DuD
Datenschutz und Datensicherheit

Biometrische Ausweise

Schutz von Personenidentitäten trotz biometrischer Erkennung

Gerrit Bleumer

Wir erleben die rasante Entwicklung zur Informationsgesellschaft. Vorher getrennte IT-Systeme werden zu einem globalen IT-System integriert, das gleichzeitig Dienste bereitstellt und Zugang zu Diensten, Waren und Geld kontrolliert. Um Mißbrauch zu begrenzen, wird die automatisierte biometrische Erkennung von Personen so normal wie heute das Benutzen von Paßwörtern. Sofern diese Entwicklung zur ungehinderten Proliferation biometrischer Daten führt, wird sie zu einer ernsten Bedrohung der Demokratie. Auch wenn es paradox klingt: Biometrische Erkennung ist möglich, ohne den prüfenden Stellen oder anderen Institutionen Zugriff auf die biometrischen Daten zu geben. Wir geben eine technische Lösung, die sich auf jüngste Forschungsergebnisse stützt.

[FOTO]

Dipl.-Inform.
Gerrit Bleumer

AT&T Labs, USA
Arbeitsschwerpunkte
• Kryptographie,
• sichere Zahlungs systeme,
• IT-Sicherheit im Gesundheitswesen
E-Mail: bleumer@acm.org

Einleitung

Wir beobachten den zunehmenden Einsatz biometrischer Erfassung von Personen und anschließender automatischer Erkennung. Insbesondere in der Strafverfolgung, aber auch bei der Videoüberwachung öffentlicher Gebäude, Straßen, Mietgaragen und Parks wird diese Methode eingesetzt. Daneben gibt es immer mehr Ressourcen im täglichen Leben, die aufgrund großen Bedarfs automatisierte Zugangskontrollen erfordern.

Autofahrer werden an Mautstellen vor Brücken, Autobahnauffahrten und Tunneln durch Videokameras erfaßt. Unternehmen, Krankenhäuser und Behörden schützen ihre Gebäude, Räume, Computer und Safes durch Fingerabdruckleser. Manche Unternehmen erfassen die Arbeitszeit ihrer Mitarbeiter, indem sie die Gesichter der ein- und ausgehenden Personen automatisch erkennen und auswerten. Banken rüsten Geldautomaten mit Videokameras aus, um durch Gesichtserkennung Kartenmißbrauch an der Quelle zu bekämpfen. Die Autoindustrie entwickelt biometrisch geschützte Fahrzeugtüren und Zündschlösser, die auf den richtigen Daumen reagieren. Man hofft, Fahrzeugdiebstahl unattraktiv zu machen und Minderjährige am Fahren zu hindern.

Die konsequente Weiterentwicklung biometrischer Erkennungsmethoden wird in Zukunft auch ermöglichen, nicht-übertragbare Ausweise elektronisch zu realisieren. Anwendungsbeispiele sind elektronische Führerscheine, Mitgliedsausweise, Fahrkarten für den Nahverkehr, Stimmzettel für Wahlen etc.

Biometrische Erkennungsmethoden sind für die erfaßten Personen deutlich bequemer und in bestimmter Hinsicht auch sicherer als konventionelle Erkennungsmethoden, die sich auf PINs, Paßwörter oder Magnetkarten stützen: Biometrische Merkmale kann man nicht vergessen oder verlieren, und man braucht und kann sie nicht in regelmäßigen Zeitabständen zu ändern.

Allein in den USA wurden 1998 rund 250 Mio. Dollar in Hard- und Software investiert, die zur biometrischen Personenerkennung dient; davon etwa 50% in der Strafverfolgung und von Geheimdiensten, 30% von Banken und Versicherungen, und 12% von Sicherheitsdiensten [11].

Biometrische Merkmale sind prinzipiell geeignet, Personen während ihres ganzen Lebens an jedem Ort schnell und zuverlässig zu identifizieren. Damit sind prinzipiell alle politischen, wirtschaftlichen und sozialen Rollen einer Person verkettbar. Wie sich jemand als Kunde, Patient, Autofahrer oder Mieter verhält, kann jederzeit Einfluß auf seine Behandlung als Versicherter, Kontoinhaber oder Arbeitnehmer haben und umgekehrt.

> Wird die Verbreitung persönlicher biometrischer Daten durch weiträumigen und unbedachten Einsatz biometrischer Sensoren nicht verhindert, so wird das Wiedererkanntwerden in beliebigen Lebenssituationen zum Normalfall; es zu verhindern, erfordert kriminelle Energie [14].

Biometrische Erfassung birgt prinzipiell auch das Risiko, daß aus den gewonnenen Daten medizinische Diagnosen abgeleitet werden. Man spricht von mehr oder weniger invasiven Erfassungsmethoden. Diese Gefahren werden vom Gesetzgeber erkannt. Siehe den Artikel von Köhntopp und Gundermann in diesem Heft.

Wir zeigen eine kryptographische Lösung für biometrische Ausweise, die biometrische Erkennung von Personen gewährleistet, aber verhindert, daß prüfende Stellen die biometrischen Daten erhalten. Wir haben früher gezeigt, wie biometrische Ausweise für elektronische Führerscheine [4] oder zur datenschutzorientierten Abrechnung medizinischer Leistungen mit gesetzlichen Krankenkassen [3] eingesetzt werden können.

Biometrische Erkennung

Biometrische Erkennung erfordert zunächst eine Initialisierungsphase, bei der die biometrischen Identitäten der später zu erkennenden Personen erfaßt und digital gespeichert werden (*Referenzabdrücke, biometric template*). Eine anschließende biometrische Erkennung erfolgt dann in zwei Schritten: Erfassung und Auswertung. Die Erfassung geschieht durch physikalische Messung mit anschließender Digitalisierung. Das Ergebnis ist ein *biometrischer Abdruck* (biometric template). Die anschließende Auswertung erfolgt durch Vergleich des aktuellen biometrischen Abdrucks mit den initialen Referenzabdrücken. Man klassifiziert biometrische Merkmale in (statische) physiologische Merkmale, die sich im Laufe eines Lebens relativ wenig verändern (Retina- und Irismuster, Fingerabdrücke, Handgeometrien, optische und thermische Gesichtsmuster), und (dynamische) Verhaltensmuster, deren Reproduktion einer größeren Streuung unterliegt, z.B. Sprechstimm-, Unterschrifts- oder Tippmuster [13].

Die Zuverlässigkeit der Erkennung wird durch zwei Fehlerwahrscheinlichkeiten angegeben: die für fälschliches Akzeptieren (*false acceptance rate*, FAR) und die für fälschliches Zurückweisen (*false rejection rate*, FRR). Für praktische Verfahren lassen sich diese Parameter in gewissen Grenzen wählen, wobei im allgemeinen eine niedrigere Rate fälschlichen Akzeptierens durch eine höheren Rate fälschlichen Zurückweisens erkauft wird und umgekehrt. Für die meisten Anwendungen wird man ein System eher mit einer geringen Rate fälschlichen Akzeptierens betreiben und dafür mehr fälschliche Zurückweisungen in Kauf nehmen. Die erreichbaren Fehlerraten nehmen von Retinascans bis zur Tippmustererkennung in der Reihenfolge ab, wie sie oben genannt sind.

Die Zeit für eine Erkennung setzt sich zusammen aus der Zeit zum Erfassen und der zum Auswerten. Physiologische Merkmale können im allgemeinen schneller erfaßt werden als Verhaltensmuster, da diese sich erst über einen Zeitraum hinweg manifestieren. Im wesentlichen hängt die Zeit zum Erfassen von den gewählten Fehlerwahrscheinlichkeiten ab, und die Zeit zum Auswerten von der Zahl der zu unterscheidenden biometrischen Abdrücke. Man ist bei automatischer biometrischer Erkennung an Verfahren interessiert, die innerhalb von 1-5 Sekunden eine Antwort liefern und wenig invasiv sind. Daher kommt z.B. DNA-Analyse nicht in Betracht. Informationen über kommerzielle Produkte findet man z.B. beim Biometrics Consortium [2].

Systemarchitekturen

Während der Initialisierungsphase wird von allen zu erkennenden Personen ein Referenzabdruck genommen. Wenn diese Referenzabdrücke zentral von einem oder mehreren Identifikationsservern vorgehalten werden, spricht man von *Online-Erkennung*, weil die anschließenden Auswertungen Online-Verbindungen zu den Identifikationsservern erfordern. Die Erfassung biometrischer Merkmale während der Initialisierung und späteren Erkennung geschieht durch Spezialhardware wie Fingerabdruckleser, Irisscanner, Mikrofone etc. Zur Auswertung kann entweder das erfassende Gerät den aktuellen biometrischen Abdruck an den Identifikationsserver übermitteln und auf dessen Auswertung warten (*push-model*) oder den erwarteten Referenzabdruck vom Identifikationsserver anfordern und die Auswertung selbst vornehmen (*pull-model*). Das BioAPI™-Consortium entwickelt entsprechende Softwareschnittstellen.

Bei *Offline-Erkennung* werden die Referenzabdrücke dezentral direkt in den Lesegeräten gespeichert, so daß diese später biometrische Abdrücke selbständig auswerten können (siehe Davida et al [10]).

Sicherheit und Akzeptanz

Dynamische Merkmale zu erkennen, ist prinzipiell fehleranfälliger, weil diese mit Absicht, bei Krankheit, Streß oder unter anderen Einflüssen ungenau reproduziert werden können. Andererseits ist die Erfassung statischer Merkmale meist invasiver und findet daher geringere Akzeptanz. Fingerabdruckleser sind die derzeit reifste und meistverwendete biometrische Technologie, da sie seit langem in der Strafverfolgung eingesetzt werden. Typische Charakteristiken kommerzieller Produkte sind FAR < 0,001% und FRR < 2% bei einer Erkennungsdauer von weniger als 2s. (Es gibt daneben Geräte, die lebende Finger von toten Fingern oder Latex-Handschuhen unterscheiden.) Gerade der Einsatz in der Strafverfolgung erschwert die Akzeptanz von Fingerabdrucklesern im zivilen Bereich. Kommerzielle Produkte liefern zwar die biometrischen Abdrücke in einem Format, das inkompatibel ist zu dem der Strafverfolgung, dennoch dürfte es den Ermittlungsbehörden im Zweifelsfall leicht fallen, die Formate abzugleichen.

Unter Datenschutzaspekten ist Online-Erkennung riskanter als die herkömmliche Erkennung durch Ausweise mit eingeprägten Portraits, denn weiterhin müssen Personen ihre Referenzabdrücke den prüfenden Stellen überlassen, und bei automatisierter Erkennung können abgefangene Referenzabdrücke leichter verwendet werden, um falsche Identitäten vorzutäuschen. Daher ist Offline-Erkennung vorzuziehen, weil den prüfenden Stellen weder Referenzabdrücke noch aktuelle biometrische Abdrücke überlassen werden.

Persönliche Piloten

Wir gehen im folgenden von Offline-Erkennung aus, bei der jede Person ihr persönliches Gerät (*mobile user device*) bei sich trägt, das biometrische Merkmale erfassen und auswerten kann. Wir sprechen bei persönlichen Geräten im folgenden kurz von *Piloten* in Anlehnung an 3Coms PalmPilot. Um Manipulation durch Benutzer zu verhindern (*tamper resistance*), erfolge die Erfassung und Auswertung in einem Sicherheitsmodul, genannt *Wächter* (*observer*), das in jeden Piloten implantiert ist. Jeder Wächter verläßt die Produktion mit einem *initialen Signierschlüssel*, mit dem er später seine Ergebnisse signieren kann. Während der Initialisierung lernt jeder Wächter den Referenzabdruck seines Benutzers, und während einer Erkennung verifiziert der Wächter den aktuellen biometrischen Abdruck und übermittelt das signierte Ergebnis an die prüfende Stelle. Dabei kontrollieren Piloten jede Kommunikation zwischen ihren Wächtern und prüfenden Stellen, so daß Wächter und prüfende Stellen selbst dann keine (biometrischen) Daten austauschen können, wenn sie beide vom Protokoll abweichen. Diese Gerätearchitektur (*wallet-with-observer*) wurde erstmals von David Chaum für offline electronic cash vorgeschlagen [8,7]. Piloten können Mobiltelefone, Organizer, PalmPilots und zukünftige Computercards sein [12]. Sie müssen eine eigene Stromversorgung und eine eigene Benutzerschnittstelle haben, an der der Benutzer Daten eingeben und der Pilot Daten ausgeben kann. Weiterhin müssen sie Kommunikationsschnittstellen zu den Ge-

räten der prüfenden Stellen besitzen. Beispiele sind Funk-, Netz- oder Infrarotverbindungen. Für die Wächter kommen insbesondere Implementierungen in Betracht, die die Erfassung, Auswertung und Signatur auf einem einzigen Chip realisieren. Ein Fingerabdruck-Lesechip ist z.B. AuthenTecs FingerLoc™ System [1]. Prototypen von Mobiltelefonen mit implantiertem biometrischen Erkennungschip werden im EU-Projekt CASCADE von GEMPlus (France) ARM (UK) und Nokia (Finland) mit Unterstützung der EU entwickelt [9].

Die Offline-Erkennung durch Piloten verhindert, daß biometrische Abdrücke in die Hände von Zweiten und Dritten fallen, solange Piloten nicht verloren oder gestohlen werden. Selbst bei Diebstahl gewinnt der Angreifer jedoch allenfalls *eine* biometrische Identität, nicht Hunderte oder gar Tausende wie im Fall „angezapfter" Identifikationsserver oder deren Datenleitungen. Weiterhin bietet Offline-Erkennung durch Piloten die Möglichkeit zur anonymen Identifikation. Anonymität ist bei Online-Erkennung prinzipiell nicht zu erreichen.

Biometrische Ausweise

Aufgrund korrekter Identifizierung können einmalige oder kurzfristige Zugangsrechte gewährt werden, zum Beispiel zu Räumen, Computern usw. Oft geht es aber um dauerhaftere Rechte, wie zum Beispiel bei Ausweisen, Urkunden, Zeugnissen und Führerscheinen. Wir sprechen im folgenden kurz von *Ausweisen*. Unter Datenschutzaspekten ist es wünschenswert, daß Benutzer ihre eigenen Ausweise verwalten und damit auch die Kontrolle behalten, wer ihre Ausweise einsieht und wer nicht. Herkömmlich werden Ausweise meist durch Dokumente mit aufgedrucktem Foto des Besitzers realisiert, so daß ein Übertragen der Ausweise erschwert ist. Es ist also naheliegend, für eine elektronische Implementierung die oben skizzierte Offline-Erkennung mit Piloten zu verwenden, weil die Piloten sowohl die biometrische Erkennung als auch die dezentrale Speicherung der Ausweise übernehmen können.

Wir zeigen nun eine Implementierung elektronischer Ausweise, die Sicherheit und Datenschutz in einem Maß garantiert, das mit herkömmlichen Methoden nicht erreicht werden kann. Wir betrachten Aussteller, Besitzer und Prüfer von Ausweisen. Besitzer erreichen Anonymität dadurch, daß sie gegenüber Ausstellern und Prüfern (verschiedene) Pseudonyme verwenden. Es gibt drei Transaktionen:

- Ein Benutzer führt sich unter neuem Pseudonym bei einem Aussteller ein.
- Ein Aussteller stellt einem Besitzer einen Ausweis aus.
- Ein Besitzer zeigt einem Prüfer seinen Ausweis vor.

Bei jeder Transaktion interagiert der Pilot eines Besitzers inklusive seinem Wächter mit dem Gerät eines Ausstellers oder Prüfers.

Die folgende kryptographische Implementierung verwendet als Bausteine *interaktive Beweisprotokolle* (*interactive proofs of knowledge*) und *blinde Signatursysteme* (*blind signatures*). Grob werden sie wie folgt verwendet: Zu jedem Benutzerpseudonym gibt es Zeugen. Beide können durch z.B. durch 230- bis 310-stellige Dezimalzahlen repräsentiert werden. Um ein Pseudonym benutzen zu können, muß der Benutzer beweisen, daß er einen passenden Zeugen kennt. Dies geschieht mittels eines interaktiven Beweisprotokolls, ohne dabei dem Aussteller den Zeugen zu verraten. Die Nicht-Übertragbarkeit der Ausweise wird durchgesetzt, indem der Benutzer sowohl beim Einführen eines Pseudonyms als auch beim Vorzeigen eines Ausweises biometrisch verifiziert wird. Man erzwingt dies durch das Zerlegen des Zeugen eines Pseudonyms in zwei Teile, wobei der eine Teil nur dem Pilot und der andere Teil nur dem Wächter bekannt ist. Um sein Pseudonym benutzen zu können, ist der Pilot stets auf die Mithilfe des Wächters angewiesen, der dafür die biometrische Erkennung verlangt. Die elektronischen Ausweise werden durch Signaturen auf Pseudonyme realisiert. Inhalt und Art der Ausweise sind durch die öffentlichen Verifikationsschlüssel des Ausstellers spezifiziert. Zum Beispiel gibt es verschiedene Verifikationsschlüssel für Führerscheine verschiedener Klassen etc. Um Unverkettbarkeit seiner Transaktionen und damit Anonymität zu erreichen, muß der Benutzer Signaturen auf Pseudonyme bekommen können, die der Aussteller nicht kennenlernt. Daher wird ein blindes Signatursystem verwendet.

Wir skizzieren die Transaktionen nun genauer. Die kryptographische Beschreibung steht in [4], wobei das Signatursystem aus [5] verwendet werden kann.

Startpseudonyme Einführen

Pilot und Wächter formen zusammen ein neues Startpseudonym ψ für den Benutzer. Sie wählen für das Startpseudonym einen Zeugen z, dessen einen Teil z_P nur der Pilot und dessen anderen Teil z_W nur der Wächter kennt. Um sich bei einem Aussteller unter dem gewählten Startpseudonym einzuführen, sendet der Pilot das Startpseudonym mit einer Signatur des Wächters. Diese Signatur bestätigt, daß der Wächter an der Bildung von ψ beteiligt gewesen ist und einen Teilzeugen kennt. Wenn der Wächter jetzt seinen Benutzer biometrisch erkennt, dann beweisen Wächter und Pilot dem Aussteller durch ein interaktives Beweisprotokoll, daß sie zusammenpassende Teilzeugen (z_P, z_W) für ψ kennen. Wenn dieses Protokoll erfolgreich beendet wird, registriert der Aussteller das Startpseudonym ψ für den Benutzer. Der Pilot gibt seinem Wächter einen symbolischen Namen für den Teilzeugen z_W. Damit kann der Pilot seinen Wächter später auffordern, z_W erneut zu verwenden (siehe Abb. 1).

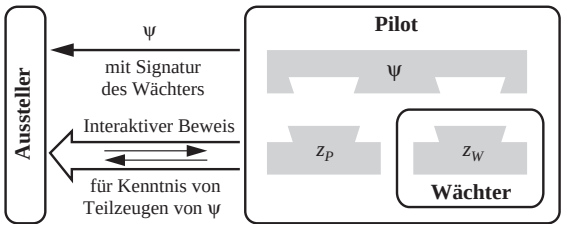

Abb. 1: Einführung eines Pseudonyms

Ausweise Ausstellen

Der Benutzer stellt eine Kommunikationsverbindung zwischen seinem Pilot und dem Aussteller her. Der Aussteller gibt dem Pilot eine blinde Signatur auf das registrierte Startpseudonym. Die blinde Signatur des Ausstellers erlaubt dem Pilot, eine Signatur σ' des Ausstellers auf ein Zwischenpseudonym ψ' zu bekommen, das der Aussteller nicht erfährt, aber für das der Pilot einen Teilzeugen z'_P bestimmen kann, so daß (z'_P, z_W) zusammenpassende Teilzeugen für das Zwischenpseudonym ψ' sind (siehe Abb. 2). Ein Benutzer kann mehrere Aus-

weise vom selben Aussteller unter einem oder verschiedenen Pseudonymen anfordern.

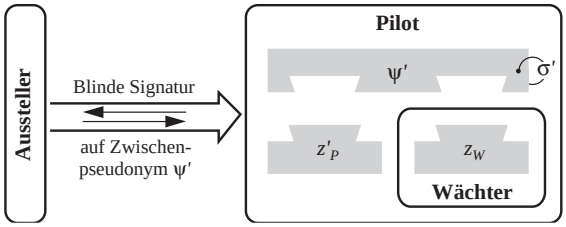

Abb. 2: Ausstellen eines Ausweises

Ausweise Vorzeigen

Der Benutzer stellt eine Kommunikationsverbindung zwischen seinem Pilot und dem Prüfer her. Der Pilot transformiert sein Zwischenpseudonym mit Signatur des Ausstellers in ein Zielpseudonym ψ'' mit Signatur σ'' des Ausstellers. Die Transformation erlaubt dem Pilot wiederum, einen Teilzeugen z''_P zu finden, so daß (z''_P, z_W) zusammenpassende Teilzeugen für das Zielpseudonym sind. Für das anschließende Beweisprotokoll mit dem Prüfer fordert er seinen Wächter auf, den Teilzeugen z_W zu verwenden. Nur wenn der Wächter jetzt seinen Benutzer biometrisch erkennt, nimmt

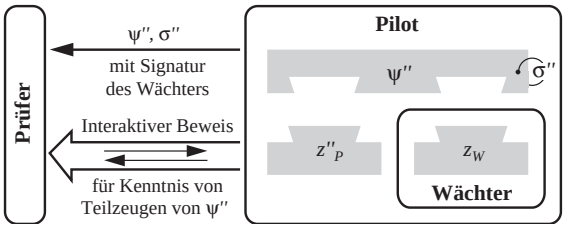

Abb. 3: Vorzeigen eines Ausweises

er an dem Beweiprotokoll teil (Abb. 3).

Sicherheitsdiskussion

Mathematisch ist die Transformation von Startpseudonymen in Zwischenpseudonyme (mit zugehörigen Signaturen) dieselbe wie die von Zwischenpseudonymen in Zielpseudonyme (mit zugehörigen Signaturen). Der Unterschied ist nur, daß die Transformation von Startpseudonymen innerhalb eines interaktiven Signierprotokolls stattfinden, während die Transformation von Zwischenpseudonymen lokal vom Pilot durchgeführt wird. Die Transformation garantiert, daß jedes Pseudonym und jede dafür gültige Signatur mit gleicher Wahrscheinlichkeit ausgegeben werden und somit Start-, Zwischen- und Zielpseudonyme unverkettbar sind. Der Pilot ist also frei, neue Zielpseudonyme aus dem Zwischenpseudonym oder vorigen Zielpseudonymen zu erzeugen. Insgesamt lernen die Aussteller und Prüfer nicht mehr darüber, welche Ausstell- und Prüftransaktionen vom selben Benutzer stammen, als was die Inhalte der Ausweise ohnehin erschließen lassen.

Damit die elektronischen Ausweise nicht zwischen Personen übertragbar sind, muß verhindert werden, daß der Pilot Zwischenpseudonyme in Zielpseudonyme transformiert, zu denen er allein einen Zeugen kennt. In diesem Fall bräuchte er beim Vorzeigen des Ausweises nicht die Hilfe seines Wächters und könnte so eine biometrische Prüfung umgehen. Beliebige Personen könnten dann den Ausweis des Benutzers selbst verwenden. Als zugrundeliegendes blindes Signatursystem kommt daher nur ein restriktives in Frage. Bei diesen ist garantiert, daß der Empfänger nur Signaturen auf Pseudonyme erhalten kann, die gemäß der beabsichtigten Transformation gebildet sind. Restriktive blinde Signatursysteme ohne lokale Transformierbarkeit wurden 1992 für Offline E-Cash Systeme vorgeschlagen [8,6]. Ein für diese Anwendung benötigtes restriktives Signatursystem mit lokaler Transformierbarkeit ist vom Autor entwickelt worden [5].

Wie sicher ist das System noch, falls der Manipulationsschutz einiger Wächter überwunden wird? In diesem Fall werden maximal alle Ausweise übertragbar, die von den zerstörten Wächtern bewacht wurden. Die Signierschlüssel der Aussteller werden nicht kompromittiert, und die Ausweise ehrlicher Benutzer sind nicht betroffen.

Fazit

Persönliche Geräte haben das Potential, viele Funktionalitäten wie Brieftasche, Organizer, Telefon, Pager, Diätplaner usw. mobil und über dieselbe Benutzerschnittstelle anzubieten. Sie haben ein noch größeres Potential, die Benutzeridentifikation gegenüber verschiedenen Institutionen und Systemen zu vereinfachen und gleichzeitig ein bisher nicht erreichbares Maß an Datenschutz durchzusetzen.

Wir haben skizziert, wie Benutzer sich biometrisch identifizieren können, ohne ihre Anonymität aufzugeben, und wie nichtübertragbare elektronische Ausweise realisiert werden können, bei denen sogar die einzelnen Transaktionen eines Benutzers unverkettbar bleiben. Die vorgeschlagenen kryptographischen Verfahren können mit jeder biometrischen Erfassung kombiniert werden, sie sind effizient und in persönlichen Geräten implementierbar.

Literatur

[1] AuthenTec: http://www.semi.harris.com
[2] http://www.biometrics.org/
[3] Gerrit Bleumer, Matthias Schunter: Datenschutzorientierte Abrechnung medizinischer Leistungen; DuD 21/2 (1997) 88-97.
[4] Gerrit Bleumer: Biometric yet Privacy Protecting Person Authentication; Information Hiding Workshop '98, LNCS 1525, Springer-Verlag, Berlin 1998, 101-112.
[5] Gerrit Bleumer: Many-Time Restrictive Blind Signatures; AT&T Technical Report 98.38.1; http://www.research.att.com/library/trs
[6] Stefan Brands: Untraceable Off-line Cash in Wallet with Observers; Crypto '93, LNCS 773, Springer-Verlag, Berlin 1994, 302-318.
[7] David Chaum: Achieving Electronic Privacy; Scientific American (August 1992) 96-101.
[8] David Chaum, Torben Pryds Pedersen: Wallet Databases with Observers. Crypto '92, LNCS 740, Springer Verlag, Berlin 1993, 89-105.
[9] http://www.dice.ucl.ac.be/crypto/cascade/
[10] George I. Davida, Yair Frankel, Brian J. Matt, B. J. On Enabling Secure Applications Through Off-Line Biometric Identification; IEEE Symposium on Security and Privacy, IEEE Press 1998, 148-159.
[11] Constance Loizos: Biometrics – The identification that you'll never leave home without; Red Herring, 9/98, 22-24.
[12] Andreas Pfitzmann, Birgit Pfitzmann, Matthias Schunter, Michael Waidner: Trusting Mobile User Devices and Security Modules; Computer 30/2 (1997) 61-68.
[13] Benjamin Miller: Vital signs of identity; IEEE spectrum 31/2 (1994) 22-30.
[14] Klaus Müller, Axel Pfau: Biometrische Verfahren zur Verifikation der Personenidentität; DuD 16/7 (1992) 346-352.