DIGITALE ZERTIFIKATE – MARKT, BEDEUTUNG, ENTWICKLUNG

EINE ÜBERSICHT

INHALTSVERZEICHNIS

1. MANAGEMENT SUMMARY

Die Mitteilung, der einzige Schweizerische Zertifizierungsdienstenabieter stelle seinen Dienst ein, hat im letzten Jahr zu einiger Aufregung in der Presse und Teilen der Wirtschaft geführt sowie Reaktionen von amtlicher Stelle provoziert[1]. In der Zwischenzeit drängen neue Anbieter mit identischem Businessmodell auf den Schweizer Markt (Eurotrust/VeriSign, Signtrust u.a.).Man hat den Eindruck, es handle sich hier um ein derart wichtiges Thema, dass sich höchste Regierungsstellen, ja sogar das Parlament damit befassen müssten. Ist diese Aufregung berechtigt und wenn ja, was ist zu tun? In diesem Artikel wird aufgezeigt, welche Bedeutung den Zertifizierungsinstanzen zukommt, welche rechtlichen Grundlagen eine wichtige Rolle spielen und welche Lösungen sich in der Wirtschaftswelt etablieren werden. Dieser Artikel hat zum Ziel, die ganze Thematik „Digitale Signaturen" und „Zertifizierungsdienste" aus der Sicht der Marktteilnehmer zu beleuchten. Es wird deshalb darauf verzichtet, die Rechtsquellen detailliert zu zitieren.

Es wurde versucht, die geltenden Regeln möglichst länderneutral darzustellen. Wenn etwas von grösster Bedeutung für das Verständnis der behandelten Thematik ist, dann die Internationalität der Sachverhalte. Es ist eine Tatsache, dass Geschäftsfälle mit internationalem Bezug auch für KMUs immer mehr Bedeutung erlangen. Die Schweiz folgt beim elektronischen Geschäftsverkehr mehrheitlich den Regeln der EU. Die Schweiz hat jedoch eine gewisse Leaderrolle übernommen, da sie als eines der ersten Länder Europas über eine Gesetzgebung verfügt, die eine vollumfängliche elektronische Abwicklung von Geschäftstransaktionen ermöglicht. Mehr dazu im Kapitel 2.

Zertifikatssysteme dienen u.a. der Identifikation eines Marktteilnehmers bzw. Bürgers. Es wird eine Vielzahl von Systemen entstehen, die die Identifikation einer Person zulassen, die aber nicht zwingenderweise gesetzeskonform (nach Signaturgesetz) sein werden. Dazu zählen die netzwerkbasierten Identifikationssysteme, wie sie für die übergreifende Nutzung von Internet Diensten zur Anwendung kommen werden[2]. Identifikationssystem ist eben nicht automatisch gleich Signatursystem, eine differenzierte Betrachtung tut not.

Die Marktentwicklung in diesem Bereich ist noch recht offen, trotzdem zeichnen sich einige zentrale Trends ab. So lässt sich der Zertifizierungsdiensteanbieter, wie er in den Signaturgesetzen beschrieben wurde, unter ökonomischen Bedingungen nicht in die Praxis übertragen. Es erfolgt eine Differenzierung der Funktion als auch des Angebots. Für die Marktteilnehmer bedeutet dieses Enwicklung einen Fortschritt, da die Verschlankung der Prozesse zu einer Kostenoptimierung und zu einer besseren Preisstruktur führen wird.

Für E-Government Anwendungen wird es unumgänglich sein, eine eigene Registrierungsstelle zu betreiben und Zertifikate als service publique anzubieten. Dies bedeutet aber nicht, dass der Staat die gesamte Infrastruktur aufbauen muss. Eine effiziente Funktionsverteilung dürfte der Schlüssel zum Erfolg werden. Der Auftritt der heute auf dem Markt aktiven Anbieter wird sich auf Grund der ökonomischen Gesetzmässigkeiten in der nächsten Zeit wesentlich verändern. Sonst besteht nur sehr geringe Chance, dass sie als Unternehmen erfolgreich sein werden.

---

[1] Artikel in der NZZ vom 25. Mai 2001: http://www.nzz.ch/2001/05/25/em/page-article7ECWZ.html und http://www.nzz.ch/2001/05/25/em/page-article7EWHP.html).

[2] In letzter Zeit ist hier vor allem Microsoft mit ihrer .NET Initiative aktiv geworden, die eine Komponete namens „Passport" enthält. Dies ist eine digitale Identität zur Verwendung der .NET Dienste. Vergleichbare Dienste wurden auch von AOL und SUN angekündigt.

2. DIE PRAKTISCHE BEDEUTUNG DER DIGITALEN SIGNATUR

Um zu verstehen, welche Bedeutung Digitalen Signaturen im B2B-Bereich heute zukommt, sei dies an einem kurzen Beispiel dargestellt:

Ein Unternehmen U bestellt Ware bei einem Lieferanten L. Es besteht seit Jahren eine E-Commerce Lösung, welche den Austausch elektronischer Rechnungen ermöglicht (z.B. EDIFACT und neu XML basierend). Bis anhin wurden die verschickten Rechnungen von L von beiden Parteien fein säuberlich auf Papier gebracht und physisch archiviert. Durch die Änderung der MWSt Verordnung und der dazugehörenden Ausführungsbestimmungen[3] wird es den Parteien nun ermöglicht, die Rechnungen nur noch als Datenstrom zu versenden, sofern diese digital signiert sind. Folglich unterschreibt L seine Rechnungen an U und andere Kunden mit einer *Digitalen Signatur*. Die Prüfung durch U erfolgt unmittelbar bei Erhalt und umfasst im einfachen Fall die Verifikation der Signatur, im erweiterten die Prüfung der Unterschriftsberechtigung und allenfalls bereits die Überprüfung spezieller, anwendungsspezifischer Elemente. Anschliessend wird eine signierte Empfangsbestätigung geschickt und die Daten werden elektronisch archiviert, wie dies in den revidierten Aufbewahrungsvorschriften OR 962ff. nun generell zulässig ist[4]. Im Falle einer Revision kann der Revisor nun mittels technischer Hilfsmittel die Rechnungen bei Sender und Empfänger abgleichen und sich Gewähr verschaffen, ob die Rechnungen ordnungsgemäss ausgestellt wurden. Dazu muss er die damals gültigen Schlüssel, bzw. Zertifikate der Parteien kennen. Diese wurden durch die Parteien ebenfalls archiviert (entweder durch sie selbst oder durch einen beauftragten Dritten[5]). Sowohl U wie auch L müssen über die Software verfügen, die es ermöglicht, Rechnungen digital zu signieren bzw. zu prüfen. Dazu gehören ferner die erwähnten Zertifikate (mehr dazu unten) sowie Hardware in Form einer Smartcard oder eines sogenannten „Tokens" (z.B. einen einfachen Speicherbaustein, welcher am USB Anschluss des Endgeräts angeschlossen werden kann). Zusätzlich muss die Archivierungssoftware in der Lage sein, Zugriffe auf alte Signaturen zu ermöglichen, bzw. diese zu verifizieren (Anforderung der Revisionsfähigkeit).

[3] Verordnung des EFD über elektronisch übermittelte Daten und informationen, in Kraft ab 1.3.2002, http://www.admin.ch/ch/d/as/2002/259.pdf
[4] Im Parlament am 22.12.1999 verabschiedet
[5] Hier kommt EBPP (Electronic Bill Presentment and Payment) Anbietern eine grosse Bedeutung zu.

3. WAS REGELT EIN SIGNATURGESETZ?

Die *Digitale Signatur*[6] (dies ist das technische Verfahren, welches der *Elektronischen Signatur* nach schweizerischem Verständnis zu Grunde liegt[7]), ermöglicht es, die Teilnehmer einer elektronischen Transaktion unzweifelhaft zu identifizieren, die integrität der Transaktion sicherzustellen und die gesetzliche Vermutung der sogenannten Nichtabstreitbarkeit[8] zu statuieren. Gleichzeitig wird eine hohe Beweiskraft erzielt, indem die Eigenschaften der eigenhändigen Unterschrift[9] abgebildet und mit weiteren Sicherheitsmerkmalen ergänzt werden.

Für den Einsatz der *Digitalen Signatur* bedarf es einer umfassenden Infrastruktur (sog. Public Key Infrastruktur, PKI). Die nachfolgende Grafik zeigt die Prozesse, die bereitgestellt werden müssen:

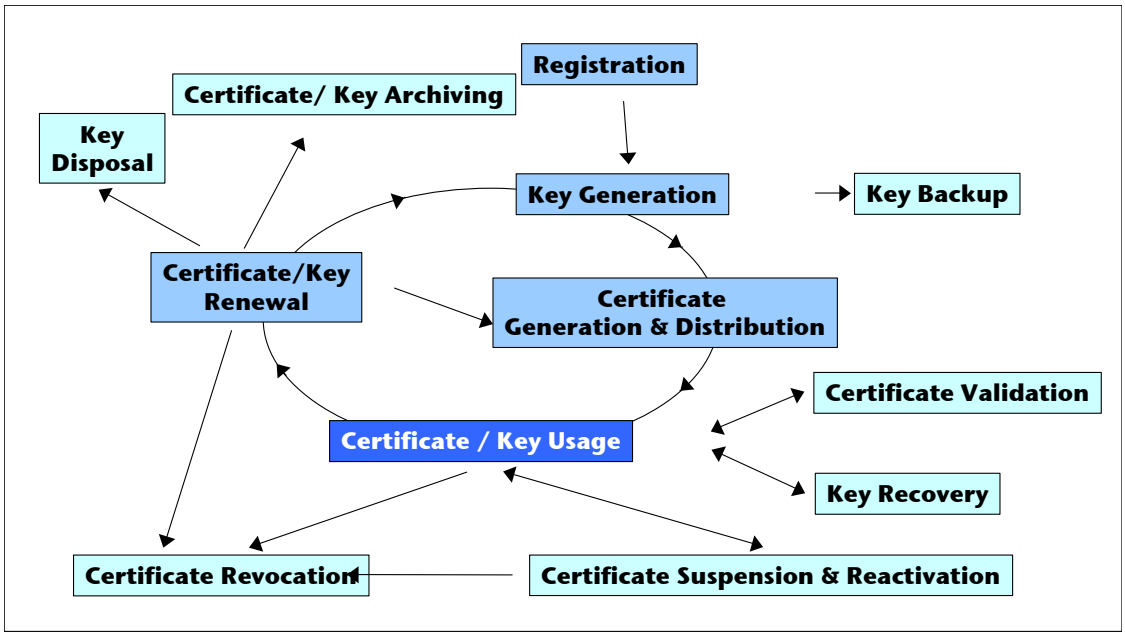

Fig. 1 Funktionen

Die Prozesse im inneren Kreis bilden das Gerüst, die tragende Struktur der PKI. Die Aussenprozesse sind zwar ebenfalls sehr wichtig, werden aber nur unter bestimmten Bedingungen durchlaufen. Schlüsselgenerierung und Zertifizierung als auch Verteilung sind hingegen für das minimale Funktionieren des Systems unbedingt notwendig. Zentrale Bestimmungen sind diejenigen, welche das Erzeugen und die Behandlung des privaten Schlüssels enthalten. Sie sind für die Sicherheit und Vertrauenswürdigkeit des Gesamtsystems entscheidend, nicht aber für den Business Case (mehr dazu in 4).

In den heutigen Gesetze und Verordnungen wird implizit von einer zentralisierte Infrastruktur ausgegangen. Mit der Praxis hat dieses Bild allerdings nicht mehr viel gemein. In fortgeschrittenen Systemen werden die einzelnen Funktionen dezentralisiert und verteilt. Hier klafft eine Lücke zwischen

[6] Vgl. dazu das Tutorial in http://www.itrust.ch/deutsch/articles/Digitale_Signatur.pdf
[7] Entgegen der ungenauen Definition im schweizerischen Signaturgesetz wird in diesem Artikel konsequent an der international üblichen Terminologie festgehalten. Unter *Elektronischer Signatur* verstehen wir alle Verfahren, die geeignet sind, die Unterschriftsfunktionen abzubilden.
[8] Hier angelehnt an den Begriff aus dem Eglischen: „non repudiation“
[9] Vgl. Bruno Wildhaber, „Informationssicherheit – Rechtliche Grundlagen und Anforderungen an die Praxis“, Diss., Zürich 1993, 178ff.

der gesetzlichen Idealvorstellung und den aktuellen Entwicklungen. Wieso sich diese Entwicklung ergeben hat, zeigt sich bei den ökonomischen Betrachtungen (vgl. 4.2).

4. ÖKONOMISCHE TATSACHEN

4.1 ENABLING TECHNOLOGIE?

Man darf sich nicht der Illusion hingeben, mit Zertifizierungsinstanzen würde die ganze E-Society unmittelbar aufblühen. In Deutschland hatte das Signaturgesetz keine beschleunigende Auswirkung auf die Umsetzung des E-Commerce[10]. Wie immer, wenn eine neue Technologie auf den Markt kommt, sind die Erwartungen grenzenlos, die Ernüchterung folgt meist auf dem Fuss. Dies gilt insbesondere dann, wenn es sich um ein Verfahren handelt, welches eine radikale Änderung der Verhaltensweise des Einzelnen erfordert. Wer sich dies veranschaulichen möchte, vergleiche die Entwicklung des Warentausches bis zum Geldschein und wie lange es gedauert hat, bis sich die Anwender damit abfinden konnten, statt Münzen ein Stück Papier in der Hand zu halten (in Europa ungefähr 3500 Jahre)[11]. Hinzu kommt die Tatsache, dass niemand eine geschäftliche Transaktion auf eine neue und unbekannte Weise ausführt, nur weil die technische Infrastruktur dazu vorhanden ist. Viel bedeutender ist es, mit dem neuen Verfahren neue Anwendungen zu ermöglichen, die sich in klingende Münze umsetzen lassen (vgl. dazu 4.5). Dies ist bei der Digitalen Signatur definitiv nicht der Fall, da es sich um eine reine Infrastrukturkomponente handelt. Verträge wurden abgeschlossen, bevor man die Schrift kannte!

4.2 ROLLEN

Wenn man die Struktur des Marktes betrachtet, so ist sie sehr ähnlich wie diejenige in der Mobiltelefonie, bzw. dem Internet. Die Teilnehmer sind:

- Endkunden (Private/Unternehmen/Behörden)
- Infrastrukur Anbieter (Netzwerk, Endgeräte, SIM und *Token Produzenten*, *Zertifikate*)
- Applikationsanbieter (teilweise identisch mit Endkunden)
- Operators (ISP, Mobiltelefon Anbieter etc.)

Der Endkunde benötigt die Infrastruktur, um am elektronischen Verkehr teilnehmen zu können. Für den Kunden ist der Aussteller des Zertifikats etwa so interessant wie der Hersteller des SIM Chips, der in seinem Mobiltelefon steckt. Nun kann man mit SIM Chips sicher gutes Geld verdienen, doch ist die Anzahl der Hersteller auf wenige beschränkt. Es sind dies dieselben, die auch Smartcards für digitale Signaturen produzieren. Mit anderen Worten, das Erzeugen von Zertifikaten und das Produzieren von Hardware Tokens wie Smartcards ist ein absolutes Massengeschäft, wo nur „Economies of Scale" gelten. Der Markt wird aber vom Anwendungsanbieter beherrscht. In der Regel ist dieser identisch mit dem Betreiber der Registrierungsinstanz. Der Mobiltelefonanbieter bestimmt, welche Karte er verwenden will und welcher Anbieter zum Zug kommt. Die Produktion der Zertifikate und Karten kann geografisch unabhängig erfolgen. Alle diese Faktoren führen dazu, dass Zertifizierungsinstanzen nach dem Modell „Signaturgesetz" unheimlich grosse Mengen an Zertifikaten erstellen müssten, um kostendeckend zu sein.

[10] Aus neuhistorischer Sicht zu diesem Thema Rueppel/Wildhaber:„Public Key Infrastrukturen – Survey and Issues", bei Horster (Hrsg.): Trust Center, Braunschweig/Wiesbaden 1995.
[11] http://www.wdr.de/online/wirtschaft/euro/geldgeschichte.phtml

Einen vernünftigen ROI kann man nur mit einer klaren Positionierung und guten Marktbearbeitung erwirtschaften.

4.3 ZERTIFIKATSKLASSEN

In der aktuellen Diskussion wird meist vernachlässigt, dass es DAS Identifikationssystem nicht gibt. Bereits heute verwenden wir unterschiedlichste Hilfsmittel, um uns im täglichen Leben zu identifizieren. Wann verwenden Sie ihren Pass, wann Ihre ID, wann greifen Sie auf Ihren Fahrausweis oder vielleicht auf die Kundenkarte des Grossverteilers zurück? Dieselbe Situation wird sich auch in der virtuellen Welt ergeben. Keine ID wird jemals alle Bedürfnisse abdecken. Auch wenn sie dies könnte, würden wir sie vermutlich schon aus Gründen des Datenschutzes niemals verwenden wollen. Aus diesem Grund sollte man konsequent in Zertifikats, Identitäts- oder Signaturklassen denken. Diese Klassen sind für den Business Case der Infrastruktur entscheidend. Je weniger Klassen ich ausstellen kann, umso kleiner kann meine Infrastruktur sein, bzw. ich muss mir den Aufbau meiner PKI genau überlegen. Die Klassen unterscheiden sich durch den Aufwand, welcher für dier Erstellung und die Verwaltung notwendig ist. Zur Ausgabe eines Zertifikates nach Signaturgesetz braucht man eine teure Infrastruktur und ein umfassendes Regelwerk. Für ein Zertifikat zur E-Mail Verschlüsselung innerhalb eines geschlossenen Systems sind im Verhältnis wesentlich geringere Aufwendungen notwendig.

4.4 KOSTEN

Man kann davon ausgehen, dass die höherwertigen Zertifikate, wie sie im Signaturgesetz verlangt werden, sicherlich höhere Kosten verursachen als ein einfaches Zertifikat, wie man es z.B. zur Verschlüsselung von E-Mails benötigt. Wir sind bereit, für einen Pass eine doch ziemlich hohe Gebühr für die Erstellung bzw. die Erneuerung zu bezahlen. Machen wir das auch mit der Kundenkarte? Sicher nicht! D.h. dem Kunden können nur dann direkte Kosten auferlegt werden, wenn er diese von Gesetzes wegen übernehmen muss oder er einen sehr hohen Mehrwert/Nutzen sieht. Letzteres aufzuzeigen ist meines Wissens noch niemandem gelungen, also muss man davon ausgehen, dass die Kosten von Zertifikaten indirekt amortisiert werden müssen. Andererseits besteht die Problematik, dass hochwertige Zertifikate weniger verbreitet werden, weil die Gestehungskosten im Vergleich zu einfachen Zertifikaten um ein vielfaches höher sind.

Für eine unabhängige Zertifizierungsinstanz nach altem Muster, wie sie im Gesetz beschrieben wird, muss man mit Investitionen von mindestens 20-30 Mio. CHF rechnen. Diese Zahlen entsprechen Erfahrungswerten aus Deutschland. Der Hauptaufwand entsteht, weil die technisch-organisatorischen Anforderungen an eine öffentliche Zertifizierungsinstanz im Hinblick auf den Einsatz der Digitalen Signatur zu Recht sehr hoch geschraubt wurden[12].

4.5 NUTZEN

Der Nutzen ist für den klassischen Zertifizierungsdiensteanbieter immer über die Anzahl ausgestellter und verwalteter Zertifikate berechnet worden. Erfahrungen aus dem nahen Ausland zeigen, dass alle diese Anbieter um ihre Existenz zittern. Wie erwähnt sind die Anbieter von Zertifikaten in der Wertschöpfungskette sehr weit hinten zu finden. Den Nutzen muss man rollengerecht betrachten. Im Rollenmodell stellen Anwender völlig andere Gesichtspunkte in den Vordergrund als ein Zertifikatsproduzent. Zwischen den einzelnen Rollen bestehen zudem starke Spannungsverhältnisse. Was für den Anwender gut ist, kann für den Anwendungsanbieter überhaupt nicht attraktiv sein. Man kann sich mit Recht fragen, ob z.B. eine Bank tatsächlich Interesse hat mit Zertifikaten zu arbeiten, die es

[12] Zur Gesamtkostenbetrachtung bei PKIs vgl. http://www.itrust.ch/deutsch/articles/TCO_report10_D.pdf

ermöglichen, sowohl mit ihr direkt, aber unter Umständen auch mit der Konkurrenzbank in Verbindung zu treten. Zumal diejenige Bank, die die Initialinvestition macht (Ausbreitung von Smartcards und notwendigen Kartenlesern etc.) damit indirekt die Konkurrenz subventioniert. Dies führt zu einer zusätzlichen Marktsegementierung und einer unerwünschten Inkompatibilität der Systeme, wie wir aus z.B. aus dem E-Banking Umfeld kennen.

Hauptgrund für den fehlenden Business Case im Fall Swisskey war m.E. das fehlende Rollenverständnis bzw. das Verständnis für die Marktbedürfnisse. Swisskey hatte keine starken Anwendungen und keine genügende Kundennähe, die es erlaubt hätten, innerhalb nützlicher Frist genügend Anwender auf das System zu bringen. Die Mehrzahl der Zertifikatsanbieter kämpft mit dieser Problemstellung.

5. WIE GEHT ES WEITER?

5.1 GESCHÄFTSKUNDEN

Als Konsequenz aus den erwähnten Überlegungen haben sich in letzter Zeit international zwei Trends klar abgezeichnet, nämlich[13]:

a) der Einsatz einer eigenen bzw. internen PKI
b) die Nutzung von ASPs (Application Service Provider)
c) der Einsatz von modularen PKI Services

Es besteht nach wie vor die Möglichkeit, eine eigene PKI aufzubauen. Dies loht sich sicherlich dann, wenn man die Nutzung primär intern sieht (z.B. in internationalen Grosskonzernen). Diese Lösungen sind dann interessant, wenn konsequent auf die Standardisierung der Verfahren gesetzt wird, d.h. es handelt sich um eine Infrastrukturinvestition die ihre Kosten über mehrere Jahre, durch standardisierte und damit günstigere Prozesse einspielen muss.

Der ASP Markt ist für Europa erst im Aufbau begriffen. Hier geht es im wesentlichen um das vollständige Outsourcing von PKI Services. D.h. ein Unternehmen betreibt die PKI nicht selbst, sondern vergibt diese Aufgaben an einen ASP. Dieses Modell hat dann Vorteile, wenn man genau weiss, welche PKI Komponenten man outsourcen will und kann. Nachteile gibt es bei der Flexibilität der Services und der fehlenden Nähe zur Anwendung.

Als Variante zu b) empfiehlt sich der Anschluss an ein branchenorinetiertes PKI Modell. Das fortschrittlichste System im internationalen Bereich ist Identrus[14] der Banken. Zudem gibt es in den traditionellen B2B Vertikalmärkten entsprechende Bestrebungen zum Aufbau solcher Strukturen. Es wird davon ausgegangen, dass die PKI Services modular aufgebaut sein müssen und die Erzeugung der Zertifikate in einer teuren Infrastruktur erfolgt, welche zentral genutzt wird. Diese Infrastruktur wird in der Lage sein, verschiedene Zertifikate, basierend auf verschiedenen Certificate Policies, zu erzeugen. In einem aktuellen Identrus Projekt wird die gesamte Kundenseite als Dienstleistung der Bank aufgebaut, während die Zertifikats- und Kartenerzeugung einem Rechenzentrum übertragen wird. Gleichzeitig wird mit dem Zertifikatsangebot ein Portfolio von Identrus Anwendungen lanciert. Die zentrale Komponente, die Registrierungsinstanz, wird beim Anwender direkt betrieben. Damit hat er volle Kontrolle über die Anwendungsseite und die Abhängigkeiten zwischen Anwendung und Zertifikaten.

[13] Für einen aktuellen Marktbericht mit Fokus EU / Schweiz vgl. http://www.wildhaber.com/english/pages/ST_05_2.htm
[14] http://www.itrust.ch/deutsch/articles/Identrus_V1.1.pdf

5.2 BEHÖRDEN

Für den Einsatz von Zertifikaten im öffentlich-rechtlichen Umfeld (E-Government) ist der Aufbau einer eigenen Zertifizierungsinstanz wünschenswert. Geld verdienen kann man damit allerdings nach wie vor nicht, es handelt sich hier um einen service publique. Für den Einsatz von Digitalen Signaturen nach dem Modell des Signaturgesetzes sehen wir nur diese Möglichkeit. Dabei kann sich durchaus auch das ASP Modell aufdrängen. Dabei ist auch die gemeinsame Nutzung eines Rechenzentrums für private wie öffentliche Zwecke möglich, da die Registrierungsdienste so oder so abgekoppelt werden müssten.

Der Staat sollte Anschubhilfe leisten, wo dies aus strategischen Gründen sinnvoll erscheint. Er sollte dann sicherstellen, dass er die Registrierungsseite = Kundennähe dominiert und nicht von Dritten abhängig ist. Die gesetzlichen Grundlagen im Umfeld der Mehrwersteuer führen z.B. dazu, dass sich sehr schnell ein hohes Potential an Anwendern formiert.

5.3 PRIVATPERSONEN

Die Situation für die Privatanwender ist nach wie vor unbefriedigend. Es ist zwar damit zu rechnen, dass grössere Anbieter bestimmte Kundensegmente mit Signaturkomponenten ausrüsten werden. Für die anwendungsunabhängige Nutzung werden sich vor allem die Web basierten Single Sign On Systeme etablieren[15]. Diese könnten trotz der heute noch massiv vorhandenen Schwächen eine ernsthafte Herausforderung für die Signatursysteme darstellen, da die Vorteile für den Privatanwender offensichtlich sind. Sollten die Anbieter in absehbarer Zeit in der Lage sein, diese Systeme sicherer zu machen, sind sie als Signaturalternative durchaus ernst zu nehmen.

[15] Vgl. FN 2