Die moderne Interpretation der persönlichen Identifikation mit der eigenhändigen Unterschrift:

Die Willenserklärung von Cleopatra bis zur „Digitalen Signatur“

Vollständige Ausgabe
Februar 2009

Autor: René Baltus

Printed in Germany
ISBN 978-3-00-027268-4

René Baltus

Biometrie in beeindruckender Vielfalt:

Die Sensortechnologie Sign and Type

BVP GmbH, Bonn

Inhaltsverzeichnis

René Baltus über Biometrie und Sign-n-Type

Gestatten – René Baltus, BVP GmbH!

René Baltus, geboren 1946 in Kolumbien, belgischer Staatsangehöriger, lebt seit 1956 in Deutschland.

Er ist Meister des Elektrohandwerks, Betriebswirt des Handwerks, Strahlenschutzfachkraft, Qualitätsmanager TÜV-Cert.

Seine umfassenden beruflichen Erfahrungen und seine Vielseitigkeit konnte er seit Beginn seiner Lehre als Elektroinstallateur 1960 erwerben. Er war in den verschiedensten Bereichen tätig. Dazu gehören u.a. Arbeiten im Schaltschrank- und Verteilerbau, im Braunkohletagebau, internationale Montage von induktiven Schmelzöfen für Metalle aller Art, Hochstromanlagen für Galvanik, Maschinen und Anlagen zur Kunststoffverarbeitung, Elektroinstallationen in kerntechnischen Anlagen.

Längere Zeit war er als angestellter und freier Produktentwickler tätig, davon zeugen z.B. zwei Weltpatente für mechanische Parkhäuser. Zu seinen Erfindungen gehören u.a. eine Angärkontrolle für obergäriges Bier, Kunststoffschweißgeräte, lineare Membranpumpen, ein preiswerter Kälte- und Nässeschutz, ein „intelligenter“ Autositz, eine messende Plattform für Roboter, Mobiltelefone, abschaltbarer Türschließer für Innenräume, Be- und Entgasung von Flüssigkeiten, Wägesysteme. 30 Patente oder Patentanmeldungen behandeln alleine das Gebiet der Biometrie mit der Erfassung und Erkennung der Schrift, der PIN und des Fingerabdruckes sowie der dazu gehörenden Technologien.

Als Autor zahlreicher Artikel und als Vortragender auf vielen Biometrie-Veranstaltungen konnte er ebenfalls viel Erfahrung im Bereich der Kommunikation erwerben. Als Pionier in der Online-Wiedererkennung von Personen anhand der eigenhändigen Unterschrift war René Baltus maßgeblich daran beteiligt, biometrische Verfahren in die Verordnung und den Maßnahmekatalog zur Digitalen Signatur einzubringen.

Als Zwischenschritt bis zur flächendeckenden Einführung digitaler Signaturen für 100% der Bürger hat René Baltus vorgeschlagen, die „elektronische Blaupause“ zu nutzen. Bei diesem „Crossover-Media“ wird gleichzeitig ein Papierdokument (für den Bürger/Kunden) und ein zur elektronischen Archivierung geeignetes elektronisches Dokument forensisch korrekt eigenhändig unterschrieben.

René Baltus ist Geschäftsführer der **BVP Gesellschaft für Beratung, Verfahren, Produkte mit beschränkter Haftung**. Die BVP GmbH ist in 53125 Bonn, Auf den Steinen 7 ansässig, Tel. (0228) 257125 und (0170) 7766480.

www.sign-n-type.com

Im Jahr 1998 erhielt **René Baltus** für sein **H**andschriften-**E**rkennungs-**Sy**stem **HESY** den Innovationspreis

Fraunhofer Award Office 21

des Fraunhofer Instituts für Arbeitswirtschaft und Organisation (IAO), Stuttgart.

http://www.iao.fraunhofer.de/

Im Jahr 1999 folgte dann der

Multimedia-Gründerpreis

des Bundeswirtschaftsministeriums.

Hierzu Auszüge aus dem Bericht
Buhlen um Nachwuchs und Ideen
von Christiane Schulzki-Haddouti
in *Telepolis*, Heise Verlag, 21.04.1999
www.heise.de/tp/r4/artikel/2/2774/1.html

„Unter den zwanzig besten Gründungsideen finden sich Konzepte zur „interaktiven Marktforschung über das Internet“, „Kompressionstechnologien zur kostensparenden Übertragung von Java-Applets im Netz“ bis hin zum Handschriften-Erkennungssystem für Normalstifte, das eine direkte Verknüpfung der herkömmlichen Unterschrift mit der digitalen Signatur ermöglicht. Das Hesy-Verfahren erlaubt es, digitale Dokumente eigenhändig zu unterschreiben. Hierzu wird die mit nahezu jedem herkömmlichen Stift geleistete Schriftprobe vierdimensional in Länge, Breite, Schreibdruck und Schreibzeit auf einem Pad individuell erfaßt, digitalisiert und in das Dokument eingebunden. Der 53-jährige Erfinder René Baltus legte den ehrgeizigsten Businessplan aller Gründer vor: Er will mit Hilfe von Venture Capital eine Fertigung mit 40 Mitarbeitern aufbauen und peilt einen jährlichen Umsatz von 20 Millionen an.“

Inzwischen ist der HESY-Nachfolger **Sign and Type** marktreif.

Der FTK e.V. in Dortmund (www.ftk.de/pages/ftk.html) hat unter der Federführung von Frau Lena Weigelin das multimodale Sign-n-Type für den **NRW-Gemeinschaftsstand** auf der **CeBIT** in Halle 6 ausgewählt. Dann wurde die Auswahl mit Hilfe des Horst Görtz Institut für IT-Sicherheit an der Ruhr-Universität Bochum (www.hgi.rub.de/hgi/news/), dort Frau Verena Hintzmann und Herr Dr. Christopher Wolf, in „trockene Tücher“ gepackt – hierfür herzlichen Dank.

Ihr René Baltus

http://www.cebit.nrw.de/wirtschaft/01_BVP.html

Sign and Type

Vielfalt statt Einfalt – mit einer einzigen Sensortechnologie!

1. **Fälschungsresistente Unterschriftserfassung**
   mit 1600 Dynamikwerten/sec.
2. **Erfassung der Tippdynamik**
   mit 1600 Dynamikwerten/sec.
3. **Erkennung der PIN-Ziffern**
   mit Fuzzylogik
4. **Analoge Cursorsteuerung**
   wie Gasgeben beim Auto
5. **Physikalische Pad-Identifikation**
   mit 3D-Barcode
6. **B-R-Gen(i)e – Biometric Random Generator**
   Biometrischer Zufallsgenerator
7. **E-LTW – Electronic Learn-To-Write**
   Schreibenlernen von Buchstaben, Zahlen und Schriftzeichen
8. **GESY – Biometric Gangway**
   Erfassung der Gangdynamik = verzugslose Biometrie
9. **Fingerprintdynamic**
   Erfassung der Dynamik bei der Abgabe eines Fingerabdruckes
10. **3D-ErgoMouse**
    Ergonomisch korrekte 3D-Computermaus
11. **3D-Joystick**
    Der Joystick, der ALLE Bewegungsrichtungen erfassen kann
12. **Robodyn**
    Erfassung der Bewegungsdynamik von RoboDoc und Montageroboter
13. **Seatdyn**
    Erfassung der Bewegungen eines Fahrzeugsitzes zur Optimierung der Airbagauslösung
14. **Anemodyn**
    Erfassung von Windgeschwindigkeit und -richtung ohne bewegliche Teile

Die Sensortechnologie

HESY und **Sign and Type** (oder amerikanisiert **Sign-n-Type**) sind zwei Verfahren bzw. Geräte, die der Erfassung der Schreibdynamik bei der Leistung einer eigenhändigen Unterschrift sowie der Erfassung der Tippdynamik bei der Eingabe einer PIN (Personen-Identifikations-Nummer) dienen. Sie unterscheiden sich lediglich in der Gestaltung der Elektronik; in der Anwendung ist kein Unterschied zu bemerken.

HESY

Sign and Type

HESY ist die 15 Jahre „alte“, aber immer noch erstklassig funktionierende Version, die mit so genannten Wägezellen arbeitet. Sign and Type ist nun sechs Jahre jung und nutzt schnelle, moderne, energiesparende, mit Leuchtdioden und Fototransistor arbeitende Reflexionslichtschranken.

Die Grundidee beider Verfahren zur Erfassung der Schreib- und Tippdynamik ist dieselbe: Man lagere, wie bei HESY, eine Schreib- oder Druckplatte auf vier Wägezellen und messe deren Auslenkung, wenn die Wägezellen vom Schreib- oder Tippdruck mehr oder weniger „verbogen“ werden. Nun gibt es in der Wägetechnologie eine für den Laien babylonisch verwirrende Vielzahl von Begriffen, die sich mit Wägezellen und deren Verwandten befassen.

Eine Wägezelle besteht im Grunde genommen aus einer Flachfeder, auf der ein Dehnungsmessstreifen aufgeklebt ist. Der Dehnungsmessstreifen ist eine auf flexiblen Isolierstoff aufgebrachte lange und hauchdünne Bahn aus leitendem Material. Nun ist es bei diesen Materialien so, dass sie ihren elektrischen Widerstand ändern, wenn sie bei der Verbiegung der Feder gestreckt oder gestaucht werden. Diesen Effekt nutzt auch HESY, wenn der Schreib- oder Tippdruck die Wägezelle verbiegt.

Ganz anders funktioniert das Sign-n-Type-Verfahren. Bei Sign-n-Type lagert die Schreib- oder Druckplatte (dies kann z. B. auch ein Display sein) auf vier Federn. In einigem Abstand zur Platte sind Reflexlichtschranken montiert. Beim Schreiben oder Tippen geben die Federn entsprechend dem Schreib- oder Tippdruck etwas nach und verändern somit den Abstand der Platte zu den Reflexlichtschranken. Entsprechend dem Abstand verändert sich die Intensität des von der Leuchtdiode ausgesendeten Lichtes, diese Änderungen werden gemessen und ausgewertet. Das erfolgt hier wie bei HESY hochauflösend mit mindestens 1600 Werten/sec. und mit einer Genauigkeit von einem Tausendstel Millimeter.

Die Gebrauchsmusteranmeldung zu HESY erfolgte am 13.03.1993; die EP-Anmeldung am 11.03.1993 mit einer Förderung in Höhe von 25.000,00 DM durch die Patent- und Innovationsagentur NRW, „PINA“. Sign-n-Type ist mit dem europäischen Patent Nr. EP 01442421B1 geschützt.

Die Anwendungsbereiche

1. Fälschungsresistente Unterschriftserfassung

Im Gegensatz zu anderen biometrischen Erfassungsmethoden wie Iris-Scan oder dem eher leicht zu fälschenden Fingerabdruck besitzt die Unterschrift als freie Willenserklärung einer lebenden Person absolute Rechtsverbindlichkeit. Die digitale Signatur sollte mit einem oder mehreren biometrischen Merkmalen abgeschlossen werden (§ 15 SigV).

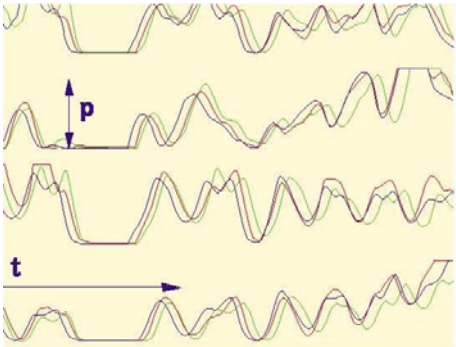
Eine Handschrift zu fälschen ist leicht – die individuelle Art des Aufsetzens, Pausierens und der Druckstärke eines Unterschrift-Leistenden zu imitieren hingegen unmöglich.

Legt man ein Dokument beim Unterschreiben auf die Sign and Type-Unit, erzeugt man auf diese Weise zugleich eine elektronische Blau-pause. Die Oberfläche registriert mit bisher ungeschlagenen und steigerungsfähigen 1600 Werten/sec. die individuelle Schreibdynamik des Schreibers und gleicht sie mit einem zuvor gespeicherten Datensatz ab. Der wohl beste Wettbewerber redet von lediglich 400 Werten/sec.

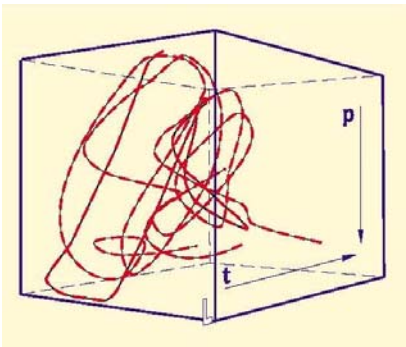
Vergleichbare Erfindungen verlangen nach teuren Spezialstiften – für Sign-n-Type ist kein teures Zubehör nötig: Das Pad kann mit jedem herkömmlichen Stift beschrieben werden.

Anwendung:

- „Elektronische Blaupause“ mit Papierdokument für Bürger und Kunde sowie einem rein elektronischen und preiswert zu archivierenden Dokument für die Verwaltungen.
- Elektronische Unterschriften unter CAD-Dokumenten, z.B. realisiert in CATIA V5.
- Alle Zugangskontrollen wie Bankautomaten, Räume, Tresore, Pilotenkanzeln, Firmen und Wohnhäuser, Waffen- und Munitionsübergaben etc.
- Arztpraxen, Apotheken



Druck- und Zeitverläufe von drei Unterschriften oben Sensor 1 bis unten Sensor 4
p = Schreibdruckhöhe
t = Schreibzeit mit Pausen



Ansicht der Druckverläufe 45° seitlich von links

2. Erfassung der Tippdynamik

Auf der Sign and Type-Unit ist ein Zahlenfeld aufgebracht, so dass die Unterschrift zusätzlich durch die Eingabe einer PIN abgesichert werden kann – die modernste Art, eine PIN fälschungssicher und resistent gegen ein Ausspähen einzugeben. Ausspähen mittels Kamera zwecklos, da die Tippdynamik nicht optisch zu erfassen ist. Damit dürfte die PIN wieder aus dem negativen Fokus der Verbraucherschützer und der IT-Sicherheitsfachleute verschwinden. Auch hier ist, wie bei der Unterschrift, eine wertabhängige Erkennungsschärfe einstellbar.

Anwendung:

- Alle Zugangskontrollen wie Bankautomaten, Räume, Tresore, Pilotenkanzeln, Firmen und Wohnhäuser etc.

3. Erkennung der PIN-Ziffern

In Konformität mit der Verordnung und dem Maßnahmekatalog zur „Digitalen Signatur“ erfolgt hier die Erkennung der PIN-Ziffern mittels einer Fuzzylogik. Die Identifizierung des Signaturschlüsselinhabers erfolgt mit Besitz (Smart-Card) und Wissen (PIN) oder mit Besitz und einem oder mehreren biometrischen Merkmalen (hier Tipp- und Schreibdynamik) mit nur einem Sensor. Dem Vernehmen nach hat dies bisher noch kein Wettbewerber in der Qualität erreicht. Nun behaupten einige Wettbewerber, dass 400 Werte/sec. ausreichen. Das mag vielleicht stimmen; ein VW-Käfer kam ja auch mit 34 PS aus – aber wer fährt schon heute noch Käfer? Ob 400 Werte/sec. für die Erkennung der Tippdynamik ausreichen (wenn sie es denn könnten), dürfte mehr als fraglich sein.

Anwendung:

- Alle Zugangskontrollen wie Bankautomaten, Räume, Tresore, Pilotenkanzeln, Firmen und Wohnhäuser etc.
- Für Kinder lassen sich statt Zahlen auch Comicfiguren, Puppen, Bären, Autos, Bälle etc. auf das Pad aufbringen.

4. Analoge Cursorsteuerung

Das Pad eignet sich ferner ausgezeichnet zur Steuerung des Cursors. Bisher erfolgt dieses ebenfalls mit ähnlichen Pads, die aber wohl nicht so richtig funktionieren; immer wieder hört man von verärgerten Notebook-Besitzern, die, besonders im Sommer, Ärger mit diesen Pads haben sollen. Des Weiteren erlauben diese Pads keine analoge Eingabe oder Nutzung. Analog bedeutet hier, dass mit der SAT-Unit die Funktionen völlig neuartig je nach Druckstärke langsam oder schneller ablaufen – wie im Auto beim Gasgeben.

Anwendung:

- Als integrierter Zusatz zur Schreib- und Tippdynamik bei allen Computerpads und in Notebooks.

5. Physikalische Pad-Identifikation

Ein verblüffend einfaches Verfahren, um jedes einzelne Pad physikalisch zu erkennen und damit die Sicherheit zu erhöhen. Hierzu wird auf der Schreibfläche jeweils ein einmaliger 3D-Barcode aufgebracht. Beim Schreiben „steigt" oder „fällt" der Stift durch die individuell unterschiedlichen „Berge" und „Täler" des Barcodes. Diese „Einbrüche" sind deutlich im Messprotokoll zu sehen und zu erkennen; damit ist dann auch das Pad zweifelsfrei identifizierbar.

Anwendung:

- Hochsicherheit und kundenspezifische Pads

6. B-R-Gen(i)e – Biometric Random Generator

Ein vielfach diskutiertes Problem der „Digitalen Signatur" ist die Erzeugung der erforderlichen Zufallszahl. Die mit der SAT-Unit erzeugbare Zufallszahl ist die erste und wohl einzige biometrische Zufallszahl. Sie wird bei der Abgabe einer Unterschrift generiert, indem die immer unterschiedlichen Verläufe der Schreibdynamik punktuell abgegriffen werden. Es entsteht eine zufällige Folge von „0" und „1", die zusammengefasst eine Zufallszahl ergeben.

Anwendung:

- Zufallsgenerator für die Digitale Signatur u.ä. Anwendungen.

7. E-LTW – Electronic Learn-To-Write

Kinder, und damit auch die Eltern, lernen stressfrei und ohne Maßregelung das Schreiben einzelner Buchstaben und Zahlen. Hierzu werden die Schreibversuche beispielsweise von Comicfiguren bewertet: Ungehalten bis zornig, wenn die Eingabe nicht so gut ist, bei Verbesserung dann lächelnd oder schnatternd. Einzelne Worte und kleine Rechenaufgaben werden ebenfalls eingegeben und mehr oder weniger „wiedererkannt".

Für Erwachsene, die chinesische (oder arabische) Zeichen oder umgekehrt lateinische Buchstaben lernen wollen, erfolgt das Feedback durch eine durch Balkencode gezeigte Prozentangabe der erreichten Genauigkeit.

Der Vorteil für alle ist, dass das Schreibenlernen ohne zwingende Anwesenheit von Eltern oder Lehrern erfolgen kann. Die gespeicherten Daten der

Versuche werden zur Kritik und Korrektur durch Lehrer oder Eltern abgerufen. Dies alles kann natürlich auch online erfolgen! So kann ein Lehrer von China aus online die Erfolge des Schülers weltweit einsehen und korrigieren.

Anwendung:

- Schreibenlernen für Kinder und Erwachsene, zu Hause und unterwegs.

8. GESY – Biometric Gangway

Das einzige verzugslos arbeitende biometrische Verfahren dürfte das Gangerkennungssystem GESY sein. Hierzu schreitet z.B. ein Vielflieger oder ein Firmenangehöriger über ein überdimensioniertes HESY (ca. 1m x 3m). Die individuelle Gangdynamik wird erfasst und mit einem vorhandenen Datensatz verglichen.

Da die Biometric Gangway sehr flach und leicht ist, ist sie bequem zu transportieren und platzsparend zu verstauen. Wer in den USA die raumfüllenden Geräte zur Erfassung der Gesichter gesehen hat, weiß wovon die Rede ist.

Alle biometrischen Verfahren, ob Unterschrift, Tippdynamik, Fingerprint, Gesichts-, Iris- oder Handflächen-Scan erfordern immer etwas Zeit zur Eingabe der Daten. Der Proband muss stehen bleiben und sein biometrisches Merkmal abgeben. Bei der Ankunft eines Jumbojets mit 50% Vielfliegern bilden sich unweigerlich lange Warteschlangen. Mit GESY ist das vermeidbar!

Anwendung:

- Zugang zu Pilotenkanzeln, Firmen, Tresoren, Hochsicherheitstrakten, Kernkraftwerken (dort erscheinen bei den jährlichen Revisionen bis zu tausend Fremdmonteure und verlangen schnellen Einlass!)
- Vielfliegererkennung etc.

9. Fingerprintdynamic

Einige Nachteile der herkömmlichen Erfassung eines Fingerabdruckes sind

- die fehlende Lebenderkennung (bei preiswerten Geräten)
- die unvermeidliche „freiwillige“ Abgabe an vielen Orten (Bierglas, Kopierer etc.)
- die angebliche (lt. Heise Online-Verlag) Fälschbarkeit mittels dünnen Silikonfolien oder sogar durch auf dünnen Kunststofffolien vom Bierglas kopierte Abdrücke

- die immer wieder unterschiedliche Druckstärke bei der Abgabe
- falsche Ablehnungen durch kleine Verletzungen oder Abrieb der Haut (Bauarbeiter, Handwerker, Putzhilfen, Hobbyhandwerker)
- die relativ leichte Erzwingbarkeit.

Die neuartige Kombination eines dynamischen biometrischen Merkmals (Dynamik der Abgabe eines Fingerabdruckes) mit einem statischen Merkmal (Finger- oder Handabdruck) erhöht die Nutzbarkeit des Fingerabdrucks. Die Erfassung und Auswertung der personentypischen Druckdynamik erhöht die Wiedererkennungsrate und unterbindet nahezu vollständig die Nutzung von Fälschungen jeder Art.

Hierzu wird ein Fingerprint-Erfasser (auch nachträglich) auf eine kleine SAT-Unit aufgebracht. Bei Erreichen des „richtigen" Druckes erfolgt blitzartig die Erfassung des Fingerabdruckes – somit immer bei demselben Druck! Des Weiteren wird während des gesamten Ablaufes die personentypische Druckdynamik erfasst.

Damit ist Sign and Type der zweite Sensor, der mit zwei Verfahren, jedoch nur auf einer einzigen Fläche, zwei biometrische Merkmale erfasst.

Anwendung:

- Alle Fingerabdruck-Sensoren.

10. 3D-ErgoMouse

Stellt man sich locker hin und winkelt den Unterarm nach oben ab, so erkennt man sofort, wie die Hand bestens zur Bedienung eines Joysticks gerichtet ist. Zur Bedienung einer herkömmlichen Computermaus muss die Hand jedoch zusätzlich gedreht werden. Laut dem schwedischen Hersteller einer ergonomisch korrekten Maus soll dies zur frühzeitigen Ermüdung bis hin zu schmerzhaften Erkrankungen des Bewegungsapparates führen.

Bei der Bedienung der 3D-ErgoMouse befindet sich die Hand in einer ergonomisch guten Stellung, der Arm liegt bequem auf. Weiterhin stehen zwei Steuerachsen mehr als üblich zur Verfügung, ebenso wie der analoge Ablauf der Bewegungen des Cursors.

Anwendung:

Jeder Computernutzer, der eine Maus benötigt.

11. 3D-Joystick

Besonders sei hier auf die möglichen Bewegungen nach oben und unten hingewiesen. Bei Spielen kann (wie in realitas schon geschehen) der Hubschrauber oder das U-Boot direkt nach oben oder unten gelenkt werden. Für neuartige Spiele ein einfaches und preiswertes Produkt.

Die „echten" Joysticks in der Luftfahrt sind sehr teuer (beim Airbus angeblich 20.000 €), groß und schwer. Der 3D-Joystick dagegen kann sehr einfach redundant, klein und leicht gefertigt werden.

Anwendung:

- Spiele, Luftfahrt, Krananlagen

12. Robodyn

Stellt man einen Handhabungsautomaten (so die offizielle Bezeichnung für Roboter) auf eine große SAT-Unit, detektiert diese jede kleinste Bewegungs- und Kraftänderung. Stößt der Roboter gegen einen Gegenstand, weicht er von seiner vorgegebenen „Laufbahn" ab oder entstehen unerlaubte Schwingungen (beim RoboDoc), so kann die Steuerung dies erkennen und entsprechende Maßnahmen, z.B. eine Notabschaltung, veranlassen.

Anwendung:

- Robotik, RoboDoc (Chirurgie-Roboter)

13. Seatdyn

Wird ein Autositz auf vier SAT-Unit-Sensoren gestellt, erkennen diese bei Unfällen sofort, wie stark und aus welchen Richtungen die unkontrollierten Kräfte auf den Fahrer einwirken. Mit diesen Werten ist eine intelligente Auslösung der Airbags durchführbar.

Anwendung:

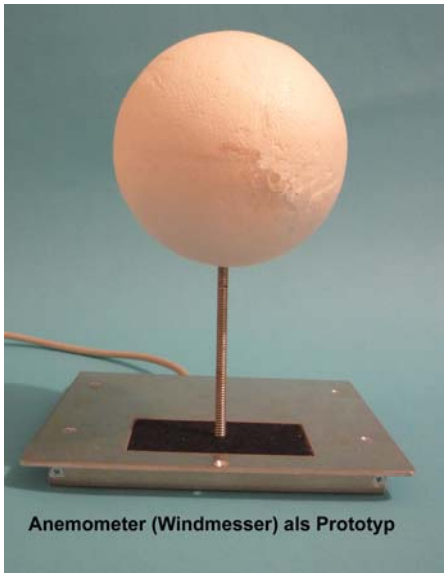
- Automotive

14. Anemodyn

Anemometer sind Geräte, die Richtung und Geschwindigkeit von Luftströmungen erfassen. Die bekanntesten sind die so genannten Halbschalen-Anemometer: Drei oder vier kleine, hohle Halbkugeln drehen sich entsprechend der Windgeschwindigkeit schneller oder langsamer; die Richtung der Luftströmung wird mit einer pfeilähnlichen, der Windrichtung folgenden Fahne (Windrichtungsgeber) erfasst.

Nachteilig ist, dass hierfür zwei Systeme erforderlich sind und dass bewegliche Teile zur Anwendung kommen. Werden Fall- und Steigewinde gemessen, sind diese Verfahren überfordert. Ferner sind sie nicht gerade preiswert, schon gar nicht, wenn die Fall- und Steigewinde gemessen werden sollen – dann kann ein Gerät leicht € 5.000,00 kosten.

Das Anemodyn besitzt dieselbe Technologie wie die Sign and Type-Unit. In die Oberfläche der SAT-Unit wird ein Gewinde eingebracht, in das ein Federstab eingeschraubt wird. Auf dem Federstab ist eine leichte Kunststoffkugel montiert. Diese Kugel neigt sich beim leisesten Anblasen, aus welcher Richtung auch immer, und kehrt bei Ausbleiben des „Windes“ wieder in ihre Ursprungslage zurück.



Anemometer (Windmesser) als Prototyp

Die Neigung und damit die Winddynamik werden erfasst und ausgewertet; nicht anders als beim 3D-Joystick.

Damit sind mit nur einem Sensor alle Windgeschwindigkeiten und Windrichtungen erfassbar – auch Steige- und Fallwinde.

Anwendung:

- Wetterstationen, auch preiswerte Hobby-Wetterstationen (siehe z.B. Conrad Elektronik)
- Überwachen von Abschattungen von Wintergärten und Gebäuden
- preiswerte Messung der Seiten- oder Scherwinde an Start- und Landebahnen mit vielen Messpunkten
- Preiswerte und dadurch vielfache Messungen von Steige- und Fallwinden an Flugplätzen, Brücken etc.

Die eigenhändige Unterschrift – mehr als nur Biometrie!

In Zeiten vieler Diskussionen über Vor- und Nachteile biometrischer Verfahren wird die eigenhändige Unterschrift immer wieder in einen 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 eine 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 – offline. 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 zu erfassen und zu speichern, die NICHT elektronisch nach SiG versiegeln wollen oder können. Das Problem der „digitalen Underdogs“ oder „digitalen Not-Haves“ wird damit obsolet.
- Eigenhändig geschriebene PIN oder Passwörter sind beliebig oft zu wechseln und zu notieren.
- 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 ihrem Faksimile nachahmbar, jedoch NIE fälschbar, so das BKA. Mit HESY werden 1600 Druckwerte/sec. erfasst; zusätzlich die Schreibzeit und die –pausen.

[2] Wer wird bei einer Paketannahme online wiedererkannt? Niemand! Erst wenn die Annahme bestritten wird, erfolgt eine offline-Verifizierung durch einen Schriftsachverständigen – wenn er denn überhaupt ein dort erfasstes Faksimile begutachtet. Das BKA 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 bzw. 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 können; 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.

[7] Für digitale Siegel nach SiG genügen „Besitz und Wissen" oder „Besitz und ein oder mehrere biometrische 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. 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 1 und 0-Folge dar.

[10] Analog zum Druck auf das Pad wird der Cursor schneller oder langsamer.

Online nachzulesen unter
www.sign-n-type.com/MehralsBiometrie_DE.pdf

Your own signature – more than just biometry!

In these times when there are numerous discussions of the advantages and disadvantages of biometric procedures, the question of using one's own signature always crops up at the same time as conventional biometric procedures are mentioned. This is a huge over-generalization, which is hardly appropriate for the refined procedures involving signatures. This is also easy to prove:

- Nobody gives out his or her own signature unintentionally.
- You cannot pass it on to somebody else. Nor can you lose it.
- The dynamics of your writing cannot be "sniffed out" or stolen.
- The signature at the end of a document is beyond any doubt a clear and explicit statement of intent.
- Given a forensically correct reading of the dynamics of your writing, a signature cannot be forged.[1]
- The system automatically detects whether the signatory is alive.
- A comparison or recognition is only done immediately as required or as wished.[2]
- A signature is the sole biometric characteristic that can be produced SIMULTANEOUSLY on paper AND electronically. The latter becomes an "electronic blueprint", which can likewise be verified by a handwriting expert – offline. The writing pressures are IDENTICAL on paper AND in the electronic blueprint.[3]
- The citizen/customer/user has a valid piece of evidence that can be presented in a court of law. "His" (or her) piece of paper that can be filed – as before. He can see what he has signed – and that is all that matters! On the other hand, the various forms of administration are given a procedure that saves on archiving costs, one that generates a genuine work flow that is not broken by different types of media.[4]
- Thus it is also possible to record and store documents in digital and paperless form from the 50% of the population that does NOT WANT or is NOT ABLE to use an electronic seal as per SiG. This immediately renders obsolete the whole matter of "digital underdogs" or "digital have nots".
- A PIN or a password written by hand can be noted and changed as often as wished.
- The field for handwriting input also allows a PIN to be entered. As before, with recognition of the number that was input – with recognition of the number AND of the typing dynamics of the person making the entry.[5]
- This then becomes a system that can be used in several different ways, which greatly improves the rates of recognition and rejection.[6]

- The following are available for stringent security requirements, and either together or in any desired combination as required: possession (chip card), knowledge (conventional PIN), biometry 1 (the dynamics of typing the PIN), biometry 2 (the dynamics of writing the PIN or password), or biometry 3 (the dynamics of writing a signature).[7]
- The amount of data required is so small that it can easily fit on a chip card.[8]
- In its capacity as a biometric random number generator, it derives a biometric random number from the writing dynamics at the same time that the writing is entered.[9]
- The user can also use the pad as a substitute for a mouse for cursor control – and this always functions, even in the event of high temperatures or high levels of relative humidity.[10]

---

[1] A signature can be imitated and a facsimile of it produced, but it can NEVER be forged. The BKA [Bundeskriminalamt = Federal Criminal Police Office] says so. HESY records 1600 pressure values per second; and in addition the writing time and pauses in writing.

[2] Who would be recognized by a package acceptance on-line? Nobody! An off-line-verification by a handwriting expert would only follow of the acceptance was questioned – as if he can tell anyway from a signature produced there! The BKA rejects this. What is missing is the pressure of the pen on the paper, or in other words, the writing dynamics recorded with large amounts of data.

[3] None of the participants can retrospectively change the documents in his possession. And certainly not if TWO signatures were made; those of the member of the public and the official, or of the customer and the salesman respectively.

[4] In which documents that were given a digital seal as per SiG will also be stored later. ONE digital archive can thus handle ALL future tasks.

[5] For that reason it was called the “analog keyboard”.

[6] A so-called “multi-mode system”. Nonetheless, it is questionable whether 100 % of the population could be recognized. According to Gauß, not so in practical terms. With HESY it would be around 95 % - the only people missing are those who cannot write AND who cannot enter a PIN or who simply want to have nothing whatsoever to do with computers. The remaining ones will have no need anyway!

[7] “Possession and knowledge” or “possession and one or more biometric characteristics" suffice for digital seals as per SiG. With a signature as well, electronic seals then become genuine digital signatures or electronic signatures.

[8] 1 kb should be adequate, but there are chips that can store up to 32 kb of data.

[9] Indispensable for electronic seals as per SiG. Since each signature is unique, with differences in the writing pressure and time sequences, it is possible to resort to a different sequence of pressure and non-pressure by means of a coordinates grid. This can be represented as a sequence of 1’s and 0’s.

[10] The cursor will be faster or slower, in the same way as the pressure on the pad – as we are accustomed to from many other things.

Sign and Type – Handwriting Recognition System

SIGN-N-TYPE is a handwriting recognition system for all conventional pens. The writing area is supported on four load cells and the invisible pressure and time sequences of the writing sample that are unique to each person and cannot be faked are recorded in four dimensions during writing.

A digital signature that is produced by your own hand is thus created by Sign-n-Type. It is encrypted using suitable mathematical algorithms and attached inseparably to the document. The signature or a password written by your own hand is used. The so-called "digital blueprint" that can be created with Sign-n-Type makes it possible for a member of the public, customer or guest to sign the usual piece of paper with his or her own hand. This ensures the authenticity and unique ownership of the written items. This also provides a piece of evidence that can be used in court – the businessman, hotel or official authorities no longer require any actual paper.

It is thus very cost-effective to archive, and easy to integrate into existing document management (DMS) or workflow management systems and likewise to provide a piece of evidence in electronic form that can be used in court, such as a hotel booking note. Both documents include the unique and identical values of the writing dynamics; it is not possible for anyone else to make a new copy or version; once written, the signature is unique and cannot be reproduced. The partner can likewise sign both documents to meet more stringent security requirements. This provides a degree of security that creates a high degree of trust and confidence at a very low price.

The recording and evaluation of the writing dynamics is a procedure that can be listed without further ado under the heading of biometric recognition methods – ultimately you need to have "knowledge" of the name or the password and the unmistakable, individual and behaviour-based writing dynamics to either recognize an authorized person or to block out an unauthorized one.
For that reason the use of a so-called "value-dependent ID field" has been proposed. Tiresome rejections of authorized persons due to low values would be avoided. But the user would be perfectly willing to sign once or twice more if need be in the case of higher values. This is a perfectly normal procedure and one that we are already used to – we are much more concerned about our wallets if they contain not just 50 Euro but the princely sum of 5,000 Euro! The mathematician has a number of tricky tasks to solve as well when it comes to a "value-dependent ID field".

Since multimodal systems have considerable advantages over a single solution for biometric or behaviour-based identification, it is thus logical to make use of the typing dynamics that are typical for each individual person when it comes to inputting a PIN.

In the same way as for the "electronic signature" (elsig) under the German signatures law, "knowledge" of a multi-number PIB (at least 6, and preferably 8 to 10 digits) or conventional passwords that are typed in can be used in addition to "possession" (of a Smartcard). We would also like to say at this point that it is useless to try to spy out the entry procedure – the invisible typing dynamics cannot be imitated as such. The unique and clear statement of intent of one's own signature is, in addition to being a form of unique identification, no longer a wasted item but instead the main part of the application.

Sign-n-Type can be used as an "analog keyboard", either with or without recording of the typing dynamics, e.g., in any bank ATM or installed in all cases where keypads or keyboards are used to input a PIN. It is then left up to the customer to decide whether to input his PIN in the conventional way or whether to personalize it via the typing dynamics.

Anyone wishing to use Sign-n-Type to authenticate a digital or electronic signature according to the law and to genuinely identify the signatory can also use a random number generated biometrically in addition to the signature data. The option of biometric random number generators would almost certainly not be so easy to implement with any other type of identification procedure.

Szenario: Tante Emma, Onkel Peter und die „Elektronische Blaupause"

Tante Emma ist 63 Jahre jung, seit jeher Hausfrau und mochte bei der Stadtverwaltung ihren Yorkshireterrier, genannt ,,Fiffi", zur Hundesteuer anmelden. Tante Emma besitzt keinen Computer und keinen Internetanschluss. Die elektronische Signatur ist für sie ein absolutes Fremdwort, sie wird höchstens fragen: „Wo muss ich denn da unterschreiben ?"

Im Bürgeramt nimmt der zuständige Sachbearbeiter ein papierenes Formular in Vierfachausfertigung und schreibt ihre Personalien, Adresse, Kontonummer und was sonst noch alles Wichtiges für die Anmeldung vonnöten ist auf. Dies erfolgt handschriftlich oder mit der Schreibmaschine. Moderne Verwaltungen haben auch schon elektronische Formulare. Diese werden auf dem Bildschirm ausgefüllt.

Nun erfolgt der Ausdruck mehrerer Exemplare, die dann von Tante Emma und dem Sachbearbeiter, nach der Lektüre und Überprüfung des Inhalts, eigenhändig unterschrieben werden. Eines davon erhält Tante Emma; den Beleg kann sie nun mit nach Hause nehmen und abheften. Der Sachbearbeiter verteilt nun ,,seine" Exemplare in der Stadtverwaltung (Steueramt, Ordnungsamt). Jeder hat ein Stuck Papier, das er bearbeiten und archivieren muss.

Noch modernere Verwaltungen scannen das Dokument und verteilen die elektronische Form dann über ein Workflowmanagement. Nach dem Scannen wird das Original vernichtet und somit auch die Originalunterschrift der Tante Emma. Das Stück Papier, in dem die individuellen und nachweisbaren Druckspuren der Unterschrift verewigt sind, landet im Reisswolf. Bestenfalls landet es im Archiv und verursacht lange noch unnötige Kosten. Immerhin, dort kann man es noch herausholen und gegebenenfalls vor Gericht als Urkundsbeweis vorlegen. Kein Gesetz schreibt vor, dass Hundersteueranmeldungen eigenhändig unterschrieben sein müssen. Hier dient die Unterschrift lediglich dem Beweis, dass jemand bewusst eine Verpflichtung (hier: Zahlen der Hundesteuer) eingegangen ist.

Onkel Peter, 65 Jahre jung, seit zwei Jahren pensioniert, hat sich nach der Auszahlung einer Lebensversicherung ein neues Auto gekauft und bringt dies nun zur Inspektion in die Werkstatt. Dort wird ein Vierfach-Formular gezückt, das „Auftrag zur Durchführung einer 10 000 km-Inspektion“ heißt. Der Annahmemeister hat es vorsorglich schon ausgefüllt, es wird nur noch durch weitere Aufträge oder Anmerkungen ergänzt. Onkel Peter unterschreibt nun diesen Formularsatz und erhält ein Exemplar ausgehändigt. Die Durchschläge wandern in die Werkstatt, in die Rechnungsabteilung und in die Statistik. Dort werden sie archiviert.

Der Geselle führt die Arbeiten durch, der Meister kontrolliert sie und unterschreibt als Verantwortlicher die korrekte Ausführung der Arbeiten. Ein Durchschlag dieser unterschriebenen Checkliste landet wieder bei der Statistik und in der Rechnungsabteilung; einen erhält Onkel Peter bei Abholung des Fahrzeuges. Onkel Peter muss auch die korrekte Übernahme des Autos unterschreiben; schließlich könnten ja irgendwelche Lackschäden vorhanden sein.

Auch hier zeigt sich wieder, dass keine der Unterschriften gesetzlich vorgeschrieben ist, sie dienen lediglich der Beweisfunktion bei späteren Streitigkeiten. Auch Onkel Peter ist kein Besitzer einer elektronischen Signatur, er kann nur eigenhändig signieren.

Diese beiden Geschichten zeigen sehr eingängig, wie durch eine zunehmende Digitalisierung die Gefahr einer Zwei-Klassen-Gesellschaft wächst. Menschen wie Tante Emma und Onkel Peter dürfen ob ihrer technischen Rückständigkeit nicht benachteiligt sein.

Quelle: Biometrische Verfahren von V. Nolde & L. Leger, Fachverlag Deutscher Wirtschaftsdienst, Köln 2002.

Folgende Ergänzungen sind nachträglich durch Baltus eingefügt.

Werden die zuvor beschriebenen Dokumente lediglich EINMAL ausgedruckt und auf HESY gelegt und eigenhändig unterschrieben, hat Tante Emma „ihr" abheftbares Stück Papier. Onkel Peter nicht anders. Die Verwaltungen haben lediglich die forensisch korrekt unterschriebene „elektronische Blaupause". Diese kann – ohne umständliche Archivierung – unverzüglich in ein Workflow integriert werden und spart somit erhebliche Kosten.

Weitere Beispiele, die eine „elektronische Blaupause" sinnvoll erscheinen lassen:

Urlaubsanträge und -scheine, Schlüsselübergaben, Geldübergaben, Werkzeugausgabe, Waffen-, Munition- und Materialausgabe, CAD-Zeichnungen, Medikamentenausgabe, Patientenerklärungen, Hotelmeldezettel, Zeugnisse (Letztere müssen im Original eigenhändig unterschrieben sein, die Kopie kann jedoch wie beschrieben papierlos archiviert werden – mit den Daten der eigenhändigen Unterschrift.).

Konsequent weitergedacht, kann folgendes „4-Stufen-Modell“ aufgezeigt werden:

1. Der unbedarfte Bürger geht wie zuvor beschrieben in das Bürgeramt. Der Beamte regelt, soweit möglich und nötig, alles für ihn.
   Ergo: Papier für den Bürger (oder Kunden), das elektronische Dokument für die Verwaltung.
2. Der Bürger geht in das Bürgeramt, findet dort ein Kiosksystem vor, an dem er nun das erforderliche Dokument aufruft, ausfüllt und direkt über das Intranet an das Bürgeramt sendet; er erhält daraufhin eine Wartenummer. Ein freier Mitarbeiter bekommt das Dokument auf den Bildschirm und ruft über die Wartenummer den Bürger zu sich. Nun füllt der Beamte unter Mithilfe des Bürgers das Formular aus, druckt es einmal aus und lässt es auf dem Sign-n-Type-Pad unterschreiben.
   Ergo: Papier für den Bürger (oder Kunden), das elektronische Dokument für die Verwaltung.
3. Der Bürger ruft zu Hause an seinem PC die Internetseite der Verwaltung auf. Er füllt am Bildschirm das Formular aus und sendet dieses über das Internet an die Verwaltung. Dort wird es an den zuständigen Mitarbeiter weitergeleitet, der sendet einen Besprechungstermin an den Bürger. Anlässlich der Besprechung füllt der Beamte unter der Mithilfe des Antragstellers das Formular aus, druckt es einmal aus und lässt es auf dem Sign-n-Type-Pad unterschreiben.
   Ergo: Papier für den Bürger (oder Kunden), das elektronische Dokument für die Verwaltung.
4. Der Bürger ist in der glücklichen Lage, eine digitale Signatur sein Eigen zu nennen. Er ruft zu Hause an seinem PC die Internetseite der Verwaltung auf, füllt am Bildschirm das Formular aus, druckt es einmal aus und unterschreibt es auf dem Sign-n-Type-Pad. Dann sendet er das Formular eigenhändig und digital mit „Besitz (SmartCard) und Wissen (PIN)“ oder „Besitz (SmartCard) und einem oder mehreren biometrischen Merkmalen“ (so §15 der Signatur-Verordnung) unterschrieben über das Internet an die Verwaltung zurück. Alles korrekt mit Trustcenter, Hashwert und Zeitstempel!
   Ergo: Als Beweis vor Gericht Papier für den Bürger (oder Kunden), das elektronische Dokument für die Verwaltung.

Online nachzulesen unter
www.sign-n-type.com/SzenarioTanteEmma.pdf

Auszüge aus der Fachliteratur

Verwendbarkeit des Handschriftenerkennungssystems HESY für Zwecke der Schriftvergleichung (Auszüge)

Expertise von Dr. Eugen Maus

1 Zusammenfassung

Das Handschriftenerkennungssystem HESY ist eine neuentwickelte Schreibwaage mit Rechnerunterstützung. Die Besonderheit des HESY besteht darin, dass das Schriftfeld des Eingabegerätes auf vier Drucksensoren gelagert ist.1 Während Schreibwaagen mit einem Sensor nur den Schreibdruck gegen die Schreibzeit darstellen können, wird beim HESY durch Errechnung der Schreibspitzenposition aus den vier Sensorsignalen auch die Wegdimension erfasst, so dass zusätzlich Informationen über die flächige Verteilung des Schreibdrucks, die Form der Unterschrift, die Schreibgeschwindigkeit, Schreibpausen usw. gewonnen werden.

Das HESY wurde zur automatischen Identifizierung von Unterschriften in elektronischen Zugangs- und Zahlungssystemen entwickelt und wird industriell gefertigt in größeren Stückzahlen zu einem niedrigen Preis angeboten2. Damit ist es auch für Schriftsachverständige im forensischen und forschenden Bereich von großem Interesse, da die mit dem HESY gewonnenen Informationen bestens geeignet sind, den Schriftvergleich nicht nur wie bisher über die Formgebung, sondern auch über den Schreibdruck durchzuführen.

2 Einleitung

Das Interesse an der Handschrift hat bislang alle technischen Neuerungen überstanden, ganz gleich ob es sich nur um die Einführung neuer Schreibgeräte, wie etwa den Kugelschreiber oder Schreibmaschinen, oder neue Techniken der Dokumentation mit Computern, Laserdruckern, virtuellen Dokumenten usw. handelte.

Die Unterschrift erfährt ihre Bedeutung insbesondere dadurch, dass sie im Unterschied zu allen anderen, der Person anhaftenden Identifikationsmerkmalen (wie Stimme, Gesicht, Fingerabdruck usw.), praktisch das einzige Merkmal ist, welches ausschließlich willentlich abgegeben wird. Ein weiterer Vorzug der Unterschrift ist, dass sie eine große Zahl personenunabhängiger Identifikatoren, wie PINs oder Spezialausweise, ersetzen kann.

Die Bedeutung der Handschrift, und damit der mögliche Einsatz von HESY, erstreckt sich auf eine Vielzahl von Bereichen:

- Forensische Schriftvergleichung: Begutachtung von Schecks, Testamenten, anonymen Schreiben usw. durch Schriftsachverständige zur Prüfung der Urheberschaft im Rahmen eines Gerichtsverfahrens.

- Graphologie: Analyse und diagnostische Auswertung von Zusammenhängen zwischen Persönlichkeits- und Schriftmerkmalen.
- Schriftpsychologie: Erforschung psychiatrischer, schulpsychologischer und anderen Probleme.
- Den informationstechnischen Bereich der automatisierten Schrift- und Unterschriftserkennung, auch im Rahmen der Sicherheitstechnik.

Ein besonderes Merkmal der Handschrift ist die Druckgebung während des Schreibens, und es hat nicht an Versuchen gefehlt, diese zu erfassen, zu erforschen und zu nutzen. Während die Erfassung der Druckgebung am vorliegenden Schriftstück (Offline-Messung) schwierig und zeitaufwendig ist (s. z.B.: DEINET et al, 1983), kann der Druck während des Schreibens (Online-Messung) inzwischen mit verschiedenen Geräten erfasst werden. Diese Erfassungsgeräte gibt es als spezielle Schreibstifte mit eingebauten Drucksensoren (Druckmess-Stifte)und als druckempfindliche Schreibunterlagen, auch als Schreibwaagen bezeichnet. Beiden Erfassungsgeräte haften Vor- und Nachteile an.

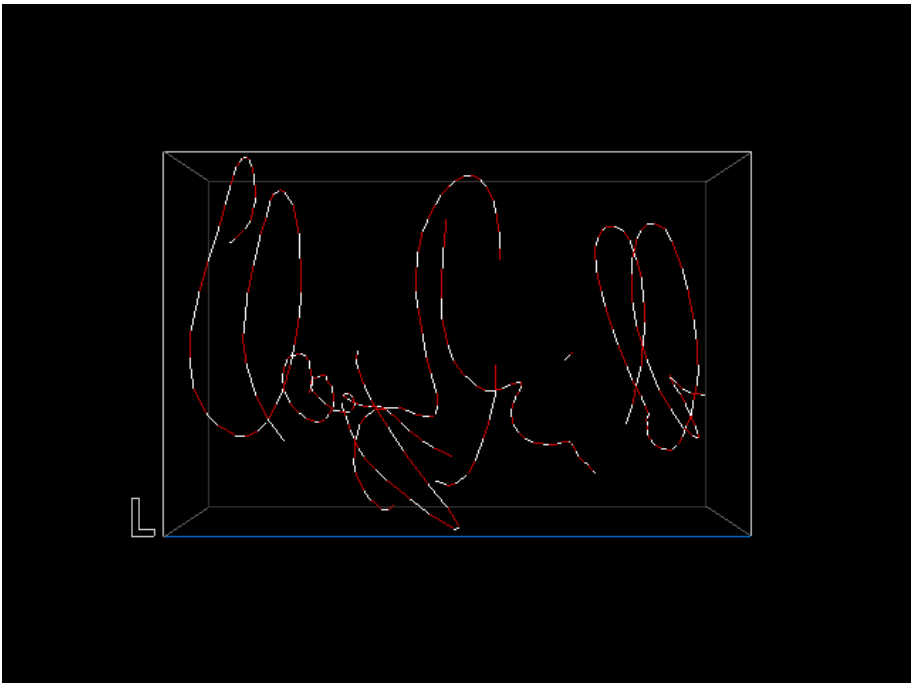
Druckmess-Stifte gestatten die Erfassung des Schreibdruckes auf prinzipiell beliebigen Arealen über beliebige Zeit. Nachteilig ist dabei u.a., dass der jeweilige Schreiber gezwungen ist, ein spezielles, ungewohntes Schreibgerät (eventuell sogar mit angeschlossenem Kabel) zu benutzen. Außerdem lassen sich nicht für alle Arten von Schreibgeräten Druckmess-Stifte herstellen. Auch bestehen aus rein mechanischen Gründen Einschränkungen hinsichtlich der Schräghaltung des Druckmess-Stiftes, die u.U. zu einer ungewohnten Schreibhaltung zwingen.

Die zuvor genannten Nachteile des Druckmess-Stiftes betreffen die Schreibwaage nicht. Schreibwaagen werden bereits seit geraumer Zeit hergestellt. Sie stellen eines der ältesten Instrumente zur Schreibdruckforschung dar, sieht man von Hilfsmitteln wie Lupe oder Mikroskop einmal ab. Die eindimensionale Schreibwaage wurde u.a. durch Steinwachs weiterentwickelt. Neuere Entwicklungen der Schreibwaage wurden beispielsweise von De Bruyne (1991) (piezoelektrische Aufnehmer) und Kobayashi et al (1998) (induktive Aufnehmer) vorgestellt. Diese Geräte können Bewegungskoordinaten, Schreibdruck, Stiftneigung usw. erfassen. Dabei kann das Schreibgerät prinzipiell beliebig gewählt werden. Dagegen ist bei der Schriftwaage das Schriftfeld begrenzt, damit der Druck der aufgelegten Hand den eigentlichen Schreibdruck nicht überlagert.

Das HESY (Handschriftenerkennungssystem) zählt zu den Schreibwaagen und ist eine der ersten Schreibwaagen, die in größeren Stückzahlen für einen breiten Anwenderkreis hergestellt werden kann. Bei diesem System werden insbesondere die dem Druckmess-Stift und herkömmlichen Schreibwaagen anhaftenden Nachteile vermieden.

Sichere Authentikation – HESY Unterschriftenprüfer

Von Claus Schönleber, Rene Baltus



1. Benutzeridentifikation*

Erkennen Sie sich auch manchmal morgens im Spiegel nicht? Nicht so schlimm. Allerdings kann es problematisch werden, wenn eine Person zweifelsfrei identifiziert werden muß. Schon im Alltag spielen wir dieses Spiel ständig beim Telefonieren. Wenn zwei Personen miteinander telefonieren, dann wollen beide sicher sein, daß am anderen Ende auch die Person sitzt,.mit der man sprechen wollte. Normalerweise macht man das in mehreren Phasen. Zunächst wird der Name abgefragt, dann achtet man auf die Stimme, auf typische Phrasen oder auf die Stimmlage. Daß dies alles nicht immer zuverlässig ist, davon leben Hollywood und die Autoren von Kriminalromanen.

Bei der Kommunikation über Leitungsnetze kann man eben nicht zuverlässig nach Gesichtszügen oder anderen rein visuellen Eigenschaften prüfen. Selbst oder gerade Videoübertragungen erlauben vielfältigste Manipulationen. Es gibt deswegen ein ganze Reihe von Verfahren, die es erlauben mehr oder weniger sicher eine Identifikation durchzuführen.

Dazu unterscheidet man drei große Gruppen:

- Prüfung von Wissen (z.B. Paßworte)
- Prüfung von Besitz (z.B. Smart Card)
- Prüfung physiologischer oder biochemischer Eigenschaften (z.B. Fingerabdruck)

1.1 Paßworte (Wissen)

Die einfachste kennen Sie alle und wenden sie wohl auch häufig an. Mit Hilfe von Paßworten identifiziert man sich in der Regel gegenüber automatisierten Dienstleistungen wie Geldautomaten, Mobiltelefonkarten, Kreditkarten oder Computerterminals.

Aber schon hier werden die Schwächen von Paßworten offensichtlich: Ist das Paßwort gut im Gedächtnis zu behalten, so ist es leicht kompromitierbar. Wird es an offensichtlicher Stelle ungesichert notiert, so ist es ebenfalls angreifbar. Ein sicheres Paßwort ist kompliziert und nicht leicht auswendig zu lernen.

Vor allem im Computerbereich wird immer noch allzu oft der Fehler gemacht kurze, gut zu behaltende Worte zu benutzen. So zum Beispiel der eigene Vor- oder Nachnahme, Namen von Freund, Freundin, Geliebter, Hund, Papagei, etc. Oder von Lieblingshelden, Dichtern oder Komponisten. Auch derbe Bezeichnungen aus dem erotischen Bereich werden gerne genutzt, weil „sich sonst keiner traut“. Hacker prüfen das als erstes nach. Und wie oft hat man Erfolg damit! Gute Paßworte bestehen aus zufälligen Zeichenfolgen, die auch Ziffern oder Sonderzeichen enthalten.

Ein Paßwort kann beim Eintippen oder Sprechen leicht ausgespäht werden.
Gerade bei Kredit- oder Scheckkarten passiert das recht häufig. Beliebter Tummelplatz zum Ausspähen sind Tankstellen am Samstagmittag. Wenn die Tankstelle voll ist und an der Kasse viele Leute stehen, läßt sich gar nicht vermeiden, daß einem beim Eintippen über die Schulter geschaut wird. Und schon ist die Geheimnummer (das Paßwort) nicht mehr geheim.

Gleiches gilt für Büros, in denen einige Computer stehen. Tippt ein Angestellter sein Paßwort ein, kann es von in der Nähe sitzenden Kollegen oder Besuchern gesehen werden. Bei der Übertragung des Paßwortes vom Terminal zum Rechner kann die Leitung angezapft sein. Das Paßwort kann dann mitprotokolliert werden. Bei heute üblichen LANs gibt es genügend Möglichkeiten, die Paßwörter, die über die Leitungen laufen, mitzuprotokollieren. Es gibt eine große Auswahl von Software für diesen Zweck. Deswegen werden in modernen Systemen Paßworte vor der Übermittlung verschlüsselt.

Um das Paßwort zu prüfen, muß es irgendwo abgespeichert sein. Solche Paßwortdateien sind extrem angreifbar.

Auch hier werden in modernen Systemen Paßworte verschlüsselt und für die Allgemeinheit unzugänglich aufbewahrt. Das Paßwort wird dabei in keinem Fall im Klartext abgespeichert, sondern nur in seiner verschlüsselten Form. Wird ein Paßwort eingetippt, so wird es zunächst verschlüsselt und das Resultat dann mit dem gespeicherten Muster verglichen. Trotzdem gibt es auch hier Programme, die unter bestimmten Voraussetzungen zumindest schlechte Paßworte sehr schnell finden.

1.2 Identifikationskarten (Besitz)

Die nächste Stufe sind Identifikationskarten. Hierbei wird damit gerechnet, daß die Kopie der Karte äußerst schwierig herzustellen ist. Man kennt zur Zeit vor allem Magnetstreifen- und verschiedenartige Chipkarten. Möchte man sich gegenüber einer anderen Instanz ausweisen, so benutzt man die Karte entsprechend. Man läßt den Magnetstreifen auslesen oder den Chipinhalt. An dieser Stelle wäre das System noch sehr angreifbar, denn Karten können verloren gehen oder werden gestohlen. Als letzte Sicherheit verlangt dann die Karte, daß sich die Person ihr gegenüber ausweist. Das geschieht üblicherweise mit einer PIN (persönliche Identifikationsnummer, meist vierstellig), also einem kurzen Paßwort. Und an dieser Stelle greifen wieder die Schwächen von Paßworten, das Problem wurde nur eine Ebene weiter angesiedelt. Daß dieses Problem tatsächlich existiert, kann man an den Schlagzeilen ablesen, die solche gestohlene Karten mitunter verursachen.

Aus diesem Grunde werden Systeme gesucht, die wirklich die Person identifizieren können, nicht ihr Wissen (Paßworte prüfen Wissen, nicht persönliche Eigenschaften). Als Absicherung sind deswegen schließlich nur biologische oder physiologische Eigenschaften des Eigentümers eines Schlüssels geeignet (Biometrik).

1.3 Fingerabdrucksysteme, Netzhautabtastung (biometrische Merkmale)

So werden in der Computertechnik zum Beispiel Fingerabdrucksysteme eingesetzt. Diese fertigen Fingerabdruckanalysen sehen sich nicht nur die Linienmuster der Fingerkuppe an, sondern suchen zusätzlich nach dem Hämoglobingehalt. Denn man könnte sonst einen Wachsabdruck oder den toten Finger des Besitzers benutzen. Solche Systeme werden dort eingesetzt, wo eine wirklich persönliche Identifikation gebraucht wird. Fingerabdrucksysteme gibt es aber schon länger ebenfalls für den PC-Bereich.

Auch wenn es ziemlich utopisch und nach James Bond klingt, auch das Muster der Netzhaut oder der Iris im Auge kann eine persönliche Identifikation ermöglichen. Im Auge kann man noch weniger manipulieren, und Fälschungen werden deswegen noch unwahrscheinlicher.

1.4 Stimmanalyse (biometrisches Merkmal)

Ein weiteres Element der menschlichen Persönlichkeit ist die Stimme. Deswegen können Identifikationssysteme auch nach charakteristischen Mustern in der Stimme suchen. Angriffspunkte sind natürlich Tonbandaufnahmen. Deswegen wird auch mit der Kombination von Stimmenanalyse und optische Analyse der Mundbewegungen experimentiert. Die Erfolge der ersten Versuche geben dieser Methode bisher recht. Es ist zuverlässiger als die Stimmanalyse allein.

Bei all dem kann man eine Erkenntnis gewinnen: Wie sicher auch die Mechanismen oder Verfahren sein mögen, der menschliche Faktor ist das Problem: Wenn ich mit meinem Paßwort nicht richtig umgehen kann, wenn mir meine Identifikation gestohlen wird oder wenn ich meine Identifikationen zu unsicher verwahre, dann mache ich jedes Sicherheitssystem zunichte.

Abb. 1: HESY - Ein Unterschriftenprüfer auf Basis der Schreibdynamik, benutzbar mit Normalstiften.

2. HESY**

Vorgeschlagen wird ein Unterschriftenprüfer, der beim Unterschreiben mit einem handelüblichen Schreibgerät online mit mehreren Druckaufnehmern alle notwendigen Informationen über die Schreibdynamik zur Verfügung stellt. Dazu zählen Gewicht, Geschwindigkeit, Zeit, Winkel, Länge und Breite. Der Unterschriftenprüfer soll aus normalen Hard- und Softwareteilen hergestellt werden können und einen unkomplizierten und zuverlässigen Betrieb gewährleisten.

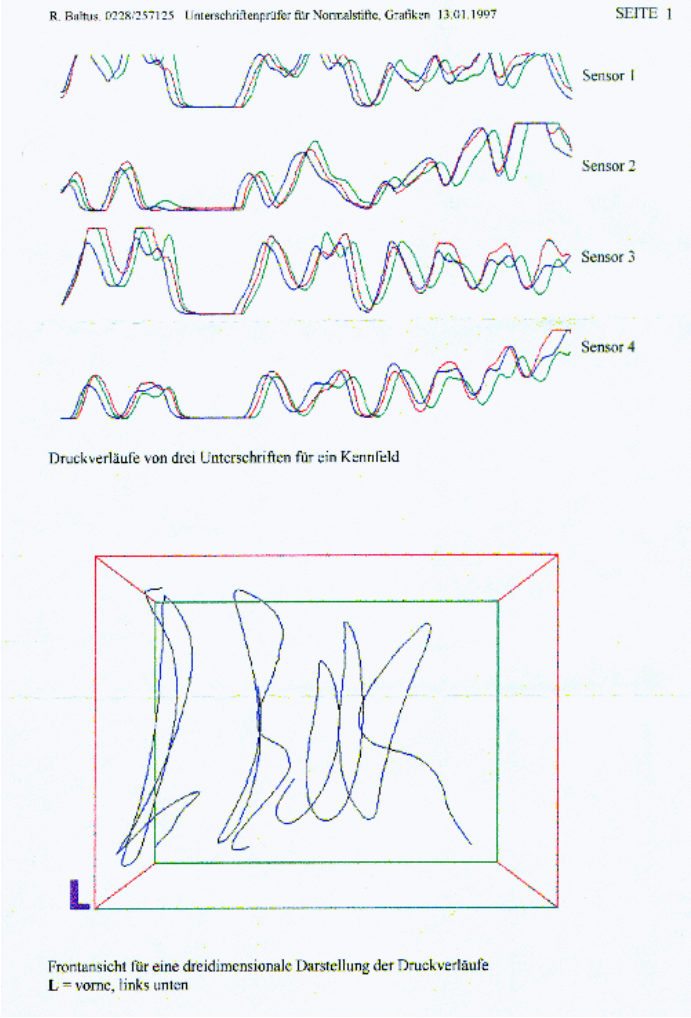


Abb. 2: Analyse der Schreibdynamik mit dem Gerät HESY.

Ein Beispiel für einen solchen Unterschriftenprüfer ist HESY (Baltus, Bonn). Es ist zuverlässig, preisgünstig und kann mit anderen, bewährten Verfahren beliebig kombiniert werden. Die Diagramme in *Abbildung 2* zeigen die unterschiedlichen Verläufe der Schreiblinien in einem 3-dimensionalen Vektorraum. Selbst eine graphisch perfekt gefälschte Unterschrift kann damit erkannt werden.

Schönleber: Verschlüsselungsverfahren für PC-Daten; Feldkirchen: Franzis'-Verlag, 1995.

Studienarbeit (Auszüge)
Projekt- und Datenmanagement im Flugzeugbau

Bearbeiter: Cand. aer. Thomas Tholl Matr. Nr. 1829510 Hospitalstr. 26 D - 70174 Stuttgart

Betreuer ISD: Prof. Dr.-Ing. habil. I. Grieger Inst. für Statik und Dynamik Pfaffenwaldring 26 D - 70569 Stuttgart

Betreuer IFB: Dipl. Ing. P.Schnauffer Inst. für Flugzeugbau Pfaffenwaldring 31 D - 70569 Stuttgart

Stuttgart 23.September 2003

Kurzbeschreibung :

Aufbauend auf CATIA V5 soll das Projekt- und Datenmanagement eines Entwicklungsbetriebes untersucht und auf luftfahrttechnische Belange zugeschnitten werden.

Anschließend soll dieses Verfahren, welches Entwicklung- wie auch Fertigungsbelange berücksichtigt, für eine neue CAD-Systemwelt am Institut erarbeitet werden, damit es als Grundlage für die Entwicklung eines Programmsystems für unkonventionelle Fluggeräte zur Verfügung steht.

Aufgabe :

- Literaturrecherche.
- Vergleich diverser Projekt- und Datenmanagementphilosophien.
- Entwurf und Beschreibung des Projektmanagements, welches für den Einsatz von CATIA V5 geeignet ist.
- Berücksichtigung der Luftfahrtindustrie hinsichtlich Entwicklungs-, Zertifizierungs- und Fertigungsrichtlinien wie auch der Kunden-Lieferanten-Beziehung.
- Einbezug neuer Konstruktionsphilosophien (parametrisierter Entwurf, digitaler Arbeitsplatz) für neue Flugzeuge in den Datenfluss.
- Entwicklung der semantischen Featurephilosophie.

Abstrakt

In der modernen Konstruktionswelt haben sich schon seit einiger Zeit CAD-Programme durchgesetzt und sind daraus nicht mehr wegdenkbar. Mit der zunehmenden Vernetzung der einzelnen Arbeitsplätze untereinander beginnen sich auch Datenmanagementlösungen durchzusetzen.

Eine vollständige Durchgängigkeit von der Entwicklung bis zur Fertigung ist allerdings noch nicht erreicht. Eine wichtige Vorraussetzung dafür ist ein Entwurf und ein genormtes Datenmanagement. Von diesem Entwurf ist zu fordern, dass er im Nachhinein an auftretende Probleme angepasst werden kann. Beide Themen werden in dieser Studienarbeit behandelt und spezifiziert.

Die Digitale Signatur und Unterschrift wird im ersten Kapitel behandelt und mit den Möglichkeiten des Datenmanagement in zweiten Kapitel verbunden. Das dritte Kapitel erklärt den parametrisierten Flugzeugentwurf, der dann im vierten Kapitel in das gesamte Projekt „Pegasus Rebell" des IFB's eingeordnet wird. Im letzten Kapitel wird ein Ausblick auf Projekte gegeben, welche an die Arbeit anknüpfen.

In the modern world of aircraft design Computer Aided Design (CAD) programmes have prevailed on the market and are a fundamental tool for the development, planning and layouting.

Due to the increase of linking and networking of single workstations, data management solutions are essential and mandatory for modern project work.

In order to achieve complete transparency and flexibility, continuous standards have to be imposed, leading from the first drafts to the final product. The most important requirement is a standardized data management. It must be possible to adjust the draft to problems that arise afterwards. These topics are mentioned and specified in these studies.

The digital signature is discussed in the first chapter and is linked to the possibilities of the data management in the second chapter. The third chapter explains the parametric aircraft model which is implemented in the complete project "Pegasus Rebell" of the IFB (fourth chapter). The last chapter gives a perspective and outlook towards future and follow-on projects.

1.5 Hesy

Auf der Suche nach einer Methode biometrische Daten fälschungssicher, von Rechtswegen anerkannt und gleichzeitig einfach zu erfassen zeigte sich, dass das Handschriften-Erkennungs- SYstem HESY ideale Möglichkeiten bietet.

HESY „... ist ein Schreibpad, welches nicht nur die Schriftposition, sondern auch die Druckstärke und Schreibgeschwindigkeit aufzeichnet. ... Diese Eigenschaft macht die mit Hesy aufgenommene elektronische Unterschrift für Rechtsverträge rechtssicher und auch für einen Schriftsachverständigen nachträglich überprüfbar."[v]

Damit rechtsverbindliche Verträge abgeschlossen werden können ist eine aktive Willenserklärung in Form einer eigenhändigen Unterschrift vorgeschrieben. Diese Unterschrift kann durch die mit HESY digitalisierte Unterschrift ersetzt werden. Ein weiterer nicht zu unterschätzender

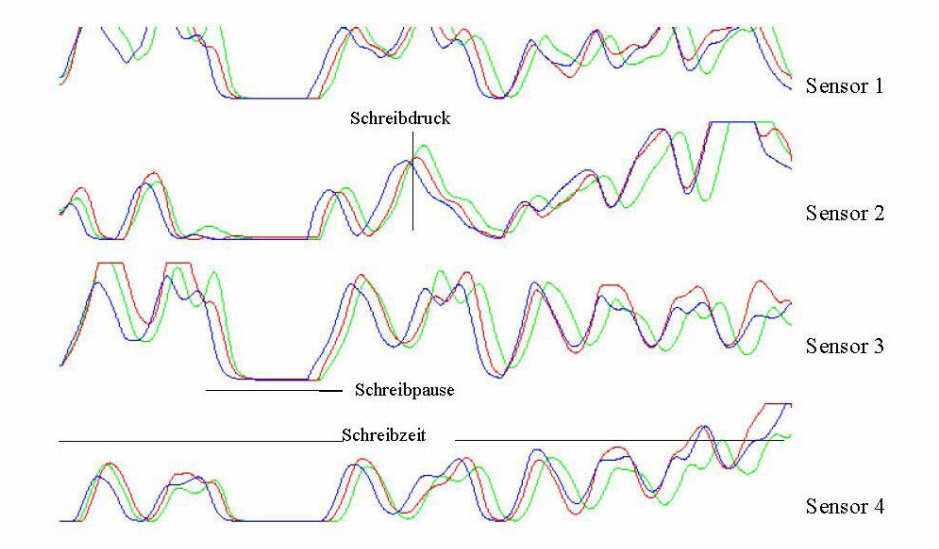
Vorteil dieses Pads ist der rechtlich geforderte Übereilungsschutz, welcher verhindern soll, dass übereilte Bekenntnisse abgegeben werden. Dadurch, dass man sich schon an die normale Unterschrift gewöhnt hat, gibt niemand leichtfertig seine eigene Unterschrift unter ein Dokument das er nicht gelesen hat.

Aufbau und Funktion

Der Aufbau von HESY ist relativ einfach und doch können damit die oben genannten Anforderungen erfüllt werden. Das Schriftfeld von HESY ist auf vier Drucksensoren gelagert. Jeder einzelne Sensor liefert jeweils während des Schreibens ständig einen genauen Druckwert. Diese Werte werden über eine Schnittstelle an ein Programm im Computer übermittelt. Mit Hilfe dieses Programms ist es daraus möglich den Linienverlauf des Stiftes zu errechnen. Dabei wird nicht nur ein herkömmliches Abbild der Unterschrift erzeugt, sondern ist es zusätzlich möglich, den genauen Druck-Zeit-Verlauf zu erkennen.

Bild 1.4 HESY Pad

Bild 1.5 Druckverläufe von 3 Unterschriften für ein Kennfeld [vi]



Mit den errechneten XY-Schreibkoordinaten, den Druck- und Zeitverlauf ergibt sich ein vierdimensionale Verlauf des Schriftbildes. Damit ist der Schriftverlauf genauer festzustellen als eine nachträgliche Analyse der Unterschrift auf Papier, denn dort fehlt der zeitliche Zusammenhang. Dieser Verlauf ist für jeden Menschen verschieden und kann durch die unbekannte Zeitkomponente nicht nachgemacht werden, unterscheidet sich aber mit jeder Unterschrift. Somit ist es erforderlich ein Kennfeld zu definieren, innerhalb dessen die Unterschrift erkannt wird.

Dieses Kennfeld kann dann an die nötigen Sicherheitsbedürfnisse angepasst werden. Es ist zum Beispiel weder nötig noch erwünscht bei jeder eingeforderten Unterschrift unter ein Dokument, eine Überprüfung vorzunehmen. Damit ist HESY zum forensischen Schriftvergleich und zur elektronischen automatisierten Schrift- und Unterschriftserkennung (auch im Rahmen der Sicherheitstechnik) einzusetzen.

Diplomarbeit (Auszüge)

Entwicklung und Test einer interaktiven Schnittstelle für den Einsatz der digitalen Unterschrift im Entwicklungs- und Fertigungsprozess eines modernen Luftfahrtunternehmens

von Joachim Greiner

durchgeführt am Institut für Flugzeugbau Universität Stuttgart

betreut von Dipl.-Ing. Peter Schnauffer

1.3 Handschrift Erkennungssystem HESY

HESY ist eine Entwicklung von Baltus [7]. Das Gerät ähnelt einem Touchpad eines Laptops. Die Aufnahme der Unterschrift erfolgt über eine, an vier Dehnmessstreifen aufgehängten Platte. Durch die Unterschiedliche Gewichtung der Platte geben die Messtreifen unterschiedliche Signale ab. Aufgrund dieser Werte können dann die Daten der Unterschrift aufgezeichnet werden.

Das System ist nicht nur in der Lage eine Unterschrift zweidimensional aufzunehmen, wie dies auf einem Papier der Fall wäre. HESY zeichnet eine Unterschrift vierdimensional auf. Zu den üblichen zweidimensionalen Koordinaten wird zusätzlich die Drucktiefe registriert, so wie die Zeitdauer der Unterschrift. Diese Daten werden dann in einer Datei abgespeichert. Da es absolut unmöglich ist, zweimal exakt die selbe Unterschrift abzuliefern, unterscheiden sich auch die aufgezeichneten Daten einer Unterschrift geringfügig. Sollten zweimal die exakten Daten auftauchen, so handelt es sich hierbei um eine Fälschung. Dieses Verfahren ist besonders fälschungssicher, denn wenn das Schriftbild kopiert wird, fehlen die Daten der Unterschrift. Auch das „Nachfahren" einer bestehenden Unterschrift würde sofort auffallen, da hier die Drucktiefe sowie die Geschwindigkeit nicht nachgemacht werden können. Somit ist die „elektronische Fälschung" der Unterschrift noch schwieriger als eine Fälschung der „normalen" Unterschrift. Beides erfüllt den Straftatbestand der Unterschriftenfälschung.

Die beiden nachfolgenden Bilder zeigen den dreidimensionalen Charakter, der von HESY aufgezeichneten Unterschrift. Abbildung 1.7 zeigt die Unterschrift von oben betrachtet, so wie sie auch auf einem Papier stehen würde. In Abbildung 1.8 ist die Unterschrift dann um 90° gedreht, also eine Ansicht von der Seite. Hierbei ist gut zu sehen, wie von HESY auch die Drucktiefen mit aufgezeichnet werden.

1.3.1 Funktionen von HESY

HESY bietet neben den Treibern, noch einen erheblichen Funktionsumfang. Alle Funktionen liegen als Programmbibliotheken (Dynamik Link Library, dll) vor, und können so unabhängig von der jeweiligen Programmiersprache angesprochen und benutzt werden. Zum Umfang gehören Funktionen, die es ermöglichen, die Unterschrift einzulesen und als Bild darzustellen. Für die Darstellung als Bild, muss die verwendete Programmiersprache jedoch über ein Element verfügen, das in der Lage ist einzelne Bildpunkte darzustellen. Dabei liegen pro Bildpunkt die Koordinaten vor. Die Darstellung der Koordinaten ist wichtig, denn in dieser Form wird die Unterschrift aufgenommen, in einzelnen Punkten pro Zeitabschnitt.

Die so erhaltenen Werte können natürlich auch abgespeichert werden. Sie liegen dann als Textdatei vor und können dann z.B. in ein Dokument eingefügt werden. Des Weiteren ist es auch möglich, die so gespeicherten Daten einer Unterschrift wieder aus der Datei einzulesen und daraus das Bild der Unterschrift zu erstellen. Diese Funktion ist dann wichtig, wenn einmal Zweifel an der Echtheit einer Unterschrift bestehen. So können dann die Daten ausgelesen werden und das Bild kann dann mit dem Bild der zweifelhaften Unterschrift verglichen werden.

Eine weitere wichtige Funktion ist die Vergleichsfunktion. Mit Hilfe dieser Funktion ist es möglich, zwei Unterschriften zu vergleichen und festzustellen, ob sie von der gleichen Person stammen. Dabei wird berücksichtigt, dass ein Mensch niemals zweimal die exakt gleiche Unterschrift abliefert, sondern dass es immer Abweichungen gibt. Der Grad der Genauigkeit der Erkennung kann hier eingestellt werden. D.h. es wird ein gewisser Toleranzbereich angegeben, wie stark die beiden Unterschriften voneinander abweichen dürfen. Dieser Bereich ist frei einstellbar.

1.4 Umsetzung am IFB

Am IFB werden als Anwendungsprogramme, in denen zu unterschreibende Dokumente erstellt werden, hauptsächlich die Office-Anwendungen wie Word und Excel verwendet. Ein weiteres wichtiges Anwendungsprogramm ist das CAD-Programm CATIA. Diese Programme sind alle mit dem PDM-System SmarTeam gekoppelt. In die Verbindung zwischen den Anwendungsprogrammen und SmarTeam wird nun noch eine Software eingebaut, die es mit Hilfe des HESY ermöglicht, eine Unterschrift in das Dokument einzufügen und dieses dann direkt in das PDM zu verschieben (einzuchecken). In Abbildung 1.10 ist diese Vorgehensweise schematisch dargestellt.

2 Umsetzung in SmarTeam

Bei installiertem SmarTeam sind in den Programmen CATIA, Word und Excel wichtige SmarTeam Funktionen wie z.B. „checkin", „checkout" oder „release" verfügbar, so dass diese Operationen direkt aus dem jeweiligen Anwendungsprogramm heraus aufgerufen werden können. Vorraussetzung hierfür ist, dass SmarTeam gestartet wurde und dass auch zwischen dem Anwendungsprogramm und SmarTeam eine Verbindung hergestellt wurde. Dies geschieht über den Befehl „Activate SmarTeam" in Word und Excel, oder über „Verbinden" in CATIA. Die Befehle befinden sich jeweils im Menü „SmarTeam" des Programms. In diesen Komplex wird jetzt noch zusätzlich HESY eingebaut.

2.2 Das Dialogfeld zum Unterschreiben

Um nun die von HESY aufgenommene Unterschrift in das Dokument einzufügen und dieses dann sofort in SmarTeam einzuspielen, wurde ein SmarTeam Skript mit dem Ereignis „on Life Cycle click checkin“ gekoppelt. Hier ist es nur möglich ein Skript vor dem eigentlichen Ereignis zu starten. Dies bedeutet, dass das Skript aufgerufen wird, sobald der Benutzer auf „checkin“ klickt. Dabei spielt es keine Rolle, ob dies in SmarTeam selbst geschieht, oder aus dem SmarTeam Menü von Word, Excel oder CATIA heraus.

Für ein ansprechendes Dialogfeld wurde aus den oben beschriebenen Gründen ein Programm in Visual Basic 6.0 geschrieben. Dieses Dialogfeld enthält alle Funktionen von HESY, sowie alle Funktionen um die Unterschrift in die jeweiligen Programme einzufügen. Dieses Programm liegt als so genannte Programmbibliothek vor und wird vom SmarTeam Skript aus gestartet. Die Datei heißt „smunterschreiben.dll" und muss in Windows als Programmbibliothek registriert sein. Dateien im dll-Format sind hartcodiert, das bedeutet sie liegen im Binärcode vor und können nicht mehr in den ursprünglichen Quellcode zurück geführt werden. Somit sind die darin enthaltenen Informationen geschützt. Dies spielt im weiteren noch eine wichtige Rolle, wenn es um die Manipulationssicherheit des Systems geht.

Multidisziplinärer Datenfluss im Entwicklungsprozess des Flugzeugbaus am Beispiel eines Senkrechtstarters

Von der Fakultät Luft- und Raumfahrttechnik & Geodäsie der Universität Stuttgart
zur Erlangung der Würde eines Doktors der Ingenieurswissenschaften (Dr.-Ing.) genehmigte Abhandlung
Vorgelegt von Peter Schnauffer
Hauptberichter: Prof. Dipl.-Ing. Rudolf Voit-Nitschmann
Mitberichter: apl. Prof. Dr.-Ing. habil. Ingolf Grieger
29. Mai 2006

Zusammenfassung

Die vorliegende Arbeit „Multidisziplinärer Datenfluss im Entwicklungsprozess des Flugzeugbaus“ verdeutlicht einen vollständig parametrisierten Flugzeugentwurf am Beispiel (un-)konventioneller Fluggeräte. Er stellt eine Möglichkeit der nahezu zeitgleichen, virtuellen Flugzeugentwicklung für konventionelle und im Speziellen für unkonventionelle Fluggeräte, unter Berücksichtung diverser, vom Entwurf bis hin zur Fertigung beteiligter, Disziplinen, Prozesse und Einrichtungen dar.
Zur weiteren Reduzierung der Entwicklungszeiten und Entwurfsrisiken im Flugzeugbau, wird mit der vorliegenden Dissertation eine Parallelisierung der Entwicklungsabläufe untersucht. Da hierfür in sämtlichen Entwicklungsbereichen Daten der entsprechenden anderen Bereiche benötigt werden, werden diese parametrisiert und in globale Abhängigkeit zueinander gesetzt.
Zur Untersuchung der Parametrisierungsmöglichkeiten wird zunächst der Datenfluss in typischen, modernen Luftfahrtunternehmen aufgezeigt und im Nachhinein eine Philosophie zum dokumentgestützten parallelen Entwurf aufgezeigt. Zur Steuerung der parametrisierten Konstruktionsdaten wurde eine Schnittstelle programmiert, mit deren Hilfe sämtliche Design- und flugmissionssteuernde Parameter verarbeitet werden.
Zur frühzeitigen Systemintegration wurde ein zusätzlicher Entwicklungsschritt eingeführt, der gerade bei unkonventionellen Aufgaben hilft, das Systemwissen der Systemlieferanten zu einem frühestmöglichen Zeitpunkt abzurufen. Dieser Schritt beinhaltet eine Aufteilung der eigentlichen Entwurfsaufgabe in zwei unabhängige Teilaufgaben, von den eine eine konventionelle Entwicklung darstellt, in welcher das Systemwissen leichtmöglichst platziert werden kann.
Die anschließende Vereinigung beider Aufgaben, kann durch die einfache Parametrisierung der Geometrien ebenso leicht durchgeführt werden, wie späte Änderungen im Entwicklungsprozess.

Basierend auf dieser Philosophie wurde ein paralleler Entwicklungsablauf über die Disziplinen Entwurf, Konstruktion, Dokumentation und Fertigung für ein konventionelles, wie auch ein unkonventionelles, Kleinflugzeug aufgezeigt.
Die Verfahren selbst richten sich nach standardisierten Richtlinien, welche auch bei Großunternehmen zum Einsatz kommen, wobei die Entwicklungszeit erheblich verkürzt werden kann.
Abschließend werden die Vor- und Nachteile dieses neuen Verfahrens erläutert.
Die sowohl das computerunterstützte Design als auch das Produktmanagement einschießende Arbeit beschäftigt sich mit einer auditierfähigen Entwicklungslösung für kleine und mittelständische Unternehmen, die Kleinflugzeuge in geringer Stückzahl mit hoher Flexibilität entwerfen. Aber auch Großunternehmen können, bedingt durch in der Luftfahrt vereinheitlichte Entwicklungsschritte von dieser Dissertation profitieren.

Abstract

The disquisition on hand „Multidisciplinary dataflow in a development process in the aircraft design“ describes a completely parameterized aircraft design for (un-)conventional air vehicles. It shows the possibility of a simultaneous and virtual airplane development for conventional and specially unconventional aircrafts with respect to miscellaneous disciplines, processes and facilities from design to manufacturing.
For a further reduction of the development time and risk in the aircraft design the disquisition on hand examines the possibility of parallelisation of several development processes. To provide each design team development data, needed in time, the dates were parameterised and set into global dependency.
In order to examine the parameterisation facilities a dataflow in a typical and modern company was stated and ex post the philosophy explained above was fitted into the parallel and document based design process. Additionally an interface was established to control the design dominant parameters.
To give system integration especially for unconventional projects the chance for an early step into the aircraft design, the design task was split up into two different tasks, into a conventional as well as an unconventional aspect. This step allows system suppliers to provide their special know-how in an earlier state of the development phase. The following merge of both tasks is easily supported by the parameterisation and allows late design changes as well.
On base of this philosophy a simultaneous development process, including the disciplines design, engineering, documentation and production, is stated for a conventional as well as for an unconventional small airplane.

The procedures themselves act in accordance with standards used by large concerns and it was stated that the development time therefore can be reduced significantly.
Advantages and disadvantages on this new procedure are shown at the end.
The both computer aided design and product management including disquisition deals with a audit compatible development solution for small and medium-sized business companies, that design small airplanes in low but flexible production rates. But even large concerns can use this disquisition due to equal aviation development standards.

Seite 98

Das Einbinden des von Baltus entwickelten und patentierten HESYs erlaubt dagegen einen papierfreien Arbeitsplatz, welcher bis zum gegenwärtigen Zeitpunkt einmalig sein dürfte.
Die Funktionsweise des am Institut durch Umprogrammierung von SmarTeam und HESY etablierten Datenflusses lässt sich leicht erläutern:
Ein elektronisches Dokument einer Partei 1 wird zunächst mit der elektronischen Signatur versehen (in Abbildung 60 eine ELA) und direkt im Anschluss gegen Manipulation geschützt. Durch den privatem Schlüssel (die **User-Identification**) der Partei 1 und ihrer Unterschrift, die sie im PDM-System über das HESY-PAD zu leisten hat, wird das geschützte Doukment eingepflegt.
Möchte sich eine Partei 2 versichern, ob es sich hierbei um eine Fälschung handelt, so kann die geleistete Unterschrift ausgelesen und genauso wie eine Unterschrift auf einem Papierdokument forensisch untersucht werden (Näheres siehe Tholl).

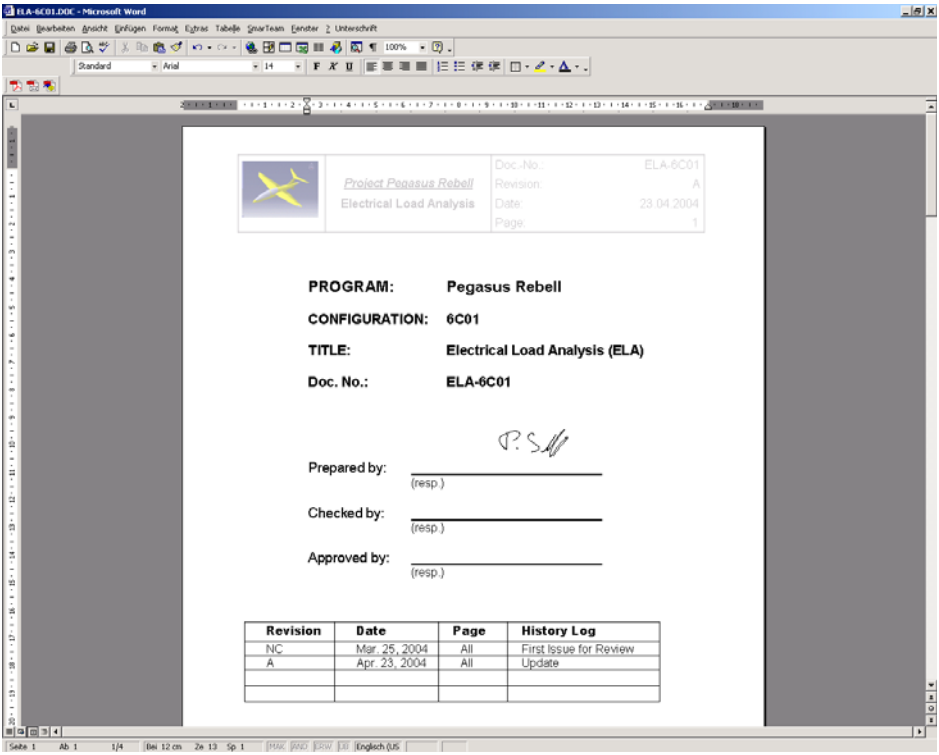


Abbildung 60: Einfügen einer elektronischen Unterschrift in ein Word-dokument

Dabei ist der grundlegende Aufbau des HESY-PADs sehr einfach: Durch vier Sensoren auf einer Unterlage, werden elektronische Signale an eine Schnittselle geleitet. Wird Druck auf diese Platte ausgeübt, so ändert sich das elektronische Signal gleichermaßen. Wird der Signal- und damit der Druckverlauf über der Zeit aufgetragen (Abbildung 61), so ergibt sich ein einzigartiges Muster, das zur Unterschriftenerkennung herangezogen werden kann. Da dieses Patent bereits gerichtliche Anerkennung [b-1]geniest, ist es ein idealer Kandidat für eine rein elektronische Datenverwaltung.
In Zusammenarbeit mit Baltus, Tholl und Greiner [g-3] wurde ein Szenario für einen möglichen Datenfluss entwickelt. Dabei wird das HESY-Signal mit den für diese Arbeit entworfenen Dokumenten sowie mit dem PDM-System selbst in Verbindung gebracht.
Wird ein Dokument von mehreren Personen unterzeichnet, so wird es zunächst mit der ersten Unterschrift geschützt; bei jeder weiteren zum Einfügen der elektronischen Unterschrift geöffnet und daraufhin wieder geschützt. (Es kann sich ja schließlich ein größerer Zeitraum zwischen den einzelnen Aktionen befinden.)

Der Umgang mit dem Ein- und Auspflegen, bzw. mit dem Einfrieren und Auftauen von Dokumenten verhält sich auf PDM-Ebene ähnlich. (‚Auftauen' soll den umgekehrten Vorgang von ‚Einfrieren' bezeichnen. Ein ‚aufgetautes' Dokument kann wieder geändert bzw. ergänzt werden.)
Allerdings werden hier zusätzlich die Unterschriften durch ein zusätzliches HESY-Modul auf Authentizität geprüft. Dazu ist jede Person angewiesen, einmalig mehre Unterschriften zu leisten, über die die aktuell Getätigte abgeprüft wird. Dies geschieht mit überraschender Genauigkeit, da die menschliche Unterschrift selbst nach einem Schlaganfall noch geleistet und auch wieder erkannt werden kann.
Abbildung 62 zeigt das Auftauen eines Dokuments in Verbindung mit der elektronischen Unterschrift. Das Einfrieren der Daten erfolgt nach gleichem Prinzip. Benutzer können durch diesen Mechanismus nicht nur erkannt, sondern es kann auch gleichzeitig geprüft werden, ob diese Person zum Kreise der Zulässigen für diese Unterschriftenleistung gehört.

Durch diese spezielle Form der Unterschriftenintegration in ein PDM können unterschiedlichste Software-Dokumente eingepflegt werden. Dieses Vorgehen ist dabei nicht mehr auf zweidimensionale Dokumente beschränkt. Mehrdimensionale Dokumente wie die DDs können nun auch als Urkunden herangezogen werden (vergleiche Abbildung 50, Abbildung 51 und Abbildung 59).

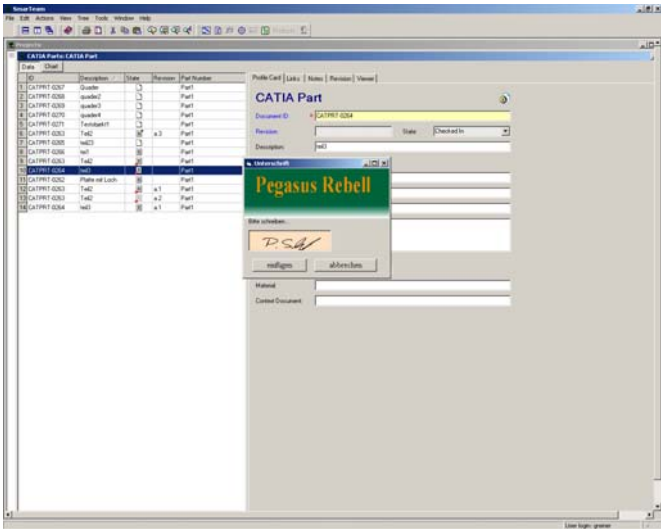


Abbildung 62: Unterschriftenmaske des HESY-Pads in Verbindung mit SmarTeam

United States General Accounting Office
(US-Rechnungshof, Auszüge)

http://www.gao.gov/new.items/d02687t.pdf

Testimony

Before the Subcommittee on Technology and Procurement Policy, Committee on Government Reform

House of Representatives

GAO

NATIONAL PREPAREDNESS

Technologies to Secure Federal Buildings

Statement of Keith A. Rhodes, Chief Technologist

For Release on Delivery Expected at 2:00 EDT Thursday, April 25, 2002

Die Studie wurde 1:1 von den u.a. Organisationen übernommen.

www.it-isac.org/documents/securing_federal_buildings.pdf

http://news.findlaw.com/hdocs/docs/gao/fedbldsec42502rpt.pdf

http://transit-safety.volpe.dot.gov/.../Additional/
GAO_Technologies_to_Secure_Federal_Bldgs.pdf

Table 1 provides a high-level description of access control technologies that can be deployed to protect federal facilities. Attachment I describes the technologies in greater detail.

Table 1: Access Control Technologies (Auszüge)
Technology

How the technology works
Effectiveness, Performance factors, User acceptance

Page 10 GAO-02-687T

Biometrics

Fingerprint scan
Patterns of fingertips are captured and compared Reliable Dirty, dry, worn fingertips
Medium, some resistance based on association with law enforcement

Hand geometry
Dimensions of hand and fingers are measured and compared
Fewer unique characteristics measured Injuries and jewelry
Good, but may require minimal training

Retina scan
Patterns of blood vessels on retina are captured and compared
One of most accurate biometrics
Hardest to use of biometric technologies Considered intrusive

Iris scan
Patterns of iris are captured and compared
One of most accurate biometrics Lighting and movement
Medium, some resistance based on sensitivity of eye

Facial recognition
Facial features are captured and compared
Dependent on lighting, positioning, updating reference template
Environmental factors
Good, but some concern about possible misuse

Speaker recognition
Cadence, pitch, and tone of vocal tract are captured and
Compared Better suited for other applications
Environment, inconsistencies, and quality of equipment
Good

Signature recognition
Rhythm, acceleration, and pressure flow of signature are captured and compared
Better suited for other applications
Erratic signatures
Good

Page 11 GAO-02-687

Keypad entry systems
Require users to enter passcodes
Substantially more secure if used in conjunction with access card system
Users may forget passcodes; vulnerable to malfunction and vandalism
Good

(Anmerkung Baltus: Unterschrift und PIN-Pad gehören zu den beliebtesten und sichersten Verfahren. Nicht berücksichtigt (da zu dem Zeitpunkt unbekannt) die Erfassung der Tippdynamik. Sign-n-Type erfasst mit nur einem Sensorpad die PIN-Ziffern, die Tipp- und Schreibdynamik!)

Biometrics

Page 3
6 GAO-02-687T

Signature recognition authenticates the identity of individuals by measuring their handwritten signatures. The signature is treated as a series of movements that contain unique biometric data, such as personal rhythm, acceleration, and pressure flow. Unlike electronic signature capture, which treats the signature as a graphic image, signature recognition technology measures how the signature is signed.

In a signature recognition system, the user signs his or her signature on a digitized graphics tablet or personal digital assistant. The system analyzes signature dynamics such as speed, relative speed, stroke order, stroke count, and pressure. The system compares not merely what the signature looks like, but also how it is signed. The technology can also track each person’s natural signature fluctuations over time. The signature dynamics information is encrypted and compressed and can then be stored in a database system, smart card, or token device. The stored template size is 1,500 bytes.

The use of signature recognition for access control seems fairly limited. A proficient "forger" is quite capable of selectively provoking false accept identifications for individual users.

The typical verification time is from 4 to 6 seconds. Several performance factors may impede signature verification. These include a user signing too quickly, a user having an erratic signature, a signature that is particularly susceptible to emotional and health changes, and using different signing positions.

Attachment I—Access Control Technologies:

Biometrics (Seite 36)

Signature Recognition

Signature recognition technology used to secure access to a handheld PC.

Source: Bio4.

Signature recognition system using a write pad.

Source: Hesy.

How the technology works, **Effectiveness**, **Performance factors**

Signature recognition authenticates the identity of individuals by measuring their handwritten signatures. The signature is treated as a series of movements that contain unique biometric data, such as personal rhythm, acceleration, and pressure flow. Unlike electronic signature capture, which treats the signature as a graphic image, signature recognition technology measures how the signature is signed.

In a signature recognition system, the user signs his or her signature on a digitized graphics tablet or personal digital assistant. The system analyzes signature dynamics such as speed, relative speed, stroke order, stroke count, and pressure. The system compares not merely what the signature looks like, but also how it is signed. The technology can also track each person's natural signature fluctuations over time.

The signature dynamics information is encrypted and compressed and can then be stored in a database system, smart card, or token device. The stored template size is 1,500 bytes.

8. Deutscher EDV-Gerichtstag vom 15. bis 17. September 1999

Authentifikation und elektronische Unterschrift Abschlußbericht

Kurzbericht des Arbeitskreises „Authentifikation“

Der Arbeitskreis Authentifikation behandelte Aspekte der Identifikation mit elektronischen Mitteln. Dabei kommen insbesondere biometrische Verfahren in Betracht. Aus der Kriminalistik ist bekannt, daß jeder Mensch individuelle, unveränderliche Merkmale hat, beispielsweise Fingerabdruck oder Stimme, wie auch charakteristische Verhaltensweisen, z.B. Tastaturanschlag oder Unterschrift. Es liegt nun nahe, diese individuellen Eigenschaften, die man sich nicht merken muß und die jeder mit sich herumträgt, zur Zugangskontrolle auch in Netzwerken heranzuziehen. Im Vorjahr (EDV-GT 98) wurden dafür verschiedene biometrische Systeme vorgestellt: Fingerabdruck, allgemeine körperliche Merkmale (Kontur, Iris, Stimme) Anschlagcharakteristik an der Tastatur. Daran wurde beim EDV GT 99 angeknüpft.

Üblicherweise erfolgt die Authentifikation eines Dokuments durch die eigenhändige Unterschrift. Zunächst wurden daher die Genauigkeit und Überprüfbarkeit des klassischen Authentifikationsmittels Unterschrift dargestellt. Dazu hat Herr Dr. Hecker vom Bundeskriminalamt ausgeführt:

Im Zeitalter der elektronischen Signatur behalte die manuell geleistete Unterschrift wahrscheinlich noch für viele Jahrzehnte ihre Bedeutung als individuelle Willenserklärung im Rechtsverkehr. Damit werde sie – und die anderen Formen der Handschrift (Textschrift/ Druckschrift) – auch weiterhin eine herausragende Rolle in der Forensik spielen, eben wegen ihrer Personenidentifizierungseigenschaft.

Zwar spielten auch in der kriminalistischen Schriftuntersuchung Aspekte der Mustererkennung zunehmend eine Rolle, jedoch vollziehe sich das Gros der Urheberidentifizierungen nach wie vor auf der Ebene des klassischen Methodenspektrums.

Neben einer Darstellung dieser Vorgehensweisen und einem Blick auf die nahe Zukunft unter dem Gesichtspunkt des aktuellen Forschungsstandes sollten insbesondere auch die Grenzen der Urheberidentifizierung über die Handschrift aufgezeigt werden. An einer Reihe von Falldarstellungen wurde darüber hinaus versucht, dem Benutzer von Schriftgutachten einige Kriterien

an die Hand zu geben, die ihm die Unterscheidung von methodisch korrekten und unseriösen Gutachten erleichtern.

Natürlich kann auch das klassische Mittel der Authentifikation, nämlich die eigenhändige Unterschrift, elektronisch umgesetzt werden. Herr Baltus hat ein dafür geeignetes, marktreifes System „Hesy“ im Arbeitskreis vorgestellt. Dabei wird der mit der Abgabe der Unterschrift verbundene Druckverlauf an einem beliebigen Stift über Wägezellen piezoelektrisch in Echtzeit erfaßt, abgespeichert und mit einem hinterlegten entsprechenden Referenzmuster verglichen. Innerhalb einer vorgebbaren Toleranzschwelle wird die Unterschrift akzeptiert, bei Überschreitung wird sie verworfen.

Neben individuell-strukturellen und biologischen Merkmalen können auch auf technischem Weg charakteristische Merkmale aus einem Dokument ermittelt und umkehrbar eindeutig zugeordnet werden. Die Bezeichnung elektronische oder digitale Unterschrift wird für unterschiedliche Vorgänge verwendet. Es kann darunter einerseits die in üblicher Weise geleistete Unterschrift mit elektronischer Meßwerterfassung und digitaler Umsetzung verstanden werden, wie sie dem Verfahren HESY zugrunde liegen. Unter elektronischer Unterschrift kann aber auch die elektronische Signatur verstanden werden. Dabei handelt es sich um die Verschlüsselung eines gehashten Dokuments. Der Hash-Vorgang erzeugt aus einem Dokument beliebiger Länge ein Unterdokument bestimmter, einheitlicher Länge. Dieses so definierte Unterdokument wird in üblicher Weise asymmetrisch ver- und entschlüsselt (je ein öffentlicher und privater Schlüssel, mit dem privaten Schlüssel wird ver-, mit dem öffentlichen Schlüssel wird entschlüsselt). Bei Identität des gehashten Unterdokuments gilt die Echtheit des Dokumentinhalts als bestätigt. Das System erfordert die Vergabe und Verwaltung von individuell vergebenen Schlüsselpaaren durch sog. „Trust Center“.

Die Bezeichnung „Unterschrift“ für diesen Vorgang erscheint unglücklich gewählt, denn „unterschrieben“ im vertrauten Sinn des Wortes wird dabei nichts. Es handelt sich vielmehr um einen rein technisch erzeugten, entindividualisierten Vorgang, der nur über einen privaten Schlüssel eine persönliche Zuordnung erhält. Der Schlüssel ist in der Regel auf einem Datenträger (z.B. einer Chipkarte), gespeichert, der Zugang erfolgt üblicherweise durch eine PIN (mit den bekannten Unsicherheiten). Dies erfolgt ebenso automatisch wie beispielsweise das Einscannen einer Unterschrift, was vom Oberlandesgericht Karlsruhe als ungenügend für das Einlegen eines Rechtsmittels erachtet wurde.

Abschließend hat Prof. Rüßmann rechtliche Aspekte bei der Umsetzung der Unterschrift in digitaler oder elektronischer Form dargelegt und dabei die Frage aufgeworfen, ob dort, wo rechtliche Regelungen heute die Schriftform

verlangen, auch elektronische Dokumente zur Formwahrung geeignet sein können. Das hält man in der deutschen Doktrin im allgemeinen für ausgeschlossen und ruft nach dem Gesetzgeber zur Schließung der Regelungslücke. Tatsächlich bereitet das Bundesjustizministerium eine gesetzliche Regelung zur sog. Textform vor. Der Referentenentwurf ist dabei bemüht, bei jedem Schriftformerfordernis des materiellen Rechts und des Verfahrensrechts festzuschreiben, ob seinem Zweck nicht auch durch die Textform genügt werden könne. Auf internationaler Ebene ist man da weniger zurückhaltend.

Prof. Rüßmann berichtete von einer Diskussionsrunde, die die Haager Konferenz für Internationales Privatrecht in Genf zu Fragen des elektronischen Geschäftsverkehrs kurz vor dem EDV-Gerichtstag veranstaltet hatte. Die dortige Empfehlung zur Behandlung der Schriftformerfordernisse in Sonderheit in der internationalen Handelsschiedsgerichtsbarkeit ging dahin, dass der Rechtsanwender entscheiden möge, ob die elektronischen Möglichkeiten zur Sicherung der Authentizität elektronischer Dokumente den traditionellen Schriftformerfordernissen funktional äquivalent seien, und bejahendenfalls die elektronischen Dokumente als zur Schriftformwahrung ausreichend ansehen möge.

Mit eben diesem Ansatz der funktionalen Äquivalenz untersuchte alsdann Prof. Rüßmann die Wahrung der der traditionellen Unterschrift zugeschriebenen Funktionen des Abschlusses der rechtsgeschäftlichen Erklärung, des Beweises des Inhalts und der Urheberschaft einer Erklärung sowie der Warnung vor dem übereilten Abschuss eines wichtigen oder gefährlichen Geschäfts durch die vorgestellten elektronischen Möglichkeiten. Sein Fazit: Mit Blick auf die Abschluss- und die inhaltsbezogene Beweisfunktion sei die elektronische Signatur dem unterschriebenen Schriftstück überlegen. Die urheberbezogene Beweisfunktion erreiche die elektronische Signatur dann, wenn der Zugang zur Signatur über biometrische Verfahren erfolge. Das Erreichen der Warnfunktion setzte psychologische Vergleiche der Wirkung einer handschriftlichen Unterzeichnung mit der Wirkung des bei der elektronischen Signatur zu beobachtenden Verfahrens voraus. Er jedenfalls fühle sich schon durch die Eingabe einer relativ komplizierten Passphrase bei PGP hinreichend gewarnt. Mit HESY als biometrischem Zugangsverfahren zur elektronischen Signatur sei schließlich die handschriftliche Unterzeichnung 1 zu 1 abgebildet, so dass bei diesem Verfahren die funktionale Äquivalenz mit Blick auf alle Funktionen der Schriftform vollständig gegeben sei.

Arbeitsrechtliches aus dem Bund-Verlag: Elektronische Unterschriften (Auszug)

Von Gerda Kneifel und Albrecht Ude
ZEIT.DE

Die Zeitschrift Computer-Fachwissen des Bund-Verlages in Frankfurt/M weist darauf hin, dass dieses Verfahren für die Mitarbeiter Risiken birgt. Denn ein absoluter Schutz vor Missbrauch der elektronischen Unterschrift ist nicht gegeben. 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: Computer-Fachwissen fuer Betriebs- und Personalraete
Ausgabe 05/2001, Bund-Verlag
http://www.bund-verlag.de/aib/index.html

Anmerkung Baltus:
Da scheint es sehr sinnvoll, die „Elektronische Blaupause“ zu nutzen. Ein Ausdruck auf Papier, diesen auf Sign-n-Type gelegt und unterschreiben. Das ist dann im Bedarfsfalle der Beweis vor Gericht.

Smart Traveler - Travel tactics for a changing world
Your Body, Your Badge (Extract)

By Dana Hawkins

National Geographic Traveler July/August 2002, page 15

When guests register at Hotel Consul in Bonn, Germany, the form, pressure, and speed of their signatures are filed electronically.

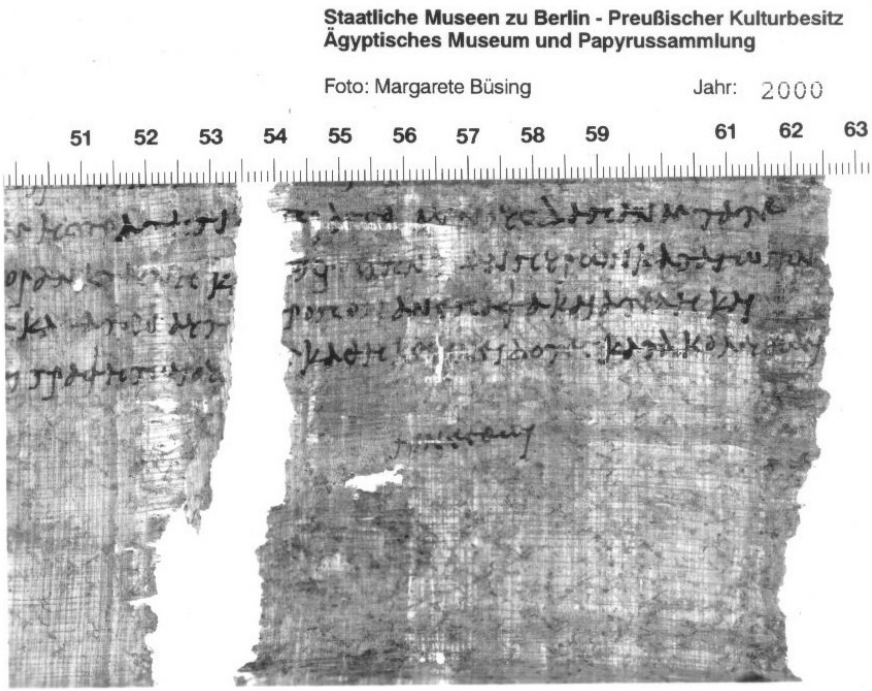
Season pass holders to Disney World theme parks in Orlando enter by passing through turnstiles equipped with two-finger geometry readers, and several cruise lines are considering tightening security by adding biometric data to the photo ID on boarding passes.

"It would ensure that the same people getting on are those who got off," says Ted Thompson, executive vice president of the International Council of Cruise Lines. HA gangway guard might be fooled by someone sneaking on in a baseball cap and sunglasses."

Die Unterschrift der Königin

Ein Berliner Papyrus trägt einen authentischen Schriftzug Kleopatras VII.

von Jörg Dendl
http://www.dendlon.de/Kleopatra.html



(bpk / Ägyptisches Museum und Papyrussammlung, SMB / Margarete Büsing)

Dieser Papyrus, der in den Räumlichkeiten des Ägyptischen Museums im Rahmen der Sonderschau „Die Handschrift der Kleopatra“ vom 26. Oktober bis zum 26. November 2000 ausgestellt war, trägt, so der an der Universität von Groningen (NL) arbeitende belgische Papyrologe **Peter van Minnen** in der Pressekonferenz, das Wort „**genesthoi“** (So soll es geschehen), geschrieben von der letzten Königin Ägyptens, Kleopatra VII. (69 - 30 v.Chr.). **Mit dieser Unterschrift** bestätigte die Königin eine Reihe von Steuer- und Zollerleichterungen für **Publius Canidius Crassus**, einen römischen General und Gefolgsmann ihres Mannes **Marcus Antonius** (82 - 30 v. Chr.).

Verlag Jörg Dendl, Hochburger Str. 25, 79312 Emmendingen,
Tel.: 07641/9376820, info@dendlon.de

René Baltus über

Biometrie und Sign-n-Type

Schrifterkennung:
Wer unterschreibt, der lebt (Auszug)

Von René Baltus

Spektrum der Wissenschaft, Magazin | 01.08.2003
http://www.spektrumverlag.de/artikel/830020

Eine persönliche Handschrift lässt sich fälschen, jedoch niemals der Vorgang des Unterschreibens. Allein der Druck des Stifts auf das Papier zeigt individuelle Verlaufsmuster.

Ein Handschlag zum Abschluss einer Geschäftsverhandlung mag im Bekanntenkreis noch angehen, doch schon das römische Zivilrecht forderte 533 n. Chr. die persönliche Unterschrift unter einem Vertrag als Nachweis der Einigung. Dass dieses Vorgehen schon im biblischen Palästina üblich war, bezeugt der Prophet Jeremias etwa 626 v. Chr. (Jeremias 32, Vers 12): „Und ich gab den Kaufbrief Baruch, dem Sohn Nerijas, des Sohnes Machsejas, vor den Augen meines Vetters Hanamel und vor den Augen der Zeugen, die den Kaufbrief unterschrieben hatten, vor den Augen aller Judäer, die im Wachhof saßen."

Auch geschickte Fälscher können daran nichts ändern: Die handschriftliche Signatur, mit Tinte und auf Papier geleistet, gilt immer noch als sicherstes Verfahren.

Es gibt auch multimodale Systeme!

Von René Baltus

c't 11/2002, S. 114: Biometrie
Leserforum
20. Mai 2002 18:47
(Nach Erstveröffentlichung redaktionell leicht überarbeitet)

Leider wird immer wieder vergessen – oder „vergessen“ – dass es auch multimodale Systeme gibt! Hierzu zählt die seinerzeit von der Fa. Bio-ID aus Berlin angebotene Kombination von Stimme, Gesicht und Lippenbewegungen.

Ein weiteres multimodales System ist das **H**andschriften-**E**rkennungs-**Sy**stem **HESY**! Es verbindet die unfälschbare vierdimensional erfasste eigenhändige Unterschrift mit der herkömmlichen PIN, wobei die PIN zusätzlich mit ihren personentypischen Tippdynamik erfasst wird. Damit ist gemeint, dass zur Erfassung des Tipprhythmus' und des Tippdruckes das gleiche Unterschriftspad genutzt wird. Den vier Wägezellen ist es nämlich „egal“, welche Dynamik sie aufnehmen – die Tipp- oder die Unterschriftsdynamik (oder beide).

Das hat zur Folge, dass der Nutzer als ersten Schritt einer Verifikation seine Karte in den Leser steckt, dann seine PIN eintippt (die Software erkennt auch zuerst die richtige Zahl), danach wird dann die Dynamik geprüft. Stimmt dieses in etwa mit den zu vergleichenden Daten überein, wird noch unterschrieben. Nun dürfen die zwei Erkennungsraten jeweils schlechter sein als bei nur einem Verfahren, mit beiden zusammen wird der Nutzer bestens erkannt! Das Überlisten jedoch dürfte mit vertretbarem Aufwand nicht zu schaffen sein. (Theoretisch geht ALLES – das bedarf keiner Diskussion mehr!)

Ferner hat dieses Verfahren den erheblichen Vorteil, dass automatisch eine Lebenderkennung, eine Willenserklärung und ein Notsystem (wenn ein Finger verletzt ist, gibt's keine Unterschrift und auch keine dynamische PIN) zur Verfügung steht, das die Eingabe einer herkömmlichen NotPIN zulässt. Es bedarf keines weiteren Tastaturblockes mehr. Diejenigen, die weiterhin ihre herkömmliche PIN (ohne Biometrie) eintippen wollen, nutzen ebenfalls dasselbe Pad.

An einem Outdoor-Geldautomaten stehen damit Besitz (Karte), Wissen (PIN) und Biometrie (Tippdynamik) zur Verfügung! Für den Kunden UND die Bank eine höhere Sicherheit. Selbst wenn die PIN ausgespäht wird, hat der Dieb erhebliche Probleme, die Tippdynamik nachzuahmen. An einem Indoor-Geldautomaten kann dann noch zusätzlich unterschrieben werden; das Fälschen der Unterschriftsdynamik ist überhaupt nicht zu schaffen!

Dass die Tippdynamik von vier bis acht Zahlen alleine nicht die Welt verbessern wird, ist mir völlig klar. Aber es wird der erste Schritt zu mehr Sicherheit sein. Multimodale Systeme werden (wegen der Schwächen einzeln eingesetzter biometrischer Verfahren) einen erheblichen Beitrag zu einer höheren Sicherheit bringen.

Bestens geeignet auch für einen Personalausweis – da wird der Bürger dann gebeten, sein Geburtsdatum einzutippen, danach wird unterschrieben. Allerdings kann man dynamische biometrische Merkmale nicht erzwingen. Nebenbei bemerkt, erfüllt das System auch schon alle Erfordernisse einer einfachen elektronischen Signatur – alleine schon deshalb, da nach Sig-Verordnung Besitz und Wissen oder Besitz und ein oder mehrere biometrische Merkmale erforderlich sind!

Ist Biometrie nur Fingerabdruck? (Leicht modifiziert)

Von René Baltus

23. Februar 2002 17:37
www.heise.de/ct/foren/S-Ist-Biometrie-nur-Fingerabdruck/forum-26195/msg-1457733/read/

Ist Biometrie nur Fingerabdruck?
René Baltus 15. Februar 2002 13:18
Leserbrief auf Telepolis:
Geldabheben per Fingerabdruck bleibt Zukunftsmusik
Stefan Krempl 11.02.2002
http://www.heise.de/tp/deutsch/html/result.xhtml?url=/tp/deutsch/inhalt/te/11819/1.html&words=Krempl

Der modifizierte Leserbrief auf Stephan Krempls Artikel passt auch bestens hierher!

Die Sparkassenorganisation hält Biometrie im Bankenumfeld frühestens in zehn Jahren für einsatzreif – die Probleme sind prototypisch für große Anwendungsszenarien. Ist Biometrie nur Fingerabdruck? In den Köpfen einiger Verantwortlicher offensichtlich: JA! Nur Biometrie kann auch etwas ganz, ganz Feines sein! Man nehme nur die eigenhändige Unterschrift. Dass Fingerabdrucksensoren flächendeckend an ÖFFENTLICHEN Geldautomat kommen werden, haben seriöse Biometer nie behauptet. Grund: diese Sensoren sind viel zu empfindlich und leichte Beute für Vandalen. Man denke nur wie lange es dauern wird, bis der erste Kaugummi daran klebt?! Ferner ist gut vorstellbar, dass viele Nutzer nicht Ihren Finger dahin legen wollen, wo schon tausend andere dies getan haben!

Daher sind sich unabhängige Fachleute darin einig, dass an derlei Geldautomaten nur BERÜHRUNGSLOSE biometrische Verfahren zur Anwendung kommen werden! So z.B. ein Irisscanner oder ein Gesichtserkenner. Daher ist die Pauschalisierung des Herrn Thiel etwas gewagt. Ist er sich dessen bewusst, dass er eine junge und neue Technologie mit derlei Prognosen in den Staub tritt? Eine Technologie, die ursprünglich in Deutschland stark vorangetrieben wurde? Wo deutsche Unternehmen und Entwickler führend waren?

Ist es nicht gut vorstellbar, dass an INHOUSE-Geldautomaten biometrische Verfahren zur Anwendung kommen? So z.B. ein Unterschriftenprüfer? Dann hat der Kunde auch noch eine Quittung aus Papier! Das kann er getrost mit nach Hause nehmen und abheften.

Dass die Biometrie immer mit „Wiedererkennen“ in Zusammenhang gebracht wird, ist ebenfalls kontraproduktiv! Ein papierenes Dokument, das auf einen Schriftprüfer gelegt wird, kann GLEICHZEITIG mit seinem elektronischen Pendant (z.B. ein ADOBE-Formular) eigenhändig unterschrieben werden! Damit steht dem Kunden/Bürger „sein“ abheftbares Papier, der Verwaltung, eben einer Sparkasse oder Stadtverwaltung, „ihr“ elektronisches Dokument zur Verfügung! Herz, was willst Du mehr?

Die unsichtbaren und somit unfälschbaren dynamischen Bestandteile der eigenhändigen Unterschrift werden untrennbar an BEIDE Dokumente angehängt! Auf dem Papier wie bisher, in der Datei mit digitalen Wasserzeichen – und beide haben die IDENTISCHEN Daten! Und beide können vor Gericht als Beweis dienen! (Siehe Expertise unter www.hesy.de.) Und beide werden erst NACHDEM die Unterschrift bestritten wurde von einem vereidigten Schriftsachverständigen, nach der Beauftragung durch den Richter, verglichen! Wie bisher! Gestritten wird zu 99% über die Inhalte eines Dokumentes, selten über die Unterschrift!

Das kann man als eine menschenwürdige Biometrie bezeichnen, gibt man doch seine Unterschrift niemals UNGEWOLLT ab! Ein eigenhändig geschriebenes Passwort oder eine eigenhändig geschriebene PIN noch weniger! Und letztere kann man, wie bisher, beliebig wechseln UND man darf sie NOTIEREN! Die seit langem von den Verwaltungen, öffentlichen sowie privaten, geforderten Kosteneinsparungen durch ein Workflowsystem sind damit leicht realisierbar! Die Verwaltungen bedürfen kein teures Archivieren der Papierflut mehr, dem Kunden/Bürger jedoch verbleibt sein Papier! Wie bisher!

Ferner darf darauf hingewiesen werden, dass es Schriftprüfungssysteme gibt, die auf dem GLEICHEN Erfassungsfeld auch die Eingabe einer PIN zulassen! Damit steht das von den Verbraucher- und Datenschützern geforderte Ersatzsystem (falls Finger oder Hand verletzt) zur Verfügung. Und wenn Herr Thiel (und der Kunde) es möchte, wird der Nutzer über seine ebenfalls personentypischen Merkmale Tipprhythmus und Tippdruck wiedererkannt! (Uralte Erkenntnis des Institutes für Bankeninformatik in Regensburg, Prof. Bartmann.) Durch derlei sogenannte „multimodale Systeme“ (hierzu zählt auch die Kombination Gesicht, Stimme, Lippenbewegung) werden die Wiedererkennungs- und Abweisungsraten erheblich verbessert! Durch derlei Systeme werden auch diejenigen in den Genuss der modernen Technik kommen, die keinen eindeutigen Fingerabdruck (man denke nur an Bauarbeiter) oder keine in etwa konstante Unterschrift haben!

Fest steht, dass die Unterschrift ein beliebtes biometrisches Merkmal ist, das keiner On-Line-Wiedererkennung bedarf! Ferner ist die bei vielen anderen Verfahren nötige gesonderte Erfassung überflüssig: der Kunde unterschreibt sowieso seine Kontoeröffnung! Und den Erhalt seiner PIN und den Erhalt seiner Scheckkarte! Und die Unterschriftenkarte! Und diese Papiere werden alle gescannt (für das Workflow) und dann als Papier archiviert (wg. der vor Gericht nutzbaren und erforderlichen eigenhändigen Unterschrift)! Nur durch Miesmacherei werden die einheimischen Interessenten davon abgehalten, die entsprechenden Programme weiterzuentwickeln. Daher sind mehrere Kreissparkassen gezwungen, amerikanische oder japanische Unterschriftenprüfer einzusetzen! Wie hatte die New York Times geschrieben? Deutschlands Unternehmen schaffen viele Arbeitsplätze – im Ausland!

Wie will ein Geldinstitut ein wirklich kostensparendes papierloses Workflowsystem einführen? Natürlich nicht mit dem Fingerabdruck alleine – da hat der Kunde ja kein Papier! Es geht doch nicht nur um Geldautomaten!!! Der Orgleiter eines großen Kölner Institutes hat mir versichert: „... mit tausend Schriftprüfern spare ich eine Million im Jahr ...“??!! Bei Kosten von 500,00 DM/Stück ist das ein ROI innert 6 Monate! Nur im Workflow und Dokumenten-Management-System! Und da ist noch kein einziger Kunde on-line wiedererkannt worden! Das kommt dann ganz langsam, mit ausgesuchten Kunden – und bringt noch mehr Einsparungen (siehe hierzu auch www.signotec.de)! Herz, was willst Du mehr?

Gar nicht zu reden von weiteren Entwicklungen, wie z.B. ein Home-Banking-„Volks“-Terminal, mit dem von zu Hause aus Bank- und Kaufaufträge eigenhändig unterschrieben werden! Natürlich sind die biometrischen Daten dann auf einer Chipkarte gespeichert! Und der Kunde hat ein Stück Papier zum Abheften! (wenn er denn will!) Er kann gerne auch eine PIN oder ein Passwort nutzen! Die darf er ja dann notieren! Das verstehen auch Tante Emma und Onkel Peter! Da wird keine 6 bis 8-stellige PIN benötigt! Und auch keine Belehrung! Da genügt „Plug and Play“! Auch Onkel Peter kann einen Netzstecker und den Stecker für das Telefon platzieren! Und damit kann er auch noch telefonieren! Herz, was willst Du mehr??

Ach so, ich habe überhaupt nichts gegen den Fingerabdruck! Nur sollte er sogenannten „Micropayments“ vorbehalten bleiben! Niemand wird eine Tageszeitung oder ein Buch, das Parkhaus oder die Straßenbahn mit einer Unterschrift bezahlen. Da eignet sich bestens die Chipkarte mit Fingerabdrucksensor! Oder eine Gesichtserkennung. Für Macropayments kommen aber nur Schriftenprüfer zum Einsatz – ab welchen Summen und die Höhe der erlaubten Summe sollte der Kunde selber festlegen können!

Auch wenn es vielen weh tut, nicht alle Bürger oder Kunden stehen dem Fingerabdruck positiv gegenüber! Schon gar nicht, wenn sie gelesen haben, dass der Eine oder der Andere mittels Kunstfingern aus Silikon (vom Baumarkt nebenan) überlistet wurden. Es soll auch vorgekommen sein, dass die Lebenderkennung von Hobbyhackern mittels Folien überlistet wurde! Siehe C´T, Heft 17/1999! Das dürfte aber bei eigenhändig geschriebenen PIN und Passwörtern und der Unterschrift einen erheblich größeren Aufwand erfordern! Abgesehen davon, dass man Fingerabdrücke ununterbrochen ungewollt abgibt! Schlimmstenfalls volltrunken unter freundlicher „Mithilfe“ von „Freunden“! Dann werden im Vollrausch digital signierte Schuldscheine produziert! Es stehen ja Chipkarte und Fingerabdruck „freiwillig“ zur Verfügung! Und digitale Signaturen sind 100% sicher, laut Gesetz!

Immer wieder wird auf den „armen“ Wiedererkennungs- und Abweisungsraten herumgeritten! Da MUSS wieder alles 150% funktionieren! Warum? Für 50 Euro wird niemand einen Überlistungsversuch starten, die habe ich sogar ungeschützt auf der Geldkarte, es lohnt also nicht. Dann kann das sogenannte Kennfeld zur Wiedererkennung ganz weit eingestellt sein! Bei höheren Summen wird das Kennfeld entsprechend immer enger. Es wird also immer schärfer geprüft! Werden für 5000 Euro bei manchen Personen drei Unterschriften verlangt, sieht jeder wie sicher die Sache ist. Muss er aber für 50 Euro dreimal unterschreiben, wird er berechtigterweise sehr zornig sein – wäre ich auch! Das ganze nennt sich dann: „Wertmäßig einstellbares Kennfeld“!

Das alles führt dann zu den sogenannten „Baltus-Axiomen“:

- Die Biometrie wird die Welt nicht verbessern!
- Es gibt kein alleinseligmachendes biometrisches Verfahren!
- Es gibt aber intelligente Kombinationen biometrischer Verfahren!

Siehe auch:
Telepolis: Vergleich von Fingerabdrücken kein wissenschaftliches Verfahren. Florian Rötzer 15.01.2002
http://www.heise.de/tp/deutsch/inhalt/co/11572/1.html
Erstmals hat ein amerikanischer Richter die Daktyloskopie nicht als Beweismittel in einem Mordprozess zugelassen, weil sie den Anforderungen der Wissenschaftlichkeit nicht entspricht.

Hat der Fingerabdruck ausgedient? Angelika Jockers 05.10.2001
http://www.heise.de/tp/deutsch/inhalt/lis/9711/1.html
Während der Fingerabdruck in Deutschland zur Verbesserung der inneren Sicherheit in Konjunktur steht, werden in den USA Zweifel an der Zuverlässigkeit immer lauter.

Sign and Type vs. Psylock

Von René Baltus

Dass der Tipprhythmus ein eindeutiges biometrisches Signal ist, hat die Uni Regensburg bewiesen.

Im Folgenden wird aus http://www.cefis.de/aussteller/psylock.htm zitiert.

„Die Psylock GmbH ist aus einem Forschungsprojekt der ibi research an der Universität Regensburg hervorgegangen. Das patentierte Psylock-Verfahren wurde mehrfach mit internationalen Innovations-Preisen ausgezeichnet."

Der Satz: „Zeige mir wie Du tippst und ich sage Dir, wer Du bist!" gilt uneingeschränkt für die Sign-n-Type-Unit.

Wesentliche Vorteile der Sign-n-Type-Unit sind jedoch:

- Wesentlich kleinere Abmessungen als eine PC-Tastatur
- Erfassung der kompletten Tippdynamik (damit ist auch der Tippdruck gemeint) mit bisher ungeschlagenen 1600 Dynamik-Werten/sec.

Dies dürfte mit der normalen PC-Tastatur wohl kaum zu realisieren sein. Die Vorteile haben zur Folge, dass wesentlich weniger Zeichen als „ein kurzer Satz" benötigt wird. Normalerweise reicht eine 6-stellige PIN aus; schon die herkömmliche 4-Stellen-PIN ist schwer zu knacken.

Das bereits vor 15 Jahren für die Erkennung der Unterschrift vorgeschlagene Verfahren des „wertmäßig einstellbaren Kennfeldes" gilt ebenfalls uneingeschränkt für die Erfassung und Auswertung der kompletten Tippdynamik mit der Sign-n-Type-Unit. Mit diesem Verfahren ist gemeint, dass für niedere Werte eine eher lasche Prüfung vorgenommen wird, für hohe Werte könnte es jedoch vorkommen, dass eine weitere PIN-Eingabe gefordert wird.

Die Sign-n-Type-Unit mit beliebig großen (oder kleinen) Schreib- und Tippflächen (normalerweise 9,0 cm x 5,8 cm) passt in fast jede herkömmliche Gegensprechanlage hinein. Ferner sind die Ziffern gegen bei Kindern beliebte Bilder wie Feuerwehr, Teddybär, Puppe, Ball, Auto, Haus, Kuchen, Kind, ein Bild von Vater, Mutter oder Oma zu ersetzen. Dann kann das Kind mit z.B. dem „Passwort" *Ball, Vater, Teddybär, Ball, Mutter* selbständig die Türe öffnen. Ein Ausspähen der kompletten Tippdynamik dürfte nahezu unmöglich sein.

„Jeder Mensch hat ein einzigartiges Tippverhalten. Getippter Text ist wie die Handschrift. **Psylock** macht mit Hilfe statistischer Methoden und Verfahren der künstlichen Intelligenz die „graphologische Analyse" einer Tippprobe."

Das kann ich nur unterstreichen, ich nehme jedoch klar Abstand von der Nutzung des Begriffes **„graphologische Analyse".** Eine derartige Analyse

mit einem Rechnerprogramm wird von seriösen Graphologen schon bei der Handschrift abgelehnt.
Auch die Unterschrift eignet sich, Gott sei Dank, nicht für eine derartige Analyse – sie wird zu routinisiert, automatisch und unbewusst geleistet. Der Satz „Zeige mir wie Du tippst und ich sage Dir, wer Du bist!“ soll ja wohl nicht in „Zeige mir wie Du tippst und ich sage Dir, **WIE** Du bist!“ verbogen werden. Es wäre auch furchtbar, wenn der Vorgesetzte zu Arbeitsbeginn nach der Eingabe des „kurzen Satzes“ vom Admin ein graphologisches Gutachten seines Mitarbeiters präsentiert bekäme.

Zitat aus http://www.graphologies.de/:

„Zweck dieser Seiten ist nicht die Erstellung eines Graphologischen Gutachtens.Das ist auf einer Internetseite oder mit einem Computerprogramm für den Laien nicht möglich.“

Und weiter:
„... und nicht mit Zeitschriften-Horoskopen oder mit dem Kaffeesatzlesen zu vergleichen ist.“

Die eigenhändige Unterschrift (Auszüge)

von Heinz Holzhauer, Athenäum Verlag Frankfurt 1973

(Kommentare in Klammern von René Baltus)

S. 45: In Rom erlaubte ein Gesetz aus dem Jahre 439 (!), daß der Testator sein Testament subskribierte *(wenn er den Inhalt vor den Zeugen geheimhalten wollte, Kaufleute unterschrieben Verträge!).*

S. 26: 12. Jahrh., Die Regelungsbedürftigkeit der Weitergabe der Siegel ergab sich aus der Tatsache, „...daß das Siegel nicht im gleichen Maße wie eine Namensunterschrift individuell charakteristisch war“ *(und auch noch immer nicht ist – das gilt auch für das digitale Siegel).*

S. 35: Schon im Mittelalter „...gewann unter Kaufleuten besonders früh die eigenhändige Subskription Bedeutung und verdrängte das Siegel als maßgebende Unterfertigung“. *(Die wussten schon, warum sie die Siegel abschafften; jetzt sollen sie wieder in elektronischer Form eingeführt werden. Warum?? Die vierdimensionale elektro-mechanische Aufnahme einer Unterschrift ist in den USA, Japan und Europa bereits an das digitale Zeitalter angepasst. Sie kann übergangslos übernommen werden.)*

S. 37: Der Fälscher konnte sich aber auch eigenmächtig oder listig einen echten Siegelstempel besorgen und damit die Falschurkunde siegeln. Ebendarum spielte die Siegelbewahrung *(Neudeutsch heißt das „Trust Center“)* eine so große Rolle und es gab zahlreiche Vorkehrungen, organisatorischer und technischer Art, die einen Mißbrauch des Siegels verhindern sollte. *(Dieses Problem besteht nach wie vor auch beim digitalen Siegel.)*

S. 42: Unterschrift von Kaiser Karl IV. 1354 unter zwei Urkunden für den Prager Bischoff.

S. 42: 1428 forderte der Lübecker Bürgermeister die Unterschrift unter einem Schuldschein.

S. 42: Zitat aus Spanngenberg, Urkundenbeweis: »Seit Mitte des 16. Jahrhunderts hört das Siegel wieder auf, ein unumgängliches Erforderniß der Originalisierung zu seyn«.

S. 43: August der Starke erließ 1724 eine Gerichtsordnung, nach der „...die Unterschrift alleine genügte“.

S. 55: Wenn aber der Sinn der Unterschrift darin liegt, dem Mangel des allographen Textes abzuhelfen, so muß sie grundsätzlich eigenhändig sein. *(Gilt verstärkt bei den elektronischen Medien!)*

S. 78: Der Sinn der Eigenhändigkeit dürfte zum Teil irrational in der **verstärkten Identifikation** des Ausstellers mit der Urkunde gesehen worden sein, die ihm psychologisch ein abschwören erschweren mochte. Der Sinn der Eigenhändigkeit wurde aber auch rational in dem spezifischen **Beweismoment** der Skriptur gesehen. *(Beides fehlt bei einem elektronischem Siegel.)*

S. 79: Bei der Untersiegelung war es gleichgültig, ob der Siegelinhaber das Siegel selbst anbrachte, oder, wie meist, von einem anderen anbringen ließ. **Der Siegelbesitz, nicht die Siegelung** war für die Authentizität der Unterfertigung entscheidend. *(Dies ist bei einem elektronischen Siegel von Nachteil! Wer hat versiegelt? Der Eigentümer, der Besitzer oder der Stellvertreter?)*

S. 84: Preußisches Allgemeines Landrecht (1749): „... schriftformbedürftige Verträge erst durch die Unterschrift Gültigkeit erlangen. In einigen Bestimmungen zusätzlich als „eigenhändig" charakterisiert.

S. 86: „... eigenhändig heißt, daß die Urheberschaft beschränkt ist: nur das Wirkungssubjekt selbst oder... *(sein bekannter und autorisierter Stellvertreter etc.)* … können unterschreiben". *(Die Urheberschaft ist bei einem Siegel unbeschränkt.)*

S. 206: Zudem bietet die Schriftform dem Erklärenden **Schutz vor Übereilung**. Die Anstrengung, die der Erklärende zur Erfüllung der Form aufwenden muß, gibt ihm einen zusätzlichen Anlaß und zeitlichen Aufschub, um **die Bedeutung der Erklärung zu überdenken**. *(Diese Anstrengung, dieser Anlass und dieser Aufschub sind bei einer PIN nicht gegeben.)*

S. 209: „… daß die Unterschrift des eigenen Namens gewisse empfehlende Eigenschaften besitzt, in dem sie durch ihr individuelles Gepräge einen Anhalt für die Beurteilung der Echtheit gewährt. *(Dies gilt in besonderem Maße bei einer vierdimensional erfassten Unterschrift!)*

Buchbesprechung

Von René Baltus

Ausnahmsweise einmal völlig subjektiv!

Die Kunst der Täuschung: Risikofaktor Mensch

Kevin D. Mitnick

mit einem Vorwort von Steve Wozniak
2003, Hardcover
400 Seiten, Format 17,0 x 24,0 cm
ISBN 3-8266-0999-9
€ 19,95

Kevin D. Mitnick, einst der meistgesuchte Verbrecher der USA, saß fünf Jahre lang im Gefängnis, weil er in zahlreiche Netzwerke großer Firmen eingebrochen war. Dabei bediente er sich häufig nicht nur seiner umfassenden technischen Hacker-Kenntnisse, sondern überlistete praktisch jedes Sicherheitssystem, indem er sich Passwörter erschlich, in Mülltonnen nach sicherheitsrelevanten Informationen suchte und falsche Identitäten vorgaukelte. Mitnick führt den Leser in die Denk- und Handlungsweise von Hackern ein, beschreibt konkrete Betrugsszenarien und zeigt eindrucksvoll die folgenschweren Konsequenzen auf, die sich aus diesen Einbrüchen ergeben. Dabei nimmt Mitnick sowohl die Perspektive des Angreifers wie auch des Opfers ein und erklärt damit sehr eindrucksvoll, wieso jeder Angriff so erfolgreich war – und wie man sich effektiv dagegen schützen kann. Kevin D. Mitnick arbeitet nach seiner Freilassung aus dem Gefängnis als IT-Sicherheitsberater. Ein ihm auferlegtes Computernutzungsverbot wurde mittlerweile aufgehoben. Sein Co-Autor William L. Simon ist Bestseller-Autor von mehr als einem Dutzend Büchern und prämierten Film- und Fernsehdrehbüchern.

Daher der Rat: Nicht kaufen!

Wie das? Ganz einfach. Möchten Sie sich als Verantwortlicher eines Unternehmens, das Server, PC, Inter- und Intranet nutzt, einen ruhigen Schlaf bewahren, folgen Sie einfach meinem Rat und kaufen Sie dieses Buch nicht. Sie werden es mir danken! Im Grunde genommen wissen und kennen Sie schon alles, was darin geschrieben steht. Warum sich dann nochmals seine Unterlassungen vorhalten lassen?

Social Engineering ist ein Anglizismus für Uralttechniken zur Überlistung von Personen. Ein bekanntes Beispiel ist die Geschichte des Hauptmanns von Köpenick. Eine weniger bekanntes handelt von einem Trick der Engländer, die verzweifelt die geänderte Anordnung der Verschlüsselungswalzen der deutschen Verschlüsselungsmaschine „Enigma“ zu erlangen suchten. Sie ließen drei Tage hintereinander an der bretonischen Küste immer zur selben Zeit dieselbe Boje von einem Kampfflugzeug bombardieren. Natürlich wurde dies auch immer brav verschlüsselt und an die vorgesetzten Stellen gemeldet. Drei Tage derselbe Text, lediglich das Datum war jeweils neu. Alles klar? Warum die Boje bombardiert wurde, interessierte niemanden. Hauptsache: Korrekte Meldung, wehrmachtsgerecht ohne einen einzigen Tippfehler. Und gerade ein oder mehrere Tippfehler hätten den Angreifer völlig durcheinander gebracht. Nur, vertippen war in Wehrmachtskreisen verpönt, auf jeden Fall in Meldungen an die vorgesetzten Stellen. Man kann sich gut vorstellen, wie viele Liegestützen der arme „Vertipper“ hätte machen müssen. Das wussten die Briten sehr genau. Social Engineering der ersten Klasse! Was aber nicht heißt, dass die deutschen Stellen nicht auch „Social Engineering“ betrieben haben. Das Beispiel soll nur zeigen, dass selbst Fachleute ersten Ranges nicht dagegen gefeit sind! Die kampferprobten Trojaner haben sich ja auch über den Tisch ziehen lassen.

Also: Doch kaufen?

Ich sage: Ja! Haben Sie wenig Zeit zum Lesen? Kein Problem, darunter leiden auch die „Sozial-Ingenieure“. Daher hat Kevin Mitnick das Wichtige in schnell lesbaren „MitnickSpots“ zusammengefasst. Das dauert Ihnen immer noch zu lange? Auch gut, dann lesen Sie Kapitel 17 ab Seite 375. Es ist ein echtes 7-seitiges Management-Papier. Nur, danach können Sie nicht mehr sagen, Sie hätten es nicht gewusst! Also: Vorsicht! Vielleicht doch nicht kaufen? Aber Mitnick kennt als „Sozial-Ingenieur“ auch sehr gut die Tücken des Sicherheitsgeschäftes.

Eine davon ist die Bequemlichkeit. Das Kapitel 16 enthält daher ein komplettes 75-Seiten-Programm, mit dem Sie Ihre Mitarbeiter sensibilisieren und schulen können. Also: Doch kaufen, preiswerter erhält man keine Schulungsunterlagen zu diesem Thema. Machen Sie es ALLEN Ihren Mitarbeitern, vom Portier über den Azubi im ersten Lehrjahr bis hin zum Vizepräsidenten, zum Geschenk – dann können Sie ruhiger schlafen. Und der Rückfluss der Investitionen? Vielleicht schon nach einem Tag oder nach einem Monat. Wo gibt es das noch?

Kevin Mitnick macht eindeutig klar, dass die beste und ausgefeilteste Technik überhaupt nicht hilft, wenn der Mensch die schwächste Stelle ist. Und er wird sie immer bleiben, sorry. Es ist an Ihnen, diese Schwachstelle zu minimieren – aber bitte nie vergessen: Eine 100-prozentige Sicherheit gibt´s nicht! Sicherheit ist kein Status, es ist ein ununterbrochener Prozess. Ein immerwährendes gegenseitiges Aufschaukeln von Angriff und Abwehr, von Angreifer und Verteidiger – nur dass die Verteidiger meist nicht die kriminelle

Energie der Angreifer besitzen und sich diese oft überhaupt nicht einmal vorstellen können! Der Kenner der Zen-Philosophie wird hier sagen: Der Weg ist das Ziel.

Als Erfinder und Spezialist für dynamische biometrische Erkennungsverfahren gingen mir die Erläuterungen zu den Passwörtern und deren operationellen Schwächen natürlich ´runter wie Öl. Obwohl immer wieder abgestritten, werden die PIN und die Passwörter in Massen an die Bildschirme geklebt – Post-It sei Dank. Oder wie oft werden die armen Unterseiten der Tastaturen zum Notieren missbraucht? Aber selbst Mitnick vergisst in seiner Aufzählung der Gruppen von Passwörtern (Familie, Freundin, Sport, Arbeit, KFZ, Haustiere und Ähnliches) eine wichtige Gruppe: die der Fäkalwörter. Da glaubt jedermann, die wären so fies, das versucht keiner – aber Hacker beginnen gerade damit! Also, man sieht, entweder die Gruppe ist Mitnick auch zu fies oder er hat sie vergessen. Hacker und Social Engineers vergessen so etwas nicht! Denen ist überhaupt nichts zu fies.

Aber Kevin Mitnick kannte auch nicht die Smart Defense-Antwort auf einen Brut Force-Angriff: das eigenhändig geschriebene Passwort. Nur so als Tipp für Sie. Hat nämlich ein bekanntes Unternehmen mit, sagen wir mal 10.000 PC-Arbeitsplätzen, nur EIN Passwort für ALLE und für ALLES, hat der Hacker es wohl vermeintlich sehr einfach. Das Passwort ist sogar bekannt. Tja, da liegt er aber nicht so ganz richtig. Er kann wo auch immer versuchen, in einen PC oder Server einzudringen, immer erfolgt die Meldung: *Bitte schreiben Sie „Wolfsburg“*. Nun muss er die unbekannte und unfälschbare Schreibdynamik so exakt in Schreibdruck, Schreibzeit und Schreibpausen niederschreiben, dass er wiedererkannt wird. Und je sensibler der Bereich, umso strenger wird die Schreibdynamik geprüft! Dann kann es vielleicht sein, dass sogar der Berechtigte dreimal unterschreiben muss! Ist das Passwort dann noch unbekannt, nun, dann hat der Hacker doppeltes Pech. Es gibt ja eine unendliche Zahl davon, man beginne nur einmal mit dem Atlas bei „Aalen“ und zähle bis „Zwickau“ durch. Wird das eigenhändig geschriebene Passwort noch mit einer tippdynamisch erfassten PIN (jeder Mensch hat seine individuelle Tippdynamik) kombiniert, gibt’s für den Angreifer wirklich ernsthafte Probleme.

Es ist auch anzunehmen, dass Kevin Mitnick noch nicht über sichere mobile Signaturkomponenten (Mobiltelefon mit „analoger Tastatur“ zur Eingabe von Zahlen und Schriftzeichen) informiert wurde. Aber das war an sich ein unerlaubter Ausflug in die fortschreitende Technik.
Kevin Mitnick zählt im Index 27-mal den Begriff „Sicherheit“ auf, von Sicherheit bis Sicherheitszertifikat. Danach folgt „Passwort“ mit 18 Erwähnungen. Scheint etwas dran 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! Sind sie offensichtlich aber nicht.

In der gerade wieder angefachten Diskussion zur flächendeckenden Einführung sogenannter „digitaler Signaturen“ (besser: digitaler Siegel) wird vorsichtshalber das Problem der Passwörter außen vor gelassen. Nach der Verordnung zur „Digitalen Signatur“ sollen diese Passwörter lediglich sechs Stellen besitzen – von einer Änderung nach vier oder sechs Wochen ist da keine Rede. Wenn schon Personen, die beruflich mit Passwörtern zu tun haben, die operationellen Schwächen nicht beachten, wie dann der unbedarfte digitale „Have-Not“?

Daher: Mitnicks Buch ist die ideale „Bibel“, vulgo Belehrungsunterlage, für zukünftige Aspiranten digitaler Siegel oder, das „schönere“ Wort soll auch zur Anwendung kommen, digitaler „Signaturen“. Also, lieber Leser, Sie sehen, Sie stehen nicht alleine da, was ja auch tröstlich sein kann. Aber ein starker Trost ist das nun gerade nicht.

Daher: Doch kaufen!

Einige schlaflose Nächte hinter sich bringen, Mitnicks Ratschläge befolgen, dann klappt´s! Immerhin ist er Insider und weiß wovon er schreibt! Viele könnten, dürfen aber nicht schreiben.

Online nachzulesen unter
www.sign-n-type.com/pdf/BuchbesprechungMitNick.pdf

Danksagung

Das Sign-n-Type-Verfahren wäre ohne die tatkräftige Unterstützung vieler Personen nicht zustande gekommen.

So gebührt Marc-Berndt Woop (GfaR, Bonn) als Schreiber der erstklassigen Erkennungssoftware und Entwickler der Elektronik mein Dank.

Ohne die unendliche Geduld und Hilfestellung von Brigitte und Marian Buczek (TecGer, Troisdorf) bei der Herstellung unzähliger Prototypen der Mechanik und der Gehäuse hätte ich schon sehr früh aufgeben müssen; herzlichen Dank!

Die Mitarbeiter der Patent- und Innovationsagentur PINA-NRW aus Dortmund waren die ersten, die das Potential des Verfahrens erkannten und für die Bereitstellung der Kostendeckung des Europapatents gesorgt haben.

Die intensive Zusammenarbeit mit Patentanwalt Prof. Dr. Helge Cohausz, Düsseldorf, führte zu einer ausgewachsenen Freundschaft. Vielen Dank!

Frau Dr. Marianne Tümpen, Herr Alexander Nediger und Andreas Piechota erkannten ebenfalls das starke Potential des Schriftprüfers und förderten das Projekt mit selten erlebter Kraft und Energie; ihnen vielen Dank für das Vertrauen.

Ein herzliches Dankeschön auch an alle Personen, die, bekannt im Vordergrund oder unbekannt aus dem Hintergrund heraus, das Projekt mit Wort und Tat gefördert haben.

Nicht zu vergessen in dieser Danksagung sind die Journalisten, die mutig und objektiv über das Projekt berichteten und immer noch berichten.

Einen Dank auch an die zahlreichen Gegner und unbequemen Fragensteller, die Kritik übten; ihre objektiven und subjektiven Einwendungen waren immer sehr anregend und führten zu Verbesserungen, neuen Produkten und Anwendungen – und oft zu Anmeldungen von Gebrauchsmustern und Patenten.

In einem „zivilen“ Buch etwas ungewöhnlich ist der Dank an meine Ausbilder beim 3. Ardennenjäger-Bataillon im belgischen Vielsalm. Sie lehrten mich vor vielen, vielen Jahren den Wahlspruch der Ardennenjäger:„Resiste et Mort“, oder in Deutsch „Halten und Beißen“, zu realisieren. Damals verflucht, war er auf dem langen und dornigen Weg oft genug die letzte Rettung vor dem Aufgeben!

Die Danksagung wäre unvollständig ohne die Erwähnung der Familie Thelen, die mit unendlicher Geduld meinen Monologen gefolgt ist und die für Besprechungen, Konferenzen und Vorführungen die Räumlichkeiten von Schloss Miel zur Verfügung gestellt hat.

Nicht zuletzt danke ich Frau Petra Wingen – sie korrigierte in mühevoller Arbeit meine Texte und stellte sie für dieses Buch zusammen.

Literaturverzeichnis

Baltus, René (1997): Beitrag in: *Öffentliche Anhörung zu den Katalogen gem. § 12 Abs. 2 und § 16 Abs. 6 der Verordnung zur digitalen Signatur (SigV)* am 19.12.97, Bonn. Sammlung der schriftlichen Stellungnahmen, die bis zum 17.12.97 beim Bundesamt für Post und Telekommunikation eingegangen sind.

Baltus, René (2001): Tagungsband: *Innovations- und Qualitätsmanagement in der Luft- und Raumfahrt*. 18. und 19. Oktober 2001, IABG GmbH Ottobrunn

Baltus, René (2002): *Der Einsatz der Biometrie bei der digitalen Signatur.* Beitrag in: Elektronische Signatur. Hrsg. VOI, Verband der Organisations- und Informationssysteme e.V. Darmstadt

Baltus, René (2002): *Ist die eigenhändige Unterschrift noch zu retten?* In: Nolde, Veronika und Leger, Lothar; Hrsg. (2002): *Biometrische Verfahren*. Fachverlag Deutscher Wirtschaftsdienst GmbH & Co. KG, Köln

Baltus, René (2003): *Das elektronische Handschriftenerkennungssystem HESY und sein Potential für die forensische Schrifterkennung.* ZFS, Zeitschrift für Schriftpsychologie und Schrifterkennung, Sektion Schriftpsychologen im Berufsverband Deutscher Psychologen, Redaktion Dr. Angelika Seibt, Rottach-Egern

Baltus, René (2003): *Schrifterkennung – Wer unterschreibt, der lebt*. In: Spektrum der Wissenschaft, Magazin 01.08.2003.
http://www.spektrumverlag.de/artikel/830020

Baltus, R. und Schönleber, C. (1995): *Sichere Authentikation – HESY Unterschriftenprüfer*. In: Schönleber, Claus (1995): Verschlüsselungsverfahren für PC-Daten. Franzis Verlag GmbH, Poing

Baltus, R. und Woop, M. (1998): *Volle Kraft voraus ins Internet-Zeitalter – rechtlich abgesichert mit der digitalen Signatur und der eigenhändigen Unterschrift*. In : Internet – frischer Wind in der Telekommunikation. Vorträge der ITG-Fachtagung anlässlich des VDE-Kongresses '98 am 21. und 22. Oktober 1998 in Stuttgart. VDE-Verlag

Baltus, R. und Woop, M. (2000): Der *Einsatz biometrischer Verfahren im DMS und bei Micro- und Macropayment*. Vortrag anlässlich des 3. Frankfurter VOI-Tages.

Behrens/Knütel/Kupisch/Seiler (1993): *Corpus Iuris Civilis – Die Institutionen.* C.F. Müller, Juristischer Verlag Heidelberg

Faulmann, Carl (1995): *Schriftzeichen und Alphabete aller Zeiten und Völker*. Augustus Verlag Augsburg

Giscard d'Estaing, Valerie-Anne (1998): *La Securité.* In: Le Livre Mondial des Inventions, 75012 Paris

Greiner, Joachim (o. Jahresangabe): Diplomarbeit: *Entwicklung und Test einer interaktiven Schnittstelle für den Einsatz der digitalen Unterschrift im Entwicklungs- und Fertigungsprozess eines modernen Luftfahrtunternehmens.* Stuttgart

Hawkins, Dana (2002): *Smart Traveler – Travel tactics for a changing world – Your Body, Your Badge.* National Geographic Traveler, July/August 2002

Heuser, Dr. Ansgar (1997): *Gesetzgebungsinitiative der Bundesregierung zum Elektronischen Rechtsverkehr – Signaturgesetz und Signaturverordnung.* Vortrag in: Drittes Forum Elektronischer Rechtsverkehr der Bundesnotarkammer. Köln, 13. März 1997

Holzhauer, Heinz (1973): *Die eigenhändige Unterschrift, Geschichte und Dogmatik des Schriftformerfordernisses im deutschen Recht.* Athenäum Verlag GmbH, Frankfurt am Main

Maus, Eugen P. (1996): *Schriftdruckmessung, Grundlagen, Methoden, Instrumente.* Scriptura Verlag Lothar Michel, Weinheim Bergstraße

Maus, Eugen P. (2001): *Das Handschriftenerkennungssystem HESY – Eine Schreibwaage mit Wegerfassung* In: Mannheimer Hefte für Schriftvergleichung. 27. Jahrgang, Heft 1+2/01, Schmidt – Römhild Verlag Lübeck

Maus, Eugen P. (2001): Expertise: *Verwendbarkeit des Handschriftenerkennungssystems HESY für Zwecke der Schriftvergleichung.* Frankenthal

Mitnick, Kevin D. (2003): *Die Kunst der Täuschung: Risikofaktor Mensch*. MITP-Verlag Bonn

Nolde, Veronika und Leger, Lothar; Hrsg. (2002): *Biometrische Verfahren*. Fachverlag Deutscher Wirtschaftsdienst GmbH & Co. KG, Köln

Pohl, Hartmut (1989): *Sicherheit der Informationstechnik*. Datakontext Verlag Köln

Ortega, Jose y Gasset (1949): *Betrachtungen über die Technik*. DVA, Stuttgart

Schnauffer, Peter (2006): Dissertation: *Multidisziplinärer Datenfluss im Entwicklungsprozess des Flugzeugbaus am Beispiel eines Senkrechtstarters – Multidisciplinary dataflow in the development process of the aircraft design on hands of a vertical take off and landing vehicle.*
http://elib.uni-stuttgart.de/opus/volltexte/2006/2688/pdf/Multidisziplinaerer_Datenfluss.pdf

Schönleber, Claus (1995): *Verschlüsselungsverfahren für PC-Daten*. Franzis Verlag GmbH, Poing

Singh, Simon (2004): *Codes – Die Kunst der Verschlüsselung.* DTV München

Tholl, Thomas (2003): Studienarbeit: *Projekt- und Datenmanagement im Flugzeugbau*. Stuttgart

United States General Accounting Office (2002): *National Preparedness – Technologies to Secure Federal Buildings.* Statement of Keith A. Rhodes, Chief Technologist. http://www.gao.gov/new.items/d02687t.pdf

Sponsorenseiten

GOLF-CLUB SCHLOSS MIEL

www.golf-schloss-miel.de

12 km westlich von Bonn liegt der Golf-Club Schloss Miel in der reizvollen Landschaft der Voreifel in der Ortschaft Swisttal-Miel.

Eine abwechslungsreiche Platzarchitektur mit anspruchsvollen Wasser- und Bunkerhindernissen ermöglicht auf 90 ha 18 interessante Spielbahnen. Der Platz wird allen sportlichen Ansprüchen gerecht. Den Mittelpunkt des Geländes bildet ein alter, über 12 ha großer Laubwald.

1768 baute der kurkölnische Staatsminister und eigentlicher Regent des Kurstaates, Freiherr von der Heyden, genannt Belderbusch, den alten Rittersitz Miel, unweit der Residenz Bonn, zu einem Wasserschloss aus. Die historischen Bauten und Außenanlagen des Schlosses sind in die Golfanlage einbezogen und verbinden den Golfsport mit einem kulturellen Angebot.

Loch 18, aufgenommen aus einem Hubschrauber
Mehr Bilder: www.golf-schloss-miel.de/impressionen.php

Die Heimat des Golfclubs Schloss Miel

Der Gartensaal:
Hier finden Hochzeiten, Feste und Mi(e)longas statt.

Die Mi(e)longas auf Schloss Miel:
Klein, aber fein!

Seit Jahren veranstaltet René Baltus die sehr beliebten Tangobälle, genannt Mi(e)longas, im unverfälschten spätbarocken Ambiente des 18. Jahrhunderts. Getanzt wird im Gartensaal, dem Wohnzimmer des Grafen Belderbusch. Die prächtigen, vollständig erhaltenen Wandgemälde des Hofmalers François Rousseau verleihen dem Saal ein ganz besonderes Flair und das fast 250 Jahre alte Eichenparkett bietet ungeahnten Tanzgenuss.

Die Gästezahl bei den Mi(e)longas ist überschaubar, neugierige Erstbesucher werden herzlich aufgenommen – wie bei Freunden zu Hause.

Anlässlich der Mi(e)longas auf Schloss Miel treten regelmäßig tangobegeisterte Hobby- und Berufskünstler auf. Die Darbietungen umfassten bisher:

Deutsche Harfe und deutsche Märchen
Ein-Frau-Schauspiel
Klavierspiel Classic meets Tango
Barocktanz
Tango-Argentino-Konzert
Live-Tango mit belgischer Frauenband
Keltische Harfe und schottische Märchen
Dichterlesung

Flyer der bisherigen Veranstaltungen
sowie weitere Infos zu den Tangobällen
auf Schloss Miel:

www.tangueria.de

BVP Gesellschaft für Beratung, Verfahren und Produkte mbH

Auf den Steinen 7, 53125 Bonn

(Dienst-)Leistungen, Kompetenzen:

Produktentwicklung, Prototypenbau, Innovation, Ideenfindung, Problemlösungen, Patentanmeldungen (aber keine Rechtsberatung!), Planung und Realisierung von physikalisch-chemischen Verfahren.

Als innovative Produkte:

Sehr preiswerter Windmesser (Anemometer) ohne bewegliche Teile für alle Windrichtungen und –stärken (auch Fall- und Steigewinde)
Biometrischer Zufallsgenerator, dreidimensional wirkende analoge Tastaturen (mit tippdynamischer Erfassung der PIN) und Joysticks, eigenhändige digitale Signatur in CATIA V5 und CAD, elektronische Blaupause, lineare Membranpumpe, mechanische Parkhäuser, Angärkontrolle für obergäriges Bier mittels kontinuierlicher CO2-Analyse.

Am Anfang war das Passwort – jetzt ist HESY!
www.hesy.de

HESY – ein patentiertes fälschungsresistentes **H**andschriften-**E**rkennungs-**Sy**stem, das mit handelsüblichen Stiften beschreibbar ist. HESY ermöglicht:

Rechtsverbindlichkeit:

Der Anwender unterschreibt z.B. seinen Vertrag auf dem HESY-Schreibpad mit einem herkömmlichen Kugelschreiber. Damit signiert er diesen Vertrag gleichzeitig auf dem Papier und als digitales Dokument. Seine Unterschrift und das digitale Dokument werden untrennbar miteinander verbunden und ggf. durch weitere Siegel gesichert. Selbstverständlich ist die digitale HESY-Unterschrift auch ohne Papier-Durchschlag valide.

Fälschungsresistenz:

Während der Anwender seine Unterschrift und/oder sein Passwort schreibt und/oder das numerische HESY-Feld nutzt, um seine PIN einzugeben, erfasst HESY die unverwechselbaren Eigenschaften der Schreib- und Tippdynamik. Ebenso wie durch Fingerabdruck oder Iris-Scan können Personen durch die aktiven Merkmale Druck, Anschlag, Schreibgeschwindigkeit und Pausen anhand ihrer Unterschrift zweifelsfrei identifiziert werden. HESY vergleicht die gewonnenen Daten mit dem hinterlegten Original. Das Original kann im Gegensatz zum leicht kopierbaren Fingerabdruck nur bewusst abgegeben worden sein.

Je nach Wertigkeit einer z.B. finanziellen Transaktion oder Empfindlichkeit eines Sicherheitsbereichs können Sicherheitsstufen durch HESY definiert und variiert werden: Möglich ist die Kombination der fälschungsresistenten rechtsverbindlichen Unterschrift mit einer PIN/einem Passwort und/oder einer Chipkarte.

Der Bedarf an fälschungssicherer digitaler Signatur ist aktuell extrem hoch. Um nur einige Beispiele zu nennen:
Bezahlverkehr im Internet – Kauf mit EC-Card, Pin & Unterschrift – Identifikation bei Passagieren in der Luftfahrt/ bei der Hotelanmeldung – HealthCare: elektronische Patientenakte – Life-Cycle-Management; Rückverfolgbarkeit des Wegs: Rohstoffe, Produkt, Verkauf – E-Learning – Workflow optimieren: Konstruktionszeichnungen rechtsgültig digital signieren (Luftfahrt/Industrie) – Dokumentenmanagement-Systeme: Stichwort papierloses Büro

www.tecger.com
Troisdorf

CNC Fräs- und Graviermaschinen

CNC Zubehör

Sonderanfertigungen