8. Elektronische Signatur

Beispiel: Wer ist mein Vertragspartner?

Herr Ulrich arbeitet als Vertriebsmitarbeiter bei einem großen Einrichtungskonzern. Die von ihm vertriebenen Wasserbetten sind ein Bestseller. Immer mehr nutzt er das Internet dazu, um Vertragsabschlüsse anzubahnen und zu finalisieren. Teilweise kennt er seine Geschäftspartner gar nicht mehr persönlich, sondern verkehrt mit diesen nur mehr per E-Mail und Telefon.

Eines Tages macht Herr Ulrich allerdings eine unangenehme Erfahrung: Per E-Mail wendet sich Herr Windig an ihn. Er sei selbst Inhaber eines Möbelstudios und habe von den tollen Produkten, die Herr Ulrich vertreibt, erfahren. Nach einem längeren Mailverkehr teilt Herr Ulrich mit, dass er eine Kollektion verschiedener Wasserbetten erwerben wolle. Herr Ulrich macht sich natürlich gleich an die Arbeit und schreibt eine halbe Nacht lang ein Angebot, welches Herr Windig einen Tag später dann auch per E-Mail bestätigt. Eine Woche später will die von Herrn Ulrich beauftragte Spedition Speedy die Wasserbetten in das Möbelstudio von Herrn Windig zustellen. Allerdings stellt sich heraus, dass sich an der angegebenen Adresse ein Fastfood-Lokal befindet und Herr Windig dort völlig unbekannt ist. Die Mitarbeiter von Speedy nehmen daher die Wasserbetten wieder mit. Herr Ulrich versucht aufzuklären, was denn passiert ist. Alle E-Mails an Herrn Windig bleiben allerdings unbeantwortet. Auch sonst muss Herr Ulrich feststellen, dass alle Angaben wie z.B. Telefonnummer, Name etc. falsch waren. Offenbar ist Herr Ulrich einem Scherzbold aufgesessen, der ihn auch schädigen wollte. Immerhin war die gesamte Arbeitszeit, die Herr Ulrich investiert hat, umsonst. Auch auf den Kosten für die Spedition Speedy bleibt Herr Ulrich sitzen.

Herr Ulrich beginnt daraufhin darüber nachzudenken, wie er zukünftig sicherstellen kann, dass seine Vertragspartner tatsächlich existieren und hinter den entsprechenden Verträgen tatsächlich jene Personen stehen, die anhand der Umstände zu erwarten sind. Sein Freund, ein Computerexperte, erzählt ihm daraufhin erstmals etwas von der elektronischen Signatur.

Die zunehmende Bedeutung elektronisch vorgenommener Willenserklärungen, Rechtsgeschäfte usw. verlangt nach Verfahren, welche die Echtheit der Herkunft (Authentizität) und die Unversehrtheit des Inhalts (Integrität) elektronisch übermittelter Daten gewährleisten. Mit anderen Worten: Wie kann man gesichert feststellen, von wem die Daten stammen? Und wie kann man überprüfen, ob diese Daten (z.B.: Vertragserklärungen, Namen etc.) noch ident sind mit denen, die der Absender wahrgenommen hat?

Die „elektronische Signatur" erfüllt diese Funktion. Laut Signaturgesetz handelt es sich dabei um „elektronische Daten, die anderen elektronischen Daten beigefügt oder mit diesen logisch verknüpft werden und die der Authentifizierung, also der Feststellung der Identität des Signators[17], dienen". In der Praxis bedient man sich dabei bestimmter Verschlüsselungsverfahren, die in diesem Zusammenhang aber keine Geheimhaltung bewirken. Vielmehr ermöglicht die Verschlüsselung nur dem rechtmäßigen Unterzeichner, eine elektronische Signatur zu erstellen, ermöglicht aber jedermann, eine elektronische Signatur zu prüfen. Die Signaturprüfung geschieht meistens mit Hilfe eines so genannten Zertifikats: Dies ist eine Datenstruktur, durch welche die für die Signaturprüfung erforderlichen Daten einem bestimmten Unterzeichner zugeordnet werden. Damit das Zertifikat nicht gefälscht werden kann, enthält es seinerseits die elektronische Signatur eines (vertrauenswürdigen) Zertifizierungsdiensteanbieters. Auch diese elektronische Signatur kann mit Hilfe eines Zertifikats geprüft werden, welches entweder vom Zertifizierungsdiensteanbieter selbst, von einem anderen Zertifizierungsdiensteanbieter oder von der Aufsichtsstelle ausgestellt wird.

Nun ein paar grundsätzliche Informationen zu den bei der elektronischen Signatur angewandten Verschlüsselungstechniken. Dabei wird das Prinzip der asymmetrischen Verschlüsselung verwendet.

Die symetrische Verschlüsselung

Um den Vorteil der asymmetrischen Verschlüsselung zu verstehen, ist es wichtig, zuerst den Nachteil einer symmetrischen Verschlüsselung zu begreifen. Bei der symmetrischen Verschlüsselung müssen der Sender und der Empfänger einen geheimen Schlüssel (siehe Abbildung 20) kennen.

[17] Signator = Unterschriftsberechtigter

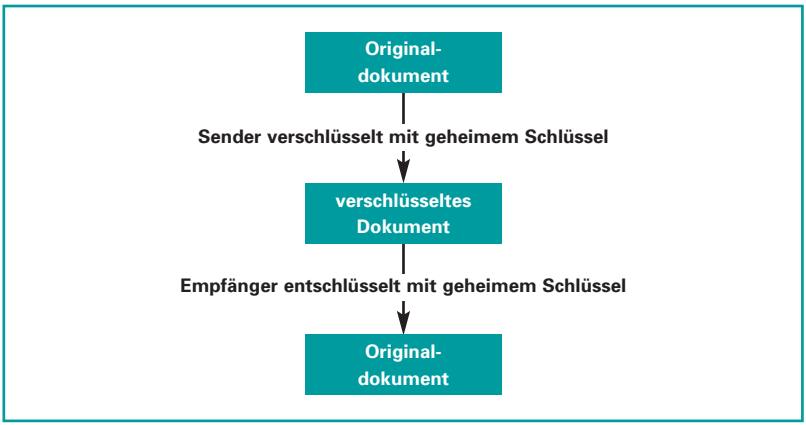

Abbildung 20: Prinzip der symmetrischen Verschlüsselung

Ein Nachteil dieses Verfahrens ist, dass Sender und Empfänger den geheimen Schlüssel vereinbaren müssen. Praktisch bedeutet das, dass z.B. bei einer E-Mail-Kommunikation der Sender und der Empfänger den geheimen Schlüssel per Telefon vereinbaren müssen. Der einzige und geheime Schlüssel darf daher nicht in dritte Hände gelangen und muss sorgfältig verwahrt bleiben. Für eine Signaturerstellung ist die symmetrische Verschlüsselung nicht verwendbar. Da derselbe Schlüssel immer im Besitz von mehreren Personen sein muss, kann nie zuverlässig festgestellt werden, wer von diesen ein Dokument verschlüsselt hat. Wenn z.B. drei Personen den gleichen symmetrischen Schlüssel besitzen und diese dasselbe Dokument verschlüsseln, unterscheiden sich die drei verschlüsselten Dokumente nicht voneinander. Eine Rückführung der Dokumente auf eine der drei Personen ist daher nicht möglich.

Die asymetrische Verschlüsselung

Diese Unzulänglichkeiten können durch die Prinzipien der asymmetrischen Verschlüsselung beseitigt werden. Bei der asymmetrischen Verschlüsselung gibt es ein Schlüsselpaar, das aus einem geheimen Teil (privater Schlüssel, Private Key) und einem nicht geheimen Teil (öffentlicher Schlüssel, Public Key) besteht. Dieser öffentliche Schlüssel kann

jedem beliebigen Kommunkationspartner mitgeteilt werden, er kann beispielsweise auch auf einer Website veröffentlicht werden. Der private Schlüssel hingegen muss, wie auch bei der symmetrischen Verschlüsselung der geheime Schlüssel, sicher verwahrt werden und darf nicht an andere weiter gegeben werden.

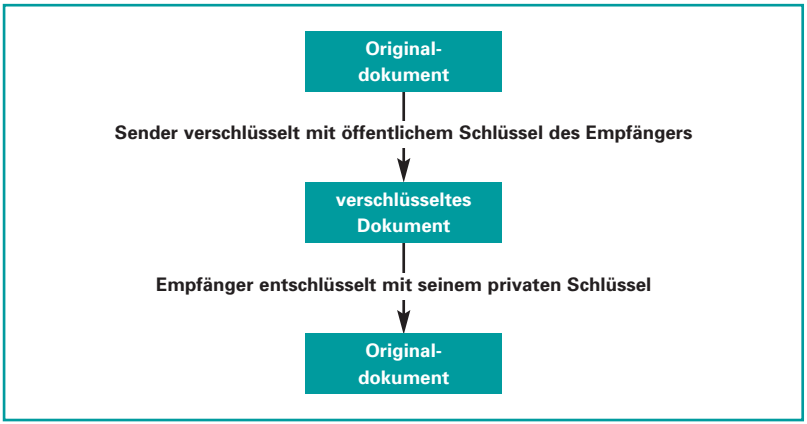

Abbildung 21: Prinzip der asymmetrischen Verschlüsselung

Der private Schlüssel ermöglicht es seinem Inhaber, z.B. Daten zu entschlüsseln (siehe Abbildung 21), digitale Signaturen zu erzeugen oder sich zu authentifizieren. Der öffentliche Schlüssel ermöglicht es jedermann, Daten für den Schlüsselinhaber zu verschlüsseln (siehe Abbildung 21), dessen digitale Signaturen zu prüfen oder ihn zu authentifizieren. Im Gegensatz zu einem symmetrischen Verschlüsselungssystem müssen die kommunizierenden Parteien keinen gemeinsamen geheimen Schlüssel kennen. Es ist daher auch nicht möglich, ein Dokument, das mit dem öffentlichen Schlüssel verschlüsselt wurde, wieder mit dem öffentlichen Schlüssel zu entschlüsseln. Nur mit dem privaten Schlüssel könnte ein solches Dokument wieder entschlüsselt werden. Umgekehrt kann nur mit dem öffentlichen Schlüssel ein mit dem privaten Schlüssel verschlüsseltes Dokument wieder entschlüsselt werden.

Dieses Prinzip macht sich die digitale Signatur zunutze. Mit dem geheimen privaten Schlüssel wird ein Dokument (oder richtiger eine mathematische Prüfsumme eines Dokuments) verschlüsselt. Weiß man jetzt, welche Person im Besitz des privaten Schlüssels ist, kann man mit Hilfe des öffentlichen (und im Internet frei zugänglich gemachten) Schlüssels überprüfen, ob tatsächlich diese Person das entsprechende Dokument verschlüsselt hat: Lässt sich nämlich mit dem öffentlichen Schlüssel das Dokument wieder herstellen, ist dieses Dokument zwingend von der Person, die als einzige den privaten Schlüssel besitzt und die es ursprünglich verschlüsselt hat.

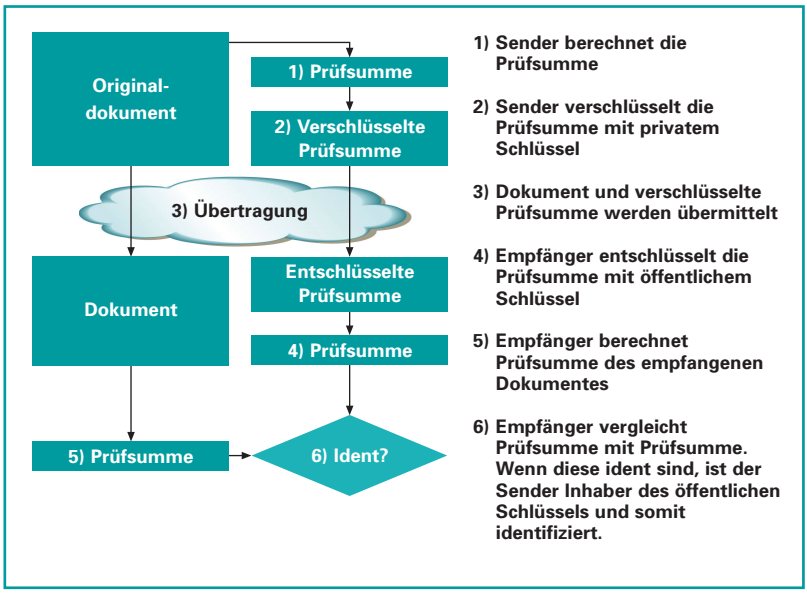

Abbildung 22: Prinzip der elektronischen Signatur

8.1 Arten der elektronischen Signatur

Die sichere elektronische Signatur

Die „stärkste" Signatur in Österreich ist die sichere elektronische Signatur. Sie ist der eigenhändigen Unterschrift rechtlich weit gehend gleichgestellt. Für die Erstellung sicherer elektronischer Signaturen sind in der Regel eine Chipkarte (z.B. Bankomatkarte), ein geeignetes Chipkarten-Lesegerät und spezielle Software erforderlich. Weiters benötigt man dafür ein qualifiziertes Zertifikat, mit dem die (vom Zertifizierungsdiensteanbieter anhand eines amtlichen Lichtbildausweises geprüfte) Identität des Chipkarten-Inhabers bestätigt wird.

Auf die sichere elektronische Signatur kann nicht verzichtet werden, wenn dem Erfordernis einer eigenhändigen Unterschrift in elektronischer Form entsprochen werden muss. Derzeit bietet die A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH mit ihrem Zertifizierungsdienst „a.sign Premium" als einziger österreichischer Anbieter qualifizierte Zertifikate für sichere elektronische Signaturen an. Diese Zertifikate können in zahlreichen Registrierungsstellen, beispielsweise in Bankfilialen, erworben werden.

Neben der sicheren elektronischen Signatur finden auch andere Formen Verwendung, so z.B. die Amtssignatur oder die fortgeschrittene Signatur. Die Unterscheidungskriterien der verschiedenen Signaturen ergeben sich zum Teil aus dem Verwendungszweck, aber auch aus der jeweiligen technischen Ausgestaltung.

Der Korrektheit halber ist hinzuweisen, dass sich im Bereich der elektronischen Signaturen in absehbarer Zeit gesetzliche Änderungen ergeben können und es daher neue Formen der elektronischen Signaturen geben kann.

Online-Banking

Die digitale Signatur ist auch für die sichere Durchführung von Banktransaktionen geeignet. Seit einiger Zeit wird häufig über Schadprogramme als Bedrohung im Online-Banking berichtet. Beispielsweise existieren Trojanische Pferde, welche eingegebene Transaktionsnummern abfangen und für vom Kontoinhaber ungewollte Überwei-

sungen missbrauchen. Solche Schadprogramme setzen sich typischerweise im Browser ihres Opfers fest.

Der Einsatz elektronischer Signaturen kann vor derartigen Angriffen wirkungsvoll schützen. Zahlreiche Banken bieten Online-Banking auf Basis elektronischer Signaturen an, wobei die Aufträge an die Bank mit der sicheren elektronischen Signatur des Kunden versehen werden.

Um sichere elektronische Signaturen erstellen zu können, benötigt man ein Chipkarten-Lesegerät mit eigener PIN-Tastatur, das ein Ausspähen der PIN ausschließt. Durch die Verwendung geeigneter Software-Komponenten (Secure Viewer) wird gewährleistet, dass die zu signierenden Daten vor der Signaturerstellung dem Signator (Unterschriftsberechtigten) z.B. auf dem Monitor präsentiert werden und Veränderungen nach der Signaturerstellung erkennbar sind.

Schadprogramme, die sich im Browser festsetzen, wirken sich auf Secure Viewer nicht aus. Sie können signierte Aufträge ohne Zutun des Kunden weder erstellen noch abändern. Überdies werden die meisten Secure Viewer einer strengen Prüfung nach anerkannten Sicherheitsvorgaben unterzogen, wobei u.a. die Unveränderbarkeit der zu signierenden Daten nachgewiesen werden muss.

In Österreich sind folgende Methoden beim Online-Banking verbreitet:

- Der vom Hamburger Unternehmen SecCommerce Informationssysteme GmbH hergestellte Secure Viewer SecSigner, für den eine Zertifizierung und eine Bestätigung nach dem deutschen Signaturgesetz vorliegen, wird vor allem bei der BAWAG P.S.K. Gruppe eingesetzt.
  Zahlreiche andere Banken setzen auf ELBA Electronic Banking, das auf der Seite des Anwenders eine Bürgerkartenumgebung (z.B. trustDesk basic von der IT Solution GmbH oder hotSign von der BDC EDV-Consulting GmbH) voraussetzt.

- Von der ARZ Allgemeines Rechenzentrum GmbH, welche zahlreiche Volksbanken, Hypobanken und Privatbanken betreut, wird ein System betrieben, das auf der Seite des Anwenders ebenfalls eine Bürgerkartenumgebung voraussetzt.

8.2 Elektronische Signaturen im E-Government

Das Konzept der Bürgerkarte ist die Grundlage von E-Government in Österreich. Die Bürgerkarte kann beispielsweise in Form einer Chipkarte (a.sign Premium, e-Card) oder virtuell (A1 SIGNATUR) vorliegen.

Zentraler Bestandteil des Konzepts ist die Bürgerkartenumgebung: eine Software-Komponente, über die Anwendungen auf Funktionen einer Chipkarte (z.B. Bankomatkarte, e-Card) zugreifen können. Die Bürgerkartenumgebung eignet sich nicht nur für E-Government-Applikationen, sondern auch beispielsweise für bestimmte Systeme im Online-Banking.

Die Bürgerkartenumgebung erlaubt sowohl die Signaturerstellung als auch die Signaturprüfung. Darüber hinaus kann damit auf zusätzliche Informationen, die auf der Bürgerkarte gespeichert sind, zugegriffen werden. Dies betrifft vor allem die „Personenbindung": eine elektronisch signierte Bestätigung der Stammzahlenregisterbehörde (Datenschutzkommission), die der in der Bürgerkarte als Inhaberin bezeichneten natürlichen Person eine so genannte „Stammzahl" zuordnet. Bei der Stammzahl handelt es sich um eine zur Identifikation bestimmte Zahl, die demjenigen, der identifiziert werden soll, eindeutig zugeordnet ist. Sie dient als Ausgangsbasis für die elektronische Durchführung von Behördenwegen. Wichtig ist allerdings zu erwähnen, dass diese Zahl von keiner Behörde dauerhaft gespeichert werden darf. Das Konzept der Bürgerkarte gewährleistet, dass immer nur aus der Stammzahl abgeleitete und nicht rückführbare „bereichsspezifische Personenkennzeichen" an die jeweilige Behörde übermittelt werden. Jeder Person sind somit für verschiedene Verwaltungsbereiche unterschiedliche Zahlen zur Identifikation zugeordnet. Somit können Behörden verschiedener Verwaltungsbereiche untereinander keinen Datenabgleich hinsichtlich konkreter Personen mit Hilfe der verwendeten Identifikationszahlen durchführen.

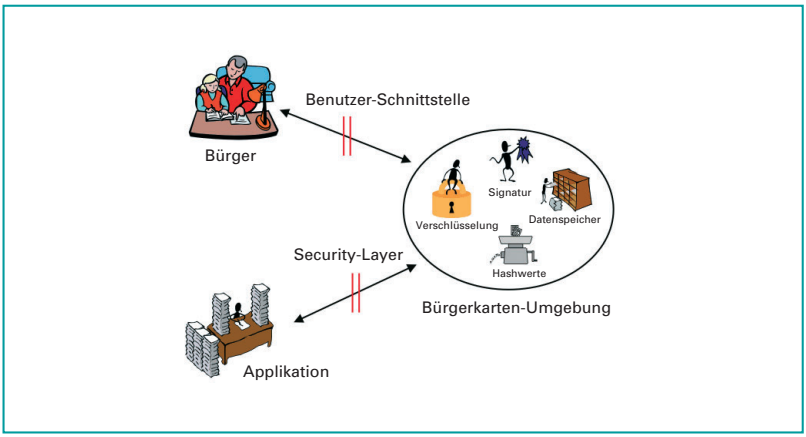

Abbildung 23: Das Modell der Bürgerkarte
(Quelle: http://www.buergerkarte.at/konzept/securitylayer/spezifikation/aktuell/introduction/Introduction.html

E-Government-Applikationen auf Basis der Bürgerkarte findet man unter http://www.help.gv.at. Ein typisches Beispiel einer Verwendungsmöglichkeit ist die Meldebestätigung. Mittlerweile können aber auch zahlreiche andere Amtswege mittels Bürgerkarte erfolgen: FinanzOnline, Strafregisterbescheinigung, Personen- und Meldeauskunft usw. Für die elektronische Zustellung gerichtlicher und behördlicher Schriftstücke gemäß E-Government-Gesetz kann man sich ebenfalls mittels Bürgerkarte beim Zustelldienst anmelden (http://www.zustellung.gv.at). Im Unterschied zu E-Mail und anderen elektronischen Kommunikationsarten ist eine erfolgreiche Zustellung bei diesem Dienst nachweisbar.

Bei der österreichischen Sozialversicherung (http://www.sozialversicherung.at) können mittels Bürgerkarte Versicherungszeiten sowie Grunddaten zur Krankenversicherung abgerufen werden. Für Vertragspartner (z.B. Ärzte) besteht überdies die Möglichkeit der Versicherungsnummernabfrage.

Weitere Informationen über die Bürgerkarte sind unter http://www.buergerkarte.at verfügbar.