Vertrauensmerkmal Unterschrift – Gestaltungskriterien für sichere Signierwerkzeuge

Johannes Kaiser
Institut für Informatik und Gesellschaft
Albert-Ludwigs-Universität Freiburg
kaiser@iig.uni-freiburg.de

Zusammenfassung: *In Zeiten des E- bzw. M-Commerce wird die praktische Akzeptanz der digitalen Signatur im wesentlichen von der Bedienbarkeit digitaler Signierwerkzeuge durch den Normalbenutzer abhängen. Dabei muss der Normalbenutzer, der meist Sicherheitslaie bleiben wird, das Signierwerkzeug fehlhandlungssicher bedienen können.*
In diesem Artikel werden Sicherheitslücken von Signierwerkzeugen diskutiert, die im Dialog mit dem Normalbenutzer entstehen können. Es wird gezeigt, dass durch die Gewährleistung von Eigenschaften der eigenhändigen Unterschrift Sicherheitslücken in Signierwerkzeugen beseitigt werden.
Daraus resultieren allgemeine Gestaltungsanforderungen, die ein adäquates Signierwerkzeug erfüllen muss. Diese Gestaltungsanforderungen werden zu Gestaltungskriterien für Signierwerkzeuge konkretisiert.

Schlüsselwörter: *Digitale Signatur, Signierwerkzeuge, Benutzbarkeit, Biometrie, Gestaltungskriterien*

1. Einleitung

Zur Gewährleistung der Sicherheit digitaler Signaturen werden im Signaturgesetz die technischen Voraussetzungen für Signierwerkzeuge festgelegt. Sind diese Voraussetzungen erfüllt, so ist der Frage nachzugehen, ob die Sicherheit des Systems auch im praktischen Einsatz, d.h. im Dialog mit dem Benutzer gewährleistet ist.
Ein radikaler Forschungsansatz geht davon aus, den Benutzer per se als schwächstes Glied in der Sicherheitskette zu betrachten [4]. Somit können durch den Benutzer im praktischen Einsatz Sicherheitslücken entstehen, die auch durch signaturgesetzkonform zertifizierte Systeme nicht verhindert werden.

Da in Zeiten des E- bzw. M-Commerce der Normalbenutzer immer mehr mit Sicherheitsanwendungen konfrontiert wird, ist neben der sicheren Benutzung auch das Vertrauen des Benutzers für die Systemakzeptanz von großer Bedeutung.
In diesem Artikel werden Gestaltungskriterien für ein Signierwerkzeug erarbeitet, die verschiedene Benutzbarkeitsprobleme und die daraus resultierenden Sicherheitslücken vermeiden. Eine derartige Problemvermeidung steigert die Vertrauenswürdigkeit und die Akzeptanz von Signierwerkzeugen.

2. Gestaltungsanforderungen für sichere Signierwerkzeuge

Untersuchungen haben bereits die mangelhafte Benutzbarkeit von Signierwerkzeugen und die daraus resultierenden Sicherheitslücken aufgezeigt [11]. Eine Folgerung daraus ist, dass ein Signierwerkzeug erst dann als sicher gelten kann, wenn es auch benutzbar ist [4]. Aufgrund der mangelhaften Benutzbarkeit von Signierwerkzeugen für Normalbenutzer sind deshalb Gestaltungsanforderungen zu erarbeiten.
Da die digitale Signatur als Äquivalent zur eigenhändigen Unterschrift gelten soll, ist eine wesentliche Gestaltungsanforderung die Gewährleistung der Unterschriftseigenschaften (vgl. Kapitel 3) durch das Signierwerkzeug.
Grundlegend für die Gestaltung benutzbarer Signierwerkzeuge ist die Annahme, dass der Normalbenutzer meist Sicherheitslaie bleiben wird. Dieser ist deshalb wenig bereit, sich mit Sicherheitsfragen bzw. Sicherheitskonzepten auseinanderzusetzen. So ist es bspw. für den Normalbenutzer oftmals ein großes Problem, das zugrundeliegende Sicherheitskonzept zu verstehen. Häufig werden in Sicherheitswerkzeugen meist kryptographische Konzepte, Prinzipien oder Protokolle ungefiltert auf der Benutzungsoberfläche

widergespiegelt. Für den Benutzer entstehen genau dann Benutzbarkeitsprobleme, wenn ihm das Sicherheitskonzept, das Sicherheitsprinzip oder der Sicherheitsdialog aus seiner realen Erfahrungswelt nicht vertraut ist. Eine exakte Definition von Konzepten, Prinzipien und Dialogen ist in [6] zu finden. Als nicht vertrautes Sicherheitsprinzip ist bspw. die asymmetrische Verschlüsselung zu nennen.
Es lässt sich daraus die folgende These ableiten, die ein allgemeines Gestaltungskriterium für Signierwerkzeuge impliziert:

Die Benutzbarkeit von Sicherheitswerkzeugen und damit die Vermeidung von Sicherheitsproblemen wird gesteigert, indem für den Normalbenutzer vertraute Konzepte, vertraute Prinzipien und vertraute Dialoge adäquat in das Sicherheitswerkzeug integriert sind.

Das für den Normalbenutzer vertraute Merkmal zur Abgabe einer Willenserklärung ist die Unterschrift. Diese besitzt für den Benutzer bekannte und vertraute Eigenschaften, wie die Gewährleistung der Schutzfunktionen und die orts- und zeitunabhängige Verfügbarkeit. Deshalb sind die folgenden Gestaltungsanforderungen an ein Signierwerkzeug zu stellen:

- die Schutzfunktionen der eigenhändigen Unterschrift müssen durch das Signierwerkzeug gewährleistet sein.
- das Signierwerkzeug muss orts- und zeitunabhängig einsetzbar sein.

Werden diese Anforderungen durch ein Signierwerkzeug erfüllt, so wird dies zu einer höheren Akzeptanz der digitalen Signatur und zu einem höheren Vertrauen in das Signierwerkzeug führen.

3. Schutzfunktionen und die PIN-Problematik

Die eigenhändige Unterschrift besitzt eine Anzahl an Schutzfunktionen, deren wichtigsten die Echtheits-, die Abschluss-, die Beweis-, die Identitäts- und die Warnfunktion sind [10]. Ein generelles Vertrauen in die digitale Signatur und deren Akzeptanz kann nur dann vorhanden sein, wenn das Signierwerkzeug die Schutzfunktionen der eigenhändigen Unterschrift erfüllt [1].
Schutzfunktionen wie Echtheits-, Abschluss- und Beweisfunktion, werden primär von der zugrundeliegenden Kryptographie gewährleistet. Diese wird durch die *perfect cryptography assumption* als gegeben vorausgesetzt. Wesentliche Voraussetzung für die Erfüllung der Echtheits-, Abschluss- und Beweisfunktion ist die Sicherstellung der Identitätsfunktion. Diese wird jedoch durch die PIN-Problematik (*Vergessen*, *Weitergeben* und *Ausspähen*) gefährdet [2]. Die PIN-Problematik entsteht dabei vor allem durch den Normalbenutzer. Dieser ist gemäß der Annahme wenig bereit, sich mit Sicherheitsfragen auseinanderzusetzen.
Ausspähen der PIN kann dabei auf zwei Arten geschehen:

1. Ausspähen durch bloße Beobachtung
2. Ausspähen auf unsicheren Systemen

Vergessen, *Weitergeben* und *Ausspähen durch bloße Beobachtung* können zu funktionalen Angriffen führen. Bei funktionalen Angriffen handelt es sich nicht um Angriffe im strengen Wortsinn, sondern um Gefährdungen, die in ihren Folgen einem Angriff gleichkommen bzw. einen Angriff auslösen können [5].
Im folgenden Kapitel werden funktionale Angriffe skizziert und eine geeignete Systemgestaltung vorgeschlagen, wodurch die Teilprobleme der PIN (*Vergessen*, *Weitergeben* und *Ausspähen durch bloße Beobachtung*) vermieden werden. In Kapitel 5 wird das Ausspähen auf unsicheren Systemen erörtert und eine Systemgestaltung zur Abwehr dieser Gefahr skizziert.

4. Einsatz biometrischer Erkennungsverfahren

Damit die Schutzfunktionen Echtheits-, Abschluss-, Beweis- und Identitätsfunktion erfüllt werden können, ist das Signierwerkzeug derart zu gestalten, so dass die PIN-Problematik nicht mehr existent ist.
Durch den Einsatz biometrischer Erkennungsverfahren zur Freischaltung der digitalen Signatur können sowohl das Problem des *Vergessens*, das Problem des *Weitergebens*, als auch das Problem des *Ausspähens durch bloße Beobachtung* in geeigneter Weise vermieden werden.

4.1 Vergessen

Aufgrund der PIN-Inflation ist für den Benutzer die Gefahr des Vergessens erhöht. Die Folge ist, dass Benutzer dazu übergehen, ihre PINs mit Hilfe einer Liste zu verwalten bzw. ein und dieselbe PIN für verschiedene Systeme benutzen.
Im ersten Fall wird ein Angreifer versuchen, diese Liste zu entwenden bzw. zu kopieren. Die zweite Fehlhandlung führt dazu, dass ein Angreifer versuchen wird, die PIN auf unsicheren Systemen auszuspähen, um so die digitale Signatur kompromittieren zu können.

Beide Fälle sind äußerst sicherheitskritisch, da die Wahrscheinlichkeit von sowohl funktionalen, als auch technischen Angriffen[1] hoch ist. So können im ersten Fall auch Angreifer ohne technisches Wissen den skizzierten Angriff durchführen.
Da die Authentifizierung durch die Abgabe eines biometrischen Merkmals erfolgt, ist das Problem des Vergessens nicht mehr existent.

4.2 Weitergeben

Die Möglichkeit der Weitergabe einer PIN wird in einigen Anwendungsszenarien als Vorteil betrachtet. So kann z.B. das Passwort der digitalen Signatur durch eine einmalige Vollmacht übergeben werden. Mit der Beendigung der Vollmacht muss der Eigentümer der digitalen Signatur das Passwort sofort ändern. Ob dies in der Praxis auch tatsächlich passiert, ist fraglich.
Wird das Passwort korrekterweise geändert, so besteht aufgrund der Struktur des Passworts oftmals die Möglichkeit, das neue Passwort zu erraten (z.B. ma09ri05a01, Name der Ehefrau: Maria, Letzte Änderung des Passwortes: 9. Mai 2001). Die Möglichkeit der Weitergabe erhöht das Risiko eines Angriffs auf die digitale Signatur.
Durch den Einsatz biometrischer Verfahren ist ein einfaches Weitergeben der Merkmalsdaten, wie es bei der PIN der Fall ist, nicht möglich. Ein Weitergeben der Merkmalsdaten, bspw. mittels eines Datenträgers, ist jedoch weiterhin möglich.

4.3 Ausspähen durch bloße Beobachtung

Eine einfache Ausspähung der PIN durch bloße Beobachtung ist in vielen Situationen gegeben. So kann bspw. beim Zahlen im Supermarkt mit der EC-Karte oftmals ein in der selben Warteschlange befindlicher Kunde die zur Authentifizierung notwendige PIN-Eingabe problemlos verfolgen.
Biometrische Verfahren dagegen, wie bspw. die biometrische Unterschriftserkennung, basieren zum Teil auf nicht sichtbaren Eigenschaften der Unterschrift, wie Schreibdruck, Schreibgeschwindigkeit und Schreibbeschleunigung. Diese nicht sichtbaren Eigenschaften können von einem Angreifer durch bloße Beobachtung nicht imitiert werden.

Durch den Einsatz biometrischer Verfahren kann somit ein Teil der PIN-Problematik vermieden werden. Zur vollständigen Vermeidung der hier diskutierten PIN-Problematik ist das Problem des Ausspähens auf unsicheren Systemen noch zu betrachten. Dies wird in Kapitel 5 erfolgen.

4.4 Die Erfüllung der Warnfunktion

Wird ein biometrisches Erkennungsverfahren zur Freischaltung der digitalen Signatur eingesetzt, so muss das verwendete Merkmal die Warnfunktion der Unterschrift, die den Unterzeichner vor Übereilung schützen soll, gewährleisten. Dies geschieht dadurch, indem eine bewusste und aktive Handlung vom Unterzeichner gefordert wird [1].
In Tabelle 1 wird eine Kategorisierung von biometrischen Merkmalen in aktive und passive Merkmale durchgeführt.
Aktive Merkmale erfordern vom Benutzer eine bewusste Handlung. Dem gegenüber erfordern passive Merkmale keine bewusste Handlung des Benutzers. Deshalb können passive Merkmale (z.B. Gesichtserkennung, Iriserkennung) auch ohne Wissen des Benutzers abgegeben und erfasst werden. Aus diesem Grund sind passive Merkmale für den Einsatz in Signierwerkzeugen abzulehnen.

Tabelle 1: Aktive und passive Merkmale für biometrische Erkennungsverfahren [11].

Passive Merkmale	Aktive Merkmale
Fingerabdruck	Stimme
Gesicht	Eigenhändige Unterschrift
Handgeometrie	Tippverhalten
Iris	
Retina	
Venenmuster der Hand	

Das Merkmal Tippverhalten ist aufgrund des notwendigen Zeitaufwands [3] und seiner Untauglichkeit für den mobilen Einsatz ebenfalls abzulehnen. Stimmerkennungsverfahren scheinen eine kostengünstige Alternative zu sein, da in vielen Endgeräten eine geeignete technische Hardware bereits vorhanden ist. Derzeit existierende Stimmerkennungsverfahren weisen jedoch noch zu geringe Erkennungsraten auf, weshalb sie derzeit nicht real einsetzbar sind. Darüberhinaus sind Replay-Attacken - das Aufzeichnen und Abspielen der Stimme - generell nicht zu verhindern.
Deshalb wird vorgeschlagen, biometrische Unterschriftserkennungsverfahren zur Freischaltung der digitalen Signatur einzusetzen.

[1] Ein technischer Angriff setzt technisches Wissen und eine entsprechende technische Ausrüstung des Angreifers voraus.

5. Mobilität als notwendiges Gestaltungsprinzip

Durch den Einsatz biometrischer Erkennungsverfahren wird ein Teil der PIN-Problematik vermieden. Jedoch ist das Ausspähen biometrischer Merkmale auf unsicheren Systemen weiterhin gegeben.
Das Ausspähen auf unsicheren Systemen ist gerade beim Einsatz biometrischer Erkennungsverfahren äußerst kritisch, da biometrische Merkmale direkt an eine Person gebunden sind und nicht wie ein Passwort beliebig veränderbar sind. Mit Hilfe eines erfolgreichen Angriffs durch Ausspähen der Merkmalsdaten auf einem fremden System kann die digitale Signatur kompromittiert werden.
In Kapitel 5.1 wird beispielhaft skizziert, dass das Ausspähen der biometrischen Merkmalsdaten auf unsicheren bzw. fremden Systemen prinzipiell nicht zu vermeiden ist. Mit Hilfe der Mobilitätseigenschaft wird in Kapitel 5.2 gezeigt, wie die Gefahr, die aus der aufgezeigten Ausspähproblematik entsteht, vermieden wird.

5.1 Ausspähen auf fremden Systemen

Biometrische Merkmalsdaten sind unweigerlich mit einer Person verknüpft. Durch diese untrennbare Bindung an eine Person ist jedoch das Ausspähen der Merkmalsdaten auch außerhalb des persönlichen Signierwerkzeuges möglich. Es ist abzusehen, dass die Benutzerauthentifizierung durch biometrische Verfahren zukünftig weit verbreitet sein wird, so dass man sich auch gegenüber fremden Systemen authentifizieren muss. So können in einem Unternehmen Zugangskontrollen für sicherheitskritische Systeme mit Hilfe biometrischer Unterschriftserkennung realisiert sein. Ein Benutzer muss sich gegenüber einem solchen System durch Abgabe eines biometrischen Merkmals authentifizieren. Nach Abgabe des biometrischen Merkmals wird ein Datensatz der biometrischen Merkmale für den Vergleich mit dem Referenzdatensatz erzeugt. Ein Ausspähen biometrischer Merkmalsdaten kann dabei durch einen man-in-the-middle Angriff zwischen dem Erfassungsgerät und der Verarbeitungseinheit geschehen.
Solche Systeme liegen außerhalb des Herrschafts- bzw. Vertrauensbereichs des Benutzers, weshalb dieser keine Kontrolle über seine personengebundenen Daten hat. Ist ein solches System nicht ausreichend vor Angriffen geschützt, wird damit unweigerlich die Wahrscheinlichkeit für einen Angriff auf die digitale Signatur erhöht.
Sind von einem Angreifer die biometrischen Merkmalsdaten ausgespäht, so ist für einen erfolgreichen Angriff auf die digitale Signatur lediglich das Entwenden der SmartCard notwendig. Auf der SmartCard müssen die sensiblen Daten, wie privater Schlüssel und biometrische Referenzdaten, gespeichert sein. Aufgrund der Unveränderbarkeit biometrischer Merkmale, kann zwischen dem Ausspähen der Daten und dem Entwenden der SmartCard eine große Zeitspanne liegen. Somit kann ein potentieller Angreifer einen Teil seines Angriffs lange Zeit vor seinem eigentlichen Angriff durch Sammeln von Merkmalsdaten unentdeckt durchführen. Damit erhöht sich die Wahrscheinlichkeit dieser Angriffe. Ein Signierwerkzeug muss diesem Problem entgegenwirken.

5.2 Das mobile vertrauenswürdige Signierwerkzeug

Eine weitere wichtige Eigenschaft der eigenhändigen Unterschrift auf Papier ist, dass sie jederzeit und an jedem Ort zur Verfügung steht. Deshalb ist eine wesentliche Anforderung an ein Signierwerkzeug dessen Mobilität.

Wird die digitale Signatur durch biometrische Unterschriftserkennung auf *einem* mobilen persönlichen Endgerät [7] freigeschaltet, so kann dadurch die Gefahr des Ausspähens von Merkmalsdaten (vgl. 5.1) verringert werden. Dieses Signierwerkzeug befindet sich im Herrschafts- bzw. Vertrauensbereich des Anwenders. Mit diesem Ansatz verbleiben die sensiblen biometrischen Merkmalsdaten auf dem persönlichen Endgerät und müssen dieses auch nicht verlassen.
Da das Ausspähen der Merkmalsdaten prinzipiell nicht vermieden werden kann (vgl. 5.1), muss das Signierwerkzeug derart gestaltet werden, dass ein erfolgreiches Ausspähen der biometrischen Merkmalsdaten auf fremden bzw. unsicheren Systemen nicht zur Freischaltung des Signierschlüssels genutzt werden kann. Dies wird dadurch erreicht, indem zur Freischaltung des Signierschlüssels das biometrische Merkmal lediglich auf dem persönlichen vertrauenswürdigen Endgerät abgegeben werden kann.
Mit diesem Ansatz ist für den Normalbenutzer die Verringerung der Ausspähproblematik intuitiv verständlich. Damit kann das subjektive Vertrauen des Benutzers gesteigert werden, das eine wesentliche Voraussetzung für die Akzeptanz des Systems ist.
Ein mögliches Endgerät ist jedoch objektiv erst dann vertrauenswürdig, wenn die sensiblen Daten auf dem Endgerät weder ausspähbar noch manipulierbar sind. Da solche Endgeräte derzeit in der Praxis (noch) nicht existieren, müssen Annäherungen gefunden werden [9].

Eine Annäherung kann der Einsatz einer vertrauenswürdigen Komponente sein, wie bspw. der SmartCard. Das mobile vertrauenswürdige Endgerät muss somit zusätzlich über einen Steckplatz für die SmartCard verfügen.

Um das digitale Signieren nicht zu gefährden, ist des weiteren zu beachten, dass die sensiblen Daten wie privater Schlüssel und biometrische Referenzdaten auf der SmartCard abzulegen sind. Auch sind zum Schutz der digitalen Signatur die kryptographischen Berechnungen auf der SmartCard durchzuführen [8]. Da die Rechenkapazitäten von SmartCards begrenzt sind, müssen effiziente Algorithmen für die Unterschriftserkennung eingesetzt werden.
Es muss also ein mobiles Endgerät, bspw. in Form eines PDAs, als Signierwerkzeug zum Einsatz kommen. Dieses Endgerät muss die Erfassung biometrischer Merkmale durch eine geeignete Hardware unterstützen.

Abschließend lassen sich die folgenden Gestaltungskriterien für sichere Signierwerkzeuge nennen:

- Zur Freischaltung der digitalen Signatur ist ein Verfahren zur biometrischen Unterschriftserkennung einzusetzen.
- Als Signierwerkzeug ist ein mobiles Endgerät zu verwenden.

6. Ausblick

Die hier aufgezeigten Gestaltungsanforderungen und die daraus entwickelten Gestaltungskriterien sind zu vertiefen und durch weitere Anforderungen bzw. Kriterien zu ergänzen. Dabei wird primär das Ziel verfolgt, die Merkmale der eigenhändigen Unterschrift auf die digitale Signatur zu übertragen. Aus den verschiedenen Anforderungen, wie bspw. der mobile Einsatz digitaler Signaturen, entstehen Realisierungs- und Sicherheitsprobleme. Diese sind in weiteren Forschungsarbeiten aufzugreifen und entsprechende Lösungsansätze zu erarbeiten. So wird in Kooperation mit der Industrie sowohl die Benutzbarkeit und die Akzeptanz der eigenhändigen Unterschrift, als auch die Qualität der Unterschriftserkennung auf einem mobilen Endgerät untersucht.
Bei der Erarbeitung möglicher Lösungen steht vor allem die Benutzbarkeit des Signierwerkzeuges und damit die sichere Bedienbarkeit durch den Normalbenutzer und Sicherheitslaien im Vordergrund.

Quellenverzeichnis

[1] AgV Jahresbericht 1999/2000, April 2000. www.agv.de

[2] A. Albrecht, „Biometrie zum Nutzen für Verbraucher?“ *Datenschutz und Datensicherheit DuD*, 24(6):332-338, Juni 2000.

[3] D. Bartmann, „Benutzerauthentifizierung durch Analyse des Tippverhaltens mit Hilfe einer Kombination aus statistischen und neuronalen Verfahren“, *Dissertation*. Technische Universität München. 2000.

[4] D. Gerd tom Markotten, J. Kaiser, „Benutzbare Sicherheit – Herausforderungen und Modell für E-Commerce-Systeme“, *Wirtschaftsinformatik*, 6:531-538, Dezember 2000.

[5] J. Kaiser, „Integration vertrauter Merkmale als Gestaltungsprinzip für sichere Systeme“, *Informationstechnik und Technische Informatik (it+ti)*, 2001, Volume 43, Heft 5.

[6] M.D. Merrill, “Component Display Theory”, in: Reigeluth, C.M. (Ed.), *Instructional-design theories and models*, An overview of their current status, Hillsdale: Lawrence Erlbaum, 1983.

[7] A. Pfitzmann, B. Pfitzmann, M. Schunter, und M. Waidner, „Trustworthy User Devices”, in Günter Müller and Kai Rannenberg (Eds.), *Technology, Infrastructure, Economy, Volume 3 of Multilateral Security in Communications*, pages 137-156, Addison Wesley Longman Verlag GmbH, 1999. ISBN 3-8273-1360-0.

[8] T. Probst, „Biometrie und SmartCards“, *Datenschutz und Datensicherheit DuD*, 24(6):322-326, June 2000.

[9] T. Probst, M. Köhntopp, „Datenschutzgerechter und datenschutzfördernder Einsatz von biometrischen Verfahren - Potential biometrischer Systeme als Privacy-Enhancing Technologies“, Beitrag zum *Potential biometrischer Verfahren als datenschutzfreundliche Technologien* bei einem Expertenpanel des BSI, 19. November 1999 in Bonn.

[10] A. Roßnagel, *Die Simulationsstudie Rechtspflege: eine neue Methode zur Technikgestaltung für Telekooperation*, Ed. Sigma. 1994.

[11] D. Scheuermann and B. Struif, *Usability of Biometrics in Relation to Electronic Signatures*, Technical report, GMD-Forschungszentrum Informationstechnik, November 2000.

[12] A. Whitten, J.D. Tygar, “Why Johnny Can't Encrypt - A Usability Evaluation of PGP 5.0”, in *Proceedings of the 8th USENIX Security Symposium*, August 1999.