Biometrie als Bindeglied zwischen Person und Identität : Teil 2

Autor(en): **Müller, Lorenz**

Objekttyp: **Article**

Zeitschrift: **Bulletin.ch : Fachzeitschrift und Verbandsinformationen von Electrosuisse, VSE = revue spécialisée et informations des associations Electrosuisse, AES**

Band (Jahr): **94 (2003)**

Heft 21

PDF erstellt am: **29.05.2024**

Persistenter Link: https://doi.org/10.5169/seals-857611

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

Biometrie als Bindeglied zwischen Person und Identität – Teil 2

Biometrisch gesicherte Authentifizierung

Globalisierte Gesellschaft, beschleunigte wirtschaftliche Abläufe, rasche Kontakte über verschiedenste Medien, wachsende und wechselnde Beziehungsnetze – all dies sind Ursachen für das auftauchende Problem der richtigen Identitätszuordnung. Was ist unter Identität zu verstehen? Ist es die eindeutige Benennung und Zuordnung einer Person zu einer Gruppe mit bestimmten sozialen, ökonomischen und legalen Rechten oder ist damit direkt das biologische Individuum gemeint? Heisst «jemanden kennen», eine Person in jeder Lebenslage auf Grund ihrer persönlichen Merkmale erkennen zu können oder lediglich im Besitz einer Visitenkarte zu sein, die angibt, wie die Person heisst und in welcher Funktion sie arbeitet?

Immer mehr wird die Identität nur noch durch Daten repräsentiert, die den gesellschaftlichen Bezug der Person, nicht aber die Person als physisches Individuum beschreiben. Im ersten Teil dieses Beitrags (*Bulletin SEV/VSE* 19/03, Seiten 17ff.) wurde gezeigt, wie die oft kaum mehr vorhandene Bindung zwi-

Lorenz Müller

schen einer Person und ihrer Identität mit Hilfe der Biometrie wieder hergestellt und gestärkt werden kann. In diesem zweiten Teil werden Schwachstellen und Probleme bei der biometrischen Identifizierung aufgezeigt. Es wird aber auch eine konkrete Lösung für ein biometrisch unterstütztes Authentifzierungssystem vorgestellt, das mehrere bekannte Schwächen eliminiert.

Schwachstelle in biometrischen Sicherheitssystemen

Eine grundlegende Schwäche der meisten Sicherheitssysteme mit biometrischer Identifikation ist das Erfassungs- und Speicherungskonzept. Die biometrischen Daten der zugangsberechtigten Personen werden im Sicherheitssystem des zu schützenden Objekts im Rahmen einer Ersteintrittsprozedur erfasst und zentral gespeichert. Bei jeder Zugangskontrolle und bei jedem Eingang muss das System wieder entscheiden, ob die biometrischen Werte der Zugang erheischenden Person einer der vielen abgespeicherten biometrischen Identitäten entsprechen. Zumindest die Messung bei der Ersterfassung muss deshalb extrem präzis sein und trotzdem ist das System natürlich anfällig auf Fehler, die direkt mit der komplexen *n-n*-Zuordnung zusammenhängen (falsche Akzeptanz einer nichtberechtigten Person, falsche Rückweisung einer berechtigten Person). Etwas verbessert wird die Situation, wenn die Person sich bei jedem Zugang selbst identifiziert und das biometrische System lediglich eine Authentifizierung vornehmen muss (*n*-1-Zuordnung). In diesem Fall muss die Messung immer noch genügend präzise sein, um allen Personen ausser einer den Zugang zu verwehren.

Mit einem solchen Identifizierungs- oder Authentifizierungskonzept (Bild 1) handelt man sich eine ganze Reihe von Nachteilen ein:

- Die biometrischen Detektoren und die erfassten Referenzmuster müssen eine sehr hohe Verifikationsqualität erlauben. Das System wird dadurch teuer und störanfällig. Ausserdem muss das System vor Angriffen auf Verfügbar-

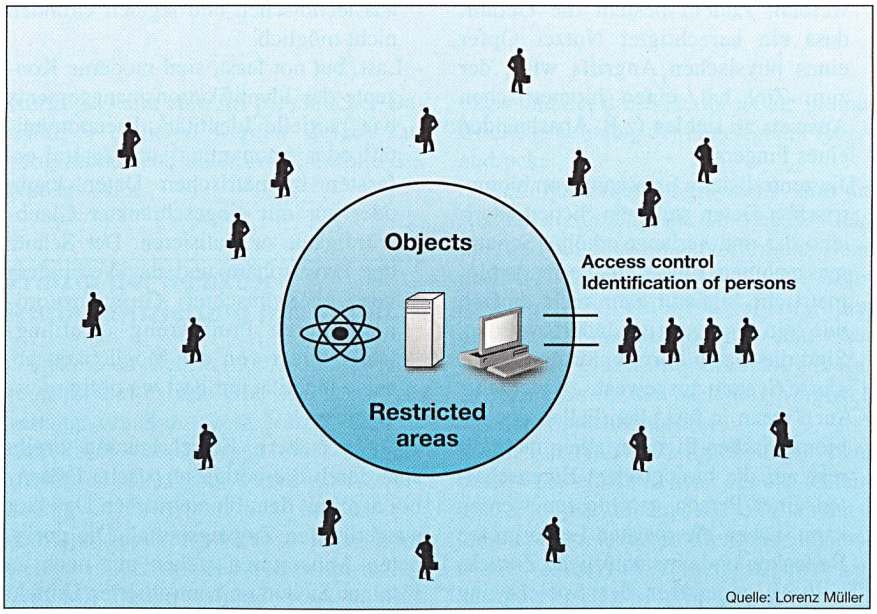

Bild 1 Objektzentrierte Identifizierung: Die Authentifizierung der zugangsberechtigten Personen wird direkt in das lokale Sicherheitssystem integriert und erfolgt nachgängig zur Identifikation beim Eingang.

Für jede zugangsberechtigte Person, die authentifiziert werden soll, muss im Sicherheitssystem zumindest eine authentifizierende Signaturinformation gespeichert sein. Die Wahrscheinlichkeit, dass eine solche Information korrumpiert wird, steigt mit der Anzahl der Nutzer. Besonders problematisch ist dies für intrinsische wertvolle Daten, wie zum Beispiel biometrische Daten[1].

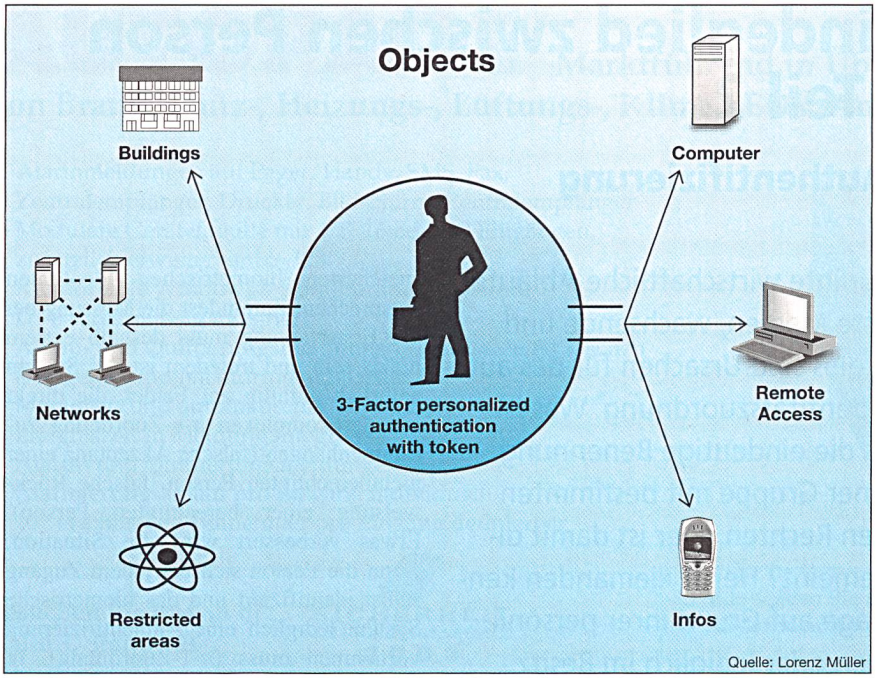

Bild 2 Personenzentrierte Identifikation: Im ersten Schritt erfolgt die Authentifizierung der Person (Identifizierung ist durch die 1-1-Beziehung zwischen Karte und Besitzer a priori realisiert). Einer aussenstehenden Instanz genügt es danach, lediglich die Echtheit des personalisierten Tokens zu verifizieren, um eine Identifikation mit Authentifikation zu erhalten.

Das Token ist mit der digitalen Aussenwelt nur durch einen einlaufenden kryptografisch gesicherten Einwegkanal verbunden. Jedes Sicherheitssystem, das die Karte kennt, kann mit Hilfe eines Challenge-Response-Protokolls die Karte und damit den autorisierten Nutzer authentifizieren. Dabei wird nur die Kartenkennung, verbunden mit einer partiellen Identität des Nutzers, öffentlich zugänglich. Alle sensitiven Daten, insbesondere die Biometrie, bleibt unter der alleinigen Kontrolle des Nutzers.

keit und gegen Täuschungsversuche zusätzlich geschützt werden.

- An jedem Eingang muss eine aufwendige und für den Nutzer störende Authentifizierungsprozedur durchlaufen werden. Zudem besteht die Gefahr, dass ein berechtigter Nutzer Opfer eines physischen Angriffs wird, der zum Ziel hat, einen biometrischen Ausweis zu stehlen (z.B. Abschneiden eines Fingers).
- Die zentralisierte Erfassung von biometrischen Daten stellt ein Sicherheitsrisiko dar und verlangt erhöhte Schutzmassnahmen. Eine einmal erfasste biometrische Signatur kann nicht einfach wie ein Passwort geändert werden. Sind die Daten korrumpiert, muss das ganze System ausgewechselt werden.
- Auch wenn in fast allen Fällen aus der biometrischen Signatur allein nicht direkt auf die biologischen Eigenschaften einer Person geschlossen werden kann, haben die meisten Leute grosse Bedenken und eine natürliche Zurückhaltung gegenüber der Speicherung ihrer biometrischen Daten in irgendwelchen Datenbanken, mögen diese auch als noch so sicher deklariert sein.
- Aus der Sicht der erfassten Person stört zudem das vollständige Fehlen der Interoperabilität zwischen den Zugangskontrollsystemen unterschiedlicher Organisationen. Die Ersterfassung muss in aller Umständlichkeit immer wieder neu gemacht werden, ein Austausch der Vergleichsdaten ist aus technischen und legalen Gründen nicht möglich.
- Last, but not least, sind moderne Konzepte des Identifikationsmanagements wie partielle Identität[2], Pseudonymität[3] oder Anonymität[4] mit zentral erfassten biometrischen Daten kaum oder nur mit eingeschränkter Glaubwürdigkeit zu realisieren. Der Schutz der Privatsphäre und das Verhindern von unerwünschter Gruppenzuordnung durch Profilierung (profiling) hängt direkt von der Möglichkeit ab, seine Identität nur dort wo nötig preiszugeben.

Eine weitere Einschränkung ergibt sich durch die nötige physische Präsenz bei dem mit dem biometrischen Detektor ausgerüsteten Zugangsportal. Die geeigneten Apparaturen stehen nur noch an wenigen Stellen im kontrollierten Umfeld zur Verfügung. Damit behindert das Authentifizierungssystem die heute unabdingbare Mobilität. Dies mag für physische Zugangskontrollen nicht relevant sein, für die Realisierung einer Authentifizierung für ein virtuelles Portal ist die Einschränkung aber unakzeptierbar. All die hier erwähnten Probleme und Nachteile sind nicht direkt eine Folge des biometrischen Authentifizierungskonzepts, sondern der heute dominierenden zentralisierten Authentifizierungsmechanismen und ihren Implementierungen.

Neuartiges mobiles Authentifizierungskonzept

An der Hochschule für Technik und Informatik, Biel, wurde unter dem Namen Cod-it ein neuartiges Authentifizierungssystem entwickelt, das die obgenannten Probleme sehr elegant löst [1]. Die Lösung basiert auf einer personifizierten Karte,

- die jedermann problemlos mit sich führen kann,
- die sich an allen Computern von beliebigen Applikationen oder Internet-Plattformen aus sicher authentifizieren lässt,
- die nur durch den autorisierten Inhaber benutzt werden kann und
- deren Sicherheit und Schlüsselverwaltung mit einem Minimum an organisatorischem Aufwand gewährleistet wird.

Der angestrebte Brückenschlag zwischen physischer Person und digitalem Ausweis muss so realisiert sein, dass man zum virtuellen Kommunikationspartner das gleiche Vertrauen aufbauen kann, wie wenn man ihm selbst begegnet wäre. Basis ist die Abkehr von einem Sicherheitskonzept, bei dem um das zu schützende physische oder logische Objekt ein Sicherheitszaun mit einem Eingang gelegt wird, bei dem sich alle zugangsbe-

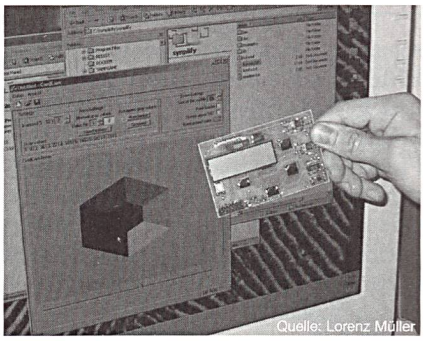

Bild 3 Prototyp der Cod-it-Authentifizierungskarte vor dem optischen Übertragungsfeld, das in jedem Browser geöffnet werden kann

Via Browser sendet das aufgerufene Sicherheitssystem eine kryptografisch verschlüsselte Nachricht, die nur von der autorisierten Karte entschlüsselt werden kann. Die Karte entschlüsselt die Nachricht nur, wenn sich der Besitzer vorgängig gegenüber der Karte korrekt authentifiziert hat. Durch die Kombination von Fingerabdrucken mit einem Geheimnis wird damit eine mobile, einfach zu handhabende 3-Faktor-Authentifizierung (Token, Geheimnis, Biometrie) realisiert.

rechtigten Personen identifizieren müssen (objektzentriertes Identifikationssystem). Neu steht im Zentrum die Person, die sich gegenüber einem persönlichen Identifizierungsportal authentifiziert (1-1-Zuordnung), das als kleines tragbares Token realisiert ist[5]. Das Token stellt dann die Verbindung mit den Sicherheitssystemen der schützenswerten Objekte her und weist seinen Inhaber mit der gerade hinreichenden partiellen Identität aus, die für den Zugang verlangt wird (Bild 2).

Die personenzentrierte Identifizierung (mit vorgängig erfolgter Authentifizierung) hat zahlreiche Vorteile. Wohl die wichtigsten sind die uneingeschränkte Mobilität, der hohe Schutz der biometrischen Daten, die flexible und leicht zu standardisierende Identifizierung der berechtigten Personen an allen Portalen und die Nutzerfreundlichkeit verbunden mit einer hohen Nutzerakzeptanz.

Realisierung

Kernstück der Cod-it-Authentifizierungstechnologie ist eine kreditkartengrosse Chipkarte mit einer biometrischen Schnittstelle zum Besitzer und einer kryptografisch gesicherten optischen Schnittstelle zur digitalen Welt (Bild 3). Dank einem einfachen Challenge-Response-Protokoll (Bild 4), das direkt über den Bildschirm auf die Karte übertragen wird, kann sich der Kartenbesitzer sofort und überall sicher ausweisen. Die biometrischen Daten sind nur noch auf der einzelnen Karte gespeichert. Diese bleibt beim Besitzer und schützt die sensitiven Daten auch bei Verlust. Simple und robuste Authentifizierung, der Schutz sensibler persönlicher Daten und uneingeschränkte Mobilität sind dadurch gewährleistet. Das Grundkonzept hat im letzten Jahr den Venture-2002-Preis der ETH und McKinsey gewonnen und wird nun im Rahmen der Spin-off-Firma AXSionics der HTA Biel zu einem Produkt weiterentwickelt. Die erste auf dem Cod-it-Konzept aufbauende Produktlinie ist ein universelles Zugangskontrollsystem, das mit einer einzigen Karte Eintritt in gesicherte Gebäude und Lokalitäten, Zutritt zum Intranet und insbesondere auch sicheren Remote Access zu IT-Systemen ermöglicht[6]. Die optische Schnittstelle kann durch zusätzliche Schnittstellen zur digitalen Welt ergänzt werden (RFID, akustische Schnittstelle, Bluetooth, USB usw.), die jedoch nur unter direkter Kontrolle des Inhabers Daten aus dem gesicherten Bereich (mit adaptierbarer Speicherkapazität) weiterreichen können. Durch die Weiterentwicklung des Cod-it-Konzepts kann eine Art persönlicher Datentresor realisiert werden, dessen Zugang immer voll unter der Kontrolle des Nutzers steht.

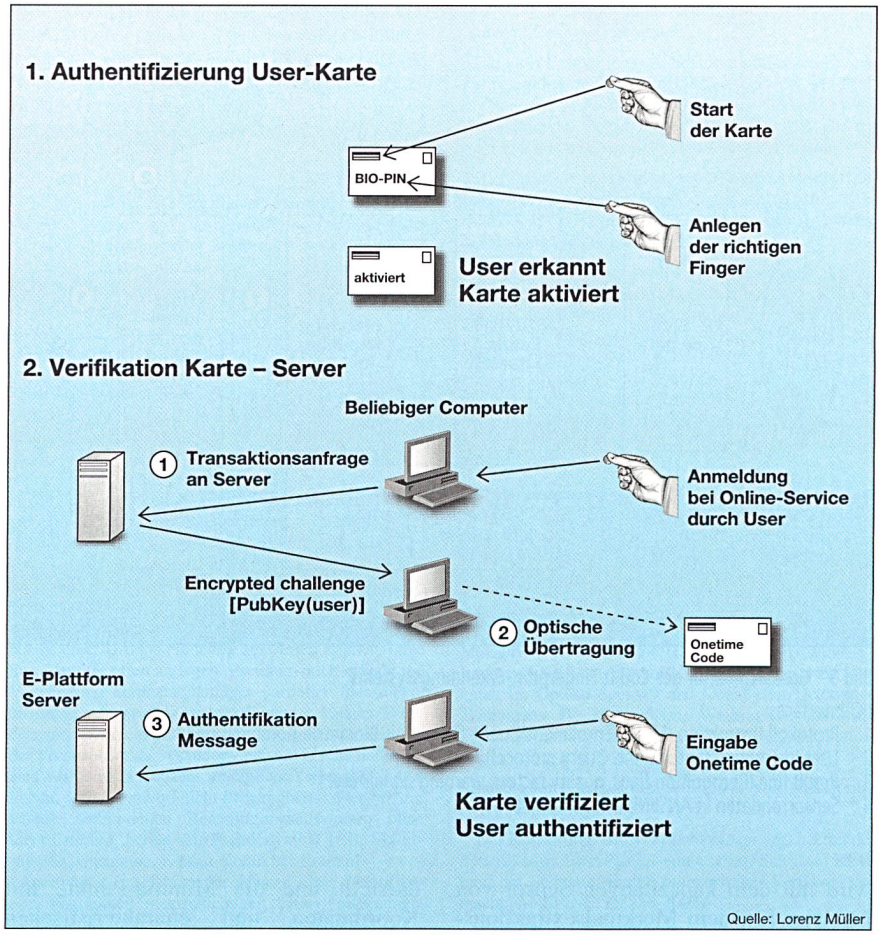

Bild 4 3-Faktor-Authentifizierung und Challenge-Response-Protokoll für die Verifizierung der Identität eines Karteninhabers durch einen Server

Erster Schritt: 3-Faktor-Authentifizierung des Nutzers durch die Karte mit einem kombinierten Protokoll (Token – Biometrie – Geheimnis)
Zweiter Schritt: Verifikation der Echtheit der Karte und damit Authentifizierung des Nutzers durch die Abwicklung eines Challenge-Response-Protokolls über eine kryptografisch geschützte optische Schnittstelle auf dem Computerbildschirm

Prinzip der 3-Faktor-Authentifizierung mit Cod-it

Im ersten Schritt des Authentifizierungsprotokolls der Cod-it-Technologie verlangt die Karte vom Nutzer, dass er sich durch das Anlegen eines Fingers ausweisen soll. Dabei wird diese Aufforderung so formuliert, dass nur der berechtigte Inhaber weiss, welcher oder welche Finger auf den Sensor zu halten sind. Mit diesem simplen Protokoll wird mit einer Nutzerhandlung eine 3-Faktor-Authentifizierung durchgeführt. Erster identifizierender Faktor ist die Tatsache, dass der Nutzer im Besitz der Karte ist, der zweite Faktor wird dadurch realisiert, dass der Nutzer ein Geheimnis kennen muss und der dritte Faktor ist die biometrische Erkennung der angelegten Fingerabdrucke.

Kern des Erkennungssystems sind die Rohdatenerfassung, die Merkmalsextraktion und der Matchingalgorithmus. Dazu gehört noch ein Speicher für die Referenzdaten und ein Protokollkontroller, der die Kommunikation mit dem User steuert und gleichzeitig die richtigen Referenzmuster für den Matching-Vergleich aus dem Speicher abruft.

Ein Fingerabdruck-Erkennungssystem besteht aus einem Sensor, der das Rillenmuster erfasst, einem Bildverarbeitungsteil, der die relevanten Merkmale herausfiltert, einem Erkennungsalgorithmus, der die globalen Merkmale bzw. die Minutia-Punkte[7] nach Lage und Eigenschaften identifiziert und einem Matchingsystem, welches das aufgenommene Muster mit dem abgespeicherten Referenzmuster vergleicht und über Akzeptanz bzw. Ablehnung entscheidet. Das Cod-it-System

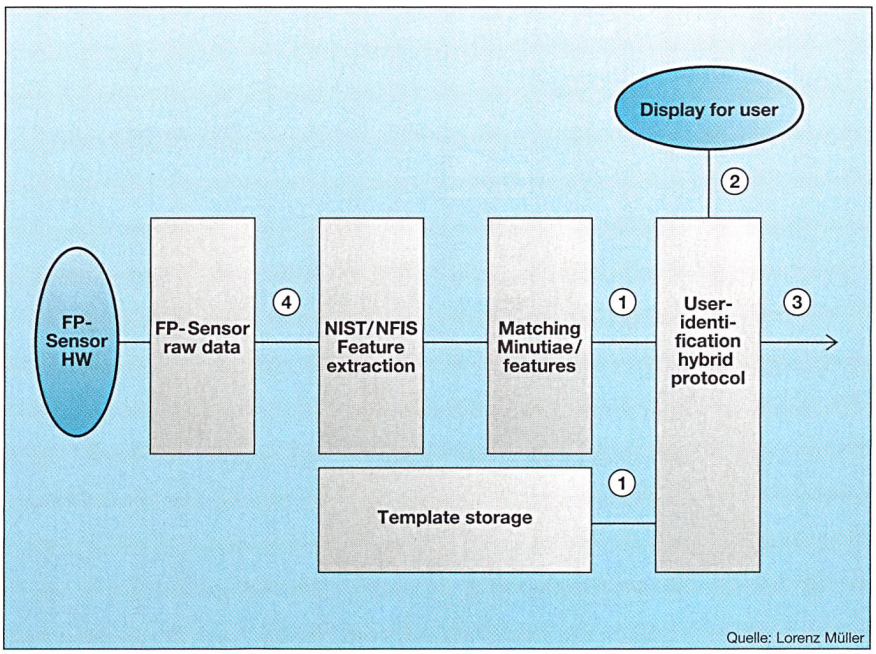

Bild 5 Grobarchitektur des Cod-it-Fingerprint-Erkennungssystems

I/O-Interfaces:
1 Protokoll-Instruktion (Mode: Enrollment/Query; Geheimnis-Biometrie-Kombination usw.)
2 User-Instruktion (Enrollment, Query protocol)
3 Result line (Recognition flags, quality factors, warning signals usw.)
4 Sensorrohdaten in ANSI/NIST-Inputformat

wird mit dem kapazitativen Sensor von Infineon [2], dem Merkmalsextraktionsprogramm des FBI (NIST/NFIS-Programm) [3], und einem selbstentwickelten Matchingalgorithmus [4] realisiert (Bild 5). Der Sensor liefert die erfassten Rohdaten in einem pixelorientierten Format als Grauwertbild dem NIST/NFIS-Programm, das quasi einen Standard darstellt und die Minutia-Punkte mit Koordinaten und charakteristischen Eigenschaften extrahiert (Bild 6). Im Matchingprogramm steckt das eigentliche biometrische Erkennungspotential. Einander entsprechende Minutia-Punkte des abgespeicherten Referenzmusters (Template) müssen mit den Minutia-Punkten des neu aufgenommen Musters (Query) zur Deckung gebracht werden. Dabei müssen sowohl die topologischen wie geometrischen Eigenschaften der beiden Minutia-Grafen verglichen und für die Zuordnung genützt werden. Der von Hans W. Kramer entwickelte Matchingalgorithmus löst diese schwierige Aufgabe besser als die von uns getesteten kommerziellen Systeme. Der Algorithmus funktioniert auch für Finger, die in beliebiger Richtung auf den Sensor aufgelegt werden, für relativ kleine nutzbare Ausschnitte im Rohdatenbild, und er kann gefälschte Gummifinger erkennen, wie sie kürzlich von T. Matsumoto beschrieben wurden[8].

Das Erkennungssystem wird nun in einen Mikroprozessor eingebettet, der direkt mit dem Sensor verbunden ist und in die Cod-it-Karte integriert werden kann.

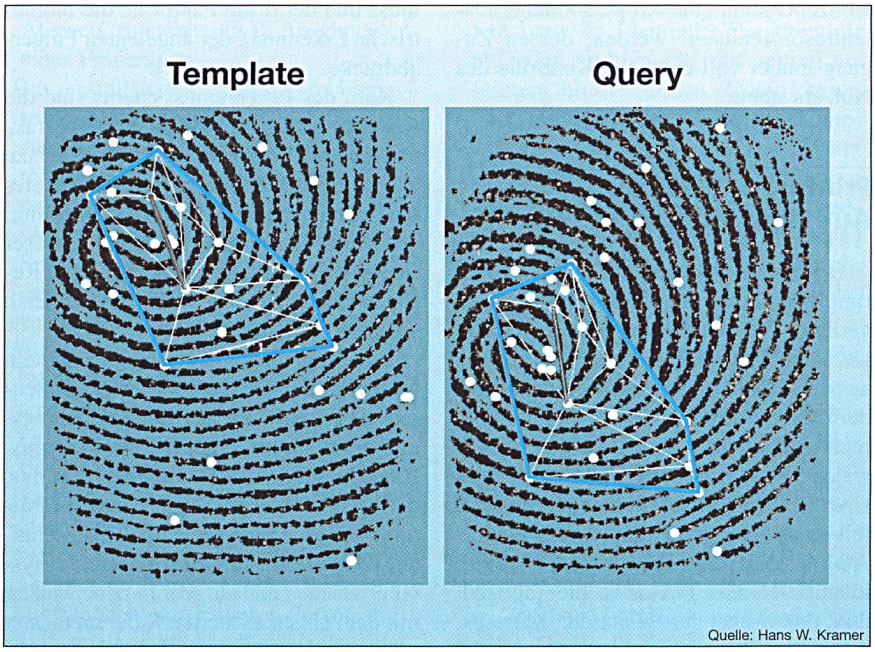

Bild 6 Matchinggrafen auf Minutia-Feldern

Anwendungspotenzial

Auf der Grundlage des Basisprotokolls (Bild 4) lassen sich nebst der simplen Authentifizierung des Inhabers zahlreiche weitere Anwendungen definieren:

- Digitale Unterschrift unter eine zwischen einem E-Plattform-Betreiber und dem Karteninhaber ausgehandelte Vereinbarung, die von beiden Seiten beweisbar ist (E-Kreditkarte mit One-time-Transaktionscode);
- Personifizierter Dangle für die Aktivierung von SW-Lizenzen oder den Zugang zu Online-Diensten;
- Digitaler Ausweis, auf den über das Internet Zugangsausweise (E-Tickets) übertragen werden können;
- E-Voting-Stimmausweis;
- E-Health-Karte;
- Schlüssel zu zentral abgelegten und verschlüsselten persönlichen Daten;
- Verwendung derselben Karte in unabhängigen Servicenetzen mit gesichertem Schutz der Privatsphäre vor Profilingangriffen;
- Nutzung als Schlüssel zu persönlichem Eigentum;
- Studentenausweis für E-Learning usw.

Mit kleinen Anpassungen, aber ohne grosse Schwierigkeiten kann die Cod-it-Authentifizierung in heutige KDC-Strukturen und Zertifikatsmechanismen integriert werden. Grundsätzlich lassen sich auf der Basis des personenzentrierten Sicherheitskonzepts praktisch sämtliche Authentifizierungswerkzeuge, die wir im täglichen Leben benutzen (Ausweise, Schlüssel, Passwörter, Eintrittskontrollen usw.) durch ein einziges Token ersetzen. Die weltweiten Bestrebungen, die Kommunikationsfunktionen des Handy mit den Rechenfunktionen des PDA zu einer universellen persönlichen Datenverarbei-

tungs- und Kommunikationszentrale zu verbinden[9], werden auch das Bedürfnis nach einem überall verwendbaren Schlüssel wecken.

Konklusion

Obschon biometrische Authentifizierung heute noch nicht ausgereift ist, wird die Technologie in der Schnittstelle zwischen Informatik und Physiologie in wenigen Jahren eine wichtige Rolle einnehmen. Der Markt ist noch sehr offen, Standardisierungen fehlen weit gehend[10], und es gibt noch keine marktbeherrschenden Unternehmen. Sicher eine Chance für innovative Ideen und Produkte, die aber – wenn daraus ein profitables Geschäft werden soll – in erster Linie die noch weit verbreitete Skepsis bei den Endnutzern überwinden müssen. Wichtig ist sicher, dass die biometrische Authentifizierung mit den Anforderungen eines modernen Identitätsmanagements vereinbar ist. Dies könnte zum Beispiel durch die Abkehr von einer objektzentrierten zu einer personenzentrierten Authentifizierung geschehen, wie sie oben skizziert ist.

Literatur

[1] Dispositif de sécurité pour transaction en ligne, EP1255178 Priorität 5. Mai 2001 und weltweit beim PCT am 3. Mai 2002.

[2] Infineon (2000): «Microsystems for Biometrics FingerTIP -FTF 1100 MF1 V2.0 CMOS Chip and System Data Book 3.3.» Munich, Germany, 2000, Status 05.00, Infineon Technologies AG, CC Applications Group.

[3] *Garris M. D., Watson C. I., McCabe R. M., Wilson C. L.* (2001): «User's Guide to NIST Fingerprint Image Software (NFIS).» Gaithersburg, MD, USA, 2001-04, National Institute of Standards and Technology (NIST).

[4] *H. W. Kramer:* Improvement of Fingerprint Verification algorithms; SWS-Diploma thesis B29.11; 2003.

Angaben zum Autor

Prof. Dr. ***Lorenz Müller*** hat Mathematik und Physik studiert und war danach längere Zeit in der Forschung tätig (Hochenergiephysik am CERN und am Stanford Linear Accelerator Center). Nach der Rückkehr in die Schweiz leitete er vorerst die Neuroinformatikgruppe an der Uni Bern, führte dann längere Zeit die Nachdiplomausbildung Eduswiss und ist heute Leiter der Dienststelle für angewandte Forschung, Entwicklung und Technologietransfer an der Hochschule für Technik und Informatik der Berner Fachhochschule. Kryptographie, Datensicherheit und Biometrie gehören seit längerem zu seinen Interessengebieten und stehen auch im Mittelpunkt der Aktivitäten seiner kürzlich mit Kollegen gegründeten Firma AXSionics.

Hochschule für Technik und Informatik, Biel, lorenz.mueller@hta-bi.bfh.ch

[1] Die bekannten Authentifizierungsmechanismen für verteilte Systeme mit indirekter Authentifizierung der Nutzer (z.B. Radius) oder der Betrieb eines vertrauenswürdigen Netzes mit einem Key Distribution Center (KDC) (z.B. Kerberos) bieten für die biometrische Datenerfassung gegenüber einer simplen Client-Server-Authentifizierung keine wesentlich verbesserte Lösung. Das Problem, aus n Personen und n biometrischen Signaturen die richtige Kombination zu finden, ist in grösseren Netzen sogar noch schwieriger. Es bestehen zwar Bestrebungen, biometrische Signaturen mit einem eindeutigen digitalen Code zu parametrisieren, was aber angesichts der natürlichen Ungenauigkeit in der physischen Messung nur bedingt möglich ist.

[2] Eine partielle Identität ist eine Teilmenge der identifizierenden Daten einer Person. Gewisse partielle Identitäten, wie z.B. die AHV-Nummer, erlauben, eine Person eindeutig zu identifizieren, andere wie Name und Vorname erlauben es im Allgemeinen nicht.

[3] Pseudonymität bezeichnet eine Situation, in der Personen sich als Inhaber bestimmter Rechte oder als Zugehörige einer Gruppe eindeutig ausweisen können, ohne ihre Identität offen zu legen. Pseudonymität erlaubt die Verwendung kontextabhängiger partieller Identitäten, die untereinander nicht verknüpft werden können. Pseudonyme stellen ein wichtiges Werkzeug für die Wahrung der Privatsphäre dar. Pseudonyme sind bereits heute ein weit verbreitetes Konzept im täglichen wirtschaftlichen Leben, jede Form von nicht-übertragbaren oder mit der Person verbundenen Berechtigungsausweisen ohne Identifizierung beruht auf Pseudonymität (z.B. Skiliftausweis, Chatname, E-Mail-Konto bei Hotmail).

[4] Anonymität bezeichnet die Absenz einer Identifikationsmöglichkeit innerhalb einer Anonymitätsmenge. Der Grad der Anonymität wird durch die Entropie der Anonymitätsmenge gemessen.

[5] Die Idee, Biometrie als Authentifizierungswerkzeug in ein persönliches Token einzubetten, ist nicht neu (z.B. die Sony Puppy Card). Neu hingegen ist die vollständige Autonomie des Cod-it-Tokens von lokaler HW und die mit der Karte realisierte 3-Faktor-Authentifikation.

[6] Das Cod-it-System ersetzt nicht gängige Authentifizierungsmechanismen in einem Netzwerk (Radius, SIM usw.), sondern ergänzt diese Systeme mit einer sicheren Verbindung zur autorisierten Person.

[7] Als Minutia-Punkte werden lokale Merkmale im Rillenmuster des Fingerabdrucks bezeichnet. Sie charakterisieren und definieren die Lage und Art von Verzweigungen, Endungen, Einschlüssen, Divergenzen, lokale Rillendichte usw. Das NIST/NFIS-Programm identifiziert je nach Qualität des Rohbildes bis zu 70 solche Minutia-Punkte mit je bis zu 7 charakteristischen Merkmalen und ihrer relativen Positionierung zu den anderen Minutia (siehe dazu auch 1. Teil des Artikels im *Bulletin SEV/VSE* 19/03).

[8] T. Matsumoto, ein japanischer Professor, konnte kürzlich zeigen, dass ein Grossteil der Fingerprint-Sensoren gefälschte Finger nicht zurückweisen (False acceptance). Im Rahmen einer Diplomarbeit an der Software Schule Schweiz wurden diese Experimente verifiziert und Gegenmassnahmen für die Verbesserung der Erkennungsalgorithmen gesucht.

Matsumoto T., Matsumoto H., Yamada K., Hoshino S.: Impact of artificial 'gummy' fingers on fingerprint systems. In: Optical Security and Counterfeit Deterrence Techniques IV, Bellingham, Washington, 2002-01-23/25, Vol. 4677; The International Society for Optical Engineering, p. 275/288.

[9] Siehe zum Beispiel das Treo-Gerät von Handspring (www.handspring.com).

[10] Das Konsortium BioAPI (www.bioapi.org) hat mit der Spezifikation BioAPI v1.1 einen ersten Schritt in Richtung der Standardisierung biometrischer Verfahren gemacht (ANSI/INCITS 358-2002).

La biométrie – trait d'union entre la personne et son identité – seconde partie

L'authentification assurée par méthode biométrique

La mondialisation de la société, l'accélération des opérations économiques, la rapidité des contacts entre les différents médias, les réseaux de relations toujours croissants et changeants – autant de causes des problèmes d'identification qui se posent. Que faut-il entendre par identité? S'agit-il de désigner une personne et de l'affecter sans équivoque possible à un groupe disposant de certains droits sociaux, économiques et légaux ou entend-on directement par-là l'individu au sens biologique? Est-ce que «connaître quelqu'un» signifie être à même de reconnaître une personne en toutes circonstances d'après ses caractéristiques personnelles ou simplement posséder une carte de visite indiquant le nom de la personne et la fonction qu'elle exerce?

Datenerfassung und Kommunikation zwischen Systemen!

Kommunikationslösungen zwischen Maschinen und Systemen auf unterschiedlichen betrieblichen Ebenen sind sehr anspruchsvoll. Komserv ist der Partner für Lösungen, welche exakt auf Ihre Bedürfnisse zugeschnitten sind – von der Anbindung der Maschinen und Sensoren bis zum Datenaustausch mit übergeordneten Systemen.

KOMSERV
Automation Competence Center

Unsere Erfahrung – Ihr Vorteil.

Komserv AG | Industriestrasse 13 | CH-6010 Kriens | Phone +41 (0)41 349 61 61 | Fax +41 (0)41 349 61 60 | info@komserv.ch | www.komserv.ch