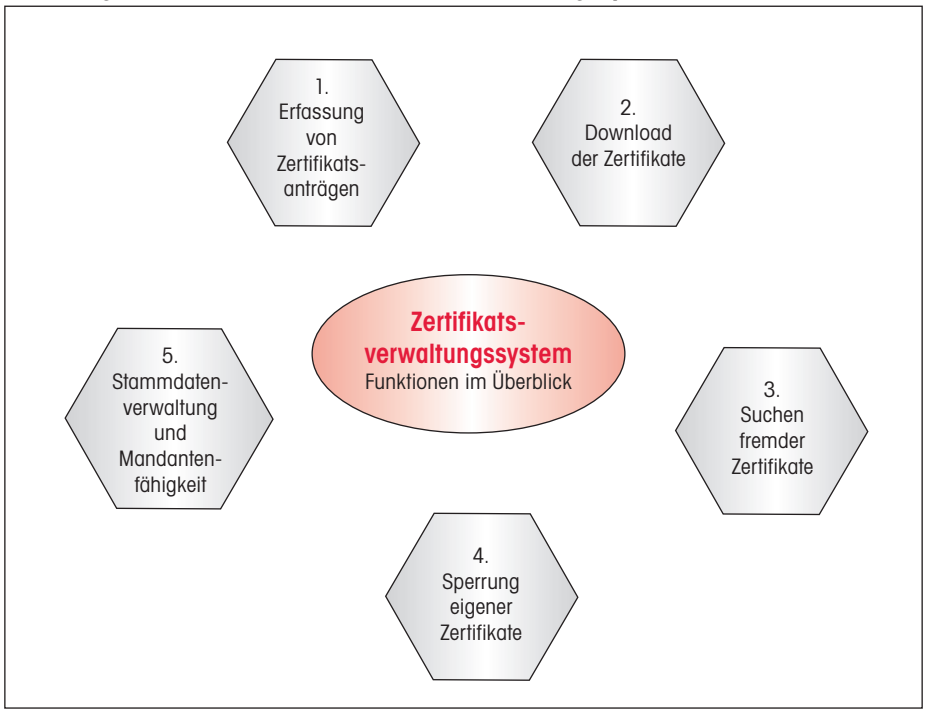
Durchschaubare Abläufe

1. Am Anfang dieses Ablaufs steht die Registrierung des Kunden. Ein Registrierungsmitarbeiter einer Sparkasse nimmt den Antrag eines Karteninhabers entgegen und erfasst dabei unter anderem Name, Geburtsdatum, Adresse, E-Mail-Adresse und Bankverbindung des Kunden, Wunsch nach Veröffentlichung des Zertifikats sowie den Zertifikatstyp (Privatkunde, Firmenkunde und andere).

2. Den Antrag unterschreibt der Registrierungsmitarbeiter mit seiner Signaturkarte. Sein persönliches Zertifikat erhält der Kunde später über eine Web-Schnittstelle, deren Internet-Adresse er in seinen Browser eingibt. Das Zertifikat wird gesichert via Internet auf seine Karte geladen, die zu diesem Zweck wie für alle Signaturanwendungen über einen Kartenleser mit dem PC verbunden sein muss.

3. Der Download-Prozess des Zertifikates richtet sich in seiner einfachen Handhabung an eine breite Zielgruppe von Endanwendern. Die zeitliche Trennung des Kartenproduktionsprozesses von der Erzeugung und Ausgabe des Zertifikates sorgt neben einer Vereinfachung des Produktionsverfahrens für eine hohe Benutzer-Akzeptanz. Der Kunde wird nicht pauschal mit den Kosten für die digitale Signatur belastet, sondern kann selbstständig entscheiden, ob er dieses Angebot nutzen möchte.

Abbildung 3: Die Funktionen des Zertifikatsverwaltungssystems



Insgesamt sind also gute Voraussetzungen für eine innovative Technologie vorhanden. Doch letztlich werden die praktischen Verwendungsmöglichkeiten den Ausschlag für den Erfolg der qualifizierten elektronischen Signatur als Alternative zur eigenhändigen Unterschrift geben.

Status quo und Zukunft

Diese Möglichkeiten gehen inzwischen weit über die genannten klassischen IT-Themen wie sichere E-Mail-Kommunikation oder Authentifizierung an Netzwerken oder Web-Portalen hinaus. Der Markt ist vor allem im Bereich E-Government in Bewegung geraten, die Zahl der hiesigen Anwendungen steigt unaufhaltsam.

Dies liegt vor allem daran, dass der Gesetzgeber den Druck erhöht. Seit April gilt das Justizkommunikationsgesetz, das den elektronischen Rechtsverkehr zwischen Richtern, Rechtsanwälten, Notaren und Bürgern regelt.

Diese haben nun die Möglichkeit, elektronische Kommunikationsformen gleichberechtigt neben der – herkömmlich papiergebundenen – Schriftform oder der mündlichen Form rechtswirksam zu verwenden. Bis zum Ende des Jahres soll der elektronische Rechtsverkehr weitgehend mit digitalen Zertifikaten abgewickelt werden.

Das Umsatzsteuergesetz verlangt bei der Übermittlung elektronischer Rechnungen ebenfalls die qualifizierte Signatur. Ganz neu: Ab dem 1. Dezember 2006 müssen Lohnsteuer-Jahresbescheinigungen zwingend elektronisch signiert beim Finanzamt eingereicht werden.

Großes Potenzial bei E-Rechnungen

Ähnliches ist bei den Ausschreibungen und Auftragsvergaben der öffentlichen Hand zu erwarten. Derzeit befinden sich zahlreiche elektronische Vergabeplattformen im Aufbau. Die Baubranche, zahlreiche Handwerker und Dienstleister sollten frühzeitig über den Nutzen der digitalen Signatur nachdenken, denn ab 2010 sollen nach EU-Vorgaben alle öffentlichen Aufträge ausschließlich elektronisch ausgeschrieben und vergeben werden, was die Verwendung elektronischer Signaturen im Angebotsprozess erforderlich macht.

Ebenfalls auf EU-Richtlinien beruht die elektronische Rechnungsstellung (E-Billing). Da alleine in Deutschland jährlich mehr als zehn Milliarden Rechnungen versendet werden, verbirgt sich dahinter ein enormes Potenzial.

Mit der kontounabhängigen Geldkarte mit Signaturfunktion bietet die S-Finanzgruppe ihren Firmenkunden die Möglichkeit, elektronische Rechnungen gemäß den Vorgaben des Umsatzsteuergesetzes zu stellen.

Prinzipiell können Unternehmen hierbei von den gleichen Vorteilen profitieren wie bei fast allen anderen Anwendungen mit der digitalen Signatur auch: Wegfall der Papier- und Portokosten, erheblich kürzere Durchlaufzeiten sowie einfache und kostengünstige Archivierungsmöglichkeiten.

Sensibilitäten beim Online-Banking

Und welche Vorteile nutzen Privatpersonen mit digitalen Zertifikaten auf der Sparkassen-Card? Dank der rechtlichen Gleichstellung der qualifizierten elektronischen Signatur mit der eigenhändigen Unterschrift können viele Behördengänge per Mausklick erledigt werden. Vorbei sind die Zeiten, in denen man für die Pkw-Anmeldung oder die Wohnsitzummeldung einen Urlaubstag einplanen musste.

Der wichtigste Anwendungsfall aber ist in der wohl sensibelsten und einer der meist genutzten Internetanwendungen überhaupt zu sehen: Künftig soll die digitale Signatur beim Online-Banking eingesetzt werden können. Auf diesem Weg kann das Sicherheitsniveau von Finanztransaktionen künftig deutlich angehoben werden.