Die Digitale Signatur

Wann kommt sie endlich?

Ein Aus- und Überblick

Autor: Moritz G. Haag

Ausbildungsstandort: Göttingen

Erstellungsdatum: 26.09.2003

Deutsches Zentrum
für Luft- und Raumfahrt e.V.
in der Helmholtz-Gemeinschaft

1. Inhaltsverzeichnis

2. Abkürzungen

BGB	Bürgerliches Gesetzbuch
CA	Certification Authority
CRL	Certificate Revocation List
DAU	Dümmster Anzunehmender User
DES	Data Encryption Standard
DL	Problem diskreter Logarithmen
EC–Karten	Electronic Cash– Karten
IT	Informationstechnologie
IuKDG	Informations- und Kommunikationsdienstegesetzes
PAA	Policy Approving Authority
PIN	Persönliche Identifikationsnummer
PKI	Public Key Infrastructure
PKS	Public Key Struktur
RA	Registration Authority
RSA	Das von Ron Rivest, Adi Shamir, and Leonard Adleman entwickelte Signatursystem
SC	SmartCard
SC API	SmartCard Standard Programmierer Schnittstelle
SigG	Signaturgesetz
SSO	Single–Sign–On
SV- Träger	Sozialversicherungs- Träger
TAN	Transaktionsnummern
TTP	Trusted Third Party
ZDA	Zertifizierungs–Dienste- Anbieter
ZPO	Zivilprozessordnung

3. Einleitung

Dieser Bericht beschäftigt sich mit der Frage, wann die elektronische Signatur kommt. Dazu werden zuerst die Vorraussetzungen und Techniken erläutert. Anschließend werden die Risiken und Hemmnisse, die einer Einführung der aktuellen Technik der digitalen Signatur, den öffentlichen Schlüsseln entgegenstehen, aufgedeckt und die damit verbunden kulturellen und rechtlichen Veränderungen zusammengetragen. Für eine umfassende Betrachtung empfiehlt es sich jedoch Q1, Q4 und W1 hinzuzuziehen. Am Ende werden mögliche Alternativen und der Rechtsrahmen elektronischer Signaturen in Deutschland und im internationalen Vergleich aufgeführt. Da abschließend von einem gemeinsamen Fundament ausgegangen werden kann, beurteile ich die aktuelle Sachlage aus meiner Sicht und fasse den Bericht ohne weitere Erläuterungen zusammen.
Eingangs beschäftige ich mich auch mit dem traditionellen Schriftverkehr, damit ich später besser auf die Vor- und Nachteile des elektronischen Schriftverkehrs eingehen kann und eine gemeinsame Basis vorhanden ist.

3.1 Sicherheitsanforderungen

Viele Dokumente erfordern gewisse Sicherheiten um Rechtssicherheit und Vertrauen der beteiligten Parteien zu gewährleisten. In der folgenden Tabelle sind diese Anforderungen aufgeführt.

Anforderung	Herkömmlich	In einer PKI
Identifikation	Ausweis	Zertifikat zur digitalen Signatur
Authentizität	Wasserzeichen	digitale Signatur
Vertraulichkeit	Versiegelter Umschlag	Verschlüsselung
Verbindlichkeit	Unterschrift	Haftungsbereich d. dig. Signatur
Integrität	Tinte + Papier ohne Ergänzungen	dig. Signatur
Zeitpunkt	Zeit + Unterschrift	Zeitstempeldienst + dig. Signatur

Tabelle 1: Sicherheitsanforderungen

3.2 manuelle Signaturen

Die Quelle dieses Abschnitts ist soweit nicht anders angegeben Q2.
Im traditionellen Schriftverkehr ist die Unterschrift ein Willensakt. Mann kann nicht aus versehen etwas unterschreiben, daher herrscht weitestgehend Signaturklarheit. Das heißt, dem Unterschreibenden ist klar, was er Unterschreibt und welche rechtlichen Folgen sich daraus ergeben.
Es gibt auch im traditionellen Schriftverkehr folgende verschiedene Unterschriften oder Signaturen.

3.2.1 rechtlich anerkannte

Sie muss für öffentliche Dokumente, Einverständniserklärungen, usw. eingesetzt werden. Sie beinhaltet den Namen des Unterzeichners und erlaubt eine eindeutige Identifikation. Pseudonyme können hier nicht verwendet werden.

3.2.2 Gesellschaftlicher Status

Diese Signatur bezeugt eine Klassenzugehörigkeit bzw. den Status in der Gesellschaft. Sie kann auch durch ein Siegel oder einen Stempel ausgedrückt werden. Meist wird nur im Namen der Gruppe signiert, und nur der Eingeweihte kann das einzelne Siegel einer bestimmten Person zuordnen

3.2.3 Kirchlicher Würdenträger

Hier werden mit einer bestimmten Signatur oder wieder einem Siegel der Rang und die Macht des Unterzeichners und damit auch die Kraft so unterzeichneter Dokumente ausgedrückt.

3.2.4 vereinfacht

Die vereinfachte Unterschrift wird von Leuten, die viel unterschreiben und Zeit sparen wollen, verwendet. Sie hilft auch die dienstliche und private Unterschrift zu trennen.

3.2.5 Kreuz

Diese Unterschrift wird verwendet, wenn von Analphabeten Unterschriften gefordert werden. Sie kennzeichnet den Unterschreibenden nicht deutlich und hat daher keine Rechtskraft. Suggeriert dem Unterschreibenden aber keinen Widerspruch erheben zu können. Auf Grund der einfachen Symbole sind auch keine graphologischen Gutachten möglich.

3.2.6 Logo, Label

Als Logo wird ein Symbol bezeichnet, das Auskunft über Herkunft und Authentizität einer bestimmten Ware gibt. Bei Logos ist der „Unterzeichner" nicht mehr zu identifizieren. Es kann nur die Gruppe ermittelt werden.

3.3 digitale Signaturen

Die digitale Signatur ist ein krypto-technischer Sicherheitsmechanismus. Sie sichert die Authentizität und Integrität elektronischer Daten. Diese Technik ist wichtig bei der Kommunikation zwischen Maschinen. (z.B. SSL u. Updates). Es gibt unterschiedliche Techniken digitaler Signaturen. Eine sind die bei den öffentlichen Schlüsseln verwendeten asymmetrischen Schlüssel. Des Weiteren gibt es z.B. noch symmetrische Schlüssel siehe dazu unter 4.10.1.. Innerhalb einer Technik gibt es unterschiedliche Signatursysteme. Siehe dazu unter 4.3. Q4

3.4 elektronische Signaturen

Die elektronische Signatur ist das elektronische Pendant zur Unterschrift auf dem Papier. Eine fortgeschrittene elektronische Signaturen erweitert den Begriff und erfüllt folgende Kriterien:
Sie ist eindeutig einem Unterzeichner zuzuordnen und wird unter dessen alleiniger Kontrolle gehalten. Sie ist logisch mit anderen Daten verknüpft. So können nachträgliche Änderungen dieser Daten erkannt werden. Qualifizierte elektronische Signaturen sind zusätzlich mit einem qualifizierten Zertifikat verknüpft, das die Identifizierung des Unterzeichners erlaubt. Q4
Im verbreiteten Sprachgebrauch und auch im weiteren Text ist als Unterschrift soweit nicht anders angegeben die eigenhändige Unterschrift gemeint, und als digitale oder auch elektronische Signaturen ist soweit nicht anderes angegeben die qualifizierte elektronische Signaturen erstellt mit der Technik der digitalen Signatur gemeint.

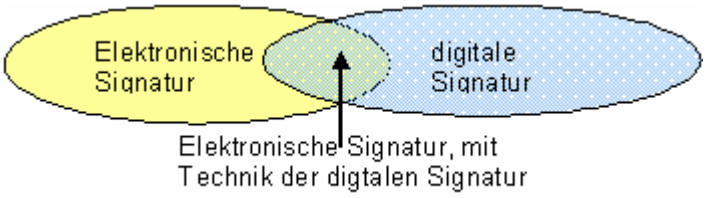

Abbildung 1: elektronische Signatur

4. Öffentliche Schlüssel

Die zurzeit am weitesten verbreitete Technik elektronischer Signaturen ist die der öffentlichen Schlüssel. Auf dieses Verfahren werde ich im folgenden Abschnitt genauer eingehen. Die Verwendung der öffentlichen Schlüssel ist an bestimmte Vorraussetzungen geknüpft. Wenn diese gegeben sind, spricht man von einer öffentlichen Schlüssel Infrastruktur(Public Key Infrastructure -PKI). Diese besteht mindestens aus der Software zum Anwenden der Schlüssel, einem sicheren Speicher zum Verwahren der Schlüssel, und einer unabhängigen Stelle, die die Identität der Schlüsselinhaber zertifiziert.

4.1 Technik

Der Anwender hat ein Schlüsselpaar, das aus einem öffentlichen und einem privaten Schlüssel besteht. Zu dem Schlüsselpaar existiert ein Zertifikat, das von einer autorisierten Stelle verwaltet wird und die Authentizität des Anwenders prüft und bestätigt. Der Sender und der Empfänger müssen über eine Software verfügen, die das Ver- und Entschlüsseln, sowie das Überprüfen des Zertifikats abwickelt. Der Sender hat seinen Schlüssel auf einem sicheren Speichermedium verwahrt ausgestattet.
Beim Unterschreiben der Nachricht wird der private Schlüssel verwendet.

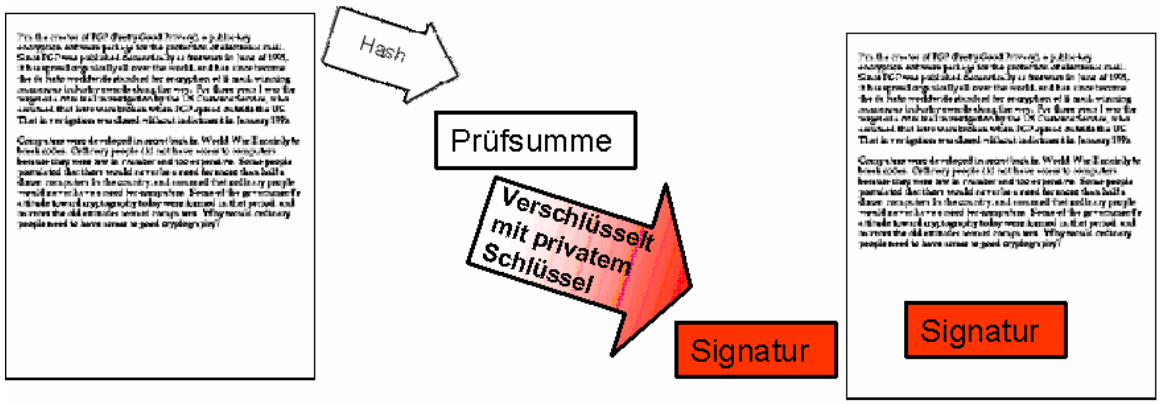

Abbildung 2: Elektronisch unterschreiben

Zum Überprüfen der Nachricht wird der öffentliche Schlüssel an die signierte Nachricht angehängt oder kann beim ZDA abgerufen werden.

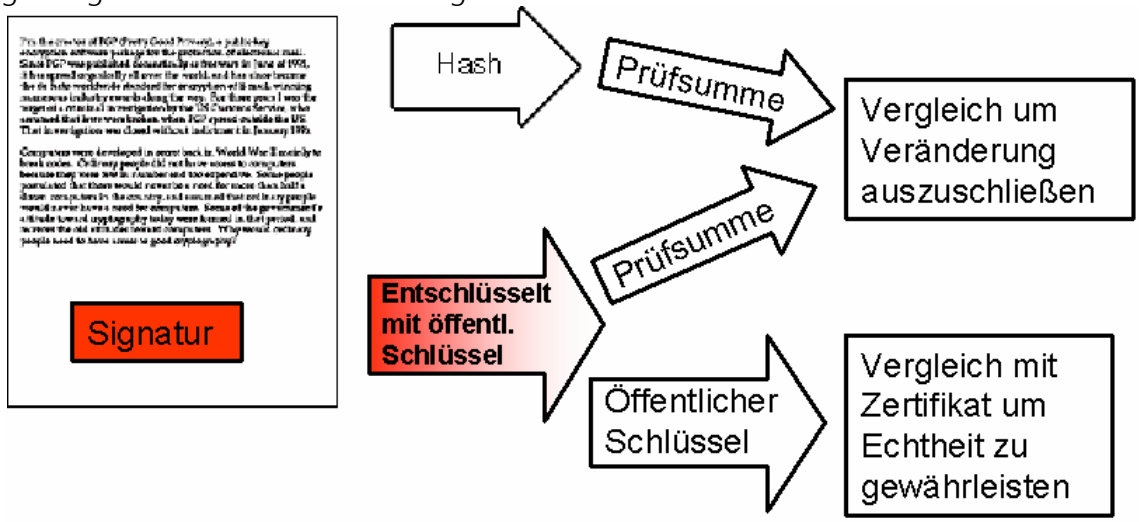

Abbildung 3: Elektronische Signatur prüfen

4.1.1 Mathematische Grundlagen

Die meisten kryptographischen Algorithmen basieren auf dem Problem diskreter Logarithmen. Zur Lösung des DL-Problems stellt sich die Frage, ob es überhaupt ein x für $x \equiv \log_y \alpha$ gibt. In der kryptographischen Anwendung kann jedoch von der Existenz dieses x ausgegangen werden. Zum anderen muss die Frage zur eigentlichen Lösung des Algorithmus beantwortet werden, also welches x die Formel $\alpha = y^x$ löst.

Zur Veranschaulichung folgt ein Beispiel von diskreten Logarithmen von a aus der Menge {1,2,…,12} zur Basis y= 2 in der Gruppe mod 13.

a	1	2	3	4	5	6	7	8	9	10	11	12
$\log_2 a$	0	1	4	2	9	5	11	3	8	10	7	6

Tabelle 2: Diskrete Logarithmen

Für kryptographische Anwendungen ist es besonders wichtig, dass der diskrete Logarithmus nicht effizient zu berechnen ist. Diese Forderung wird jedoch hauptsächlich in Gruppen modulo einer Primzahl erfüllt. Q7 Detailliertere Informationen sind in Q3 und Q7 zu finden.

4.1.2 Zeitstempel

Der Zeitstempeldienst wird zweimal aktiv. Vor und nach dem Signieren. Ein verlässlicher Zeitstempel ist wichtig, um sicher zustellen, dass das Dokument erstellt und signiert wurde als das Zertifikat gültig und sicher war. Auch beim Verifizieren wird der Zeitstempeldienst noch mal aktiv, damit bekannt ist, wann der Empfänger erstmals Kenntnis vom Inhalt der Nachricht erlangte.

4.1.3 Single-Sign-On

Single-Sign-On, kurz SSO bezeichnet eine neue Technik im Bereich der Netzwerksicherheit. Da sich viele Anwender ihre vielen Passworte notieren sind diese kontraproduktiv. Beim Single-Sign-On wird der Zugang über ein sehr sicheres Passwort oder eine SmartCard erteilt, und anschließend übernimmt der Rechner alle anfallenden Authentifizierungsanforderungen. Dadurch muss sich nur noch die SmartCard Pin gemerkt oder der Fingerabdruck eingesetzt werden.

4.1.4 SmartCard

Die SmartCard, kurz SC ist das zurzeit gebräuchlichste Speichermedium für Sicherheitslösungen. Sie hat die Größe einer Kreditkarte. Auf der Karte ist ein integrierter Mikroprozessor, der den Zugriff auf die gespeicherten Daten über PIN oder Fingerabdruck kontrolliert. Der Zugriff auf die SmartCard erfolgt über ein spezielles Lesegerät, das über eine eigene Software oder z.B. die SmartCard Standard Schnittstelle(SC API) angesteuert wird. Auf der SmartCard können Schlüssel, Zertifikate, Netzwerkprofile und Zugriffsinformationen gespeichert werden.

4.2 Zertifikate

Zertifikate ordnen einem Schlüssel verifizierte Informationen zu, um so sicherzustellen, dass der Schlüssel, der zu diesem Zertifikat gehört auch zur richtigen Person gehört. Zertifikate können entweder mit dem öffentlichen Schlüssel verschickt werden, von einer Gruppe (z.B. einer Firma für ihre Arbeitnehmer) herausgegeben werden, oder bei einem Zertifizierungs-Dienst-Anbieter hinterlegt werden.

„Folgende Daten sind in einem Zertifikat enthalten

Inhaber: *Hier stehen der Vor- und Zunamen, die Mail-Adresse, die Postleitzahl der Stadt, sowie das Land, in dem der Inhaber lebt.*

Aussteller: *Weist den Aussteller des Zertifikates aus, zeigt dessen Internet-Adresse, den Sitz des Ausstellers und die Seriennummer des Zertifikates an.*

Gültig von: *Zeigt Ihnen genau die Gültigkeitsdauer Ihres Zertifikates an.*

Fingerprint: *Ein Fingerprint ist - wie der Fingerabdruck Ihres Daumens - ein weltweit einmaliges, zur eindeutigen Identifikation dienendes Kennzeichen. Technisch gesehen ist der elektronische Fingerprint eine Art Auszug des Zertifikates. Im Online-Check des WEB.DE TrustCenters können Sie den Fingerprint und die Seriennummer überprüfen." Q6*

4.2.1 Zertifizierungs-Dienst-Anbieter

Der ZDA - auch TrustCenter oder CA (Certification Authority) genannt, prüft die Angaben und stellt das zuvor personalisierte und damit qualifizierte Zertifikat in einer öffentliche Datenbank aus der die Zertifikatsinformationen abgerufen werden können.
Das Modell sieht es auch vor, dass der Schlüssel und das Zertifikat zwar von einem ZDA ausgestellt werden (z.B. einer Bank) und die Identität des Inhabers aber in deren lokalen Stelle RA (Registration Authority) gesichert wird. Dies ist eine mögliche Sicherheitslücke, da so der ZDA als Gesamtheit leichter kompromittiert werden kann, oder sogar der Schlüssel falls er beim ZDA erzeugt wurde, ausspioniert werden kann. Der ZDA sollte nur die öffentlichen Schlüssel kennen, um den Missbrauch zu verhindern. Dann muss der private Schlüssel vom Anwender erzeugt werden. Näheres dazu beim internationalen Vergleich(5.3) und den Risiken(4.9).
Die Kommunikation zwischen den ZDA kann auf verschiedene Arten erfolgen.
Im Bridge-Modell kommunizieren alle ZDA untereinander über eine Bridge. Jedoch stellt sich hier schnell die Frage, wer diese Bridge kontrolliert und was passiert wenn diese ausfällt.
Beim Cross-Certified-Model vertrauen sich je zwei ZDA gegenseitig. Das gibt den ZDA zwar sehr viel Autonomie, dafür werden es aber auch sehr viele Verbindungen. Bei 4 ZDA sind es 14 Verbindungen und bei 8 ZDA sind es schon 56, da die Anzahl der maximalmöglichen Verbindungen sich für n ZDA gemäß n*(n-1) bestimmen lässt. Beim Vertrauensmodell gilt das Vertrauen eines ZDA gegenüber auch für alle diesem ZDA vertrauten ZDA.
Beim hierarchischen Modell werden die ZDA zu so genannten PCAs zusammengefasst. Eine PCA ist eine Policy CA. Diese legt die Richtlinien für alle angeschlossenen ZDA fest und es muss nur noch der PCA vertraut werden. Jedes Land hat dann eine PAA(Policy Approving Authority) und es existiert ein globaler ZDA in der alle ZDA letztendlich zusammen gefasst sind. Über den Zertifikatspfad lassen sich die zuständigen Organisationen jederzeit ausfindig machen.
Letztendlich wird es wohl auf eine Mischform hinauslaufen. Dass einige PCAs anderen PCAs vertrauen aber jedes Zertifikat über den Globalen ZDA erfragt werden kann.
Zum Beispiel hätte die DLR ihren eigenen Zertifikatsserver. Dieser wäre z.B. unter telesec organisiert. Deren Sicherheitsrichtlinien werden von der Regulierungsbehörde (in dem Fall der .DE-PAA) kontrolliert. Diese wäre beim globalen ZDA registriert, ähnlich wie im Domain Name Space. Ein Problem ist allerdings, wer diesen globalen ZDA leitet oder kontrolliert. Q17
Ein wichtiger Faktor sind auch die Kommunikationskosten (siehe 4.8), die in der Baumstruktur am geringsten wären.

4.2.2 Sicherheit

Sicher sind Zertifikate bis der zugehörige Algorithmus gehackt wurde bzw. die zuständige Zertifikatsstelle kompromittiert wurde bzw. nicht ausgeschlossen werden kann, dass eine der beiden Bedingungen zutrifft.

4.2.3 Gültigkeit

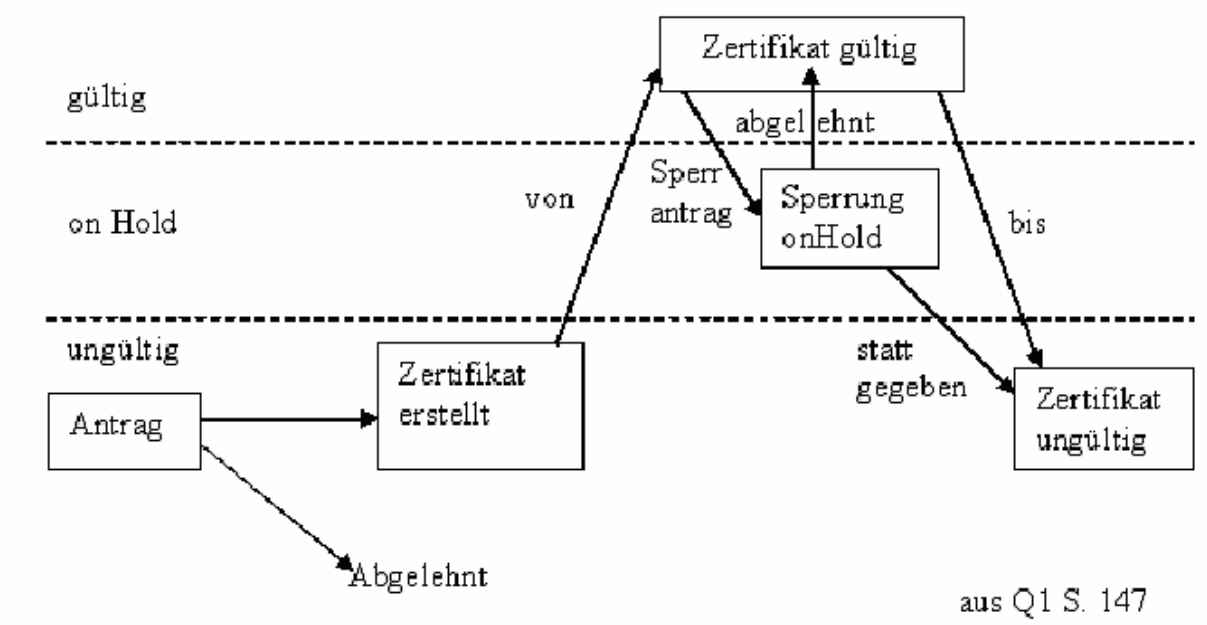

Abbildung 4: Gültigkeitszyklus qualifizierter Zertifikate

Um den Ablauf der Gültigkeit eines Zertifikats festzustellen, kann nicht immer das komplette Zertifikat beim ZDA angefragt werden, da dadurch das Datenaufkommen zu hoch wäre. Zudem werden einmal als vertrauenswürdig gekennzeichnete Zertifikate bis zum voraussichtlichen Gültigkeitsende nicht mehr neu überprüft.
Um dennoch sicherzustellen, dass gesperrte Zertifikate aus dem Verkehr gezogen werden, gibt es verschiedene Modelle. Das am weitesten ausgearbeitete ist das CRL Modell. CRL steht für Certificate Revocation List. Auf diesen Listen wird die Seriennummer aller Zertifikate veröffentlicht die ungültig sind. Wie unschwer zu erkennen ist, wird das eine sehr umfangreiche Liste. Diese Liste muss regelmäßig von allen ZDA und allen Programmen eingelesen werden.

4.3 Signatursysteme

Ein Signatursystem oder auch Schema genannt ist ein Algorithmen-Triple, bei denen einer ein Schlüsselpaar aus öffentlichem(y) und privatem(x) Schlüssel erstellt, einer erstellt aus einer Nachricht m und dem privatem Schlüssel x die Signatur p und der dritte überprüft ob die Nachricht m, der Öffentliche Schlüssel y und die Signatur p zusammen passen. Signatursysteme müssen unverfälschlich sein, dass heißt ohne den privaten Schlüssel x darf keine passende Signatur zum öffentlichen Schlüssel y erstellt werden können.Q1
RSA ist ein solches System. Es wurde 1977 von Ron Rivest, Adi Shamir, and Leonard Adleman entwickelt. Es funktioniert mit zwei großen Primzahlen p und q. Deren Produkt n wird modulus genannt. Und eine weitere Zahl y die kleiner n sein muss und keinen gemeinsamen Teiler mit (p-1)(q-1) hat. Eine 4. Zahl x muss so bestimmt sein, dass (p-1)(q-1) Teiler von (ex - 1) ist. Die Faktoren p und q können mit x abgelegt werden oder vernichtet werden.
Beim aktuellen Kenntnisstand ist es schwer den privaten Schlüssel x aus dem öffentlichen Schlüssel (n,y) zu ermitteln. Sollte jedoch p und q schnell aus n ermittelt werden können ist RSA unsicher.

4.4 Datenschutz

Die öffentlichen Schlüssel bieten durch Verschlüsselung z.B. neue Möglichkeiten des Datenschutzes. Doch es gibt auch fragliche Aspekte hinsichtlich des Datenschutzes.
Die Datenbanken der ZDA entsprechen bei flächendeckender Nutzung der elektronischen Signatur einem zentralen Melderegister. Dieses wurde bisher jedoch nicht eingerichtet um das Recht auf informelle Selbstbestimmung zu wahren. Auch kann anhand einer Nachricht die lediglich zur Wahrung der Integrität elektronisch signiert wurde, die Adresse und Identität des Absenders festgestellt werden. Es gibt im SigG §5(6) zwar die Möglichkeit Zertifikate mit Pseudonymen zu versehen, doch kann der Anbieter das Pseudonym jederzeit auflösen und es werden zusätzliche Kosten für ein weiteres Zertifikat fällig. Doch dem Anwendet bleibt auch noch die Möglichkeit eines unqualifizierten Zertifikats.
Der einzige datenschutzrechtliche Knackpunkt ist somit der ZDA, der seine Datenbank vor bösartigen, staatlichen und kommerziellen Zugriffen schützen muss. Auch wer das Zertifikat abgefragt hat, könnte gespeichert werden und somit ein Kommunikations-profil des Benutzers erstellt werden. Es hängt also alles vom ZDA und den rechtlichen Regelungen ab.

4.5 Gruppensignaturen

Gruppensignaturen erlauben Mitgliedern einer Gruppe Nachrichten im Namen der Gruppe zu signieren. Die Identität des einzelnen bleibt dabei verborgen. Sollte die Signatur missbraucht werden, kann eine autorisierte Person ermitteln welches Mitglied der Gruppe den Gruppenschlüssel eingesetzt hat. Bei den meisten Gruppensignaturen ist die Schlüsselgröße linear zur Anzahl der Gruppenmitglieder.
Spezielle Gruppensignaturen sind Multi-Signaturen bei denen der Unterzeichner nicht zurückverfolgt werden kann und Proxy-Signaturen bei denen die Identität des Unterzeichners nicht verborgen wird. Der Vorteil von Gruppensignaturen ist, dass Dokumente im Namen der Firma von verschiedenen Mitarbeitern herausgegeben werden können, aber nur ein öffentlicher Schlüssel (der öffentliche Gruppenschlüssel) benötigt wird, um das Dokument zu entschlüsseln und die Strukturen der Firma verborgen bleiben.
Der Nachteil dieser Schlüssel ist, dass für jedes neue Mitglied der Gruppenschlüssel neu erstellt werden muss. Dafür können aber jederzeit Mitglieder aus dem Schlüssel entfernt und hinzugefügt werden. Jedoch brauchen die Kommunikationspartner jedes Mal einen neuen öffentlichen Schlüssel und es dürfte leichter sein, Vertrauen aufzubauen, wenn intern die Mitglieder-Schlüssel getauscht werden, als wenn der öffentliche Schlüssel nur kurze Gültigkeitszyklen hat.
Der Autor von Q3 zeigt ab S. 88 ein neues Gruppensignaturenmodell auf.
y und x seien ein Schlüsselpaar aus öffentlichem und privatem Schlüssel. r sei eine Zufallszahl.

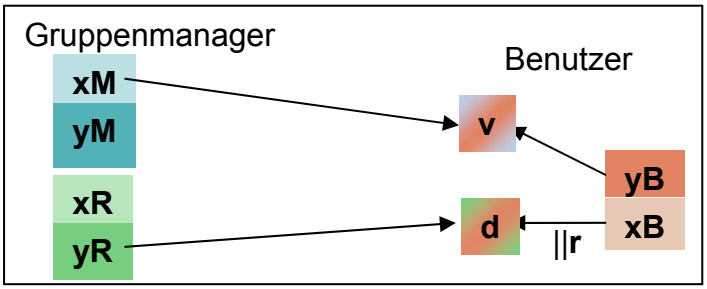

Abbildung 5: Gruppensignaturen 1

Das Zertifikat v bestätigt die Gruppenmitgliedschaft von B. Der Einmalschlüssel d wird vor jedem Signieren erzeugt. Er verhindert durch die Zufallszahl r, dass der Schlüssel xB einem Benutzer eindeutig zugeordnet werden kann.

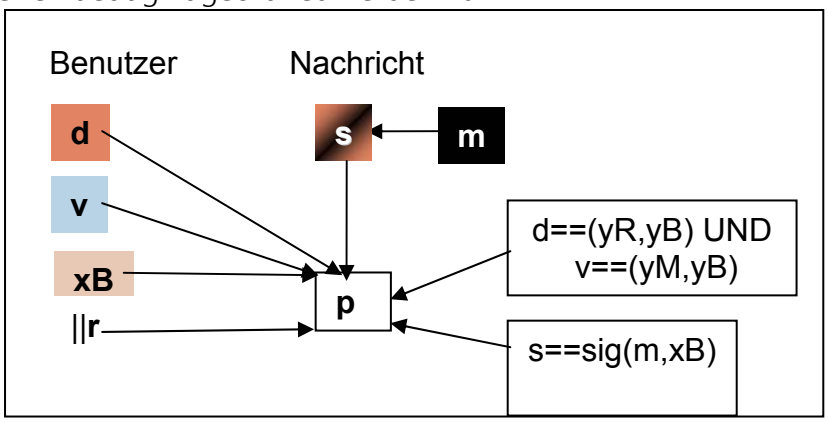

Abbildung 6: Gruppensignatur 2

Die Signatur für die Nachricht m wird nun aus d und p erstellt. Mit Hilfe von p kann die Signatur jederzeit auf yR und die Authentizität der Nachricht überprüft werden.
Der Gruppenmanager kann mit seinem Schlüssel den Einmalschlüssel d auflösen und so feststellen, welcher Benutzer den Gruppenschlüssel angewandt hat.
Ein weiterer Vorteil ist, dass der Gruppenschlüssel und der Managerschlüssel von verschiedenen Personen verwaltet werden können. Was die Missbrauchsgefahr einschränkt.
Das Problem ist allerdings, dass nur der Gruppenmanager neue Schlüssel autorisieren kann, und dass keine einzelnen Mitglieds-Schlüssel gesperrt werden können ohne den Hauptschlüssel zu ändern. Ähnlich einer Schließanlage, bei der, bei Verlust eines Schlüssels, alle Schlösser geändert werden müssen.
Derzeit ist die Technik der Gruppensignaturen aber noch nicht verbreitet und ausgereift.
Weitere Einzelheiten des Verfahrens und andere Informationen zu Gruppensignaturen sind in Q3 zu finden.

4.6 Verschlüsselung

Mit öffentlichen Schlüsseln ist auch eine Verschlüsselung der Daten möglich. Dabei werden die Daten mit dem öffentlichen Schlüssel verschlüsselt und können nur mit dem privaten Schlüssel entschlüsselt werden. Wie jedoch unter 4.10.1 erwähnt wird, sind für Verschlüsselungen größerer Datenmengen symmetrische Schlüssel geeigneter.

4.7 Anwendungen

„- Eine Killerapplikation hatte zwar niemand in petto, doch chancenreich erschien allen eine EC-Karte mit qualifizierter Signatur. So wird etwa die Deutsche Bank noch in diesem Jahr 10.000 Karten für das Online-Banking mit digitaler Signatur ausgeben. Bei der nächsten Umstellung der EC-Karten Ende 2004 sollen alle Karten mit einem signaturfähigen Chip versehen werden. Etwa zehn Prozent von sechs Millionen Kunden werden sich gegen einen kleinen Aufpreis für diese Karte entscheiden, schätzt Bernhard Esslinger von der Deutschen Bank. Bedarf erkennt Esslinger vor allem bei sicheren E-Mails. Ähnliche Überlegungen gebe es auch bereits bei den Sparkassen.

- *In Österreich sollen alle EC-Karten bis Ende 2004 signaturfähig sein, kündigte Reinhard Posch von der österreischischen IT-Sicherheitsbehörde A-SIT an. Ein Geschäftsmodell schwebt Posch bereits vor: So soll jeder Signatur- und Verschlüsselungsvorgang einen Mikrobetrag von etwa zehn Cent kosten: "Das ist immer noch viel preiswerter als 55 Cent für eine Briefmarke", sagte Posch. Bis 2010 erwartet er, dass sich etwa die Hälfte der österreichischen Bevölkerung mit der elektronischen Signatur angefreundet hat." Q7*

- *Auch Bei Web.de ist die digitale Signatur bereits verwirklicht. Da Web.de Benutzer einen Brief erhalten, ist die Postadresse des Zertifikats verifiziert, aber nicht nach dem SigG anerkannt. Mit dieser digitalen ID können die Benutzer Ihre E-Mails signieren. So können die Empfänger sicher sein, dass die digital signierte Nachricht tatsächlich vom angegebenen Benutzer stammt und nicht manipuliert wurde. Die digitale ID wird automatisch bei der Registrierung zugeteilt.*
  Nach dem das E-Mail wie gewohnt geschrieben wurde, aktiviert das Auswahlfeld "Digitale Unterschrift" im Unterpunkt "Sicherheit" den Signaturmechanismus.Q6
- *„(Wien) Der neue Service der österreichischen Sozialversicherung soll Abrechnungen von Leistungen der Vertragsärzte vereinfachen und beschleunigen. Über ein Portal senden die Ärzte ihre Verrechnungsdaten online an die Datendrehscheibe im Hauptverband. Die Abrechnungsdaten werden mit einer digitalen Signatur versehen, um die Echtheit der Daten zu bestätigen. Der Hauptverband leitet dann die eingelangten Formulare automatisch an den jeweiligen SV-Träger weiter." Q10*
- *„Beispiel Bremen: Hier werden im Rahmen des Bremer Media@Komm-Projektes „bremer-online-service" die Signaturkarten stark vergünstigt herausgegeben. Statt der 40 bis 50 EUR, die eine Signaturkarte bei TeleSec pro Jahr kostet, zahlen Bremerinnen und Bremer bis Oktober 2003 nur eine einmalige Schutzgebühr von 5 EUR." Q11*

4.8 Kosten

Für einen Firmenarbeitsplatz im ersten Jahr mit SSO, SC und Zertifikat werden etwa 100-200€ fällig. Q5
Für private Anwender entstehen etwa die gleichen Kosten. Der Anteil für das Zertifikat mit begrenzter Haftung bei Kaufverträgen www.globalsign.net bis 2500€ je Geschäft inkl. Dokumenten-Signatur und digitalem Ausweis beläuft sich auf etwa 20€ pro Jahr. www.globalsign.net
Die meisten dieser Kosten fallen für den Speicherplatz und die Kommunikation an.
Ein Zertifikat benötigt 500bytes. Die CRL benötigt 51Byte + 6Byte*Anzahl der gesperrten Zertifikate. Man geht davon aus, dass etwa 10% aller Zertifikate gesperrt werden. Da diese Daten auch versendet werden, entspricht der Speicherbedarf dem Kommunikationsbedarf je Vorgang. Wenn das System intensiv genutzt wird, sinken die Kommunikationskosten, da die Infrastruktur besser ausgelastet wird. Die Kosten je Nachricht schätzt man auf etwa 0,12$. Q17

4.9 Risiken

Trotz der ausgereiften Technik, zahlreichen gesetzlichen Regelungen und festgeschriebenen Verfahren gibt es noch zahlreiche Risiken im Umgang mit den elektronischen Signaturen. Einige Risiken beruhen auf der Umsetzung der Richtlinien.
Im deutschen Recht ist die Festlegung auf die RSA-Technik gefährlich, da eine Gesetzesänderung notwendig ist, sollte diese nicht mehr sicher sein. Innovationen werden so gebremst. Weitere, eher rechtliche als technische Risiken, sind die Fragen, wie weit die Gültigkeit zurückgezogener Signaturen reicht und wie die private Adresse geschützt wird, um das recht auf informelle Selbstbestimmung zu wahren (siehe 4.4).
Doch es existieren auch zahlreiche technische Risiken.
So ist die Unterschrift zwar schwer zu fälschen, dafür ist aber die Integrität von Papierdokumenten relativ leicht zu verletzen. Bei der digitalen Signatur ist es bis heute unmöglich die Integrität zu verletzen, dafür kann aber der Schlüssel z.B. über Trojaner relativ leicht gefälscht werden und die Fälschung kann nicht nachgewiesen werden. Q4
Auch das Eingangs erwähnte Kriterium der Signaturklarheit ist nicht erfüllt und hier liegt meiner Meinung nach das größte Risiko. Denn es ist unbekannt was der Computer alles mit meinem Schlüssel unterschreibt. Auch während ein bestimmtes Dokument signiert wird, können viele andere im Hintergrund signiert werden, oder das angezeigte Dokument wird nicht signiert.

Wenn wie im deutschen Recht vorgesehen, die privaten Schlüssel beim ZDA erzeugt werden und per SC übermittelt werden, hat auch der ZDA Zugang zum privaten Schlüssel.
Zudem müssen entsprechende Vorkehrungen zum Schutz vor Veränderungen am Verzeichnis getroffen werden. Denn damit steht und fällt PKI.
Falls falsche Zertifikate übermittelt werden, muss auch ein DAU dies erkennen können. Da nur über die Zertifikate die Authentizität geprüft werden kann.
Beim SSO werden die Authentifizierungsinformationen zwischengespeichert und ohne erneute Aufforderung oder Überprüfung vom System verwendet. Dadurch werden die Signaturklarheit und der Schutz des Schlüssels ad absurdum geführt.
Gerade im internationalen Verkehr ist das Vertrauen in die Zertifikatsstellen wichtig und hier sind Gesetze notwendig, die die Akkreditierung internationaler Zertifikatsstellen regeln. Und die Software des Anwenders muss erkennen ob es sich um eine akkreditierte Zertifikatsstelle handelt.
Das schon mehrfach angesprochene Problem, des Auslesens des privaten Schlüssels vom Rechner durch Trojaner, lässt sich durch Firewalls und Virenscanner eindämmen.
Ebenso wichtig ist es aber, die lokale Liste vertrauenswürdiger Signaturen zu sichern, da sonst jedes Zertifikat vorher durch einen Virus als vertraut registriert werden könnte.
Ein Problem, das sowohl technisch als auch datenschutzrechtlich gelöst werden muss, ist, wie das Zertifikat einer Person zugeordnet werden kann, ohne deren komplette Adresse zu veröffentlichen. Denn sonst besteht das Risiko, dass dem falschen Hans Müller vertraut wird.
Ein weiteres Risiko zeichnet sich bei der Archivierung ab. Oft müssen Daten für mindestens 30 Jahre gespeichert werden. Optische Medien weisen heute eine Höchstlebensdauer von 30 Jahren auf. Historiker wünschen sich natürlich noch längere Speicherzeiten. Zudem müsste die notwendige Software zum Lesen der Daten, die verwendeten Schlüssel, Zertifikate und Zertifikatssoftware, CRLs mitgespeichert werden.
Neben diesen organisatorischen Problemen, besteht auch noch das des Datenverlusts. Hier können durch Materialalterung oder durch das Einlesen mit veränderter Technik einzelne Bits zerstört werden. Dann kann die Integrität des Dokuments nicht mehr sichergestellt werden. Bei Papierdokumenten hingegen ist es nicht so gravierend, wenn ein Farbpigment verblasst. Auch die Signatur würde dann nicht mehr als authentisch gelten. Eine eigenhändige Unterschrift kann zwar möglicherweise verblassen, ihre biometrischen Merkmale verändern sich jedoch auch im Laufe des Jahrhunderts nicht. Wann immer die gespeicherten Daten einer Auffrischung bedürfen, stellt dieser Aktualisierungsvorgang immer eine Möglichkeit zur zufälligen und beabsichtigen Datenkorruption dar. Q4
Im Unterschied zur eigenhändigen Unterschrift sind elektronische Signaturen stärker technikbasiert. Der Unterschreibende ist nicht nur wie bei der eigenhändigen Unterschrift auf einfache Mittel angewiesen, sondern auf die Verfügbarkeit einer funktionierenden technischen Infrastruktur. Er benötigt u.a. einen Rechner mit Bildschirm und Stromquelle, einen Chipkartenleser und vielfältige Software.
Störungen beim Unterschreiben wie z.B. nicht funktionierende Kugelschreiber sind in der Papierwelt leicht erkennbar und ein Ersatz ist leicht zu beschaffen. Die Nutzer verfügen dabei über stabile Kriterien für geeignete und nicht geeignete, gute und weniger gute Signierwerkzeuge. Demgegenüber ist es einstweilen alles andere als klar, wie im Falle einer nicht-funktionstüchtigen Software zu verfahren ist. Er wird ebenso wenig wissen, in welche Abhängigkeiten er sich begibt. Q4

4.10 Alternativen

Es gibt zahlreiche Alternativen zur elektronischen Signatur oder auch nur zur Technik der digitalen Signatur. Die gebräuchlichsten habe ich hier aufgeführt und erläutert.

4.10.1 Symmetrische Schlüssel

Es gibt Algorithmen wie z.B. DES, die mit einem Schlüssel arbeiten. Dieser kann die Daten ver- und entschlüsseln. Sie arbeiten deutlich schneller als asymmetrische Schlüssel erfüllen jedoch nicht alle unter 3.1 angesprochenen Sicherheitsanforderungen. So können alle, die den Schlüssel kennen ihn auch anwenden. Damit ist zwar die Integrität der Daten gegeben aber die Kriterien der Authentizität und die Identität werden nicht erfüllt. Daher dienen sie überwiegend der Verschlüsselung. Diese Daten können dann allerdings asymmetrisch digital signiert werden.

4.10.2 Kreditkarten

Bei allen Kreditkartensystemen, die sich nur in Grundgebühr und Leistungsumfang unterscheiden werden die Rechnungen zunächst von der Kreditkartenorganisation bezahlt, die diese Auslage vom Kreditkarteninhaber in der Regel monatlich begleichen lässt. Sie sichern Identität und Kreditwürdigkeit des Karteninhabers und stellen je nach Kreditkartenart ein bestimmtes Vertrauen her. Da bei Verlust die Karte gesperrt werden soll, ist sie auch relativ sicher gegen Missbrauch geschützt. Durch das (in Deutschland) vorhandene 14-tägige Rückgaberecht ist auch das Bedürfnis des Kunden abgedeckt.

4.10.3 Passwörter

Beide Partner müssen das Passwort kennen. Wer das Passwort kennt, kann es auch anwenden. Wenn Passwörter unverschlüsselt übermittelt werden, können sie sehr leicht ausspioniert werden. Dieses System wird daher fast nur noch in Verbindung mit z.B. symmetrischen Schlüsseln genutzt.

4.10.4 PIN / TAN

Das PIN/TAN System arbeit mit einer PIN, die dem Benutzer einmal mitgeteilt wird und meistens auch geändert werden kann. Sie ist Grundvorrausetzung zur Nutzung des gesicherten Dienstes. Über die TAN kann der einzelne Vorgang jederzeit nachvoll zogen werden. TANs werden dem Anwender über ein anderes Medium (z.B. Post) übermittelt und können nur einmal verwendet werden. Sie sind daher sehr sicher und wenn man eine ausspionieren sollte, kann man noch nicht auf andere schließen. Die Unveränderlichkeit der übermittelten Daten ist nicht gegeben. Durch die kurzen Verarbeitungszeiten bietet sich aber kaum eine Möglichkeit die Daten zu verändern.

5. elektronische Signaturen

5.1 Hemmnisse

Wie während dieses Berichts deutlich geworden ist, sind die technischen und rechtlichen Vorraussetzungen für den Einsatz elektronischer Signaturen schon länger gegeben.
Dennoch konnten sie sich bisher nicht durchsetzen.
Die folgende Kurve veranschaulicht den Akzeptanzverlauf gegenüber dem PKI-Konzept seit seiner Entwicklung.

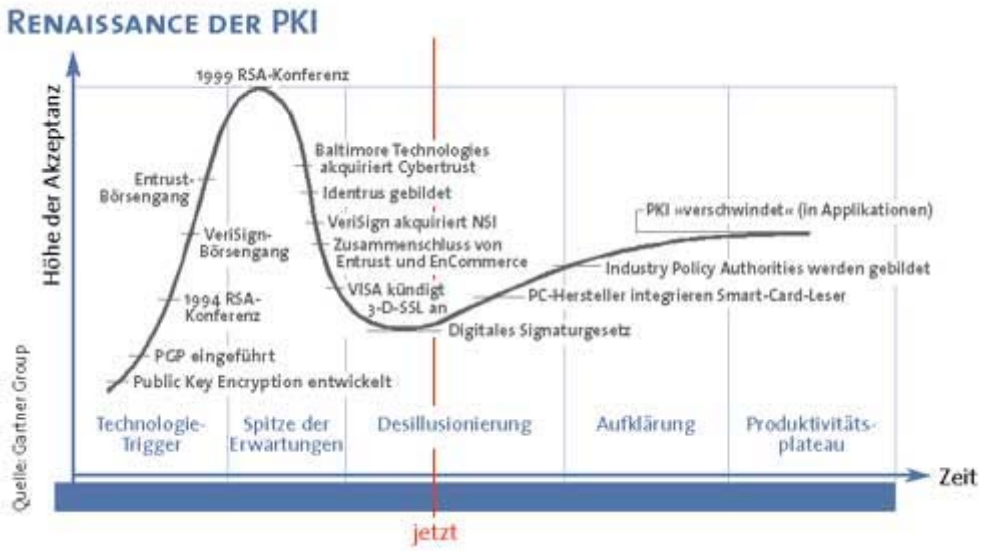

Abbildung 7: Verlauf der Akzeptanz des PKI-Konzeptes

Zu den zahlreichen Hemmnissen zählen vor allem die nationalen Unterschiede und die Systemvielfalt auf dem Markt. Allein innerhalb der EU werden 11 unterschiedliche Signatursysteme verwendet (Q7). Und auch die Bundesregierung nutzt unterschiedliche Signaturen (Q12). Solange der Verbraucher keinen Überblick über den Markt erhält, kann er sich bei dieser komplexen Materie nicht zu einer Festlegung durchringen. Gerade bei Unternehmen, die Ihr komplettes Sicherheitssystem umstellen müssten, sind solche Investitionen von Rechtssicherheit und Zukunftssicherheit abhängig.
Des Weiteren ist keine "Killerapplikation" (Q7), also keine Anwendung die durch den Einsatz der elektronischen Signatur revolutioniert würde vorhanden, die die Inkaufnahme der verbleibenden Risiken (siehe dazu 4.8) rechtfertigen. Die zahlreichen Alternativen (siehe dazu 4.10) die existieren und an die die Anwender sich oft schon gewöhnt haben, sind komfortabel genug für die bisherigen Anwendungszwecke. Dass einige Anwendungen wie z.B. E-Government teilweise mit höheren(!) Kosten belegt werden (Q7) ist insofern unverständlich, als dass die schon vorhandenen Anschaffungs- und Unterhaltungskosten schon abschreckend wirken. Wie das Beispiel Bremen (4.7) zeigt, sind die Kosten ein wichtiges Kriterium.
Auf ein weiteres Hemmnis werde ich unter den soziokulturellen Aspekten eingehen. Es geht darum, dass die Unterschrift ein Ritual ist, und weite Teile der Bevölkerung das Unterschreiben bewusst in der von Ihnen gewohnten Form durchführen wollen.
Das letzte Hindernis betrifft die komplizierte Anwendung der elektronischen Signaturen wie hier am Beispiel einiger Empfehlungen von telesec gezeigt werden soll.

"Verwenden Sie die PKS-Karte niemals bei Anwendungen, Maschinen, Türen oder Apparaten, deren Funktionen ihnen unbekannt, verdächtig oder unzuverlässig erscheinen

Sollten Sie nach Ausführen einer digitalen Signatur noch Zweifel an der Richtigkeit der signierten Informationen haben, prüfen Sie die digitale Signatur unverzüglich selbst , noch bevor Sie die signierte Information Dritten zur Verfügung stellen und vergewissern sie sich auf diesem Weg, dass der signierte Inhalt auch dem entspricht, was Sie signieren wollten.

Überzeugen Sie sich vor dem Einsatz von Signaturkomponenten, dass sich der PC noch in einer vertrauenswürdigen und zuverlässigen Konfiguration von Hard- und Software befindet. Verhindern Sie eine Beeinflussung der Signaturkomponenten durch Computerviren, trojanische Pferde, sonstige unerwünschte Manipulation oder nicht vertrauenswürdige Ergänzungen an der Software des PC, indem Sie regelmäßig am Marktverfügbare Prüfprogramme einsetzen um diese Fälle vor der Nutzung der Signaturkomponenten aufzudecken. Achten Sie darauf, dass während des Einsatzes der Signaturkomponenten keine Online-Verbindung zu Ihrem PC bestehe bzw. dass eine zuverlässige Trennung vom Netz durch entsprechende technische Komponenten vorgenommen wird. "Q15

Dies sind sicherlich alles sinnvolle Hinweise, doch welcher Anwender kann sich daran halten, wenn die elektronische Signatur so einfach sein soll wie die Unterschrift. Kaum ein Anwender kann die Funktion und Zuverlässigkeit der Geräte beurteilen. Ebenso wenig können beim Versand signierte Nachrichten nachträglich überprüft werden oder gar dem Empfänger vorenthalten werden. Ein mehrstufiges Konzept, das diese Möglichkeiten bietet, wird durch den gesteigerten Aufwand eine geringe Akzeptanz erfahren. Und die Sicherung des Computer ist auch ein schwieriger Punkt, da auch Trojaner oft erst im Nachhinein entdeckt werden können und ein kompletter Virenscan vor jedem Signieren ist unrealistisch. All diese Sicherheitsanforderungen können nur von einem integrierten System abgedeckt werden, das beim Signieren die nötigen Schritte ohne expliziten Eingriff des Anwenders ausführt. Der Zugriff auf die Signatur müsste wie bei einer Firewall standardmäßig gesperrt sein und individuell vom Anwender freigeschaltet werden.

Abschließend zeigt die folgende Grafik welche Priorität die Unternehmen (nach Branchen) dem Thema PKI in den nächsten 12 Monaten zukommen lassen wollen.
Basis 46/201/39/46 Antworten, Angaben in Prozentwerten.

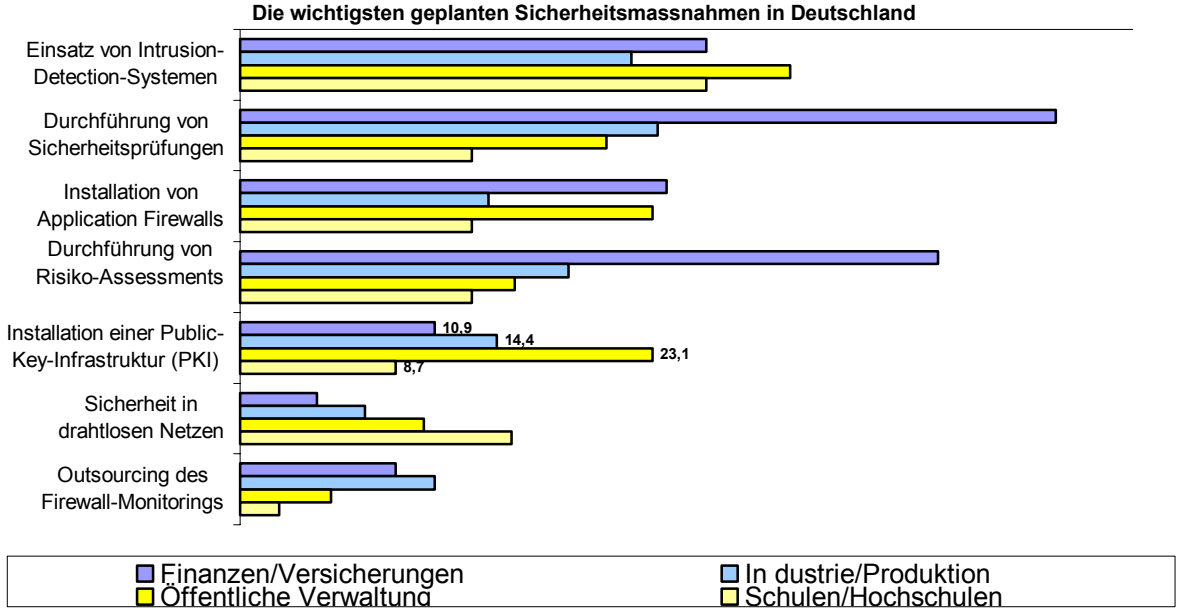

Abbildung 8: Geplante Sicherheitsmassnahmen 2002/2003 Q16

In Anbetracht der schwachen Konjunktur dürften die Investitionen noch zurückgehen, vor allem im Bereich der öffentlichen Verwaltung und Schulen.

5.2 Rechtliche und soziokulturelle Aspekte

Wenn es nun aber um einen elektronischen oder digitalen Ersatz der Schriftform geht, ist folgende Präzisierung nötig: Die oft genannte Forderung nach einer „Gleichstellung der digitalen Signatur mit der handschriftlichen Unterschrift" ist irreführend. Ein Papier-Dokument kann beispielsweise nicht digital signiert werden. Die digitale Signatur gehört zum elektronischen – oder eigentlich auch digitalen – Dokument, wie die Unterschrift zum Papier. Eine Gleichstellung kann daher nur zwischen digital signierten elektronischen Dokumenten und der Schriftform geschehen.

Es gibt mehrere kontextgebundene Mindestmerkmale eines Rechtsdokuments in den heute existierenden Rechtssystemen. Zuerst ist sicherlich die Sprache zu nennen. Sogar die Rechtsdokumente der Europäischen Union werden in allen Mitgliedstaatsprachen verfasst. Des Weiteren ist die Identifizierung des Autors und der weiteren betroffenen Personen unumgänglich. Wer keine Rechtsidentität hat, dem wird eine formell konforme Rechtsidentität zugewiesen. Anonyme Erklärungen oder private Äußerungen, beispielsweise in Tagebüchern, deren Urheber/Autor nicht zweifelsfrei bekannt ist, sind keine juristischen Dokumente. Die typische Struktur eines Rechtsdokuments variiert zwischen den Kulturen. Sie unterscheiden sich etwa bzgl. der Frage, ob Unterschriften notwendig oder welche Rituale vorgeschrieben sind. Die angesprochenen Sicherheitsmerkmale werden durch Stempel, Siegel, Unterschriften, Anwesenheit von Zeugen, Art des Papiers bzw. anderer Datenträger, Ort der Aufbewahrung, Zugriffsrecht, usw. gewährleistet. Das wichtigste Merkmal der Kontextgebundenheit zeigt sich mit Blick auf die Sprachdeutung. Denn meistens gibt es eine ganz besondere, nur in der Gesetzgebung verwandte Sprache. Diese differiert auch innerhalb eines Sprachraumes, z.B. zwischen Deutschland und Österreich.

Nun stellt sich die Frage ob er der Cyberkontext ein Kontext ist. Eine Steininschrift kann wegen der physischen Eigenschaften des Datenträgers und der Inschrift mehrere Jahrtausende lang erhalten bleiben. Dennoch können die semantischen Veränderungen der Sprache und die semiotische Veränderungen des Sprachkontextes die Deutung der Steininschriften dermaßen erschweren, dass sie sehr oft sehr lange Zeit nicht entschlüsselt werden können. Hier ist jeder Versuch einer technologischen Lösung grundsätzlich nur eine vorübergehende Lösung oder sogar eine Scheinlösung.

Für den Umgang mit Rechtsdokumenten kommt hinzu, dass das Internet sich bisher jeder nationalen Regelung wirksam entzieht. Einige nationalen Gesetze gegen Fälschungen von Informationen oder Identitäten sind zwar theoretisch anwendbar, haben sich aber bei der Anwendung im Internet als wirkungslos erwiesen. Da Rechtsordnungen komplexe, weitgehende und in erster Linie nationale Deutungssysteme sind, ist das ein großes Problem, dass gelöst werden muss, bevor elektronische Dokumente verwendet werden können. Erst muss ein international allgemein akzeptiertes Deutungssystem gefunden werden wie z.B. in der Mathematik.

Dies soll mit der Signaturrichtlinie erreicht werden. Deren Ziele wie folgt zusammengefasst werden können: Es geht um die Förderung der sicheren grenzüberschreitenden elektronischen Kommunikation. Eine Vorraussetzung dafür ist, dass elektronische Unterschriften, die in einem Mitgliedstaat erstellt werden, in allen anderen Mitgliedstaaten verifiziert werden können. Um einen freien Markt zu gewährleisten, muss das Angebot von Zertifizierungsdiensten auf europäischer Ebene gelten und sollte sich nicht nur an nationalen Märkten ausrichten. Das erfordert allerdings auch, dass elektronische Signaturen in jedem Mitgliedstaat gleichermaßen anzuerkennen sind.

Mit der Bereitstellung eines Rechtsrahmens allein können jedoch noch nicht alle Aufgaben als bewältigt gelten. Viele offene Fragen betreffen vor allem mathematische

wie technische, rechtliche wie ökonomische, psychologische wie ethische Belange und Fragen zu deren Sicherheit, Nutzbarkeit, Akzeptabilität, (kulturellen) Beherrschbarkeit und (moralische) Verantwortbarkeit.
Die digitale Technik bringt vollkommen andere Erfahrungen in Bezug auf Ton-, Bild- und Textinformationen als wir sie bisher von der analogen oder gar papierfundierten Informationsverarbeitung kennen. Es gibt nichts greifbares mehr, dass man „schwarz auf weiß" besitzt und mitnehmen kann. Es gibt nur noch binäre Codes und deren Inhalt hängt noch stärker, als der der Schrift, von der Interpretation ab. Und diese unterschiedlichen Zustände lassen sich ohne aufwendige technische Hilfsmittel nicht interpretieren. Es lässt sich unschwer erkennen, dass die digitale Kommunikation und Informationsverarbeitung weit reichende Folgen auf das menschliche Kommunikationsverhalten hat
Die Schrift ist das sinnlich wahrnehmbare Resultat von Schreibhandlungen, bei denen es einen direkten Zusammenhang zwischen bestimmten Handbewegungen und einem Schriftzug gibt. Alle auf Papier gebrachten Inhalte sind anzufassen, vorzeigbar, nachprüfbar, zuordenbar usw.
Vor allem, wenn die Inhalte Vereinbarungen von rechtlicher Relevanz betreffen, hat die Schriftform vor allem einen präventiven Zweck, nämlich für alle Fälle Gewissheit über die Verpflichtung oder die Berechtigung zu einer Leistung bieten zu können.
In engem Zusammenhang damit steht ein kulturell verankertes Charakteristikum der Papierwelt: Viele Schriftstücke werden mit einer Unterschrift versehen. Dies gilt sogar für maschinell Erstelltes. Dadurch wird der Zusammenhang zwischen dem Text und seinem Autor über seine eigenhändige Unterschrift bindend hergestellt und die Authentizität der Erklärung gesichert. Diese Unterschrift ist ohne größeren technischen und finanziellen Aufwand realisierbar. Der Kontext, der zum Erstellen des Textes und der Unterschrift gehört (Ort, Zeit, Art und Weise u.ä.) und der in der Papierwelt in gewisser Weise ermittelt werden kann, stellt ein weiteres Charakteristikum dar. Digitale Dokumente und elektronische Signaturen werden demgegenüber weitgehend kontextfrei übermittelt und reproduziert bzw. können in einem völlig neuartigen Kontext erscheinen.
Die Unterschrift ist als rechtlich bindend bekannt und hat eine Warnfunktion und es wird gelehrt, vor dem Unterschreiben zu prüfen, was unterschrieben wird. Doch kann diese Prüfung beim elektronischen Signieren vollzogen werden?
Die Komplexität des Verfahrens steht der erwünschten Transparenz entgegen. Selbst die visuelle Wahrnehmbarkeit der Prozesse ist nur eine mehrfach transformierte, elektronisch vermittelte. Nach Stetter C, Schreiben und Programm: Zum Gebrauchswert der Geisteswissenschaften, erschienen in Der vernetzte Mensch. Sprache, Arbeit und Kultur in der Informationsgesellschaft, Aachen, Verlag Mainz 1999, S. 159f. ist *"der Gebrauchswert erstens von der sozialen Akzeptanz dieses Produkts in der jeweiligen Gesellschaft und zweitens vor allem von der kulturellen Kompetenz der Nutzer wesentlich abhängig [… und …] eine Technologie, die nicht eingebettet ist in einen Handlungskontext von Menschen, die ihre Möglichkeiten und Risiken verstehen und besonnen mit ihr umzugehen wissen, hat nicht die geringste Chance, von der Gesellschaft, die diese Menschen insgesamt bilden, auf Dauer akzeptiert zu werden".* Es gibt also einen engen Zusammenhang zwischen einer technischen Lösung und der Kompetenz der Nutzer im Umgang mit dieser. Doch noch bestehen Kompetenzprobleme. Potentielle Nutzer sind irritiert, zeigen Handlungsunsicherheiten, es kommt entsprechend zu Handlungsfehlern. Der Nutzer steht vor einer neuen Situation und erwartet, im Geschäfts- wie Privatleben bisher alltägliche und eingeübte Handlungsweisen mit einem analogen Aufwand an Zeit und Kosten fortführen zu können. Gleichzeitig erhofft er durch die Verwendung elektronischer Signaturen vor allem in Hinblick auf die genannten Sicherheitsmerkmale vergleichbare Ergebnisse. Er ist immer vom ZDA, der so

genannten TTP, abhängig, wenn er die Signatur benutzen will. Wichtige Kriterien, die hier beachtet werden müssen, sind Sicherheit, Anonymität, Vertrauen, Freiheit und „Privatheit".

„Die angesprochene Beherrschbarkeit eines Prozesses ist dann gegeben, wenn es gelingt, diesen auf der Grundlage vorausschauenden planenden, gestaltenden Denkens "restlos" so zu konzipieren, zu realisieren und in Zweck-Mittel-Zusammenhängen zu nutzen, dass das angestrebte Ziel ohne unbeabsichtigte Effekte - vor allem negativ bewerteter Art - erreicht wird." Q4

Die Verantwortung der Nutzer besteht darin, in Entscheidungs- oder Wahlsituationen durch Tun oder Unterlassen dazu beizutragen, dass die Einführung und Nutzung im genannten Sinne unsicherer technischer oder technisch instrumentierter Lösungen verhindert und soweit Einführung und Nutzung sicherer Lösungen gefördert wird.

Manuelle Signaturen (siehe 3.2) und auch die elektronische können als Kultur betrachtet werden. *„Mit diesem Begriff werden üblicherweise jene Handlungsbereiche bezeichnet, in denen der Mensch auf Dauer angelegte, den kollektiven Sinnzusammenhang gestaltende Produkte, Produktionsformen, Lebensstile, Verhaltensweisen, Leitvorstellungen u.ä. hervorbringt." Q4*

Kultur umfasst sowohl ideelle wie auch materielle Bereiche, und auf Dauer aber sowohl räumlich wie auch zeitlich begrenzt angelegte Hervorbringungen (etwa im Unterschied zur Mode). In dieser weitgefassten Kulturdefinition tritt die Unterschrift in Wechselwirkung mit der Gesellschaft. Daher folgt nun ein Vergleich der die Ansätze der verschiedenen Kulturen teilweise wiedergibt.

Diese Informationen sind Q4 entlehnt und dort belegt und weiter ausgeführt.

5.3 Internationaler Vergleich

Im folgenden Abschnitt werden allgemeine Vorraussetzungen für den internationalen Einsatz elektronischer Signaturen formuliert. In den Ausführungen zu den einzelnen Ländern ist dann zu sehen in wieweit diese der Empfehlung entsprechen und wo noch Handlungsbedarf besteht. Da es sich um Momentaufnahmen oder bestimmte Projekte der einzelnen Länder handelt, ist kein direkter Vergleich anhand einer Tabelle möglich. Die Quelle für die Informationen ist, soweit nicht anders angegeben, Q4.

5.3.1 Deutschland

Die zuständige Behörde ist das Bundesministerium für Wirtschaft(www.bmwi.de). In Deutschland regelt das SigG den Umgang mit digitalen Signaturen
Der ZDA hat die Identifizierung des Antragstellers nach § 5Abs. 1 des Signaturgesetzes anhand des Personalausweises oder eines Reisepasses, der auf eine Person mit Staatsangehörigkeit eines Mitgliedstaates der Europäischen Union oder eines Staates des Europäischen Wirtschaftsraumes ausgestellt worden ist, oder anhand von Dokumenten mit gleichwertiger Sicherheit vorzunehmen. Soweit ein Antrag auf ein qualifiziertes Zertifikat mittels eines mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehenen elektronischen Dokuments des Antragstellers gestellt wird, kann der ZDA von einer erneuten Identifizierung absehen. Die Identifizierung ist vor Übergabe des qualifizierten Zertifikats und vor Einstellung in das Zertifikatsverzeichnis gemäß § 4 Abs. 1 vorzunehmen. Die erste Fassung des SigG vom 1.8.1997 (als Art. 3 des Informations- und Kommunikationsdienstegesetzes - IuKDG) war das weltweit erste Gesetz seiner Art für den gesamten Rechtsraum eines Staates. Es hatte notwendigerweise Experimentiercharakter, da sich das technische Umfeld erst herausbildete. Am 22.5.2001 trat das neu gefasste SigG (jetzt mit dem Titel "Gesetz über Rahmenbedingungen für elektronische Signaturen") in Kraft, das die erste Fassung komplett ersetzte. Leider ist die Neufassung nicht gerade geeignet, das Verständnis der Materie zu erleichtern.
In diesem Zuge wurde § 126 BGB um einen Abs. 3 ergänzt, in dem die "elektronische Form" als Alternative für die bisherige Schriftform anerkannt wird. Weiter gilt ein neuer § 292a der Zivilprozessordnung (ZPO). Danach gilt zugunsten einer in elektronischer Form vorliegenden Willenserklärung (entsprechend den Anforderungen des § 126a BGB) der sog. Beweis des ersten Anscheins. Darüber hinaus wurden weitere 36 Gesetze und Verordnungen angepasst.

5.3.2 EU

Am 19. Januar 2000 wurde die europäische Richtlinie 1999/93/EG vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen bekannt gegeben (EU 2000). Die Richtlinie selbst trat am Tag ihrer Veröffentlichung in Kraft und ist seither für die Mitgliedstaaten verbindlich. Für ihre Rechtswirksamkeit auch gegenüber Privaten bedarf es allerdings noch der Umsetzung ihrer Vorschriften in nationales Recht. Die EU-Richtlinie fordert im Wesentlichen, dass der Anwender den Schlüssel alleine verwalten kann und jedem ZDA der Zugang zum Markt ermöglicht werden muss. Die elektronische Signatur soll mit der traditionellen Unterschrift gleichgesetzt werden.

5.3.3 Österreich

Das österreichische Bundesministerium für Wirtschaft und Arbeit hat eine Initiative rund um die digitale Signatur gestartet. Gefördert werden sollen 3-5 (auch Pilot-)Projekte, die die Anwendungsmöglichkeiten der digitalen Signatur im b2b/b2c Bereich aufzeigen sollen.Q9

Weitere Informationen zu Österreich gibt es im Internet unter http://www.a-sit.at/Deutsch/dokument.htm

5.3.4 Großbritannien

Hier wurde im Mai 2002 die "Electronic Communications Bill" verabschiedet. Bemerkenswerterweise wird ausdrücklich festgestellt, dass grundsätzlich alle Arten elektronischer Signaturen, also auch nicht-qualifizierte, Rechtswirkungen entfalten können. Anstatt alle Gesetze zu aktualisieren wurde die Regierung ermächtigt eine Anpassung der Formvorschriften an die Anforderungen der elektronischen Kommunikation vorzunehmen. Die durch die Regierung zu beachtenden Regeln sind dabei ausdrücklich festgelegt. Q4

5.3.5 Irland

In Irland wird mit der am 10.07.2000 unterzeichneten "Electronic Commerce Bill 2000" ein sehr liberaler Ansatz verfolgt. Grundsätzlich werden alle Arten elektronischer Signaturen rechtlich anerkannt und Informationen in elektronischer Form wurden mit solchen, die in einem Papierdokument enthalten sind gleichgestellt. Es bleibt hierbei den Parteien selbst überlassen, dass ihren Anforderungen entsprechende Sicherheitsniveau zu bestimmen.

5.3.6 Frankreich

Frankreich hat am 13. März 2000 ein Gesetz angefertigt, welches eine neue Definition des schriftlichen Beweises einführt, wonach dieser sowohl aus Papier als auch aus einem digitalen Träger bestehen kann. Ein Schriftstück in elektronischer Form hat denselben Beweiswert wie ein Schriftstück auf einem Papierträger soweit der Autor sicher identifiziert werden kann und das Schriftstück in einer Weise hergestellt und verwahrt wird, durch die seine Integrität sichergestellt wird. Im Falle eines Konflikts ist es Aufgabe eines Richters, festzustellen, ob dem elektronischen oder demjenigen aus Papier der höhere Beweiswert zukommt. Gleichzeitig wird das Konzept der elektronischen Signatur in den Code Civil eingeführt. Die Vertrauenswürdigkeit des Verfahrens wird vermutet, wenn die elektronische Signatur gemäß den in einem Dekret des Conseil d'Etat festgelegten Konditionen erstellt, die Identität des Unterzeichners versichert, und die Integrität des Dokuments verbürgt wird.

5.3.7 Dänemark

In Dänemark ist im Frühjahr 2000 ein neuer Gesetzesentwurf mit dem Ziel der Umsetzung der europäischen Richtlinie über elektronische Signaturen entstanden. Es ist eine relativ strikte Regelung für die Überwachung von ZDA geplant. Vor Aufnahme seiner Tätigkeit muss jeder ZDA diese bei einer staatlichen Stelle anzeigen. Darüber hinaus hat er einen jährlichen Rechenschaftsbericht abzulegen, der der Bestätigung eines unabhängigen Prüfers bedarf.

5.3.8 Schweden

Schweden plant ein ähnliches System, aber ergänzt dieses um ein freiwilliges Akkreditierungssystem im Rahmen der SWEDAC.

5.3.9 Benelux

Auch die Gesetzesentwürfe in Belgien und Luxemburg schlagen eher die Richtung einer strengen staatlichen Aufsicht über die ZDA ein.
In den Niederlanden wurde gegen Ende 1999 ein Konzept veröffentlicht, das zeigt, dass man den Markt hauptsächlich sich selbst überlassen will. Die TTP-Kammer soll nicht der Zertifizierung der ZDA dienen. Sie soll alle operationellen Fragen dem Markt selbst überlassen und ein öffentliches Register aller ZDA bereithalten, unabhängig von der Qualität der von ihnen ausgegebenen Zertifikate.

5.3.10 Finnland

Finnland ist in diesem Rahmen insbesondere durch sein Experiment mit digitalen Identitätskarten (FINEID) bekannt: Diese bestehen aus einer Chipkarte, die nach dem Prinzip eines Personalausweises durch staatliche Stellen an jeden Bürger ausgegeben wird und mit der die Erstellung elektronischer Signaturen möglich sein soll.

5.3.11 Schweiz

Das Bundesamt für Justiz hat im Rahmen der Vorarbeiten zur rechtlichen Regelung der digitalen Signatur kürzlich ein Gutachten zur Positionierung der digitalen Signatur im schweizerischen Privatrecht erstellt (Bundesamt für Justiz, Digitale Signatur und Privatrecht, VPB 63.46, Bern 1999).

5.3.12 USA

In den USA ist am 1.10.2000 der "Electronic Signatures in Global and National Commerce Act" in Kraft getreten, dessen Ziel es ist die Rechtswirksamkeit schriftlicher Vertragsabschlüsse über elektronische Medien sicherzustellen. Das Gesetz versteht unter elektronischer Signatur ein elektronisches Geräusch, Zeichen oder Verfahren, das mit einem Vertrag oder einer sonstigen Aufzeichnung verbunden oder logisch verknüpft ist. Vor dem Hintergrund des Gewaltenteilungsprinzips beachtlich ist das Recht der staatlichen Regulierungsbehörden, das Signaturgesetz verbindlich auszulegen. Weiter haben sie die Möglichkeit, den Anwendungsbereich des Gesetzes nach einem öffentlichen Anhörungsverfahren zu erweitern. Die Suche nach der besten Technik überlässt der US - Gesetzgeber weitgehend dem Markt.

5.3.13 Japan

Das Japanische Parlament verabschiedete ein Gesetz für den Umgang mit elektronischen Signaturen. Es trat am 1. April 2001 in Kraft. Auch ausländische ZDA können gemäß diesem Gesetz akkreditiert werden. Das 47 Artikel umfassende Gesetz regelt den Einsatz elektronischer Signaturen, den Umgang mit qualifizierten Zertifikaten und die Vorraussetzungen zur Akkreditierung der ZDA.

5.3.14 Ungarn

Der ungarische Gesetzentwurf setzt sich die Anerkennung der Gültigkeit elektronischer Dokumente in allen Bereichen der Gesellschaft zum Ziel. Die Problematik der digitalen Unterschrift und Kryptologie wurde auch im Projekt aus dem Jahre 1997 "Öffentlicher Schlüssel und Sicherheitsvorsorge für Daten des Netzes HUNGARNET" gelöst. Das Projektziel ist die Koordinierung der Arbeiten an den Dienstleistungen vom Typ HUNGARNET-CERT und an der Schaffung der Zertifikationsautorität.

5.3.15 Polen

In Polen findet das Thema der elektronischen Signaturen bisher noch keine breite Beachtung. Im Allgemeinen besteht im polnischen Gesetzbuch der Anspruch, dass ein schriftlicher Vertrag durch die eigenhändige Unterschrift bestätigt werden muss. Für die über Internet zu schließenden Verträge und für die Anwendung digitaler Signaturen ist damit ein praktisches Hindernis gegeben. Zwar wird im neuen polnischen Bankenrecht vom 29. 08. 1997 betont, dass die Willenserklärung bei Vertragsschließung mit elektronischen Mitteln möglich ist, die auf diese Weise vorbereiteten Urkunden müssen jedoch gut versichert und festgehalten sein. Man betont auch, dass elektronische Formen im Vergleich mit den traditionellen schriftlichen Formen der Urkunden erhalten bleiben.

5.3.16 Russland

An neuen und an der Verbesserung schon existierender Gesetze wird gearbeitet. Dabei sollen auch die rechtlichen Regelungen der EU, soweit sie Probleme des Datenschutzes betreffen, ins russische Rechtssystem einbezogen werden. Schon im Jahre 1979 wurde ein Gesetz "Über den Beweiswert elektronischer Urkunden" angenommen, in dem diese Urkunde als gleichwertig mit der schriftlichen Urkunde angesehen wurde. 1995 wurde ein Gesetz über den Informationsschutz angenommen und in Übereinstimmung mit diesem Gesetz kann auch die elektronische Unterschrift für bestimmte Urkunden benutzt werden. Es handelt sich hier besonders um die durch staatliche Institutionen vorbereitete Urkunden, die auch von speziell dazu berechtigten Personen identifiziert werden können. Einige Vorschriften, die im Zivilgesetzbuch vom 1996 formuliert sind, regeln bereits die Gültigkeit elektronisch vorbereiteter Verträge und damit auch die rechtmäßige Verwendung elektronischer Signaturen. Auch hat sich bereits eine Agentur für Kommunikation und Information in Russland gebildet, die die benutzte elektronische Signaturen bewilligen soll und deren Zuständigkeit auch die Vergabe von Lizenzen für die Anwendung von Kodierungsmittel und -methoden umfasst.

5.3.17 China

Die meisten chinesischen Seiten sind nur unzureichend in die englische Sprache übersetzt. Es gibt hier zwar zahlreiche Seiten zum Stichwort PKI, und somit auch eine Bewegung jedoch konnte ich keine verwendbaren Informationen finden.

5.3.18 ASIA-PACIFIC ECONOMIC COOPERATION (APEC)

In Bezug auf E-Commerce wurde bereits während des Kongresses im Jahre 2000 das „Digtal Signature and Certificates" Gesetz verabschiedet. Dieses Gesetz gewährt der elektronischen Signatur die gleiche Rechtskraft wie der manuellen Unterschrift. Die entsprechenden Verordnungen sind bereits im Mai 2002 verabschiedet worden. Q13

5.3.19 Vereinte Nationen

Auf der Ebene der Vereinten Nationen hat deren Handelsrechtskommission am 23.11.1997 einen Entwurf einheitlicher Regeln über elektronische Signaturen veröffentlicht. Dieser enthält Mindestsicherheitsstandards sowie Regelungen zur Authentisierung, Zertifizierung und Haftung von ZDA und Zertifizierungsstellen. Er dient als einer der Grundlagen für die internationale Diskussion.

5.3.20 Zusammenfassung

Wie hier gezeigt wurde, bestehen international noch sehr große Unterschiede. Vor allem was den Umgang mit ZDAn und der Definition qualifizierter Zertifikate betrifft. Daher wird ein grenzübergreifender Einsatz noch auf sich warten lassen. Zumal die Unter **Fehler! Verweisquelle konnte nicht gefunden werden.** erwähnte Infrastruktur zwischen den ZDA noch erstellt wurde. Zwischen einzelnen Firmen und Organisationen die gemeinsame Richtlinien verfolgen (auch international) ist der Einsatz allerdings schon möglich. Unter Umständen bedeutet dies jedoch, dass ein Benutzer viele Schlüssel und Zertifikate benötigt. Je nachdem an wie vielen Systemen er beteiligt ist.

6. Zusammenfassung und eigene Meinung

Es ist wichtig in der Diskussion zwischen digitaler und elektronischer Signatur zu unterscheiden. Auch welche Bedürfnisse gedeckt werden sollen, muss geklärt werden. Geht es nur im die Integrität der Daten, so ist die digitale Signatur ein geeignetes Werkzeug. Sollen aber alle in 3.1 aufgeführten Sicherheitsanforderungen erfüllt werden, bedarf es der elektronischen Signatur.
Hier gibt es inzwischen Regeln und Verfahren, die nahezu alle Bereiche der traditionellen Unterschrift abdecken. Zertifikate gewährleisten die Authentizität und Identität, Gruppensignatur können für Stellvertretungen eingesetzt werden. Unterschiedliche Schlüssel gewährleisten die Trennung von privater und geschäftlicher Unterschrift. Eine vereinfachte Unterschrift kann entfallen, da die elektronische Unterschrift sehr schnell anzuwenden ist.
Es gibt viele Menschen, die einen Computer haben und auch im Umgang mit E-Mail geübt sind. Auch der elektronische Handel setzt sich immer mehr durch. Trotzdem konnte sich die elektronische Signatur bisher nicht durchsetzen.
Das liegt vor allem daran, dass für die meisten Verträge nur relevant ist, dass der Unterzeichner zahlen kann. Dies ist durch eine Kreditkarte hinreichend sichergestellt.
Nur bei Verwaltungsgängen ist es wichtig dass es sich bei der Person auch um diese handelt. Diese sind jedoch so selten, dass sich die Investition und der Aufwand elektronischer Signaturen nicht lohnen. Denn wie im Bereich 5.1 deutlich wird, ist es in der Praxis wesentlich teurer und aufwendiger als die Theorie vermuten lässt.
Doch auch die vielen Risiken (siehe 4.9) sind noch nicht überwunden. Da die meisten Risiken die Sicherheit der Systeme betreffen, auf denen sie eingesetzt werden sollen ist auch noch keine Lösung in Sicht. So können z.B. trojanische Pferde oder böswillige ZDA den Schlüssel missbrauchen.
Wenn diese überwiegend technischen Risiken gelöst werden sollten, so besteht noch ein Akzeptanzproblem seitens der Anwender. Der fehlende persönliche Bezug zur Unterschrift, erfordert ein Umdenken, da das Unterschreiben an sich ein Ritual ist, das dem elektronischen Signieren fehlt. (siehe 5.2)
CIO (eine große Fachzeitschrift) titele „Nur fast tot" und schrieb *[…]Einzig das Konzept der öffentlichen Schlüssel sei sehr ansprechend gewesen. Die Anbieter seien arrogant gewesen, während die Firmen es ohne zu überlegen gekauft hätten. Das habe nur solange funktioniert, wie es die Umsätze zuließen. PKI sei ein Musterbeispiel des IT-Booms gewesen. […]Ein großer Anbieter (Entrust) habe PKI inzwischen als Auslaufmodell bezeichnet. Während die Technologie der digitalen Signatur erhalten bliebe, werde der Ausdruck PKI nicht mehr verwendet. PKI sei kein Gesamtkonzept mehr. Sondern die digitale Signatur werde in bestehende Sicherheitssysteme eingeflochten. Damit werde Abstand von riskanten Prestigeprojekten genommen und sich mehr auf erfolgsversprechende Projekte konzentriert. Damit seien die elektronischen Signaturen nicht am Ende, aber der Weg werde langsamer beschritten werden. […]* Q14

Ich persönlich werde die elektronische Signatur nicht nutzen, da die Sicherheitsrisiken überwiegen und keine Anwendung verfügbar ist, die diese Risiken rechtfertigt. Zumal man eine Signatur nicht begrenzen kann und somit der komplette Rechtsrahmen auch im negativen Sinne ausgeschöpft werden kann (falsche Meldeverfahren, Käufe, statt nur falscher E-Mails). Die digitale Signatur hingegen verwende ich bereits und halte sie für sinnvoll. Die Authentizität der Daten und die Identität des Autors kann im Zweifelsfall auch über das Telefon geklärt werden.

7. Verzeichnisse

7.1 Stichwortverzeichnis

7.2 Abbildungen

7.3 Tabellen

8. Quellenverzeichnis

Quellen ohne Datumsangabe wurden im September 2003 abgerufen.

Q1 Digitale Signaturen: mit 11 Tabellen//Andreas Bertsch/Berlin, Springer 2002

Q2 La signature:du sceau à la clè numérique; histoire, expertise, interpretation/2./ Alain Buquet/ Paris, Éd. Service Gutenberg XXIe siècle , 2000

Q3 Group signature schemes and payment systems based on the discrete logarithm problem /1./ Jan Camenisch/Konstanz, Hartung-Gorre, 1998

Q4 Elektronische Signaturen: kulturelle Rahmenbedingungen einer technischen Entwicklung // Christian J Langenbach/Berlin, Springer, 2002

Q5 E-Mail anfrage an Dr. H. Sponholz MoTechno - Mobile Technologies/08.09.2003

Q6 Freemail-Nutzerhilfe, www.freemail.de

Q7 Digitale Signaturen im Aufwind, Heise-Online-newsticker, http://www.heise.de/newsticker/data/wst-14.05.03-004/ , 14.05.03

Q8 Berechnung diskreter Logarithmen, Steffen Muhle, http://danae.uni-muenster.de/~lembeck/lehre/ws02/seminar/03_muhle.pdf, 2002-12-16

Q9 Impulsprojekt Digitale Signatur, BMWA, http://www.electronic-business.at/links/677.html

Q10 Digitale Signatur für Sozialversicherung, Telekom-Presse, http://www.telekom-presse.at/channel_internet/news_9812.html, 29.07.2003

Q11 http://www.ummelden.de Bereich Digitale Signatur

Q12 Schlafender Wolf, manager-magazin.de , http://www.manager-magazin.de/ebusiness/artikel/0,2828,243231,00.html, 03.04.2003

Q13 APEC-Nachrichtentechniken und Informationsarbeitsgruppe 27. Sitzung, http://www.apectelwg.org/apecdata/telwg/27tel/plenary/p14.htm , März 2003

Q14 Only Mostly Dead, CIO Magazine, http://www2.cio.com/research/security/edit/a05232002.html, May 23, 2002

Q15 Informationen zur Teilnahme am Public Key Service, Deutsche Telekom, http://www.telekom.de/dtag/t-telesec/telesec_showdatei/1,2626,14,00.pdf

Q16 Blind oder blauäugig, sandra gerbich, http://www.informationweek.de/index.php3?/studien/studie18a.htm, 12.09.2002

Q17 National Institute of Standards and Technology, Public Key Infrastructure Study-Final Report, http://csrc.nist.gov/pki/documents/mitre.ps , April 1994

8.1 Weiterführende Literatur

W1 Der Vertragsabschluss via Internet im Internationalen Wirtschaftsverkehr//Christian Bierekoven/Köln, Heymann, 2001 462S.

http://www.hack.gr/users/dij/crypto/overview/publickey.html Funktionsweise

http://www.counterpane.com/pki-risks-ft.txt Counterpane Internet Security

http://www.signaturrecht.de/eu-richtlinie/eu-richtlinie.html Eu Richtlinie

http://www.bmwi.de/Navigation/Technologie-und-Energie/Informationsgesellschaft/medienrecht.html Gesetzestexte zum Thema Medienrecht

http://www.icisc.org/ International Conference on Information Security and Cryptololgy

http://csrc.nist.gov/pki/documents National Institute of Standards and Technology (eng.)

http://www.pkiforum.com/main.html Aktuelle News zum Thema PKI

http://www.openca.org/

http://www.mozilla.org/projects/security/pki/

http://www.datenschutz.ch/anforderungen_elektronische_datenuebermittlung_2002-03.pdf

http://singlesignon.net/

9. Anlagen

9.1 Arbeitsprotokoll

04.09.03	Bearbeitungsschwerpunkte festlegen, Quellen suchen
05.09.03	Extrahieren relevanter Textpassagen
10.09.03	Gliederung verfeinern, Bücher suchen , ausleihen und durchsehen
11.09.03	Bücher überfliegen und relevante Kapitel lesen
12.09.03	Präsentation –Folienüberschriften/Themen
15.09.03	Präsentation –Inhalte
15.09.03	Bericht schreiben Einleitung
16.09.03	Bericht schreiben Technik
17.09.03	Präsentation mit Erkenntnissen aus dem Berichts aktualisieren
17.09.03	Bericht schreiben / Daten u. Diagramme aufbereiten
18.09.03	Bericht schreiben (Hemmnisse/Zertifikate)
19.09.03	Bericht schreiben (Internationale Vergleich)
22.09.03	Bericht schreiben (Soziokulturelle /Rechtliche Aspekte)
23.09.03	Verzeichnisse erstellen
24.09.03	Rechtschreibprüfung
25.09.03	„Letzter Schliff"

9.2 Flüchtige Quellen

Q5
Von: H Sponholz [HS@motechno.com] An: Haag, Moritz
Betreff: AW: Preis-Anfrage / Bestellung.

Hallo Herr Haa,
zur marktüblichen Preisindikation:
a) Einzelnutzer je nach Produkt ca 100-200 EUR,
(wir bedienen Konsumenten in diesem Umfeld allerdings nicht.)
b) Gewerbliche nutzer in der von Ihnen geannter Funktionalität 100-200 EUR pro Arbeitsplatz abhängig von der SW-Umgebung und dem Produktanbieter. Bei komplexen Projekten und Anpassungen können - abhängig vom Anbieter mehr verlangt werden.

Mit freundlichen Gruessen / Regards
Hanno Sponholz

+49.179.2068462
+49.30.95993029

Mail address:
Dr. H. Sponholz
MoTechno - Mobile Technologies
PF 35 03 61
D - 10212 Berlin

Shipping/Office address:
MoTechno.de
Ehrenbergstr. 11-14
D-10245 Berlin