Die Krise des Signaturmarktes: Lösungsansätze aus betriebswirtschaftlicher Sicht

Lothar Fritsch, Heiko Rossnagel

Lehrstuhl für M-Commerce
Johann Wolfgang Goethe Universität Frankfurt
Gräfstr. 78
60054 Frankfurt
lothar.fritsch@m-lehrstuhl.de
heiko.rossnagel@m-lehrstuhl.de

Abstract: Auch sieben Jahre nach der Verabschiedung des deutschen Signaturgesetzes werden nur vereinzelt Anwendungen für qualifizierte elektronische Signaturen angeboten. Mit rund 30.000 qualifizierten Signaturzertifikaten in Deutschland bis Januar 2004 [Si04], sind die Hoffungen bezüglich der elektronischen Signatur bei weitem nicht erfüllt worden. Dieser Beitrag beschäftigt sich mit der aktuellen Marktsituation und Gründen für das vorliegende Marktversagen. Es werden aktuelle Initiativen, die der qualifizierten elektronischen Signatur zum Durchbruch verhelfen sollen, untersucht und bewertet. Abschließend werden Lösungsansätze für einen funktionierenden Zertifizierungsdienstemarkt auf Basis der Diffusionstheorie, der Informationsmärkte und Netzwerkökonomie gegeben.

1 Einleitung

Mit rund 30.000 qualifizierten Signaturzertifikaten in Deutschland bis Januar 2004 [Si04] sind die Hoffungen bezüglich der elektronischen Signatur bei weitem nicht erfüllt worden. Anwendungen wurden bislang nur vereinzelt realisiert und Anfang 2002 dachten sogar zwei Trust Center darüber nach, den Zertifizierungsbetrieb wieder komplett einzustellen [Si02] [Dt02]. Die rechtlichen Rahmenbedingungen für qualifizierte elektronische Signaturen sind längst gegeben, und die Anwendungsmöglichkeiten sind interessant. Umso verblüffender ist die geringe Marktdurchdringung der Zertifizierungsdienste. Dieser Beitrag untersucht die aktuelle Marktsituation unter betriebswirtschaftlichen Gesichtspunkten und gibt Empfehlungen für eine Neugestaltung des Marktes für Zertifizierungsdienstleistungen.

2 Aktuelle Marktsituation

Derzeit gibt es in Deutschland 24 akkreditierte Trust Center, allerdings bieten viele nur branchenspezifische Lösungen an. Im Folgenden werden nur die nicht auf spezielle Berufsgruppen spezialisierten Trust Center berücksichtigt. Zunächst wird untersucht, für welche Anwender die Trust Center ihre qualifizierten Zertifikate vorrangig ausstellen.

	Privatanwender	Unternehmen / Behörden
AuthentiDate International AG	0	✓
Deutsche Post Signtrust GmbH	✓	✓
D-Trust GmbH	✓	✓
TC TrustCenter AG	0	✓
T-TeleSec	✓	✓

Tabelle 1: Das Angebot an personalisierten Chipkarten auf dem Markt

Es werden sowohl für Privatanwender, als auch für Unternehmen / Behörden personalisierte Chipkarten angeboten. Die AuthentiDate International AG hat sich allerdings mit ihren Komplettlösungen auf Geschäftskunden spezialisiert. Der Fokus der Unternehmen liegt auf der Gewinnung von Geschäftskunden.

2.1 Die Preisstrategie

Dieser Abschnitt beschränkt sich auf die Preise für das Ausstellen einer signaturgesetzkonformen personalisierten Chipkarte zur Erzeugung qualifizierten elektronischer Signaturen.

	Ausstellung Zertifikat	Jährliche Grundgebühr	Summe 2-jährige Nutzung
D-Trust GmbH	41 €	29 €	99 €
Deutsche Post Signtrust GmbH	0 €	39 €	78 €
TC Trust Center	8 €	62 €	132 €
T-TeleSec	23,57 €	42,95 €	109,47 €

Tabelle 2: Preise für eine personalisierte Chipkarte inkl. Mwst.

Bei allen Unternehmen müssen die Kunden eine jährliche Grundgebühr, unabhängig von der Nutzungsintensität der Karte entrichten. Ein zusätzliches Entgelt für eine Zertifikatsüberprüfung oder ähnliches fällt nicht an.

2.2 Die Vertriebsstrategie

Das Unternehmen AuthentiDate International AG hat sich auf Komplettlösungen für Geschäftsprozesse spezialisiert. Viele Funktionen und Dienste werden als integrierter Bestandteil der Produkte von Partnerfirmen angeboten. Außerdem ist das Unternehmen weltweit tätig. Durch die in New York ansässige AuthentiDate, Inc. werden die Produkte und Services auch in den USA, unter der Berücksichtigung der dortigen Signaturgesetze angeboten. Die TC TrustCenter AG arbeitet mit Vertriebspartnern zusammen, die die Produkte entweder in ihre Gesamtlösungen integrieren oder die Produkte der TC Trust-Center AG in ihr eigenes Produktportfolio aufnehmen. Die TC TrustCenter AG agiert verstärkt im Bankenumfeld. Die Firmen Deutsche Post Signtrust GmbH und D-Trust GmbH verfügen über ein breites Partnernetzwerk. Diese Kooperationspartner stellen die notwendigen Anwendungen für qualifizierte elektronische Signaturen zur Verfügung. Das T-TeleSec Trust Center ist ein Geschäftsbereich der T-Systems ITC Security, die die Trust Center Services im Zusammenhang mit ihren Security Lösungen anbieten. Für die Lösungen der T-TeleSec wird auch der Flächenvertrieb der T-Com genutzt [Me03]. Die Produkte des T-TeleSec Trust Centers werden europaweit angeboten.

2.3 Die finanzielle Situation der Trust Center

An dieser Stelle wird nur auf die finanzielle Lage der Deutsche Post Signtrust GmbH und der D-Trust GmbH eingegangen, da die Jahresabschlüsse der anderen Trust Center beim Registergericht nicht verfügbar waren.

Deutsche Post Signtrust GmbH: Der Gesamtumsatz der Deutsche Post Signtrust GmbH betrug im Geschäftsjahr 2002 428.069,92 Euro. Das ist im Vergleich zum Vorjahr mit einem Gesamtumsatz von 459.508,84 Euro ein leichter Umsatzrückgang. Der Jahresfehlbetrag für das Jahr 2002 belief sich auf -8,8 Millionen Euro. Dieser Verlust wurde aufgrund eines Ergebnisabführungsvertrages durch die Deutsche Post eBusiness GmbH übernommen. Im Geschäftsjahr 2001 konnte durch die signaturgesetzkonformen Produkte Signtrust Start und Signtrust Identity lediglich einen Umsatz von 81.836,12 Euro generiert werden. Das sind nur 17,81 % des Gesamtumsatzes in Höhe von 459.508,84 Euro. Die beiden großen umsatzstarken Bereiche waren 2001 die PKI-Lösungen und die Plattform-Einrichtung [Si02].

D-Trust GmbH: Die Höhe der Umsatzerlöse belief sich für das Geschäftsjahr 2001 auf 2.128.356,26 Euro und sank im Jahr 2002 auf 1.220.804,19 Euro. Die gewöhnliche Geschäftstätigkeit im Jahr 2002 verursachte einen Verlust in Höhe von -1,9 Millionen Euro. Ohne den Beherrschungs- und Ergebnisabführungsvertrag mit der Bundesdruckerei GmbH, wäre das die D-Trust GmbH bereits im Jahr 2001 überschuldet gewesen. Ein Fortbestand des Unternehmens ist nur durch weitere Ausgleichszahlungen durch die Muttergesellschaft sichergestellt [Dt02].

3 Gründe für den geringen Markterfolg

In diesem Abschnitt zeigen wir, welche methodischen Schwächen beim Marktangebot der Trust Center aus betriebswirtschaftlicher Sicht erkennbar sind. Zu Grunde legen wir die Theorie der Netzwerkeffekte, insbesondere nach [SV98], die Diffusionstheorie nach [Ro03] sowie eine eigene Analyse von Angebot, Nachfrage und Preisen der Signaturdienstleistungen und –angebote. Auf den Aspekt der fehlenden Standardisierung und Inkompatibilitäten wird hier, über die Netzeffekttheorie hinaus, nicht näher eingegangen. Dies wird oft als der wichtigste Grund für die mangelnde Durchsetzung der qualifizierten Signatur gesehen. Zur Beseitigung dieses Problems beteiligen sich die Trust Center alle an mindestens einer Arbeitsgruppe, entweder an der T7 e.V [T704] mit der ISIS-MTT-Spezifikation [IS04] oder innerhalb des Signaturbündnisses [Si204]. Neben diesem Problem werden auch fehlendes Vertrauen in die Sicherheit der Technik, zu umständliche Softwarewartungszyklen mit der Akkreditierung nach Signaturgesetz sowie fehlende Softwareergonomie der Endbenutzersoftware gesehen. Im Vergleich dazu allerdings wirken die bei der Regulierung des Marktes für qualifizierte Signaturen nicht berücksichtigten wirtschaftlichen Mechanismen deutlich schwerer.

Kosten-/ Nutzenverteilung wurde nicht berücksichtigt: Jeder zukünftige Kunde wird sich bei der Kaufentscheidung nach seiner persönlichen Kosten-/Nutzenverteilung richten [HB00]. Aus diesem Grund wird untersucht, welche Kundengruppe bei einer bestimmten Anwendung die Kosten für die Anschaffung der personalisierten Chipkarte inklusive Kartenleser trägt und welcher Kundengruppe daraus ein finanzieller Vorteil entsteht. Die Analyse wurde unter den folgenden Annahmen durchgeführt:

1. Die Analyse basiert auf der aktuellen Preisstruktur für personalisierte Chipkarten.
2. Relevant für diese Analyse ist nur der finanzielle Vorteil. Der Aspekt Zeiteinsparung wird für private Anwender vernachlässigt, da dies aufgrund der wenigen Anwendungen pro Privatperson nicht ins Gewicht fällt.
3. Bei Unternehmen und staatlichen Einrichtungen wird der Aspekt Zeiteinsparung als Nutzen definiert, denn hier fällt die Masse ins Gewicht.
4. Eingesparte Portokosten werden nur als Nutzen gewertet, wenn der einzelne Anwender durch die Nutzung der elektronischen Signatur eine Vielzahl an Briefen pro Monat einsparen kann.
5. Des Weiteren gibt es Anwendungen, bei denen die Transaktion zwischen zwei Akteuren aus derselben Kundengruppe stattfindet. In diesem Fall werden in der Tabelle zwar die Kosten und der Nutzen bei der gleichen Akteursgruppe verbucht, dabei fallen die Kosten aber nicht bei demselben Signaturschlüsselinhaber an wie der Nutzen. Als Beispiele seien hier Homebanking und automatisierte Bestellung bei Lieferanten, genannt. Eine Ausnahme bilden die Anwendungsgebiete elektronische Rechnung und Archivierung. In diesen Fällen fallen sowohl die Kosten, als auch der Nutzen bei ein und demselben Signaturschlüsselinhaber an.

Die Ergebnisse der Kosten-/Nutzenanalyse sind in Tabelle 3 zusammengefasst.

	Privatpersonen		Unternehmen		Staatliche Einrichtungen	
	Kosten	*Nutzen*	*Kosten*	*Nutzen*	*Kosten*	*Nutzen*
Angebote zu Ausschreibungen			■	■		■
Elektronische Steuererklärung	■		■			■
Zugriff a. amtliche Verzeichnisse	■		■	■		■
Elektronische Wahlen	■					■
Beantragung von Dokumenten	■					■
Meldung n. Wohnungswechsel	■					■
Elektronische Mahnverfahren			■	■		■
Elektronische Marktplätze	■	■	■	■	■	■
Automatisierte Bestellung			■	■	■	■
Online- Banking	■		■	■	■	
Vertragsänderungen online	■			■		
Elektronische Rechnungen			■	■		
Archivierung			■	■	■	■
Summe	**8**	**1**	**9**	**9**	**4**	**10**

Tabelle 3: Kosten-/Nutzenverteilung für die einzelnen Signaturanwendungen

Die Analyse zeigt, dass ein Privatanwender bei allen acht potenziellen Anwendungen die Kosten für die Signaturerzeugung tragen muss und dabei nur bei einer einzigen Anwendung, der Teilnahme an elektronischen Marktplätzen, einen finanziellen Nutzen für sich verbuchen kann. Gleichzeitig müssen die Anbieter von Signaturanwendungen mit erheblichem Aufwand Signaturanwendungssysteme zur Verfügung stellen. Die aus beiden Aspekten sich ergebenden totalen Wechselkosten als Summe der Wechselkosten der Anwender und der Anbieter auf neue, signaturfähige Systeme sind immens und stellen einen Hinderungsgrund dar [SV98].Obendrein werden bei den meisten Verträgen für Zertifizierungsdienstleister Anschaffungs- und Jahresgebühren fällig, welche die Wechselkosten für die Nutzer noch erhöhen. Hohe Rüst- und Wechselkosten stehen bei der Diffusion neuer Technologien in der Theorie von Rogers [Ro03] allerdings im Widerspruch zur Eigenschaft der Ausprobierbarkeit („Triability“), die Eigenschaft erfolgreicher Innovationen ist. Nach Rogers muss eine Innovation experimentell ausprobierbar sein, ohne bereits folgenschwere Investitions- oder Infrastrukturentscheidungen treffen zu müssen. Ausprobierbare Innovationen stellen für einen neugierigen Anwender ein geringeres Risiko dar als Alles-oder-Nichts-Infrastrukturen. Unglücklicherweise sind viele der Anwendungen für Signaturen solche, die eine komplexe, vernetzte, integrierte Infrastruktur mit vielen Teilnehmern verlangen. Bei den Unternehmen ergibt sich ein sehr viel ausgeglicheneres Bild. Sie müssen bei neun von zehn potenziellen Anwendungen die Kosten tragen, können dafür aber auch bei neun Anwendungen einen finanziellen Nutzen aus der Verwendung einer elektronischen Signatur ziehen. Am Besten stellt sich die Situation für das Marktsegment staatliche Einrichtungen dar. In diesem Segment gibt es elf mögliche Anwendungen, wobei die staatliche Einrichtung nur in vier Fällen für die Kosten aufkommen muss.

Demgegenüber stehen zehn Anwendungen, bei denen sie finanziell von der Verwendung einer qualifizierten elektronischen Signatur profitieren. Nach der Analyse der Kosten-/Nutzenverteilung kann festgestellt werden, dass für die drei Marktsegmente Privatanwender, Unternehmen und staatliche Einrichtungen die Verteilung der Kosten nicht mit dem erzielten Nutzen übereinstimmen. Der Privatanwender wird hier deutlich benachteiligt. Er hat die meisten Kosten zu tragen, während die Unternehmen und staatlichen Einrichtungen den Nutzen für sich verbuchen können [Mo03].

Keine Preisdifferenzierung: Ein weiteres Problem liegt in der aktuellen Preisstruktur für Trust Center Produkte. Entscheidet sich ein Kunde für die Anschaffung einer personalisierten Chipkarte, kann er sich nicht zwischen verschiedenen Tarifen entscheiden. Dabei gibt es unterschiedliche Marktsegmente, die ganz unterschiedliche Verwendungsprofile haben. Dies wurde bei der Preisfestsetzung überhaupt nicht berücksichtigt. Vor allem fehlt ein attraktives Einstiegsangebot, um ganz gezielt neue Privatkunden zu gewinnen. In der Kundenwahrnehmung handelt es sich bei Signaturzertifikaten und den damit verbundenen Dienstleistungen um Informationsgüter. Hierbei erwartet man Skaleneffekte, die sich mindernd auf den Produktionspreis der angebotenen Informationsware auswirken. Je höher der Ausstoß der Informationsware, desto geringer sollte ihr Preis ausfallen [SV98].

Fokussierung auf Geschäftskunden: Wie in Kapitel 2 gezeigt, sprechen die Trust Center mit ihren Produkten und Lösungen hauptsächlich Unternehmen und staatliche Einrichtungen an. Es werden vor allem Lösungen für Massensignaturen, zum Beispiel für den elektronischen Rechnungsversand oder zur Archivierung angeboten. Auch die Preise sind für den Privatanwender wenig attraktiv. Die Ursache für diese Problematik ist nicht alleine bei den Trust Centern zu suchen, denn es gibt zurzeit kaum attraktive Anwendungsmöglichkeiten für den Privatverbraucher. Die E-Government-Initiativen stecken noch in der Anfangsphase, und andere Anwendungsmöglichkeiten gibt es nur wenige. Hier liegt aber auch das Grundproblem, denn solange nicht eine breite Masse über qualifizierte Zertifikate verfügt, wird auch kaum jemand bereit sein, Anwendungen für den privaten Signaturschlüsselinhaber zu entwickeln. Für die Trust Center steckt allerdings im Privatkundensegment ein großes Potential, denn erst wenn die Privatanwender mit dem Umgang von personalisierten Chipkarten vertraut sind, können die Unternehmen das ganze Potenzial der neuen Technik ausschöpfen. Für Unternehmen und staatliche Einrichtungen liegen viele Einsparungsmöglichkeiten in Anwendungen, an denen Privatpersonen beteiligt sind, so zum Beispiel der elektronische Rechnungsversand oder nahezu alle E-Government- Anwendungen.

4 Initiativen zur Förderung Qualifizierter Elektronischer Signaturen

Eine Möglichkeit die Durchsetzung der qualifizierten Signatur zu beschleunigen, ist das Aufbringen der Signaturfunktion auf bereits verbreitete Trägermedien, wie die Krankenversicherungskarte, der digitale Ausweis im Chipkartenformat und die JobCard. Im Folgenden werden wir diese Initiativen vorstellen und bewerten.

4.1 Gesundheitskarte

Mit dem am 1. Januar 2004 in Kraft getretenen Gesundheitsgesetz wurde die Ablösung der bisherigen Krankenversicherungskarte durch die elektronische Gesundheitskarte zum 1. Januar 2006 festgelegt. Die neue Gesundheitskarte soll neben den verwaltungstechnischen Daten der alten Krankenversichertenkarte auch das papiergebundene Rezept ersetzen und den Ärzten mit Hilfe von abgestuften Zugangsrechten den Zugriff auf Patientenakten freigeben. Außerdem wird auf der Rückseite ein Auslandskrankenschein abgebildet sein [He204]. Wird diese elektronische Gesundheitskarte mit einer Signaturfunktion ausgestattet, verfügen schon 2006 mehr als 80 Millionen Versicherte [Si04] über eine Signaturkarte. Eine Ausstellung von Gesundheitskarten mit Signaturfunktion würde die Situation am Markt kaum verändern. Lediglich die Subvention der Karte und der Zertifikatsausstellung würde auf den Beitragszahler der Krankenversicherungen umgelegt. Die Rüstkosten für den heimischen PC des Anwenders, Kartenleser und Treibersoftware bleiben. Skaleneffekte könnten – bei vorhandenem Angebot von Anwendungen – allerdings eintreten. Da die Gesundheitskarte kein offener Standard ist, dürfte es schwierig werden, Attributzertifikate später zur Karte hinzuzuladen oder das zuständige Trust Center zu wechseln, falls die Angebote unattraktiv werden oder andere attraktivere Angebote entstehen. Wie die Zertifizierungsdienstleistung als solche auf Basis der Gesundheitskarte bepreist werden kann, ist völlig unklar.

4.2 Elektronischer Personalausweis

Unter anderem Italien, Estland, Belgien und Finnland haben bereits den Personalausweis mit Signaturfunktion. Auch in Deutschland gibt es derzeit Überlegungen einen solchen Ausweis einzuführen [FS04]. Er soll dieselben Sicherheitsmerkmale wie der aktuelle Personalausweis haben und zusätzlich das qualifizierte elektronische Signieren ermöglichen. Dies wäre eine große Chance für die Verbreitung der elektronischen Signatur, doch es gibt Einwände [He04]. Pro Jahr werden nur rund 10 Prozent aller Personalausweise erneuert, weshalb sich die Signaturfunktion relativ langsam verbreiten würde. Außerdem ist es nicht sicher, ob die verwendeten kryptographischen Lösungen den Gültigkeitszeitraum eines Personalausweises von 10 Jahren überstehen würden. Aus Sicht der Diffusionstheorie ist bei der Einführung eines Ausweises mit Signaturfunktion der Markt immer noch darauf angewiesen, dass eine starke Nachfrage nach der Signaturfunktion die Nutzer dazu bringt, sich schnell neue Personalausweise zu beschaffen, da ansonsten eine kritische Masse mit den Erneuerungszyklen der Ausweisausgabe zu langsam entsteht und Skaleneffekte erst spät eintreten können [SV98]. Rüstkosten entstehen immer noch durch Anschaffung und Installation von Kartenleser und Treibersoftware. Auch hier müssen Anwendungen für Nutzer zum Einsatz kommen, welche die Rüstkosten durch Nutzen aufwiegen. Unklar ist beim Personalausweis, ob und wie nachträgliche Attributzertifikate oder Wechsel der Zertifizierungsdiensteanbieter technisch und preislich gelöst werden können.

4.3 Job Card

Im August 2002 hat die Bundesregierung beschlossen, bis zum Jan. 2006 für alle Arbeitnehmer eine JobCard einzuführen [IT04]. Die Arbeitsverwaltung soll so unkomplizierten Zugriff auf Beschäftigungszeiten, auf die Höhe der Entgeltzahlungen und auf Angaben über die Auflösung eines Beschäftigungsverhältnisses bekommen. Der Zugriffsschutz auf die zentral gespeicherten Leistungsdaten kann durch die signaturgesetzkonforme Signaturkarte gewährleistet werden. Die Arbeitgeber könnten durch die JobCard rund 500 Millionen Euro jährlich einsparen, da rund 60 Millionen ausgedruckte Dienstbescheinigungen an die Behörden und die Archivierung wegfallen würden [He04]. Durch die Realisierung der JobCard würden ab 2006 circa 40 Millionen Arbeitnehmer [Si04] über eine Signaturkarte verfügen.. Die JobCard hat ähnliche Eigenschaften wie die Gesundheitskarte. Sie wird von der Arbeitnehmerschaft mit Abgaben finanziert und dient vor allem der öffentlichen Verwaltung zur Effizienzsteigerung von Prozessen. Der spezifische Nutzen für die Träger der Karten ist unklar. Hohe Skaleneffekte sind möglich, falls der Verbreitung der Karten entsprechende Anwendungen gegenüber stehen. Für private Nutzung durch den Endnutzer sind Rüstkosten für Lesegeräte und Softwareinstallationen notwendig.

4.4 Mobile Signaturen

Das Mobile Electronic Signature Consortium (mSign), dessen Aufgabe es war, eine sichere applikationsübergreifende Infrastruktur für den Einsatz mobiler Signaturen zu entwickeln, hat 2000 eine Lösung für mobile Signaturen vorgestellt [Ms00]. Hierbei handelt es sich um einen Dienst, der die eigentliche Signaturerstellung an einen Signierserver delegiert. Wie in [R+03] gezeigt, ist eine solche Infrastruktur für qualifizierte Signaturen nach dem Signaturgesetz (SigG) ungeeignet. Die mSign Lösung ist zusätzlich an unzureichender Technik gescheitert und mittlerweile in Raddiccio [Ra04] integriert. Vielversprechender erscheint hier der Ansatz zu sein, eine Lösung auf Basis einer signaturfähigen SIM Karte anzustreben [FR04]. Mit der WIM Spezifikation der Open Mobile Alliance (OMA) existiert bereits ein technisch ausgereifter Standard [OM02] und im Rahmen des EU Projektes Wireless Trust for mobile Business (WiTness) wurde eine solche signaturfähige SIM Karte entwickelt [Wi04]. Eine mobile Signatur auf Basis einer signaturfähigen und nach Common Criteria evaluierten SIM Karte würde, wie in [R+03] gezeigt, die Anforderungen durch das SigG erfüllen. Bisher konnte sich die WIM aufgrund fehlender Geschäftsmodelle noch nicht am Markt etablieren, aber in [Ro04] wurde eine flexible Zertifizierungsmöglichkeit vorgestellt, die im Folgenden kurz dargestellt wird.

Certification on Demand (CoD)

Bei diesem Konzept wird der Vertrieb von signaturfähigen Smart Cards in die Vertriebsstruktur der Mobilfunkprovider eingegliedert, ohne dass die Kunden an ein bestimmtes Trust Center gebunden werden. Dazu werden beim SmartCard- Hersteller zusätzlich zur Teilnehmerkennung IMSI und dem individuellen Schlüssel Ki, ein Schlüsselgenerator für Signaturschlüsselpaare und der öffentlichen Schlüssel der

RootCA auf die SIM-Karte aufgebracht. Der Mobilfunkprovider übergibt dann die Karte zusammen mit einer Nullpin zur Aktivierung der Signierfunktion, seinem Kunden, der sofort nach Erhalt die Telefon- und Datenübertragungsfunktion nutzten kann. Interessiert sich der Kunde auch für die Signaturfunktion, kann er sich bei einer Registrierungsstelle identifizieren lassen und seinen öffentlichen Schlüssel hinterlegen. Außerdem übermittelt der Kunde seine mit dem privaten Schlüssel chiffrierten Identifikationsdaten an das Trust Center. Gleichzeitig übermittelt die Registrierungsstelle den öffentlichen Schlüssel und die Identifikationsdaten des Kunden an das Trust Center. Stimmen die von der Registrierungsstelle übermittelten Daten mit den vom Kunden übermittelten Daten überein, stellt das Trust Center ein Zertifikat aus und sendet es direkt an das mobile Endgerät. Durch das von der RootCA für das Trust Center ausgestellte Zertifikat kann der Kunde die Gültigkeit seines Zertifikates überprüfen [Ro04]. Dadurch könnten auch völlig neue Geschäftsfelder erschlossen werden, beispielsweise im Zusammenhang mit Location Based Services. Daher ist für Kunden von mobilen Signaturen ein kundenspezifischer Nutzen vorhanden (Mobilität des Signiermittels). Auch die Rüstkosten sind als relativ gering zu betrachten, da lediglich eine neue SIM- Karte mit Kryptofunktionalität, sowie eine Signatursoftware zusätzlich zum vorhandenen Mobiltelefon notwendig sind. Diese Anschaffungskosten könnten wiederum vom Mobilfunker subventioniert werden, der durch den durch mobile Signaturapplikationen entstehenden Traffic Gewinne erzielen kann. Durch die nachträgliche Zertifizierung mit COD entstehen beim Wechsel zu einem anderen Zertifizierungsanbieter kaum Wechselkosten. Auch die Eigenschaft der Ausprobierbarkeit ist mittels Certification on Demand gegeben, da der potentielle Nutzer die Signaturfunktionalität erproben kann, bevor Kosten für die Zertifizierung entstehen.

4.5 Bewertung

Die Ausprobierbarkeit bei den in den Abschnitten 4.1 – 4.3 vorgestellten drei Initiativen ist sehr gering –der Nutzer bekommt eine Karte in die Hand, deren Zusatznutzen er sich selbst erschließen muss. Damit verschafft keine der drei Lösungen dem Nutzer in den Feldern Triability, Bepreisung und Rüstkosten einen wesentlichen Vorteil. Einzig auf Skaleneffekte bei breiter Streuung der Trägertechnologie in der Bevölkerung scheint hier gehofft zu werden. Es handelt sich um eine Fortschreibung des bisherigen Vertriebs von Signaturzertifikaten mit der Schrotschußmethode – hier werden viele Millionen Signaturkarten an Bürger ausgegeben, die weder über einen PC noch über einen Internetzugang verfügen. Die Finanzierung der Infrastruktur übernimmt in den drei Modellen im Wesentlichen der Steuerzahler. Interoperabilität und Standardisierug der verwendeten Sicherheitstechnologien ist indes nicht zu erwarten. Daher dürften die Netzwerkeffekte und Skaleneffekte insbesondere in der Anfangsphase langsamer anlaufen als von den Proponenten der Initiativen erhofft. Als Beispiel kann hier die dänische Signaturinitiative OCES („Offentlige Certifikater for Elektroniske Services“) genannt werden. Dieses von der dänischen Regierung im März 2003 gestartete Projekt ermöglicht es jedem Bürger ein kostenloses Zertifikat zu erhalten. Bisher besitzen allerdings erst 145.000 dänische Bürger (weniger als 3% der Bevölkerung) eine solche Signatur [Hv04].

Weiterhin besteht die Gefahr, dass durch die subventionierte Ausgabe von Signaturkarten, ein Zertifizierungsanbieter eine Monopolstellung erlangt und somit ein Wettbewerb im Zertifizierungsmarkt zerstört wird.

Die mobile Signatur birgt gegenüber der herkömmlichen auf einem PC erzeugten Signatur einige Vorteile. Das mobile Endgerät, wie ein Mobiltelefon, ein PDA oder eine Kombination aus beiden, ist heute für einen Großteil der Bevölkerung zu einem ständigen Begleiter geworden. Der Umgang mit den mobilen Geräten ist den Menschen mehr vertraut als der Umgang mit Chipkartenleser und Smart Card. Ein weiterer großer Vorteil der mobilen Signatur sind die Analogien zur eigenhändigen Unterschrift. Eine eigenhändige Unterschrift kann jederzeit mit einfach verfügbaren Mitteln und ortsunabhängig geleistet werden. Dies würde durch die qualifizierte mobile Signatur auch ermöglicht. Durch die Vertrautheit der Anwender mit dem Mobiltelefon und durch die gewonnene Mobilität entsteht ein höherer relativer Kundennutzen gegenüber den herkömmlichen Signiersystemen. Des Weiteren zeichnet sich die hier skizzierte mobile Signatur durch geringe Rüstkosten, ein höheres Maß an Ausprobierbarkeit und geringere Wechselkosten aus.Hilfreich für die Durchsetzung der mobilen Signatur könnte die Tatsache sein, dass es schon heute mehr Mobilfunkkunden (78,3 Prozent [Re03] der Gesamtbevölkerung) als Internet-Teilnehmer (58 Prozent [Re03] der Erwachsenen) gibt.

5 Zusammenfassung

Nach der Analyse des aktuellen Marktes und der Zukunftsinitiativen sind wir überzeugt, dass bei Regulierung und Implementierung des Marktes für Zertifizierungsdienste wesentliche wirtschaftliche Mechanismen unbeachtet blieben. Zur Gestaltung eines zukünftigen, wirtschaftlich funktionierenden Marktes sollten die wirtschaftlichen Mechanismen ausreichend berücksichtigt werden. Als wesentliche Mechanismen konnten identifiziert werden:

- **Ausprobierbarkeit der Signaturinfrastruktur**: Die probeweise Teilnahme an Zertifizierungsinfrastrukturen und Signaturanwendungen muss ohne große Investitionen möglich sein. Nur so können durch positive Rückkopplung und überzeugte Nutzer große Nutzerzahlen überhaupt erreicht werden. Die Signaturtechnologie sollte sich an verbreiteter Technologie orientieren, ohne Zeitverträge erprobbar sein und das Testen und Vergleichen mehrerer Anwender erlauben.

- **Rüstkosten für Nutzer**: Installationskosten für Nutzer sollten gering ausfallen. Installationsgebühren, teure Hardware, aufwändige Installationen und Umstellung von Anwendungssystemen verhindern die Diffusion von neuen Signatursystemen in den etablierten Markt.

- **Wechselkosten für Nutzer**: Zur Erzeugung von Wettbewerb und zum Erhalt der Kundenzufriedenheit ist es unerlässlich, die Wechselkosten für Nutzer gering zu halten. Ist ein Nutzer mit einem Anbieter unzufrieden, so etabliert sich ein gesunder Markt nur, wenn der Nutzer Alternativen hat, seine Zertifizierungsdienstleistung zu beziehen. Der Wechsel zu einem anderen Anbieter muss mit vernünftigem Aufwand machbar sein – insbesondere kommen das Auswechseln von Kartenterminals, Ändern von Treibersoftware und der Wechsel ganzer Anwendungssysteme nicht in Frage.

- **Spezifische Anwendernutzen**: Signaturangebote müssen den spezifischen Anwendernutzen in den Vordergrund rücken. Ohne einen neuen, oder wesentlich verbesserten Nutzen im Vergleich zum etablieren Signaturangebot wird kein Nutzer die Technologie adaptieren. Mögliche Anwendernutzen sind mehr Flexibilität, mehr Mobilität (bei mobilen Signaturen) und mehr Einsatzmöglichkeiten.

- **Kosten-Nutzen-Verhältnis**: Die Neugestaltung des Signaturmarktes muss eine bessere Symmetrie des Kosten-Nutzen-Verhältnises zwischen den Nutzern und den Anbietern von Signaturtechnik implementieren, damit Investitionen in die Technik auf beiden Seiten Gewinne abwerfen [LR05].

- **Preisdifferenzierung**: Die Bepreisung der Zertifizierungsdienste spielt eine wesentliche Rolle bei der Marktakzeptanz. Von den bisherigen Modellen, die im Wesentlichen aus Paketpreisen und Grundgebühr bestanden muss abgerückt werden. Eine nutzenorientierte und anwendungsorientierte Preisdifferenzierung drückt den Nutzen besser aus, der leztendlich gezahlt wird. Die Nutzniesser des Signatureinsatzes sollten die Kosten tragen. Ein Beispielmodell zur Finanzierung eines Zertifizierungsdienstes über Verzeichnisgebühren findet sich in [LR05].

- **Standardisierung**: Technische Standards müssen vor der Produktentwicklung und nicht danach spezifiziert werden. Wechsel und Wettbewerb können nur in standardisierten Umgebungen zu vernünftigen Kosten stattfinden.

Bei Berücksichtigung der oben genannten Kriterien erscheinen die staatlichen Initiativen zur Verbreitung von Signaturen auf Chipkarten wenig erfolgversprechend. Mobile Signaturen mit Certification on Demand hingegen haben das Potential, den Signatur- und Zertifizierungsdienstleistungsmarkt von Grund auf neu auszurichten. Die Fokussierung auf Mobilfunkteilnehmer, die Verwendung der vorhandenen Terminals sowie das flexible Protokoll zum Wechsel oder Nachladen von Zertifikaten bei Anbieterwechsel oder dem Annehmen neuer Angebote schaffen eine wesentliche Voraussetzung für geringe Wechselkosten und geringe Rüstkosten. Ausprobierbarkeit ist gegeben, und der spezifische Anwendernutzen, welcher in den Vordergrund tritt, ist die Mobilität des Signiermittels und seiner Einsatzumgebung zusammen mit dem Nutzer. Skaleneffekte mobiler Signaturen stehen den staatlichen Karten nicht nach, wenn man berücksichtigt, dass es in Deutschland im Mai 2003 laut RegTP mehr als 60 Millionen Mobilfunknutzer gab.

Literaturverzeichnis

[Dt02] Jahresabschlüsse der D-Trust GmbH, zu den Geschäftsjahren 2001 und 2002.

[FS04] Project "Feasibility Study Electronic Identity Card", http:// www.uni-kassel.de/fb10/oeff_recht/english/projekte/projekteDigiPerso_eng.ghk

[FR04] L. Fritsch; H. Rossnagel: SIM based Mobile Electronic Signatures: Enabling M-Business with Certification on Demand. Card Forum International Vol.8 Nr.1 Jan/Feb 2004.

[HB00] A. Hillenbrand; F. Büllingen: Erfolgsfaktoren digitaler Signaturen, in: Datenschutz und Datensicherheit, Jg. 24, Heft 2, Seiten 80-84.

[He04] Heise online: Markt für E-Signaturen kommt langsam in Schwung, www.heise.de/newsticker/meldung/43695, (16.01.2004).

[He204] Heise online: Mit der Gesundheitskarte im Zeitplan, www.heise.de/newsticker/meldung/43653, (30.03.2004).

[Hv04] J. Hvarre: Electronic signatures in Denmark: free for all citizens; In: e-signature and law journal, vol. 1 , no1, 2004

[IS04] ISIS-MTT Spezifikation, http://www.teletrust.de/anwend.asp?id=30410&Sprache=D_&HomePG=0

[IT04] ITSG Informationstechnische Servicestelle der Gesetzlichen Krankenversicherung GmbH: die JobCard, www.itsg.de/download/BroschuereJobcard.pdf, (30.03.2004).

[LR05] S. Lippmann, H. Rossnagel: Geschäftsmodelle für signaturgesetzkonforme Trust Center; erscheint in: Tagungsband der 7. internationalen Tagung Wirtschaftsinformatik 2005

[Me03] Meta Group: Unternehmensprofil T-Systems International GmbH, erstellt im Rahmen der Studie IT-Security im Jahr 2003, www.metagroup.de/studien/2003/security/profile/tsystems-profile.pdf, (12.01.2004).

[Mo03] R. Mock-Hecker: Digitale Signatur – Nutzenpotenziale und Stand der Einführung; Vortrag im Rahmen der Omnicard Berlin am 15.01.2003, www.s-trust.de/veranstaltungen/omnicard_2003_vortrag.pdf (31.03.2004).

[Ms00] Mobile Electronic Signature Consortium: mSign Business White Paper, 2000

[OM02] Open Mobile Alliance: Wireless Identity Module Version 1.1; 24.10.2002; member.openmobilealliance.org/ftp/Public_documents/SEC/Permanent_documents/

[R+03] J. Ranke; L. Fritsch; H. Rossnagel: M-Signaturen aus rechtlicher Sicht; in: Datenschutz und Datensicherheit, 27. Jg., Heft 2, S. 95-100.

[Ra04] Radicchio, www.radicchio.org

[Re03] Regulierungsbehörde für Telekommunikation und Post: Jahresbericht 2003, www.regtp.de/imperia/md/content/aktuelles/jb2003.pdf, (07.03.2004).

[Ro03] E.M. Rogers: Diffusion of Innovation, Fifth Edition, Free Press 2003

[Ro04] H. Rossnagel: Mobile Qualified Electronic Signatures and Certification on Demand, Proceedings of the 1st European PKI-Workshop Research and Applications (EuroPKI 2004), Springer LNCS 3093, S. 274-286.

[SV98] Shapiro, C.; Varian, H.R.: Information rules: A strategic Guide to the Network Economy, Boston 1998

[Si02] Jahresabschlüsse der Deutsche Post Signtrust GmbH, zu den Geschäftsjahren 2001 und 2002.

[Si04] R. Sietmann: Chipkarten im Aufwind, in c't 2004, Heft 3, S.26 – 28.

[Si204] Signaturbündnis, www.signaturbuendnis.de , (10.07.2004)

[T704] T7 – ISIS, www.t7-isis.de, (10.07.2004)

[Wi04] European IST Project „Wireless Trust for Mobile Business"(WiTness): SIM Application Hosting - Detailed description of the concept, www.wireless-trust.org/publicdocs/Witness_32275_D4_ExecSum.pdf, (1.11.2004)