Sicherheit im Internet

Immer dringender wird der Ruf nach mehr Sicherheit, Vertraulichkeit und Verbindlichkeit im Internet. Authentisierungsverfahren, insbesondere digitale Signaturen, sollen Geschäftsbeziehungen im Netz auf sichere Füße stellen und Online-Geschäften den Durchbruch verschaffen.

Von Uwe Knierim und Dr. Klaus Manhart

Eigentlich ist Bargeld die zuverlässigste, einfachste und diskreteste Art, um Dinge käuflich zu erwerben. Der Ladenbesitzer ist sich sicher, daß er sein Geld hat, gleichzeitig kann der Kunde davon ausgehen, daß man weder an seiner Identität interessiert ist, noch Fragen über die Herkunft des Geldes stellt. Zudem weiß der Kunde, an wen er sich wenden kann, falls es mit der Ware irgendwelche Probleme gibt.

Dieses einfache ökonomische Prinzip gerät in der Welt der elektronischen Netze ins Wanken. Zwar hat vordergründig das Einkaufen in virtuellen Verkaufsräumen für Kunden und Händler viele Vorteile. Man kann jederzeit Olivenöl in der Toscana bestellen, Software herunterladen und nach einem Gebrauchtwagen weit über das eigene Wohnumfeld hinaus suchen. Und dem Verkäufer bieten Verkaufsräume ohne Personal, Miete, Raumpflege, Strom und Heizung hohe Renditen.

Die Krux am Electronic Commerce ist die Sicherheit beim Bezahlen. So will der Kunde sicher gehen, daß seine Daten nicht für weitere Geldtransfers verwendet werden, Fremde die übermittelten Daten nicht abgreifen können und die bestellte Leistung auch tatsächlich erbracht wird. Umgekehrt will der Verkäufer darauf vertrauen können, daß der Besteller von Waren oder Dienstleistungen mit den gemachten Angaben identisch ist, damit er später auch sein Geld erhält. Und so sind sich alle Beteiligten einig: Wenn das Internet als Medium für geschäftliche – aber auch andere verbindliche und vertrauliche – Transaktionen dauerhaft erfolgreich sein soll, dann nur mit verläßlichen Sicherheitslösungen.

Eine ganze Palette technischer Verfahren wurde in der Vergangenheit vorgeschlagen, um Vertrauen, Authentizität und Integrität im Internet zu gewährleisten: elektronische Signaturen, Smart Cards, Scanner für Fingerabrücke, Netzhautscans, Dongles und anderes mehr (siehe Überblick auf Seite 22).

Bild: Deutsches Museum, München

.Chiffriermaschine ENIGMA – mit ihr wurden während des Zweiten Weltkriegs auf deutscher Seite Funksprüche ver- und entschlüsselt. Die Chiffrierung beruhte auf der systematischen Veränderung von Buchstaben. Zu sehen ist die ENIGMA im Deutschen Museum Bonn vom 8. September bis 7. November

INFO

Einladung

zum Funkschau-Seminar E-Commerce – Technik-Kompetenz für Entscheider. Informationen auf Seite 54 oder im Internet unter www.funkschau.de

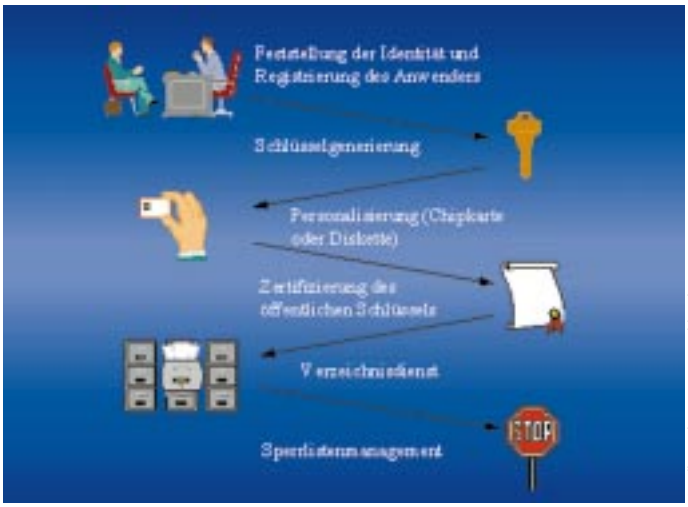
Biometrie – sicher, aber problematisch

Die kompliziertesten Methoden wären für potentielle Anwender auch die sichersten. Denn alle einfachen Methoden stellen immer nur die Tatsache fest, daß am Ende ein bestimmtes Authentifizierungstool vorhanden ist, nicht aber unbedingt die zu authentisierende Person. Mit einem Pincode, einer Smart Card, einem bestimmten Rechner oder einem Hardware-Dongle erhält man keinen Aufschluß darüber, ob diese Identifizierungstools auch tatsächlich vom Eigentümer eingesetzt werden. Mit komplexeren biometrischen Verfahren läßt sich hingegen über die Netzhaut oder den Fingerabdruck eine eindeutige Identität der Person feststellen. So hat etwa Siemens eine Fingerprint-Lösung entwickelt, die über eine Kontaktfolie die Druckstellen aufnimmt. Dies läßt sich samt Software sogar auf einer Smart Card unterbringen. Netzhautscans sind heute technisch ausgereift und relativ leicht umzusetzen, doch ist der Aufwand allein in der Hardware wesentlich höher als bei der Fingerprint-Lösung. Neben dem Schutz von Sicherheitstrakten ist der Einsatz aktuell bei Bankautomaten denkbar.

Die Methoden mit den höchsten Sicherheitsstandards sind aber auch gleichzeitig mit den größten Problemen behaftet, wenn es um den Schutz der Privatsphäre geht. Da die Mehrheit der Kunden berechtigte Vorbehalte dagegen hat, auf Schritt und Tritt über Fingerabdrücke und Netzhautscans verfolgt zu werden, lassen sich breite Marktlösungen derzeit damit wohl kaum realisieren.

Digitale Signaturen vor dem Durchbruch

Eine von vielen Seiten angestrebte Lösung ist das Public-Key-Verfahren (PKI). Public-Key-Systeme basieren auf kryptografischen Verfahren. Dabei hält der Kunde einen öffentlichen und einen privaten Schlüssel bereit. Bei der Übermittlung von Daten, zum Beispiel von Kreditkarteninformationen, werden diese mit dem öffentlichen Key des Empfängers verschlüsselt und versandt. Nur der Adressat kann dann die Nachricht mit seinem privatem Schlüssel wieder in ein lesbares Format übertragen. Mit dem Public-Key-Verfahren lassen sich auch digitale Signaturen erzeugen: sie sind einmalig, an einer Person über deren Schlüsselpaar gebunden und ermöglichen zudem das Überprüfen der Unversehrtheit einer Nachricht. Damit der Public Key auch als digitale Signatur eingesetzt werden kann, ist eine andere Vorgehensweise nötig. Aus der zu übermittelnden Nachricht wird mit einem Hash-Verfahren (Streuspeicherung, wobei eine Hash-Funktion einem Schlüssel K eines Datums eine Adresse a zuordnet, an der dieses Datum zu speichern ist) eine Prüfsumme erzeugt, die mit dem eigenen privaten Key verschlüsselt wird. Das Ergebnis ist die digitale Signatur, die der eigentlichen Nachricht angehängt wird. Auf der Empfängerseite wird dann die Signatur mittels des Public Key des Empfängers entschlüsselt und mit der selbst erzeugten Prüfsumme verglichen. Stimmen die Prüfsummen überein, ist die Authentizität und die Integrität der Nachricht belegt.



Quelle: Teletrust Deutschland e.V.

Der grobe Ablauf einer Zertifizierung

Aber ein Knackpunkt bleibt noch: Wie wird gewährleistet, daß sich hinter einem digitalen Zertifikat – dem elektronischen Ausweis bestehend aus Private Key und Public Key – auch eine bestimmte, sicher identifizierbare Person verbirgt? Dies ist nun kein technisches Problem, sondern eher ein logistisches. Es müssen Stellen eingerichtet werden, an denen sich der Antragsteller bei persönlichem Erscheinen eindeutig ausweist und seine Keys dort persönlich erhält.

Dieser kritische Punkt ist auch gesetzlich geregelt und im Artikel 3 (bekannt als Signaturgesetz) des Informations- und Kommunikationsdienste-Gesetz (IuKDG), das am 1.8.1997 in Kraft getreten ist, in den Rahmenbedingungen sehr genau festgelegt. Als zuständige staatliche Instanz wurde die Regulierungsbehörde für Telekommunikation und Post festgeschrieben.

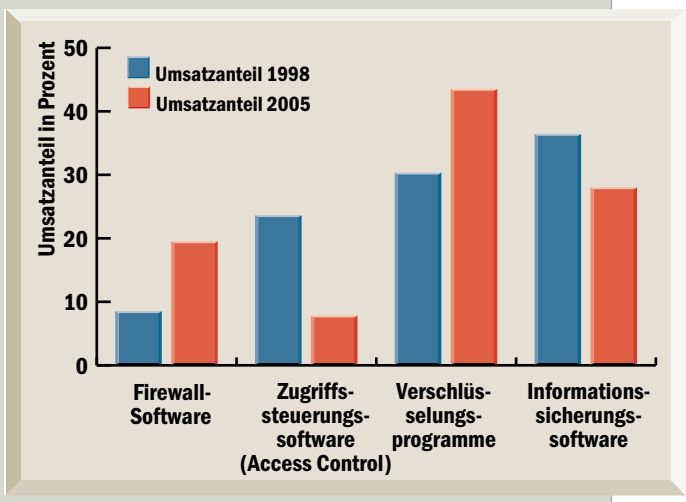
Am 25. Januar diesen Jahres hat die Regulierungsbehörde in Mainz ihr Wurzelverzeichnis in Betrieb genommen. An dieser Stelle können Zertifikate aller zugelassenen Zertifizierungsstellen auf ihre Gültigkeit überprüft werden. Allerdings gibt es zur Zeit nur eine

TREND

Der europäische Markt für Netzsicherheits-Software

Nach einer Studie der Unternehmensberatung Frost & Sullivan profitieren in Europa insbesondere verwandte Märkte vom explosionsartigen Wachstum des E-Commerce. So wird der europäische Markt für Netzsicherheits-Software, der 1998 ein Volumen von 1,13 Milliarden US-Dollar aufwies, bis zum Jahr 2005 auf mehr als 24 Milliarden US-Dollar ansteigen. Als wichtigste Wachstumssegmente der Zukunft nennt die Studie Virtual Private Networks und Public Key Infrastructure Software. Aufgrund der positiven Prognosen für E-Commerce investieren Endbenutzer früh in Verschlüsselungstechniken. Im Jahr 1998 beliefen sich die Umsätze hier auf 345,8 Millionen US-Dollar, bis 2005 wird mit einem Anstieg auf 10,8 Milliarden US-Dollar gerechnet – das entspricht einer jährlichen Wachstumsrate von 63,6 Prozent.

Grafik: Funkschau



Der europäische Markt für Netzsicherheits-Software; Umsatzverteilung nach Produktart

einzige Genehmigung für eine Zertifizierungsstelle – und zwar für die Deutsche Telekom.

Zahlreiche weitere Anträge liegen wohl vor, aber über die Antragsteller oder auch nur über deren Anzahl macht die Regulierungsbehörde keine Angaben. Bekannt ist jedoch, daß sich mit Commerzbank, Dresdner Bank, HypoVereinsbank und Deutscher Bank vier Großbanken zusammengeschlossen haben, um mit TC Trustcenter (www.trustcenter.de) ein eigenes Zertifizierungsverfahren zu betreiben. TC Trustcenter befindet sich allerdings noch in der Antragsphase, die im übrigen von den Betreibern als projektbegleitend dargestellt wurde. Das bedeutet, daß während der gesamten Aufbauphase die gesetzlichen Vorgaben auf Konformität überprüft werden. Für die Banken übernimmt TC Trustcenter zusätzlich die Aufgaben der Zertifizierungsinstanz in einer weltweiten Zertifizierungsarchitektur, die derzeit von Identrus aufgebaut wird. Ziel von Identrus ist die schnelle Verbreitung eines sicheren elektronischen Geschäftsverkehrs auf der Basis einheitlicher Regeln und Verträge.

Der Aufwand für ein zugelassenes Trustcenter ist relativ hoch. Neben den Anforderungen an die Datensicherheit und den aufwendigen Programmierarbeiten sind zudem erhebliche Investitionen in die Gebäudesicherheit erforderlich. Trustcenter sind damit Dreh- und Angelpunkt einer funktionierenden Sicherheitsinfrastruktur im Internet.

Die Deutsche Telekom als einziges staatlich zugelassenes Trustcenter bietet Signaturdienste seit Anfang Januar diesen Jahres an. Dazu nutzt die DTAG ihre 500 T-Punkt-Läden, in denen man gegen ein einmaliges Entgelt von 50 Mark eine Chipkarte mit den Keys beantragen kann. Für die Dienste des Trustcenters

ÜBERBLICK

Authentisierung – die wichtigsten Verfahren

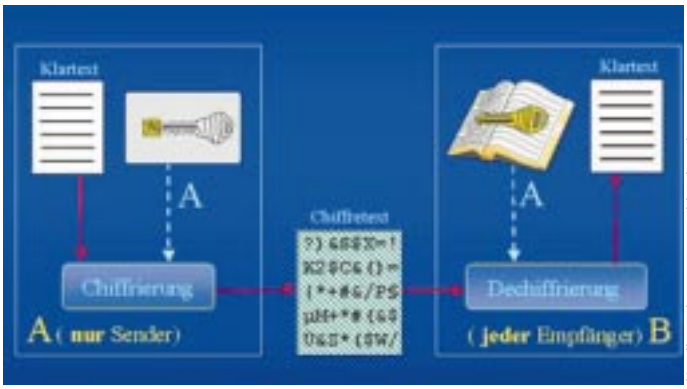
PIN und TAN: PINs (persönliche Identifikationsnummern) und TANs (Transaktionsnummern) sind vor allem beim Homebanking verbreitete Authentifizierungsverfahren. Die PIN legitimiert dabei gegenüber dem Rechner der Bank. Sie ist nur dem User bekannt. TANs dienen zur sicherungspflichtigen Übersendung von Aufträgen (zum Beispiel Überweisungen). Jede TAN kann nur einmal verwendet werden.

HBCI: Das Homebanking Computer Interface (HBCI), eine Entwicklung der deutschen Banken und Sparkassen, ist vergleichbar mit einer elektronischen Unterschrift. Damit soll der Service des Kreditgewerbes ausgeweitet, die Handhabung vereinfacht sowie ein zuverlässiger Schutz gegen Hackerangriffe geschaffen werden. HBCI stellt eine einheitliche Schnittstelle für das gesamte Bankgewerbe zur Verfügung. Auf TANs wird verzichtet, es beruht vielmehr neben dem öffentlichen Schlüssel auf einem geheimen RSA-Kunden-Schlüssel. Außerdem findet die Übertragung über einen eigenen Kanal statt. Sämtliche Spitzengremien führender Bankenorganisationen haben sich auf diesen Standard geeinigt und der Zentrale Kreditausschuß hat ihn verabschiedet.

Smart Cards: Die Chipkarte oder Smart Card ist wegen ihrer herausragenden Eigenschaften bezüglich Sicherheit, Multifunktionalität und Mobilität nicht mehr aus modernen Sicherheitssystemen wegzudenken. Mit vergleichsweise geringen Mitteln können erhebliche Verbesserungen des Sicherheitsniveaus und der Benutzerfreundlichkeit erzielt werden – im Vergleich zu konventionellen Systemen.
Die Chipkarte repräsentiert den berechtigten Benutzer gegenüber einem IT-System. Der Benutzer identifiziert sich gegenüber der Chipkarte durch seine persönliche PIN. Die Chipkarte hat eine eindeutige und kryptographisch gesicherte Identität, die vom System im Rahmen einer auf dem 'Challenge and Response' Prinzip beruhenden Authentisierung überprüft werden kann. Somit ist es nicht möglich, eine gefälschte Identität anzunehmen. Der Zugang zum System ist von Besitz (Chipkarte) und Wissen (PIN) abhängig, welches eine erhebliche Verbesserung zum Paßwort (nur Wissen) darstellt.
Beim Einsatz als Multifunktionskarte ist die Chipkarte beispielsweise als sicherer Speicher (durch PIN geschützt), als elektronische Geldbörse, zur Erzeugung digitaler Signaturen, zur kryptographischen Sicherung vertraulicher oder authentischer Kommunikation sowie zur Unterstützung eines sicheren Login (zum Beispiel ‚Single Sign On') geeignet.

Biometrie: Biometrische Verfahren basieren darauf, daß jeder Mensch über einzigartige, nicht kopierbare Körper- und Verhaltensmerkmale verfügt. Diese können im Gegensatz zur Chipkarte nicht gestohlen oder verloren werden. Schon heute können Fingerabdrücke durch Sensoren gemessen, Stimmfrequenzen bei Schlüsselwörtern durch ein Mikrofon aufgenommen und ausgewertet oder charakteristische Gesichtszüge durch Videobilder zur Identifizierung herangezogen werden. Eine weitere Möglichkeit ist das Erkennen des personentypischen Rhythmus' beim Schreiben auf einer Tastatur. All diese Merkmale können in Zukunft auf einer Chipkarte gespeichert werden. Über den Chipkartenleser entsteht eine Verbindung zum entsprechenden Sensor. Die Chipkarte kann dann – beispielsweise am Netzhautmuster oder dem Fingerabdruck – erkennen, ob der Benutzer auch derjenige ist, für den er sich ausgibt. Um für ein biometrisches Verfahren in Frage zu kommen, muß ein Personenmerkmal allerdings einige Voraussetzungen erfüllen. Es muß einzigartig sein und sollte sich im Laufe der Zeit wenig verändern

Digitale Signatur: Die digitale Signatur ist eine Art elektronischer Unterschrift, mit der elektronische Daten unterschrieben werden können. Die digitale Signatur garantiert, daß die Daten nicht verändert wurden und wirklich vom Erzeuger der Signatur stammen. Dabei ist eine elektronische Unterschrift mehr als eine handschriftliche Unterschrift: Sie bestätigt nämlich sowohl den Inhalt einer Nachricht als auch die Identität des Benutzers. Solange ein bestimmter Sicherheitslevel (Hash-Funktion) verwendet wird, gibt es keine Möglichkeit, eine Unterschrift von einem Dokument auf ein anderes zu übertragen oder das Dokument zu verändern. Die kleinste Änderung im Dokument bewirkt, daß der Überprüfungsvorgang scheitert.
In der Praxis verläuft das Versenden einer signierten Datei in folgenden Schritten:
1. Beim Verschicken einer E-Mail signiert der Absender diese mit seinem privaten Schlüssel, dem elektronischen Pendant zur „echten" Unterschrift.
2. Der Empfänger prüft nun die Echtheit des Absenders, indem er die Signatur mit dem öffentlichen Schlüssel des Absenders decodiert. Läßt sich die Unterschrift so verifizieren, ist die Nachricht eindeutig vom Absender und außerdem nach dem Signieren nicht mehr nachträglich geändert worden.
In Zukunft werden zugelassene Zertifizierungs-Stellen Kennungen an Personen oder Firmen vergeben, die sich dort zuvor persönlich ausgewiesen haben. Dazu bestimmt das Multimedia-Gesetz von August 1997 im Artikel 7, daß die Anbieter für die Vergabe der Signaturen eine Lizenz bei öffentlichen Stellen beantragen müssen.



(Quelle: Teletrust Deutschland e.V.)

Das Grundprinzip bei der digitalen Signatur: Asymmetrische Verschlüsselung zur Authentifizierung

wird ein Jahresbeitrag von 100 Mark erhoben.

Es gibt übrigens keine Pflicht, eine Zertifizierung durch die staatlichen Organe absegnen zu lassen. Allerdings werden ohne staatlichen Segen die Zertifikate geringere Sicherheit und somit auch eine geringere Akzeptanz bieten. Denn die Regulierungsbehörde setzt hohe Ansprüche an die Zuverlässigkeit und Vertrauenswürdigkeit eines Antragstellers, bevor sie eine Genehmigung zur Zertifizierung nach dem Signaturgesetz ausspricht.

Jedoch für firmeninterne Transaktionen und kleinere geschlossene Benutzergruppen ist die unregulierte Verwendung von Zertifikaten durchaus interessant, denn der hohe Verwaltungs- und Kostenaufwand einer gesetzesfesten Lösung würde sich hier nicht lohnen. Ein gutes Beispiel dafür sind zahlreiche Ärzte-Teams, die über diverse Gesundheitsnetze ihre Erfahrungen und damit sehr sensible Daten austauschen.

Wichtig ist auch, daß die Art des Schlüssels im Grunde keine Rolle spielt. Ob nun ein RSA-Algorithmus verwendet wird oder eine PGP-Verschlüsselung, sollte in einem Trustcenter keine Rolle spielen. Dieses sollte mit den verschiedenen Methoden ebenso zurechtkommen, wie mit unterschiedlichen Schlüssellängen. Bei RSA ist eine Schlüssellänge von 512 bit weitverbreitet. Aber es gibt auch Schlüssel mit 1.024 bit oder mehr. Dabei ist die Schlüssellänge entgegen den vielen Fachdiskussionen im normalen Geschäftsverkehr nicht von allzu großer Bedeutung. Selbst ein 40-bit-Schlüssel kann nur mit erheblichem Aufwand geknackt werden. Gefahren drohen eben doch eher bei Verlust der Chipkarte und durch ausspionieren von PIN-Codes. Die sicherste Methode bestünde wohl offensichtlich in der Kombination aus den Key-Systemen mit Chipkarten, auf denen eine Fingerabdruck-Technologie integriert wäre.

Schwachstellen in der Praxis

Neben der eindeutigen Identifizierung des Zertifikatträgers durch die Vergabestelle (hier besteht zum Beispiel durch die Vorlage gefälschter oder entwendeter Ausweise eine Sicherheitslücke) gibt es noch eine weitere Schwachstelle. Und die besteht in der sicheren Aufbe-

EXPERTEN-KOMMENTAR

Bewertung von Authentisierungsverfahren

Von Dipl. Mathematiker Klaus Keus, Referatsleiter „Akkreditierung und Lizenzierung" im BSI, Bundesamt für Sicherheit in der Informationstechnik.

„Zur technischen Realisierung von Authentisierungsverfahren bieten sich unter anderem Hardware-Token, Software-Token und Smart Cards an. Die Vor- und Nachteile dieser technischen Möglichkeiten sind hinsichtlich der Praktikabilität, Sicherheit, Akzeptanz und der Zukunftsperspektiven von der Anwendung abhängig. Das Hardware-Token ist im Verhältnis ein teueres, aber von der Rechenleistung her ein hochwertiges Verfahren. Die Anwendung findet in der Regel im Hochsicherheitsbereich statt. Es ist überall da praktikabel, wo es auf einen hohen Durchsatz an Daten ankommt. Insofern die biometrischen Authentikationsverfahren eine hohe Zuverlässigkeit aufweisen, werden sie auch in diesen Anwendungsbereichen eingesetzt.

Klaus Keus, Referatsleiter Akkreditierung und Lizenzierung im BSI

In Bereichen mit niedrigem Sicherheitsbedarf („einfache" digitale Signatur, zum Beispiel E-Mail in der normalen Bürokommunikation) wird sicherlich das Software-Token Anwendung finden. Es ist im hier genannten Anwendungsbereich praktikabel, preiswert und bietet einen akzeptablen Durchsatz. Die Anwenderakzeptanz ist hoch und es ist zu erwarten, daß es auch in der Zukunft so bleibt. Das Sicherheitsniveau ist allerdings gering. Die Einbindung von biometrischen Authentisierungsverfahren ist denkbar. Die Smart Card als Authentisierungs-Token wird im Konsumer-Bereich zukünftig eine breite Anwendung finden. Die Sicherheitsleistungen sind sehr hoch, da eine Kombination aus HW und SW verwendet wird. Die Authentisierung findet über „Besitz und Wissen" statt. Die Verwendung von Smart Cards ist preiswert, findet eine hohe Akzeptanz und wird auch künftig im Massengeschäft eingesetzt werden. Insbesondere Multifunktionskarten werden, neben der Sicherheitsleistung, durch die Vielfachanwendung einen wesentlichen Mehrwert für den Benutzer bereitstellen. Eine zukünftige Kombination mit biometrischen Authentisierungsverfahren könnte die Sicherheitsleistung noch weiter steigern – Lösungen solcherart sind heute allerdings noch nicht in Marktreife verfügbar.

Biometrische Authentisierungsverfahren selber werden heute meistens in Hochsicherheitsanwendungen eingesetzt. Eine Verbreitung für den allgemeinen Einsatz im Alltag ist noch nicht so weit fortgeschritten, daß hier eine genügend große Stückzahl für eine Marktdurchdringung erreicht wird. Infolge der unterschiedlichen angewendeten Verfahren, vom Fingerabdruckverfahren über Iriserkennung bis hin zur Handflächen- oder Unterschriftenerkennung, ist sowohl die Benutzerakzeptanz sehr unterschiedlich als auch die Sicherheitsaussagen breitbandig. Für zukünftige Einsatzbereiche in Hochsicherheitsanwendungen wird man sicherlich eher tendentiell eine kombinierte Lösung aus unterschiedlichen Verfahren, zum Beispiel Gesichtserkennung in Kombination mit Gesichtsmotorik oder Spracherkennung, einsetzen. Problematisch ist allerdings noch die Frage der vertrauenswürdigen Speicherung und Anwendung solcher persönlicher Daten, das heißt, das Problem der Trennung von Besitz und Wissen. Die heute im Konsumer-Bereich eingesetzte Technik ist in den unteren und mittleren Preissegmenten noch nicht so fortgeschritten, daß eine solche Technik dieser Preiskategorien auch die erforderliche Sicherheit bietet."

wahrung der Zertifikate. In der Regel befinden sich die Keys auf dem Rechner des Zertifikatträgers und sind nur durch ein einfaches Paßwort geschützt. Wenn der Rechner unbeobachtet steht, hat ein potentieller Angreifer viel Zeit für seine Attacke. Außerdem ist es unpraktisch, da man seine Keys immer nur von einem Rechner aus verwenden kann. Abhilfe schafft hier die Chipkarte. Auf ihr lassen sich der Haysche Algorithmus und der Public Key sowie auch der Privat Key unterbringen. Damit verbleiben auf dem Rechner keine sensiblen Daten. Obwohl die Karte PIN-geschützt ist, gilt auch hier, daß die Sicherheit nur so groß sein kann, wie die schwächste Stelle in der Sicherheitskette. Eine Smart Card kann entwendet werden, und wenn vorher die PIN ausspioniert wurde, nützt das gesamte Signatursystem nichts mehr. Ein weiterer Nachteil der Chipkarte ist, daß man einen Kartenleser für seinen Rechner benötigt.

Als Konsequenz kann eigentlich nur geschlossen werden, daß die technische Umsetzung von Sicherheitslösungen allein nicht ausreicht. Vielmehr werden die Kunden sorgfältig darauf achten müssen, mit wem sie E-Commerce betreiben. Dabei kommt es sehr auf etablierte Markenbegriffe an. Dubiosen unbekannten Firmen wird man eher weniger sein elektronisches Geld anvertrauen. Hingegen werden sich große Chancen für kleine regionale Anbietern eröffnen, die in der Lage sind, E-Commerce mit direktem Kundenkontakt zu verbinden. Eine Reklamation läßt sich eben einfacher vorbringen, wenn sich der Lieferant in der Region befindet und nicht auf den Bahamas. Umgekehrt werden die E-Shop-Besitzer die bewährten Methoden der etablierten Versandhäuser einsetzen müssen, um sich einen seriösen Kundenstamm zu generieren. Dazu gehören Bonitätsprüfungen, Identitätskontrollen, Testabbuchungen, aber auch Stundungsmöglichkeiten. Was für den Katalogverkauf per Telefon gilt, hat auch im E-Commerce unbeschränkt Gültigkeit. Tatsächlich ist die geringe Verbreitung von Kartenlesern und der Aufwand für Chipkarten mit digitaler Signatur das zentrale Problem, um die elektronische Unterschrift und damit E-Commerce zu einem selbstverständlichen Alltagsphänomen werden zu lassen. Am Ende muß man kein Hellseher sein um vorauszusagen, daß sich die digitale Signatur dann durchsetzen wird, wenn sie zum Standardbestandteil der weitverbreiteten Geldkarten geworden ist und die Computerhersteller ihre Rechner ebenfalls standardmäßig mit Kartenlesern ausrüsten. *(GK)*

KONTAKTE IM INTERNET

Sicherheit und Authentisierung im Internet

Teletrust Wissensforum Gute Artikelsammlung	http://www.teletrust.de/index-jf.htm
Linksammlung zum Thema Sicherheit/Kryptographie	http://www.burks.de/krypto.html
Electronic Commerce Infonet - Sicherheit	http://www.electronic-commerce.org/sicherheit/index.html
Sicherheit in der Informationsgesellschaft Sehr gute Infosammlung	http://www.sicherheit-im-internet.de/
Telekom Gute Übersichtsartikel	http://www.telekom.de/angebot/telesec/vertrau/index.htm
Glossar und Lexikon	http://www.glossar.de/glossar/z_verschluessel.htm
Security-Server Uni Siegen	http://www.uni-siegen.de/security/

INTERVIEW

„Digitale Signatur wird sich in 2-3 Jahren durchsetzen“

Christina Zucker ist zuständig für Marketing und Öffentlichkeitsarbeit bei TC Trustcenter in Hamburg.

Funkschau: *TC Trustcenter soll sich als führende deutsche Zertifizierungsinstanz etablieren. Welchen Weg schlagen Sie hierfür ein?*
Zucker: TC TrustCenter hat sich zum Ziel gesetzt, sowohl signaturgesetzkonforme als auch nicht-regulierte Zertifikate auszustellen. Wir wollen für möglichst viele Anwendungen und Anforderungen von Kundenseite offen bleiben. Wir werden zum Beispiel SET-Zertifikate für sichere Kreditkartentransaktionen über das Internet ausstellen. Natürlich werden wir viel im Bankenbereich und auch speziell für unsere Gesellschafter realisieren, aber wir sind keineswegs ein reines Banken-TrustCenter, sondern offen für alle Unternehmen.

Christina Zucker, TC TrustCenter

Funkschau: *Das Zertifizierungsverfahren von TC TrustCenter befindet sich noch in der Antragsphase. Wann soll die Aufbauphase abgeschlossen sein?*
Zucker: Im Herbst bezieht TC TrustCenter neue Räumlichkeiten mit einem Hochsicherheitstrakt. Vorher kann die Evaluierung auf keinen Fall abgeschlossen werden.

Funkschau: *Konkret gefragt: Wann kann ich mir meinen elektronischen Ausweis bei Ihnen bestellen?*
Zucker: Bereits seit mehr als zwei Jahren stellt TC TrustCenter elektronische Ausweise zur Verfügung. Diese können online unter www.trustcenter.de beantragt werden. Wir stellen Server-Zertifikate und Software-Zertifikate aus, aber natürlich auch elektronische Ausweise für Mitarbeiter eines Unternehmens zum Beispiel für die sichere Kommunikation per E-Mail.

Funkschau: *Wie steht es um die weltweite Verwendbarkeit Ihres Zertifizierungsverfahrens?*
Zucker: Technisch gesehen basieren Zertifikate auf Standards, die international anerkannt und verbreitet sind. Wichtig für die weltweite Verwendbarkeit von Zertifikaten ist die Interoperabilität und die Entwicklung von Kriterien, hinsichtlich derer Trustcenter als vertrauenswürdig gelten. Erst wenn die Teilnehmer wissen, welchen Zertifikaten von welchen Trustcentern sie vertrauen können, wird der Einsatz von Zertifikaten auch international funktionieren. Noch gibt es allerdings keine internationale Übereinkunft der Trustcenter untereinander über die gegenseitige Anerkennung ihrer Zertifikate.

Funkschau: *Wann wird sich nach Ihrer Einschätzung der elektronische Ausweis auf breiter Basis durchsetzen?*
Zucker: Wir gehen davon aus, daß sich der elektronische Ausweis in den nächsten zwei bis drei Jahren durchsetzen wird.

INFO

Wer macht was?

Eine ganze Reihe von Firmen und Institutionen haben sich dem zukunftsträchtigen Gebiet Authentisierung/Sicherheit verschrieben. Die wichtigsten Organisationen und Unternehmen und ihre Arbeit stellen wir Ihnen vor.

TeleTrusT : Die TeleTrusT Deutschland e.V. hat sich zur Aufgabe gemacht, die Akzeptanz der digitalen Signatur als Instrument zur Rechtssicherheit einer Transaktion zu erreichen. Hierfür unterstützt TeleTrusT die Forschung zur Sicherheit des elektronischen Datenaustausches und die Anwendung ihrer Ergebnisse sowie die Entwicklung von Standards. Auf dem Gebiet der Authentisierung soll mit Institutionen in anderen Ländern zusammengearbeitet und die Ziele und Standards innerhalb der Europäischen Union harmonisiert werden. Konkret beschäftigt sich die TeleTrusT Deutschland schon seit einigen Jahren mit biometrischen Identifikationsverfahren. Ziel ist der schrittweise Ersatz von PIN und TAN durch biometrische Merkmale.
■ Info: www.teletrust.de

Fraunhofer Gesellschaft: Biometrische Verfahren werden zum großen Teil bei der Fraunhofer Gesellschaft entwickelt. Zusammen mit der DCS AG Berlin sind die am Fraunhofer-Institut produzierten biometrischen Systeme, die Personen eindeutig und zuverlässig über die Stimme, das Gesicht und die Mimik erkennen, unter dem Namen BioID bereits im Einsatz. Über das „klassische“ Anwendungsgebiet biometrischer Systeme der Zugangskontrolle hinaus beschäftigen sich die Forschungsarbeiten am Fraunhofer-Institut für Integrierte Schaltungen IIS-A mit der Entwicklung sogenannter intelligenter Benutzerschnittstellen. Der Computer lernt, Personen innerhalb eines größeren Bildausschnittes bzw. vor wechselndem Hintergrund zu identifizieren, wie dies für menschliche Betrachter möglich ist.
Ein Ableger des Fraunhofer-Instiuts – recognitic, Gesellschaft für digitale Bildverarbeitung – professionalisiert und kommerzialisiert die Basisentwicklungen des Instituts in Form von Software-Produkten, die eine automatische Dokumentenverarbeitung und -sicherung ermöglichen. Die Entwicklungen richten sich dabei stark auf eine Kombination von biometrischen Verfahren (Fingerabdruckanalyse und Analyse der Unterschriftendynamik) mit Methoden der Dokumentenverschlüsselung und digitaler Wasserzeichen.
■ Info: www.iis.fhg.de

Siemens AG: Die Siemens AG setzt beim Thema Authentifizierung auf Biometrie und hier insbesondere auf den Fingertip. Nach Einschätzung des Unternehmens wird dies künftig eines der wichtigsten Verfahren zur digitalen Authentifizierung sein und gegenüber anderen Systemen die größte Akzeptanz finden. Bei diesem Verfahren zur Zugangskontrolle genügt ein kurzer Tip mit dem Finger auf einen Sensor, damit der angeschlossene Mikrochip anhand dieses persönlichen Fingerabdrucks erkennt, ob der Nutzer tatsächlich zugangsberechtigt ist. Gegenüber den bisher eingesetzten „Geheimzahlen“ (PIN) ist der Fingertip wesentlich komfortabler und um ein Vielfaches sicherer. Geplant ist unter anderem der Einbau des Fingertip-Moduls in Mobiltelefone und Smart Cards.
■ Info: www.siemens.de

Bild: Infineon

Der Fingertip-Sensor der Siemens-Tochter Infineon Technologies AG: Der rund 160 Quadratmillimeter große Sensor erlaubt das zuverlässige Einlesen und Auswerten des Fingerabdrucks. Dank seiner Kleinheit und dem niedrigen Energieverbrauch im Sleep-Mode (5 mW) eignet sich der Chip für Geräte wie Handy oder Laptop, die zeitweise über Akku mit Energie versorgt werden

Utimaco Safeware: Die Utimaco Safeware AG entwickelt IT-Sicherheitslösungen für die Anwendungsbereiche Mobile/Desktop-Authentisierung, Zugriffskontrolle, Verschlüsselung, Digitale Signatur und Sicherheitsinfrasturktur (Smart-Card-Leser, etc.). Hauptaugenmerk legt das Unternehmen auf sicherheitskritische Branchen wie Banken und Versicherungen, Behörden und Teile der Industrie.
■ Info: www.utimaco.de/

TC Trustcenter: Das TC Trustcenter versteht sich als Security Provider mit dem Ziel, Sicherheit im Internet für jeden Teilnehmer zugänglich zu machen. Dazu wird eine Zertifizierungsinstanz betrieben. Das Trustcenter übernimmt die Identifizierung der Teilnehmer, das Ausstellen, Bereitstellen, Aktualisieren und Sperren der elektronischen Ausweise – der Zertifikate. Mit den Ausweisen können Unternehmen, Behörden und private Teilnehmer das Internet für vertrauliche, verbindliche und authentische Transaktionen nutzen (siehe Interview mit Christina Zucker).
■ Info: www.trustcenter.de

Deutsche Telekom AG: Die Telekom hat sich unter dem Produktzentrum T-TeleSec der Sicherheitsproblematik angenommen. Sie entwickelt gemeinsam mit Herstellern und Anwendern Sicherheitsdienste, um allgemeine beziehungsweise individuelle Sicherheitskonzepte bereitzustellen. T-Tele SecCrypt gewährleistet die Authentifikation aller Teilnehmer, egal ob vertrauliche Dokumente oder Datenfiles übermittelt werden oder vertrauliche Telefongspräche geführt werden sollen. Zusammen mit der Möglichkeit der Digitalen Signatur soll T-TeleSecCrypt damit in Zukunft alle Voraussetzungen für eine rechtsverbindliche und beweisverwertbare Telekommunikation bringen.
■ Info: www.telesec.de/

Brokat Infosysteme AG: BROKAT hat sich als Anbieter von Lösungen für Internet Banking, Internet Brokerage und Internet Payment entwickelt. Einen Schwerpunkt sieht das Unternehmen im Aufbau von Sicherheitslösungen bei der Kombination von Internet und Mobilfunk.
■ Info: www.brokat.de/

Bundesamt für Sicherheit in der Informationstechnik: Untersuchungen von Sicherheitsrisiken sowie Entwicklung und Zulassung von Sicherheitsvorkehrungen in der Informationstechnik – das sind die Aufgaben des BSI. So ist das Bundesamt für Zertifizierungsprobleme, digitale Signatur, Computerviren oder die IT-Sicherheit zuständig und unterstützend tätig. Auch die Beratung in Fragen der Sicherheit in der Informationstechnik unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen gehört zum Aufgabenspektrum des BSI (siehe Experten-Kommentar von Klaus Keus).
■ Info: www.bsi.bund.de

Regulierungsbehörde für Telekommunikation und Post (Reg TP): Die Regulierungsbehörde überwacht die Rahmenbedingungen des Informations- und Kommunikationsdienste-Gesetzes (IuKDG), das am 1.8.1997 in Kraft getreten ist..
■ Info: www.regtp.de/