HTW Chur
Hochschule für Technik und Wirtschaft

Fachhochschule Ostschweiz
University of Applied Sciences

Churer Schriften
zur Informationswissenschaft
Herausgegeben von Josef Herget und Sonja Hierl

Arbeitsbereich
Informationswissenschaft

Schrift 5

Realisierungsmöglichkeiten einer Zertifizierungsstelle für digitale Zertifikate in der Schweiz

Nina Braschler

Chur 2005

Churer Schriften zur Informationswissenschaft
Herausgegeben von Josef Herget und Sonja Hierl
Schrift 5

Realisierungsmöglichkeiten einer Zertifizierungsstelle für digitale Zertifikate in der Schweiz

Nina Braschler

Verlag: Arbeitsbereich Informationswissenschaft
ISSN: 1660-945X
Chur, Februar 2005

Keywords

Digitale Unterschrift, Hashfunktion, PGP, Schlüssel, Verschlüsselung, Zertifizierung, Zertifikat, Zertifizierungsstelle Schweiz

Abstract

Anerkannte Zertifizierungsstellen generieren und verwalten öffentliche Schlüssel oder Zertifikate, welche zur Überprüfung verbindlicher, elektronischer Signaturen von Dritten benötigt werden.

In dieser Arbeit werden mögliche Umsetzungen einer solchen Zertifizierungsstelle für digitale Zertifikate in der Schweiz dargestellt. Dazu bleibt abzuklären, warum die Schweiz bis zum heutigen Zeitpunkt ohne anerkannte Zertifizierungsstelle dasteht und wo für den digitalen Signatureinsatz potentielle Bereiche gesehen werden. Aus strategischer Sicht steht die Frage im Vordergrund, wie eine anerkannte Zertifizierungsstelle konkret realisiert werden kann.

Bevor auf die Beantwortung der Fragen eingegangen wird, führt der erste Teil der Arbeit in die Thematik der digitalen Signatur und der Zertifizierungsstelle ein. Anschliessend werden diverse Einsatzmöglichkeiten der digitalen Signatur dargestellt und der Zertifikatmarkt wird einer Analyse unterzogen.

Darauf aufbauend werden nach einer Darstellung der aktuellen Situation bezüglich Zertifizierungsstellen in der Schweiz, fünf Strategien formuliert, welche in der Folge kritisch gewürdigt werden. Zum Schluss gibt die Handlungsempfehlung darüber Auskunft, welche Strategie zum jetzigen Zeitpunkt am sinnvollsten erscheint.

Inhaltsverzeichnis

Seite

1. Executive Summary

Mit der digitalen Signatur können Dokumente elektronisch unterschrieben werden. Da bei der vollständig elektronischen Geschäftsabwicklung an einem Dokument nicht ersichtlich ist, ob dieses während der Übermittlung verändert worden ist und ob es tatsächlich vom Geschäftspartner stammt, bilden die Identifikation des Absenders sowie die Wahrung der Datenintegrität die bedeutsamsten Voraussetzungen für sichere digitale Transaktionen. Für die Authentizität eines Absenders bürgt eine Zertifizierungsstelle, welche digitale Zertifikate vertreibt. Mit Hilfe der Zertifikate können die digitalen Signaturen, welche zuvor vom Absender mit dem privaten Schlüssel signiert worden sind, überprüft werden und daraus kann auf einen eindeutigen Urheber geschlossen werden. Die Zertifizierungsstelle muss, damit Zertifikate für die verbindliche elektronische Signatur verwendet werden können, den in den gesetzlichen Grundlagen verankerten Voraussetzungen entsprechen.

Für die Inbetriebnahme einer solchen anerkannten Zertifizierungsstelle ergeben sich mehrere Probleme: Erstens bestehen zum jetzigen Zeitpunkt für die Anwendung digitaler Signaturen kaum geeignete Applikationen. Zweitens ist die elektronische Unterschrift trotz potentieller Einsatzgebiete unter den Anwendern nicht bekannt. Drittens sind die gesetzlichen Voraussetzungen in mancher Hinsicht sehr vage formuliert und teilweise nicht in praktikabler Weise umsetzbar.

Bezüglich der konkreten Realisierung einer anerkannten Zertifizierungsstelle in der Schweiz existiert im Moment hauptsächlich die Möglichkeit, eine Zertifizierungsinstanz einzurichten, welche wohl den gesetzlichen Anforderungen entsprechen würde, nicht aber Zertifikate für die ganze Nation ausstellen kann. Das heisst, dass die Zertifizierungsstelle im kleinen Rahmen aufgebaut wird, wobei aber eine Erweiterung nicht auszuschliessen ist.

Um die Zertifizierungsstelle unter Berücksichtigung dieser Einwände finanziell und praktisch umzusetzen, ist entweder die Bildung eines Wirtschaftskonsortiums, die Fusion bestehender privater Zertifizierungsstellen, die Auslagerung der Zertifizierungsstelle ins Ausland, die Beteiligung des Bundes an einer privaten Zertifizierungsstelle oder die Errichtung einer staatlichen Zertifizierungsstelle vorstellbar. Obwohl prinzipiell alle Eventualitäten umsetzbar sind, sofern ein geeigneter Business-Case für die digitale Signatur geschaffen worden ist, darf eine Zusammenarbeit zwischen Wirtschaft und Staat als beste Strategie angesehen werden, da so die Entwicklungen der digitalen Signatur sowohl im amtlichen als auch im privatwirtschaftlichen Umfeld gefördert werden. Zudem ergibt die Variante der Beteiligung des Bundes an einer privaten Zertifizierungsstelle für beide Seiten den geringsten Kostenaufwand, was die Attraktivität dieser Realisierungsmöglichkeit fördert.

2. Einleitung

E-Commerce, E-Business, E-Government – diese Begriffe zeigen, dass immer mehr Bereiche der Kommunikation elektronisch stattfinden und Transaktionen gänzlich ohne Papier geschehen. Der Wandel von auf Papier basierten hin zu digitalen Abläufen stellt im Zusammenhang mit Dokumenten, welche Schriftlichkeit erfordern, nicht nur neue Anforderungen an die Administration und Sicherheit, sondern insbesondere auch an die Unterschrift selbst.[1]

Während herkömmliche Geschäftsabwicklungen mit einer handschriftlichen Unterschrift ihre rechtliche Verbindlichkeit erlangen, ist es heute im Zuge der rasanten Entwicklungen in der Informations- und Kommunikationstechnologie möglich, Dokumente mit Hilfe der digitalen Signatur rechtsverbindlich zu unterschreiben. Die digitale Signatur soll dank moderner Verschlüsselungstechnologien, welche die Wahrung der Vertraulichkeit garantieren, den elektronischen Geschäftsverkehr für Anbieter und Verbraucher sicher gestalten.[2] Das Verfahren der digitalen Signatur besteht aus einem öffentlichen und einem privaten Schlüssel, wobei der öffentliche Schlüssel gleichzeitig Teil eines digitalen Zertifikates, welches den Absender eindeutig identifiziert und somit dessen Authentizität beglaubigt, ist.[3]

Für die Ausstellung von digitalen Zertifikaten ist eine Anbieterin von Zertifizierungsdiensten zuständig. Sie überprüft die Identität einer Person und zertifiziert diese in der Regel mit einem Dokument, welches das digitale Zertifikat (inklusive öffentlichem Schlüssel der zu zertifizierenden Person und weiteren Informationen über den Antragsteller) enthält.[4] Mit diesem „elektronischen Ausweis“ kann sich eine Person digital identifizieren, wodurch eine der wichtigsten Voraussetzungen für die digitale Signatur geschaffen ist. [5]

Zertifizierungsdiensteanbieterinnen nehmen im Zusammenhang mit der digitalen Signatur eine wichtige Rolle ein. Sie bilden eine Schnittstelle zwischen zwei Parteien und erfordern deshalb ein hohes Mass an Sicherheit, Zuverlässigkeit und Vertrauenswürdigkeit. Genauste Überprüfung der Personendaten, Beurteilung über die Korrektheit der angegebenen Daten, sowie das Ausstellen und Verwalten von digitalen Zertifikaten gehören zu den gängigen Aufgaben einer Anbieterin von Zertifizierungsdiensten.

Problemstellung und Zielsetzung

Damit Zertifizierungsstellen qualifizierte Zertifikate[6] anbieten können, werden sie von einer unabhängigen Anerkennungsstelle akkreditiert. Bis heute existiert in der Schweiz keine anerkannte Zertifizierungsdiensteanbieterin, welche digitale Zertifikate generieren kann. Wohl gibt es private Anbieter von Zertifizierungsdiensten, jedoch ist zu beachten, dass nicht beglaubigte Zertifizierungsstellen keine dem schweizerischen Zertifizierungsgesetz (ZertES) entsprechenden Zertifikate ausstellen können, was eine nationale und internationale Verwendung der Zertifikate für den Einsatz verbindlicher digitaler Signaturen verunmöglicht.

[1] Vgl. Bitzer, Brisch [1999] S. 1.

[2] Vgl. Bitzer, Brisch [1999] S. 2.

[3] Vgl. Dohmann et al. [2002] S. 70.

[4] Vgl. Hansen, Neumann [2001] S. 186.

[5] Vgl. Bertsch [2001] S. 3.

Trotz bestehender Gesetze scheinen die Entwicklungen der digitalen Signatur und die dazugehörigen Infrastrukturen in der Schweiz zu stagnieren.

In dieser Diplomarbeit bleibt abzuklären, aus welchen Gründen die Schweiz bis zum heutigen Zeitpunkt noch keine anerkannte Zertifizierungsstelle hat und wo die potentiellen Einsatzbereiche für die digitale Signatur gesehen werden. Ein erstes Ziel (Kapitel 5: Ökonomische Betrachtung einer Zertifizierungsstelle in der Schweiz) ist die Darstellung diverser Einsatzmöglichkeiten der digitalen Signatur, worin auch verschiedene Projekte aus dem Ausland beleuchtet werden, sowie die Analyse des schweizerischen Zertifikatmarktes. Darauf hin wird untersucht, warum in der Schweiz bis zum heutigen Zeitpunkt keine anerkannte Zertifizierungsstelle ihre Dienste anbietet.

Aus strategischer Sicht steht die Frage im Vordergrund, wie eine Zertifizierungsstelle realisiert werden kann. Ein weiteres Hauptziel dieser Arbeit ist deshalb in Kapitel 6 (Mögliche Strategien für eine Zertifizierungsstelle in der Schweiz) die Formulierung von mehreren Strategien und eine anschliessende kritische Beurteilung. Dabei wird auch aufgezeigt, mit welchen Kosten die Umsetzung der verschiedenen Strategien verbunden ist.

Bevor auf die Zertifizierungsdiensteanbieterinnen in der Schweiz und deren Situation eingegangen wird, soll in Kapitel 3 (Digitale Signaturen) ein Überblick über die digitale Signatur gegeben sowie deren Voraussetzungen aufgezeigt werden. Dabei wird der Begriff der digitalen Signatur, die dafür nötigen Technologien und Gesetze, sowie der Zusammenhang von digitalen Signaturen und Zertifikatsanbietern erläutert. Anschliessend wird in Kapitel 4 (Die Zertifizierungsstelle) die Zertifizierungsstelle mit Begriffsdefinitionen, den angebotenen Diensten sowie den gesetzlichen Grundlagen in der Schweiz abgehandelt, womit beabsichtigt ist, einige Problembereiche und Voraussetzungen für Zertifizierungsdienste aufzuzeigen.

Abgrenzung

Die Strategieentwicklung für die Gründung einer anerkannten Zertifizierungsdiensteanbieterin ist speziell auf die Schweiz ausgerichtet. Aspekte aus dem internationalen Umfeld werden in die Arbeit mit einfliessen, jedoch müssen ausländische Gegebenheiten an das nationale Umfeld angepasst werden.

Sofern nicht anders erwähnt, stützt sich diese Arbeit auf das schweizerische Rechtssystem. Eine Kompatibilität mit der Europäischen Signaturrichtlinie ist bereits in der schweizerischen Gesetzgebung integriert.

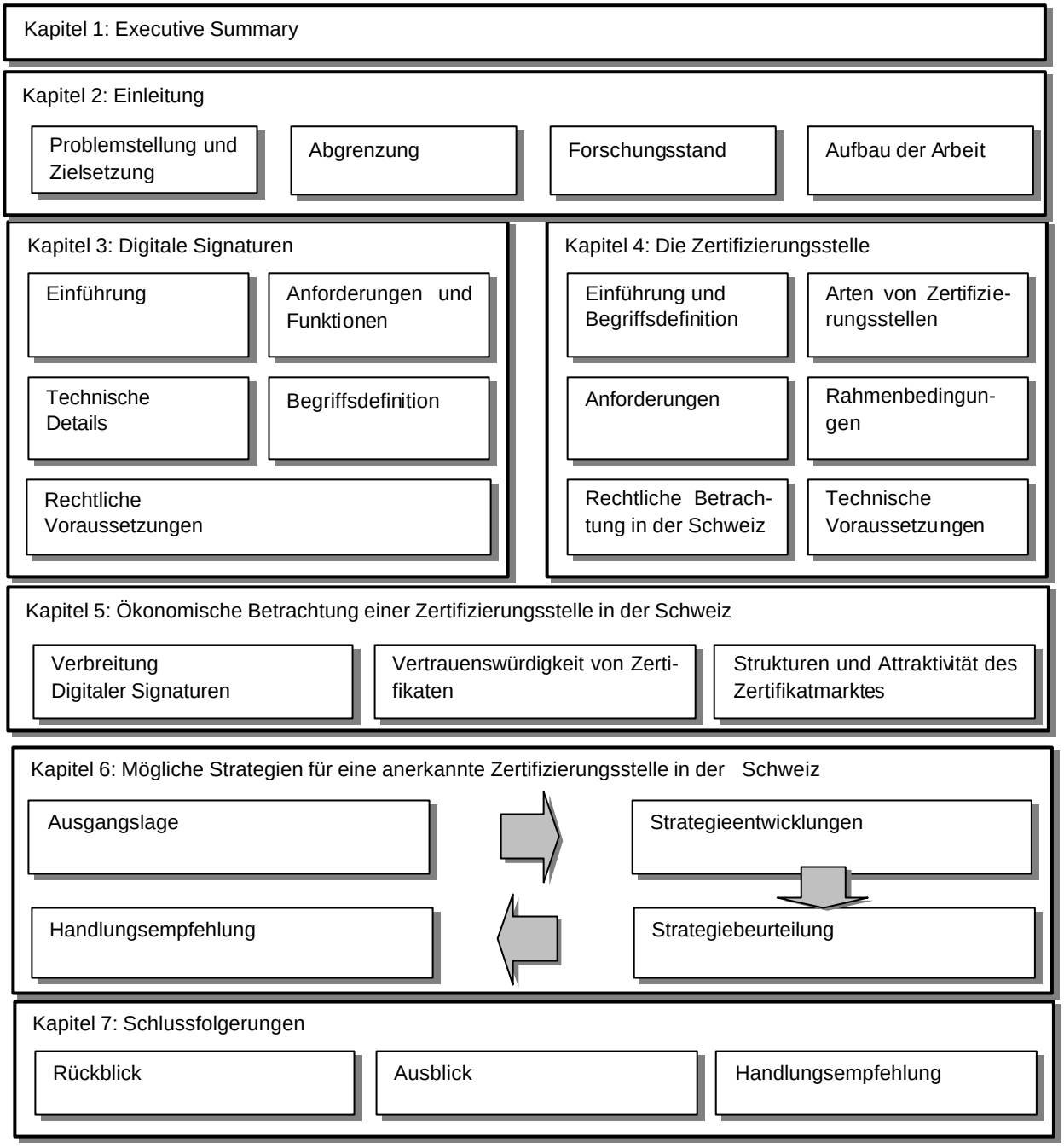
Forschungsstand

Da die digitale Signatur technisch durchaus umsetzbar ist, kann weitgehend auf vorhandene Literatur, welche bis in die zweite Hälfte der neunziger Jahre zurückreicht und immer noch aktuell ist, zurückgegriffen werden. Auch über Zertifizierungsstellen und Public Key Infrastruktur-Systeme als organisatorische Realisierung der digitalen Signatur wurde vieles geschrieben. Als um die letzte Jahrtausendwende in den einzelnen europäischen Ländern inklusive der Schweiz die Gesetzesentwürfe ausgearbeitet wurden, sind länderübergreifende Vergleiche der Gesetze, deren Bezug zur Europäischen Signaturrichtlinie und deren praktische Umsetzungsmöglichkeiten gemacht worden. Vielfach wurden einzelne Gesetze kom-

[6] Vgl. Ziff. 0 (Einführung und Begriffsdefinition).

mentiert und kritisch beurteilt. Obwohl die Signatur- und Zertifizierungsdienstgesetze gewisse Grundlagen zur Realisierung einer anerkannten Zertifizierungsstelle beitragen, wurden erst ansatzweise praktikable Strategien für eine konkrete Umsetzung erarbeitet. Ein Beispiel hierfür ist die Studie, welche im Auftrag des eidgenössischen Justiz- und Polizeidepartement im Jahre 2001 durchgeführt wurde und abklärt, ob die Schweiz einen amtlichen digitalen Ausweis braucht.[7] Darin werden zwei Strategien vorgeschlagen, wie eine anerkannte Zertifizierungsstelle in der Schweiz umgesetzt werden können, jedoch ist bis zum heutigen Zeitpunkt keiner der beiden Vorschläge realisiert worden.

Aufbau der Arbeit



[7] Vgl. Marzetta et al. [2001].

Abbildung 1: Aufbau der Arbeit

3. Digitale Signaturen

Dieses Kapitel erläutert sowohl die technischen als auch die rechtlichen Grundlagen digitaler Signaturen und bildet somit eine Basis für die folgenden Ausführungen der Arbeit.

Einführung

Digitale Signaturen sind das elektronische Pendant zur eigenhändigen Unterschrift. Sie schaffen die Möglichkeit, auf asymmetrischer Verschlüsselungsbasis Dokumente elektronisch zu unterschreiben und unterstützen somit einen papierlosen Geschäftsverkehr.

3.1.1. Elektronische Signatur – eigenhändige Unterschrift

Mit der eigenhändigen Unterschrift bestätigt eine Person ihre rechtsverbindliche Willenserklärung. Sie kann als biometrischer Vorgang angesehen werden und ist dementsprechend immer einem bestimmten Menschen zuzuordnen. Die Bindung eigenhändiger Unterschriften an ein Dokument bewirkt, dass eine vom Dokument abgetrennte Unterzeichnung keine verbindliche Gültigkeit erreicht. [8]

Elektronische Unterschriften sind ein maschinelles Erzeugnis und können optisch nicht mit einer herkömmlichen Unterschrift verglichen werden. Sie bestehen lediglich aus einer Bitfolge und sagen deshalb nichts über die Identität des Unterschreibenden aus.

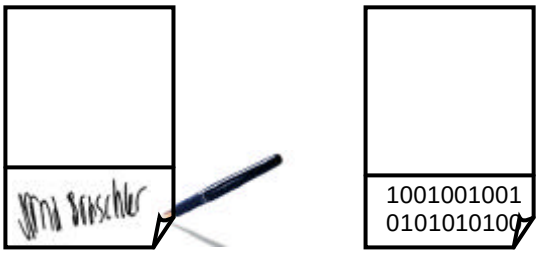


Abbildung 2: Eigenhändige Unterschrift und digitale Signatur
(Quelle: Horster [1996] S. 2)

Während bei einer konventionellen Unterschrift immer ersichtlich war, was unterschrieben wurde, kann ein elektronisches Dokument für den Unterschreibenden unsichtbare Funktionen, worüber er keine Kenntnis hat, enthalten. [9] Diese Problematik und weitere Punkte, wie beispielsweise die Authentifizierung des Absenders, stellen hohe technische und rechtliche Anforderungen an digitale Signaturen.

Anforderungen und Funktionen digitaler Signaturen

3.1.2. Funktionen

Wo die Schriftlichkeit rechtsverbindliche Wirkung hat, steht immer auch das Schutzinteresse des Unterzeichnenden im Vordergrund, auf welches auch im Bereich elektronischer Kom-

[8] Vgl. Horster [1996] S. 2 und 8.

[9] Vgl. Horster [1996] S. 9.

munikation nicht verzichtet werden kann.[10] Somit müssen digitale Signaturen die gleichen Aufgaben wie die eigenhändige Unterschrift erfüllen. Die folgende Tabelle stellt die einzelnen Funktionen sowie deren Kommentierung mit dem Verfahren der digitalen Signatur dar.[11]

Funktion	Beschreibung	Schriftformfunktion mit digitaler Signatur
Abschlussfunktion	Der Abschluss oder die Vollendung einer Erklärung wird willentlich zum Ausdruck gebracht und hebt sich vom blossen Entwurf ab. Das Dokument kann mit der am Ende stehenden Unterzeichnung nicht mehr verändert werden.	Bei der digitalen Signatur entscheidet der Unterzeichnende selbst, welche Daten digital signiert werden. Wichtig ist die Erkennbarkeit der Daten, auf welche sich die Signatur bezieht.
Identitätsfunktion	Die Unterschrift weist den Unterzeichnenden eines Dokumentes eindeutig aus.	Die digitale Signatur erfüllt diese Funktion durch die Verwendung von öffentlichen und privaten Schlüsseln, welche einer vertrauenswürdigen dritten Instanz entstammen.[12]
Echtheitsfunktion	Die Schriftform erbringt durch die Unterschrift den Nachweis über die Urheberschaft der Erklärung.	Die signierten Daten müssen beim Verfahren der digitalen Signatur in die Signatur miteinbezogen werden, um Änderungen bei der Signaturüberprüfung festzustellen.[13]
Warnfunktion	Sie schützt den Unterzeichnenden vor übereiligem Unterschreiben. Vorgängig soll die rechtsverbindliche Wirkung, welche aus dem Dokument hervorgeht, klar gemacht werden.	Bevor ein elektronisches Dokument digital signiert wird, muss ein Hinweis über die willentliche Beabsichtigung der Erzeugung der Signatur erscheinen.

[10] Vgl. Koch [1998] S. 148.

[11] Vgl. Horster [1996] S. 3.

[12] Vgl. Ziff 3.1.6 (Die digitale Signatur als Anwendung asymmetrischer Kryptographie und Ziff. 4 (Die Zertifizierungsstelle).

[13] Vgl. Ziff. 0 (Digitaler Fingerabdruck).

Funktion	Beschreibung	Schriftformfunktion mit digitaler Signatur
Beweisfunktion	Unterschriften müssen zu einem späteren Zeitpunkt als Beweismittel eingesetzt werden können.	Das signierte elektronische Dokument ist so zu kennzeichnen, dass ein Vorhandensein der Signatur erkennbar und nachvollziehbar ist. Dies ermöglicht der Zeitstempel, welcher bezeugt, dass zu einem bestimmten Zeitpunkt eine digitale Signatur ihre vollumfängliche Gültigkeit besass.[14]

Tabelle 1: Funktionen digitaler Signaturen
(Quelle: Eigene Darstellung in Anlehnung an Horster [1996] S. 3 und Koch [1998] S. 148f.)

3.1.3. Anforderungen an digitale Signaturen

Aus den oben stehenden Ausführungen lassen sich folgende Anforderungen an einen sicheren Einsatz von digitalen Signaturen ableiten:[15]

- ***«Vertraulichkeit:***
  Die Inhalte von Nachrichten sollen gegenüber allen Instanzen ausser dem vorgesehenen Empfänger vertraulich bleiben.
- ***Integrität:***
  Manipulationen an Nachrichteninhalten sollen erkannt werden können.
- *Authentizität:*
  Fälschungen von Absenderangaben sollen erkannt werden können.
- ***Verfügbarkeit:***
  Das Kommunikationssystem soll den gewünschten Nachrichtenaustausch zwischen Absender und Empfänger ermöglichen.
- ***Zurechenbarkeit:***
  Das Absenden beziehungsweise Empfangen einer Nachricht soll gegenüber Dritten nachgewiesen werden können.»

Für den rechtsverbindlichen Einsatz digitaler Signaturen müssen diese Kriterien erfüllt sein. Ansonsten ist eine Gleichstellung mit der eigenhändigen Unterschrift nicht möglich.

[14] Vgl. Ziff. 3.1.4 (Zeitstempel).

[15] Bertsch [2001] S. 3.

3.1.4. Zeitstempel

Während eigenhändige Unterschriften ein Leben lang als individuelle Willenserklärung eingesetzt werden können, sind digitale Signaturen in der Regel nur über einen bestimmten Zeitraum gültig.[16] Vergleichen lässt sich dies mit einer persönlichen Kreditkarte, welche nach einer bestimmten Zeit ablaufen und daraufhin wieder erneuert wird, im Falle eines Verlustes aber auch gesperrt werden kann. Zur Erneuerung der Kreditkarte werden die Daten des Karteninhabers überprüft und allfällig berichtigt. Auch digitale Signaturen können einer Sperrung unterliegen oder ablaufen. Wichtig ist, dass beim Einsatz von digitalen Signaturen zum Zeitpunkt der Erzeugung immer ihre Gültigkeit - mittels Bescheinigung, «*dass bestimmte digitale Daten zu einem bestimmten Zeitpunkt vorliegen*»[17] - nachgewiesen werden kann. Eine abgelaufene oder gesperrte Signatur hat keine verbindliche Wirksamkeit. Dieser Nachweis wird durch eine vertrauenswürdige dritte Partei gewährleistet.[18]

Technische Details digitaler Signaturen

3.1.5. Einführung in die Kryptographie

Die Kryptographie bildet die Grundlage für einen sicheren Datenaustausch über Computernetzwerke. Bei kryptografischen Verfahren werden Inhalte von elektronischen Nachrichten mittels Verschlüsselung unleserlich gemacht, um die Einsicht der Daten durch Dritte zu verhindern. Die Verschlüsselung (Chiffrierung) überführt den Klartext einer Nachricht in einen Chiffretext, die Entschlüsselung (Dechiffrierung) erzeugt aus dem Chiffretext wieder den ursprünglichen Klartext.[19] «*Die Daten werden bei der Chiffrierung so verändert, dass der verschlüsselte Text ohne den richtigen Schlüssel auch mit grossem Aufwand nicht entziffert werden kann.*»[20]

Kryptografische Verfahren werden überall dort eingesetzt, wo Daten vertraulich behandelt werden müssen, beispielsweise beim digitalen Signieren, bei grundsätzlicher Geheimhaltung von Daten oder bei der Zugangskontrolle zu Rechnernetzen.[21]

Symmetrische Kryptographie

Bei der symmetrischen Kryptographie wird nur ein Schlüssel zur Ver- und Entschlüsselung verwendet, den sowohl Sender als auch Empfänger kennen müssen. Ein Nachteil dieses Systems ist die Gewährleistung eines absolut sicheren Schlüsseltransportes vom Sender zum Empfänger. Gerät der Schlüssel unterwegs in falsche Hände, kann eine später versendete, geheime Nachricht problemlos entziffert werden. Ein weiteres Problem bildet die grosse Anzahl von Schlüsseln, da für zwei unterschiedliche Kommunikationspartner jeweils ein eigenes Schlüsselpaar notwendig ist.[22]

---

[16] Vgl. Bertsch [2001] S. 156.

[17] Art. 12 ZertES.

[18] Vgl. Ziff 4 (Die Zertifizierungsstelle).

[19] Vgl. Kopp [1998] S. 6.

[20] Graber [2000] S. 10.

[21] Vgl. Grundlagen der Kryptographie [2004, 11. August].

[22] Vgl. Dohmann et al. [2002] S. 134.

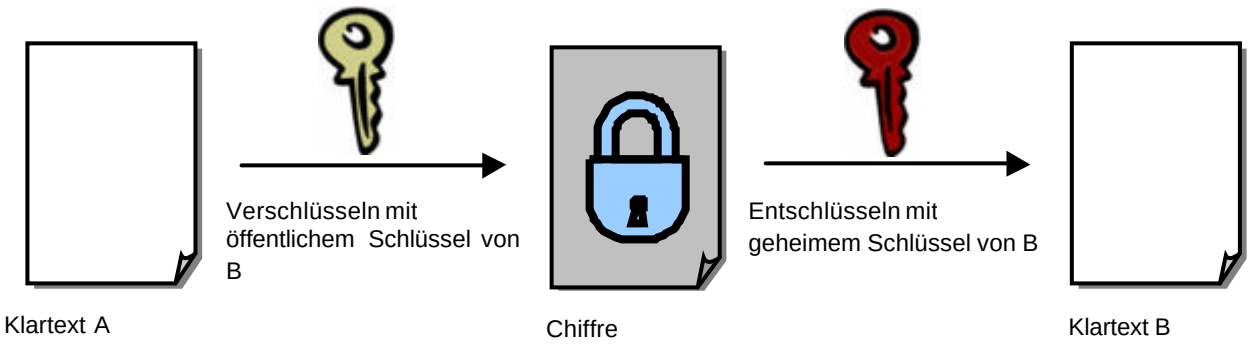
Asymmetrische Kryptographie

Die asymmetrische Kryptographie verwendet zwei verschiedene Schlüssel; den öffentlichen Schlüssel (public key) zum Verschlüsseln, den privaten Schlüssel (private key) zum Entschlüsseln, weshalb dieses Verfahren auch „Public Key-Verfahren" genannt wird. Der öffentliche Schlüssel wird der breiten Öffentlichkeit bekannt gemacht. Den privaten Schlüssel kennt jedoch nur der Besitzer selbst. Demzufolge gehört zu jedem öffentlichen ein privater Schlüssel, aus dem einen kann aber nicht auf den anderen geschlossen werden. Möchte Person A ein verschlüsseltes Dokument der Person B übermitteln, so verschlüsselt sie das Dokument mit dem öffentlichen Schlüssel von Person B. Sobald das chiffrierte Dokument übermittelt wurde, kann Person B mit dem nur ihr bekannten privaten Schlüssel die Nachricht wieder dechiffrieren.[23]

3.1.6. Die digitale Signatur als Anwendung asymmetrischer Kryptographie

Das digitale Signieren und Verschlüsseln eines Dokumentes

Das asymmetrische Verschlüsselungsverfahren wird auch bei der digitalen Signatur eingesetzt. Für das Verschlüsseln wird wiederum der öffentliche Schlüssel, für das Entschlüsseln der private Schlüssel des Empfängers eingesetzt.



[23] Vgl. Dohmann et al. [2002] S. 134.

Abbildung 3: Asymmetrische Verschlüsselung
(Quelle: Dohmann et al. [2002] S. 135)

Während die Verschlüsselungsprozedur nur für die Geheimhaltung des Dokumentes verantwortlich ist, kann mit der Signatur die Authentizität des Absenders sowie die Integrität der signierten Daten nachgewiesen werden. Für die Erzeugung der Signatur wird der geheime Schlüssel des Senders eingesetzt, wobei der Empfänger die Signatur mit dem öffentlichen Schlüssel des Senders überprüfen kann.

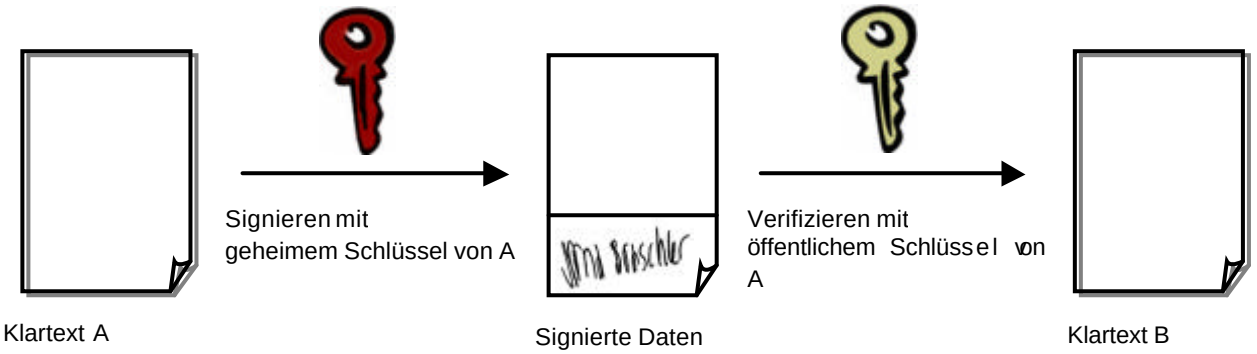


Abbildung 4: Asymmetrische Signatur
(Quelle: Eigene Darstellung in Anlehnung an Bitzer, Brisch [1999] S. 89)

Die Authentizität wird dadurch gewährleistet, dass der öffentliche Schlüssel aus einem digitalen Zertifikat stammt und von einer vertrauenswürdigen Stelle, einer Zertifizierungsstelle oder eines Trust Centers zertifiziert wurde. Dieses Zertifikat bürgt für die Identität eines Absenders und kann sowohl vom Empfänger als auch von anderen Kommunikationspartnern eingesehen werden.[24]

Digitaler Fingerabdruck (Hashfunktion)

Für die Gewährleistung der Datenintegrität wird nicht das ganze Dokument signiert sondern es wird eine mathematische Funktion, die Hashfunktion, auf das Dokument angewendet. Der daraus entstandene Hashwert, welcher keine Rückschlüsse auf die ursprünglichen Daten zulässt und für jedes Dokument einzigartig ist, wird daraufhin digital signiert.[25] Sobald eine Nachricht nach Generierung der Prüfziffer und der anschliessenden Anwendung der asymmetrischen Signatur verändert wird, ergibt dies bei der Überprüfung des Hashwertes durch den Empfänger nicht mehr dieselbe Ziffer. Damit werden Datenveränderungen nach Erstellung der Signatur erkannt. Falls es nicht, oder nur sehr schwer möglich ist, zwei Nachrichten mit derselben Prüfsumme zu erstellen, handelt es sich um eine sichere Hashfunktion. Der daraus resultierende sichere Hashwert wird auch als digitaler Fingerabdruck bezeichnet.[26]

Der Sender unterschreibt nun eine Nachricht, indem er vorgängig den Hashwert generiert und diesen Wert anschliessend mit seinem privaten Schlüssel signiert. Diese Signatur wird der eigentlichen Nachricht angehängt und versendet.

[24] Vgl. Ziff. 4 (Die Zertifizierungsstelle).

[25] Vgl. Hansen, Neumann [2001], S 178.

[26] Vgl. Hansen, Neumann [2001] S. 178.

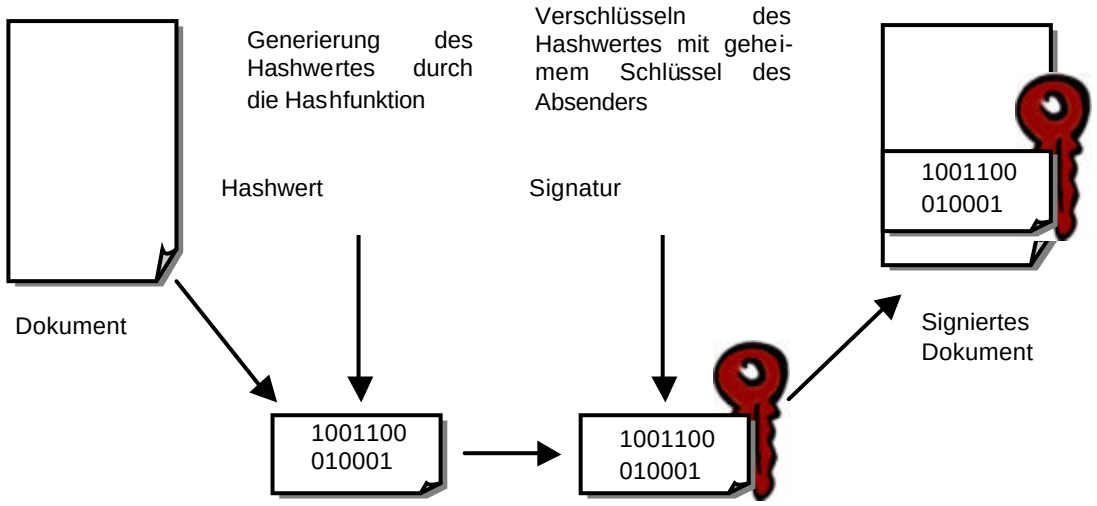


Abbildung 5: Digitale Signatur mit Hashfunktion
Quelle: Bitzer, Brisch [1999], S. 22

Der Empfänger entschlüsselt mit dem öffentlichen Schlüssel des Absenders die Signatur und ermittelt danach aus dem erhaltenen, entschlüsselten Dokument wiederum den Hashwert, welcher mit dem Wert aus der Signaturentschlüsselung verglichen wird. Stimmen die Werte überein, kann auf eine unveränderte Meldung geschlossen werden.

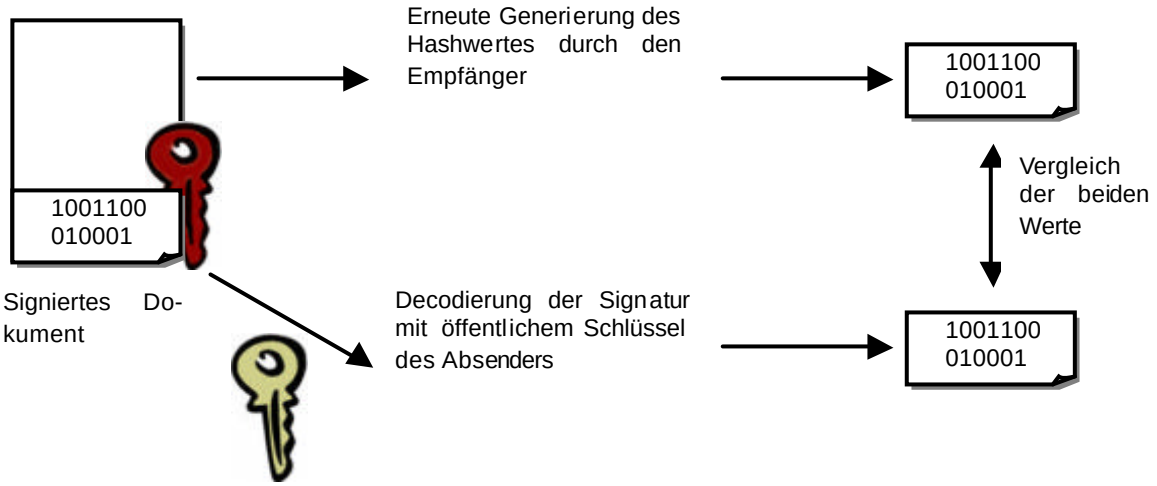


Abbildung 6: Decodierung einer digitalen Signatur mit Hashwert
(Quelle: Bitzer, Brisch [1998] S. 24)

Hashwerte nachzuahmen, beziehungsweise zu fälschen ist mit dem Geburtstagsangriff möglich. «Bei diesem Angriff wird versucht, vor der eigentlichen Signaturoperation zwei Dokumente mit gleichem Hashwert zu finden, um eines danach dem Opfer des Angriffs zur Signatur vorzulegen und es anschliessend durch das andere zu ersetzten.»[27] Obwohl dieser Angriff erhebliche Rechnerleistung erfordert und mehrere Monate dauern kann, ist er eine ernstzunehmende Bedrohung für 128-Bit-Hashfunktionen. Vor allem in der Industriespionage könnten solche Fälschungen äusserst lukrativ sein, besonders dann, wenn das Überleben

[27] Der Geburtstagsangriff auf die digitale Signatur [2004, 11. August].

der eigenen Unternehmung davon abhängt. Schwieriger wird es, 256-, 348- oder 512-Bit-Hashfunktionen zu imitieren, weshalb deren Verwendung als sicherer eingestuft werden kann und sie die Immunität gegenüber dem Geburtstagsangriff eher gewährleisten.[28]

Authentifizierungssysteme

Damit keine unerwünschte Erzeugung der digitalen Signatur durch Missbrauch eines privaten Schlüssels entsteht, braucht es Authentifizierungssysteme. Herkömmliche Authentifizierungsmöglichkeiten wie beispielsweise Passwortschutz gewährleisten keine vollumfängliche Sicherheit, da der Mensch an seinem Wissen, beziehungsweise an seinem Besitz erkannt werden kann, was ein mögliches Kopieren erleichtert. Die biometrische Authentifizierung erkennt den Menschen an seinem Sein, und kann deshalb schwer nachgeahmt werden.[29] Mittels physischem Fingerabdruck oder dem Lesen der Augeniris kann sich eine Person eindeutig autorisieren und anschliessend die Signatur erzeugen.

Begriffsdefinition

Vor dem Hintergrund oben stehender Ausführungen wird der Begriff digitale Signatur folgendermassen definiert: [30]

«Unter einer elektronischen Unterschrift (digitale Signatur) versteht man einen kryptographisch geschützten Nachweis, dass ein eindeutig identifizierter Benutzer einen Datenbereich (ein digitales Dokument) unterzeichnet hat. Eine digitale Signatur ist ein mit einem privaten Signaturschlüssel erzeugtes Siegel für einen Datenbereich, das mit Hilfe eines zugehörigen öffentlichen Schlüssels den Inhaber und die Unverfälschtheit der Daten erkennen lässt […].»

Wenn die digitale Signatur zum Zeitpunkt der Erzeugung zusätzlich auf einem gültigen Zertifikat basiert, welches einer anerkannten Zertifizierungsstelle entstammt, spricht man von einer qualifizierten elektronischen Signatur.[31]

Rechtliche Voraussetzungen digitaler Signaturen

Ein Eckpunkt für die rechtliche Verbindlichkeit digitaler Signaturen bildet die Gleichstellung der eigenhändigen Unterschrift mit der digitalen Signatur.[32] Im schweizerischen Obligationenrecht ist bis zum jetzigen Zeitpunkt nur die eigenhändige Erbringung der Unterschrift verankert.[33] Die gesetzliche Veränderung für die Verwendung digitaler Signaturen ist vorgesehen und wird in einem neuen Artikel 13 Abs. 2 des Obligationenrechts wie folgt festgehalten: «*Der eigenhändigen Unterschrift gleichgestellt ist die qualifizierte elektronische Signatur, die auf einem qualifizierten Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten im Sinne der Bundesgesetzes vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich*

[28] Vgl. Der Geburtstagsangriff auf die digitale Signatur [2004, 11. August].

[29] Vgl. Biometrie, ein Überblick [2004, 9. August].

[30] Hansen, Neumann [2001] S. 184.

[31] Vgl. Hansen, Neumann [2001] S. 184 und Ziff. 4 (Die Zertifizierungsstelle).

[32] Vgl. Bundesamt für Justiz [2004, 11. August].

[33] Vgl. Art. 14 OR.

der elektronischen Signatur beruht und auf den Namen einer natürlichen Person lautet.»[34] Die entsprechenden Gesetzesentwürfe[35] und Gesetzesänderungen für den Einsatz elektronischer Signaturen bestehen bereits, das Inkrafttreten der Anpassungen und neuen Gesetze wird gemäss Auskunft des Bundesamtes für Justiz wird auf 1. Januar 2005 erwartet.

[34] Art 21 ZertES.

[35] Vgl. Ziff. 0 (Rechtliche Betrachtung einer schweizerischen Zertifizierungsstelle).

4. Die Zertifizierungsstelle

Das folgende Kapitel gibt einen Einblick in die Aufgaben und Organisation einer Zertifizierungsstelle.

Einführung und Begriffsdefinitionen

Zertifizierungseinrichtungen tragen die Verantwortung, dass Absender von digital signierten Dokumenten eindeutig einem öffentlichen Schlüssel zugeteilt sind. Öffentliche Schlüssel versinnbildlichen, in diesem Zusammenhang auch Zertifikate und beinhalten Angaben zum Zertifikatsinhaber.[36] Möchte eine Person fortan Dokumente digital unterschreiben, so muss ihr Zertifikat bei einer Zertifizierungsstelle registriert werden, damit die Kommunikationspartner deren Identität mittels öffentlichen Schlüssels jederzeit überprüfen können.

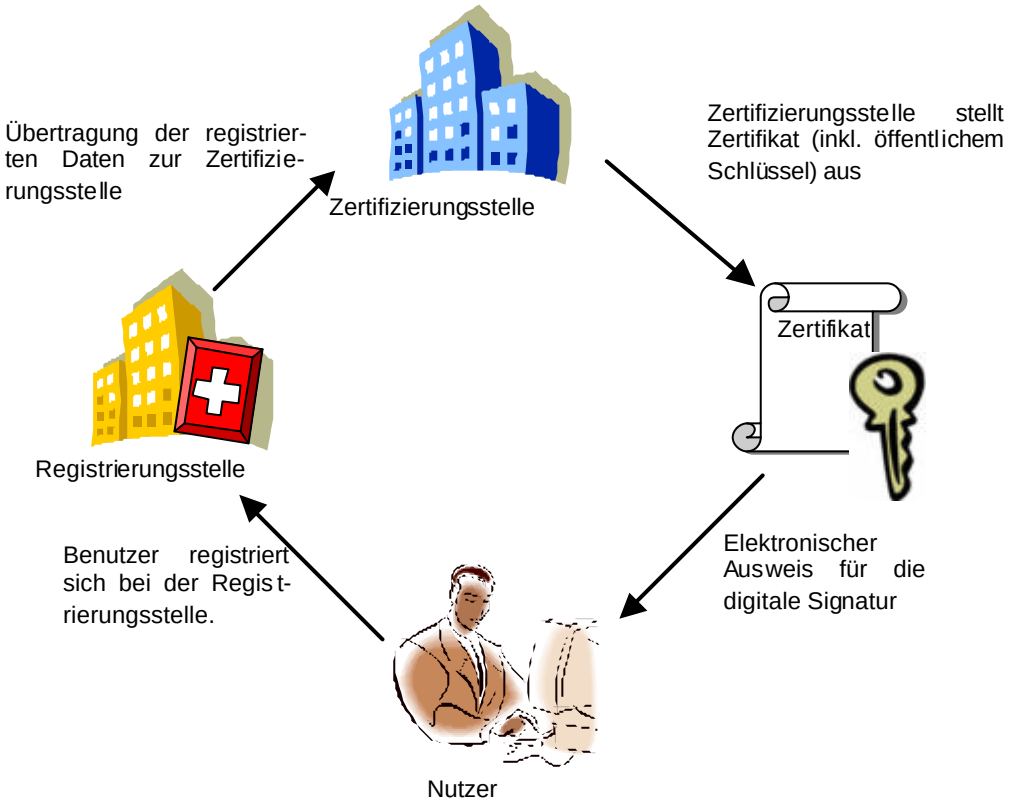


Abbildung 7: Zertifikatsantrag

(Quelle: Hansen, Neumann [2001], S. 186)

Nach erfolgter Registrierung bei der Zertifizierungsstelle erhält der Nutzer das Zertifikat mit dem öffentlichen Schlüssel und weiteren Informationen über den Antragssteller. Das Zertifikat wird von der Zertifizierungsstelle mit einer digitalen Signatur versehen und schliesslich dem Antragssteller übermittelt wird. Die Echtheit des Zertifikats kann anhand dieser digitalen Signatur durch Dritte jederzeit überprüft werden.[37]

[36] Vgl. Dohmann et al. [2002] S. 140.

[37] Vgl. Hansen, Neumann [2001] S. 186f.

Zunächst sollen einige Begriffe definiert werden, um anschliessend auf die Aufgaben, die Pflichten sowie die technischen Voraussetzungen einer Zertifizierungsstelle einzugehen.

Public Key Infrastruktur (PKI):

«Die technisch-organisatorischen Einrichtungen, die zur Ausgabe und Verwaltung von privaten und öffentlichen Schlüsseln, sowie den Zertifikaten nötig sind, werden unter dem Begriff Public Key Infrastruktur zusammengefasst.»[38]

Zertifizierungsdiensteanbieterin, Zertifizierungsstelle, Certification Authority (CA), Trust Center:

Zertifizierungsdiensteanbieterinnen bilden eine dritte Partei zwischen zwei Kommunikationspartnern und sorgen dafür, dass der öffentliche Schlüssel einer bestimmten Person zugehörig ist, indem sie die elektronische Zertifizierung von öffentlichen Schlüsseln vornehmen und diese verwalten.[39] Zertifizierungsdiensteanbieterinnen können sich freiwillig von der Anerkennungsstelle akkreditieren lassen.

Registrierungsstelle, Registration Authority (RA):

Sie «*verifizieren die Identität der Antragssteller und organisieren die Zertifikatsausgabe im Namen der Certification Authority.*»[40] Als Registrierungsstelle können die Zertifizierungsdiensteanbieterinnen selbst, aber auch öffentliche Ämter oder private Institutionen auftreten.

Anerkennungsstelle, Certification Body (CB):

Sie «bestätigt die Konformität bestimmter Produkte, Dienstleistungen oder Verfahren mit bestimmten Normen in einem schriftlichen Dokument»[41]. Die Anerkennungsstelle bezeugt also, dass eine Zertifizierungsstelle die gesetzlich verankerten Voraussetzungen für eine Anerkennung erfüllt. In der Schweiz tritt das Wirtschaftsprüfungs- und Beratungsunternehmen KPMG als akkreditierte Anerkennungsstelle auf.[42]

Die Anerkennung in der Schweiz ist ein privatrechtliches Rechtsgeschäft. Mögliche Streitigkeiten zwischen Anerkennungsstellen und Zertifizierungsstellen unterliegen nicht dem Verwaltungsrecht, sondern werden von den Zivilgerichten entschieden.[43] Durch diese Regelung soll die Administration des Bundes entlastet werden.[44]

Akkreditierungsstelle:

Die Akkreditierungsstelle anerkennt die Anerkennungsstellen und wird vom Bund bestimmt. Diese Akkreditierung unterliegt in der Schweiz dem öffentlichen Recht. Sie ist verpflichtet, der Öffentlichkeit eine Liste der anerkannten Zertifizierungsstellen zur Verfügung zu stellen. Die Schweizerische Akkreditierungsstelle (SAS) des Bundesamtes für Metrologie und Akkreditierung (metas) akkreditiert die Stellen, die für die Anerkennung der Zertifizierungsstellen

[38] Legler [2000] S. 6.

[39] Vgl. Schlauri [2001] S. 66, Ramsauer et al. [2001] S. 194.

[40] Public-Key-Infrastrukturen [2004, 19. Juli].

[41] Ramsauer et al. [2001] S. 194.

[42] Vgl. KPMG [2004, 11. August].

[43] Vgl. Botschaft zum ZertES S. 5694.

[44] Vgl. Schlauri [2001] S. 82.

zuständig sind.[45] «*Besteht keine akkreditierte Anerkennungsstelle, anerkennt die SAS die Zertifizierungsstellen.*»[46]

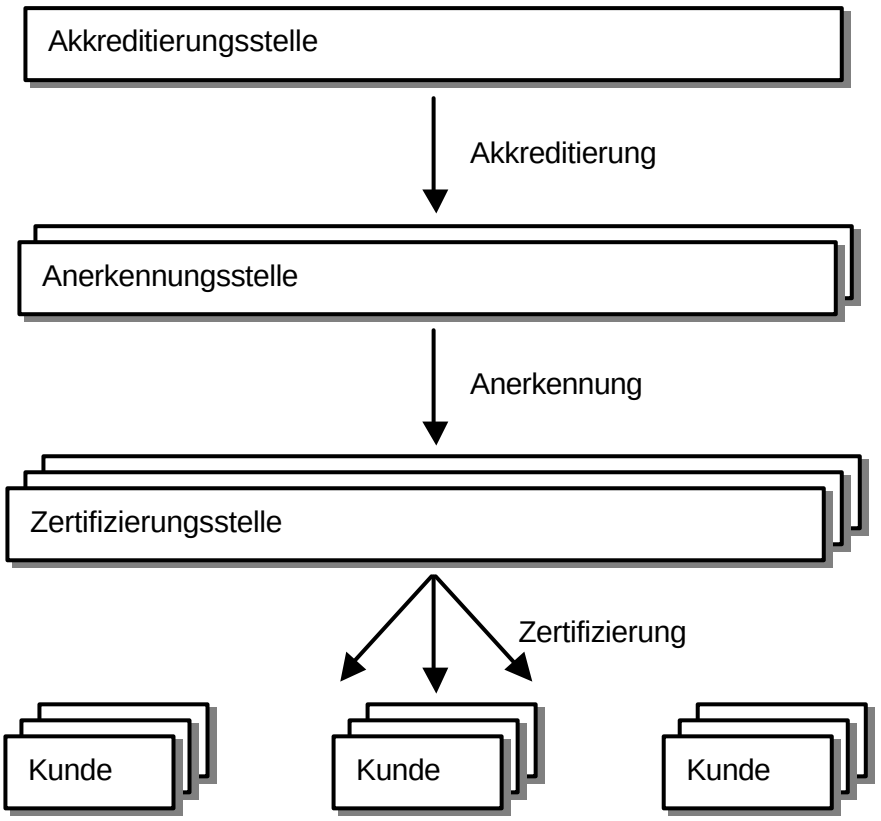


Abbildung 8: Public Key Infrastruktur
(Quelle: Schlauri [2001] S. 82)

Zertifikat:

«Ein digitales Zertifikat ist ein digitales Dokument, das von einer Zertifizierungsstelle digital signiert wird und einen bestimmten öffentlichen Schlüssel (sowie weitere Informationen) eindeutig einer Person oder einer Organisation zuordnet.»[47]

Entspricht ein Zertifikat den gesetzlichen Anforderungen eines bestimmten Landes, wird es also von einer anerkannten Zertifizierungsstelle ausgegeben, kann von einem qualifizierten Zertifikat gesprochen werden. Darin müssen nach schweizerischem Recht die Seriennummer, eine Kennzeichnung, dass es sich um ein qualifiziertes Zertifikat handelt, der Name oder das Pseudonym des Inhabers des Signaturschlüssels, der Signaturprüfschlüssel, die Gültigkeitsdauer sowie der Name und die Signatur der ausstellenden Zertifizierungsstelle enthalten sein.[48] Ein weit verbreiteter Standard für digitale Zertifikate ist X.509.[49] Dieses Format wird in der Regel von den Internetbrowsern unterstützt.

[45] Vgl. Art. 1 Abs. 1 VZertES.

[46] Art. 1 Abs. 2 VZertES.

[47] Hansen, Neumann [2001] S. 186.

[48] Vgl. Art. 7 Abs. 1 ZertES.

[49] Vgl. Graber [2000]. S. 14.

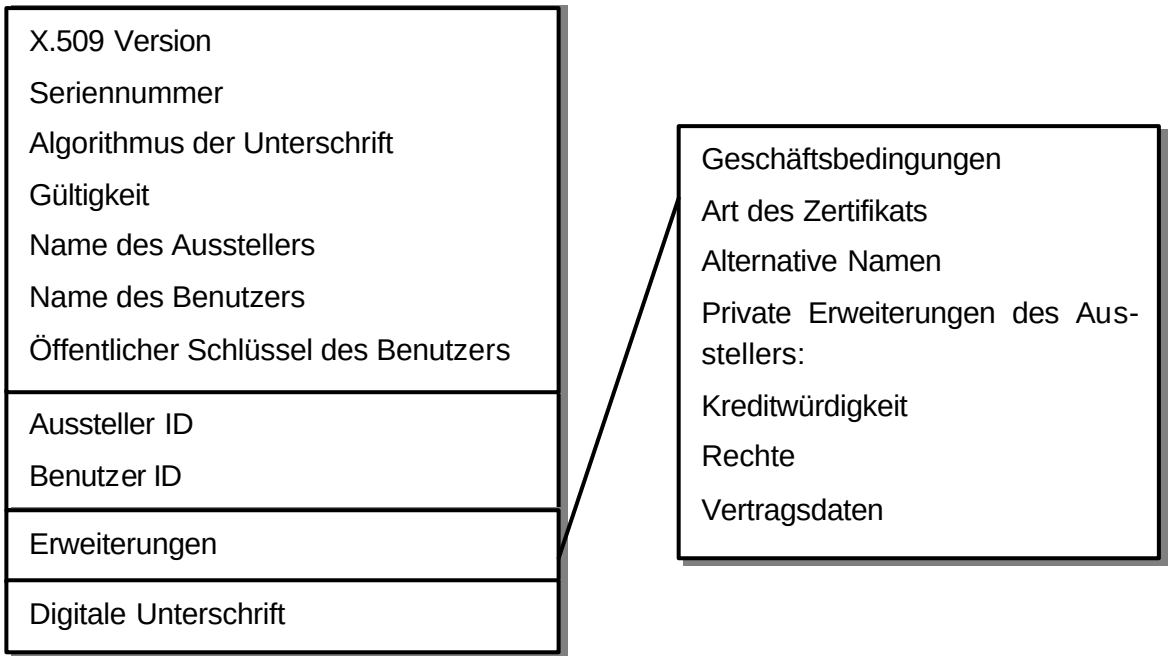


Abbildung 9: Aufbau von X.509-Zertifikaten
(Quelle: Hansen, Neumann [2001] S. 187)

Falls die digitale Signatur der eigenhändigen Unterschrift gleichgestellt wird, muss der öffentliche Schlüssel aus einem qualifizierten Zertifikat stammen.

Je nach dem, wie genau die Personenidentifikation ausfallen muss, wird zwischen verschiedenen Zertifikatsklassen unterschieden.[50] So fällt ein Zertifikat, welches über ein Online-Formular angefordert wird in eine niedrigere Klasse, als ein qualifiziertes Zertifikat. Um von einer Zertifizierungsstelle ausgestellte Zertifikate zu nutzen, muss vorgängig ein Wurzelzertifikat (Root Certificate) installiert werden. Mit einem Wurzelzertifikat können alle von einer bestimmten Zertifizierungsstelle stammenden Zertifikate überprüft werden. Bei der Installation des Wurzelzertifikates ist dessen Ursprung stets zu kontrollieren.[51]

Arten von Zertifizierungsstellen

4.1.1. Private, anerkannte Zertifizierungsstelle

Eine oder mehrere private Organisationen können als solche Zertifizierungsstellen auftreten. Sie unterliegen den gesetzlichen Vorschriften und sind dementsprechend in der Lage, qualifizierte Zertifikate herauszugeben. Private, anerkannte Zertifizierungsstellen bieten ihre Dienste öffentlich, das heisst einem breiten Publikum an. Deshalb von einer öffentlichen Zertifizierungsstelle zu sprechen ist nicht angebracht, da auch eine staatliche sowie eine private, dem breiten Publikum zugängliche Zertifizierungsstelle, über ein öffentliches Zertifikatsangebot verfügt.[52]

[50] Vgl. Sichere Internet-Kommunikation mit Zertifikat [2004, 22. Juli].

[51] Vgl. A-Trust [2004, 9. August].

[52] Vgl. Oppliger [2002, 29. November].

4.1.2. Staatlich anerkannte Zertifizierungsstelle

Bei einer staatlich anerkannten Zertifizierungsstelle übernimmt der Staat die verantwortungsvolle Aufgabe, die Zertifikate nach dem Zertifizierungsgesetz auszustellen und zu verwalten. Wie bei privaten, anerkannten Zertifizierungsstellen ist auch diese in der Lage, qualifizierte Zertifikate auszustellen.

4.1.3. Private Zertifizierungsstelle

Die privaten Zertifizierungsstellen unterscheiden sich zwischen internen und dem breiten Publikum zugänglichen Zertifizierungsstellen. Letztere bieten Zertifikate für die Öffentlichkeit an, während bei der firmeneigenen Zertifizierungsstelle nur Zertifikate im internen Umfeld einer Organisation (Mitarbeiter und Kunden) ausgestellt werden. Beiden Typen ist jedoch gemein, dass sie keine qualifizierten Zertifikate anbieten können, was einen Einsatz für die qualifizierte digitale Signatur verhindert.

Anforderungen an anerkannte Zertifizierungsstellen

Für eine Anerkennung muss die Zertifizierungsstelle zuverlässiges Arbeiten in allen Bereichen garantieren. Dazu gehört gut ausgebildetes Personal, die Verwendung von vertrauenswürdigen Systemen und Produkten[53] und die Gewährleistung der vertraulichen Behandlung der Personendaten. Ausserdem müssen sie über ausreichende Finanzmittel verfügen, um etwa das Haftungsrisiko für Schäden oder mögliche Forderungen nach einer Geschäftsaufgabe decken zu können. Auch sollten alle einschlägigen Informationen eines qualifizierten Zertifikates über einen angemessenen Zeitraum archiviert werden, damit diese in einem juristischen Verfahren als Beweismittel eingesetzt werden können.[54]

Rahmenbedingungen

4.1.4. Anerkennung

Damit sich eine schweizerische Zertifizierungsstelle anerkennen lassen kann, muss sie weitgehend oben stehenden Anforderungen genügen. Zudem sind ein Eintrag ins Handelsregister sowie der Abschluss der notwendigen Versicherungen für allfällige Haftungsansprüche durch Dritte unerlässlich.[55]

Diese Voraussetzungen gelten auch für ausländische Zertifizierungsdiensteanbieterinnen. Eine ausländische Zertifizierungsstelle kann jedoch nur von einer schweizerischen Anerkennungsstelle anerkannt werden, wenn diese im eigenen Land bereits von einer Anerkennungsstelle akkreditiert worden ist, die Anerkennung durch das entsprechende Recht erworben hat und die nötigen Voraussetzungen des ausländischen Rechts sich mit denjenigen des schweizerischen Rechts decken. Ausserdem müssen die ausländischen Anerkennungsstel-

[53] Vgl. Ziff. 0 (Technische Voraussetzungen einer Zertifizierungsstelle).

[54] Vgl. SiRL Anhang II.

[55] Vgl. Art. 3 Abs. 1 ZertES.

len über gleichwertige Qualifikationen wie eine schweizerische verfügen und eine Zusammenarbeit mit der schweizerischen Anerkennungsstelle gewährleisten.[56]

Auf die Möglichkeit der gegenseitigen Anerkennung von Zertifizierungsstellen (Crosscertification) wird in der schweizerischen Gesetzgebung bewusst verzichtet. In der Botschaft zum Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur wird dies damit begründet, dass das vorgeschlagene System eine grössere Transparenz über das Anerkennungsverfahren bietet.

4.1.5. Pflichten

Eine anerkannte Zertifizierungsstelle muss für die Personenidentifikation verlangen, dass die Antragsteller persönlich erscheinen und ihre Identität nachweisen.[57] Die Zertifizierungsstelle kann hierfür die Registrierungsstellen einsetzen. Ferner soll sich die Zertifizierungsstelle «*vergewissern, dass die Person, welche ein qualifiziertes Zertifikat verlangt, im Besitz des entsprechenden Signaturschlüssels ist.*»[58]

Die Führung eines Tätigkeitsjournals, die Ungültigkeitserklärung qualifizierter Zertifikate, das Erstellen eines für alle einsehbaren Verzeichnisses aller gültigen und ungültigen Zertifikate, sowie das Versehen der Zertifikate mit einem Zeitstempel gehören ebenfalls zu den erforderlichen Aufgaben einer anerkannten Zertifizierungsstelle.[59] Die Zertifizierungsstelle darf nur die öffentlichen Schlüssel verwalten und muss ihre Kunden über die Aufbewahrungsmöglichkeiten des privaten Schlüssels sowie über seine Missbrauchsrisiken informieren. Ausserdem müssen die Zertifizierungsstellen die allgemeinen Geschäftsbedingungen zur Verbesserung der Transparenz in einem Certification Practice Statement publizieren.[60]

4.1.6. Haftung und Versicherung

Falls die anerkannte Zertifizierungsstelle ihren Pflichten nicht gerecht wird und ein Zertifikatsinhaber deswegen Schaden erleidet, haftet sie gegenüber dem Inhaber des Zertifikates, sofern sie nicht nachweisen kann, dass sie kein Verschulden trifft.[61] Dabei ist sie auch zum Ersatz reiner Vermögensschäden (Vermögensschäden, welche nicht Personen- oder Sachschäden sind) im Sinne einer milden Kausalhaftung verpflichtet.[62] Auch für das Fehlverhalten von Registrierungsstellen steht sie ein. Ausserdem hat der Gesetzgeber die Umkehr der Beweislast[63] vorgesehen, welche die Haftungssituation zu Lasten der Zertifizierungsstelle verschärft. Durch den Ersatz der reinen Vermögensschäden sowie durch die Umkehr der Beweislast wird das Risiko kaum abschätzbar. Die Versicherbarkeit setzt die Abschätzung des Risikos aber voraus, was zur Folge hat, dass das Risiko „reine Vermögensschäden“ wegen

[56] Vgl. Art. 3 Abs. 2 ZertES.

[57] Vgl. Art. 8 Abs. 1 ZertES.

[58] Art. 8 Abs. 3 ZertES.

[59] Vgl. Art. 9, Art. 10, Art. 11 und Art. 12 ZertES.

[60] Vgl. Botschaft zum ZertES S. 5697.

[61] Vgl. Art. 16 Abs. 1 ZertES und Ramsauer [2000] S. 70.

[62] Vgl. Botschaft zum ZertES S. 5700.

[63] Vgl. Art. 16 Abs. 2 ZertES.

Unkalkulierbarkeit heute in der Schweiz nur schwer oder nicht versicherbar ist.[64] Für die Anerkennung ist der Abschluss einer Versicherung aber notwendig.

Rechtliche Betrachtung einer schweizerischen Zertifizierungsstelle

4.1.7. Verordnung über die Dienste der elektronischen Zertifizierung (ZertDV)

Wie bereits erwähnt muss die digitale Signatur für ihren verbindlichen Einsatz der eigenhändigen Unterschrift gleichgesetzt werden. Dies kann jedoch nur geschehen, wenn die Sicherheit digitaler Signaturen sowie das nahtlose Funktionieren einer Public Key Infrastruktur gewährleistet sind. Da die technische Umsetzung der digitalen Signatur weitgehend gelöst ist, stellt sich nun die Frage nach dem rechtlichen Regelungsbedarf.[65]

Aus diesem Grund ist am 12. April 2000 die Verordnung über Dienste der elektronischen Zertifizierung (ZertDV) vom Bundesrat verabschiedet worden und am 1. Mai 2000 in Kraft getreten.[66] «*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.*»[67] Gemäss Art. 21 Abs. 2 ZertDV gilt sie «*bis zum Inkrafttreten einer entsprechenden gesetzlichen Regelung, längstens aber bis zum 31. Dezember 2009.*»

Die Schweiz hat mit dieser Verordnung einen ersten Schritt zur Anerkennung elektronischer Signaturen unternommen und hat somit eine Anpassung an die Bedürfnisse der Informationsgesellschaft vorgenommen.[68]

4.1.8. Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES)

Da die Verordnung nur eine begrenzte Gültigkeit hat, begann kurz darauf die Ausarbeitung eines Entwurfes für das Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES). Dieses Gesetz darf als eine Ergänzung beziehungsweise als eine Korrektur der ZertDV angesehen werden und weist somit dieselbe Struktur wie die Verordnung auf.[69] Gleichzeitig mit der Regelung der Zertifizierungsstellen werden auch die entsprechenden Gesetzesänderungen im Anhang aufgeführt.

Am 6. Juli 2001 verabschiedete der Bundesrat zuhanden des Parlaments den Gesetzesentwurf zusammen mit der entsprechenden Botschaft. Darauf nahmen die eidgenössischen Räte am 19. Dezember 2003 das ZertES an. Die Referendumsfrist ist am 8. April 2004 abgelaufen, das Inkrafttreten des Gesetzes wird, wie erwähnt, auf 1. Januar 2005 erwartet.[70] Zum

[64] Vgl. Anhang C (Haftpflichtversicherung der Zertifizierungsstelle).

[65] Vgl. Schlauri [2001] S. 71.

[66] Vgl. Dörr [2003] S. 231.

[67] Art. 1 Abs. 1 ZertDV.

[68] Vgl. Dörr [2003] S. 332.

[69] Vgl. Dörr [2003] S. 250.

[70] Vgl. Helbling, Kaiser [2004, 21. Mai].

ZertES ist nach Ablauf der Referendumsfrist eine neue Verordnung (VZertES) ausgearbeitet worden, welche seit dem 1. Juni 2004 als Entwurf vorliegt. Sie soll die ZertDV vom 12. April 2000 mit dem Inkrafttreten des ZertES ablösen.[71]

4.1.9. Exkurs: Europäische Signaturrichtlinie (SiRL)

Die Europäische Signaturrichtlinie wurde am 13. Dezember 1999 von der Europäischen Union verabschiedet und «soll die Verwendung elektronischer Signaturen erleichtern und zu ihrer rechtlichen Anerkennung beitragen. Sie legt rechtliche Rahmenbedingungen für elektronische Signaturen und für bestimmte Zertifizierungsdienste fest, damit das reibungslose Funktionieren des Binnenmarktes gewährleistet ist.»[72] Die SiRL definiert zusammenfassend ihre Ziele folgendermassen:[73]

Harmonisierung der Regeln über die Anerkennung von digitalen Signaturen und die Akkreditierung von Zertifizierungsinstanzen

- Vertrauensbildung und Akzeptanz hinsichtlich neuer Technologien
- Förderung der sicheren grenzüberschreitenden Kommunikation
- Förderung der Interoperabilität von Produkten für elektronische Signaturen
- Zertifizierungsdienstangebot auf europäischer Ebene
- Marktzugang für elektronische Signaturen (Dienste und Produkte)
- Sicherer Informationsaustausch für Unternehmer und Konsumenten
- Wettbewerbsförderung zwischen Akkreditierungssystemen für Zertifizierungsinstanzen

Nach dieser Richtlinie haben alle EU-Staaten die rechtliche Anerkennung im Sinne der SiRL zu regeln und ein freiwilliges, staatliches Akkreditierungssystem für Zertifikatsanbieter einzuführen. Mittlerweile haben viele Staaten die dazugehörigen Gesetze und Verordnungen erlassen und dementsprechend auch Zertifizierungsstellen eingerichtet.[74] Mit der Zertifizierungsdiensteverordnung hat auch die Schweiz die Signaturrichtlinie autonom umgesetzt.[75]

Technische Voraussetzungen einer Zertifizierungsstelle

4.1.10. Computerbasierte Sicherheit

Die technischen Sicherheitsanforderungen für Zertifikatsanbieter basieren auf den technischen und administrativen Vorschriften über Dienste der elektronischen Zertifizierung. Dazu zählen unter anderen folgende Komponenten:[76]

[71] Vgl. Art. 15 und Art. 16 VZertES.

[72] Art. 1 SiRL.

[73] Vgl. Dörr [2003], S. 51f.

[74] Vgl. Oppliger [2002, 29. November].

[75] Vgl. Schweizer Bank [2000, 1. September].

[76] Dörr [2003] S. 248 und Technische und administrative Vorschriften über Dienste der elektronischen Zertifizierung.

«Für die Generierung der Signaturschlüssel sind technische Sicherheitsvorkehrungen erforderlich, welche gegen alle Eindringversuche geschützt sind und ein Kopieren oder Extrahieren des privaten Schlüssels aus der Einrichtung nicht erlauben.

Der Zertifizierungsdiensteanbieter muss für die Generierung der Schlüssel der Antragssteller stets einen Algorithmus verwenden, der den Empfehlungen der ALGO[77] von EESSI[78] entspricht. […]

Die Registrierungsstelle, die einen Antrag zur Suspendierung oder zum Widerruf eines Zertifikates an den Zertifizierungsdiensteanbieter stellt, muss dafür einen sicheren Kommunikationskanal verwenden, welcher die Integrität, die Authentizität und die Vertraulichkeit der Daten gewährleistet.»

Auch wenn eine Zertifizierungsstelle alle vorgeschriebenen Sicherheitsaspekte berücksichtigt, ist die Sicherheitsproblematik dennoch nicht gelöst. Die Zertifikatsanwender, vor allem Privatpersonen, verfügen oft über ungenügende Schutzeinstellungen an ihren PCs. Auch weisen die Anwenderprogramme selbst häufig Sicherheitslücken auf und für die verlässliche Anwendung von digitalen Signaturen kommen deshalb nur wenige Programme in Frage. Eine Lösung bestünde darin, alle persönlichen Anwenderprogramme selbst zu zertifizieren, was aber für den Normalnutzer nicht zumutbar wäre.[79]

4.1.11. Sicherheit der Infrastruktur

Um einen hohen Sicherheitsstandard zu erbringen, müssen zusätzlich auch bauliche Vorkehrungen getroffen werden. Dazu zählen insbesondere die Einrichtung einer Alarmanlage im Gebäude der Zertifizierungsstelle, gesonderte hochsichere Rechnerräume, Überwachungssysteme, Brandmelder und Sprinkleranlagen sowie Zugangsschleusen.[80]

[77] Die Abkürzung ALGO steht für Algorithms Group.

[78] ESSI bedeutet Europäische Initiative für Standardisierung der elektronischen Signatur.

[79] Vgl. Gespräch mit SwissCERT.

[80] Vgl. D-Trust [2004, 22. Juli].

5. Ökonomische Betrachtung einer Zertifizierungsstelle in der Schweiz

Im folgenden Kapitel wird auf die Problematik der Verbreitung digitaler Signaturen sowie auf deren Einsatzgebiete eingegangen. Anschliessend werden die Merkmale des Schweizer Zertifikatsmarktes dargestellt und erläutert.

Verbreitung von digitalen Signaturen

Schlagworte wie E-Government, E-Banking, E-Identitätskarte – um nur einige zu nennen – prägten das Ende des 20. und den Beginn des 21. Jahrhundert. Nach Erlass der SiRL war in sämtlichen europäischen Ländern ein klarer Trend zu erkennen, künftig alle Geschäfte nur noch elektronisch zu betätigen. Doch auf die anfängliche Euphorie folgte sodann die Ernüchterung: Unter den Endanwendern, hauptsächlich den Privatpersonen, ist die digitale Signatur nicht bekannt und dementsprechend besteht auch kein Bedürfnis, diese anzuwenden. Gleichzeitig verloren Unternehmen riesige Summen an Geld in Internetprojekten, was die Einführung der digitalen Signatur mangels Finanzierungsmöglichkeiten und mangels Anwendungsmöglichkeiten verzögert. Auch der Bund ist von Sparmassnahmen betroffen und hat Pläne wie die Schaffung einer elektronischen Identitätskarte (eID) wieder eingestellt.[81]

Nach der neusten Medienmitteilung des Kantons Zürich fordert der Regierungsrat den Bund jedoch auf, das Projekt der Einführung der digitalen Identitätskarten umgehend wieder aufzunehmen, mit der Begründung, dass nur mit einer solchen Lösung der elektronische Geschäftsverkehr zwischen Verwaltungen, Unternehmen sowie Einwohnerinnen und Einwohnern sicher und vertraulich ablaufen sowie der Datenschutz und die Rechtssicherheit gewährleistet werden kann.[82] Demnach gibt es durchaus sinnvolle Anwendungen für die qualifizierte elektronische Signatur. Im Folgenden wird auf verschiedene Einsatzgebiete der digitalen Signatur beziehungsweise der qualifizierten Zertifikate eingegangen. Die vorgeschlagenen Bereiche sind nicht abschliessend und unterliegen einer kritischen Würdigung.

5.1.1. E-Government

Steuererklärungen elektronisch ausfüllen, online abstimmen und wählen, Registerauszüge übers Internet direkt nach Hause bestellen - solche Vorgänge werden unter dem Begriff E-Government zusammengefasst. Mittels E-Government stellt der Staat seine Dienstleistungen rund um die Uhr zur Verfügung und möchte dadurch eine höhere Transparenz und Flexibilität in der Verwaltung erreichen.[83]

Der Vorteil digitaler Signaturen im amtlichen Umfeld lässt sich am Beispiel der elektronischen Steuererklärung veranschaulichen. Bisher konnten Steuererklärungen wohl elektronisch ausgefüllt werden, jedoch war eine eigenhändige Unterschrift am Ende doch notwendig, weshalb viele den herkömmlichen Weg bevorzugten. Der Einsatz der qualifizierten digitalen Signatur würde dieses Problem beheben und es könnten enorme Kosten im Bereich der Dateneingabe sowie Portokosten seitens der Steuerbehörde eingespart werden.

---

[81] Vgl. Palumbo [2004, 16. Mai].

[82] Vgl. SDA – Basisdienst [2004, 24. Juli].

5.1.2. Elektronische Vertragsabschlüsse

Dort wo bei elektronischen Verträgen das Gesetz die Schriftlichkeit als gegenseitige Willensübereinstimmung verlangt, wird die digitale Signatur angewendet.[84] Somit können Privatpersonen Verträge mit Versicherungen, Banken etc. bequem von zu Hause aus unterschreiben.

Ursprünglich wurde hier ein riesiges Potential für digitale Signaturen gesichtet. Weil Verträge aber auch mündlich oder über E-Mail abgeschlossen werden können und somit keine Schriftlichkeit, beziehungsweise keine digitale Signatur verlangen, wird hier die elektronische Unterschrift doch nicht den Erwartungen entsprechend benötigt.[85]

Bei Vertragsabschlüssen im Business to Consumer-Bereich geht meistens eine persönliche Beratung voran, womit eine Kundenbeziehung zwischen Unternehmen und Kunde aufgebaut wird. Der Aufwand, bei einem gemeinsamen Treffen die Verträge unmittelbar zu unterschreiben, ist somit kleiner als die Signaturerzeugungsprozedur. Durch das Wegfallen des persönlichen Kundenkontaktes hätte die Unternehmung kaum Gelegenheit, ein Vertrauensverhältnis und somit eine Kundenbindung aufzubauen. Gerade in gesättigten Märkten wie beispielsweise im Versicherungs- oder Bankenmarkt ist dies aber äusserst wichtig.

5.1.3. Gesundheitsbereich und Gesundheitskarte

Im medizinischen Bereich können elektronische Signaturen zur Datenübertragung von Arzt zu Arzt, von Labor zu Arzt, von Arzt zu Krankenkassen zum Einsatz kommen. Eine Veränderung von Patientendaten während der Übermittlung hätte fatale Folgen, weshalb die Dateninteg rität hier besonders zu überprüfen ist.[86]

Ein zurzeit in der Presse viel diskutiertes Projekt ist die Einführung einer Gesundheitskarte in Deutschland. Diese Karte würde zunächst als Speicher für elektronische Rezepte fungieren. Ein freiwilliger Ausbau der Karte mit Informationen über medizinische Daten, Notfallversorgung, Arzneimittel und mit elektronischem Arztbrief sowie elektronischer Patientenkarte ist bereits geplant.[87] Die digitale Signatur kommt dann in Frage, wenn die Ärzte auf die Gesundheitskarte zugreifen wollen um Dokumente zu signieren, oder wenn der Patient - durch die Signatur autorisiert - seine Patientendaten auf dem Server einsehen möchte.[88] Obwohl das Projekt vorerst nur für Deutschland besteht und eine Umsetzung frühestens im Jahre 2006 erwartet wird, könnte eine Gesundheitskarte auch in der Schweiz Einzug nehmen. Wäre dies tatsächlich der Fall, so müssten alle Einwohner der Schweiz über eine qualifizierte digitale Signatur verfügen, was sich wiederum positiv auf die Ausstellung von Zertifikaten auswirken würde.

5.1.4. Jobkarte

Ein weiteres Projekt Deutschlands ist die Jobkarte. Diese soll Zugriff auf die Daten aller Arbeitnehmer ermöglichen, beispielsweise zu den Beschäftigungszeiten, zur Entlöhnung sowie

---

[83] Vgl. Eidgenössisches Finanzdepartement [2002].

[84] Vgl. Stejskal [2003] S. 30.

[85] Vgl. Gespräch mit Swisskey.

[86] Vgl. Dörr [2003] S. 31f.

[87] Vgl. Schulzki-Haddouti [2004, Heft Nr. 10].

[88] Vgl. Neue Zürcher Zeitung [2004, 23. Juli].

zur Auflösung des Arbeitsverhältnisses. «*Damit sollen Verwaltungsabläufe der Arbeitsämter und der Stellenvermittlungsbüros beschleunigt werden.*»[89] Auch hier wird die Umsetzung des Projektes nicht vor 2007 erwartet, aber die Einführung der Jobkarte gehört neben der Gesundheitskarte zum grössten Kartenprojekt Deutschlands. Um keine neuen Infrastrukturen aufbauen zu müssen, stützt sich das Verfahren der Jobkarte auf vorhandene Strukturen, namentlich auf das Signaturverfahren. Die Karte selbst wird in diesem Zusammenhang als Schlüssel, um die zentral abgespeicherten Informationen frei zuschalten, dienen. «*Für die Ausstellung einer Jobkarte ist die persönliche Erscheinung des Arbeitnehmers bei einer Registrierungsstelle notwendig, worauf die Schlüssel und Zertifikate durch ein Trustcenter erstellt werden.*»[90] Allerdings ist, wie bei der Gesundheitskarte auch, zu beachten, dass hochsensible Daten in einer zentralen Datenbank für Angreifer zu Spionagezwecken äusserst verlockend sind. Dementsprechend müssen Systeme entwickelt werden, welche nach aussen vollständig abgesichert werden können.

Falls die Jobbkarte in Deutschland einen grossen Erfolg verzeichnet, wäre deren Einführung auch in der Schweiz denkbar. Die für die Jobkarte und Gesundheitskarte benötigten Zertifikate würden dem Zertifikatsmarkt einen erheblichen Aufschwung geben.

5.1.5. E-Invoicing

Unter diesem Begriff wird die rein elektronische Rechnungsabwicklung verstanden. Damit der frühere Papierbeleg, welcher als Urbeleg für die Steuerverwaltung notwendigerweise vorhanden sein musste, durch eine elektronische Beglaubigung ersetzt werden kann, braucht es für den Integritätsschutz die digitale Signatur. Durch E-Invoicing können die Gesamtprozesskosten beachtlich reduziert werden. Beim Rechnungssteller entfallen der Druck, die Verpackung und der Versand der Rechnung, beim Rechnungsnehmer werden die Arbeitsschritte stark vereinfacht.[91]

5.1.6. Elektronische Archivierung von Geschäftsakten

Die Frage nach der elektronischen Archivierung ist nach einem vollständig digital abgeschlossenen Geschäft berechtigt. Gemäss Verordnung über die Führung und Aufbewahrung der Geschäftsbücher vom 24. April 2002 Art. 2 Abs. 2 ist es zulässig, Dokumente elektronisch zu archivieren. Hingegen muss dabei beachtet werden, dass nur dann veränderbare Informationsträger eingesetzt werden können, wenn ein technisches Verfahren zur Anwendung kommt, welches die Integrität der gespeicherten Informationen gewährleistet (z.B. digitale Signaturen).[92] Offen bleibt aber, ob zu diesem Zweck qualifizierte elektronische Signaturen verwendet werden müssen, oder ob eine „normale“ digitale Signatur ausreicht.[93]

[89] Schulzki-Haddouti [2004, Heft Nr. 10].

[90] Schulzki-Haddouti [2004, Heft Nr. 13].

[91] Vgl. Gatti [2004, 17. März].

[92] Vgl. Art. 9 Abs. 1 GeBüV.

[93] Vgl. Stejskal [2003] S. 35.

Vertrauenswürdigkeit von Zertifikaten mit Schweizer Qualität

Das Vertrauen in ein Zertifikat hängt vom Aussteller und dessen angegliederten Registrierungsstellen ab.[94] Je nach dem, ob ein Zertifikat über ein Online-Formular beantragt wird, oder ob für die Registrierung ein persönliches Erscheinen nötig ist, wird diesem Zertifikat sicherlich eine höhere Verlässlichkeit zugeschrieben. Die Annahme, dass einer staatlich anerkannten Zertifizierungsstelle das grösste Vertrauen entgegengebracht werden würde, ist unberechtigt, im Gegenteil, Zertifizierungsanbietern, welche den landeigenen Gesetzen entsprechen, kann, unabhängig von deren Ort oder deren Ansiedelung, ohnehin in höchstem Masse vertraut werden.[95] Ausserdem identifiziert sich der Nutzer, wie bereits erwähnt, über die Registrierungsstellen und ob diese danach den Antrag ins Ausland, zu einer privaten Zertifizierungsinstanz oder einer staatlichen Zertifizierungsstelle weiterleiten, spielt für den Kunden schlussendlich keine Rolle. Wichtig ist, dass die Registrierungsstellen die Antragsteller nach Vorschrift überprüfen und dass die Zertifizierungsstellen einen gesetzesgemässen Betrieb führen. Die Schweiz muss für die zuverlässige Zertifikatsausgabe die Registrierung so regeln, dass die Prozesse für alle Beteiligten transparent dargestellt werden.

Strukturen und Attraktivität des Zertifikatmarktes

Ein Grund für die bisherige schleppende Verbreitung der digitalen Signatur stellt das so genannte Huhn-Ei-Problem dar, «welches besagt, dass wegen der fehlenden Anwendungen sich niemand ein Zertifikat beschafft und wegen der fehlenden Zertifikate niemand eine Anwendung dafür bereitstellt.»[96] Der Einsatz der digitalen Signatur muss von allen Seiten gutgeheissen werden. Die fehlende Akzeptanz von bloss einem Part genügt, dass sich die digitale Signatur nicht durchsetzt. In der Schweiz ist genau diese Situation eingetreten und die digitale Signatur besitzt folglich ein Nischendasein.

Dies liegt zum einen daran, dass die Endanwender den Nutzen der digitalen Signatur nicht kennen, ihn beziehungsweise noch nicht entdeckt haben. Für die Privatpersonen ist die Anschaffung eines qualifizierten Zertifikates mit grossem Aufwand verbunden und die finanzielle Investition lohnt sich nicht, wenn berücksichtigt wird, dass die digitale Signatur nur wenige praktische Anwendungsbereiche hat. «*Dem Kunden können nur dann direkte Kosten auferlegt werden, wenn er diese von Gesetzes wegen übernehmen muss oder er selbst einen hohen Mehrwert sieht.*»[97] Bis jetzt konnte dieser Mehrwert aber noch nicht aufgezeigt werden und es besteht auch keine gesetzliche Verankerung, dass jeder Schweizer Bürger im Besitz eines selbst finanzierten, qualifizierten Zertifikats sein muss. Schliesslich kann er, wo die Schriftlichkeit erfordert wird, gratis seine eigenhändige Unterschrift benutzen. Die Lösung

[94] Vgl. Marzetta et al. [2001] S. 12.

[95] Marzetta et al. [2001] deklarieren auf Seite 12 den Staat als vertrauenswürdigste Instanz.

[96] Marzetta et al. [2001] S. 8.

[97] Wildhaber [2002] S. 18.

dieses Problems ist eine indirekte Amortisierung der Zertifikatskosten.[98] Denkbar wäre das Szenario, dass die Steuerbehörden diese Kosten übernehmen, da sie durch die elektronische Steuererklärung erhebliche Kosten einsparen können.[99] Damit entsteht aber wiederum ein neuer Konflikt: Andere potentielle Anwendungen in der Privatwirtschaft werden dadurch indirekt subventioniert und daran hat der Staat kein Interesse, da er nicht als alleiniger Geldgeber für Zertifikate fungieren möchte. Damit wäre der Teufelskreis wieder geschlossen.

Zum anderen liegt es an der fehlenden Zusammenarbeit zwischen Staat und Wirtschaft. Während der Staat abwartet, bis die Wirtschaft eine geeignete Lösung hinsichtlich des fehlenden Business-Case und des Aufbaus einer anerkannten Zertifizierungsstelle liefert, erwartet die Wirtschaft ihrerseits, dass der Staat diese Problematik endlich in die Hand nimmt.[100] Die hohen technischen und organisatorischen Anforderungen an eine anerkannte Zertifizierungsstelle sind für die Wirtschaft in realistischer und rentabler Weise nicht umzusetzen.[101] Da ändert auch die Tatsache nichts, dass eine heute eingerichtete anerkannte Zertifizierungsstelle eine Monopolsituation und somit einen Wettbewerbsvorteil in der Schweiz hätte. Auch für den Staat sind die Kosten einer staatlichen Zertifizierungsstelle zu hoch und er verzichtet deshalb auf ein „Service-Public“-Angebot.

Gezielte Zusammenarbeit wäre zweifellos hilfreich. Die existierenden privaten Anbieter von Zertifizierungsdiensten versuchen sich durch eigene Produkte zu profilieren. Die Banken haben mit anderen Lösungen den digitalen Signatureinsatz ausgeklammert und dieser wird deshalb vorerst auch nicht weiter verfolgt. Die bestehenden Zertifikate beschränken sich auf interne PKI-Systeme und können nicht an mehreren Orten eingesetzt werden. Derartige Entwicklungen zielen keineswegs auf einen gemeinsamen Nenner und sind für den öffentlichen Betrieb einer anerkannten Zertifizierungsstelle kontraproduktiv. Würden Staat und Wirtschaft gemeinsam an Projekten für den Signatureinsatz arbeiten und nicht für jede Anwendung ein anderes Zertifikat verlangen, könnte längerfristig ein Zertifikatsbedürfnis geschaffen werden.

5.1.7. Hohe Markteintrittsbarrieren

Die Akkreditierung von Anerkennungsstellen durch die Akkreditierungsstellen ergeben bei einem derart kleinen Markt keinen grossen Sinn und bildet für künftige anerkannte Zertifizierungsstellen eine Hürde, in den Markt einzutreten, obwohl diese nur indirekt tangiert sind. Zudem verursachen solche Anerkennungsverfahren riesige Kosten, welche für andere Zwecke verwendet werden können. Sinnvoller wäre die direkte Anerkennung der in- und ausländischen Zertifizierungsstellen durch die SAS.[102] Trotz den sehr hohen gesetzlichen Anforderungen werden weder in der Verordnung (VZertES) noch im ZertES selbst konkrete Aussagen zur Umsetzung gemacht. Zwar sind einige materielle Angaben verankert, aber die wichtigen Daten, insbesondere bei der technischen Umsetzung, fehlen. Ausserdem wird durch

[98] Vgl. Wildhaber [2002] S. 18.

[99] Vgl. Ziff. 5.1.1 (E-Government).

[100] Vgl. Sonntags Zeitung [2001, 11. November] und Neue Zürcher Zeitung [2001, 11. Mai].

[101] Vgl. Gespräch mit SwissCERT.

[102] Vgl. Stellungnahme zur VZertES [2004, 26. Juni].

die jetzige Haftungsregelung die Möglichkeit der Versicherbarkeit stark eingeschränkt.[103] Die grossen finanziellen Investitionen in eine Anerkennung sowie der fehlende Business-Case für qualifizierte Zertifikate macht die Branche zusätzlich unattraktiv.

[103] Vgl. Anhang C (Haftpflichtversicherung der Zertifizierungsstellen) und Ziff. 4.1.6 (Haftung und Versicherung).

6. Mögliche Strategien für eine anerkannte Zertifizierungsstelle in der Schweiz

Bevor auf die Strategieentwicklungen und deren Beurteilungen eingegangen wird, soll zuerst die Lage in der Schweiz dargestellt werden. Damit verbunden ist auch ein Blick auf die Situationen in den Nachbarländern.

Ausgangslage

Die Schweiz verfügt momentan nur über private Anbieterinnen von Zertifizierungsdiensten. Trotz des eher unattraktiven Marktes ist diese Situation für die Entwicklungen im E-Business und für potentielle Signaturanwender unbefriedigend. Bis jetzt wurden noch keine geeigneten Lösungen gefunden, eine anerkannte Zertifizierungsstelle zu errichten, obwohl von Wirtschaft und Staat eine solche begrüsst würde.

Zunächst wird am Beispiel der Firma Swisskey AG aufgezeigt, wo die Probleme einer Zertifizierungsstelle liegen und wo Verbesserungen angebracht werden könnten. Warum die Akkreditierung nicht in Frage kommt und weshalb der private Betrieb als äusserst interessant eingeschätzt wird, soll an der privaten Zertifizierungsstelle SwissCERT AG dargelegt werden. Schlussendlich zeigt das Beispiel der SwissSign AG, dass die Anerkennung dennoch lukrativ sein kann. Die Inhalte der folgenden Kapitel gehen aus persönlichen Gesprächen mit den jeweiligen Firmen hervor.

6.1.1. Swisskey AG: Vergangenheit einer potentiell anerkannten Zertifizierungsstelle

Die Swisskey wurde 1998 von der Swisscom, der Telekurs Holding AG und Digisigna, dem Verein der Handelskammern der Schweiz und des Fürstentums Liechtenstein gegründet. Swisskey erfüllte als einzige Zertifizierungsdiensteanbieterin in der Schweiz die Voraussetzungen für eine Anerkennung, musste ihre Dienste aber, aus Mangel an verkauften Zertifikaten im Jahre 2001 wieder einstellen.

Swisskey war als öffentliche Zertifizierungsstelle tätig und stellte hauptsächlich Zertifikate für Privatpersonen aus, wovon im Jahre 2001 ungefähr 10'000 im Umlauf waren. Gleichzeitig arbeitete Swisskey an der Ausarbeitung der Zertifizierungsdiensteverordnung (ZertDV) mit und hatte somit sowohl zur Wirtschaft als auch zum Staat engen Kontakt. Zum Zeitpunkt ihrer Tätigkeit war Swisskey nicht akkreditiert, weil diese damals weder in einer Verordnung noch in einem Gesetz verankert war. Hätte Swisskey aber das Inkrafttreten der ZertDV längerfristig überlebt, wäre einer Anerkennung nichts im Wege gestanden.

Auflösung von Swisskey AG

Einerseits hatte Swisskey mit technischen Sicherheitsproblemen zu kämpfen, welche nach wie vor nicht gelöst sind. Andererseits ist, wie bereits erwähnt, die digitale Signatur unter den Privatanwendern nicht bekannt. Um einen Gewinn zu erwirtschaften, hätte Swisskey mindestens eine Million Zertifikate verkaufen müssen. Ausserdem bemerkten die Banken erst später, dass die Swisskey-Zertifikate ebenso gut bei der Konkurrenz eingesetzt werden können und sie waren deshalb nicht bereit, für ihre Kunden Mehrzweckzertifikate anzuschaffen.[104]

[104] Vgl. Wildhaber [2002].

Nach der Auflösung von Swisskey sind viele Firmen einen Schritt zurückgegangen und haben ihre elektronischen Identitäten wieder selbst gemanagt.[105] Politiker forderten, der Bund solle aktiv werden und die notwendige Infrastruktur zu Verfügung. Eine Studie bezüglich einer schweizerischen digitalen Identitätskarte sollte als Entscheidungsgrundlage dienen. Darin werden jedoch keine konkreten Empfehlungen gemacht.[106] Die Folge war, dass Staat und Wirtschaft einfach abwarteten. Damit ist das Problem aber nicht gelöst, im Gegenteil, die jetzige Situation verlangsamt die Fortschritte im E-Business und die Entwicklung der Schweiz zur Informationsgesellschaft.

Misserfolgsfaktorenanalyse von Swisskey AG

Misserfolgsfaktor	Beschreibung	Verbesserungsvorschlag
Fehlende Applikationen	Wenige Anwendungsmöglichkeiten für die digitale Signatur	Ausübung von Druck für die Entwicklung entsprechender Applikationen
Fehlende Akzeptanz der Nutzer	Unbekanntheit der digitalen Signatur Undurchschaubares Konzept	Gezieltes Marketing an die breite Öffentlichkeit
Falsche Schwerpunkte gesetzt	Energie in Ausarbeitung der ZertDV gesteckt Folge: keine Pflege der Kundennähe, wenig Eingehen auf Kundenbedürfnisse	Grössere Konzentration auf Kundenbeziehungen zur Förderung der Akzeptanz der digitalen Signatur
Konzentration auf den B2C-Bereich	Zertifikatsausstellung für Privatpersonen	Konzentration der Klientel auf den B2B-Bereich

Tabelle 2: Misserfolgsfaktorenanalyse der Firma Swisskey AG

(Quelle: Eigene Darstellung in Anlehnung an Gespräch mit Swisskey AG)

Trotz der Fehlschläge verzeichnete Swisskey auch einige Erfolge. So nahm sie als erste Zertifizierungsstelle in der Schweiz eine Pionierrolle ein und hat dadurch die nötigen politischen Prozesse angestossen. Gleichzeitig war sie als offizielle Zertifizierungsstelle vom Staat akzeptiert. Obwohl Swisskey zu wenige Zertifikate im Umlauf hatte, war die Anzahl verkaufter Zertifikate im Verhältnis zu den europäischen Nachbarländern dennoch nicht unter dem Durchschnitt.[107]

6.1.2. SwissCERT AG und SwissSign AG: praktizierende private Zertifizierungsstellen

SwissCERT, 2001 gegründet, versucht sich zu profilieren, indem sie Zertifikate im Angebot hat, welche zu mehreren Zwecken verwendet werden können ohne dass sich die verschiedenen Applikationsanbieter konkurrenziert sehen. Die Banken beispielsweise benötigen eine spezielle Lizenz, um das Signaturverfahren auf Kundenzertifikate von SwissCERT anzuwen-

[105] Vgl. Bossard [2004, 20. Februar].

[106] Vgl. Sonntags Zeitung [2001, 11. November].

[107] Vgl. Ziff. 6.1.3 (Blick ins Ausland).

den. Auf diese Weise wird der gewünschte Investitionsschutz erreicht, da die Konkurrenz die SwissCERT-Zertifikate ohne Kostenbeteiligung nicht nutzen kann.[108] Zu den Kunden von SwissCERT zählen hauptsächlich Firmen, welche keine eigene PKI besitzen, die digitale Signatur aber dennoch intern und für Kunden verwenden möchten.

Gründe für keine Akkreditierung

Kriterium	Begründung
Unrealistisches Gesetz	Keine Umsetzung des ZertES in realistischer Form Unausführbarkeit der Haftungsregelung
Keine Sicherheitsgarantie bei den Privatanwenderprogrammen	Sicherheitslücken in Anwenderprogramme der privaten Computer[109]
Kein Business-Case für qualifizierte Zertifikate	Keine geeigneten Applikationen für qualifizierte Zertifikate Fehlende Bekanntheit der digitalen Signatur[110]
Hohe Kosten für Akkreditierung	Kosten der Akkreditierung: zwischen CHF 180'000 und CHF 450’000 Keine Garantie für höheren Umsatz

Tabelle 3: Gründe für keine Akkreditierung der SwissCERT AG
(Quelle: Eigene Darstellung in Anlehnung an Gespräch mit SwissCERT AG)

Die Produkte von SwissCERT sind so konzipiert, dass eine spätere Anerkennung durchaus möglich wäre womit die Akkreditierung nicht gänzlich ausgeschlossen wird.

Trotz diesen für eine Akkreditierung negativen Ergebnissen strebt die private Zertifizierungsstelle SwissSign die Anerkennung an. Anders als SwissCERT und Swisskey möchte sie die Zertifikate für die Kunden gratis zur Verfügung stellen. Dabei muss jedoch beachtet werden, dass für die Registrierung nach wie vor Kosten bestehen, welche vom Nutzer übernommen werden. SwissSign hebt sich dadurch von den anderen Zertifizierungsstellen ab, dass sie eine eigene PKI-Software entwickelt hat, welche den gesetzlichen Anforderungen entspricht. Obwohl auch SwissSign bestätigt, dass kein Business-Case für qualifizierte Zertifikate in der Schweiz besteht, möchte sie durch gezielte Schaffung von Applikationen in enger Zusammenarbeit mit Applikationsanbietern einen solchen erarbeiten. Deshalb läuft die Finanzierung dieser Zertifizierungsstelle viel mehr über den Vertrieb der eigenen Software als über den Zertifikatsverkauf.

6.1.3. Blick ins Ausland

Nach Erlass der Signaturrichtlinie und nachdem die nötigen Infrastrukturen und Gesetze erstellt worden sind, klagen auch die europäischen Nachbarländer über mangelnde Anwendungsmöglichkeiten der digitalen Signatur. Die EU sieht vor allem im E-Government grosses Potential für den Signatureinsatz, weshalb viele Staaten auf eine elektronische Identitätskarte setzen. Diese soll sowohl das Tor zum virtuellen Rathaus öffnen als auch für andere An-

[108] Vgl. SwissCERT Cute [2004, 27. Juli].

[109] Vgl. Ziff. 4.1.10 (Computerbasierte Sicherheit).

[110] Vgl. Ziff. 0 (Strukturen und Attraktivität des Zertifikatmarktes).

wendungen nützlich sein. In Italien zum Beispiel werden eID's bald für alle 40 Millionen Einwohner zur Verfügung stehen, aber auch Frankreich und Österreich planen deren Einführung.[111] Ob die elektronische Identitätskarte aber von den Bürgern beantragt wird und ob sie sich national verbreiten wird, kann nicht abgeschätzt werden. Fest steht, dass in Finnland, welches bezüglich elektronischer Identitätskarte eine Pionierrolle einnimmt, im Jahre 2002 nur gerade 0,2 Prozent der Bevölkerung eine elektronische Identitätskarte beantragten.[112] Dennoch verspricht sich die EU mit der digitalen Identitätskarte das Identifikationsmittel der Zukunft.[113]

Diesen Entwicklungen entsprechend werden zum jetzigen Zeitpunkt auch in Europa die Zertifizierungsstellen nicht von Anträgen überrannt, im Gegenteil, die Situation darf mit derjenigen in der Schweiz verglichen werden: Wenige Applikationen, dementsprechend wenige Zertifikate und kein Signaturbedürfnis seitens der Bevölkerung.

Praxisbeispiel Österreich

Obwohl sich oben genannte Entwicklungen auch in Österreich abzeichnen, ist dieses Land in der aktuellen eEurope-Studie der Europäischen Kommission auf den vorderen Plätzen gelandet.[114] Erklären lässt sich dies am neu lancierten E-Government Gesetzt, welches eine zentrale Regelung des E-Government verfolgt. Dies bleibt auch für die nationalen Zertifizierungsstellen nicht ohne Folgen.

A-Trust ist eine Tochter österreichischer Banken, inklusive der Nationalbank sowie der Telekom Austria, der Wirtschaftskammer und der Rechtsanwalts- und Notariatskammer wurde im Jahre 2002 akkreditiert. Schon bei ihrer Gründung im Jahre 1999 steckte sie die Ziele hoch: In fünf Jahren sollen 300'000 Chipkarten mit elektronischen Signaturen im Umlauf sein.[115] Der erwartete Erfolg blieb aber aus, derzeit sind bei A-Trust lediglich 30'000 Nutzer registriert.[116] Mit der Einführung der Bürgerkarte erhofft sich A-Trust einen enormen Kundenzuwachs und eine gleichzeitige Verbreitung der digitalen Signatur.

Warum A-Trust aber nicht mangels Kunden ihre Dienste wieder einstellen musste, lässt sich daran erklären, dass A-Trust anfänglich hauptsächlich Firmen oder Behörden als Zielgruppe definiert hat.[117] Zudem scheint es für die österreichischen Banken kein Problem zu sein, mit Mehrzweckzertifikaten zu arbeiten. Da A-Trust in Österreich eine Monopolsituation als einzige anerkannte Zertifizierungsstelle einnimmt und ein hervorragendes Marketing betreibt, funktioniert auch die Zusammenarbeit mit Staat und Wirtschaft. Auch Kooperationen mit Informatikfirmen scheinen zu bestehen, denn A-Trust konnte ihre Stammzertifikate in Microsoft Betriebssysteme integrieren, womit ein grosser Schritt in Richtung Userfreundlichkeit beim Einsatz von Zertifikaten erreicht wurde.[118]

---

[111] Vgl. Palumbo [2004, 16. Mai].

[112] Vgl. Oppliger [2002, 29. November].

[113] Vgl. SDA-Basisdienst [2004, 23. Juli].

[114] Vgl. Government Computing [2004, 17. Mai].

[115] Vgl. Polster [1999, 10. Juli].

[116] Vgl. Konar [2004, 24. Februar].

[117] Vgl. Polster [1999, 10. Juli].

[118] Vgl. A-Trust [2004, 9. August].

Strategieentwicklungen

Eine anerkannte Zertifizierungsstelle leistet ihren Beitrag zur Weiterentwicklung des E-Business und des E-Government. Bevor über die Einführung einer elektronischen Identitätskarte in der Schweiz diskutiert wird, sollte sie vorerst in der Lage sein, qualifizierte Zertifikate herauszugeben. Die Bemühungen ein eID-Projekt, welches schlussendlich aber mangels anerkannter Zertifizierungsstelle nicht umzusetzen ist, auszuarbeiten, würden sich nicht lohnen. Allenfalls würde die Gewissheit, eine anerkannte Zertifizierungsstelle errichten zu können, die Verbreitung der digitalen Signatur in der Schweiz beschleunigen.

Da der Markt, wie aus oben stehenden Ausführungen hervorgegangen ist, nicht besonders attraktiv ist und anzunehmen ist, dass die Bevölkerung den qualifizierten Zertifikaten anfangs sehr zurückhaltend gegenüberstehen wird, muss berücksichtigt werden, dass die Zertifizierungsinfrastruktur den Gegebenheiten angepasst wird. Erfahrungen im Ausland zeigen, dass es reicht, wenn die Zertifizierungsstelle zu Beginn nur 1000 bis 5000 qualifizierte Zertifikate verwalten kann. Eine grosse Zertifizierungsstelle kann wegen den damit verbundenen immensen Kosten längerfristig nicht finanziert werden.

Der Betrieb einer kleinen Zertifizierungsstelle reduziert Verwaltungs- und Personalaufwände und kann somit Kosten einsparen. Sobald die Nachfrage nach qualifizierten Zertifikaten vorhanden ist und dementsprechend ein grösserer Umsatz erwirtschaftet wird, ist eine Aufstockung möglich. Wichtig dabei ist, dass der Fokus nicht nur auf die nächsten drei Jahre gerichtet wird, sondern auf die nächsten zehn bis zwanzig Jahre. Verzeichnet eine Zertifizierungsstelle in den ersten Jahren keinen hohen Gewinn, schreibt sie gar rote Zahlen, so kann sie über mehrere Jahre hinweg dennoch erfolgreich sein. Dies setzt aber voraus, dass genügend finanzielle Mittel vorhanden sind, was vor allem durch möglichst tief gehaltene Kosten erreicht werden kann. Im Folgenden werden einige Strategien erläutert, welche diese Begebenheiten berücksichtigen.

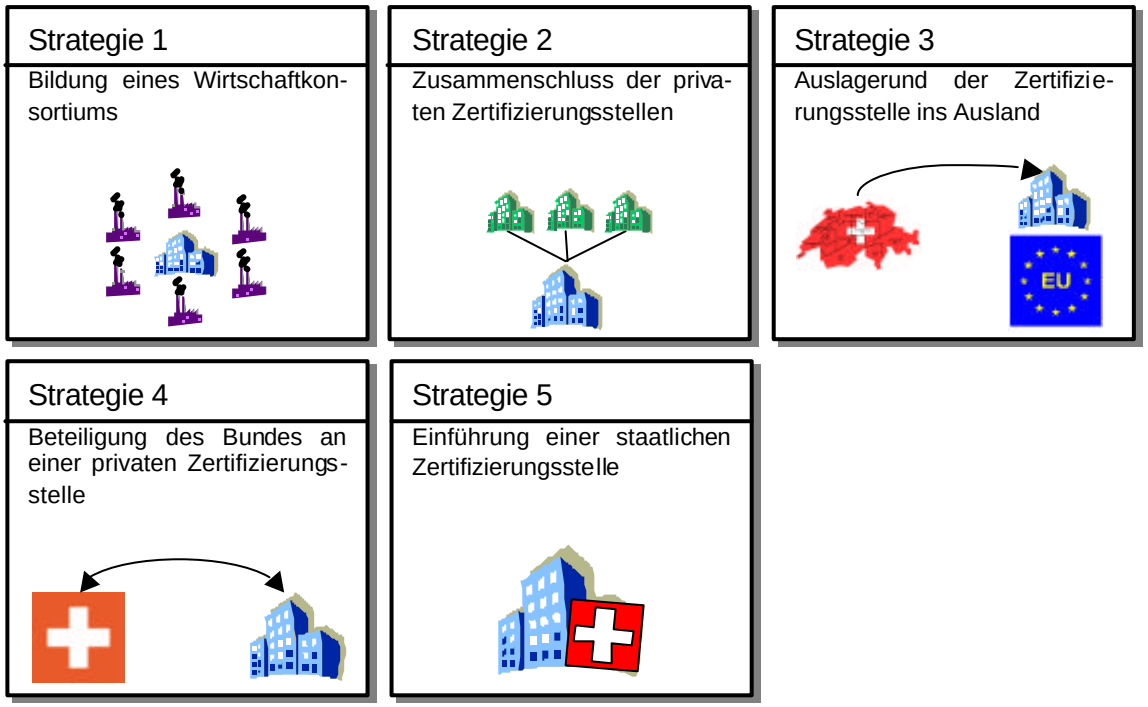


Abbildung 10: Übersicht über die zu diskutierenden Strategien
(Quelle: Eigene Darstellung)

6.1.4. Strategie 1: Bildung eines Wirtschaftskonsortiums

Für die Bildung eines Wirtschaftskonsortiums, welches den Aufbau und Betrieb einer Zertifizierungsstelle gänzlich finanziert, sind mehrere Beteiligungen aus den verschiedenen Branchen des Dienstleistungssektors nötig. Somit können alle Meinungen hinsichtlich der Einsatzgebiete der digitalen Signatur berücksichtigt werden und es entstehen keine Konflikte innerhalb der jeweiligen Zweige. Das Zertifizierungsstellen-Team wird vom Konsortium bestimmt. Auch die Räumlichkeiten werden zur Verfügung gestellt, wobei denkbar ist, dass die Zertifizierungsstelle ihren Sitz innerhalb einer dem Konsortium beigetretenen Firma hat. Die Zertifikatskosten für die Kunden müssen möglichst niedrig gehalten werden. Durch gezielte Zusammenarbeit beispielsweise auch mit dem Staat können die Kosten möglicherweise gar gänzlich von den Mitgliedern übernommen werden. Als Registrierungsstellen könnten die Poststellen auftreten, welche dank ihrer landesweiten Verteilung für die Antragsteller gut zu erreichen sind.

Bei der Ausarbeitung von Applikationen für die digitale Signatur ist auf eine Zusammenarbeit innerhalb der einzelnen Zweige, sowie zwischen Konsortium und Zertifizierungsstelle zu achten. Wichtig dabei ist der ständige Dialog zwischen den einzelnen Vertretern, damit gezielt auf einen gemeinsamen Nenner, nämlich ein Mehrzweckzertifikat, hingearbeitet werden kann. Vorstellbar bei dieser Strategie wäre auch, dass öffentliche Ämter dem Konsortium beitreten können, womit auch der Staat seine Interessen vertreten könnte.

Kostenschätzung der Zertifizierungsstelle über 5 Jahre[119]		
	Initialaufwand	Aufwand pro Jahr
Anerkennungsprozess	CHF 300'000	CHF 40'000
Grundinfrastruktur	CHF 500'000	CHF 178'000
Versicherung (exkl. Vermögenshaftpflicht)	CHF 0	CHF 52'800
Personal Zertifizierungsstelle	CHF 0	CHF 600'000
Instruktion und Entschädigung der Registrierungsstellen (ca. 2700 Poststellen)	CHF 540'000	CHF 225'000
Marketing	CHF 600'000	CHF 300'000
Total	CHF 1'940'000	CHF 1'395'800
Gesamtkosten für 5 Jahre	CHF 8'919'000	

Tabelle 4: Kostenschätzung Strategie 1
(Quelle: eigene Darstellung in Anlehnung an Marzetta et al. [2001] S. 60)

6.1.5. Strategie 2: Zusammenschluss der privaten Zertifizierungsstellen und anschliessende Anerkennung

Statt mit kleinen Insellösungen der einzelnen privaten Zertifizierungsstellen zu arbeiten, ist ein Zusammenschluss der privaten Zertifizierungsstellen und eine anschliessende Anerkennung denkbar. Dabei werden der Zertifizierungsstelle jedoch keine externen Geldquellen zur Verfügung gestellt. Die bestehenden Kunden werden zu gleichen Konditionen von der neuen Zertifizierungsstelle übernommen. Durch die Fusion ist das erforderliche Fachpersonal sowie die technischen Infrastrukturen bereits vorhanden, was eine grosse Kostenersparnis bewirken kann. Eigene Erfindungen könnten patentiert werden und finden auch bei qualifizierten Zertifikaten Anwendung.[120] Zu beachten ist, dass die Kosten für die Zertifikate entsprechend zwischen Applikationsanbieter und –nutzer aufgeteilt werden. Für die Registrierung ist eine Zusammenarbeit mit der Post oder mit bestehenden Kunden denkbar, denn die Zertifizierungsstelle kann wegen schlechter schweizweiter Erreichbarkeit nicht gleichzeitig auch als einzige Registrierungsstelle auftreten.

Die Zertifizierungsstelle ist, da sie bereits über Kundschaft verfügt, vorerst nicht auf das breite Publikum angewiesen, hätte jedoch zum Beispiel für die Einführung einer eID die nötige Infrastruktur bereit. Gerade durch das Fehlen von externer finanzieller Unterstützung muss die Zertifizierungsstelle besonders auf ein zweckmässiges Marketing achten und einen geeigneten Business-Case in Zusammenarbeit mit Wirtschaft und Staat erarbeiten.

[119] Vgl. Anhang B (Herleitung der Zahlen für die Kostenschätzung).

[120] Vgl. Ziff. 6.1.2 (SwissCERT und SwissSign: praktizierende private Zertifizierungsstellen).

Kostenschätzung der Zertifizierungsstelle über 5 Jahre[121]		
	Initialaufwand	Aufwand pro Jahr
Anerkennungsprozess	CHF 300'000	CHF 40'000
Grundinfrastruktur	CHF 100'000	CHF 178'000
Versicherung (exkl. Vermögenshaftpflicht)	CHF 0	CHF 52'800
Personal Zertifizierungsstelle	CHF 0	CHF 600'000
Instruktion und Entschädigung der Registrierungsstellen (ca. 2700 Poststellen)	CHF 540'000	CHF 225'000
Marketing	CHF 600'000	CHF 300'000
Total	CHF 1'540'000	CHF 1'395'800
Gesamtkosten für 5 Jahre	CHF 8'519'000	

Tabelle 5: Kostenschätzung Strategie 2
(Quelle: eigene Darstellung in Anlehnung an Marzetta et al. [2001] S. 60)

6.1.6. Strategie 3: Auslagerung der Zertifizierungsstelle ins Ausland

Für eine Auslagerung der Zertifizierungsstelle ins Ausland ist ein Eingreifen des Staates sicher sinnvoll. Dieser muss mit der ausländischen Zertifizierungsstelle über eine Zusammenarbeit hinsichtlich der zusätzlichen Versorgung der Schweiz mit qualifizierten Zertifikaten verhandeln. Die anschliessende Anerkennung würde vom Staat finanziert. Was die Zertifikatskosten für die Nutzer und Applikationsanbieter in der Schweiz betrifft, so wird entweder das System der ausländischen Zertifizierungsstelle übernommen oder ein eigenes Konzept in Zusammenarbeit der mit Wirtschaft erarbeitet.

Als Registrierungsstellen könnten die lokalen Einwohnerämter fungieren. Die Organisation, wie diese mit der ausländischen Zertifizierungsstelle vernetzt und finanziert werden, wird ebenfalls vom Staat übernommen. Denkbar ist eine Kostenaufteilung zwischen ausländischer Zertifizierungsstelle und Staat, wobei der grössere Aufwand zu Lasten des Staates geht. Auch das bereits bestehende Marketing kann, sofern es sinnvoll ist, mit wenigen Anpassungen auf die Schweiz angewendet werden.

Da die fremdländischen Zertifizierungsdiensteanbieter ebenfalls über mangelnde Kundschaft klagen[122], können sie mit einer Zusammenarbeit ohne grösseren Aufwand einen Kundenzuwachs verzeichnen. Gleichzeitig wird die Schweiz durch das Outsourcing, was die Zertifizierungsstellen angeht, entlastet und kann sich vollständig auf die Verbreitung der digitalen Signaturen konzentrieren.

[121] Vgl. Anhang B (Herleitung der Zahlen für die Kostenschätzung).

[122] Vgl. Ziff. 6.1.3 (Blick ins Ausland).

Kostenschätzung der Zertifizierungsstelle über 5 Jahre[123]		
	Initialaufwand	Aufwand pro Jahr
Anerkennungsprozess	CHF 300'000	CHF 40'000
Grundinfrastruktur	CHF 0	CHF 178'000
Versicherung (exkl. Vermögenshaftpflicht)	CHF 0	CHF 52'800
Personal Zertifizierungsstelle	CHF 0	CHF 150'000
Instruktion und Entschädigung der Registrierungsstellen (ca. 3000 Einwohnerämter)	CHF 600'000	CHF 225'000
Marketing	CHF 600'000	CHF 300'000
Total	CHF 1'500'000	CHF 945'800
Gesamtkosten für 5 Jahre	CHF 6'229'000	

Tabelle 6: Kostenschätzung Strategie 3
(Quelle: eigene Darstellung in Anlehnung an Marzetta et al. [2001] S. 60)

6.1.7. Strategie 4: Beteiligung des Bundes an einer privaten, anerkannten Zertifizierungsstelle[124]

In dieser Strategie wird eine private Zertifizierungsstelle vom Bund für die Anerkennung und für den weiteren Betrieb finanziell unterstützt. Damit nimmt der Staat aber nicht einfach nur die Geldgeberfunktion ein, sondern er sichert für sich selbst ein gewisses Mass an Einfluss. Die Zertifikatskosten könnten zwischen Bund, Wirtschaft und Nutzer aufgeteilt werden. Als Registrierungsstellen treten beispielsweise die Post, die Handelsregisterämter oder die Gemeindeverwaltungen auf.

Damit die Zertifizierungsstelle längerfristig selbst tragend wird, müssen sowohl Bund als auch Wirtschaft in geeignete Anwendungen investieren und die rasche Entwicklung und Verbreitung der digitalen Signatur vorantreiben. Das Marketing wendet sich zudem nicht nur an potentielle Zertifikatskäufer, sondern auch an die Entwickler und Betreiber der Anwendungen. Sind genügend Zertifikate verkauft und ist die Existenz der Zertifizierungsstelle gesichert, kann der Bund seinen Anteil verkaufen oder sich zurückziehen. Somit hat er nur anfängliche Starthilfe geleistet, um danach den Zertifikatsmarkt wieder der Wirtschaft zu überlassen.

Kostenschätzung der Zertifizierungsstelle über 5 Jahre[125]		
	Initialaufwand	Aufwand pro Jahr
Anerkennungsprozess	CHF 300'000	CHF 40'000

[123] Vgl. Anhang B (Herleitung der Zahlen für die Kostenschätzung).

[124] Vgl. Marzetta et al. [2001] S. 55ff.

[125] Vgl. Anhang B (Herleitung der Zahlen für die Kostenschätzung).

Kostenschätzung der Zertifizierungsstelle über 5 Jahre[125]		
	Initialaufwand	Aufwand pro Jahr
Grundinfrastruktur	CHF 0	CHF 178'000
Versicherung (exkl. Vermögenshaftpflicht)	CHF 0	CHF 52'800
Personal Zertifizierungsstelle	CHF 0	CHF 600'000
Instruktion und Entschädigung der Registrierungsstellen (ca. 2700 Poststellen)	CHF 540'000	CHF 225'000
Marketing	CHF 600'000	CHF 300'000
Total	CHF 1'440'000	CHF 1'395'800
Gesamtkosten für 5 Jahre	CHF 8'419'000	

Tabelle 7: Kostenschätzung Strategie 4
(Quelle: eigene Darstellung in Anlehnung an Marzetta et al. [2001] S. 60)

6.1.8. Strategie 5: Einführung einer staatlich anerkannten Zertifizierungsstelle[126]

In dieser Strategie richtet der Staat selbst im Hinblick auf die Einführung eines digitalen Ausweises eine anerkannte Zertifizierungsstelle ein, welche hauptsächlich durch den Bund finanziert wird. Dabei könnten die Behörden, welche auch die Pass- und Identitätskarten-Anträge bearbeiten, als Registrierungsstellen eintreten. Die Zertifikate werden aber nicht gratis an die Nutzer abgegeben, sondern können freiwillig gegen eine Gebühr bezogen werden. Falls gewisse, für die Anwender relevante Applikationen einen digitalen Ausweis vorschreiben, dürfen die Kosten nicht zu Lasten des Nutzers fallen.[127]

Um eine zu grosse Konzentration der Verbreitung der digitalen Signatur auf das E-Government zu verhindern, sollte der Staat in Zusammenarbeit mit der Wirtschaft möglichst viele Anwendungen für die digitale Signatur zur Verfügung stellen. Die Erarbeitung eines dazugehörigen geeigneten Marketingkonzeptes ist selbstverständlich.

Kostenschätzung der Zertifizierungsstelle über 5 Jahre[128]		
	Initialaufwand	Aufwand pro Jahr
Anerkennungsprozess	CHF 300'000	CHF 40'000
Grundinfrastruktur	CHF 500'000	CHF 178'000
Versicherung (exkl. Vermögenshaftpflicht)	CHF 0	CHF 52'800

[126] Vgl. Marzetta et al. [2001] S. 57ff.

[127] Vgl. Ziff. 0 (Strukturen und Attraktivität des Zertifikatmarktes).

[128] Vgl. Anhang B (Herleitung der Zahlen für die Kostenschätzung).

Kostenschätzung der Zertifizierungsstelle über 5 Jahre[128]		
	Initialaufwand	Aufwand pro Jahr
Personal Zertifizierungsstelle	CHF 0	CHF 600'000
Instruktion und Entschädigung der Registrierungsstellen (ca. 3000 Einwohnerämter)	CHF 600'000	CHF 225'000
Marketing	CHF 600'000	CHF 300'000
Total	CHF 2'000'000	CHF 1'395'800
Gesamtkosten für 5 Jahre	CHF 8'979'000	

Tabelle 8: Kostenschätzung Strategie 5
(Quelle: eigene Darstellung in Anlehnung an Marzetta et al. [2001] S. 60)

Strategiebeurteilung

6.1.9. Strategie 1: Bildung eines Wirtschaftskonsortiums

Der Einfluss eines solchen Konsortiums wäre sehr gross. Dank der vielen Vertreter aus der Wirtschaft können Entwicklungen im Markt früh erkannt werden und die Reaktion der Zertifizierungsstelle darauf würde schnell erfolgen. Ausserdem können Zertifikate angefertigt werden, welche mit den Verschiedenen Anwendungen aus der Wirtschaft kompatibel wären. Ein weiterer Vorteil ist, dass je mehr Firmen dem Konsortium beitreten, desto kleiner der finanzielle Aufwand pro Mitglied ausfällt. Der Staat würde eine derartige Lösung bestimmt begrüssen. Er könnte sich, ohne Rücksicht auf die Wirtschaft und ohne grösseren finanziellen Aufwand, für seine Anwendungen der qualifizierten Zertifikate bedienen. Falls die Post als Registrierung auftritt, ist es für die Nutzer einfach, ihre Zertifikate zu beantragen, da die Poststellen für die Bevölkerung in der Regel gut zu erreichen sind.

Weil aber zur Bildung eines solchen Konsortiums möglichst mehrere Vertreter aus allen Branchen auftreten sollen, ist die Umsetzbarkeit dieser Strategie als eher schwierig einzuschätzen. Dazu sollte in jeder Branche ein potentieller Business-Case für die qualifizierte Signatur bestehen und die Firmen müssten zur Überzeugung kommen, dass die digitale Signatur die beste Lösung für ihr E-Business-Problem darstellt. Ansonsten lohnt sich für die Unternehmen der finanzielle Aufwand nicht. Wie aus Kapitel 5.3 hervorgeht, haben viele Firmen zum Teil schon riesige Geldsummen für Internetprojekte ausgegeben und sind deshalb nicht mehr Willens, ohne absehbaren Erfolg noch einmal zu investieren. Da die Zertifizierungsstelle mit Hilfe des Konsortiums neu aufgebaut werden muss, ist zudem zu berücksichtigen, dass neues Fachpersonal sowie neue Räumlichkeiten und Informatiksysteme notwendig sind.

Die Finanzierung über ein Konsortium stellt bestimmt eine gute Lösung dar, jedoch dürfte die Tatsache, dass wirklich alle Branchen im Konsortium vertreten sein müssen, dazu beitragen, dass diese Strategie praktisch nicht umsetzbar ist.

6.1.10. Strategie 2: Zusammenschluss der privaten Zertifizierungsstellen und anschliessende Anerkennung

Erlangt die Zertifizierungsstelle als einzige in der Schweiz die Anerkennung, darf sie mit Aufträgen von Staat und Wirtschaft rechnen und kann voraussichtlich einen Kundenzuwachs verzeichnen. Zudem hätte sie mit keiner Konkurrenz mehr zu kämpfen. Für den Staat fallen mit dieser Lösung, was die Zertifizierungsstelle betrifft, keine Kosten an und er kann sich auf die Signaturverbreitung in seinem Umfeld konzentrieren. Auch die Wirtschaft kann sich der qualifizierten Zertifikate bedienen, vorausgesetzt sie schafft geeignete Applikationen dazu. Durch die private Tätigkeit der Zertifizierungsstelle ist es ihr möglich, Partnerschaften mit den verschiedenen Branchen einzugehen, um längerfristig potentielle Zertifikatskunden anzuwerben. Bei der möglichen Tätigkeit der Post als Registrierungsstellen, würde es für die Antragsteller bei der Registrierung keine Verwirrungen geben. Jedoch ist von einer Delegation des Registrierungsprozesses an bestehende Kunden wegen der Undurchsichtigkeit für die Antragsteller abzuraten. Einer der grösseren Vorteile dieser Strategie ist, dass das Fachpersonal und die Infrastrukturen bereits vorhanden sind.

Die Fusion erfordert von den bestehenden Zertifizierungsstellen höchste Flexibilität. Es ist fraglich, ob die privaten Zertifizierungsstellen ihre Erfindungen mit den anderen teilen möchten, oder ob sie sich weiterhin auf einem bestimmten Gebiet spezialisieren und folglich auf eine Zusammenarbeit verzichten. Auch das längerfristige Bestehen der Zertifizierungsstelle ist nicht garantiert, da der Zusammenschluss und die Akkreditierung nicht erhebliche Kosteneinsparungen mit sich bringen. Es kann auch schlecht abgeschätzt werden, inwieweit Staat und Wirtschaft tatsächlich auf qualifizierte Zertifikate zurückgreifen und ob sich Privatpersonen welche anschaffen werden.

Da die privaten Zertifizierungsstellen, wegen ihren Erfindungen eher nicht für eine Kooperation bereit sind, wird es schwierig, diese Strategie umzusetzen. Dazu wird sicher auch der finanzielle Aspekt beitragen. Noch gibt es keine Applikationen für qualifizierte Zertifikate und die einzelnen Zertifizierungsstellen halten sich mit eigenen Produkten über Wasser.

6.1.11. Strategie 3: Auslagerung der Zertifizierungsstelle ins Ausland

Das Vorhandensein und Funktionieren einer ausländischen akkreditierten Zertifizierungsstelle sowie die Verankerung der Anerkennung ausländischer Zertifizierungsstellen im ZertES[129] erleichtert die Umsetzung dieser Strategie. Für die Schweiz spielt es prinzipiell keine Rolle, wo sie ihre qualifizierten Zertifikate bezieht[130], zumal die Registrierung im eigenen Land stattfinden würde. Obwohl der Staat für die Akkreditierung, möglicherweise für die Versicherung und für den Unterhalt der Infrastrukturen mit jährlichen Kosten rechnen muss, fällt der finanzielle Aufwand geringer aus, als bei einer staatlichen Zertifizierungsstelle. Zudem kann die im Gesetz vorgeschriebene Zusammenarbeit[131] zwischen den in- und ausländischen Anerkennungsstellen bewirken, dass Projekte, welche im Ausland laufen, ebenfalls in der Schweiz Anwendung finden und somit wesentlich zur Signaturverbreitung beitragen würden. Auch könnte auf das Fachwissen von erfahrenem Personal zurückgegriffen werden.

[129] Vgl. Art. 3 ZertES.

[130] Vgl. Ziff. 0 (Vertrauenswürdigkeit von Zertifikaten mit Schweizer Qualität).

[131] Vgl. Art. 3 Abs. 2 ZertES.

Ein grosses Problem entsteht aber bei der Organisation, welche den ganzen Prozess ins Rollen bringt. Wird sich der Bund eingestehen, dass die Schweiz zum jetzigen Zeitpunkt nicht fähig ist, eine eigene Zertifizierungsstelle zu betreiben und soll sie deswegen aufs Ausland angewiesen sein? Ein weiterer Nachteil ist die geringe Marktreaktionsmöglichkeit der Zertifizierungsstelle bezüglich des Schweizer Marktes, da die ausländische Zertifizierungsstelle sich in erster Linie auf den heimischen Markt konzentriert. Falls sich ausländische Projekte für qualifizierte Zertifikate nicht auf die Schweiz übertragen lassen, wird es deshalb sehr schwierig, dieselben qualifizierten Zertifikate zu verwenden. Zudem ist zu beachten, dass die ausländische Zertifizierungsstelle die Umstände des Akkreditierungsprozesses und den Betrieb zusätzlicher Registrierungsstellen nur in Kauf nimmt, wenn die Zertifikate in der Schweiz tatsächlich genutzt werden.

Eine Zusammenarbeit zwischen In- und Ausland wäre denkbar. Auch von der finanziellen Seite wäre diese Strategie durchaus lukrativ. Jedoch dürfte die Schweiz zu viel Nationalstolz besitzen, als dass sie von einer ausländischen Zertifizierungsstelle abhängig sein möchte, vor allem dann, wenn über die Einführung einer eID diskutiert wird.

6.1.12. Strategie 4: Beteiligung des Bundes an einer privaten, anerkannten Zertifizierungsstelle

Die finanzielle Beteiligung des Bundes an einer privaten, anerkannten Zertifizierungsstelle ist gut möglich. Der Staat kann mit dieser Lösung seine Interessen deponieren und verhindert damit „inkompatible Experimente" der einzelnen Kantone sowie der privaten Zertifizierungsstellen.[132] Ausserdem kann die private, anerkannte Zertifizierungsstelle «*flexibel und schnell auf den Markt reagieren und sie ist offen für Kooperationen mit Partnern, die passende Zusatzdienstleistungen anbieten.*»[133] Durch solche Kooperationen sowie durch den Status eines Monopols könnten weitere Kunden sowohl aus dem wirtschaftlichen als auch aus dem staatlichen Umfeld angezogen werden. Auch die Koordination der Registrierungsstellen würde, sobald diese definiert sind, reibungslos ablaufen, vor allem dann, wenn der Staat die öffentlichen Ämter dazu zur Verfügung stellt. Damit die digitale Signatur verbreitet wird, kann die Zertifizierungsstelle als Vermittlungsstelle zwischen Wirtschaft und Staat auftreten und dieses Vorhaben gezielt fördern. Ein zusätzlicher Vorteil ist, dass das Personal und die Infrastrukturen der vorgängig privaten Zertifizierungsstelle nahtlos übernommen werden können.

Allerdings muss eine private Zertifizierungsstelle erst ihren Willen für eine allfällige Zusammenarbeit mit dem Staat äussern oder der Staat muss auf die private Zertifizierungsstelle zugehen, was erst dann geschehen wird, wenn für beiden Seite ein geeigneter Business-Case für qualifizierte Zertifikate vorliegt.

Die Kostenaufteilung zwischen Staat und Zertifizierungsstelle, die Möglichkeit, Kooperationen mit der Wirtschaft einzugehen machen diese Strategie sehr attraktiv. Es muss jedoch angemerkt werden, dass dieser Vorschlag bereits im Jahre 2001 bestand[134], bis jetzt aber noch nicht realisiert wurde, was vor allem auf den fehlenden Business-Case zurückzuführen

[132] Vgl. Marzetta et al. [2001] S. 56.

[133] Marzetta et al. [2001] S. 56.

[134] Vgl. Marzetta et al. [2001] S. 55ff.

ist. Die Zertifizierungsstelle muss hier also vor allem Druck ausüben, damit geeignete Applikationen für qualifizierte Zertifikate entwickelt werden.

6.1.13. Strategie 5: Einführung einer staatlich anerkannten Zertifizierungsstelle

Da bei dieser Strategie die ganze Organisation vom Staat übernommen wird, kann die Zertifizierungsstelle Zertifikate entwickeln, welche hauptsächlich dem Staat zu Nutzen kommen. Zudem könnte die Wirtschaft mit wenig Aufwand die staatlichen Zertifikate in ihre Anwendungen integrieren. Der bereits diskutierte Konflikt, für Zertifikate zu bezahlen, welche anschliessend auch bei der Konkurrenz eingesetzt werden können, fällt hier für die Wirtschaft weg. Da sowohl Registrierung als auch Zertifizierung auf amtlicher Ebene ablaufen, können die Prozesse für Zertifizierungsstelle und Nutzer anschaulich definiert werden.

Eine staatliche Zertifizierungsstelle einzurichten, ohne auf vorhandene Infrastrukturen zurückzugreifen, ist mit enormen Kosten verbunden, welche zum jetzigen Zeitpunkt vom Staat unter Berücksichtigung der allgemeinen Sparmassnahmen schwer aufzuwenden sind. Zudem besteht die Gefahr, Zertifikate zu entwickeln, welche nur im E-Government verwendet werden könnten und somit für die Wirtschaft unbrauchbar sind. Dies würde die gewünschte Verbreitung der digitalen Signatur in allen Kreisen verhindern.

Vor allem der finanzielle Aspekt dürfte hier wesentlich zum Scheitern der Strategie beitragen. Obwohl eine zu starke Konzentration der Zertifikate auf den E-Government-Bereich denkbar ist, dürfte dieses Szenario eher nicht eintreten, weil die Wirtschaft in der Lage ist, ihre Applikationen so anzupassen, dass die staatlichen Zertifikate dennoch verwendet werden können.

6.1.14. Gesamtbeurteilung

Die Vertrauenswürdigkeit der Zertifikate ist bei allen Strategien gegeben[135], weshalb sie nicht immer einzeln erwähnt wurde. Zudem gilt für alle vorgeschlagenen Strategien, dass der Betrieb einer anerkannten Zertifizierungsstelle nach erfolgtem Aufbau zum jetzigen Zeitpunkt eine Monopolsituation in der Schweiz besitzt. Somit darf die Zertifizierungsstelle, welcher Ansiedelung sie auch immer entstammt, damit rechnen, dass für die Verwendung von qualifizierten Zertifikaten in allen Bereichen auf diese zurückgegriffen wird. Die Bildung eines Wirtschaftskonsortiums, der Zusammenschluss der privaten Zertifizierungsstellen und die anschliessende Anerkennung sowie die Beteiligung des Bundes an einer privaten Zertifizierungsstelle fördern ausserdem den Wirtschafsstandort für E-Commerce in der Schweiz.[136] Strategien 3 (Auslagerung ins Ausland) und 5 (Einrichtung einer staatlichen Zertifizierungsstelle) tun dies nur bedingt.

Zu beachten ist, dass das Wirtschaftskonsortium und die staatliche Zertifizierungsstelle Gefahr laufen, Zertifikate nur für Applikationen, welche vom jeweiligen Geldgeber vorgeschlagen werden, zu entwickeln. Obwohl in Kapitel 5.2 sowohl der Staat die Wirtschaft als auch die Wirtschaft den Staat auffordert, geeignete Lösungen für eine anerkannte Zertifizierungsstelle vorzuschlagen und umzusetzen, heisst das nicht, dass die beiden Seiten gewillt sind, Mehrzweckzertifikate zu verwenden.

---

[135] Vgl. Ziff. 0 (Vertrauenswürdigkeit von Zertifikaten mit Schweizer Qualität).

[136] Vgl. Marzetta et al. [2001] S 56.

	Strategie 1	Strategie 2	Strategie 3	Strategie 4	Strategie 5
Umsetzbarkeit	(×)	(✓)	(✓)	✓	✓
Finanzierbarkeit	✓	(×)	✓	✓	(×)
Ersichtlichkeit der Transparenz	✓	✓	(✓)	✓	✓
Marktreaktionsmöglichkeit	✓	✓	(×)	(✓)	×
Beeinflussbarkeit der Entwicklungen durch den Staat	×	(×)	✓	✓	✓
Beeinflussbarkeit der Entwicklungen durch die Wirtschaft	✓	(✓)	(×)	(✓)	×
Verwendbarkeit der Zertifikate für mehrere Anwendungen	(✓)	(✓)	(✓)	✓	(✓)
Zurückgreifbarkeit auf Personal und Infrastrukturen	×	✓	✓	✓	×

Tabelle 9: Übersicht über die Strategieberuteilung
(Quelle: Eigene Darstellung)

Legende:

✓	Gut möglich
(✓)	Bedingt möglich
(×)	Nicht gut möglich
×	Unmöglich

Handlungsempfehlung bezüglich der Strategien

Für die Einrichtung einer anerkannten Zertifizierungsstelle in der Schweiz müssen in erster Linie die Umsetzbarkeit und die Finanzierbarkeit berücksichtigt werden. Die anderen Kriterien, welche aus Tabelle 9 ersichtlich sind, dürfen als zusätzliche Vorteile bei einer allfälligen Entscheidung für die eine oder andere Strategie betrachtet werden. Demzufolge kommen für eine anerkannte Zertifizierungsstelle insbesondere Strategie 3 (Auslagerung ins Ausland) und Strategie 4 (Beteiligung des Bundes an einer anerkannten Zertifizierungsstelle) in Frage. Werden die anderen Faktoren zusätzlich berücksichtigt, so schneidet Strategie 4 am besten ab.

Dennoch sei hier nochmals betont, dass die Fixierung auf eine bestimmte Strategie keinen Sinn macht, da die anderen Strategien ebenfalls umgesetzt werden können, falls die Bereit-

schaft für die Bildung eines Konsortiums (Strategie 1), für eine Fusion (Strategie 2) oder für eine staatliche Zertifizierungsstelle (Strategie 5) vorhanden ist.

Schlussendlich sollte auch die Richtung, in welche sich die Anwendungen der digitalen Signaturen entwickeln, berücksichtigt werden. Wird die digitale Signatur zukünftig hauptsächlich im staatlichen Umfeld benutzt, so errichtet der Staat eine Zertifizierungsstelle, kommt sie ausschliesslich in der Wirtschaft zum Einsatz, ist von einer staatlichen Zertifizierungsstelle abzusehen. Der wahrscheinlichste Fall wird sein, dass eine Trennung der beiden Bereiche nicht gemacht werden kann und somit die digitale Signatur früher oder später überall zum Einsatz kommt. Damit ist eine Aufteilung der Kosten zwischen Staat und Wirtschaft (Strategie 4) am plausibelsten.

7. Schlussfolgerungen

Rückblick

Wie in Kapitel 3 (Digitale Signaturen) festgestellt wurde, stellt die digitale Signatur technisch gesehen ein teilweise bereits gelöstes Problem dar. Auch für den Betrieb einer anerkannten Zertifizierungsstelle selbst gibt es klare technische und administrative Vorschriften sowie eine dazugehörige gesetzliche Grundlage. Allerdings haben Applikationsanbieter und auch die Zertifizierungsstellen nach wie vor mit technischen Sicherheitsproblemen, welche vor allem die Anwenderprogramme der Nutzer betreffen, zu kämpfen.

Ein noch grösseres Problem bereitet die breite Akzeptanz bei den Nutzern und damit zusammenhängend die Verbreitung der digitalen Signatur. Obwohl die elektronische Unterschrift auch im Alltag grosses Potential besitzt, wurden wichtige Projekte, welche zur Verbreitung der digitalen Signatur beigetragen hätten wieder eingestellt. Dies teilweise wegen Sparmassnahmen, teilweise wegen Konflikten, aber auch aus strategischen Gründen, wie beispielsweise mangelnde Kundenbeziehung im B2C-Bereich. In einigen Fällen wurde sogar gänzlich auf die Verwendung der digitalen Signatur verzichtet und es wurde auf andere Lösungen ausgewichen. Auch internationale Entwicklungen zeigen, dass die digitale Signatur durchaus nützlich wäre, die dazugehörigen Applikationen aber noch nicht bestehen und die neue Form der Unterschrift von den Nutzern somit als unwichtig eingeschätzt wird.

Trotz diesen Fakten gibt es Anwendungen für digitale Signaturen, worauf in Kapitel 6 (Mögliche Strategien für eine anerkannte Zertifizierungsstelle in der Schweiz) nach einer Darstellung der Situation in der Schweiz und nach der Feststellung, dass die momentan herrschende Situation für Staat, Wirtschaft und Privatpersonen unbefriedigend ist, Strategien für eine Zertifizierungsstelle entwickelt wurden. Wichtig dabei ist die Beachtung, dass anfänglich keine riesige Institution für die Zertifikatsausgabe einzurichten ist, sondern dass im Hinblick auf ausländische Gegebenheiten eine kleine Zertifizierungsstelle mit wenig Personal erhebliche Kosten einsparen kann und somit, da die Budgets der Geldgeber ohnehin beschränkt sind, eher die Möglichkeit hat, längerfristig zu bestehen.

Bei den vorgeschlagenen Strategien geht es weniger darum, eine Strategie als besonders geeignet weiter zu empfehlen, sondern die aktuellen Entwicklungen bezüglich Verbreitung digitaler Signaturen, im Hinblick auf eine Gründung einer anerkannten Zertifizierungsstelle, zu berücksichtigen.

Ausblick

Blickt man in der Geschichte zurück, so wird ersichtlich, dass bereits vor der digitalen Signatur Entwicklungen und Neuerfindungen auf Skepsis gestossen sind. Dennoch haben sich beispielsweise die Elektrizität oder das Internet im Laufe der Zeit weitgehend durchgesetzt, sogar soweit, dass es für einen Teil der Bevölkerung heute unvorstellbar wäre, keinen Strom oder keinen Internetanschluss zu besitzen. Ähnliches dürfte mit der Verbreitung der digitalen Signatur geschehen. In naher Zukunft wird die digitale Signatur hauptsächlich im Business to Business-, im Business to Government- und im Government to Government-Bereich zum Einsatz kommen. Dennoch sollten, hinsichtlich der Anwendung der digitalen Signatur durch

die breite Öffentlichkeit, keine individuellen Zertifikate für die genannten Bereiche geschaffen werden, sondern eines, welches den Nutzen für alle Beteiligte erbringt.

In weiter Zukunft ist es durchaus denkbar, dass die digitale Signatur die herkömmliche Unterschrift allmählich ablösen wird. Dazu wird jeder Bürger der Schweiz ein eigenes Zertifikat, welches er für seine Signatur verwendet, besitzen und damit alle Dokumente vor allem im Government to Consumer- und im Business to Consumer-Bereich ausschliesslich elektronisch unterschreiben. Der öffentliche Schlüssel und der dazugehörende private Schlüssel werden als elektronisches Identifikationsmittel schlechthin auftreten. Nicht nur zum digital Signieren, sondern auch beispielsweise am Zoll oder an Flughäfen sollen sie zur Identitätskontrolle zum Einsatz kommen.

Für die Zertifizierungsstellen bedeutet dies, dass sie in naher Zukunft ihre Institution vor allem für Geschäfte im B2B-, B2G- und G2G-Bereich ausrichtet. Jedoch darf sie damit rechnen, dass die digitale Signatur früher oder später auch beim breiten Publikum auf Interesse stossen wird. Diese Entwicklung kann die Zertifizierungsstelle mit geeigneten Produkten und einem entsprechenden Marketing erheblich beeinflussen, weshalb sie sich schon heute überlegen muss, wie die Zertifikate von morgen aussehen sollen und wo deren Einsatz sinnvoll erscheint.

Handlungsempfehlung für zukünftige, anerkannte Zertifizierungsstellen

Allein das Existieren einer anerkannten Zertifizierungsstelle reicht nicht, um die digitale Signatur beim breiten Publikum bekannt zu machen. Dass ein geeignetes Marketing und geeignete Applikationen ebenfalls notwendig sind, wurde bereits erwähnt.

Was in diesem Zusammenhang noch nicht betrachtet wurde, ist die Bequemlichkeit der Nutzer. Der Normalnutzer ist heute nicht in der Lage, die digitale Signatur zu erzeugen, beziehungsweise zu überprüfen, auch wenn er die dazu nötigen Schlüssel und Zertifizierungsinstanzen zu Verfügung hätte. Es darf zwar angenommen werden, dass die Nutzer, sobald ein Signaturbedürfnis besteht, schnell begreifen, wie das Verfahren der digitalen Signatur vor sich geht. Dennoch sollten die Prozesse der Signaturerzeugung und die Installationen der notwendigen Programme in diesem Masse vereinfacht werden, dass es auch einem nicht geübten Computeranwender ohne grösseren Aufwand gelingt, den eigenen PC signaturtüchtig zu machen. Die Zertifizierungsstelle muss also nicht nur ihre Dienste zur Verfügung stellen, sondern auch in der Lage sein, benutzerfreundliche Produkte zu erarbeiten und die Prozesse für die Nutzer einfach darzustellen. Schon heute geben die Banken beispielsweise ihre Software auf einer CD-ROM heraus, die ohne weitere Vorkehrungen des Nutzers alles auf dem entsprechenden PC installiert. Die automatisch ablaufende Softwareinstallation ist auch für die Zertifikate einzuführen.

Damit die Anwenderprogramme sicher für die digitale Signatur verwendet werden können, wäre eine Zusammenarbeit mit den entsprechenden Informatikfirmen denkbar. Auch Erfahrungsaustausche zwischen den einzelnen Zertifizierungsstellen können für solche Entwicklungen besonders im Hinblick auf die internationale Verwendung der digitalen Signatur hilfreich sein. Von einem alleinigen Operieren einer anerkannten Zertifizierungsstelle ohne ge-

eignete Partnerschaften und Kooperationen mit anderen Zertifizierungsstellen, mit Softwareentwicklern und mit Applikationsanbietern ist deshalb abzuraten.

Abkürzungsverzeichnis

Abs.	Absatz
AG	Aktiengesellschaft
ALGO	Algorithms Group
Art.	Artikel
Aufl.	Auflage
B2B	Business to Business
B2C	Business to Consumer
B2G	Business to Government
G2G	Government to Government
ca.	circa
CA	Certification Authority
CB	Certification Body
CD-ROM	Compact Disc Read-Only Memory
CHF	Schweizer Franken
E	Electronic
eID	elektronische Identitätskarte
ESSI	European Electronic Signature Standardisation Initiative
et al.	et alii
etc.	et cetera
EU	Europäische Union
exkl.	exklusive
f.	und folgende Seite/und folgender Artikel
ff.	und folgende Seiten/Artikel
GeBüV	Geschäftsbücherverordnung
GmbH	Gesellschaft mit beschränkter Haftung
Hrsg.	Herausgeber
inkl.	inklusive
IT	Information Technology
IuD	Information und Dokumentation
M	Mobile
Mio.	Millionen
PKI	Public Key Infrastruktur
OR	Obligationenrecht

RA	Registration Authority
PC	Personal Computer
S.	Seite
SAS	Schweizerische Akkreditierungsstelle
SiRL	Signaturrichtlinie
u.a.	unter anderem
Vgl.	vergleiche
VZertES	Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur
z.B.	zum Beispiel
ZertES	Zertifizierungsgesetz
ZertDV	Zertifizierungsdiensteverordnung
Ziff.	Ziffer

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

Bertsch, A. [2001]:

Digitale Signaturen. Berlin; Heidelberg; New York; Barcelona; Hongkong; London; Mailand; Paris; Tokio: Springer, 2001

Bitzer, F.; Brisch, M. [1999]:

Digitale Signatur: Grundlagen, Funktion und Einsatz. Berlin; Heidelberg; New York; Barcelona; Budapest; Hongkong; London; Mailand; Paris; Singapur; Tokio: Springer, 1999

Bossard, K. [2004, 20. Februar]:

Sichere Identität. In: Neue Zürcher Zeitung, 20. Februar 2004

Dohman, H.; Fuchs, G.; Khakzar, K. (Hrsg.) [2002]:

Die Praxis des E-Business: Technische, betriebswirtschaftliche und rechtliche Aspekte. Braunschweig; Wiesbaden: Vieweg, 2002

Dörr, B. S. [2003]:

Elektronische Signaturen und Haftung der Anbieter von Zertifizierungsdiensten: Eine Darstellung am Beispiel der Regelungen in der EU, Deutschland, Grossbritannien und der Schweiz. Zürich; Basel; Genf: Schulthess, 2003

Eidgenössisches Finanzdepartement [2002]:

Regieren in der Informationsgesellschaft: Die eGovernment-Strategie des Bundes. Bern: Eidgenossisches Finanzdepartement, 2002

Gatti, R. [2004, 17. März]:

Durchgehend und ganz ohne Papier. In: Handels Zeitung, 17. März 2004

Graber, C. [2000]:

Digitale Zertifikate: Infrastruktur für ein sicheres Internet. In: Geschäftsplattform Internet: Rechtliche und praktische Aspekte. Zürich: Schulthess, 2000

Government Computing [2004, 17. Mai]:

eGovernment in Österreich: Wien belegt Spitzenplatz im europäischen Vergleich. In: eGovernment Computing, 17. Mai 2004

Hansen, H. R.; Neumann, G. [2001]:

Wirtschaftsinformatik I. (8. Aufl.) Stuttgart: Lucius und Lucius, 2001

Helbling, C.; Kaiser, A. [2004, 21. Mai]:

Kommt jetzt die Tasten-Unterschrift?: Praktischer Nutzen der elektronischen Signatur. In: Neue Zürcher Zeitung, 21. Mai 2004

Horster, P. (Hrsg.) [1996]:

Digitale Signaturen: Grundlagen, Realisierungen, Rechtliche Aspekte, Anwendungen. Braunschweig; Wiesbaden: Vieweg, 1996

Koch, F. A. [1998]:

Internet Recht. München: Oldenbourg, 1998

Konar, R. [2004, 24. Februar]:

Das Kreuz mit der virtuellen Unterschrift. In: Wirtschaftsblatt, 24. Februar 2004

Kopp, W. [1998]:

Rechtsfragen der Kryptographie und der digitalen Signatur: Seminararbeit. München: Ludwig-Maximilians-Universität München, Juristische Fakultät, 1998

Legler, T. [2001]:

Electronic Commerce mit digitalen Signaturen in der Schweiz: Kurzkommentar zur Zertifizierungsdiensteverordnung. Bern: Stämpfli, 2000

Marzetta, A.; Stöckle, R.; Vaterlaus, O. [2001]:

Braucht die Schweiz einen amtlichen digitalen Ausweis?. Bern: Eidgenössisches Justiz- und Polizeidepartement, 2001

Neue Zürcher Zeitung [2004, 23. Juli]:

Chipkarten sollen deutsches Gesundheitswesen heilen. In: Neue Zürcher Zeitung, 23. Juli 2004

Neue Zürcher Zeitung [2001, 11. Mai]:

Digitale Identität für die Katz. In: Neue Züricher Zeitung, 11. Mai 2001

Oppliger, R. [2002, 29. November]:

Wie weiter mit dem „Wer ist wer“ im Netz?: Digitale Zertifikate und elektronische Identitätskarten. In: Neue Zürcher Zeitung, 29. November 2002

Palumbo, D. [2004, 16. Mai]:

Schweizer Bürger können sich vorerst nicht digital ausweisen. In: Neue Zürcher Zeitung, 16. Mai 2004

Polster, C. [1999, 10. Juli]:

Elektronische Unterschrift wird Monopolgesellschaft. In: Wirtschaftsblatt, 10. Juli 1999

Ramsauer, M. [2000]:

Die Regelung der Public Key Infrastruktur in der Schweiz. In: Geschäftsplattform Internet, Rechtliche und praktische Aspekte. Zürich: Schulthess, 2000

Ramsauer, M.; Geiser, J-M.; Dietschi, R.; Bundesamt für Kommunikation, Biel [2001]:

Die digitale Signatur: technische, organisatorische und rechtliche Aspekte. In: Internet und Electronic Business: Herausforderung an das Management. Zürich: Orell Füssli, 2001

Schlauri, S. [2001]:

Die Digitale Signatur: Basistechnologie des elektronischen Geschäftsverkehrs. In: Internet-Recht und Electronic Commerce Law. Lachen, St. Gallen: Dike, 2001

Schulzki-Haddouti, C. [2004, Heft Nr. 13]:

Alles auf eine Karte: Die Jobcard in schwerem Fahrwasser. In c’t Magazin für Computer Technik, Heft Nr. 13, 2004

Schulzki-Haddouti, C. [2004, Heft Nr. 10]:

Signaturbündnis macht Dampf: Industrie setzt auf ehrgeizige Kartenprojekte der Bundesregierung. In: c’t Magazin für Computer Technik, Heft Nr. 10, 2004

Schweizer Bank [2000, 1. September]:

Globalisierung verlangt Standards. In: Schweizer Bank, 1. September 2000

SDA – Basisdienst [2004, 23. Juli]:

Zürcher Regierungsrat fordert elektronische Identitätskarte. In: Schweizerische Depeschenagentur – Basisdienst, 23. Juli 2003

Sonntags Zeitung [2001, 11. November]:

Die Einführung der digitalen Unterschrift verzögert sich. In: Sonntags Zeitung, 11. November 2001

Stejskal, C. [2003]:

Elektronische Signaturen: Einsatzmöglichkeiten im Bankenumfeld. In: Swiss Banking Scool, Nr. 208. Zürich: Haupt Verlag, 2003

Wildhaber, B. [2002]:

Wie weiter nach Swisskey – Rechtliche und ökonomische Rahmenbedingungen für Anbieter von Zertifizierungsdiensten. In: Anwaltsrevue; Publikationen des Schweizerischen Anwaltsverbandes, Heft Nr. 3, 2002

Materialien

Botschaft zum Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES)

vom 3. Juli 2001

Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES)

vom 19. Dezember 2003

Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (SiRL)

Schweizerisches Obligationenrecht (OR)

Bundesgesetz vom 30. März 1911 betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches, SR 220

Technische und administrative Vorschriften über Dienste der elektronischen Zertifizierung

vom 1. September 2001, SR 784.103.1

Verordnung über die Führung und Aufbewahrung der Geschäftsbücher (Geschäftsbücherverordnung; GeBüV)

Vom 24. April 2002 (Stand am 18. Juni 2002), SR 221.431

Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur

(VZertES)

Verordnung über die elektronische Signatur, Entwurf vom 1. Juni 2004

Zertifizierungsdiensteverordnung (ZertDV)

Verordnung über die Dienste der elektronischen Zertifizierung, vom 12. April 2000, SR 784.103

Internetverzeichnis

A-Trust
www.a-trust.at
Stand 9. August 2004

Biometrie, ein Überblick
http://www.informatik.hu-berlin.de/~schalig/
Stand 9. August 2004

Bundesamt für Justiz
www.ofj.admin.ch
Stand 11. August 2004

Der Geburtstagsangriff auf die digitale Signatur
http://www.cast-forum.de/pdf/nachwuchstag2003/CAST_031120-Blumenstein-infoblatt.pdf
Stand 11. August 2004

Grundlagen der Kryptographie
http://www.informatik.tu-darmstadt.de/TI/Lehre/SS04/Seminar/PKI/slides/1.1%20Grundlagen%20Kryptographie.pdf
Stand 11. August 2004

KPMG
www.kpmg.ch
Stand 11. August 2004

Public-Key-Infrastrukturen
http://www.teletrust.de/themen.asp?id=80310&Sprache=D_&HomePG=0
Stand 19. Juli 2004

Sichere Internet-Kommunikation mit Zertifikat
http://www.trustcenter.de/infocenter/tc_signieren-und-verschluesseln_de.pdf
Stand 22. Juli 2004

Stellungnahme zur Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur

http://www.wildhaber.com/

Stand 26. Juli 2004

SwissCERT Cute

http://www.swisscert.com/cute/SwissCERT-CUTE.pdf

Stand 27. Juli 2004

Auskunftspersonen

AWK Group, Leutschenbachstrasse 45, 8050 Zürich
Oliver Vaterlaus
4. August 2004

Bundesamt für Justiz, 3003 Bern
Dr. Felix Schöbi
10. August 2004

KPMG , Badenerstrasste 172/170, 8026 Zürich
Reto Grubenmann
3. August 2004

Lanexpert SA, Glattower, 8301 Zürich
Christian Graber, Direktor Niederlassung Zürich, Ex-Geschäftsführer von Swisskey AG
22. Juli 2004

SwissCert AG, Gartenstrasse 10, 8002 Zürich
Daniel Büttiker, Geschäftsführer
21. Juli 2004

SwissSign AG, Löwenstrasse 1, 8001 Zürich
Joseph A. Doekbrijder, Geschäftsführer
11. August 2004

Swoffice GmbH, Hauptstrasse 53, 9053 Teufen
Adrian Bischof, Entwicklungsleiter
8. August 2004

Winterthur Versicherungen, General Guisan-Strasse 40, 8401 Winterthur
Urs De Maddalena, Haftpflichtspezialist
17. August 2004

3V Beratungen GmbH, Quellenstrasse 8, 9016 St. Gallen
Reto Braschler, Geschäftsführer und Versicherungsexperte
19. August 2004

Anhang A: Gesprächsleitfaden

Realisierungsmöglichkeiten einer Zertifizierungsstelle für die digitale Signatur in der Schweiz

Firma: *Swisskey AG*	Datum: *22. Juli 2004*
Kontakt: *C. Graber*	Funktion: *Ex-Geschäftsführer*
Telefon:	E-Mail:

A: Einleitung

B: Allgemeines zur Firma

1. Gründungszweck
2. Finanzierung
3. Haupttätigkeiten
4. Kundensegmente
5. Ansiedelung
6. Zertifikatsangebote

C: Aufhebung der Firma

1. Misserfolgsfaktoren
2. Erfolgsfaktoren
3. Folgen für die Kunden
4. Hauptgründe für Firmenschliessung

D: Zukünftige Zertifizierungsstellen:

1. Handlungsempfehlung
2. Zukünftiges Potential für Zertifikate
3. Zukünftiges Kundenpotential
4. Rolle des Staates bei einer Neugründung einer anerkannten Zertifizierungsstelle

Realisierungsmöglichkeiten einer Zertifizierungsstelle für die digitale Signatur in der Schweiz

Firma: *SwissCERT AG*	Datum: *21. Juli 2004*
Kontakt: *D. Büttiker*	Funktion: *Geschäftsführer*
Telefon:	E-Mail:

A: Einleitung

B: Firma allgemein

1. Gründungszweck
2. Finanzierung
3. Haupttätigkeiten
4. Kundensegmente
5. Ansiedelung

C: Betrieb einer privaten Zertifizierungsstelle

1. Gründe für privaten Betrieb
2. Rentabilität
3. Business-Case für Anerkennung
4. Kosten der Anerkennung
5. Erfüllung von Zusatzkriterien für Anerkennung

D: Zukünftige Zertifizierungsstellen

1. Handlungsempfehlung
2. Zukünftiges Potential für Zertifikate
3. Zukünftiges Kundenpotential
4. Rolle des Staates bei einer Neugründung einer anerkannten Zertifizierungsstelle

Anhang B: Herleitung der Zahlen für die Kostenschätzung

Anerkennungsprozess:

Gemäss Auskunft der KPMG, Anerkennungsstelle für Zertifizierungsdiensteanbieterinnen in der Schweiz, variieren die Preise für die Anerkennung je nach Anzahl verschiedener Zertifikatstypen und Server und je nach Verwendung verschiedener Standards zwischen CHF 180'000 und CHF 450'000. Bevor der eigentliche Anerkennungsprozess durchgeführt werden kann, muss sich die Zertifizierungsstelle einer Vorakkreditierung unterziehen, welche zwischen CHF 25'000 und CHF 50'000 kostet. Die Anerkennung kann sich somit über mehrere Jahre hinziehen. Zudem ist zu beachten, dass die Vorschriften für die Anerkennung jedes Jahr neu überprüft werden, was ebenfalls mit Kosten verbunden ist.[137] Deshalb wird beim jährlichen Aufwand der Betrag von CHF 40'000[138] aufgeführt.

In dieser Arbeit wurde bewusst nicht der Maximalbetrag des Anerkennungsprozesses gewählt, da die Zertifizierungsstelle im kleinen Rahmen aufgebaut wird und deshalb keine grosse Anzahl Server und diverse Standards verwenden werden. Die Vorakkreditierungskosten sind im Preis inbegriffen.

Grundinfrastruktur:

Da in Folge der Nichtbekanntgabe vertraulicher Daten keine Auskunft über mögliche Infrastrukturkosten seitens der Zertifizierungsstellen und seitens der Anerkennungsstelle gegeben werden konnte, wurden die Kosten mit jenen einer kleineren Informatikfirma, welche Software vertreibt und über ähnliche infrastrukturelle Voraussetzungen wie eine Zertifizierungsstelle verfügen muss, verglichen. Die Detailkosteneinteilung könnte wie folgt aussehen:

Komponente der Infrastruktur	Initialaufwand	Aufwand pro Jahr
Räumlichkeiten	CHF 0	CHF 80’000
Clients inkl. Software und Lizenzen	CHF 18’000	CHF 18’000
Server inkl. Hardware	CHF 150’000	CHF 80’000
Büroeinrichtung	CHF 25’000	CHF 0
Total	CHF 193’000	CHF 178’000

Tabelle 10: Detailkostenschätzung der Grundinfrastruktur
(Quelle: eigene Darstellung in Anlehnung an Gespräche mit AWK Group und Swoffice GmbH)

Da nicht ausfindig gemacht werden konnte, wie viel die Kosten bei der Zertifizierungsstelle für die Archivierung und für die wenn möglich in Echtzeit abzurufende Zertifikatsüberprüfung betragen, wurde der Preis für die Grundinfrastruktur auf CHF 500’000 erhöht, dennoch fällt er markant weniger hoch aus, als ihn Marzetta et al. [2001] auf der Seite 60 mit 4 Mio. CHF vorgeschlagen haben. Gemäss Auskunft von der AWK Group, welche diese Empfehlung

[137] Vgl. Gespräch mit Swisskey AG.

[138] Genauer Betrag konnte nicht ausfindig gemacht werden. Es handelt sich hier um einen Schätzungswert der Verfasserin.

machte, darf mit wesentlich weniger Kosten gerechnet werden, wenn die Zertifizierungsstelle mit einer kleinen Verwaltung von Zertifikaten rechnet.

Für die Strategie 2 (Zusammenschluss der privaten Zertifizierungsstellen und anschliessende Anerkennung) wurde für die Grundinfrastruktur trotz der vorhanden Geräte mit einem Betrag von CHF 100'000 gerechnet. Damit sollte das Zusammenführen der IT-Systemen (Datenübernahme etc.) gedeckt werden.

Der jährliche Aufwand zum Unterhalt der Infrastrukturen wird, gestützt auf das Gespräch mit der Swoffice GmbH, mit CHF 178'000 budgetiert. Darin enthalten sind sowohl die Abschreibungen als auch der Unterhalt der Geräte, die jährlichen Lizenzkosten sowie die monatliche Miete der Büroräumlichkeiten.

Versicherung:

Die Prämie für die Vermögenshaftpflichtversicherung konnte wegen der fehlenden Abschätzbarkeit des Risikos nicht ausfindig gemacht werden.[139] Jedoch darf angenommen werden, dass je grösser das Risiko ist, desto höher die Prämie ausfallen wird. Bei grossen Risiken kann die Prämie schnell über CHF 100'000 steigen.[140] Für die anderen Versicherungen müsste die Zertifizierungsstelle bei einer Lohnsumme von CHF 600'000 etwa mit folgenden jährlichen Prämien rechnen:

Kostenschätzung der Versicherungen (exkl. Vermögenshaftpflichtversicherung)[141]	
Unfallversicherung	CHF 6'600
Kollektive Krankenversicherung (Lohnausfall)	CHF 5'700
Pensionskasse	CHF 38'000
Betriebshaftpflichtversicherung (Personen- und Sachschäden)	CHF 500
Geschäftsversicherung inklusive EDV (Feuer, Diebstahl, Wasser, Einrichtungen etc)	CHF 2'000
Total (exklusive Haftpflichtversicherung)	CHF 52'800

Tabelle 11: Kostenschätzung der Versicherungsprämien
(Quelle: Eigene Darstellung in Anlehnung an Gespräch mit 3V Beratungen GmbH)

Der Betrag der Versicherungsprämie wird, wenn die Haftpflichtversicherung dazu kommt, erheblich höher ausfallen, was für die gesamte Kostenschätzung berücksichtigt werden muss. Ein Initialaufwand für die Versicherungsprämie ist nicht nötig, da die Prämie ab Inkrafttreten der Versicherung jährlich bezahlt werden muss. Anerkannte ausländische Zertifizierungsstellen müssen sich in der Schweiz nur dann zusätzlich versichern, wenn ihre bisherige Deckung für die Haftung in der Schweiz nicht ausreicht.[142]

[139] Vgl. Anhang C (Haftpflichtversicherung der Zertifizierungsstellen).

[140] Vgl. Gespräch mit 3V Beratungen GmbH.

[141] Vgl. Gespräch mit 3V Beratungen GmbH.

[142] Vgl. Gespräch mit Bundesamt für Justiz.

Personal Zertifizierungsstelle:

Da die Zertifizierungsstelle zu Beginn über vier Mitarbeiter verfügt, wurde mit einem durchschnittlichen Jahreseinkommen von CHF 150'000[143] pro Mitarbeiter gerechnet, worauf auf den jährlichen Aufwand von CHF 600'000 geschlossen werden kann. Auch hier ist ein Initialaufwand nicht nötig, die Schulungen und Einarbeitung sind in den Löhnen der Mitarbeiter mit inbegriffen. Darin ebenfalls enthalten sind mögliche Lohnschwankungen.

Instruktion und Entschädigung der Registrierungsstellen:

Die Registrierungsstellen müssen für die Inbetriebnahme einer Zertifizierungsstelle so informiert werden, dass sie die Antragssteller gesetzesgemäss überprüfen können. Da dies mit maximal einem halben Tag Schulung durch die Zertifizierungsstelle zu bewältigen ist, kann mit fünf Stunden à CHF 40 pro Registrierungsstelle gerechnet werden. Die CHF 40 entsprechen einem Durchschnittsstundenlohn eines Angestellten mit einem Jahreseinkommen von ungefähr CHF 80'000.

Durch das Outsourcing des Registrierungsprozesses fällt bei den entsprechenden Ämtern ein grösserer Aufwand an. Um diesen zu entschädigen, werden der Registrierungsstelle die Kosten, welche pro Antrag anfallen, verrechnet. Eine Antragsstellung dauert ca. 15 Minuten. Bei einem Durchschnittstundenlohn von CHF 180 (Stundenansatz für externen Service) ergibt dies pro Antrag CHF 45. Wenn jedes Jahr 5000 Zertifikate verkauft werden, muss den Registrierungsstellen CHF 225'000 überwiesen werden.

Marketing:

Da die Zertifizierungsstelle dem breiten Publikum ihr Angebot erst bekannt machen muss, muss sie genügend Mittel in ein ausgezeichnetes Marketing stecken. Die Schätzung des Betrages 600'000 Initialaufwand und 300'000 Jahresaufwand beruht auf Erfahrungswerten. Der Initialaufwandbetrag ist deshalb so hoch angesetzt, weil die Zertifizierungsstelle ihr Marketing möglichst an die ganze Schweiz richten soll. Je nach Übertragungsmedium kann sowohl dieser, als auch der jährliche Betrag dennoch erheblich höher ausfallen.

[143] Vgl. Gespräch mit Swisskey AG

Anhang C: Haftpflichtversicherung der Zertifizierungsstellen

Um eine Vorstellung zu erhalten, mit welchem Aufwand eine Zertifizierungsstelle für die Versicherungsprämie machen muss, wurde diesbezüglich eine Anfrage an die Winterthur Versicherungen gemacht. Herr De Maddalena, Haftpflichtspezialist der Winterthur Versicherungen nahm dazu folgendermassen Stellung:

«Die Durchsicht der umfangreichen Unterlagen (Botschaft des BR zum ZertES) vom 3. Juli 2001, Entwurf für das Bundesgesetz über elektronische Signatur, ZertES, vom 19.12.2003 sowie Entwurf zur Verordnung, VZertES, vom 1. Juni 2004) zeigen folgendes: (Um Ihnen schnell eine Antwort bieten zu können, sind meine Ausführungen stichwortartig. Gerne stehe ich Ihnen aber allenfalls für ein Gespräch zur Verfügung. (052 - 261 3232))

Es soll eine neue Kausalhaftung eingeführt werden (Art. 16 ZertES) 2. Das Gesetz sieht eine Sicherstellungspflicht vor durch Versicherung (gemäss Art. 3, Abs. 1f ZertES in Verbindung mit Art. 2, Abs. 1 VZertES) respektive durch gleichwertige Garantie (Art. 2, Abs. 2 VZertES).

Zu (1) Haftung

Leider hat der Gesetzgeber sich wieder einmal die Arbeit leicht gemacht: Wenn das Risiko schwer fassbar ist, statuiert man eine neue (milde) Kausalhaftung (Botschaft Seite 5689) und zwar auch für so genannte reine Vermögensschäden (Vermögenseinbussen, welche nicht Personen- oder Sachschäden sind). Ausserdem wird eine Umkehr der Beweislast vorgesehen (Art. 16, Abs. 2 ZertES), was die Haftungssituation massiv zu lasten der Anbieterin verschärft. Es scheint, dass sich der Gesetzgeber bewusst war, dass durch Haftungsverschärfung die Möglichkeiten der Versicherbarkeit eingeschränkt werden. In der Botschaft, Seite 5701, kann dazu nachgelesen werden: "Die gegenteilige Lösung liesse aus der vorgeschlagenen Kausalhaftung eine Gefährdungshaftung werden, mit der für den Zertifizierungsdienstanbieter schwer abschätzbaren und damit auch kaum versicherbaren Folgen." Dabei übersieht der Gesetzgeber, dass mit der vorgesehenen Kausalhaftung mit Umkehr der Beweislast das Risiko ebenso schwer, resp. kaum abschätzbar wird.

Zu (2) Haftpflichtversicherung

Die Versicherbarkeit setzt in jeder Versicherungsbranche, also auch in der Haftpflichtversicherung; u.a. die Abschätzbarkeit des Risikos voraus. Aufgrund der bisher vorliegenden Unterlagen fehlt es an der versicherungs- technisch notwendigen Abschätzbarkeit. Dies bedeutet, dass - zumindest heute- das Risiko "reine Vermögensschäden", weil nicht kalkulierbar, unversicherbar ist. […] Ich weise darauf hin, dass die Winterthur zurzeit keine Haftpflichtversicherung für Zertifizierungsdienste im Bereich der elektronische Signatur anbietet.»

Bisher erschienene Schriften

Ergebnisse von Forschungsprojekten erscheinen jeweils in Form von Arbeitsberichten in Reihen. Sonstige Publikationen erscheinen in Form von alleinstehenden Schriften.

Derzeit gibt es in den Churer Schriften zur Informationswissenschaft folgende Reihen:
Reihe Berufsmarktforschung

Churer Schriften zur Informationswissenschaft – Schrift 1
Reihe Berufsmarktforschung – Arbeitsbericht 1:
Josef Herget
Thomas Seeger
Zum Stand der Berufsmarktforschung in der Informationswissenschaft
in deutschsprachigen Ländern
Chur, 2004 (im Druck)
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 2
Reihe Berufsmarktforschung – Arbeitsbericht 2:
Josef Herget
Norbert Lang
Berufsmarktforschung in Archiv, Bibliothek, Dokumentation
und in der Informationswirtschaft: Methodisches Konzept
Chur, 2004 (im Druck)
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 3
Reihe Berufsmarktforschung – Arbeitsbericht 3:
Josef Herget
Norbert Lang
Gegenwärtige und zukünftige Arbeitsfelder für Informationsspezialisten
in privatwirtschaftlichen Unternehmen und öffentlich-rechtlichen Institutionen
Chur, 2004
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 4
Sonja Hierl
Die Eignung des Einsatzes von Topic Maps für e-Learning
Vorgehensmodell und Konzeption einer e-Learning-Einheit unter Verwendung von Topic Maps
Chur, 2005
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 5
Nina Braschler
Realisierungsmöglichkeiten einer Zertifizierungsstelle für digitale Zertifikate in der Schweiz
Chur, 2005
ISSN 1660-945X

Über die Informationswissenschaft der HTW Chur

Die Informationswissenschaft ist in der Schweiz noch ein junger Lehr- und Forschungsbereich. International weist diese Disziplin aber vor allem im anglo-amerikanischen Bereich eine jahrzehntelange Tradition auf. Die klassischen Bezeichnungen dort sind Information Science, Library Science oder Information Studies. Die Grundfragestellung der Informationswissenschaft liegt in der Betrachtung der Rolle und des Umgangs mit Information in allen ihren Ausprägungen und Medien sowohl in Wirtschaft und Gesellschaft. Die Informationswissenschaft wird in Chur integriert betrachtet.

Diese Sicht umfasst die Teildisziplinen Bibliothekswissenschaft, Archivwissenschaft und Dokumentationswissenschaft. Auch neue Entwicklungen im Bereich Informationswirtschaft werden gezielt aufgegriffen und im Lehr- und Forschungsprogramm berücksichtigt.

Der Studiengang Information und Dokumentation wird seit 1998 als Vollzeitstudiengang in Chur angeboten und seit 2002 als berufsbegleitender Studiengang in Zürich. Künftig wird ein berufsbegleitender Masterstudiengang das Lehrangebot abrunden.

Der Arbeitsbereich Informationswissenschaft vereinigt Cluster von Forschungs-, Entwicklungs- und Dienstleistungspotentialen in unterschiedlichen Kompetenzzentren.

Folgende Kompetenzzentren sind im Aufbau:

- Strategic Research
- Information Management & Competitive Intelligence
- Records Management
- Library Consulting
- Information Engineering Laboratory

Diese Kompetenzzentren werden künftig in einem eigenständigen Institut für Informationswissenschaft zusammengefasst werden.

IMPRESSUM

Verlag & Anschrift

Arbeitsbereich Informationswissenschaft, Chur

IuD - Information und Dokumentation
HTW - Hochschule für Technik und Wirtschaft
University of Applied Sciences
Ringstrasse 37
CH-7000 Chur

www.iudchur.net / www.fh-htwchur.ch

ISSN 1660-945X

Studienleiter

Prof. Dr. Josef Herget
Telefon: +41 81 286 24 44

Email: Josef.herget@fh-htwchur.ch

Sekretariat

Telefon : +41 81 286 24 24
Fax : +41 81 286 24 00
Email: clarita.decurtins@fh-htwchur.ch