eCommerce
mCommerce

Mobile Endgeräte als vertrauenswürdige Terminals

Einfache Handhabung komplexer Sicherheit

Autor: **Robert Nitschke**
Datum: **15.01.2003**

Zusammenfassung:
Durch den Einsatz von elektronischen Signaturen in Kombination mit einem mobilen Endgerät ist es möglich, sichere Geschäfte abzuschließen, bei denen sich die Vertragspartner an unterschiedlichen Orten befinden. Neue Kommunikationssysteme wie UMTS und WLAN bieten dabei schnellere und bessere Übertragungsmöglichkeiten; die notwendigen Infrastrukturen werden derzeit aufgebaut. Mobile Endgeräte können dabei als vertrauenswürdige Terminals mit fortgeschrittenen elektronischen Signaturen die Sicherheit von mobilen Transaktionen garantieren und u.a. die Lücke bis zum flächendeckenden Einsatz von Signaturkarten mit qualifizierten elektronischen Zertifikaten in Deutschland ausfüllen.

NOVOSEC
Aktiengesellschaft

Sulzbacher Straße 29-39
65824 Schwalbach am Taunus, Deutschland
Telefon +49 (0) 6196/88289-0
Telefax +49 (0) 6196/88289-11
contact@novosec.com, www.novosec.com

Sulzbacher Straße 29-39, 65824 Schwalbach am Taunus, Deutschland
Telefon +49 (0) 6196/88289-0, Telefax +49 (0) 6196/88289-11
contact@novosec.com, www.novosec.com

Infrastrukturen werden aufgebaut

Die Möglichkeiten, mittels eines mobilen Endgerätes Geschäfte durchzuführen, werden ständig erweitert; schließlich besitzt die Mehrheit der deutschen Bevölkerung bereits ein Mobilfunktelefon. Wurden in der Vergangenheit Geschäfte meist über mobile Endgeräte lediglich angebahnt und nachträglich direkt vor Ort abgeschlossen, so kann jetzt auch der Vertragsabschluss mittels mobiler Endgeräte erfolgen.
Mobile Netze sind flächendeckend verfügbar und werden stetig verbessert. Zu den bestehenden Kommunikationssystemen (z.B. GSM) kommen neue wie UMTS (Universal Mobile Telecommunications System) und WLAN (Wireless Local Area Network) (siehe Whitepaper „Forza UMTS, forza WLAN“). Durch den technischen Fortschritt verschwimmen die Grenzen zwischen PC, Mobiltelefon und Personal Digital Assistants (PDA); Beispiele hierfür sind der MDA von T-Mobile und der XDA von O2. Am Ende dieser technischen Entwicklung steht ein leistungsfähiges, mobiles, multi-funktionales Endbenutzergerät, das, über mobile Kommunikationssysteme mit dem Internet verbunden, als vertrauenswürdige Plattform für Online-Einkäufe, Geld- und Aktiengeschäfte, zur Erstellung vertraulicher Dokumente etc. dient.

Mobile Verfahren werden zukünftig einen nicht unbeträchtlichen Teil der elektronischen Transaktionen ausmachen. Sicherheit spielt aber auch bei mobilen Transaktionen eine entscheidende Rolle. Vor allem die Authentisierung (siehe E-Government-Handbuch des BSI, http://www.bsi.de) der Kommunikationspartner ist wichtig. So muss z.B. gewährleistet werden, dass eine Bank ihren Kunden auch über sein mobiles Endgerät verlässlich authentifizieren kann, damit der Kunde vorhandene Bankanwendungen nicht nur über das Internet, sondern auch mobil nutzen kann. Zum Zweck der Authentisierung bieten sich unter anderem auch elektronische Signaturen oder das mobile TAN-Verfahren an.

Elektronische Signaturen nehmen an Bedeutung zu

Elektronische Signaturen bieten für Transaktionen über offene Netze überzeugende Vorteile; z. B. gewährleisten sie die Authentizität der Nachrichten. Behörden, Kreditinstitute, Unternehmen aber auch Bürger können mit der elektronischen Signatur ihren elektronischen Geschäftsverkehr nicht nur sicherer gestalten, sondern auch deutlich vereinfachen. Der Einsatz digitaler Zertifikate erlaubt dabei die Überprüfung der Identität des Kommunikationspartners.

Die meisten europäischen Länder haben in den letzten Jahren Gesetze bzgl. der elektronischen Signatur verabschiedet und erfüllen damit Anforderungen der EU-Richtlinie 1999/93/EC. So ist beispielsweise im Mai 2001 in Deutschland das "Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Formschriften" im Bundesgesetzblatt verkündet worden. Damit ist die Erwartung verbunden, dass die Nutzung der elektronischen Signatur in Deutschland verstärkt an Bedeutung gewinnen wird. Elektronische Signaturen sind inzwischen in Deutschland rechtlich weitestgehend mit handschriftlichen Unterschriften gleichgestellt. Mit der Gleichstellung von elektronischer Signatur und eigenhändiger Unterschrift können auch Verträge, für die bisher die traditionelle Schriftform notwendig war, künftig auf elektronischem Weg abgeschlossen werden. Durch Signaturgesetz-konforme Identifikationsmechanismen können Dienstleistungen angeboten werden, die bislang nur durch den Staat selbst übernommen werden.

NOVOSEC Aktiengesellschaft

Sulzbacher Straße 29-39, 65824 Schwalbach am Taunus, Deutschland
Telefon +49 (0) 6196/88289-0, Telefax +49 (0) 6196/88289-11
contact@novosec.com, www.novosec.com

Die weite Verbreitung von Signaturkarten in Deutschland steht noch aus

Zur Nutzung der elektronischen Signatur werden weltweit verstärkt Signaturkarten ausgegeben. Die Ausgabe dieser Signaturkarten erfordert dabei eine qualitativ hochwertige Kundenregistrierung sowie eine Reputation als vertrauenswürdige Instanz am Markt. Als potenzielle Emittenten können folgende Einrichtungen/Branchen agieren:

- Staat (mit seinen Behörden)
- Banken/Kreditkartenunternehmen
- Mobilfunknetzbetreiber
- Sonstige Karten-ausgebende Stellen (z.B. Mitarbeiterausweis, Kundenkarten)

In vielen Ländern der Welt übernimmt der Staat seine Rolle der Ausweis-ausgebenden Instanz. Eine Vorreiterrolle nimmt dabei Malaysia ein. Dort wird die sogenannte Government Multipurpose Card an die Bürger sowie Personen mit einem ständigen Wohnsitz in Malaysia ausgegeben. Diese Karte ist eine Multifunktionskarte, die sowohl als Führerschein dienen kann, mit einer Kreditkartenfunktion ausgestattet ist, medizinischen Daten des Eigentümers trägt und, falls gewünscht, mit einem privaten Schlüssel den Eigentümer befähigt, elektronische Signaturen zu erzeugen. Auch mehrere europäische Staaten wie beispielsweise Estland oder Finnland geben bereits elektronische Identitätskarten, sogenannte Bürgerkarten, an ihre Bevölkerung aus (siehe Whitepaper "Die Bürgerkarte - Der digitale Personalausweis wird Realität in Europa"). Mit deren Hilfe werden nicht nur die Amtsgeschäfte der Bürger vereinfacht, auch nicht-staatliche Firmen können – analog zu dem herkömmlichen Personalausweis in der realen Welt – einen staatlichen Identitätsnachweis für ihre Geschäfte über das Internet verwenden.

Bislang gibt es in Deutschland noch keinen Beschluss, Signaturkarten als Bürgerausweise analog zu dem bestehenden Personalausweis auszugeben. Länder wie Belgien, Estland, Finnland, Italien, Österreich und auch die Schweiz sind derzeit in diesem zukunftsweisenden Geschäftsfeld Deutschland einen guten Schritt voraus. Signaturkarten werden in Deutschland derzeit noch stärker von den Banken (z.B. Deutsche Bank WebSign 24-Karte, Einsatz von Signaturkarten im Pilotbetrieb bei der HypoVereinsbank) als von den Behörden (z.B. Pilotprojekt Digitaler Dienstausweis beim BMI und BSI) emittiert. Die staatliche Ausgabe von Signaturkarten hätte unter anderem den Vorteil, dass sich schneller ein Standard entwickeln kann. Mehrere europäische Länder setzen bereits eine Bürgerkarte ein (siehe Whitepaper „Die Bürgerkarte - Der digitale Personalausweis wird Realität in Europa“).

Bei all den guten Ansätzen der Nutzung der Chipkartentechnologie im Bereich eGovernment in Europa ist davon auszugehen, dass die Bürgerkarte ebenfalls in Deutschland kommen wird, ansonsten würde sich der Vorsprung der anderen europäischen Länder nur weiter vergrößern. In der Zwischenzeit werden Alternativen für die Absicherung der Geschäftstransaktionen über mobile Netze benötigt.

Neben der Möglichkeit, Mobile TAN einzusetzen (siehe Whitepaper „Mobile TAN - Das Handy ersetzt die TAN-Liste“) können auch fortgeschrittene elektronische Signaturen verwendet werden.

Fortgeschrittene Signaturen füllen die Lücke aus

Im Sinne des Signaturgesetzes sind „elektronische Signaturen“ Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen.

Sulzbacher Straße 29-39, 65824 Schwalbach am Taunus, Deutschland
Telefon +49 (0) 6196/88289-0, Telefax +49 (0) 6196/88289-11
contact@novosec.com, www.novosec.com

Unter den elektronischen Signaturen gibt es „fortgeschrittene elektronische Signaturen“, die

- ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind,
- die Identifizierung des Signaturschlüssel-Inhabers ermöglichen,
- mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und
- mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Die Gleichstellung zwischen herkömmlicher Unterschrift und elektronischer Signatur gilt allerdings nur für die „qualifizierten elektronischen Signaturen“, die als Spezialfall der fortgeschrittenen elektronischen Signatur zusätzlich auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und mit einer sicheren Signaturerstellungseinheit erzeugt werden. Sollte dies allerdings nicht gefordert werden, können auch fortgeschrittene elektronische Signaturen eingesetzt werden. Solange also keine Signaturkarten mit qualifizierten elektronischen Zertifikaten für einen flächendeckenden Einsatz zur Verfügung stehen, können fortgeschrittene elektronische Signaturen diese bestehende Lücke ausfüllen, sofern durch weitere Maßnahmen ein adäquates Sicherheitsniveau gewährleistet ist.

Das Signaturgesetz ist technologieoffen gestaltet. So werden die einzelnen Methoden nicht vom Gesetzgeber vorgeschrieben; es müssen allerdings eine Reihe von Anforderungen, vor allem bzgl. der Sicherheit, erfüllt werden. Mit gewissen Maßnahmen ist es möglich, das mobile Endgerät in Verbindung mit fortgeschrittenen elektronischen Signaturen für sichere Geschäftstransaktionen einzusetzen.

Mobiles Endgerät dient als vertrauenswürdiges Terminal

Viele Firmen setzen derzeit bereits mobile Endgeräte gerade auch für ihre Außendienstmitarbeiter ein. Mittels eines mobilen Endgerätes können Arbeitsabläufe vereinfacht werden. So nutzen z.B. Mitarbeiter der Post ein mobiles Kartenterminal zur Abwicklung von Zahlungen per Nachnahme.

Sollten jedoch höhere Sicherheitsanforderungen bestehen (z.B. bzgl. der Integrität der Daten oder der Authentizität der Kommunikationspartner), ist der Einsatz von elektronischen Signaturen erforderlich. Es werden dabei Möglichkeiten gesucht, diese Signaturen einfach und kostengünstig in das System zu integrieren. Bei vielen Ansätzen muss ein erheblicher Aufwand betrieben werden, um z.B. Smartcards anzubinden. Mobilfunkanbieter und Banken haben dabei unterschiedliche Zielvorstellungen. Während Mobilfunkanbieter Dual Chip-Lösungen favorisieren, bei denen das Handy neben dem GSM-Chip einen weiteren kleinen Chip, auf dem die Identifikationsdaten gespeichert sind, besitzt, favorisieren Banken Dual Slot-Lösungen, bei denen das Mobiltelefon einen zusätzlichen Kartenschlitz besitzt, in den beispielsweise eine Bankkarte eingeführt werden kann. Es geht aber auch anders. Ohne allzu großen Aufwand lässt sich das mobile Endgerät als vertrauenswürdiges Terminal, als sogenannte „virtuelle Smartcard“, einsetzen. „Virtuell“ bedeutet in diesem Fall, dass der private Schlüssel, der für die Erstellung der elektronischen Signatur verwendet wird (siehe auch E-Government-Handbuch des BSI, http://www.bsi.de) zwar in Software gespeichert ist, aber dass die Sicherheit gleich hoch wie bei einem Hardware-Token ist. Gerade bei einigen Transaktionen im Außendienst sind teilweise die Unterschriften von zwei Außendienstmitarbeitern notwendig. Das Einholen der

Sulzbacher Straße 29-39, 65824 Schwalbach am Taunus, Deutschland
Telefon +49 (0) 6196/88289-0, Telefax +49 (0) 6196/88289-11
contact@novosec.com, www.novosec.com

benötigten Unterschriften bedeutet einen hohen Aufwand und Zeitverlust. Durch die Verwendung einer entsprechenden fortgeschrittenen elektronischen Signatur mittels mobilen Endgeräts kann der Prozess beschleunigt und vereinfacht werden. Der Außendienstmitarbeiter kann z.B. bei einem Zulieferer in München die Ware inspizieren und bei Gefallen seine Unterschrift „gemeinsam“ mit seinem Kollegen im Hamburger Büro unter den Kaufvertrag setzen. Auf diesem Wege können gerade kleine und mittlere Unternehmen, die nicht über eine umfangreiche Vertreterregelung verfügen, schnell und einfach Verträge mit ihren Geschäftspartnern abschließen.

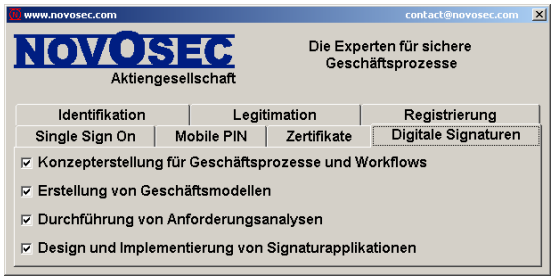
Der Einsatz des mobilen Endgerätes ermöglicht es, das Gesamtgerät als virtuelle Klasse 3-Signatureinheit zu betrachten. Der Vorteil dabei ist, dass mehrere Signaturschlüssel (für unterschiedliche Applikationen) auf das Gerät eingebracht werden können. Das umständliche Wechseln der Signaturkarten entfällt dabei. Zusätzlich erhöht sich dadurch die Sicherheit nochmals, da gegenüber öffentlicher Klasse 3 Signatureinheiten Manipulationen (gesamtes Terminal ist ein Trojaner) ausgeschlossen werden können, da der Benutzer in der Regel das komplette Gerät stets bei sich trägt. Weiterhin kann auch die Benutzerfreundlichkeit wesentlich erhöht werden, da die fehleranfällige Installation der Klasse 3-Lesegeräte entfällt. Mit Hilfe des mobilen Endgerätes können auch komplexere Daten (z.B. Grafiken, längere Texte) signiert werden, da bei mobilen Endgeräten ein grafisches Display mit erheblich höherer Auflösung als bei den heutigen Klasse 3-Terminals zur Verfügung steht. Diese Klasse 3-Terminals haben in der Regel lediglich ein 2-zeiliges Display mit maximal 16 Buchstaben pro Zeile.

Fazit

Der Einsatz elektronischer Signaturen kann und wird den alltäglichen Geschäftsverkehr vereinfachen. Signaturkarten konnten sich bislang in Deutschland nicht als Identifikationsmedien durchsetzen. Dennoch werden Signaturkarten in der Zukunft eine zentrale Rolle einnehmen; vor allem wenn in Deutschland wie in anderen europäischen Ländern die (elektronische) Bürgerkarte eingeführt wird. Für den Fall, dass die Schriftform erfüllt werden muss, können auf dem elektronischen Weg nur qualifizierte elektronische Signaturen eingesetzt werden. Andere elektronische Signaturen sieht der Gesetzgeber zu diesem Zweck nicht vor. Sofern jedoch keine Schriftform erfüllt sein muss, können Mobile TAN oder fortgeschrittene elektronische Signaturen eingesetzt werden. Mittels einer fortgeschrittenen Signatur kann ein mobiles Endgerät als vertrauenswürdiges Terminal eingesetzt werden und mindestens bis zur flächendeckenden Einführung von qualifizierten elektronischen Signaturen Geschäfte schnell und sicher mobil abgewickelt werden. Gerade die massive Verbreitung von Mobiltelefonen in Deutschland lässt vermuten, dass dank der neuen Kommunikationssysteme UMTS und WLAN der mCommerce belebt wird.

Wünschen Sie nähere Informationen zu diesem Thema? Wir freuen uns auf Ihre Anfragen.

robert.nitschke@novosec.com



Weitere Artikel finden Sie unter:
http://www.novosec.com/downloads