

Seminararbeit an der Wirtschafts- und Sozialwissenschaftlichen Fakultät der
Universität Fribourg, Schweiz

Digitale Signatur

Anwendungen in der Zukunft?

vorgelegt von

Thomas Marthaler
Grubenweg 11
3052 Zollikofen

und

Philip Suter
Arvenweg 2
5703 Seon

eingereicht bei

Prof. Dr. A. Meier
Professor for Information Technology

Fribourg, 30. Oktober 2003



Inhaltsverzeichnis

Inhaltsverzeichnis.....	I
Darstellungsverzeichnis	III
Einleitung	IV
1 Grundlagen der digitalen Signatur.....	1
1.1 Aufbau und Funktionsablauf der digitalen Signatur	2
1.1.1 Aufbau	2
1.1.2 Funktionsablauf.....	2
1.1.2.1 Voraussetzungen.....	2
1.1.2.2 Ablauf.....	2
1.2 Verschlüsselung.....	4
1.2.1 Die Verschlüsselungsmethoden.....	5
1.2.2 Andere Verschlüsselungsmethoden.....	5
1.3 Grad der Sicherheit	8
1.3.1 Technische Sicherheit.....	8
1.3.2 Sicherheit der Schlüssel	8
1.3.3 Gewährleistung der Authentizität.....	8
2 Rechtliche Grundlage	10
2.1 Verordnung über Dienste der elektronischen Zertifizierung (Zertifizierungsdienstverordnung, ZertDV)	10
2.2 Entwurf des Bundesgesetzes über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES)	11
2.3 Anpassung der bestehenden Rechtsprechung	11
3 Beispiele aus dem öffentlichen Sektor.....	12
3.1 Guichet virtuel	12
3.1.1 Vorstellung des Projektes.....	12
3.1.2 Einsatzmöglichkeiten der digitalen Signatur	13
3.2 Vote électronique.....	14
3.2.1 Das Genfer Pilotprojekt	14
3.2.2 Das Neuenburger Pilotprojekt	16
3.2.3 Das Zürcher Pilotprojekt.....	17
3.2.4 Einsatzmöglichkeiten der digitalen Signatur	17
3.3 TaxMe Online.....	18
3.3.1 Vorstellung des Projektes.....	18
3.3.2 Einsatzmöglichkeiten der digitalen Signatur	18
4 Beispiele aus dem Dienstleistungssektor.....	19
4.1 Bedeutung für die Wirtschaft	19
4.2 Banken.....	19
4.2.1 Hypothek per E-Mail	20
4.2.1.1 Ablauf heute.....	20
4.2.1.2 Ablauf mit Hilfe der digitalen Signatur	20
4.3 Versicherungen.....	21



4.4	Treuhand-Unternehmen	21
4.5	Bedeutung für den Dienstleistungssektor	21
5	Vergleich der Projekte aus den beiden Sektoren	22
6	Fazit und Ausblick	23
	Literaturverzeichnis	24
	Quellenverzeichnis.....	26



Darstellungsverzeichnis

Abbildung 1: Ablauf	4
Abbildung 2: Inhalt von www.ch.ch	12
Tabelle 1: Vergleichsmatrix.....	22



Einleitung

Im Rahmen des Wirtschaftstudiums an der Universität Fribourg müssen alle Studenten pro Studienjahr eine Semesterarbeit schreiben. Wir haben uns für das Thema digitale Signatur entschieden, weil wir uns für die modernen Kommunikationstechnologien interessieren und der Meinung sind, dass diese Art von Unterschrift in Zukunft eine wichtige Rolle spielen wird.

Unsere Ausführungen beschränken sich auf die Schweiz und Schweizer Organisationen.

Ziel der Arbeit ist es, in einem ersten Teil die rechtlichen und technischen Grundlagen zu vermitteln. In einem zweiten Abschnitt werden wir anhand von Beispielen aus dem öffentlichen Sektor sowie aus dem Dienstleistungssektor den Stand der Entwicklung in der Praxis aufzeigen. Gleichzeitig diskutieren wir einige zukunfts-trächtige Anwendungsgebiete der digitalen Signatur.

Abschliessen werden wir unsere Arbeit mit einem Vergleich der beiden Sektoren, dem Fazit und einem Ausblick.

Wir möchten an dieser Stelle die landläufige Meinung dementieren, dass digital signierte Dokumente automatisch elektronisch verschlüsselt werden. Tatsache ist, dass jedes digital signierte Dokument, das abgefangen wird, auch gelesen werden kann, sofern der Absender das Dokument selbst nicht noch zusätzlich verschlüsselt hat. Hierzu ein Beispiel:

In der Ritterzeit wurden wichtige Dokumente mit einem Siegel versehen. Der Empfänger konnte somit sicher sein, dass der Inhalt nicht verändert wurde und die Botschaft auch tatsächlich vom angegebenen Absender stammt. Wurde dieser Brief aber unterwegs abgefangen, konnte er ohne Probleme aufgebrochen und gelesen werden. Wollte man dies verhindern, musste man eine Geheimsprache anwenden. Dasselbe gilt auch heute noch für die elektronischen Dokumente.

Philip Suter hat die Kapitel 1 und 3 verfasst, Thomas Marthaler die Kapitel 2 und 4. Die Punkte 5 und 6 sind im Team geschrieben worden.



1 Grundlagen der digitalen Signatur

Mit zunehmender Nutzung des Internets steigt auch das Bedürfnis nach Sicherheitsverfahren, welche die Integrität¹ und Authentizität² von elektronischen Dokumenten garantieren. Dies leistet die digitale Signatur, der bei der Einführung von Online-Anwendungen eine Schlüsselrolle zukommt.

«Bei digitalen Signaturen handelt es sich um eine kryptographische Technik, mit der die Integrität und Authentizität von digitalen Informationen gewährleistet werden kann. Insofern sind digitale Unterschriften mit handgeschriebenen Unterschriften vergleichbar.

Solche digitalen Unterschriften sollen folgende Eigenschaften aufweisen:

- Sie sollten schwer zu fälschen sein: das heisst, nur der Besitzer des privaten Schlüssels kann die Signatur erstellen.
- Sie sollten verbindlich sein: ein signiertes Dokument kann später nicht abgelehnt werden.
- Das Dokument muss durch die Signatur unveränderbar werden, nachträgliche Änderungen müssen unmöglich sein.
- Sie dürfen nicht übertragbar sein: die Unterschrift kann nicht entfernt und an einer anderen Stelle wieder in ein Dokument eingefügt werden.

Eine digitale Signatur muss also die Integrität einer Nachricht vermitteln und einzigartig sein. Solche Unterschriften sollen verhindern, dass einem signierten Text weitere Textteile hinzugefügt werden können. Auch wäre es verheerend, wenn die digitale Signatur von einem signierten Dokument einfach auf ein anderes Dokument übertragen werden könnte.»³

¹ Integrität = Echtheit des übermittelten Dokumentes

² Authentizität = Gewissheit über die Identität des Absenders

³

http://www.ifi.unizh.ch/ikm/Vorlesungen/ebusiness02/Arbeiten/Public%20Key%20Infrastructure_Seminararbeit_SS02.pdf, S. 16



1.1 Aufbau und Funktionsablauf der digitalen Signatur

1.1.1 Aufbau

«Bei digitalen Signaturen werden asymmetrische Verschlüsselungsverfahren eingesetzt. Es wird bei diesen Verfahren mit zwei Schlüsseln gearbeitet, die als privater und öffentlicher Schlüssel bezeichnet werden. Die Dokumente, die mit dem privaten Schlüssel verschlüsselt werden, können nur mit dem korrespondierenden öffentlichen Schlüssel wieder entschlüsselt werden. Der private Schlüssel muss unbedingt geheim bleiben. Der öffentliche Schlüssel darf jedermann bekannt sein.»⁴

1.1.2 Funktionsablauf⁵

1.1.2.1 Voraussetzungen

Jeder Anwender, der elektronische Dokumente mit einer digitalen Signatur versehen will, muss zuerst den privaten und öffentlichen Schlüssel bei einer Zertifizierungsstelle beantragen und registrieren lassen. Die Zertifizierungsstelle nimmt die Personalien des Antragsstellers entgegen und weist diese Angaben einem bestimmten öffentlichen Schlüssel zu. Dieses Zertifikat ist öffentlich frei zugänglich. Sobald ein Empfänger eine digital signierte Nachricht erhält, kann er den öffentlichen Schlüssel bei der Zertifizierungsstelle nachprüfen lassen und bekommt so die absolute Sicherheit, dass der Absender auch wirklich derjenige ist, den er vorgibt zu sein.

Eine solche Registrierung bei einer Zertifizierungsstelle ist also die Voraussetzung um überhaupt digital signierte Dokumente zu übermitteln.

1.1.2.2 Ablauf

Alle nachfolgend beschriebenen Schritte beziehen sich auf die Abbildung 1.

Schritt 1:

Die Zertifizierungsstelle, auch Trustcenter genannt, stellt einen sogenannten «digitalen Pass» aus, der aus einem öffentlichen Schlüssel und einem privaten Schlüssel besteht (vgl. letzter Punkt). Der Absender besitzt zu diesem Zeitpunkt 3 Dinge: einen öffentlichen Schlüssel, einen privaten Schlüssel und das zu übermittelnde Dokument.

Schritt 2:

Aus der Zeichenfolge des Dokumentes generiert der Absender nun per Computer mit einem bestimmten Algorithmus einen sogenannten Hash-Wert. Diese Zahlenfolge ist jetzt eine Art von Fingerabdruck des Textes. Diese Zahlenfolge identifiziert also das zu versendende Dokument eindeutig.

⁴ http://www.systor.com/dl_know_bizpub_digitale_signatur.pdf, S. 4

⁵ vgl. http://www.systor.com/dl_know_bizpub_digitale_signatur.pdf



Anschliessend wird dieser Hash-Wert mit dem privaten Schlüssel des Absenders verschlüsselt. Weiter könnte das Dokument selbst noch verschlüsselt werden, damit es, sollte es abgefangen werden, nicht gelesen werden kann. Diese Chiffrierung muss aber nicht unbedingt vorgenommen werden, da die Integrität und Authentizität auch sonst gewährleistet ist.

Schritt 3:

Dem Empfänger werden nun 4 Dinge übermittelt: der verschlüsselte Hash-Wert, der verwendete Algorithmus, das eigentliche Dokument und der öffentliche Schlüssel, damit der Empfänger den Hash-Wert wieder entschlüsseln kann.

Schritt 4:

Der Empfänger entschlüsselt mit dem öffentlichen Schlüssel den Hash-Wert. Gleichzeitig generiert der Empfänger selber mit dem gleichen Algorithmus wie der Absender einen Hash-Wert aus dem Dokument. Stimmen die beiden Werte überein, so ist die Integrität des Textes sichergestellt, d.h. die Nachricht wurde nach dem Absenden nicht mehr verändert.

Schritt 5:

Schliesslich prüft der Empfänger die Absenderkoordinaten mit dem öffentlichen Schlüssel nach, damit die Authentizität des Absenders sichergestellt ist, d.h. dass der Absender auch derjenige ist, den er vorgibt zu sein. Dazu ruft er beim Zertifizierungsdienst die Informationen zu diesem öffentlichen Schlüssel ab.

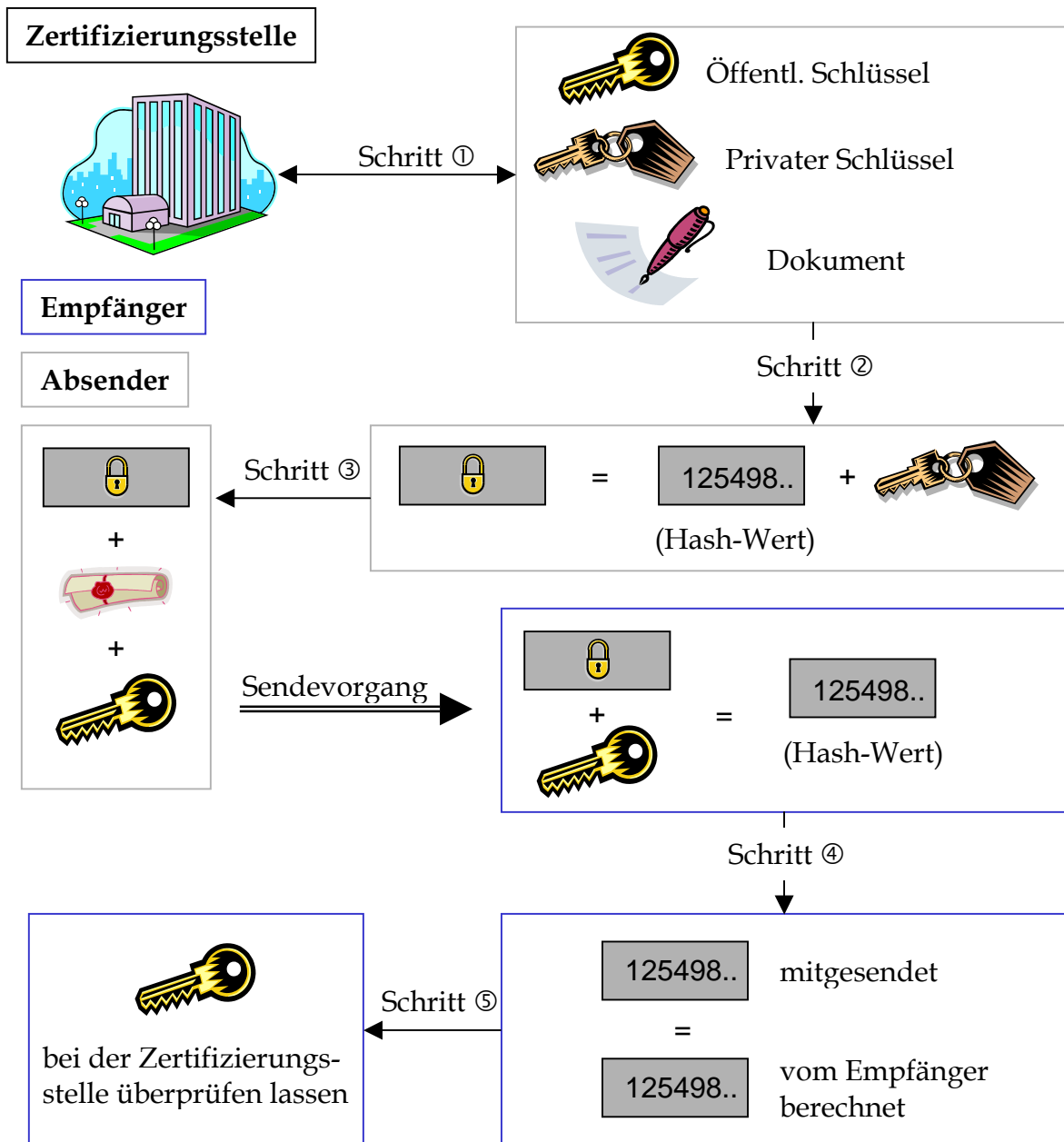


Abbildung 1: Ablauf

1.2 Verschlüsselung

«Kryptographie ist die Wissenschaft, welche sich mit der Verschlüsselung und Entschlüsselung von Daten und den damit zusammenhängenden Möglichkeiten beschäftigt.

Die Kryptographie basiert darauf, dass der Empfänger über ein geheimes Wissen verfügt, welches ihm erlaubt, die zuvor verschlüsselte Nachricht zu entschlüsseln. Die Methoden der Verschlüsselung sind Algorithmen, welche meistens bekannt sind. Der eigentliche Schlüssel zum Geheimnis bleibt jedoch verborgen. Es gibt zwar



Kryptographiesysteme, die auf einem geheimen Algorithmus beruhen, doch diese werden aufgrund ihrer Nichteinsehbarkeit nur ungern verwendet.»⁶

1.2.1 Die Verschlüsselungsmethoden

«Es gibt verschiedene Verschlüsselungsalgorithmen, welche eine Nachricht (Klartext) in eine scheinbar sinnlose Zeichenfolge (kodierte Nachricht, Chiffretext) umwandeln, und umgekehrt. Symmetrische Algorithmen unterscheiden sich von asymmetrischen durch die Anzahl Schlüssel. Die Symmetrische Verschlüsselung kommt mit einem Schlüssel aus. Hingegen braucht es bei der asymmetrischen Verschlüsselung zwei Schlüssel, welche mathematisch miteinander zusammenhängen.»⁷ Schliesslich gibt es noch hybride Verfahren, welche eine Kombination der symmetrischen und asymmetrischen Verschlüsselungsmethoden sind.

1.2.2 Andere Verschlüsselungsmethoden

Eine weitere Verschlüsselungsmethode ist die asymmetrische Verschlüsselung. Dieses Verfahren wird heute sehr oft verwendet, weil es sehr sicher ist. Auch bei der digitalen Signatur wird diese Art von Verschlüsselung angewandt.

Im Asymmetrischen Verschlüsselungsverfahren, auch Public-Key Verschlüsselung genannt, existieren zwei verschiedene Schlüssel, die mathematisch miteinander zusammenhängen:

Privater Schlüssel (Private Key): «Dieser bleibt grundsätzlich beim Eigentümer des Schlüssels und wird zum Entschlüsseln von verschlüsselten Nachrichten verwendet, die mit dem zugehörigen öffentlichen Schlüssel verschlüsselt wurden.»⁸

Öffentlicher Schlüssel (Public Key): «Dieser Schlüssel des Schlüsselpaares muss der Eigentümer des Schlüsselpaares zuerst an einen Absender übergeben, damit dieser dann Nachrichten für den Eigentümer (Empfänger) des öffentlichen Schlüssels verschlüsseln kann.»⁹

⁶

http://www.ifi.unizh.ch/ikm/Vorlesungen/ebusiness02/Arbeiten/Public%20Key%20Infrastructure_Seminararbeit_SS02.pdf, S. 8

⁷

http://www.ifi.unizh.ch/ikm/Vorlesungen/ebusiness02/Arbeiten/Public%20Key%20Infrastructure_Seminararbeit_SS02.pdf, S. 9

⁸

http://www.ifi.unizh.ch/ikm/Vorlesungen/ebusiness02/Arbeiten/Public%20Key%20Infrastructure_Seminararbeit_SS02.pdf, S. 12

⁹

http://www.ifi.unizh.ch/ikm/Vorlesungen/ebusiness02/Arbeiten/Public%20Key%20Infrastructure_Seminararbeit_SS02.pdf, S. 12



«Bei der Berechnung der beiden Schlüssel geht man folgendermassen vor:

1. Zwei zufällige, grosse Primzahlen p und q wählen.
2. Das Produkt aus den zwei Primzahlen berechnen: $n = p \cdot q$
3. eine kleine Zahl e zufällig wählen, so dass $e < (p-1)(q-1)$.
Bedingung ist, dass e und $(p-1)(q-1)$ keine gemeinsamen Teiler (ausser 1) besitzen.
4. Die Zahl d mit Hilfe des Euklidischen Algorithmus berechnen:
$$d = e^{-1} \text{ mod } (p-1)(q-1)$$

Ein Zahlenbeispiel:

1. Zwei zufällige, grosse Primzahlen: $p = 3$ und $q = 11$
2. Das Produkt aus den zwei Primzahlen: $n = p \cdot q \Rightarrow 33 = 3 \cdot 11$
3. Eine kleine Zahl e zufällig wählen: $e < (p-1)(q-1) \Rightarrow e < (3-1)(11-1) = 20$
Bedingungen: 1) $e < 20$
2) e und $(p-1)(q-1)$ keine gemeinsamen Teiler:
Mögliche Lösungen: $e = 3, 7, 9, 11, 13, 17, 19$, eine auswählen, z.B. 13
4. Die Zahl $d = e^{-1} \text{ mod } (p-1)(q-1)$ berechnen:
$$d = 13^{-1} \text{ mod } (3-1)(11-1) = 13^{-1} \text{ mod } 20 = 17$$

Nun kann man n und e als öffentlichen Schlüssel (Public Key) veröffentlichen. Die Zahl d muss geheim gehalten werden, denn sie bildet zusammen mit n den privaten Schlüssel (Private Key). Die 2 Primzahlen p und q werden nicht mehr gebraucht und sollten gelöscht werden.

Anhand der folgenden Formeln wird der Gebrauch der zwei Schlüssel verdeutlicht:

$$y = x^e \text{ mod } n$$

$$x = y^d \text{ mod } n$$

wobei x = Klartext und y = Chiffretext ist.

Bei unserem Zahlenbeispiel würden $n = 33$ und $e = 13$ den öffentlichen Schlüssel darstellen, während $n = 33$ und $d = 17$ zusammen den privaten Schlüssel ergeben. Angewendet auf ein Beispiel würde die Verschlüsselung so aussehen:



Gegeben: $x = \text{Klartext} = 30$

Gesucht: $y = \text{Chiffretext}$

Lösung: $y = x^e \bmod n \Rightarrow y = 30^{13} \bmod 33 = 6$

Chiffretext = 6

Möchte der Empfänger den Chiffretext dekodieren, verwendet er die folgende Formel:

$$x = y^d \bmod n \Rightarrow x = 6^{17} \bmod 33 = 30 = \text{Klartext}$$

Ein beträchtlicher Nachteil des asymmetrischen Verfahrens ist die Geschwindigkeit. Algorithmen für Public-Key Verschlüsselungen arbeiten etwa tausend mal langsamer als symmetrische Algorithmen. Der Grund ist die enorme Schlüssellänge, die im Normalfall von 768 bis 2058 Bit sein kann.»¹⁰

Bei der digitalen Signatur werden der öffentliche und der private Schlüssel andersherum angewendet. Das heisst, man unterzeichnet das Dokument mit dem geheimen Schlüssel, damit sichergestellt ist, dass die Signatur nur vom Besitzer dieses Schlüssels stammt. Nachher kann jeder der im Besitze des entsprechenden öffentlichen Schlüssels ist überprüfen, ob die Nachricht auch wirklich vom erwarteten Empfänger stammt und nicht unterwegs von einer anderen Person verändert worden ist.

¹⁰

http://www.ifi.unizh.ch/ikm/Vorlesungen/ebusiness02/Arbeiten/Public%20Key%20Infrastructure_Seminararbeit_SS02.pdf, S. 12 ff



1.3 Grad der Sicherheit

1.3.1 Technische Sicherheit

Eine 100%-Sicherheit gibt es nie, denn eine Verschlüsselung ist nur so sicher, wie der leistungsfähigste Computer. Das bedeutet, dass man den Grad der Sicherheit mit der Rechenleistung von Computern vergleicht. Man sagt, eine Verschlüsselung ist sicher, wenn eine computergestützte Lösung sehr lange (mehrere Jahre) dauert, man spricht daher auch von «rechnerisch sicher». Ist demzufolge eine Verschlüsselungsmethode rechnerisch nicht mehr sicher, wird sie entsprechend ausgebaut oder ersetzt.

Aus technischer Sicht ist die digitale Signatur also sicher.

1.3.2 Sicherheit der Schlüssel

Ein wie unter Punkt 1.2.2 beschriebenes Verschlüsselungssystem steht und fällt mit dem privaten Schlüssel. Kommt dieser Schlüssel aus irgend welchen Gründen an die Öffentlichkeit, ist der Missbrauch sehr wahrscheinlich. Es ist demzufolge von entscheidender Bedeutung, dass die privaten Schlüssel sehr sorgfältig gelagert werden.

1.3.3 Gewährleistung der Authentizität

Aus technischer Sicht ist es problemlos möglich ein passendes Schlüsselpaar zu generieren und zu benutzen. Wer garantiert nun, dass der entsprechende Schlüssel auch wirklich zu der Person gehört, die das Dokument signiert hat? Der alleinige Besitz eines solchen Schlüsselpaares genügt also nicht, um eine vertrauenswürdige Identität zu gewährleisten.

An dieser Stelle treten die Zertifizierungsstellen, auch Trust Center genannt in Aktion. Diese Zertifizierungsinstanz ist eine natürliche oder juristische Person, die die Zuordnung von öffentlichen Schlüsseln zu natürlichen Personen bescheinigt.

Das Trust Center hat zwei Hauptaufgaben:

1. Registration Authority (Annahmestelle)
Hier geht es primär darum, den Antragsteller zu identifizieren. Wichtig ist, dass nur natürliche Personen ein Schlüsselpaar registrieren lassen können, d.h. juristische Personen müssen bevollmächtigte Personen registrieren lassen um die digitale Signatur anwenden zu können.
2. Certification Authority
Darunter versteht man die technische Erzeugung von Schlüsselpaaren und Zertifikaten, z.B. auf eine Chipkarte.



Weitere Aufgaben des Trust Centers sind beispielsweise die Pflege des Schlüsselverzeichnisses, die Aufbewahrung der Schlüssel inkl. Key Recovery, der Zeitstempeldienst (Gültigkeitsüberprüfung, Einhalten von Fristen) und der Sperrdienst bei Missbrauch.

Die Trust Centers sind also für die Erzeugung von Schlüsselpaaren und die Identifizierung bzw. Zertifizierung von natürlichen Personen zuständig. Ein ausgestelltes Zertifikat enthält folgende Angaben:

- Name des Inhabers des öffentlichen Schlüssels
- Öffentlicher Schlüssel
- Algorithmus der zur Berechnung des Hash-Wertes benutzt wird
- Laufnummer
- Gültigkeitsdauer
- Einschränkungsbestimmungen

Zwei bekannte Zertifizierungsstellen in der Schweiz sind die SwissCERT AG¹¹ und die SWISSETrust¹².

¹¹ für weitere Informationen über die SwissCERT AG siehe: <http://www.swisscert.com>

¹² für weitere Informationen über die SWISSETrust siehe: <http://www.swisstrust.ch>



2 Rechtliche Grundlage

«Verträge bedürfen zu ihrer Gültigkeit nur dann einer besonderen Form, wenn das Gesetz eine solche vorschreibt».¹³ Artikel 11/1 des schweizerischen Obligationenrechts legt grundsätzlich die Formfreiheit für Verträge fest. So können formfreie Verträge ohne Probleme über das Internet abgewickelt werden. Ein klassisches Beispiel hierzu wären die E-Shops, die täglich Kaufverträge mit ihren Kunden über das Internet abschliessen.

Probleme mit dem Abschluss von Verträgen in digitaler Form ergeben sich erst, wenn das Gesetz dessen Schriftlichkeit vorschreibt. Die schriftliche Form bedeutet, dass alle Personen die verpflichtet werden sollen, den Vertrag eigenhändig unterschreiben müssen.¹⁴ So darf zum Beispiel ein Mieter nur Änderungen an der Mietsache vornehmen, wenn der Vermieter schriftlich zugestimmt hat.

Heute ist es somit noch nicht möglich, rechtsgültige Verträge, die der Schriftlichkeit bedürfen, über den elektronischen Weg abzuschliessen. Der Bundesrat ist nun daran diesen Umstand mit Erneuerungen im Rechtssystem zu ändern. Folgende Neuerungen und Änderungen müssen vorgenommen werden:

1. Es müssen neue gesetzliche Grundlagen für Anbieter von Zertifizierungsdiensten (Zertifizierungsstellen, Trust Center) und Anerkennungsstellen geschaffen werden.
2. Die bestehende Rechtsprechung muss zum Teil den neuen Anforderungen angepasst werden.

Im Folgenden werden diese Neuerungen und Änderungen kurz erklärt.

2.1 Verordnung über Dienste der elektronischen Zertifizierung (Zertifizierungsdienstverordnung, ZertDV)

Die ZertDV ist am 1. Mai 2000 in Kraft getreten und hat laut Art. 1 ZertDV folgenden Zweck: «Diese Verordnung legt im Sinne einer Versuchsregelung die Voraussetzungen für die freiwillige Anerkennung der Anbieterinnen von Zertifizierungsdiensten fest und regelt ihre Tätigkeiten im Zusammenhang mit der Ausstellung von elektronischen Zertifikaten.»¹⁵

Die Zertifizierungsstellen müssen ihre Produkte nicht anerkennen lassen. Nicht anerkannte Zertifikate werden aber nicht der eigenhändigen Unterschrift gleichgestellt sein und können somit nicht zum Abschluss rechtsgültiger Verträge, bei denen das Gesetz die schriftliche Form vorschreibt, verwendet werden.

Die Verordnung definiert im Weiteren die relevanten Begriffe in Zusammenhang mit der digitalen Signatur und regelt die Aufsicht über die anerkannten Anbieterinnen von Zertifizierungsdiensten.

¹³ Art. 11, Abs. 1 OR

¹⁴ Art. 14, Abs. 1 OR

¹⁵ Art. 1, Abs. 1 ZertDV



2.2 Entwurf des Bundesgesetzes über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES)

Schon bei der Verabschiedung der ZertDV hat der Bundesrat angekündigt, dass er eine Vorlage erarbeiten will, die für die Anerkennung der digitalen Signatur sorgt. Mit dem ZertES will er nun sein Versprechen einlösen.

Inhaltlich weicht der Entwurf des neuen Gesetzes kaum von der noch geltenden Verordnung ab. Neu dazu kommt aber die Haftung, da auf Verordnungsebene keine Abweichung von der Haftungsordnung im Obligationenrecht erlaubt ist.

Im Frühling 2003 wurde das Gesetz von der Rechtskommission des Nationalrates zu Ende beraten. Es folgt die Debatte in der Rechtskommission des Ständerates und im Ständerat. Realistischerweise muss davon ausgegangen werden, dass das ZertES nicht vor dem 1. Januar 2005 in Kraft treten wird.¹⁶

2.3 Anpassung der bestehenden Rechtsprechung

Die in diesem Kapitel gemachten Aussagen, beziehen sich auf Vorschläge und Entwürfe des Bundesrates. Die definitive Rechtsprechung kann davon noch abweichen. Die wichtigste Änderung betrifft sicherlich das Obligationenrecht. Der neu eingeführte Artikel 14, Absatz 2^{bis} OR setzt Zitat: «die qualifizierte elektronische Signatur, die auf einem qualifizierten Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten im Sinne des Bundesgesetzes vom ... über Zertifizierungsdienste im Bereich der elektronischen Signatur beruht und auf den Namen einer natürlichen Person lautet» der eigenhändigen Unterschrift gleich.

Weiter werden der Art. 59a OR, der die Haftung für Signaturschlüssel regelt und die Art. 929aOR / Art. 931 Abs. 2^{bis} OR, die die Führung des Handelsregister mittels Informatik regeln, eingeführt. Art. 13 Abs. 2 OR wird aufgehoben. Von verschiedenen Artikeln sollen die Randtitel geändert werden.

Von der Anpassung der bestehenden Rechtsprechung sind ferner betroffen: das Zivilgesetzbuch, das Topographiegesetz vom 9. Oktober 1992, das Marktschutzgesetz vom 28. August 1992, das Designgesetz vom 5. Oktober 2001 und das Patentgesetz vom 25. Juni 1954.

¹⁶ Laut einer E-Mail Auskunft am 24.04.2003 von Felix Schöbi, Bundesamt für Justiz



Mit dem Projekt «Guichet virtuel» sollen folgende Ziele erreicht werden:

- Es soll ein nach den Alltagsproblemen der Bürger gegliederter Zugang zu den Behörden geschaffen werden.
- Die gesuchten Informationen sollen möglichst rasch und einfach zu finden sein. Dem User wird eine Navigationshilfe zur Verfügung gestellt, die ihm aufzeigt, wo er sich innerhalb des Verwaltungsapparates befindet. Weiter wird ein Tracking-System angestrebt, d.h. dem Kunden werden die Bearbeitungsschritte und die Weiterleitung seines Anliegens mitgeteilt. Mit diesem Verfahren kann die Transparenz der Verwaltungen gesteigert werden, da die Abläufe nachvollziehbar werden.
- Die Internetseite soll von interessierten Bürgern mitgestaltet werden. Das Angebot soll den Bedürfnissen der User angepasst und laufend verbessert werden. Die Projektleiter denken, dass sich bald ein reger E-Mail-Kontakt zwischen der Verwaltung und den Anwendern entwickeln wird.
- Die grösseren Gemeinden und Städte, die über ein grösseres Budget und vielleicht schon über einen eigenen Internetauftritt verfügen, sollen beim Projekt als «Zugpferde» wirken. Gleichzeitig sollen kleinen Gemeinden Hilfen angeboten werden, damit auch diese möglichst schnell und kostengünstig einen Internetauftritt realisieren können.
- Der Zugang zu www.ch.ch soll für alle Bürger möglich gemacht werden. Für Interessierte, die keinen eigenen Internetanschluss haben, sind Zugänge z.B. auf den Gemeindeverwaltungen oder Poststellen geplant.

3.1.2 Einsatzmöglichkeiten der digitalen Signatur

Auch beim Kontakt mit Behörden ist es heute nicht möglich Geschäfte abzuschliessen, bei denen die persönliche Unterschrift Voraussetzung ist. Mit der Gleichstellung der digitalen Signatur mit der konventionellen Unterschrift würde der Guichet virtuel extrem aufgewertet werden. Der ganze «Papierkram» mit den Verwaltungen könnte problemlos per Internet abgewickelt werden. Vor diesem Hintergrund sind die Einsatzmöglichkeiten der digitalen Signatur sehr zahlreich. Hier nur einige Beispiele:

- Gesuche für Führerausweise könnten beim Strassenverkehrsamt auf elektronischem Weg eingereicht werden.
- Stipendiengesuche könnten direkt per Mausklick abgewickelt werden. Heute steht nur das Formular auf dem Internet zur Verfügung (Kanton Bern).
- Alle Änderungen der persönlichen Angaben (z.B. Adressänderungen) könnten den Verwaltungen elektronisch übermittelt werden.
- Die Transaktionen unter den Verwaltungsinstanzen könnten übers Internet erfolgen.

Der Einsatz der digitalen Signatur würde den Verwaltungsapparat vereinfachen und effizienter machen. Viele Daten und Formulare, wie z.B. Steuererklärungen, müssten nicht mehr erfasst oder eingescannt werden, was zu enormen Einsparungen von Ressourcen führen würde.¹⁸

Dem Gegenüberzustellen sind die zusätzlichen Kosten der Informatikmittel.

¹⁸ vgl. Kapitel 3.3, TaxMe Online, Seite 18



3.2 Vote électronique

Das Ziel des Bundes mit dem Projekt «Vote électronique» ist es, die Ausübung politischer Rechte auch über elektronische Verfahren zu ermöglichen. Er hat dazu eine Arbeitsgruppe ins Leben gerufen, die die Fragen in Zusammenhang mit elektronischen Abstimmungssystemen und der Schaffung eines harmonisierten Stimmregisters auf Bundesebene klären soll. Für dieses Projekt wurden für die Jahre 2001 bis 2004 ungefähr 7,5 Mio. Franken budgetiert. Der Bund hat die Kantone aufgefordert, eigene Projekte in Zusammenhang mit eVoting vorzuschlagen. Genf, Neuenburg und Zürich sind dieser Aufforderung nachgekommen und sind nun daran ihre Projekte zu realisieren. Im den folgenden Kapiteln sollen die Pilotprojekte der drei Kantone vorgestellt werden.¹⁹

3.2.1 Das Genfer Pilotprojekt²⁰

Im März 2001 hat die Genfer Regierung das Projekt offiziell gestartet und sich ihre Partner für die Realisierung ausgewählt. Es geht darum, neben der Stimmabgabe an der Urne und per Post für den Bürger eine dritte Möglichkeit zur Ausübung seiner demokratischen Rechte zu schaffen. Die folgenden Gründe sprachen für ein «Vote électronique» - Projekt:

- Nach der Einführung der brieflichen Stimmabgabe stieg die Stimmbeteiligung im Kanton Genf durchschnittlich um 20%. Heute machen 95% der Stimmbürger von der brieflichen Stimmabgabe gebrauch und Genf hat eine der höchsten Stimmbeteiligungen landesweit. Diesem positiven Trend soll mit der Möglichkeit der elektronischen Stimmabgabe weiter Vorschub geleistet werden.
- Laut dem Bundesamt für Statistik haben 55% der Schweizer einen Internetzugang, Tendenz steigend. Somit stellt die Infrastruktur für die Bürger kein grosses Problem dar.
- Für die ungefähr 580000 Auslandschweizer und für Menschen mit eingeschränkter Mobilität würde das neue System wesentliche Erleichterungen schaffen.
- Der öffentliche Dienst sollte sich den wandelnden Lebensgewohnheiten der Bevölkerung anpassen.
- Die direkte Demokratie eignet sich gut für eine elektronische Lösung, da Wahlen und Abstimmungen häufig sind und die Bürger zahlreiche Rechte haben (Referendum, Initiative)
- Genf ist auch Sitz einiger wichtiger IT - Organisationen und daher prädestiniert, die neuen Technologien auch zu fördern.

Die Projektverantwortlichen haben sich folgende, zwingende Regeln definiert, die eine elektronische Abstimmungslösung erfüllen muss:

1. Elektronisch abgegebene Stimmen dürfen weder abgefangen noch verändert oder umgeleitet werden können.
2. Niemand hat Zugang zur elektronischen Urne vor der offiziellen Öffnung.
3. Nur registrierte Stimmberechtigte haben Zugang zum System.
4. Jeder Stimmberechtigte kann nur einmal abstimmen.

¹⁹ Vgl. <http://www.admin.ch/ch/d/egov/ve/index.html>

²⁰ Vgl. http://www.geneve.ch/chancellerie/e-government/doc/pre_projet_eVoting_eng.pdf



5. Die Geheimhaltung der Stimme ist gewährleistet. Es besteht zu keinem Zeitpunkt eine Verbindung zwischen dem Stimmberechtigten und seiner Stimme.
6. Die eVoting Seite muss alle Angriffe abwehren können.
7. Die Stimmberechtigten werden vor Diebstahl ihrer Identität geschützt.
8. Die Anzahl elektronisch verschickter Stimmzettel muss mit der Anzahl zurückgekommener elektronischer Stimmzettel übereinstimmen.
9. Es muss möglich sein, zu beweisen, dass ein bestimmter Stimmberechtigter per eVoting abgestimmt hat.
10. Das System darf keine Stimmen akzeptieren, die ausserhalb der Öffnungszeiten der elektronischen Urne abgegeben wurde.
11. Die Verantwortlichen können Leute bestimmen, die die Funktion des Systems überprüfen.

Mit folgenden Massnahmen werden die gemachten Vorgaben erfüllt:

- Die Urne wird von zwei Repräsentanten der politischen Parteien mit zwei Passwörtern «abgeschlossen». Zudem kann die elektronische Urne erst ab einem vorher bestimmten Zeitpunkt wieder geöffnet werden. Dieses Verfahren garantiert, dass beim Öffnen immer Politiker verschiedener Parteien anwesend sein müssen und damit die demokratische Kontrolle gewährleistet ist.
- Die politischen Repräsentanten schicken eine grosse Anzahl an Teststimmen in eine Testurne. Bei der Auswertung dieser Urne müssen die Stimmen mit den abgeschickten Teststimmen identisch sein, inhaltlich und quantitativ. So können Softwarefehler mit grosser Wahrscheinlichkeit ausgeschlossen werden.
- Auf dem Weg im Internet werden die Daten chiffriert.
- Dem elektronischen Wahlzettel wird ein für jeden Benutzer ein anderes Bild angehängt. Dieses Bild gibt einen weiteren Schutz vor Hackern und gibt dem User die Sicherheit, dass er mit der offiziellen Internetseite verbunden ist.
- Die Internetseite ist zertifiziert. Die Zertifikate können jederzeit von den Stimmberechtigten eingesehen werden.
- Die Identität der Stimmenden und die Stimmen werden an verschiedenen Orten gespeichert.
- Vor dem Öffnen der elektronischen Urne, wird diese mit Hilfe eines Algorithmus «geschüttelt». Es wird so verunmöglicht, einen Zusammenhang zwischen den Stimmzetteln und der Reihenfolge bei deren Eingang herzustellen.

Die in Genf verwendete Lösung braucht keine speziellen Komponenten am Computer des Users. Dem Stimmmaterial wird zusätzlich einfach eine persönliche Identifikationsnummer beigefügt. Diese Nummer wechselt bei jeder Abstimmung und wird zur Identifikation der Stimmberechtigten auf dem Server gebraucht.

Die Abstimmung über das Internet ist in vier Phasen aufgeteilt:

1. Der User muss sich mit einem ersten, persönlichen, 16-stelligen Code anmelden. Die Chance eine Nummer durch ausprobieren zu finden, liegt bei eins zu fünf Milliarden. Dem identifizierten Wähler wird ein elektronischer Stimmzettel zugeschickt.
2. Der Benutzer stimmt ab.



3. Das System verlangt eine Bestätigung der Wahl. Der User muss nun seine Identität mit seinem Geburtsdatum, seinem Heimatort und einem zweiten Sicherheitscode bestätigen.
4. Das System bestätigt den Eingang der Stimme mit Eingangsdatum und -zeit.

Am Sonntag, 19.01.2003 konnten die Bürger der Genfer Gemeinde Anières, als erste weltweit, an einer Abstimmung über das Internet teilnehmen. Von den 741 Stimmberechtigten, die an die Urne gingen, machten 323 (43,7%) vom neuen Angebot Gebrauch. Die Stimmbeteiligung lag bei hohen 63,77%. Bisher nahmen ungefähr 50% der stimmberechtigten Einwohner von Anières an kommunalen Abstimmungen teil. Auch aus technischer Sicht war der Versuch ein Erfolg: Ein beauftragtes Unternehmen hat vergebens versucht, in den Server der Staatskanzlei einzudringen. Den einzigen Zwischenfall verursachte eine Schaltuhr, die den Server zu früh vom Netz nahm. Das Problem konnte aber schnell behoben werden. Das Auszählen der Stimmen fand unter Aufsicht von Vertretern der Parteien und der Bundeskanzlei statt und dauerte nur 73 Sekunden. Die Verantwortlichen sind nun daran, den Versuch auszuwerten und rechnen damit, bald weitere elektronische Abstimmungen durchführen zu können.²¹

3.2.2 Das Neuenburger Pilotprojekt²²

Der Kanton Neuenburg hat schon bei Projektbeginn beschlossen, dass er die meisten Leistungen, die mit dem vote électronique zusammenhängen von Anfang an zur Verfügung stellen will. Folgende elektronische Möglichkeiten zur Ausübung der politischen Rechte sollen Angeboten werden:

- Die elektronische Stimmgabe bei Abstimmungen und Wahlen auf Gemeinde-, Kantons-, und Bundesebene;
- Die elektronische Unterzeichnung von Initiativen und Referenden auf Gemeinde- und Kantonebene.

Der Kanton Neuenburg hat den Vorteil, dass er mit seinen 62 Gemeinden im Informatikbereich sehr eng zusammenarbeitet:

- 55 Gemeinden sind im Neuenburger Informatiknetz zusammengeschlossen. Dadurch können die administrativen Tätigkeiten für 98% der Bevölkerung online abgewickelt werden.
- 58 Gemeinden benutzen die vom Informatikdienst der Stadt Neuenburg betreuten Anwendungen.
- Der Kanton Neuenburg speichert schon heute die Personaldateien auf einer zentralen Datenbank, die jeden Abend mit den neusten Informationen aus den Gemeinden aktualisiert wird.
- Die drei wichtigsten Informatikzentren des Kantons haben beschlossen, gemeinsam einen einzigen Guichet virtuel für die ganze Bevölkerung zu schaffen.

²¹ Vgl. http://www.geneve.ch/chancellerie/e-government/doc/Rapport_Final9.pdf und <http://www.swissinfo.ch/sde/Swissinfo.html?siteSect=105&sid=1575998>

²² Vgl. http://www.admin.ch/ch/d/egov/ve/projekte/projekte_neuenburg.html und <http://www.ne.ch/neat/site/jsp/rubrique/rubrique.jsp?styleType=marron&DocId=7573>



Diese gute Koordination senkt die Projektkosten erheblich und beschleunigt den Ablauf.

Die Sicherheitsmassnahmen des Projekts decken sich im Grossen und Ganzen mit denen des Kantons Genf. Zu erwähnen ist einzig, dass die Neuenburger für den Erhalt ihres Zugangscodes ein amtliches Gesuch einreichen müssen. Weiter ist ein Zusammenarbeitsvertrag mit den Behörden zu unterzeichnen, der die Rechte und Pflichten beider Parteien festlegt.

Die Aufbauphase des Projekts dauert voraussichtlich noch bis Ende Juni 2003. Im 2. Semester 2003 soll das System auf seine Tauglichkeit geprüft werden. 2004 soll es dann für die Bürger von Neuenburg möglich sein, die neue Dienstleistung in Anspruch zu nehmen.

3.2.3 Das Zürcher Pilotprojekt²³

Von den drei kantonalen vote électronique Projekten ist das des Kantons Zürich noch am wenigsten weit fortgeschritten. Das Hauptproblem liegt bei der ausgeprägt dezentralen Organisation des Kantons. Zudem sind die EDV-Systeme der Kommunen nicht aufeinander abgestimmt und die Einwohner- und Stimmregister werden auf unterschiedlichste Weise geführt. Die erste Aufgabe ist somit der Aufbau eines kantonalen Stimmregisters. Dieses soll in Form einer Sicht auf die gemeindeeigenen Datenbanken, die auf Kantonsebene zusammengefügt sind, verwirklicht werden.

Für die Verantwortlichen im Kanton Zürich kommt als Abstimmungssystem nicht nur das Internet in Frage. In Betracht gezogen werden auch Lösungen mit Mobiltelefonen, TV und möglichen weiteren Übermittlungsgeräten.

Die Evaluationsphase der Unternehmen, die sich für die Erstellung einer eVoting - Lösung (mit zentralem Stimmregister) beworben haben, wurde im Mai 2003 abgeschlossen. Sobald der Zuschlag erfolgt ist, werden die Zürcher Verantwortlichen die Details der technischen Durchführung bekannt geben. Ein erster Test soll das System im Dezember 2003 bei den Studienratswahlen an der Universität Zürich durchlaufen. Die Durchführung der ersten kantonalen Abstimmung ist für den Herbst 2004 geplant.²⁴

3.2.4 Einsatzmöglichkeiten der digitalen Signatur

Die Sicherheit beim Genfer eVoting Projekt ist zweifelsfrei auch ohne den Einsatz der digitalen Signatur gewährleistet. Diese würde aber eine wesentliche Vereinfachung des Ablaufes schaffen, da nur noch zum Zugreifen auf den Server ein Sicherheitscode gebraucht würde. Das Eingeben des Geburtsdatums, des Heimatortes und eines PIN vor dem Abschicken des elektronischen Stimmzettels würden überflüssig. Auch im Kanton Neuenburg wäre das Abstimmen und Wählen ohne eine elektronische Unterschrift möglich. Das Sammeln von Unterschriften für Referenden und Initiativen würde jedoch erst bei der Einführung der digitalen Signatur möglich.

²³ Vgl. http://www.admin.ch/ch/d/egov/ve/projekte/projekte_zuerich.html

²⁴ Laut eMail - Auskunft von Susanne Sorg-Keller, Chefin Kommunikationsabteilung des Regierungsrats des Kantons Zürich



3.3 TaxMe Online²⁵

3.3.1 Vorstellung des Projektes

Seit Januar 2003 haben die Steuerpflichtigen des Kantons Bern die Möglichkeit, ihre Steuererklärung online über das Internet zu verfassen und einzureichen. Das Programm wird auf den Servern des Kantons Bern zur Verfügung gestellt. Es ist daher unabhängig vom jeweils verwendeten Betriebssystem und verlangt keine Installation auf dem PC des Users. Die erhobenen Daten werden der Steuerverwaltung über eine sichere Verbindung (128 Bit Verschlüsselung) übermittelt. Dort können die Steuerdaten direkt in die Veranlagungssysteme übernommen werden, was eine kürzere Durchlaufzeit der Steuererklärungen möglich macht. Dieser Zeitgewinn wird dringend benötigt, da der Kanton Bern mit dem neu eingeführten, einjährigen Veranlagungssystem einen wesentlichen Mehraufwand zu bewältigen hat.

Die online Erfassung der Steuerdaten läuft folgendermassen ab:

1. Der Benutzername und das Passwort werden den Steuerpflichtigen mit der schriftlichen Steuererklärung zugeschickt.
2. Die Daten können mit TaxMe Online einfach erfasst werden.
3. Die Freigabeerklärung wird ausgedruckt, unterschrieben und zusammen mit den Belegen an die Steuerverwaltung geschickt.
4. Die Verwaltung kann die Daten nach Erhalt der Freigabeerklärung verarbeiten.

Die Vorteile von TaxMe Online können wie folgt zusammengefasst werden:

- Es werden keine Daten auf dem PC des Users gespeichert.
- Die Navigation im Programm ist dank seiner Baumstruktur übersichtlich.
- Die Daten können orts- und zeitunabhängig erfasst werden.
- Während des Ausfüllens steht dem User die Wegleitung stets zur Verfügung.
- Noch offene Eingaben sind leicht zu erkennen.
- Ein Datenverlust ist fast auszuschliessen, da die Daten laufend gespeichert werden.
- Angaben, die der Steuerverwaltung bekannt sind, werden direkt angezeigt und müssen nicht neu eingegeben werden.
- Die Berechnungen werden vom System automatisch ausgeführt.
- Eingegebene Daten stehen dem Steuerpflichtigen bei der nächsten Erfassung wieder zur Verfügung.

3.3.2 Einsatzmöglichkeiten der digitalen Signatur

Die digitale Signatur würde TaxMe Online noch perfektionieren. Die Freigabeerklärung und die einzureichenden Belege könnten ebenfalls auf elektronischem Weg übermittelt werden.

²⁵ Vgl. <http://www.sv.fin.be.ch/taxme/2002/index/on-taxmeonline.htm>



4 Beispiele aus dem Dienstleistungssektor

Im Folgenden wird die Bedeutung der digitalen Signatur für den Dienstleistungssektor anhand konkreter Beispiele aufgezeigt. Einleitend zu diesem Punkt wird kurz auf die Bedeutung für die Wirtschaft im allgemeinen eingegangen.

4.1 Bedeutung für die Wirtschaft²⁶

In den letzten Jahren ging man davon aus, dass die rechtliche Anerkennung der digitalen Signatur eine entscheidende Voraussetzung für die gedeihliche Entwicklung des elektronischen Handels sei. Nur durch diese Anerkennung könne das notwendige Vertrauen für eine breite Akzeptanz des elektronischen Handels entstehen. Die Realität stellt diese Annahme in Frage. Die letzten paar Jahre zeigten, dass sich der elektronische Handel – mindestens in bestimmten Kategorien – auch ohne explizite Anerkennung der digitalen Signatur mit sehr grossen Wachstumsraten entwickelt. Die traditionellen Akteure wie Banken, Kreditkartenunternehmen und der online-Handel haben offensichtlich ausreichend sichere Verfahren für den Verkauf und die Bezahlung bereitstellen können, wie beispielsweise SET²⁷ oder eCash²⁸. In den beiden Fällen werden zwar auch digitale Signaturen verwendet, ihr Einsatz spielt sich jedoch im Hintergrund ab, und die elektronischen Schlüssel beziehen sich nicht auf die beteiligten Personen. Die Verbindlichkeit der Verfahren ist über Verträge zwischen den Teilnehmern und der zentralen Organisation geregelt. Die Sicherheit des Lieferanten wird durch (eine Art von) Direktzahlung erreicht.

In der Praxis können u.U. auch sehr einfache Verfahren den Beteiligten eine ausreichende Sicherheit gewähren. Wenn sich beispielsweise der Besteller mit der Nummer der Postcheque-Karte identifiziert und die Post dafür sorgt, dass die Auslieferung der Ware nur an eine zum Karten-Inhaber passende Adresse geschieht, so ist für eine bestimmte Art von Geschäften wohl schon eine genügend grosse Sicherheit erreicht.

4.2 Banken

Der Datenverkehr zwischen einer Bank und einem Kunden ist fast immer persönlich und vertraulich. Diese Tatsache schafft sehr viele Anwendungsgebiete der digitalen Signatur. Beispielsweise beim Telebanking fürs Einloggen, für die Abwicklung internationaler Handelsfinanzierungen im Trade-Finance, beim Einsatz von Kreditkarten im Online-Shopping oder im Schreibverkehr zwischen der Bank und dem Kunden.

Denkbar ist auch ein elektronischer «Bank-Safe». Der Kunde deponiert dort nicht mehr wie im traditionellen Bank-Safe seine Wertpapiere und Wertsachen, sondern schützenswerte, elektronische Daten. Dies sind vielleicht Firmendaten von kleinen und mittleren Unternehmen, welche diese fortan verschlüsselt aufbewahren können. Eine weitere Idee wäre die Einrichtung einer elektronischen «Werkbank». Sie könnte dem Bank-Kunden dazu dienen, die Kontakte mit seiner Kundschaft darüber abzuwickeln, d.h. darüber verschlüsselte und signierte Dokumente zu verschicken, zu

²⁶ Vgl. <http://www.ofj.admin.ch/themen/ri-ir/digsig/intro-d.htm>

²⁷ SET = Secure Electronic Transactions

²⁸ eCash = digitales Geld



archivieren und gegebenenfalls durch die Bank beglaubigen zu lassen. Denkbar wäre auch, dass zwei Parteien unter Ausschluss von Drittpersonen über die «Werkbank» an bestimmten Dokumenten arbeiten und über Inhalte verhandeln könnten.²⁹

Zusammenfassend kann man sagen, dass die Banken überall dort die digitale Signatur einsetzen könnten, wo die Authentizität und die Integrität des Kunden bei elektronischen Dokumenten und Geschäften gefordert ist. Wie ein solches Geschäft mit Hilfe der digitalen Signatur abgewickelt werden könnte, wird im nächsten Punkt erläutert.

4.2.1 Hypothek per E-Mail

Ein Traum vieler Menschen ist das Eigenheim. Selten ist es aber möglich, das Haus oder die Wohnung vollständig aus eigener Kraft zu finanzieren. Die Lösung ist schnell gefunden: die Bank muss einem mit einer Hypothek unter die Arme greifen.

4.2.1.1 *Ablauf heute*

Hat man sich für eine Hypothek entschieden, trifft man sich mit der Bank. Dabei werden die Einzelheiten des Vertrages ausgearbeitet, d.h. die Sicherheiten des Antragstellers werden abgeklärt, die Höhe des Kredites wird festgesetzt, die Finanzierungsvarianten ermittelt, Laufzeit und Amortisation besprochen. Sobald sich beide Parteien einig geworden sind, kann der Vertrag unterzeichnet werden und ist somit rechtsgültig. Die Bank kann sicher sein, dass die Angaben korrekt sind und vom Antragsteller selbst stammen und dieser auch die Verantwortung dafür trägt. Anschliessend wird dem Kunden das Geld überwiesen und er kann frei darüber verfügen.

4.2.1.2 *Ablauf mit Hilfe der digitalen Signatur*

Mit der digitalen Signatur könnte das oben beschriebene Verfahren deutlich abgekürzt und vereinfacht werden. Die Beratung und Ausarbeitung des Vertrages könnte bequem per E-Mail abgewickelt werden. Der Kunde müsste somit nicht persönlich bei der Bank vorsprechen und den Vertrag unterzeichnen. Ort und Zeit spielen so keine Rolle mehr. Die Authentizität und die Integrität der elektronischen Korrespondenz wäre dank der digitalen Signatur jeder Zeit sichergestellt.

Dies verdeutlicht, wie effizient und bequem solche Bankgeschäfte zukünftig abgewickelt werden könnten.

²⁹ Vgl. <http://emagazine.credit-suisse.com/article/index.cfm?aoid=3995>



4.3 Versicherungen

Versicherungen bieten immer mehr Dienstleistungen an. Dabei steigt auch laufend die Anzahl abgeschlossener Verträge und eine grosse Menge von wichtiger Korrespondenz muss abgewickelt werden.

Für den Abschluss einer Versicherung wird man oft von einem Versicherungsagenten besucht, der die Ausarbeitung des Vertrages vornimmt. Dabei werden wichtige und vertrauliche Daten ausgetauscht. Demzufolge ist es notwendig, dass die Angaben korrekt sind und auch von den entsprechenden Personen stammen, bzw. verarbeitet werden.

Mit der Anwendung der digitalen Signatur wäre es möglich, Verhandlungen und Verträge per E-Mail abzuwickeln. Die Authentizität und Integrität wäre sichergestellt.

Offensichtlich könnte auch bei den Versicherungen die digitale Signatur für die Verhandlung und Abschliessung von Verträgen effizient und kostensparend ihre Anwendung finden.

4.4 Treuhand-Unternehmen

Treuhand-Unternehmen bieten eine Reihe von Dienstleistungen an, wie beispielsweise Revisionen, Expertisen, Steuerberatung, Unternehmens-Beratung, wirtschaftsjuristische Beratung, Buchhaltung, Immobilengeschäfte, etc.

Bei solchen Dienstleistungen werden sehr viele Dokumente zwischen dem Treuhand-Unternehmen und den Kunden ausgetauscht. Wie bei den Versicherungen und den Banken könnte hier die digitale Signatur die Kommunikation stark vereinfachen. Dank dem digitalen Siegel könnten Verträge und wichtige Dokumente schnell und einfach per E-Mail zugestellt werden. Die Authentizität und die Integrität der Dokumente wäre jeder Zeit gewährleistet.

4.5 Bedeutung für den Dienstleistungssektor

Die drei Beispiele aus dem Dienstleistungssektor verdeutlichen, welches Anwendung-Potenzial der digitalen Signatur in diesem dritten Sektor schlummert. In keinem anderen Sektor werden eine derart grosse Anzahl von Dokumenten auf dem normalen Wege ausgetauscht, weil die Authentizität und Integrität sichergestellt sein muss. Dies verursacht grosse Wartezeiten und hohe Kosten. Durch die Anwendung der digitalen Signatur könnte ein Grossteil dieser Korrespondenz deutlich beschleunigt und rationalisiert werden. Einsatzmöglichkeiten der digitalen Signatur gäbe es im Dienstleistungssektor sicher genug.



5 Vergleich der Projekte aus den beiden Sektoren

Uns scheint es am Sinnvollsten den Vergleich der Projekte in Form einer Matrix mit anschliessendem Kommentar zu präsentieren.

Kriterien Projekte	Wichtigkeit*	Fortge- schrittenheit	Ausbaumö- glichkeiten	Zielgruppe	wichtigste Projektziele
eGuichet	***	**	***	alle Bürger	Informationsplatt- form
Genf	*	**	**	Stimmberechtigte	Zus. Möglichkeiten zur Wahrnehmung politischer Rechte
Neuchâtel	***	*	***	Stimmberechtigte	
Zürich	*	*	***	Stimmberechtigte	
TaxMe	*	***	*	Steuerpflichtige	Effizienzsteigerung
Banken	*	**	*	Kunden	Dienstleistungs- erweiterung
Versicherungen	*	**	*	Kunden	
Treuhandfirmen	*	**	*	Kunden	

Tabelle 1: Vergleichsmatrix

* Unter Wichtigkeit wird die Unabdingbarkeit der digitalen Signatur für das entsprechende Projekt verstanden.

Symbolerklärung:

Wichtigkeit

*** sehr wichtig

** wichtig

* unwichtig

Fortgeschrittenheit

*** fertiggestellt

** fortgeschritten

* in Entwicklung

Ausbaumöglichkeiten

*** gut ausbaubar

** ausbaubar

* schlecht ausbaubar

Für die Projekte eGuichet und Neuchâtel ist die digitale Signatur für eine 100%-tige Ausführung unabdingbar. Beim virtuellen Schalter werden Dokumente ausgestellt, bei denen die Authentizität und Integrität unbedingt sichergestellt sein muss. Im Kt. Neuenburg ist die digitale Signatur notwendig, da Unterschriften für Initiativen und Referenden sonst nicht übers Internet gesammelt werden könnten. Die weiteren Projekte funktionieren auch ohne die digitale Signatur, dessen Anwendung lediglich eine Vereinfachung der Abläufe bringen würde.

Auffallend ist, dass die digitale Signatur im Dienstleistungssektor vergleichsweise bis jetzt unwichtig ist.

Wir betrachten das eGuichet-Projekt als fortgeschritten, weil ungefähr die Hälfte der Informationen bereits auf dem Internet einsatzbereit und abrufbar ist. Das Projekt ist noch stark ausbaufähig, denn bis alle Gemeinden angeschlossen sind und auch komplexe Dienstleistungen (z.B. Ausstellung eines Passes) angeboten werden, wird es noch eine gewisse Zeit dauern. In Genf wurde bis jetzt ein erster Versuch mit



eVoting in einer Gemeinde durchgeführt. Geplant ist, das Projekt auf den gesamten Kt. Genf auszudehnen. In Neuenburg und Zürich stecken die eGovernment-Projekte noch in den Kinderschuhen. Bis die volle Funktionsfähigkeit aufgebaut ist, braucht es noch eine gewisse Zeit und viel Arbeitseinsatz. Die elektronische Erhebung der Steuerdaten im Kt. Bern ist schon voll funktionsfähig. Für die nächsten Steuerperioden kann das System nur noch geringfügig verbessert werden.

Die bereits bestehenden Angebote im Dienstleistungssektor sind voll funktionsfähig. Mit der Einführung der digitalen Signatur könnte das bestehende Dienstleistungsangebot mit der bestehenden Infrastruktur noch erweitert werden.

Im Vergleich zum öffentlichen Sektor ist der Dienstleistungssektor für die Anwendung der digitalen Signatur bereit. Die Vorhaben der öffentlichen Hand bedürfen noch einiger Anpassungen und Weiterentwicklungen.

Die Ausrichtung der Projekte beider Sektoren zielt auf die Kunden ab. Die Klienten des öffentlichen Sektors sind Steuerpflichtige, Stimmbürger und alle Personen, die mit den Behörden den Kontakt suchen.

Ziel in beiden Sektoren ist es, das Dienstleistungsangebot auszubauen, zu vereinfachen und die Effizienz bei der Abwicklung der Aufträge zu steigern.

6 Fazit und Ausblick

Zu Beginn unserer Arbeit waren wir der Ansicht, dass die digitale Signatur in der Schweiz schon viel weiter verbreitet ist und ihre Anwendung findet. Wir mussten aber sehr bald feststellen, dass dem nicht so ist. Als Ursache betrachten wir eindeutig die fehlende Gleichstellung der digitalen Signatur mit der handschriftlichen Unterschrift im Schweizer Obligationenrecht. Aus diesen Gründen fiel es uns dementsprechend schwer, praktische Beispiele aus dem Dienstleistungssektor zu finden. Alle betrachteten Organisationen im Dienstleistungssektor und im öffentlichen Sektor sind stark bemüht ihre Produkte den neuen Technologien so anzupassen, dass die Einführung und Anwendung der digitalen Signatur keine grösseren Investitionen und Anpassungen mehr erfordern werden.

Voraussichtlich wird per 01.01.2005 die rechtliche Gleichstellung der digitalen Signatur mit der handschriftlichen Unterschrift erfolgen. Damit wird die Voraussetzung geschaffen, dass Institutionen diese neue Technologie als wertschöpfende Komponente in ihre Kundenbeziehungen einbringen können. Sofern die Kunden der modernen Authentifizierungsmethode vertrauen, steht unserer Ansicht nach dem Erfolg der digitalen Signatur nichts mehr im Weg.



Literaturverzeichnis

Bundeskanzlei: Guichet virtuel (2003-03),

<http://www.admin.ch/ch/d/egov/gv/index.html> (2003-05-18, 16:14 MEZ)

- Vote électronique (2002-12), <http://www.admin.ch/ch/d/egov/ve/index.html> (2003-05-18, 16:35 MEZ)

Bürge U.: Digitale Signatur und Recht - Voraussetzungen, Stand und Aussichten der rechtlichen Anerkennung in der Schweiz (2000-06-23),

<http://www.ofj.admin.ch/themen/ri-ir/digsig/intro-d.htm> (2003-04-23, 10:05 MEZ)

Bürki E.: Digitale Unterschrift: Bald Standard im E-Business (2001-07-25),

<http://emagazine.credit-suisse.com/article/index.cfm?aid=3995> (2003-04-23, 10:30 MEZ)

Gremlich R., Zumsteg F.: Public Key Infrastructure, Kryptographie und digitale Signaturen (2002-05-29),

http://www.ifi.unizh.ch/ikm/Vorlesungen/ebusiness02/Arbeiten/Public%20Key%20Infrastructure_Seminararbeit_SS02.pdf (2003-04-23, 09:15 MEZ)

Hensler, R.: The Geneva Internet voting system (2003-01-15),

http://www.geneve.ch/chancellerie/e-government/doc/pre_projet_eVoting_eng.pdf (2003-05-18, 16:41 MEZ)

- L'application genevoise de vote par Internet (2003-01-15),

http://www.geneve.ch/chancellerie/e-government/doc/pres_projet_eVoting_fra.pdf (2003-05-18, 16:44 MEZ)

Muralt Müller, H.: www.ch.ch - ein Projekt von Bund, Kantonen und Gemeinden

(2003-02-10), http://www.admin.ch/ch/d/egov/gv/kurzportraet/projekt_d.pdf (2003-05-18, 16:28 MEZ)

République et Canton de Genève: Résultats du vote du 19 janvier 2003 à Anières (GE),

http://www.geneve.ch/chancellerie/e-government/doc/Rapport_Final9.pdf (2003-05-18, 16:56 MEZ)

République et Canton de Neuchâtel: Information générale sur les projets Neuchâtelois de gouvernement électronique (eGovernment) (2002-11-01),

<http://www.ne.ch/neat/site/jsp/rubrique/rubrique.jsp?StyleType=marron&DocId=7573> (2003-05-18, 17:24 MEZ)

Schweizerischer Bundesrat: Botschaft zum Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (Zert ES) (2001-07-03),

<http://www.admin.ch/ch/d/ff/2001/5679.pdf> (2003-05-25, 21:47 MEZ)

Steuerverwaltung des Kantons Bern: TaxMe Online,

<http://www.sv.fin.be.ch/taxme/2002/index/on-taxmeonline.htm> (2003-05-18, 17:34 MEZ)



swissinfo: Erfolgreiches eVoting (2003-01-19),

<http://www.swissinfo.ch/sde/Swissinfo.html?siteSect=105&sid=1575998> (2003-05-18, 17:02 MEZ)

SYSTOR AG: Rechtsgültige Verträge; Die digitale Signatur setzt sich durch,

http://www.systor.com/dl_know_bizpub_digitale_signatur.pdf (2003-04-23, 09:50 MEZ)

Theisen, Manuel R.: Wissenschaftliches Arbeiten 11. Auflage, Verlag Franz Vahlen München, 2002



Quellenverzeichnis

- Verordnung über Dienste der elektronischen Zertifizierung (Zertifizierungsdienstverordnung, ZertDV) vom 12. April 2000 (Stand am 23. Mai 2000), verfügbar unter <http://www.admin.ch/ch/d/sr/7/784.103.de.pdf>
- Entwurf Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (Zert ES), verfügbar unter <http://www.admin.ch/ch/d/ff/2001/5716.pdf>
- Schweizer Obligationenrecht vom 30. März 1911