Elektronische Signatur – Eignung des biometrischen Merkmals „Fingerabdruck“ als möglicher PIN-Ersatz

Gottfried Daimer, Till Teichmann

Bayerische Hypo- und Vereinsbank AG
Sederanger 5
80538 München
gottfried.daimer@hvb.de, till.teichmann@hvb.de

Abstract: In diesem Dokument werden einige Aspekte der Verknüpfungsmöglichkeit zwischen elektronischer Signatur und Biometrie behandelt. Es werden die gesetzesmäßigen Anforderungen und die bestehenden Standards hinsichtlich der Einsatzmöglichkeiten biometrischer Verfahren beleuchtet. Die Auswirkungen beim Einsatz der Biometrie auf die verschiedenen Bereiche (wie z.B. Sicherheit, Prozesse und Benutzerfreundlichkeit) werden diskutiert.

1 Einführung

In einer Welt, in der elektronische Medien nicht mehr wegzudenken sind, spielen zwei Begriffe eine immer bedeutender Rolle: Elektronische Signatur und Biometrie. Die elektronische Signatur ist im Zusammenhang mit der Bestrebung sowohl staatlicher Stellen als auch privater Unternehmen zu sehen, ihre Verwaltung effizienter und bürgerfreundlicher bzw. ihre Geschäftsprozesse flexibler und produktiver als bisher zu gestalten. Die Bedeutung, die sie für diese Bestrebungen spielt, spiegeln sich in Initiativen wie Bund Online 2005[1] und dem Signaturbündnis[2], JobCard[3] oder der rechtlichen Gleichstellung der (qualifizierten) elektronischen Signatur mit der eigenhändig geleisteten Unterschrift wieder.

Biometrische Verfahren spielen vor allem bei der Identifikation und Authentisierung von Personen z.B. an Zugangssystemen eine bedeutende Rolle. Mit der Marktreife von einer Vielzahl von Systemen, die Personen anhand ihrer biometrischen Merkmale identifizieren, rückt jedoch immer mehr die mögliche Kombination der elektronischen Signatur mit biometrischen Verfahren zum Schutz von Sicherheitsfunktionen durch Benutzer-

---

[1] Ziel der Registrierungsinitiative "Bund Online 2005" ist es, alle onlinefähigen Dienstleistungen der Bundesverwaltung bis zum Jahr 2005 elektronisch verfügbar zu machen.

[2] Bündnis von Teilnehmern aus Staat und Wirtschaft, das auf Initiative der Bundesregierung initiiert wurde. Ziel des Bündnisses ist es, die Anwendung, Verbreitung und Einführung chipkartenbasierter elektronischer Signaturen und anderer PKI-Anwendungen in Deutschland zu fördern. [SBü04][Ros03]

[3] Modellprojekt der Bundesregierung zur zentralen Speicherung von Arbeitnehmerdaten unter Einsatz der elektronischen Signatur. [JC04]

Authentisierung in den Mittelpunkt des Interesses. Die biometrische Authentisierung kann daher als Ersatz oder Ergänzung zur Prüfung der Personal Identification Number (PIN) verwendet werden.

2 Grundbegriffe

Durch die **Authentifizierung** wird die Identität einer Person anhand eines bestimmten Merkmals, z.B. des Fingerabdruckes, überprüft. Eine Authentifizierung kann anhand der Merkmale Besitz, Wissen, Sein (biometrisches Merkmale) und Ort erfolgen.

Anhand verschiedener Kriterien werden in Tabelle 1 die biometrischen Merkmale den Authentifizierungsmerkmalen "Besitz" und "Wissen" gegenüber gestellt:

	Wissen	**Besitz**	**Biometrie**
Beispiele	Passwort, PIN	Schlüssel, Ausweis	Fingerabdruck, Gesicht
Kopierbarkeit	„Software“	einfach bis sehr schwierig	einfach bis sehr schwierig
Verlust	„vergessen“	einfach	schwierig
Diebstahl	ausspionieren	möglich	sehr schwierig
Weitergabe	einfach	einfach	einfach bis schwierig
Änderbarkeit	einfach	einfach bis schwierig	einfach bis sehr schwierig

Tabelle 1: Vergleich Authentifizierungsverfahren

Zur Authentifizierung einer Person kann eine Kombination von zwei oder mehr der genannten Möglichkeiten benutzt werden. Ein Beispiel dafür ist die Authentifizierung am Geldautomaten. Zum einen ist man im *Besitz* einer ecKarte, zum anderen besitzt man das *Wissen* der zur ecKarte gehörigen PIN. Je mehr der genannten Möglichkeiten verwendet werden, desto höher ist die Sicherheit, dass es sich um die entsprechende Person handelt.

Gemäß § 2 Z 1. [SigG01] definiert sich die (einfache) **elektronische Signatur** als "Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen". Dies kann ein einfaches, an eine Email angehängtes Bild sein. So eine einfache elektronische Signatur ist nicht zweifelsfrei einer Person zuzuordnen. Es bedeutet, dass sie weder die Integrität des signierten Dokumentes noch die Authentizität des Unterzeichners sicherstellt und somit keine juristische Beweiskraft besitzt.

Um rechtlich wirksame Geschäfte zu tätigen, ist mindestens eine fortgeschrittene oder qualifizierte elektronische Signatur erforderlich, die den Anforderungen des § 2 Z 2 [SigG01] bzw. des § 2 Z 3 [SigG01] genügt. Sie wird mit Hilfe mathematischer Verfahren und eines privaten kryptografischen Schlüssels generiert. Ausschließlich mit dem dazugehörigen öffentlichen Schlüssel und mit dem dazugehörigen Zertifikat kann die geleistete elektronische Signatur jederzeit überprüft und dem Schlüsselinhaber eindeutig zugewiesen werden. Auf diese Weise kann die Unverfälschtheit der Daten (Integrität) und die Authentizität des Autors eindeutig verifiziert werden.

Biometrie ist die Lehre von der Vermessung körpereigener Eigenschaften. Bei ihr erfolgt die Erhebung bestimmter physischer / physiologischer (passiver) Merkmale oder verhaltenstypischer (aktiver) Merkmale von Personen, wie z.B. des Fingerabdruckes, der Stimme / des Sprachverhaltens, des Tippverhaltens (z.B. PSYLock der Universität Regensburg [Ba04]), der Handgeometrie oder der Augen-Iris- oder Retina-Merkmale.

Die erhobenen individuellen Daten werden mit Hilfe mathematisch-statistischer Methoden ausgewertet und die Ergebnisse zur Identifizierung (aus einem undefinierten Personenkreis) oder zur Authentifizierung (aus einem definierten Personenkreis) des Users verwendet. Ein detaillierter Vergleich der verschiedenen biometrischen Verfahren ist nicht Gegenstand dieser Arbeit. Für eine Vertiefung dieses Themas wird daher auf weiterführende Fachliteratur verwiesen (z.B. [LS01]).

3 Authentifizierung: Besitz und Wissen vs. Biometrie

Ein Vergleich der heute in der Praxis verwendeten Authentifizierungsverfahren zeigt, dass diese eine erhebliche Sicherheitslücke aufweisen. Im Folgenden werden die heute gängigen Authentifizierungsverfahren der Biometrie gegenübergestellt und anhand möglicher Risiken bewertet. Außerdem werden biometrische Authentifizierungsverfahren mit ihren Vor- und Nachteilen als Alternative zu den heute verwendeten dargestellt.

3.1 Sicherheitslücke der Authentifizierungsverfahren: Wissen

Geheimzahlen / PINs und Passwörter (Wissen) können vergessen oder aufgrund mangelhafter Vorsichtsmassnahmen erraten, ausspioniert oder gestohlen werden. Darüber hinaus können sie leicht mutwillig weitergegeben werden (Angriff von Innen). Ein Passwort kann zudem mit Hilfe von Brute-Force[4]- oder Wörterbuch-Attacken[5] erraten werden.

3.2 Sicherheitslücke der Authentifizierungsverfahren: Besitz

Eine Karte, ein Token oder ein Schlüssel (Besitz) kann gestohlen werden. Im worst-case-Szenario gibt der Besitzer ungewollt seine Authentifizierungsmerkmale „Besitz“ und „Wissen“ an eine fremde Person. Die Wahrscheinlichkeit des Missbrauchs dieser Merkmale ist daher sehr hoch. Es sei denn, der rechtsgültige Besitzer reagiert schnell und ändert seine PIN bzw. lässt seine Chipkarte sperren, bevor der Angreifer diese missbrau-

---

[4] Versuch, ein Passwort zu erraten, indem vom Angreifer alle (oder zumindest eines erheblichen Teils der in Frage kommenden) Varianten ausprobiert werden. [Sch96]

[5] Angriffsmethode, bei der vom Angreifer versucht wird, von einem bekannten Passwort auf andere Passwörter zu schließen.

chen kann. Zusätzlich besteht die Gefahr, dass der Besitzer das Merkmal mutwillig weitergegeben kann.

3.3 Biometrische Authentifizierungsverfahren als Alternative

Die in Kapitel 3.1 und 3.2 beschriebenen Schwächen der Authentifizierungsverfahren mittels Wissen oder Besitz können mit dem Einsatz eines biometrischen Merkmals als Ersatz für die PIN behoben werden.

Da das **Fingerabdruck-Verfahren** eines der bekanntesten und für den betrachteten Sachverhalt am besten einsetzbar ist, werden im Folgenden einige Argumente für und wider den Einsatz speziell dieses Authentifizierungsverfahrens diskutiert. Der Leser soll erfahren, an welchen Problemen der Einsatz des Fingerabdruck-Verfahrens als Ersatz für die PIN bisher gescheitert ist. Jedoch soll zudem vor Augen geführt werden, wie sinnvoll der Einsatz dieses Authentifizierungsverfahrens in diesem Zusammenhang wäre.

Die Datenerhebung und –verifizierung erfolgt bei diesem Verfahren durch das Auflegen eines Fingers auf die Oberfläche eines Sensors. Dieser scannt den Fingerabdruck, wobei die sog. Minuzien (Linienendungen, Verzweigungen), aber auch die makroskopische Merkmale des Fingers (Linien, Schleifen, Bögen) von Bedeutung sind. Das Scann-Ergebnis wird zur Berechnung des zum Fingerabdruck gehörigen Hash-Wertes, der im Personalisierungsvorgang auf der Chipkarte abgelegt wird, oder zum Vergleich mit einem bereits erzeugten Hash-Wert des gleichen Fingerabdrucks verwendet. Die Rohdaten, die bei dem Scan-Vorgang eines Fingerabdrucks erhoben und abgespeichert werden, betragen ca. 65 kb. Die anfallenden Daten werden mit einem Algorithmus komprimiert, so dass nur noch wenige 100 Bytes pro Fingerabdruck anfallen.

Folgende **Vorteile** sprechen für den Einsatz des Fingerabdrucks als PIN-Ersatz: Während bei Authentifizierungsverfahren anhand von Besitz und / oder Wissen eine personenbezogene Authentifizierung zugrunde liegt, spricht man bei biometrischen Authentifizierungsverfahren von p**ersonengebundener Authentifizierung**. Aus diesem Grund kann das biometrische Merkmal "Fingerabdruck" im Gegensatz zu den Authentifizierungsverfahren mittels Besitz und Wissen weder vergessen, verloren noch entwendet werden. Der Benutzer führt dieses immer mit sich. Außerdem ist mit dem Einsatz des Fingerabdruckes eine Vereinfachung des Authentifizierungsprozesses verbunden: Statt eine mehrstellige PIN einzugeben wird nur ein Finger auf einen Sensor aufgelegt. Insgesamt ist dadurch im Vergleich zu den Authentifizierungsmerkmalen mittels Besitz und Wissen eine Erhöhung der **Benutzerfreundlichkeit** gegeben.

Neben der verbesserten Benutzerfreundlichkeit auf Kundenseite können auf Seiten des Anbieters **Kosteneinsparungen** realisiert werden. Diese resultieren aus der Tatsache, dass der Druck und der Versand von PIN-Briefen entfallen und der HelpDesk- bzw. Hotline-Aufwand für das Zurücksetzen bzw. die Neuvergabe von Passwörtern bzw. PINs nicht mehr erforderlich ist. Zusätzlich bedeutet der Einsatz des biometrischen Merkmals "Fingerabdrucks" einen **Sicherheitsvorteil**. Das physische Merkmal einer Person ist

nicht auf eine andere Person übertragbar. Die entsprechende Qualität des Systems vorausgesetzt, ist damit in automatisierten Systemen in stärkerem Maße davon auszugehen, dass die Person selbst sich gegenüber dem System authentifiziert, als etwa bei PIN- oder Passwort-Systemen.

Den genannten Vorteilen bei der Verwendung des Fingerabdrucks zur Benutzer-Authentifizierung stehen folgende **Nachteile** gegenüber: Biometrische Merkmale sind zum Teil von äußeren Einflüssen abhängig. So kann z.B. der Hautzustand (u.a. Trockenheit, Feuchtigkeit) die Erfassungsgenauigkeit des Fingerabdrucks beeinflussen.

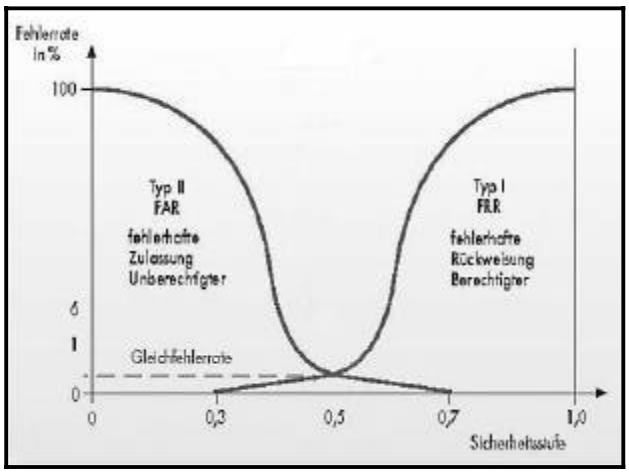

Abbildung 1: Fehlerkurven

Aus diesem Grund ist niemals eine hundertprozentige Übereinstimmung zwischen dem bei der Registrierung der Person festgestellten Referenzwertes und dem beim Authentifizierungsvorgang erhobenen Fingerabdrucks möglich. Daher wird es immer einen minimalen Prozentsatz an Personen geben, die fälschlicherweise abgewiesen (FRR = False Rejection Rate[6]) oder fälschlicherweise als berechtigte Personen identifiziert (FAR = False Acceptance Rate[7]) werden. Die **Zuverlässigkeit von biometrischen Systemen** ist nicht 100%-ig gesichert. Dieser Mangel ist jedoch vernachlässigbar, wenn zur eindeutigen Authentifizierung des Benutzers zudem die entsprechende Chipkarte vorhanden ist (Besitz plus biometrisches Merkmal).

Des Weiteren besteht die Möglichkeit ein biometrisches System mittels eines gut erfassten Abbildes des Fingerabdrucks (z.B. mit Hilfe eines Silikon- oder Gelantinefingers)[Ma02] zu täuschen. Zur Vermeidung dieses Missbrauchs wäre eine so genannte

---

[6] Die Fehlabweisungsrate wird berechnet als FRR = (Anzahl fehlerhafter Zurückweisungen) / (Anzahl der autorisierten Zugriffsversuche) X 100.

[7] Die Falschakzeptanzrate errechnet sich nach folgender Formel: FAR = (Anzahl fehlerhafter Identifizierungen) / (Anzahl der nicht autorisierten Zugriffsversuche) X 100.

Lebenderkennung[8] notwendig. Eine Lösung dieses Problems ist zum einen organisatorisch, zum anderen technisch denkbar. Organisatorisch wäre eine zusätzliche Kontrolle durch Dritte (z.B. in der Filiale) möglich. Technisch existiert derzeit noch keine hinreichend gute Lösung.

Ein weiteres Problem stellt die Tatsache dar, dass Personen (z.B. aus "Berufsgruppen mit hohem Anteil an handwerklichen Tätigkeiten" (vgl. hierzu [LS01], S. 107) nicht anhand ihres Fingerabdruckes identifiziert werden können. Der Anteil dieser Personen liegt bei maximal einem Prozent und kann somit vernachlässigt werden.

4 Anforderungen an biometrische Authentifizierungsverfahren im Allgemeinen und das Fingerabdruck-Verfahren im Speziellen

An alle biometrischen Verfahren werden allgemeine Anforderungen zur eindeutigen Authentifizierung von Personen gestellt: Das zu verwendende biometrische Merkmal muss zum einen bei einer ausreichend großen Anzahl der Personen vorhanden sein (**Universalität**) und sich bei jedem der Personen hinreichend unterscheiden (**Einzigartigkeit**). Darüber hinaus darf das biometrische Merkmal im Laufe der Zeit keinen Veränderungen unterworfen sein (**Beständigkeit**) und muss durch ein technisches System quantitativ messbar sein (**Erfassbarkeit**).

Des Weiteren müssen von den biometrischen Authentifizierungsverfahren folgende Kriterien erfüllt sein, damit sie als praxistauglich eingestuft werden können. Als eines der Kriterien ist die **technische Umsetzbarkeit** des Verfahrens zu nennen, die durch die Schnelligkeit und die Kompatibilität der Verfahren bedingt ist. Dieses Kriterium wird durch das Fingerabdruck-Verfahren erfüllt: Der Durchschnittswert für die Überprüfung eines Fingerabdruckes liegt zurzeit bei etwa zehn Sekunden. Durch die heute gegebene Standardisierung der Verfahren ist die Kompatibilität der verschiedenen Lösungen untereinander sichergestellt.

Zudem müssen von der zum biometrischen Verfahren gehörigen Hardware folgende Kriterien erfüllt sein: **Robustheit**, **Genauigkeit** und **Sicherheit.** Diese Eigenschaften werden durch die heute zur Verfügung stehenden Fingerabdruck-Scanner zum Teil erfüllt: Sie sind robust und scannen den Fingerabdruck in ausreichender Qualität ein. Jedoch ist die Überwindungsresistenz bei den heutigen Sensoren nur teilweise gegeben, weil ein Scanner durch ein künstliches Abbild des Fingerabdrucks getäuscht werden kann.

Eine wichtige Rolle bei der Realisierung von biometrischen Verfahren spielt die **ökonomische Machbarkeit**. Der Aufwand muss in einem gesunden Verhältnis zum Nutzen stehen. Insgesamt ist festzustellen, dass die Kosten für Fingerabdruck-Sensoren allge-

---

[8] Unter einer Lebenderkennung wird der Nachweis verstanden, dass eine natürliche Person das physische Merkmal am Sensor abgibt.

mein in den letzten Jahren erheblich zurückgegangen sind. Innerhalb der Produktpalette weisen die Streifensensoren das beste Preis-Leistungs-Verhältnis auf.

Die **Nutzerfreundlichkeit** (Zuverlässigkeit, Einfachheit und Hygiene) als ein weiteres zu erfüllendes Kriterium ist für die Praxistauglichkeit bei dem Fingerabdruck-Systemen gegeben: Sie arbeiten bis zu einem bestimmten Grad zuverlässig (vgl. hierzu FRR bzw. FAR in Kapitel 3.4). Da es sich bei Fingerabdrucksystemen im Allgemeinen um lokale Systeme handelt, werden diese nur von wenigen Personen – meist jedoch nur von einer Person – benutzt. Daher liegt in diesem Fall kein Problem mit der Hygiene des Systems vor. Es können im Allgemeinen keine gesundheitlichen Schäden auftreten.

Das letzte zu betrachtende Kriterium stellt die Gewährleistung des **Datenschutzes** dar. Dieser ist bei dem Fingerabdruckverfahren gegeben, wenn die Referenzdaten (Hash-Wertes des erhobenen Fingerabdruckes) auf einem sicheren Medium aufbewahrt werden und dieses nicht mehr verlassen können.

5 Technische Aspekte bei der Verwendung von biometrischen Authentifizierungsverfahren

5.1 (De-)Zentrale Ablegung des physischen Merkmals

Allen biometrischen Verfahren gemeinsam ist, dass vor der möglichen Authentifizierung der Einzelperson ein Referenzwert erhoben und an zentraler oder dezentraler Stelle abgelegt werden muss (**Aufnahme** und **Speicherung**). Da das aktuell erhobene physische Merkmal beim Authentifizierungsvorgang gegen diesen Referenzwert abgeglichen wird und dieses Merkmal nicht wie eine PIN oder ein Passwort austauschbar ist, ist eine missbräuchliche Verwendung dieser Daten zu verhindern. Dies wird durch die Speicherung des physischen Merkmals auf einem Datenträger, der sich in der persönlichen Verwahrung des Benutzers (z.B. Chipkarte) befindet, geleistet. Ein zusätzlicher Vorteil dieser Lösung ist, dass dem Benutzer eventuell vorhandene Ängste vor Verletzung des Datenschutzes bzw. seiner persönlichen Rechte genommen werden können.

5.2 Unterschiedliche Authentifizierungsverfahren auf der Chipkarte

Bisher wurden Chipkarten in der Biometrie nur als Datenträger genutzt. Zur Erhöhung der Sicherheit biometrischer Systeme erscheint es notwendig, nicht nur die Referenzdaten in einer Chipkarte zu speichern, sondern dort auch den Vergleich mit den aktuell aufgenommenen Verifikationsdaten in der Chipkarte durchzuführen. Auf diese Weise könnte die Chipkarte die eigentliche Authentifizierung ausführen, ohne dass die Referenzdaten die Karte verlassen und nach erfolgreicher Authentifizierung die Anwendung

"elektronische Signatur" zur Benutzung freigeben. Die Authentifizierung des Benutzers anhand des Fingerabdruckes kann mittels zweier unterschiedlicher Verfahren (template-on-card (TOC) oder dem match-on-card (MOC)) erfolgen.

Bei dem Verfahren **template-on-card (TOC)** werden die Daten zur Authentifizierung von der Karte an eine entsprechende externe Entscheidungsinstanz (z.B. einen zentralen Server) gesendet. Die Instanz überprüft den aktuell eingescannten Fingerabdruck mit den gespeicherten Daten auf der Karte. Verläuft diese Prüfung erfolgreich, wird der Zugang zur geschützten Anwendung (z.B. elektronische Signatur) freigegeben. Andernfalls wird der Benutzer zurück gewiesen. Da bei diesem Verfahren die Kommunikation mit einer externen Instanz stattfindet, besteht die Gefahr der Datenmanipulation durch einen Angreifer. Dieser kann sich damit den unerlaubten Zugriff auf eine bestimmte Anwendung oder ein System verschaffen.

Bei dem Verfahren **match-on-card (MOC)** erfolgt der Abgleich des aktuell eingescannten Fingerabdrucks mit dem auf der Karte abgelegten Referenzwert innerhalb der Karte. Dies bedeutet, dass die biometrischen Daten zu keinem Zeitpunkt die Chipkarte verlassen. Ein Missbrauch der persönlichen Daten ist hierdurch nahezu ausgeschlossen. Einen weiteren Vorteil stellt die Tatsache dar, dass die aufwendige Pflege der Datenbank für die biometrischen Merkmale entfällt.

5.3 Vergleich von Fingerabdruck-Sensoren

Zum Einlesen des Fingerabdruckes können unterschiedliche **Ausprägungen von Sensoren** zum Einsatz kommen: Ein einfacher Fingerabdruck-Sensor, ein Kartenleser mit Fingerabdruck-Sensor oder eine Tastatur mit Fingerabdruck-Sensor. Bei einem einfachen Fingerabdruck-Sensor besteht die Gefahr der Manipulation durch Dritte, da zum Abgleich des aktuell eingescannten Fingerabdrucks mit dem Referenzwert eine Kommunikation zwischen dem externen Fingerabdruck-Sensor und dem zugehörigen System (Rechner) stattfinden muss. Eine Tastatur mit Fingerabdruck-Sensor macht aus sicherheitstechnischer Sicht nur Sinn, wenn in dieser zusätzlich auch der Chipkartenleser integriert ist und der Abgleich der Referenzwerte innerhalb der Tastatur erfolgt. Die optimale Lösung stellt ein Kartenleser mit integriertem Fingerabdruck-Sensor dar, da hier die Authentifizierung des Benutzers mittels match-on-card-Verfahren stattfindet.

Hinsichtlich des **Scan-Verfahrens** können die Fingerabdruck-Sensoren untergliedert werden in Vollbild- und Streifen-Sensoren. Die Streifen-Sensoren sind sehr viel günstiger, da die Sensorfläche erheblich kleiner ist als bei den Vollbild-Sensoren. Ein Nachteil dieser Sensoren besteht in der evtl. Bildverzerrung, die durch die Bewegung des Fingers auftreten kann. Dieser Nachteil wird jedoch mit zunehmender technischer Weiterentwicklung in der nächsten Zeit behoben werden.

In Einzelfällen besteht bei bestimmten Fingerabdruck-Sensoren die Möglichkeit, dass sich auf dem Sensor verbleibende Latenzfingerabdrücke ohne Anwesenheit des Berechtigten (z.B. durch Anhauchen) reaktivieren lassen. Damit sind eine unerwünschte Akzeptanz und ein Missbrauch möglich. Die Behebung bzw. Vermeidung dieses Problems,

dass nur bei Flächensensoren auftreten kann, erfolgt durch geeignete Software- und Systemmaßnahmen. Entsprechende Software-Lösungen speichern die Lagekoordinaten der einzelnen eingescannten Fingerabdrücke ab und lehnen Fingerabdrücke ab, deren Lage genau mit dem letzten Abdruck übereinstimmt.

6 Gesetzliche Rahmenbedingungen und Standards

Wenn das biometrische Merkmal "Fingerabdruck" im Bereich der elektronischen Signatur als Ersatz für die PIN verwendet werden soll, sind bei der Realisierung einige gesetzliche Rahmenbedingungen und technische Standards zu berücksichtigen. Im Folgenden erfolgt eine kurze Gegenüberstellung der gesetzlichen Grundlagen, die für den Einsatz des Fingerabdrucks als PIN-Ersatz bei der elektronischen Signatur eine Rolle spielen: Das Signaturgesetz in Verbindung mit der Signaturverordnung in der Fassung des Jahres 2001 und die EU-Richtlinie aus dem Jahr 1999. Außerdem wird unter Hinzunahme der beiden erstgenannten Gesetzestexte in der Fassung des Jahres 1997 eine kurze historische Entwicklung der biometrischen Merkmale zur Authentifizierung vor Freigabe der elektronischen Signatur aufgezeigt.

6.1 Signaturgesetz und Signaturverordnung

In § 16 Abs. 2 Satz 3 der [SigV97] ist die Nutzung biometrischer Merkmale als zusätzliches Identifikationsmerkmal (zu Besitz und Wissen) vorgesehen. Bei elektronischen Signaturen ist allerdings zu beachten, dass die biometrische Identifikation nach Artikel 3, [1] des [SigG97]) nur zusätzliches Merkmal zur wissensbasierten Identifikation (PIN-Eingabe) zugelassen ist (vgl. §16, [4] [SigG97]).

In Rahmen der Neuformulierung des Signaturgesetzes von 2001 wurde der vielfachen Forderung aus Fachkreisen entsprochen, die Nutzung biometrischer Merkmale künftig nicht nur ergänzend, sondern auch als Alternative zur PIN zuzulassen. Erstmals sind damit für die Authentifizierung von Nutzern der elektronischen Signatur neben Passwort- und Geheimzahlen auch biometrische Merkmale gestattet.

Der Forderung des Signaturgesetzes, dass dem Signator die vollständige Kontrolle über den Signaturvorgang zu gewähren und „die unbefugte Verwendung von Signaturerstellungsdaten verlässlich [zu] verhindern“ (§ 18 Abs. 1 [SigG01]) ist, ist durch die Verwendung eines biometrischen Merkmals als Personen gebundenes Merkmal eher möglich als durch das Authentifizierungsmerkmal PIN. Denn zur erfolgreichen Authentifizierung ist in diesem Fall der Besitz der Karte und körperliche Anwesenheit des rechtskräftigen Besitzers der Karte zwingend erforderlich. Bei Verwendung der Merkmale "Besitz" und "Wissen" ist dagegen der Besitz der Karte und nur die "Anwesenheit" der zugehörigen PIN erforderlich. Diese jedoch kann gestohlen worden sein.

Eine weitere implizite gesetzliche Forderung des [SigG01] und des [SigV01] besteht darin, dass die Chipkarte vor der ersten Nutzung zur Erzeugung einer elektronischen Signatur durch einen entsprechenden Authentifizierungsmechanismus initial "entriegelt" werden muss. Dies kann z.B. durch eine Transport-PIN oder aber durch einen Fingerabdruck geschehen. Im zweiten, dem sichereren Fall ist eine mit biometrischer Funktionalität ausgestattete Karte notwendig. Bei Verwendung einer Transport-PIN besteht die Gefahr, dass diese durch eingeschleuste Hacker-Software abgefangen wird. Einmal im Besitz der (Transport-)PIN kann ein Angreifer in weiterer Folge beliebig viele zu signierende Daten an die Chipkarte senden. Der Chipkarte ist es nicht möglich zu erkennen, ob die (Transport-)PIN vom legitimen Benutzer eingegeben wurde oder ob er von einer Hacker-Software gesandt wurde. Diese Problematik ist bei Verwendung des Fingerabdrucks als biometrisches Merkmal erheblich entschärft.

	1997	2001
Ziel	Ausschluss einer möglichen Authentifizierung durch eine andere Person (z.B. durch Weitergabe der PIN).	Erhöhung des Komforts für den Nutzer, indem es sich keine PIN mehr merken braucht.
Biometrie	Es wird immer eine Chipkarte (Nachweis des Besitzes) und eine PIN (Nachweis des Wissens) zur Erzeugung der elektronischen Signatur benötigt. Die Biometrie ist nur eine mögliche Ergänzung.	Es wird immer eine Chipkarte (Nachweis des Besitzes) gefordert. Neben der PIN (Nachweis des Wissens) zur Erzeugung der elektronischen Signatur wird als gleichwertige Alternative zugelassen.

Tabelle 2: Vergleich Signaturgesetz von 1997 und 2001

In Tabelle 2 werden die Ziele der Gesetzesgrundlage und die Berücksichtigung der Biometrie in diesen Gesetzestexten der Fassung aus dem Jahr 1997 mit der Fassung des Jahres 2001 verglichen. Es zeigt sich eine deutliche Erweiterung des Fokuses.

6.2 EU-Richtlinie von 1999

In der EU-Richtlinie von 1999 zur elektronischen Signatur sind ausschließlich allgemeine Anforderungen enthalten. Die sichere Signaturerstellungseinheit muss gewährleisten, dass „die für die Erzeugung der Signatur verwendeten Signaturerstellungsdaten mit hinreichender Sicherheit nicht abgeleitet werden können …“[EU99].

6.3 Datenschutzrechtliche Aspekte

In der Öffentlichkeit wird der Einsatz von biometrischen Verfahren besonders intensiv diskutiert. Ein Thema, das die Menschen dabei besonders beschäftigt, ist die Verletzung ihrer Persönlichkeitsrechte oder der Schutz ihrer persönlichen Daten. Viele haben Bedenken, dass mit ihren biometrischen Daten Missbrauch getrieben werden kann. Oft

scheitern Projekte schon an der Tatsache, dass der Nutzen und die Missbrauchsmöglichkeiten gegenübergestellt werden und die Fronten sich total verhärten. Aus diesem Grund ist es wichtig, dass auch bei Verwendung von biometrischen Merkmalen datenschutzrechtliche Aspekte eine besondere Beachtung erfahren.

Aus datenschutzrechtlicher Sicht spricht nichts gegen den Einsatz einer Chipkarte mit biometrischen Daten, wenn diese ausreichend geschützt sind. Durch das in Kapitel 5.2 beschriebene MOC-Verfahren wird das Auslesen biometrischer Informationen aus der Chipkarte verhindert.

6.4. Standards

Für die Chipkarte bestehen bereits Standards und Spezifikationen, die die Identifikation und Authentifikation mittels dieses Trägermediums detailliert regeln. Biometrische Verfahren wurden international in den ISO/IEC SC 37 Standardisierungsgruppen spezifiziert.

ISO/IEC 7816-11 ist der wichtigste Standard für den Einsatz biometrischer Verfahren in Verbindung mit Chipkarten. Teile des Chipkarten-Standards ISO/IEC 7816 wurden innerhalb des Subkomitees “Cards and Personal Identification“ (SC 17) erneut überarbeitet. Im Besonderen erfolgte eine Anpassung des vierten Teils ("Organization, security and commands for interchange") dieses Standards, in dem Kartenkommandos und Datenobjekte spezifiziert werden, die für die biometrische Benutzer-Authentisierung relevant sind. In Teil 11 ("Personal verification through biometric methods") des Chipkarten-Standards ISO/IEC 7816 werden die Kartenkommandos für die biometrische Benutzer-Authentisierung beschrieben. In diesem Teil wurde unter anderem auch das Match-on-card (MOC) Verfahren inklusive der zu verwendenden Formate standardisiert. Es wurde auch bereits in [CWA04] integriert.

In [Te04] wird für die Verifikation des Besitzers auf den [RFC01] verwiesen, in dem die genaue Syntax für die Speicherung und Verwendung von biometrischen Daten beschrieben wird. Für den Einsatz von Fingerabdrucksensoren sind folgende Standards entscheidend:

- ISO/IEC 19794 Biometric Data Interchange Formats
- ISO/IEC 19785 CBEFF (Common Biometric Exchange File Format)
- ISO/IEC 19784 BioAPI (Rahmenformat zum Austausch biometrischer Daten und das “Biometric Application Programming Interface“

7 Schlussfolgerungen und Ausblick

Die in diesem Papier geführte Diskussion zeigt, dass die Biometrie (Fingerabdruck), Chipkarten und elektronische Signaturen eine mögliche Kombination darstellen. Die

Chipkarte sorgt dafür, dass der geheime Schlüssel, die Karte nicht verlässt und aufgrund des match-on-card-Verfahrens ist es nicht möglich, dass der Zugriff auf Anwendungen der Chipkarte durch unautorisierte Personen geschieht oder persönliche biometrische Daten aus dem Chip der Karte ausgelesen werden. Neben der Sicherheit wird durch diese Kombination außerdem die Benutzerfreundlichkeit verbessert. Insgesamt gesehen ist trotz der genannten Nachteile ein Einsatz der Biometrie als PIN-Ersatz zu befürworten. Allerdings ist ein hoher Grad an Überzeugungsarbeit zu leisten, um den Anwender von den genannten Vorteilen bzw. dem Mehrwert der genannten Kombination zu überzeugen.

Literaturverzeichnis

[Ba04] Bartmann, D.; Breu, C.: Eignung des psychometrischen Merkmals Tippverhalten zur Benutzerauthentisierung, In: Bartmann et al. (Hrsg.): Kopplung von Anwendungssystemen–FORWIN-Tagung 2004. Aachen 2004. S.321-343.

[CWA04] CWA 14890: Application Interface for Smart-Cards used as Secure Signature Creation Devices, CEN ISSS ESIGN K Specification, 2004.

[EU99] EU-"Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen", Richtlinie 1999/93/EG, 1999

[GIF03] Global Interoperability Framework for identification, authentication and electronic signatures (IAS) with smart cards, Part 1, 2, 3, March 2003.

[ISO7816] ISO/IEC 7816 Identifion cards – Integrated circuit(s) cards with contacts, Part 4, 11, 2003.

[JC04] http://www.itsg.de/download/BroschuereJobcard.pdf, Abruf am 15.11.2004.

[LS01] Lenz, J-M; Schmidt, C.: Die elektronische Signatur, Bank-Verlag Köln, 2001.

[Ma02] Matsumoto, Tsutomu et. al.: Imput of artifial „gummy" fingers on Fingerprint Systems, http://cryptome.org/gummy.html, 2002

[RFC01] RFC 3039 – Internet X.509 Public Key Infrastruture Qualified Certificate Profile, 2001.

[Ros03] Rosenhauer, Albrecht: Signaturbündnis. Vorgaben und Konvergenzziele für das Signaturbündnis, In: DuD 6 / 2003, S. 363-369

[SBü04] www.signaturbuendnis.de, Abruf am 15.11.2004.

[Sch96] Schneier, Bruce: Angewandte Kryptographie: Protokolle, Algorithmen und Sourcecode in C, Addison-Wesley, 1996.

[SigG97] Bundesministerium für Wirtschaft und Arbeit: Gesetz über Rahmenbedingungen für elektronische Signaturen, 1997

[SigV97] Bundesministerium für Wirtschaft und Arbeit: Verordnung zur elektronischen Signatur (Signaturverordnung- SigV), 1997

[SigG01] Bundesministerium für Wirtschaft und Arbeit: Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften, Bundesgesetzblatt S.876 ff, 2001.

[SigV01] Bundesministerium für Wirtschaft und Arbeit: Verordnung zur elektronischen Signatur (Signaturverordnung- SigV), Bundesgesetzblatt S.3074, 2001.

[Sm02] Smith, R.E.: Authentication. Addision Wesley, 2002.

[Te04] ISIS-MTT Working Group of TeleTrusT Deutschland e.V.: ISIS-MTT, Version 1.1. Format-Verlag, Bonn, 2004.