Ein subjektiver Bericht über ein Streitgespräch

Am 2.12.03 fand in den Räumen des SigLab in Bonn das erste, und hoffentlich nicht letzte, Streitgespräch über die Vor- und Nachteile von digitalen Siegeln, allgemein als digitale „Signaturen“ propagiert, und eigenhändig geleistete digitalen Unterschriften statt.

Das Plädoyer für die digitalen Siegel hielt Herr Rechtsanwalt Klaus Brisch, Partner im Büro Graf von Westphalen, Köln.
Für die eigenhändige digitale Unterschrift und die tippdynamische Pin ergriff René Baltus, der Erfinder eines Handschriften-Erkennungs-SYstems, Classic-Sign, das Wort.[1]

Neben weiteren Juristen waren noch Besucher aus öffentlicher Verwaltung, Geldinstituten und Anbieter von Schrifterkennern anwesend.

Vorweg sei der Hinweis erlaubt, dass die Verordnung zum Geseztz zur sogenannten digitalen „Signatur“ sehr wohl die eigenhändige Unterschrift als auch die tippdynamisch erfasste Pin zur echten Identifikation des Signaturschlüsselinhabers oder Unterzeichners beinhalten!

Herr Brisch begann mit seinem juristisch und technisch erstklassigen Vortrag über die Gesetzeslage in Deutschland und der EU.
Er berichtete von seiner Arbeit in den EU-Ausschüssen und, sozusagen als „Highlight“, von einem „Schauprozess“, bei dem es um die Beweiskraft digitaler Siegel ging.

Korrekterweise hielt sich Herr Brisch an der Tastsache, dass die Richter (die wie im richtigen Leben gearbeitet haben) lediglich die **Rechtmäßigkeit der Langzeitarchivierung** zu beurteilen hatten. Ein Thema, das auch für eigenhändige digitale Signaturen (Alpha-Signaturen) von eminenter Bedeutung ist. Die Archivierung von Unterschriftsdaten unter der Empfangsquittung für ein Paket fallen wohl nicht darunter. Die von Verträgen, Bestellungen, Übergabe von Waffen und Munition, Schlüssel, Arbeitszeugnisse und Ähnlichem sehr wohl.

Für die anwesenden Fachleute war es im Grunde nur eine Wiederholung der seit langem unveränderten Argumente für die digitalen Siegel nach SiG und SigV.

An diesem Punkt kann nun von der 1. Synthese gesprochen werden.

1. **SigLab-Synthese:**
   Alle Verfahren für eigenhändige digitale Signaturen (Apha-Signaturen) als auch digitale Siegel müssen oder sollten abgestuft eine dem Gesetz oder dem Richterrecht angepassten Archivierung bis hin zu 30 Jahren oder mehr erlauben. (**Anm- Baltus:** Die Synthesen sind lediglich im Bonner SigLab entstanden, stehen aber sonst in keinem Zusammenhang mit dem MSC Köln und seinem Bonner Ableger.)

Da im Umfeld der Langzeitarchivierung inbegriffen, wurde nur kurz das Problem der Quersumme (Hash) aller Daten des, wie auch immer, signierten oder versiegelten Dokumentes, angeschnitten. Klar war den Beteiligten, dass auch die Daten der Schreibdynamik einer eigenhändigen Unterschrift oder der tippdynamisch erfassten Pin untremnnbar mit dem Dokument verbunden sein müssen. Dass dies möglich ist, zeigen deutsche, israelische und amerikanische Softwaren. (SignoTec, Penflow und CIC).
Daraus darf dann die 2. Synthese abgeleitet werden:

2. **SigLab-Synthese:**
Alle Identikationsdaten des Unterzeichners oder die Daten der Chipkarte/Pin sind mit transparenten und nachweisbaren Verfahren untrennbar mit dem elektronischen Dokument zu verbinden. Idealerweise und das Vertrauen in die elektronischen Siegel und Unterschriften stärkend, wäre es, wenn z.B. nur die Gesellschaft für forensische Schrifuntersuchung, GfS, die dynamischen Daten der

Unterschriften extrahieren könnte. Die an sich wertlose Faksimile der Unterschrift kann unverschlüsselt und für jedermann sichtbar im Dokument verbleiben.

Der 2. Synthese folgt automatisch die unstrittige und selbstverständliche 3..

3. **SigLab-Synthese:**
   Jegliche Veränderung der Daten eines digital signierten oder versiegelten Dokumentes sind im geöffneten Dokument sofort deutlich sichtbar an zu zeigen.

Der Einwand eines Teilnehmers aus dem IT-Strategiestab eines grossen Bundesamtes regte eine heisse Diskussion an mit der Frage, warum überhaupt unterschrieben oder versiegelt werden müsse. In seinem Amt werden unzählige Papieranträge bearbeitet. Diese sind zwar unterschrieben, aber wer da unterschrieben habe, könne er nicht prüfen und es wäre sowieso uninteressant. Der Antrag wird förmlich geprüft, wenn alles stimmig sei, wird er genehmigt, nach Eingang der Schlussrechnung wird auf das angegeben Konto die Subventionssumme überwiesen. Schluss.

Der selbe Teilnehmer warf auch die Frage auf, ob z.B. die Beantragung eines Führerscheines überhaupt unterzeichnet werden müsse.
Nicht zu unrecht; auch Baltus räumte ein, dass die Beantragung seines Führungszeugnisses nach Belegart „0“ an sich keine Unterschrift bedarf. Unstrittig war allerdings, auch bei den DigSiegel-Protagonisten, dass der Empfang eines Dokumentes, hier beispielsweise der Führerschein, sehr wohl quittiert werden müsse. Die einen meinten, die Versiegelung (?) mittels Karte und Pin genüge (?), die anderen waren für eine eigenhändige Willenserklärung mit der Unterschrift. Letzteres ist ja auch sinnvoll, da dder empfänger „sein“ Stück Papier mitnehmen kann; niemand kann ihm etwas siegeln lassen, war er gar nicht gesehen hat!

Allerdings wurde Seitens der Siegelprotagonisten zugegeben, dass die digitale Versiegelung ein Ausdrucken des versiegelten (sie nannten es naturgemäs: „signierten“) Dokumentes erst NACH der Versiegelung erlaubt!
Der Vesiegelnde sieht hierbei nicht, was er tatsächlich versiegelt oder (nach politisch korrektem Sparchgebrauch) „signiert“ hat! Dieses nachträglich erstellte papierene Dokument hat vor Gericht Null Beweiswert -es könnte ja von jedem gescannt oder sonstwie kopiert und damit auch verändert worden sein.
Damit konnte zu diesem Punkt leider keine Synthese erarbeitet werden. Bei den digitalen Siegel nach SiG ist kein Papier für den Unbedarften vorgesehen.

Es bleibt das ungelöste Problem der digitalen Versiegelungen: die Darstellungskomponente und damit automatisch verbunden die nicht beantwortete Frage, was denn der Unbedarfte mit als beweisfähiges, bei Gericht vorzeigbares und seine Sicht der Dinge darlegendes Dokument mit nach Hause nimmt. Was, wenn sein Pc abstürtzt? Wo ist dann der Beweis?
Hier folgt dann immer der „lustige“ Hinweis, dass ja auch Häuser und damit das papierdokument abbrennen würden. Ja, das stimmt; eine grausige Vorstellung.
Meine Gegenfrage, was denn öfter geschehen würde, eine Hausbrand oder eine PC-Absturz, bleibt immer unbeantwortet.
Selbst wenn der Unbedarfte eine Diskette oder eine CD hat -er weiss nicht, was er zuvor tatsächlich versiegelt hat.[2] Ob die Richter heute schon die technische Ausstattung haben um eine DVD lesen können, muss auch noch geklärt werden. Und werden sie in 30 Jahren noch ein Diskettenlaufwerk besitzen, um ein heute gespeichertes digitales Siegel bewerten zu können?

Diese Fragen leiten über zu dem sehr wichtigen Einwand eines Juristen (nicht Herr Brisch!).
Baltus betonte nochmals, die Pin müsste nach dem Vortrag eines BSI-Fachmannes 8stellig sein. Der im DigSiegelgeschäft fleissige Jurist meinte lapidar: „Das sei nur die PRIVATE Meinung des BSI-Mitarbeiters gewesen!“

Diese Aussage muss man sich auf der Zunge zergehen lassen:
Ein Bundesamt für Sicherheit in der Informationstechnik (BSI), das in einem Gesetzgebungsverfahren, neben der Prüfung der Sicherheit des DigSigs-Verfahrens, die gesamte Organisation und die Protokollierung der Konferenzen zur Aufgabe hat, lässt **unwidersprochen durch seinen Vorgesetzten** einen Kryptofachmann seine PRIVATE Meinung darlegen.
Dann müssten auch die unbequemen Äusserungen von BSI-Fachmann Dr. Ansgar Heuser (in einem Vortrag vor der Notarkammer, s.u.) zur privaten Meinung erklärt werden.
Also hätten wir nun schon zwei BSI-Mitarbeiter, die nichts anderes zu tun haben, als ihre private Meinung öffentlich Kund zu tun.

Bei solchen „Argumenten" erübrigt sich jeder Versuch einen Konsens oder eine Synthese herbei zu führen. Sie zeigen aber auch, auf welchem tönenernen Fundament die jetzige DigSig-Argumentation steht.

Der „Weltmeister" im Hacken, Kevin Mitnick, verbreitet in seinem Buch „Die Kunst der Täuschung" Gott sei Dank (werden nun einige seufzen!) „nur" seine private Sicht der Dinge. Hier ein Textauszug aus der Buchbesprechung http://a-sig.com/BuchbesprechungMitNick.pdf :

Kevin Mitnick zählt im Index 27 mal den Begriff „Sicherheit" auf, von Sicherheit bis Sicherheitszertifikat.
Danach folgt sofort „Passwort" mit 18 Erwähnungen. Scheint etwas daran zu sein, an den operationellen Schwächen der Passwörter!
Auf Seite 364 meint Mitnick zur Auswahl der Paßwörter folgendes: Das Passwort muss ...
... für Standard-Nutzerkonten wenigstens **acht Zeichen und für privilegierte mindestens zwölf Zeichen lang sein**,
... mindestens eine Nummer und ein Symbol und einen Groß- und einen Kleinbuchstaben enthalten,
... es folgen noch weitere Kriterien, die aber alle an sich bekannt sein sollten. Sollten! ##

Damit läuft auch der (witzige?) Einwand eines Juristen (nicht Herr Brisch!): „..... dass Baltus eine 16stellige Pin verlange ..." wohl ins Leere.
Baltus hat als Einziger bei der vom BSI-Fachmann anheim gestellte Abstimmung für eine 8stellige Pin gestimmt -49 der Anwesenden für eine 6stellige! Das müsste auch im Protokoll der Sitzung auch so niedergeschrieben sein.

Da Baltus es, im Gegensatz zu Herrn Brisch (der seinen Vortrag bis auf zwei kleine Unterbrechungen durchzog), vorzog zu jeder seiner Folien Diskussionen zu zu lassen (Klar, dann wird auch nichts vergessen!), wurde auch trefflich über die Zweiteilung der Gesellschaft in digitale „Haves" und „Have-Nots" gestritten.
Leider war in dieser Frage keine Bewegung bei den DigSigel-Protagonisten zu verzeichnen. Das Problem ist einfach nicht existent. Argument: Da Anfang nächsten Jahres die Job-Karte in 40 Millionen-Auflage rauskomme (unklar blieb, wer das bezahlt!) würde die Frage nicht auftauchen!
Also werden 40 Millionen Deutsche gezwungen, sich eine oder mehrere 8stellige Pin zu merken. Wohlgemerkt, zusätzlich zu den schon jetzt vorhandenen Pin der Bank- und Kreditkarten, zusätzlich zu den jetzt schon eingesetzen Passwörtern für Raum-, Server-, Notebook- und PC-Zugänge!

Hier sei nun die Frage erlaubt, ob der Hinweis, dass man für alle Karten die selbe Pin nutzen kann, nicht an Beihilfe zum Betrug (oder wie immer Juristen das Delikt nennen mögen) grenzt?
Grund ist, dass bei Verlust aller Karten (z.B. gestohlene Brieftasche) und Nutzung des Geburtsdatums (aus dem Personalausweis; kann man am besten behalten) der Dieb nun mit allen Karten digital versiegeln kann -der Arme schon geschädigte Tropf kommt vom Regen in die Traufe: ALLE Siegelungen werden ihm gnadenlos zugeordnet!
Die digitalen Siegel sind 100 % sicher -Pech gehabt. Hätte der Arme nun nicht eine Pin für alle

Siegel gehabt, wäre er nicht so hoch geschädigt worden -wird der Richter sagen! Also: Zahlen!

Was aber mit denen, die keinen PC und keinen Internetzugang haben? Wird zusätzlich zur Jobkarte auch ein PC verschenkt? Oder ein Modem? Sind alle Tastaturen in den Unternehmen und Verwaltungen (wo dann die Nutzung Jobkarte ja dann vorgeschrieben sein wird) gegen ein Ausspähen der Pin bei der Eingabe geschützt?[3] So wie heute in jeder Tankstelle? Na denn. Aber die Gnade der u.a. Urteile ist nicht auf die DigSig übertragbar!! Klar, man kann die Karten sofor sperren lassen -wenn man den Diebstahl merkt. Die Kölner können ein Lied über Taschendiebe singen!

Statt einer Synthese wird hier ein Dissens deutlich sichtbar:
Kann der Staat 40 Millionen seiner Bürger dazu zwingen sich eine oder mehrere, möglichst komplizierte, 8stellige Pin zu merken? Die 4stellige der Bankkarte ist das Ergebnis eines Privatvertrages zwische der Bank und dem Kunden! Und man nutzt u.U. die Bankkarte wesentlich öfter -was der Merkfähigkeit dient. So die Harvard Universität in eine Studie.

Eine weitere Diskussion ergab sich aus der Frage, wie denn ein normaler Mensch entscheiden könne, welche der vier Versiegelungen er nun nutzen darf oder muss!
Zur Erinnerung, es gibt folgende Auswahl:

Einfache „Signatur"; Fortgeschrittene „Signatur"; Qualifizierte „Signatur" und die Qualifizierte „Signatur" mit Anbieterakkreditierung. Viel Spass!

Dass aber nicht alles so heiss gegessen wird, wie gekocht, zeigte ein Teilnehmer deutlich auf. Dem zu Folge sind auch echte digitale Signaturen der anderen Art lt. EU-Rrichtlinie zugelassen![4]

Die Vertreterin eines für Rationalisierung in der Verwaltung zuständigen Bundesamtes war mit Baltus der Ansicht, dass eine „Elektronische Blaupause" (Papier für den Bürger/Kunden, elektronisches Formular für die Verwaltung) eine gute Sache sei. Insbesondere im Bezug auf den unbedarften Bürger, der keine DigSig sein Eigen nennt, nicht damit umgehen kann oder will!

Diese wohl wichtigste Synthese war erst richtig zugänglich nachdem Baltus das „Vier-Stufen-Modell" erläuterte. Allerdings wurde diese Synthese nicht von den absoluten DigSig-Protagonisten getragen.

4. SigLab-Synthese:

Die „Elektronische Blaupause" in Verbindung mit den Verfahren digitaler Siegel erlaubt es, jeden Bürger digital Signieren zu lassen.

Das von Baltus vorgestellte Vier-Stufen-Modell:

1. **Der unbedarfte Bürger** besucht sein Bürgerbüro. Der Beamte ruft das elektronische Dokument auf und füllt es gemeinsam mit dem Bürger aus. Dann erfolgt lediglich **ein** papierener Ausdruck. Der Bürger liest das Dokument; ist er mit dem Inhalt einverstanden, legt er es auf einen Schrifterfasser und UNTERschreibt GLEICHZEITIG beide Dokumente -das Papierene sowohl wie auch das Eektronische. Die Verwaltung hat kein Papier mehr, der Bürger „sein" vor Gericht vorzeigbares Dokument! Die Daten der Unterschriftsdynamik sind mit Verfahren digitaler Siegel (Hash. Zeitstempel, Verschlüsselung) untrennbar mit dem Dokument verbunden. Ob hier ein Trust-Center den Zeitstempeldienst oder die Archivierung übernimmt, bleibt der Kreativität der jeweiligen Marketingabteilungen überlassen.

2. **Der etwas kundige Bürger** besucht sein Bürgerbüro und findet dort ein „Bürgerterminal“ vor. Dort ruft er das gewünschte Dokument auf und füllt es selbsttätig aus. Dann sendet er es einfach ab, das Intranet leitet es an den zuständigen Beamten. Dieser ruft den Bürger auf und bittet ihn zu sich. Der Beamte ergänzt das Formular und druckt es einmal aus. Rest: Siehe Oben. Hinweis: Das Bürgerterminal kann beispielsweise auch in einer Postfiliale oder wo auch immer stehen!

3. **Der kundigeBürger** ruft zu Hause an seinem PC über das Internet (oder eine Diskettte oder CD, nutzt er es öfters, hat er es sowieso gespeichert) das Formular auf, füllt es aus und sendet es an den zuständigen Beamten oder an die Verteilerstelle. Er erhält einen verbindlichen Termin (oder evt. Mehrere zur Auswahl?) Der Beamte ergänzt das Formular. Der Bürger erscheint zum Termin, bearbeitet das Formular gemeinsam mit dem Beamten. Dieser druckt es einmal aus. Rest siehe Oben.

4. **Der sehr kundige Bürger** ruft zu Hause an seinem PC über das Internet (oder eine Diskettte oder CD, nutzt er es öfters, hat er es gespeichert) das Formular auf, füllt es aus und sendet es nach SigG digital versiegelt oder digital unterschrieben an den Beamten, der bestätigt den Eingang (oder auch nicht?). Selbstredend kann der sehr kundige Bürger auch vor Ort oder an Bürgerterminals digital versiegeln oder unterschreiben. Wenn er mutig ist auch ohne Papierausdruck!

Mit dieser Vorgehensweise ist ausnahmslos **jeder** Bürger dazu in der Lage digital zu unterschreiben oder zu versiegeln (zur Not auch mit den berühmten Drei Kreuzen!). Der eine oder der andere merkt es nicht oder es ist ihm egal -wie bei einem Paketempfang. Dort wird ebenfalls digital signiert; allerdings forensisch nicht verwertbar.

Nur diese Vorgehensweise erlaubt den Verwaltungen, ein (nahezu) komplett papierloses Archiv zu installieren. Alle anderen Lösungen bedürfen immer zwei Archive: ein herkömmliches für die, die nicht digital unterschreiben oder versiegeln können oder wollen und das zweite für die, die digitale Siegel und Unterschriften leisten können.

Rückfluss der Investition

Das wichtigste aber ist der Rückfluss der Investitionen und der erfolgt schnellstens. Kostet ein Schrifterfasser komplett implementiert beispielsweise 250 € sparte er nach Aussagen des Organisationsleiters einer grossen rheinischen Sparkasse 500 € im Jahr!
Wo gibt es Systeme, die nach 6 Monaten anfangen richtig Geld zu verdienen?

In den vorbeschriebenen vier Stufen erkennt man sofort die wohl vom Gesetzgeber gewollte Abstufung der vier digitalen Siegel. (1. Einfache „Signatur“; 2. Fortgeschrittene „Signatur“; 3. Qualifizierte „Signatur“ und 4. die Qualifizierte „Signatur“ mit Anbieterakkreditierung.)
Warum die Dominanz der Trustcenter-basierten und Pin-gestützten digitalen Siegel propagiert und vehement gefördert werden, entzieht sich der herkömmlichen Meinungsbildung.

Massensiegelungen

Ein im Geschäft der digitalen Siegel tätigen Anwesender hatte eine Blackbox mitgebracht, die signaturkonform die Massensiegelung von Rechnungen nach EstG erlaubte.
Ein interessantes Thema, ohne Zweifel. Insbesondere wurde darauf hingewiesen, dass die Telekom damit auf einen Schlag Millionen Rechnungen versiegeln könnte. Wofür das auch immer das nutzen sollte.
Dem Bürger, der die Mehrwehrtsteuer (oder Umsatzsteuer) seiner Telefonrechnung nicht verrechnen mit seiner zu zahlenden Umsatzsteuer kann, ist es sowieso egal.

Dem Bürger oder Unternehmer, der das könnte aber seine Steuererklärung nicht digital einreichen kann, ist es auch egal.
Es ist auch dem Empfänger der Rechnung völlig egal, wer da nun die Pin eingetippt hat. Da kann sich ja das Finanzamt drum kümmern.
Lediglich ein paar Großunternehmen, die in der Lage sind ihre Steuererklärung voll digital erstellt und versiegelt ein zu reichen, wird das interessieren. Aber welche Unternehmen sind das?

Hier ist auch die Frage erlaubt, warum der Gesetzgeber (aussser zur Förderung digitaler Siegel) vorgeschrieben hat, dass digital erstellte Rechnungen auch digital versiegelt sein müssen.
Der angegeben Grund war, den Betrug mit dem Vorabzug der Mehrwertsteuer zu unterbinden. Eine gute Sache, kein Zweifel. Aber diese Betrugsmasche lohnt nur bei hohen Summen und im EXPORT!
Der Laie muss wissen, dass wenn die exportierte Ware die bundesrepublikanisch Grenze überschreitet, der Exporteur den Anteil der Mehrwert- oder Umsatzszteuer erstattet bekommt -auch wenn der Kunde im Ausland noch gar nichts gezahlt hat!
Der normale Bürger und der normale Unternehmer, der im Inland liefert, kann von dieser Möglichkeit eher selten Gebrauch machen.

Also werden wegen und gegen 100 oder 1000 Gesetzesbrecher nun alle Rechnungen versiegelt.
Besser und einfacher ist es dem Ratschlag von Steuerfachleuten zu folgen und den Erstattungsbetrag erst nach dem, nachgewiesenen (!), Eingang von Zahlungen des Auslandskunden zu leisten. Dem Gesetzestreuen entstehen dadurch keine Verluste, da er erst nach dem Eingang der Zahlungen seinen Anteil der Umsatzsteuer zahlen muss oder, exakt, verrechnen kann.
Es ist auch kaum vorstellbar, dass bekannte Großunternehmen wie VW, Porsche oder Thyssen oder andere dem Betrug mit der UST frönen.

Zusammenfassung:

Die Veranstaltung brachte keine Antworten für die kritischen Fragen zu digitalen Siegeln. Teilweise wurde das Verfahren der „Elektronischen Blaupause“ akzeptiert und als gangbarer Weg in die papierlose Verwaltung erkannt.
Allerdings konnten gemeinsan nutzbare Verfahren für digitale Siegel uznd digitale Unterschriften heraus gearbeitet werden. So zu sagen der oder die „kleinste(n) gemeinsame(n) Nenner“.

Ergänzend sei noch angemerkt:

Etwas wurde noch allgemein über die Biometrie diskutiert. Daher noch einige Hinweise.

Die drei Baltus Biometrik Axiome:

1. Die Biometrik wird die Welt nicht verbessern.
2. Es gibt kein alleinseligmachendes biometrisches Verfahren.
3. Es gibt aber intelligente und menschenwürdige Kombinationen.

Ein Ein-Seiten-Management-Papier zur elektronisch erfassten Unterschrift.

René Baltus, Auf den Steinen 7, 53125 Bonn. 0170/7766 480, 0228/257125, www.hesy.de 16.05.2002

Die eigenhändige Unterschrift –mehr als nur Biometrie!

In Zeiten vieler Diskussionen über Vor- und Nachteile biometrischer Verfahren wird die eigenhändige Unterschrift immer wieder in einem Topf mit herkömmlichen biometrischen Merkmalen geworfen. Eine Pauschalisierung, die dem feinen Verfahren der Unterschriftsleistung wohl kaum gerecht wird. Dies ist auch leicht belegbar:

Niemals gibt man die eigenhändige Unterschrift ungewollt ab!

Man kann sie nicht weitergeben! Nicht verlieren!

Die Schreibdynamik kann nicht ausgespäht oder gestohlen werden!

Die UNTERschrift **am Ende eines Dokumentes** ist unbestritten eine eindeutige Willenserklärung!

Sie ist, forensisch korrekte Erfassung der Schreibdynamik vorausgesetzt, unfälschbar![1]

Die Lebenderkennung ist automatisch im System enthalten!

Nur bei Bedarf oder auf Wunsch erfolgt sofort ein Vergleich oder Wiedererkennung![2]

Die Unterschrift kann als einziges biometrisches Merkmal GLEICHZEITIG auf Papier UND elektronisch geleistet werden! Letzteres ist dann eine „Elektronische Blaupause", die ebenfalls von einem Schriftsachverständigen verifizierbar ist –off-line! Die Schreibdrücke sind im Papier UND in der elektronischen Blaupause IDENTISCH![3]

Somit hat der Bürger/Kunde/Nutzer ein vor Gericht gültiges Beweisstück! „Sein" abheftbares Stück Papier –wie bisher! Er sieht, was er UNTERschreibt –und nur das gilt! Die Verwaltung erhält dafür ein Archivkosten sparendes Verfahren, das einen echten, medienbruchlosen Workflow generiert![4]

Damit sind auch die Dokumente derjenigen 50% der Bevölkerung digital und papierlos erfaß- und speicherbar, die NICHT elektronisch nach SiG versiegeln wollen oder können! Das Problem der „digitalen Underdogs" oder „digitalen Nothaves" wird damit obsolet!

Eigenhändig geschriebene PIN oder Paßwörter sind beliebig oft wechsel- und notierbar!

Das Feld zur Schrifteingabe erlaubt die Eingabe einer PIN! Wie bisher mit Erkennung der eingegeben Zahl –oder mit Erkennung der Zahl UND der Tippdynamik des Eingebenden![5]

Dies ist dann ein mehrfach genutztes System, das die Wiedererkennungs- und Abweisungsraten deutlich verbessert![6]

Für hohe Sicherheitsansprüche stehen dann je nach Anforderung zusammen oder in beliebiger Kombination zur Verfügung: Besitz (Chipkarte), Wissen (herkömmliche PIN), Biometrie 1 (Tippdynamik der PIN), Biometrie 2 (Schreibdynamik von PIN oder Passwort), Biometrie 3 (Unterschriftsdynamik).[7]

Die Datenmenge ist so gering, daß sie bequem auf eine Chipkarte paßt.[8]

Als biometrischer Zufallsgenerator wird gleichzeitig mit der Schrifteingabe aus der Schreibdynamik eine biometrische Zufallszahl ermittelt![9]

Der Nutzer wird das Pad auch als Mausersatz zur Cursorsteuerung einsetzen -und das funktioniert immer, auch bei hohen Temperaturen oder hoher Luftfeuchtigkeit.[10]

[1] Die Unterschrift ist in ihrer Faksimile nachahmbar, jedoch NIE fälschbar! So das BKA! Mit HESY werden 1046 Druckwerte/sec erfaßt; zusätzlich die Schreibzeit und die -pausen! Siehe die Expertise in www.hesy.de, und den Vortrag vor dem EDV-Gerichtstag 1999, dort die Auszüge aus dem Buch „Forensische Handschriftenerkennung" von Dr. M. Hecker.

[2] Wer wird bei einer Paketannahme on-line wiedererkannt? Keiner! Erst, wenn die Annahme bestritten wird erfolgt eine off-line-Verifizierung durch einen Schriftsachverständigen –wenn er denn überhaupt eine dort erfaßte Faksimile begutachtet! Das Bundes-kriminalamt lehnt dies ab. Es fehlt der Druck des Stiftes im Papier, also die mit hohen Datenmengen erfaßte Schreibdynamik!

[3] Keiner der Beteiligten kann nachträglich das in seinem Besitz befindliche Dokument ändern! Schon gar nicht, wenn ZWEI Unterschriften getätigt wurden! Die des Bürgers und des Beamten oder des Kunden und des Verkäufers!

[4] In dem auch später digital nach SiG versiegelte Dokumente gespeichert werden! EIN digitales Archiv ist dann zukünftig ALLEN Aufgaben gewachsen!

[5] Daher erhielt das Pad die Bezeichnung: „Analoge Tastatur"!

[6] Ein sogenanntes „Multimodales System"! Allerdings ist fraglich ob 100 % der Bevölkerung wiedererkannt werden kann. Nach Gauß praktisch nicht! Mit HESY wohl aber 95 % -es fehlen lediglich die, die nicht schreiben UND sich keine PIN merken können oder überhaupt die Segnungen des Computerzeitalters nicht in Anspruch nehmen wollen. Der Rest wird wohl keinen Bedarf haben!

[7] Für digitale Siegel nach SiG genügen „Besitz und Wissen" oder „Besitz und ein oder mehrere biometrisches Merkmale"! Mit der Unterschrift werden elektronische Siegel dann zu echten digitalen Unterschriften oder elektronischen Signaturen!

[8] 1 kb sollte reichen, es gibt aber Chips, die bis zu 32 kb Daten speichern können.

[9] Für elektronische Siegel nach SiG unverzichtbar! Siehe hierzu die Darstellung der Schreibdynamik in der HESY-Expertise in www.hesy.de, dort Seite 12. Da jede Unterschrift ein Unikat mit etwas abweichenden Druck- und Zeitverläufen ist, kann mittels eines Koordinatennetzes immer eine andere Abfolge von Druck-Nichtdruck abgegriffen werden. Diese stellen sich dann als I und 0-Folge dar.

[10] Analog zum Druck auf das Pad wird der Cursor schneller oder langsamer –wie man es von vielen anderen Dingen gewohnt ist.

---

1 Persönliche Daten siehe: http://www.hesy.de/Broschuere_4c_4s_6_E2.pdf

2 Die Zeitschrift Computer-Fachwissen des Bund-Verlages: So kann, wer sich einen Schlüssel illegal beschafft hat, Unterschriften beliebig fälschen. Zudem können die Dokumente manipuliert werden. Ein Mitarbeiter kann andere Dokumente, als diejenigen, die ihm auf dem Bildschirm angezeigt werden, untergeschoben bekommen. Die signiert er dann ahnunglos --mit allen rechtlichen Folgen. Quelle: http://www.zeit.de/2001/23/Hochschule/jl02.html

3 **Diebstahl der EC-Karte PIN ausgespäht**

Wer die ec-Karte verliert, zahlt den Schaden, wenn der Dieb das Konto plündert. Denn die Gerichte gehen in der Regel davon aus, dass man fahrlässig die PIN-Nummer zusammen mit der ec-Karte verwahrte. Doch nun hatte ein

Bankkunde Glück, der darlegen konnte, dass seine PIN eventuell ausgespäht wurde: Er habe regelmäßig auf dem Weg zur Arbeit an derselben Filiale zum Geldabheben angehalten. Da außerdem die Abschirmvorrichtungen am Automaten minimal waren, liege ein Ausspähen im Bereich des Wahrscheinlichen. Es könne durchaus sein, dass der Kontoinhaber bei diesen Abhebungen, die meist zur selben Zeit stattfanden, vom Täter bei der PIN-Eingabe beobachtet und danach gezielt bestohlen worden sei, gab ihm das Landgericht Berlin Recht (Az: 51 S 292/98).

Urteile ec-Karten-Diebstahl

Hat ein Dieb einen Einbruch verübt und daraufhin mit der gestohlenen ec-Karte Geld abgehoben, lässt sich allein daraus noch nicht schließen, dass die Karte gemeinsam mit der Pin gelagert wurde (Oberlandesgericht [OLG] Oldenburg, Az. 9 U 23/00).

4Unterschreiben Sie Ihre MS-WORD oder PDF-Dokumente über ein Signature Pad (Schreibtablett) oder Tablet PC und Sie erhalten eine elektronische Signatur, die hinsichtlich Sicherheit ihresgleichen sucht. Die vom Signaturdienst erstellten elektronischen Signaturen erfüllen alle die im Artikel 2 Abs.2 der für sämtliche EU-Staaten verbindlichen EU-Direktive definierten Anforderungen für fortgeschrittene elektronischen Signaturen.

Quelle: http://www.signature-perfect.com/german/index_de.html