Ausarbeitung zum Thema „Die digitale Signatur“ Proseminar Internetökonomie SS 2003

Manuel Voigt (Matrikelnr.703120)

manuel.voigt@student.hpi.uni-potsdam.de

31. August 2003

Zusammenfassung

In diesem Dokument wird der rechtliche Rahmen und die Funktionsweise der digitalen Signatur beschrieben. Es handelt sich um eine Ausarbeitung zu dem Vortrag „Die digitale Signatur - Funktionsweise und rechtlicher Rahmen“, der im Rahmen des Proseminars „Internetökonomie“ im Sommersemester 2002 an der Universität Potsdam gehalten wurde.

Die Ramenbedingungen zur digitalen Signatur befinden sich im Gesetz zur digitalen Signatur und in der Verordnung zur digitalen Signatur.

Der Benutzer, der ein elektronisches Dokument digital signieren möchte, lässt sich zuerst von einer Zertifizierungsstelle, die von der Regulierungsbehörde für Telekommunikation und Post zugelassen ist, ein Schlüsselpaar generieren und aushändigen. Dieses Schlüsselpaar besteht aus einem privaten und einem öffentlichen Schlüssel. Von dem zu verschlüsselnden Dokument wird zuerst ein Hashwert berechnet und dieser dann mit dem privaten Schlüssel des Senders verschlüsselt. Anschließend wird das Dokument zusammen mit dem verschlüsselten Hashwert an den Empfänger versendet. Der Empfänger kann den Hashwert mit dem öffentlichen Schlüssel des Senders entschlüsseln und vergleicht diesen Hashwert mit dem von Empfänger berechneten und mitgeschickten Hashwert des Dokuments. Stimmen beide Hashwerte überein ist die digitale Signatur gültig.

Durch die Verwendung der digitalen Signatur kann die Verbindlichkeit, d.h. ob das Dokument wirklich von der Person, die angegeben ist stammt, und die Integrität, d.h. ob das Dokument nach der Signierung verändert, des Dokuments gesichert werden. Die Verbindlichkeit ist gesichert, da nur der Sender den Hashwert des Dokuments verschlüsseln kann. Denn nur der Sender besitzt

den privaten Schlüssel. Die Dokumentintegrität wird durch die Berechnung, Signierung und Überprüfung des Hashwertes des Dokuments erreicht.
Die digitale Signatur ist in einigen Bereichen der Rechtssprechung zugelassen und ist eine sichere Methode die Verbindlichkeit und die Integrität von elektronischen Dokumenten zu garantieren.

Inhaltsverzeichnis

1 Einleitung

In vielen Bereichen der Wirtschaft und im privatem Bereich ersetzt die elektronische Post (E-Mail) den herkömmlichen Brief. Unglücklicherweise sind die elektronischen Daten nicht immer sicher und geschützt. Durch die Verwendung der digitalen oder elektronischen Signatur kann man die Integrität und die Verbindlichkeit von elektronischen Dokumenten sichern. Die Funktionsweise und der rechtliche Rahmen der digitalen Signatur sollen in diesem Dokument beschrieben werden.

2 Vergleich elektronischer Dokumente mit herkömmlichen schriftlichen Dokumenten

In diesem Abschnitt wird ein Vergleich von herkömmlichen schriftlichen Dokumenten und herkömmlichen elektronischen Dokumenten vorgenommen. In diesem Vergleich soll die Verfälschbarkeit und Sicherheit dieser beiden Dokumenttypen gegenüber gestellt und die Notwendigkeit der digitalen Signatur dargestellt werden.
Weder schriftliche noch herkömmliche elektronische Dokumente können als sicher bezeichnet werden. Bei schriftlichen Dokumenten können Unterschriften sehr leicht und von geübten Personen sogar ununterscheidbar gefälscht werden. Ferner können sogar die Inhalte von schriftlichen Dokumenten geändert werden. Ist ist sehr schwer nachzuweisen, ob die Änderungen vom Author des Dokuments gemacht wurden oder ob die Änderungen von einen dritten Person getätigt wurden. Ebenso kann man bei unterschriebenen Dokumenten nicht unterscheiden ob Änderungen vor dem Unterschreiben durch den Autor oder nach dem Unterschreiben von einer dritten Person gemacht wurden.
Herkömmliche elektronische Dokumente können ebenfalls leicht manipuliert werden. Änderungen an elektronischen Dokumenten sind nicht mehr rekonstruierbar. Ferner kann nicht festgestellt werden, ob die Änderungen durch menschliche Fehler oder durch vorsätzliche Manipulation entstanden sind. Ebenso ist das Abbilden einer eigenhändigen Unterschrift in ein elektronisches Dokument nicht sehr sicher, da auch diese Unterschrift wie bei herkömmlichen schriftlichen Dokumenten leicht gefälscht werden kann.
Durch das Verwenden der digitalen Signatur wird das Verändern von elektronischen Dokumenten erschwert und die Fälschungssicherheit der Dokumente erhöht.

3 Beschreibung des rechtlichen Rahmens der digitalen Signatur

Der rechtliche Rahmen der digitalen Signatur ist im Gesetz zur digitalen Signatur (Signaturgesetz, SigG) und in der Verordnug zur digitalen Signatur (Signaturverordnung, SigV) beschrieben.
Das Gesetz zur digitalen Signatur ist am 01.08.1997 in Kraft getreten und ist im Artikel 3 des Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste enthalten. Das Ziel des Gesetzes zur digitalen Signatur ist es Rahmenbedingungen zu schaffen, unter denen digitale Signaturen als sicher gelten und Fälschungen digitaler Signaturen oder Verfälschungen von signierten Daten zuverlässig festgestellt werden können. Zusätzlich ist am 01.11.1997 die Verordnung zur digitalen Signatur in Kraft getreten. Die Signaturverordnug basiert auf §16 des Gesetzes zur digitalen Signatur.

3.1 Signaturgesetz

Das Signaturgesetz beinhaltet 25 Paragraphen, die in sechs Abschnitte aufgeteilt sind.
Der erste Abschnitt enthält die ersten drei Paragraphen und ist mit „Allgemeine Bestimmungen“ betitelt. Im ersten Paragraphen ist der Zweck und Anwendungsbereich des Gesetzes definiert. In diesem Paragraphen lautet es unter anderem: „Zweck des Gesetzes ist es, Rahmenbedingungen für elektronische Signaturen zu schaffen.“ Im zweiten Paragraphen werden Begriffe, die im Gesetzestext vorkommen wie „elektronische Signatur“ oder „Signaturschlüssel“ erklärt. Im dritten Paragraphen, der sich ebenfalls im ersten Abschnitt befindet, wird die für dieses Gesetz zuständige Behörde genannt. Es steht dort geschrieben: „Die Aufgaben der zuständigen Behörde nach diesem Gesetz und der Rechtsverordnung [...] obliegen der Behörde nach § 66 des Telekommunikationsgesetzes.“ Im § 66 des Telekommunikationsgesetzes wird die Regulierungbehörde für Telekommunikation und Post genannt. Daraus folgt, dass die Regulierungsbehörde die für die digitale Signatur zuständige Behörde ist.
Der zweite Abschnitt des Signaturgesetzes enthält die Paragraphen 4 bis 14. In diesem Abschnitt werden die Rechte und Pflichten eines Zertifizierungsdienstanbieters definiert. Ein Zertifizierungsdienstanbieter nimmt die Zuordnung eines Schlüssels zu einer Person vor und garantiert diese. In den Paragraphen dieses Abschnittes sind zum Beispiel die Anforderungen an einen Zertifizierungsdienstanbieter beschrieben. Er muss zum Beispiel Deckungsvorsorge in Höhe von 250000 Euro treffen, damit er seine gesetzliche Verpflichtung zum Ersatz von Schäden nachkommen kann. Ein Schaden kann zum Beispiel das Stehlen von Schlüsselpaaren vom Zertifizierungsdienstanbieter sein. Die gestohlenen Schlüssel können für kriminelle Aktionen missbraucht werden. Außerdem ist in diesem Abschnitt die Vergabe von Schlüsseln vom Zertifizierungsdienstanbieter an einen Kunden definiert. In diesem Abschnitt werden auch Datenschutzbestimmungen und die Haftung von Zertifizierungsdienstanbieter beschrieben.

Der dritte Abschnitt ist mit „Freiwillige Akkreditierung“ bezeichnet und umfasst die Paragraphen 15 und 16 In diesen beiden Paragraphen wird die freiwillige Akkreditierung beschrieben. Freiwillige Akkreditierung nennt man den Vorgang in dem eine juristische oder natürliche Person zu einem Zertifizierungsdienstanbieter wird. Desweiteren wird der Inhalt der Zertifikate, die die Regulierungbehörde für den Zertifizierungsdienstanbieter ausstellt, beschrieben. Dieses Zertifikat bestätigt die rechtskonforme Zulassung des Zertifizierungsdienstanbieters.
Im vierten Abschnitt, der die Paragraphen 17 und 18 umfasst wird auf die technische Sicherheit in den Zertifizierungsstellen eingegangen. Hier werden Sicherheitsvorschriften für technische Produkte, die in Zertifizierungsstellen eingesetzt werden können, beschrieben. Ebenfalls werden in diesem Abschnitt des Signaturgesetzes die Rechte und Pflichten von Prüf- und Bestätigungsstellen definiert. Diese Stellen prüfen technische Produkte, die in den Zertifizierungsstellen eingesetzt werden können. Auch diese Prüf- und Bestätigungsstellen müssen von der Regulierungsbehörde überprüft und genehmigt worden sein.
Im fünften Abschnitt, die aus den Paragraphen 19 und 20 besteht, werden die Aufsichtsmöglichkeiten der Regulierungsbehörde und die Mitwirkungspflicht der Zertifizierungsdienstanbieter vorgeschrieben. Ein Zertifizierungsdienstanbieter muss, wenn die Regulierungsbehörde dies wünscht, der Regulierungsbehörde alle Bücher, Schriftstücke, Verträge und sonstige Dokumente vorlegen. Ebenso ist ein Zertifizierungsdienstanbieter verpflichtet der Regulierungsbehörde Auskunft zu geben .
Der letzte Abschnitt enthält die Paragraphen 21 bis 25. In ihm stehen die Schlussbestimmungen des Gesetzes. Hier findet man unter anderem die Bußgeldvorschriften sowie die Kosten und Beiträge für die Genehmigung und den Betrieb einer Zertifizierungsstelle.

3.2 Signaturverordnung

Für die konkrete Ausführung des Signaturgesetzes werden Ausführungsbestimmungen in der Signaturverordnung definiert. So werden das Genehmigungsverfahren und die Richtlinien sowie die Rechte und Pflichten für Zertifizierungsdienstanbieter in dieser Verordnung beschrieben. Die Signaturverordnung besteht aus 19 Paragraphen. Es werden die Verfahren zur Erteilung, Rücknahme und Widerruf von Genehmigungen zum Bertrieb einer Zertifizierungsstelle beschrieben. Ebenfalls wird das Antragsverfahren zur Vergabe von Zertifikaten[1] von der Zertifizierungsstellen an ihre Kunden erklärt. Ferner sind die Voraussetzungen und Qualifikation für den Betreiber einer Zertifizierungsstelle und die Mitarbeiter der Zertifizierungsstelle in der Signaturverordnung vorgeschreiben.

[1] Ein Zertifikat ist ein Schlüsselpaar, das von der Zertifizierungsstelle erstellt wird und dem Kunden dann ausgehändigt wird. Ferner wird in der Zertifizierungsstelle eine Zuordnung des Schlüsselpaares zu dem Kunden vorgenommen. Die geschieht zum Beispiel durch einen Eintrag in eine Datenbank.

4 Funktionsweise der digitalen Signatur

4.1 Asymetrische Verschlüsselung

Zum Erzeugen einer digitalen Signatur wird die asymetrische Verschlüsselung benutzt. Asymetrische Verschlüsselung bedeutet, dass man zum Verschlüsseln einen anderen Schlüssel verwendet als zum Entschlüsseln. Die beiden Schlüssel werden privater Schlüssel und öffentlicher Schlüssel genannt. Der private Schlüssel dient bei der digitalen Signatur zur Erzeugung der Signatur. Er befindet sich meistens auf einer Chipkarte und kann nur von der dem Schlüssel zugeordneten Person benutzt werden. Zu diesem Zweck ist die Chipkarte mit einer PIN gesichert[2], die nur der dem Schlüssel zugeordnete Benutzer wissen kann und soll.
Der öffentliche Schlüssel dient zum Entschlüsseln der digitalen Signatur und ist jedem Empfäger eines Dokuments des entsprechenden Absenders bekannt. Oft wird der öffentliche Schlüssel mit dem signierten Dokument mitgeschickt.

4.2 Erzeugung der digitalen Signatur

Der Absender, der ein Dokument digital Signieren möchte erstellt dieses und berechnet anschließend den Hashwert dieses Dokumentes. Hierzu kann ein beliebiger Hash-Algorithmus verwendet werden. Der Hash-Algorithmus muss nur dem Empfänger des digital Signierten Dokuments bekannt sein. Aus Sicherheitsgründen sollte eine starke Hashfunktion[3] verwendet werden. Die Berechnug des Hashwertes ist nötig um die Integrität des signierten Dokuments zu gewährleisten. Außerdem ist die Verschlüsselung schneller, da nur der Hashwert, der kleiner ist als das ursprüngliche Dokument ist, verschlüsselt werden muss. Der berechnete Hashwert des Dokuments wird mit dem privaten Schlüssel des Absenders verschlüsselt. Anschließend werden das Dokument sowie die digitale Signatur, bei der es sich um den verschlüsselten Hashwert des Dokuments handelt an den Empfänger versendet.
Die digitale Signatur schützt nicht die Vertraulichkeit des Inhalts des signierten Dokuments, da diese im Klartext an den Empfänger verschickt wird. Möchte der Absender zusätzlich die Vertraulichkeit des Dokuments sichern, muss er das Dokument ebenfals verschlüsseln. Die Verschlüsselung des Dokumentes ist strikt von der digitalen Signatur des Dokumentes zu trennen. Die Erstellung einer digitalen Signatur soll Abbildung 1 verdeutlichen.

---

[2] Der private Schlüssel, der sich auf der nicht auslesbaren Karte befindet ist dem Schlüsselbesitzer nicht bekannt. Er kann ein Dokument nur Signieren wenn er die Karte und die dazugehörige PIN kennt.

[3] Eine starke Hashfunktion ist eine Einwegfunktion (d.h aus dem Hashwert läßt sich nicht der der Hashfunktion übergebene Wert ermitteln) und die mit der Hashfunktion errechneten Werte müssen kolisionsfrei (d.h. zu keinen zwei verschieden Argumente der Hashfunktion soll der gleiche Hashwert von der Funktion berechnet werden) sein.

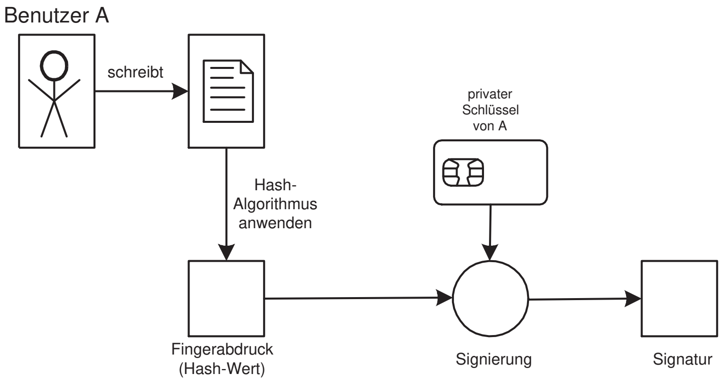

Abbildung 1: Erstellung einer digitalen Signatur

4.3 Kontrolle der digitalen Signatur

Der Empfänger erhält vom Sender das originale Dokument und die digitale Signatur des Dokuments. Um die digitale Signatur zu überprüfen, muss der Empfänger zuerst den verschlüsselten Hashwert des Dokuments, der die digitale Signatur ist, entschlüsseln. Diese Entschlüsselung erfolgt mit dem öffentlichen Schlüssel des Absenders. Dieser Schlüssel kann mit dem Dokument und der dem Dokument zugehörigen digitalen Signatur mitgeschickt werden. Nach der Entschlüsselung erhält der Empfänger den Hashwert der Dokuments, der vom Absender berechnet wurden. Anschließend berechnet der Empfänger mit der gleichen Hashfunktion wie der Absender den Hashwert des mitgeschickten Dokumentes. Stimmen der berechnete und der entschlüsselte Hashwert überein, so ist die digitale Signatur gültig und die Integrität des Dokuments gewährleistet. Wäre das Dokument während der Übertragung von einer dritten Person verändert worden, würde sich der vom Empfänger errechnete Hashwert von dem verschlüsselten Hashwert des Absenders unterscheiden. Dies ist auf den Kolisionsfreiheit der verwendeten Hashfunktion zurückzuführen. Den Entschlüsselungsvorgang des Empfängers ist in Abbildung 2 dargestellt.

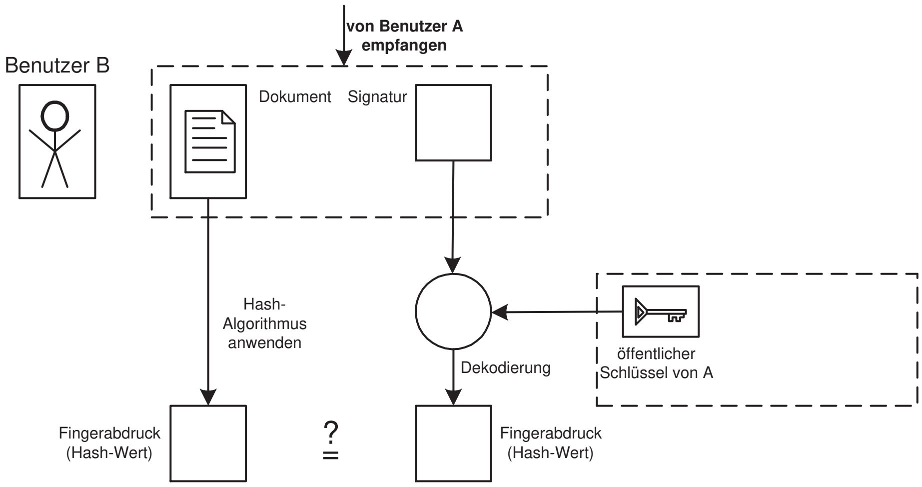

Abbildung 2: Überprüfung einer digitalen Signatur

5 Zertifizierungsstellen

5.1 Warum werden Zertifizierungsstellen benötigt?

In diesem Abschnitt wird geklärt was Zertifizierungstellen mit der digitalen Signatur zu tun haben und warum diese benötigt werden. Man stelle sich folgende Situation vor:
Ein Krimineller bestellt bei einem Händler teure Waren. Er signiert die Bestellung mit seinem privaten Schlüssel und schickt den dem privaten Schlüssel zugehörigen öffentlichen Schlüssel mit dem Bestellung an den Händler. Der Kriminelle gibt in der Bestellung nicht seinen eigenen Namen und Adresse an, sondern den einer anderen Person (die er nicht besonders gut leiden kann). Der Händler schickt die Waren mit der Rechnung an die falsche Person.
Man erkennt in diesem Beispiel genau, dass der Händler eine Versicherung braucht, dass die digitale Signatur genau von der Person stammt, deren Name auch in der Bestellung steht. Für diese Zuordnung von einem Schlüsselpaar zu einer Person sind Zertifizierungstellen zuständig. Die Schlüsselvergabe von Zertifizierungsstellen und die Sicherheitsanforderungen an Zertifizierungsstellen sind im Signaturgesetz und in der Signaturverordnung beschrieben.

5.2 Schlüsselvergabe von Zertifizierungsstellen

Ein Kunde, der seine Dokumente digital signieren möchte, muss sich bei einer Zertifizierungsstelle anmelden und ein Schlüsselpaar generieren lassen. Dieses Schlüsselpaar zertifiziert die entsprechende Zertifizierungsstelle. Um ein Schlüsselpaar beantragen zu können muss der Kunde seine Identität eindeutig nachweisen. Dies kann zum Beispiel durch die Vorlage eines Personalausweises geschehen. Die Zertifizierungsstelle händigt dem Kunden dann sein Schlüsselpaar aus und speichert die Daten des Kunden in ihrer Datenbank. Nun kann die Zuordnung des öffenlichen Schlüssels zu einer bestimmten Person überprüft werden und eine kriminelle Handlung, wie oben beschrieben, ist nicht mehr möglich.

5.3 Sicherheitanforderungen an Zertifizierungsstellen

Bei der Beantragung zum Betrieb einer Zertifizierungsstelle (freiwillige Akkreditierung) müssen unter anderem auf Verlangen Mitarbeiterqualifikations- und Führungszeugnisse vorgelegt werden, da sichergestellt werden soll, dass das Personal der Zertifizierungssstelle über entsprechende Qualifikationen im juristischen und administrativen Bereich verfügt und nicht kriminell vorbelastet ist. Zusätzlich muss nachgewiesen werden, dass die Geräte und Programme, die in der Zertifizierungsstelle eingesetzt werden sollen, den Stand der Technik entsprechen. Dies kann zum Beispiel duch das Benutzen von gesprüften Komponenten geschehen. Zu diesen Komponenten, die auch Signaturanwendungskomponenten genannt werden, gibt es ein extra Kapitel in diesem Dokument. Es muss ebenfalls bei der Beantragung einer Zertifizierungsstelle das gesamte Sicherheitskonzept für die Zertifizierungsstelle dargestellt werden. Zusätzlich muss der Betreiber einer Zertifizierungsstelle einen hohen Geldbetrag besitzen um eventuell entstehende Schadenersatzforderungen seiner Kunden bezahlen zu können. Schadenersatz muss zum Beispiel gezahlt werden wenn aus der Datenbank der Zertifizierungsstelle Schlüsselpaare von Kunden entwendet werden. Es sollte ebenfalls bei einer Zertifizierungsstelle ein Mix von Sicherheitsverkehrungen an den Signaturanwendungskomponenten selbst und an der Einsatzumgebung existieren. Unter diesem Mix versteht man sichere Signaturanwendungskomponenten und die sichere Verwahrung der Signaturanwendungskomponenten. Die sichere Verwahrung kann zum Beispiel durch Videoüberwachnung, sichere Türen und Schlösser und duch einen Wachschutz erreicht werden.

6 Signaturanwendungskomponeten

Bei Signaturanwendungskomponenten handelt es sich um Hard- und Softwarekomponenten, die für die Erstellung und Überprüfung einer digitalen Signatur benötigt werden. Signturanwendungskomponenten sind zum Beipiel die Hashwertberechnungssoftware oder ein Chipkartenleser. Die Zertifizierungsstellen müssen die Signaturanwendungskomponenten nicht selber entwickeln sondern können diese von Fremdherstellern kaufen. Diese Fremdhersteller haben sich auf die Herstellung von bestimmten Signaturanwendungskpomponenten spezialisiert.

6.1 Sicherheitsanforderungen an Signaturanwendungskomponenten

Für die Signaturanwendungskomponenten wurden von der Regulierungsbehörde Vorschriften definiert. Es müssen bei Softwaresignaturanwendungskopmponenten, die zur Erstellung oder Überprüfung einer digitalen Signatur genutzt werden, eindeutige Bildschirmmeldungen an den Benutzer ausgegeben werden. Solche Bildschirmmeldungen sind zum Beispiel die Anzeige einer Meldung beim Erstellen einer digitalen Signatur. Desweiteren müssen die Daten, die mit der erstellten digitalen Signatur signiert werden, angezeigt werden. Ebenso muss bei der Überprüfung einer digitalen Signatur eindeutig das Ergebnis der Überprüfung angezeigt werden. Auch sollten die Signaturanwendungskomponenten eine leicht verständliche Bedienungsanleitung besitzen.

6.2 Prüfung von Signaturanwendungskomponenten

Die Signaturanwendungskomponenten werden von unabhängigen Prüf- und Bestätigungsstellen überprüft. Diese Stellen vergeben für überprüfte und genehmigte Signaturanwendungskomponenten ein Gütesiegel. Diese Komponenten können dann von den Zertifizierungsstellen verwendet werden. Die Aufgaben und Pflichten der Prüf- und Bestätigungsstellen werden im Signaturgesetz beschrieben.

7 TeleSec - eine Zertifizierungsstelle

Als Beipiel einer Zertifizierungsstelle soll hier kurz die TeleSec und eines ihrer Produkte beschrieben werden. Bei der TeleSec handelt es sich um eine bei der Regulierungsbehörde für Telekommunikation und Post akkreditierte Tochterfirma von T-Systems. Da die TeleSec akkreditiert ist, erfüllt sie die hohen technischen und administrativen Anforderungen des Signaturgesetzes. Ferner war die TeleSec die erste in Deutschland zugelassene Zertifizierungsstelle.
Die TeleSec bietet neben Produkten für Geschäftskunden ein Out-of-the-Box-Produkt für private Nutzer und kleine Firmen an. Das Komplettpaket besteht aus einem SmartCard-Terminal sowie einer Chipkarte nebst Zertifikat für ein Jahr. Das Zertifikat wird im Web beantragt und nach Ausstellung auch dort heruntergeladen. Zuvor muss ein Fax mit der Antragsnummer und einer Kopie des Personalausweises an die TeleSec gefaxt werden. Ist das Zertifikat installiert, kann es benutzt werden um Mails und Daten zu signieren.

8 Quellen

- Dokument: „Sinn der Signatur“ von der Regulierungs für Telekommunikation und Post
- Signaturgesetz vom 16 Mai 2001 und Signaturverordnung

Internetseiten:

- www.heise.de
- www.regTP.de
- www.vnunet.de

Abbildungsverzeichnis