Aktivierung von Smartcards durch Biometrie (Fingerprintverfahren)

Norbert Pohlmann, Utimaco Safeware AG

Inhalt

Abstrakt

Die Nachteile einer Benutzerauthentisierung alleine durch PIN oder Passwort liegen auf der Hand: Neben der Unsicherheit und der Gefahr des Missbrauchs durch Diebstahl oder Ausspionieren verursacht menschliches Versagen (Vergesslichkeit oder Unachtsamkeit) hohe Administrierungskosten. Biometrische Verfahren bieten hier einen Ausweg, da die benutzten Merkmale nicht vergessen oder verloren und nur schwer kopiert werden können. Im Vergleich verschiedener Methoden stellt sich das Fingerprintverfahren als die praktikabelste und kostengünstigste Lösung dar, die hinreichend sicher ist. Da aus biometrischen Merkmalen wegen ihrer naturbedingten minimalen Schwankungen keine Schlüssel abgeleitet werden können, bietet sich die Kombination mit einer intelligenten Smartcard als Lösung an, die höchstmögliche Sicherheitsanforderungen erfüllt.

Hohe Kosten durch vergessene Passworte

Passworte und PINs werden zu oft vergessen, verloren, kopiert oder gestohlen. Kurze PINs oder „schlechte“ Passworte können mit intelligenten Programmen geknackt oder sogar von einem Unbefugten erraten werden. 30 bis 40 Prozent aller Helpdesk Calls in einer Organisation fallen durch vergessene Passworte an. Die Kosten pro User liegen in der Regel zwischen US$ 100-200 im Jahr. (s. Morgan Keegan&Co., Gartner Group)

Daher muss eine Lösung gefunden werden, die höchste Sicherheitsanforderungen erfüllt und gleichzeitig so bequem zu handhaben ist, dass die Benutzer sie auch immer verwenden und dabei die Vorschriften der Sicherheitspolitik einhalten. Was liegt also näher, als biometrische Verfahren zur Identifizierung der Nutzer einzusetzen?

Biometrische Verfahren

Biometrie ist die Identifikation und Authentisierung mittels biologischer Charakteristika. Biometrie benutzt physiologische oder verhaltenstypische Charakteristika zur Authentisierung, also personengebundene Merkmale. Biometrische Merkmale haben den Vorteil, dass sie nicht gestohlen und im Allgemeinen nur schwer kopiert werden können.

Biometrische Merkmale können auf viele Arten gemessen werden. Die unterschiedlichen Verfahren messen das Tippverhalten an einer Tastatur, die Fingergeometrie, das Fingerlängenverhältnis oder die Handgeometrie. Weitere Möglichkeiten sind: Stimmanalyse, Gesichtserkennung, Unterschriftendynamik, Erfassung des Netzhautmusters, Erfassung des Irismusters, Erfassung des genetischen Codes (DNA-Analyse) und die Fingerabdruckerfassung (unterschiedliche Verfahren). Alle diese Möglichkeiten tauchen auch in unterschiedlichen Kombinationen auf.

Ein Merkmal sollte sich im Laufe der Zeit möglichst wenig ändern, damit es für biometrische Verfahren geeignet ist und damit es immer wieder verwendet werden kann.

Bild 1: Zukunftsaussichten?

Eigenschaften des verwendeten biometrischen Merkmals

In der Praxis werden biometrische Merkmale in passive und aktive Merkmale aufgeteilt.

Passive Merkmale sind zum Beispiel: Gesicht, Retina, Iris, Fingerabdruck, Daktylogramm, Ohr, Handgeometrie, Venenmuster auf dem Handrücken und Geruch.

Aktive Merkmale sind zum Beispiel: Unterschrift, Schreibverhalten, Stimme/Sprechverhalten, Tippverhalten an der Tastatur und Gestik/Mimik beim Sprechen.

Es werden aber auch Merkmalskombinationen verwendet, zum Beispiel die Erfassung des Gesichts und der Gesichtsdynamik beim Sprechen kombiniert mit der Stimmerkennung.

Ein Merkmal muss folgende Eigenschaften besitzen, damit es für ein biometrisches Verfahren verwendet werden kann:

1. **Einzigartigkeit des Merkmals**
   Das Merkmal muss einzigartig in dem Sinne sein, dass es bei verschiedenen Menschen hinreichend verschieden ist.
2. **Konstanz**
   Das Merkmal sollte sich im Laufe der Zeit möglichst wenig ändern. Kleinere Veränderungen können adaptive biometrische Verfahren ausgleichen. Besteht die Gefahr des Verlustes oder der Unverwendbarkeit des Merkmals, sollte ein Ersatzsystem vorgesehen werden.
3. **Merkmalsverbreitung**
   Ein Merkmal sollte, um für biometrische Verfahren geeignet zu sein, bei möglichst vielen der potentiellen Nutzer vorhanden sein. Es gibt jedoch kleine Bevölkerungsgruppen, die gewisse Merkmale nicht aufweisen. So besitzt zum Beispiel ein kleiner Bevölkerungsanteil keine ausgeprägten Fingerabdrucksstrukturen. Ferner ist die Verwendung mancher Merkmale für andere Gruppen, zum Beispiel für Blinde oder Stumme, nicht geeignet. In diesem Fall muss ein alternatives Verfahren zur Verfügung gestellt werden.

Möglichkeit zur willentlichen Beeinflussbarkeit durch den Nutzer

Einige biometrische Merkmale bieten die Möglichkeit, neben dem Hauptmerkmal eine zusätzliche Information des Merkmalsträgers abzugeben.

So besteht beim Fingerabdruckverfahren die Möglichkeit, mehrere Finger zu registrieren und je nach Wahl des entsprechenden Fingers dem System eine Zusatzinformation zu geben. Bei der Stimmerkennung, die typisch mit einem festen, frei wählbaren Schlüsselwort kombiniert ist, besteht ebenfalls die Möglichkeit, durch Anlernen und Speichern verschiedener Schlüsselwörter eine Steuerinformation an das System zu geben. Diese Eigenschaft gewinnt besondere Bedeutung in Anwendungsszenarien, in denen mit einer Erpressung des Merkmalsträgers gerechnet werden muss. Der erpresste Merkmalsträger kann auf diese Weise einen stillen Alarm abgeben, ohne dass der Erpresser dies erkennt.

Benutzerakzeptanz

Ein weiterer wichtiger Punkt bei der Verwendung biometrischer Verfahren ist die Akzeptanz durch die Benutzer. Die folgenden Aspekte sind hier entscheidend:

1. Komfort bei der Benutzung
   Hier spielen der Zeitaufwand im Normalfall, die Einfachheit der Handhabung, der Zeitaufwand bei der Registrierung, die Häufigkeit der Aktualisierung des Musters, der Aufwand zur Referenzdatenerfassung, der Zeitaufwand im Sonderfall (False Rejection), die Möglichkeiten einer zeitweiligen Ersatzlösung und der Aufwand dieser Ersatzlösung beim Benutzer eine wichtige Rolle.
2. Vertrautheit / Transparenz
   Bei diesem Aspekt ist entscheidend, ob die Vertrautheit mit bereits bekannten und etablierten Vorgängen und die Bereitschaft zur Kooperation beim Benutzer vorhanden sind. Dazu muss der Benutzer die Zusammenhänge und Abläufe verstehen.
3. Belästigung
   Für eine hohe Benutzerakzeptanz spielen die Hygiene und das Eindringen in die persönliche Schutzsphäre des Benutzers eine wichtige Rolle.
4. Vorurteile und Ängste
   Vorurteile gegen den Vorgang der Registrierung im System oder der Benutzung, die Angst vor Missbrauch beim Vorgang der Registrierung oder der Benutzung und die Frage, ob die Methode auch erkennungsdienstlich verwendet wird, sind hier entscheidend. Bei der Methode des Netzhautscannings könnten die Benutzer Angst vor Verletzungen haben.

Vergleich der biometrischen Verfahren

Die oben dargestellten Kriterien der Benutzerakzeptanz, der Einzigartigkeit, Konstanz und Verbreitung des Merkmals sowie der technischen und finanziellen Aufwendungen müssen in Relation zur Sicherheit der Identifizierung gesetzt werden. Die folgende Tabelle ist einem Bericht von Morgan Keegan & Co über biometrische Verfahren entnommen:

Rank	Accuracy	Convenience	Cost	MOC integration
1	DNA	Voice	Voice	**Finger**
2	Iris	Face	Signature	Voice
3	Retina	Signature	**Finger**	
4	**Finger**	**Finger**	Face	
5	Face	Iris	Iris	
6	Signature	Retina	Retina	
7	Voice	DNA	DNA	

Source: Morgan Keegan&Co report January 2001

Die linke Spalte zeigt die Rangfolge der biometrischen Verfahren in Bezug auf ihre Sicherheit. Das sicherste Merkmal ist der genetische Fingerabdruck. Allerdings ist ein ausschlaggebender Nachteil die Nicht-Akzeptabilität: Für die tägliche Arbeit oder häufige Anwendung ist dieses Verfahren nicht geeignet, es findet allenthalben im Kriminalitätsbereich (Fahndung nach Schwerverbrechern, Sexualtätern) Anwendung.

Die Iriserkennung bietet eine hohe Sicherheit, erfordert allerdings hohen technischen Aufwand und wird nur für Hochsicherheitsanwendungen eingesetzt werden können. Das Gleiche gilt für die Retina.

Für die alltäglichen Sicherheitsanforderungen im Business-Bereich ist daher das Fingerprintverfahren das hinreichend sichere und absolut komfortable geeignete Verfahren.

Vorzüge von Biometrie gegenüber Passwort/PIN

Mehr Sicherheit im Sinne der elektronischen Signatur

Das Signaturgesetz sieht eine PIN zur Authentisierung vor. Aber: Eine PIN kann weitergegeben oder ausgeliehen werden, eine PIN ist wie eine „Vollmacht" übertragbar. Die PIN ist leicht zu kopieren und erzeugt keine Bindung an die Person. Die Frage bleibt: Interagiere ich mit der Person XY oder nicht?

Die biometrische Authentisierung bietet eine wesentlich höhere Sicherheit der Authentizität der interagierenden Personen im Sinne der elektronischen Signatur. Eine Weitergabe der Authentisierungsinformation ist nicht möglich. Das bedeutet ganz eindeutig ein wesentlich höheres Maß an Sicherheit.

Kostenersparnis

Ein wichtiges Argument ist auch die Senkung des internen Administrationsaufwandes, der durch vergessene Passworte entsteht. Das Vergessen eines Passwortes kostet durchschnittlich zwischen 55 und 85 Dollar. Die Authentisierung durch biometrische Verfahren bedeutet hier eine große Kostenersparnis.

Benutzerkomfort und Bequemlichkeit

- Die Notwendigkeit, in regelmäßigen Zeitabständen das Passwort zu ändern, fällt weg.
- Der Benutzer muss sich keine Passworte mehr ausdenken, die er sich unter Umständen nur schwer merken kann. Je ungewöhnlicher ein Passwort ist, desto sicherer ist es – und desto schwerer zu merken.
- Der Benutzer muss sich nicht viele verschiedene Passworte für eine Vielzahl von Anwendungen merken.
- Der interne Administrationsaufwand, der durch vergessene Passworte entsteht, wird gesenkt (Kostenersparnis).
- SingleSignOn erlaubt die einmalige Authentisierung und ersetzt damit gleich verschiedene PINs und Passworte. Dies bedeutet auch eine enorme Zeitersparnis.
- Die biometrische Authentisierung ist schneller und einfacher als jede Alternative.

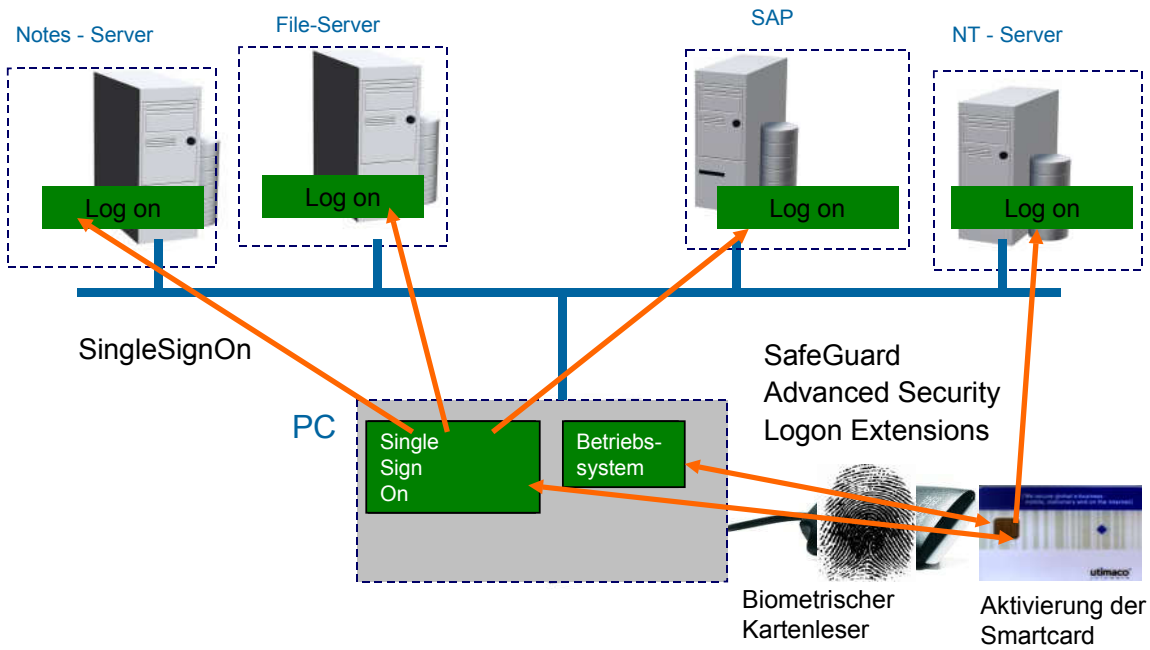

Bild 2: Biometrische Authentisierung

Denkbare Fehlerquellen

Die größten Fehlerquellen bei biometrischen Verfahren sind die Falschakzeptanz und die Falschrückweisung. Falschakzeptanz nennt man die Wahrscheinlichkeit, dass eine nicht berechtigte Person aufgrund ähnlicher biometrischer Charakteristika akzeptiert wird. Falschrückweisung bedeutet entsprechend die Wahrscheinlichkeit, einer berechtigten Person den Zugang zu verweigern, weil die Übereinstimmungserfordernisse biometrischer Charakteristika zu rigide gehandhabt werden.

Die Übereinstimmungserfordernisse bei biometrischen Merkmalen müssen immer einen gewissen Spielraum offen halten. Der Fingerabdruck zum Beispiel kann durch äußere oder physiologische Temperaturschwankungen oder unterschiedliche Stimmungen der Person (Schwitzen, Aufregung) geringfügige Abweichungen zeigen, die einkalkuliert sein sollten. Ebenso müssen Rückstände von Staub, Schmutz, Fett auf der Haut berücksichtigt werden.

Genau aus diesem Grund kann man aus biometrischen Merkmalen keinen Schlüssel ableiten, der ja immer eine genaue mathematische Berechnung enthält, die keine Schwankungen zulässt.

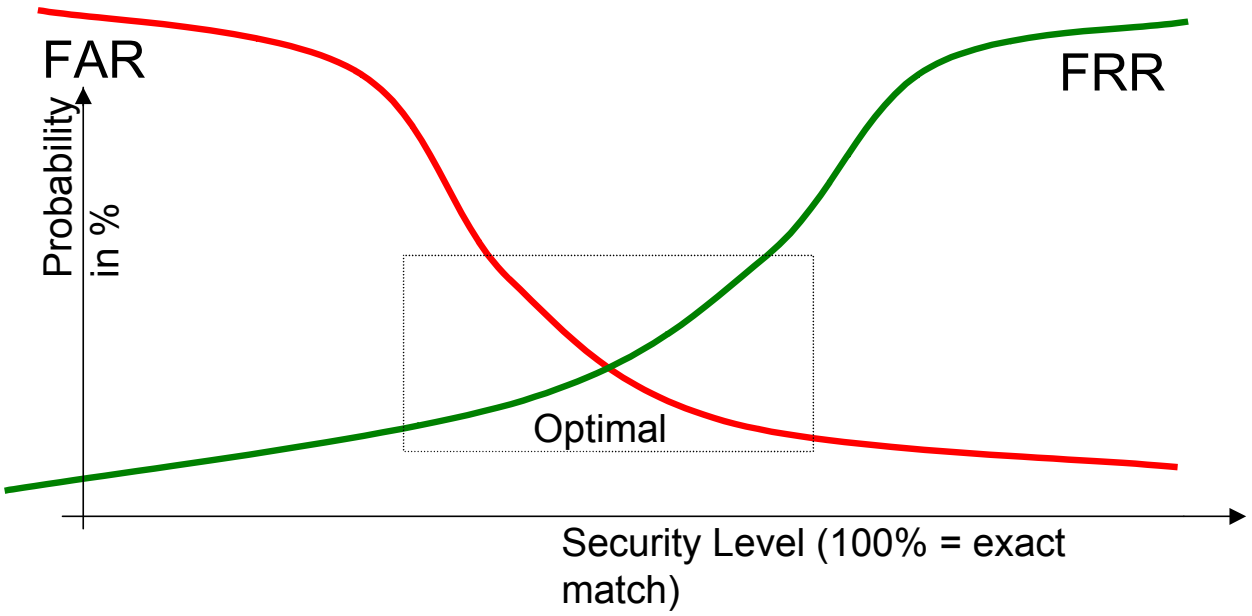

Bild 3: Wahrscheinlichkeit der Falschakzeptanz und Falschrückweisung

Die Wahrscheinlichkeit der Falschakzeptanz und der Falschrückweisung müssen in eine akzeptable Relation zum Sicherheitslevel gebracht werden. Das Verfahren des Precise Pattern Matching verringert die Raten der Falschakzeptanz und der Falschrückweisung auf einen akzeptablen Faktor, der vernachlässigt werden kann.

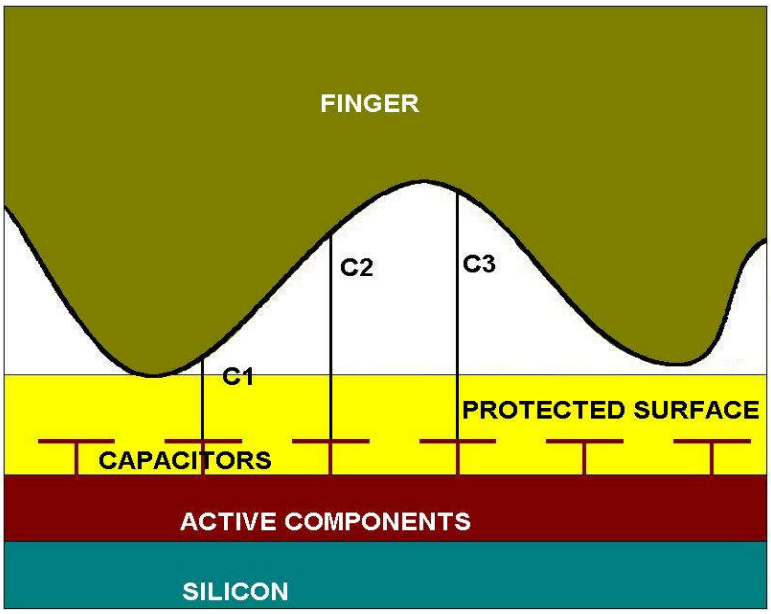

Bild 4: Ergebnis des Precise Pattern Matching ist ein 3D-Bild

Prinzip „Wissen“ und „Besitz“

Die Eingabe von Passworten per Tastatur ist immer noch das gebräuchlichste Verfahren zur Authentisierung von Personen in der IT-Welt. Dieses Verfahren hält sich hartnäckig gegenüber inzwischen verfügbaren weit sichereren Methoden, die zusätzlich zum Prinzip "Wissen" (Passwort) eine zweite Hürde, den "Besitz" eines Authentisierungstoken (z. B. eine Smartcard) nutzen. Passwortattacken gehören zu den häufigsten Angriffen auf die Informationssicherheit und zu den einfachsten. Schon nach wenigen Minuten finden intelligente Crackerprogramme die Passworteinträge einer Windows Registry. Snifferprogramme scannen den Netzverkehr nach typischen Strings, die Passworte enthalten. Und ganz ohne zusätzlichen Aufwand lassen sich viele Kennworte einfach und schnell nach der Methode "Trial and Error" erraten. Ist diese Schranke erst genommen, steht dem Angreifer die ganze digitale Welt des Passwortbesitzers offen.

Aus diesem Grund nutzen sicherheitssensible Organisationen heute vermehrt Smartcards als digitale Ausweise oder planen zumindest deren Einsatz in naher Zukunft. Die Plastikausweise im Scheckkarten-Format speichern Passworte oder kryptographische Schlüssel in einem sicheren "Tresor". Gehen sie verloren, sind sie ähnlich wie eine EC-Karte für den Finder völlig wertlos, weil sie ihre geheimen Informationen nur nach Eingabe einer PIN preisgeben. Im Unterschied zur EC-Karte funktionieren sie allerdings nicht nach dem unsicheren Magnetstreifenprinzip, sondern nutzen einen intelligenten Chip mit einem nahezu unüberwindbaren Sicherheitssystem. Smartcards können aber noch viel mehr. Die in vielen gängigen Smartcards bereits heute integrierten Krypto-Prozessoren können selbständig digitale Signaturen berechnen und dabei ohne Umweg über das unsichere PC-System, den geheimen Signatur-Schlüssel des Besitzers direkt auf der Karte nutzen. Wer sich für solche PIN-geschützen RSA-Smartcards entscheidet, ist bestens gerüstet für die Anforderungen des

Signaturgesetzes an qualifizierte digitale Signaturen, die Rechtsverbindlichkeit garantieren.

Kombination von Smartcard und Fingerprint

Die Vorteile des Einsatzes einer intelligenten Smartcard mit integriertem Krypto-Prozessor können genutzt werden, ohne dass Unternehmen die Unsicherheiten des Verlustes oder Diebstahls der PIN in Kauf nehmen müssen: Wenn die Smartcard mit dem Fingerprint des Benutzers aktiviert wird, ist das Prinzip des Wissens (einer PIN) durch ein genetisches „Wissen“ ersetzt, das nicht verloren gehen oder vergessen werden kann. Und das auch nicht absichtlich an Kollegen oder Helfer weitergegeben werden kann. Der geheime Schlüssel des Benutzers, der direkt auf dem unknackbaren Sicherheitssystem Smartcard gespeichert ist, kann nur durch die unverwechselbare und unmittelbare biometrische Identifizierung des authentischen Nutzers aktiviert werden.

Denkbare Angriffe

Denkbare Angriffsmöglichkeiten auf die Fingerprint-Authentisierung wären der Verlust oder Diebstahl des biometrischen Merkmals: Dem Verlust oder der Unbrauchbarkeit durch Verletzungen kann dadurch vorgebeugt werden, dass mehrere Merkmale (in dem Fall mehrere Finger) optional gespeichert werden. Der Diebstahl setzt wirklich extreme kriminelle Energie voraus und wäre nur in einem Hochsicherheitszusammenhang realistisch denkbar. In diesem Kontext gibt es sehr viele organisatorische und personelle Sicherheitsmaßnahmen, die alle überwunden werden müssten, so dass diese Möglichkeit als unrealistisch angesehen werden kann.

Eine Maßnahme gegen denkbare technische Angriffe auf das Zielsystem PIN-Datenbank ist die Match-On-Card-Technologie.

Verbindung zwischen Digitaler Signatur und Biometrie

Der konventionelle Weg: Die Passwort Datenbank

Der einfachste und auch universellste Weg, Biometrie und digitale Signatur zu verbinden, ist sicherlich der folgende: Der Benutzer identifiziert sich gegenüber einem Zielsystem (meist PC-Applikation) mittels seines biometrischen Merkmals. Die Applikation vergleicht den gemessenen Wert mit dem Referenzwert (Template) des Benutzers, der in einer Datenbank gespeichert ist. Stimmen die beiden Werte genügend überein, wird eine dem Template zugeordnete gespeicherte PIN aus der Datenbank gelesen. Diese PIN wird dann für eine konventionelle Anmeldung beim Signaturdevice (Smartcard oder Schlüsseldatei) des Benutzers verwendet. Das Signaturdevice erzeugt die geforderten digitalen Signaturen.

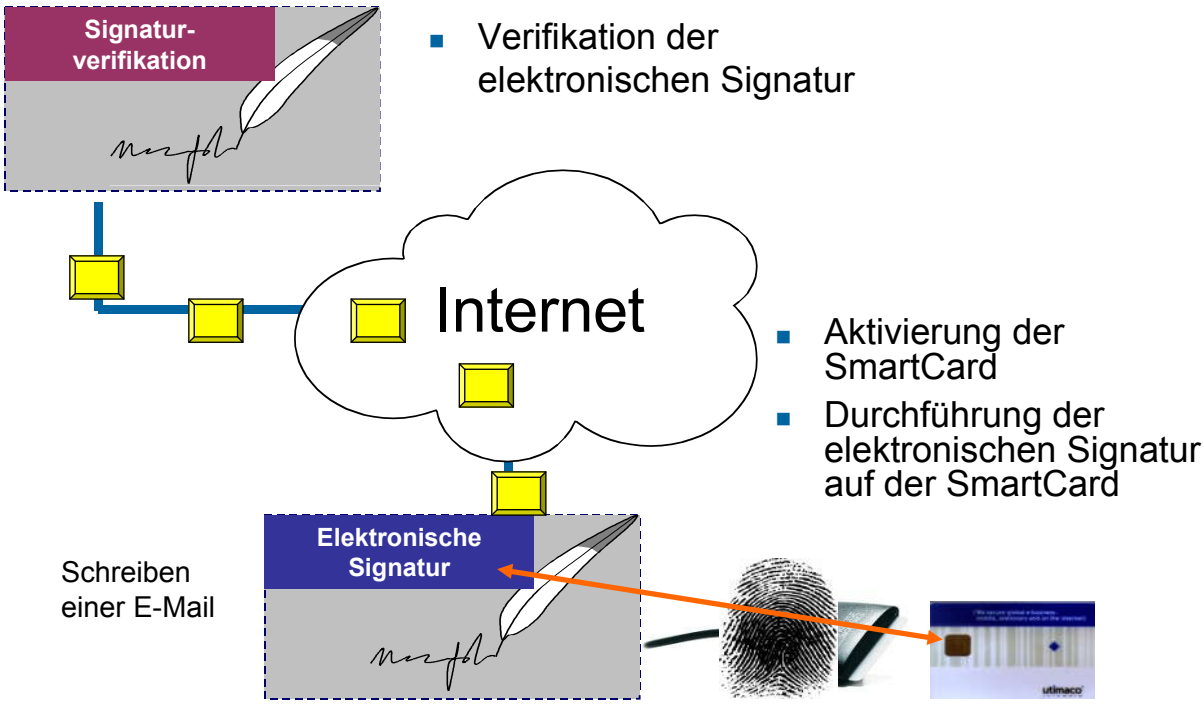

Bild 5: Aktivierung der elektronischen Signatur

Obwohl diese Vorgang für den Benutzer so aussieht, als hätte er sich biometrisch - zum Beispiel mit seinem Fingerabdruck - an seinem Signaturdevice angemeldet, so ist dies in Wahrheit weiterhin über den Umweg einer PIN erfolgt. Dies hat eine Reihe von Vor- und Nachteilen:

Vorteile:

- Der Benutzer muss sich keine PIN für sein Signaturdevice merken und kann diese somit auch nicht vergessen. (allgemeiner Vorteil bei Verwendung von Biometrie zur Anmeldung)
- Das Signaturdevice selbst muss nicht an die Biometrie angepasst werden. Konventionelle, eventuell schon im Einsatz befindliche Devices (etwa Smartcards) können ohne Änderung weiter verwendet werden. Die biometrische Anmeldung wird "darum herum" gebaut.

Nachteile:

- Die Authentisierung gegenüber dem Signaturdevice selbst erfolgt weiterhin über eine PIN. Kennt jemand die PIN, kann er Signaturen leisten, ohne zuvor eine Biometrische Erkennung durchlaufen zu müssen.
- Kennt der Benutzer die PIN, kann er das Signaturdevice immer noch an andere Personen weitergeben, die dann damit Signaturen leisten können. Eine eindeutige Zuordnung Signatur : Benutzer ist weiterhin nicht möglich.
- Größter Nachteil: Die PIN für dieses Signaturdevice (und die aller anderen Nutzer des Systems) liegt in einer Datenbank (und nicht nur im Kopf des Benutzers) abgespeichert. Gelingt es einem

Angreifer, die Datenbank auszulesen oder die Kommunikation zwischen Datenbank und Client-PC abzuhören, kann er sich die PIN aneignen und für die eigene Anmeldung zum Signaturdevice des Benutzer verwenden.

- Da aus einem biometrischen Messvorgang kein eindeutiger Schlüssel abgeleitet werden kann, kann die PIN in der Datenbank auch nicht besonders sicher verschlüsselt werden. Woher sollte man den Schlüssel zur Entschlüsselung der PIN nehmen? In der Regel wird hierfür ein fix programmierter Schlüssel in der Software verwendet, der nur geringe Sicherheit bietet.
- Gelingt es einem Angreifer, sein eigenes Template in die Datenbank an die Stelle des Templates eines rechtmäßigen Benutzers einzuschleusen, kann er sich selbst beim System anmelden und das System wird ihn an dem (eventuell zuvor gestohlenen) Signaturdevice des Benutzers anmelden.

Match On Card – Logon mit Fingerabdruck

Smartcards sind derzeit die sicherheitstechnisch beste Lösung, um digitale Signaturen zu erzeugen. Durch Ihre Fähigkeit, selbst Rechenoperationen durchzuführen, können Smartcards in die Lage versetzt werden, Biometrische Verfahren auszuführen. Die Idee des sogenannten "Match-On-Card"-Verfahrens ist bestechend einfach:

Anstatt einer PIN wird ein biometrisches Template des rechtmäßigen Benutzers in der Karte nicht rücklesbar hinterlegt. Um sich bei seiner Karte zu authentisieren und damit die Signaturfunktionen zu aktivieren, sendet der Benutzer keine PIN an die Karte, sondern einen aktuellen Scan seines biometrischen Merkmals. Anstatt eine PIN Zeichen für Zeichen zu vergleichen, vergleicht die Karte den aktuellen Scan mit dem gespeicherten Template mittels eines Biometrischen Vergleichsalgorithmus (daher der Name "Match-On-Card"). Abgesehen davon, dass der Vergleichsalgorithmus komplexer ist, ist der Vorgang vom Prinzip her nahezu identisch mit dem Logon mittels PIN.

Smartcards mit solchen Fähigkeiten sind seit Ende 2000 erhältlich. Erste Anwendungen dieser Technologie sind seit dem zweiten Quartal 2001 verfügbar. Als biometrisches Merkmal wird derzeit der Fingerabdruck benutzt.

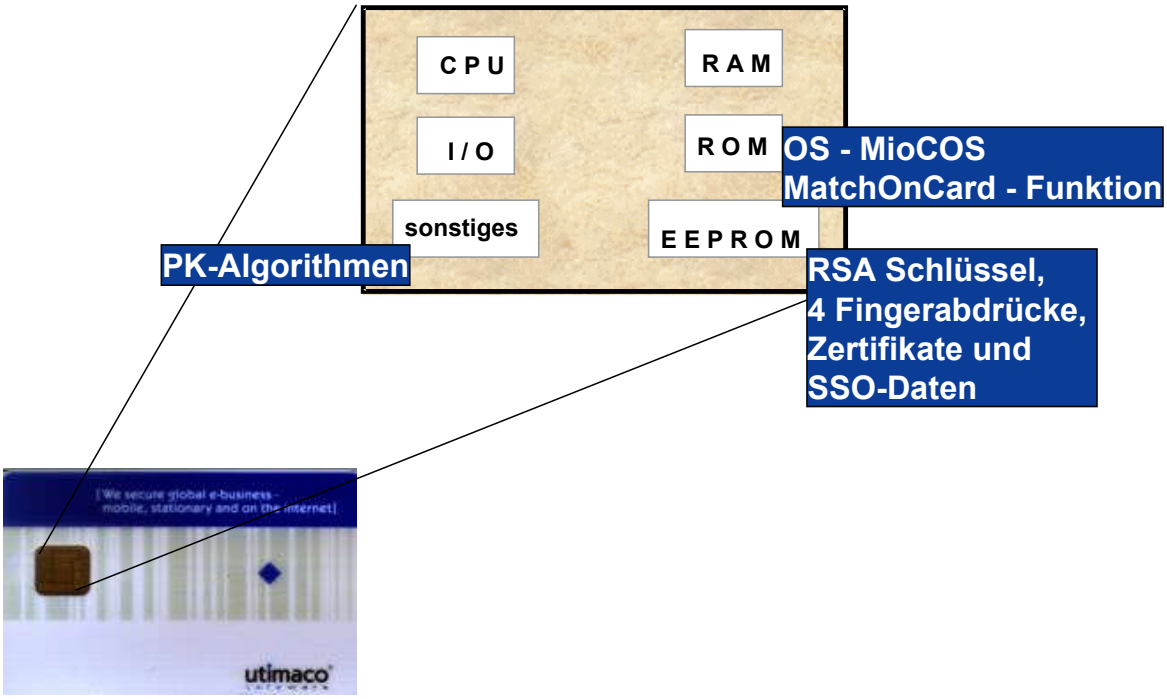

Bild 6: Smartcard mit Algorithmen und Match-On-Card-Funktion

Obwohl diese Methode relativ gut geeignet ist, Biometrie und Kryptographie zu vereinen, gibt es auch hier spezifische Vor- und Nachteile:

Vorteile:

- Echte Anmeldung direkt über das biometrische Merkmal (Fingerabdruck). Es ist keine PIN mehr im Spiel, die vergessen, gestohlen oder weiter gegeben werden kann.
- Durch Speicherung und Prüfung des biometrischen Merkmals direkt in der Karte ist es nicht mehr nötig, eine separate Datenbank zu führen, in der Templates oder PINs gespeichert werden. Damit fallen viele potentielle Angriffspunkte weg. Des weiteren vereinfachen sich Installation und Administration der Software, da solche Datenbanken auch nicht installiert oder repliziert werden müssen.
- Die Mobilität des Benutzers wird unterstützt. Da alle zur Verifikation seines Merkmals nötigen Daten in seiner Karte gespeichert sind, kann er auch off-line ohne Verbindung zu einem Template-Server arbeiten und Signaturen leisten.
- Viele Benutzer fühlen sich unwohl bei dem Gedanken, dass ihre Biometrischen Daten in einer zentralen Datenbank gespeichert werden. Bei Match-On-Card sind diese Bedenken unnötig, da der Benutzer diese Daten in seiner Karte immer bei sich hat und diese außerdem nicht einmal von dort wieder auslesbar sind.

Nachteile:

- Nicht anwendbar für reine Softwarelösungen mit Schlüsseldateien anstatt Smartcards.

- Obwohl anstatt der PIN nun ein "biometrischer" Datenstrom zur Karte geschickt wird, und der Vergleichsalgorithmus komplexer ist, bleibt es letztlich doch ein Datenstrom und kann im Grunde mit einer sehr langen PIN verglichen werden. Wenn es jemandem gelingt, diesen Datenstrom herauszufinden (was sicherlich schwieriger ist als bei einer PIN), kann er sich damit gegenüber der Karte authentisieren.
- Match-On-card ist (noch) nicht standardisiert. Um ein solches System zu realisieren, ist eine Zusammenarbeit zwischen Biometrie-Hersteller und Smartcard-Hersteller nötig. Das heißt, nicht jede heute verfügbare Smartcard und nicht jede heute verfügbare Software, die Smartcards benutzt, kann mit Match-On-Card verwendet werden.
- Nicht jedes biometrische Verfahren eignet sich für Match-On-Card. Verglichen mit einem heutigen Pentium PC hat eine Smartcard nur eine geringe Rechenleistung. Es muss daher ein biometrisches Verfahren eingesetzt werden, das in einem solch schwachen Rechner in "vernünftiger" Zeit (etwa eine Sekunde) abgearbeitet werden kann. Auch dürfen die biometrischen Templates nicht zu viel Platz beanspruchen, da der Platz auf Smartcards beschränkt ist Fingerabdruck-Verfahren sind daher am besten für Match-On-Card geeignet.

SafeGuard Biometrics von Utimaco Safeware bietet eine einfache Lösung für das Prinzip Besitz und Biometrie („genetisches Wissen“) mit Einbindung der Match-On-Card-Technologie: Ein neuer Smartcard-/Fingerabdruckleser mit einem neuartigen Fingerprint-Algorithmus von Precise Biometrics kombiniert mit einem neuen Betriebssystem für Smartcards mit Match-On-Card-Funktion von Miotec, intelligent eingebunden in Sicherheitsanwendungen von Utimaco Safeware AG.

Zusammenfassung

Viele Kunden wollen eine höhere Sicherheit in den neuen Geschäftsprozessen. Das Einleiten einer Aktion mit hohen Konsequenzen muss eindeutig und beweisbar sein, damit wirklich kritische Geschäftsprozesse in das Internet gebracht werden und eine sichere und beherrschbare Informationstechnik realisiert werden kann.

Benutzerkomfort und Bequemlichkeit in Verbindung mit Sicherheitsfunktionen ist für die Verwendung von Sicherheitsmechanismen ein wichtiger Erfolgsfaktor. Mit dem Biometrie-Leser kann man nicht nur die Bequemlichkeit und den Komfort erhöhen, sondern gleichzeitig ein wesentlich höheres Maß an Sicherheit erreichen. Die Regeln zur sicheren Verwendung von Passworten werden nicht mehr als lästige Pflicht empfunden, sondern können bequem eingehalten werden, zum Beispiel mit der Hilfe von SingleSignOn-Verfahren.

Die Nutzung von Biometrie an Stelle einer PIN vereinfacht den Prozess für den User noch mehr und erhöht nochmals den Sicherheitslevel der e-Business Implementierung. Wenn die SmartCard mit Hilfe des Fingerabdruckes aktiviert wird, kann eine höhere Sicherheit bei gleichzeitig höherer Bequemlichkeit und Kostenersparnis erreicht werden, da die Kosten für möglicherweise vergessene PINs wegfallen.

Die Kombination der beiden Identifizierungs- und Authentisierungsverfahren SmartCard und Fingerprint ist deshalb so günstig, weil sie einen für Geschäftsprozesse angemessen hohen Sicherheitslevel bietet und gleichzeitig höchsten Benutzerkomfort, große Kostenersparnis und Investitionssicherheit gewährleistet.

Kasten1: Zukunftsaussichten

- 1 Smartcard für alle Anwendungen statt unzähliger Karten im Portemonnaie: Scheckkarte, Geldkarte, Rabattkarte, Mitgliedsausweis, Krankenkassenkarte, Bahncard, Magnetkarte für die Tiefgarage, Mitarbeiterausweis, Geldkarte, Clubkarte, ...
- Fingerprint-Sensor auf der Chipkarte selbst macht Fingerprint-Lesegerät überflüssig
- Signaturgesetz und Sicherheitssysteme mit nachweislich sicherer Technologie sorgen für hohe Sicherheit, zum Beispiel SafeGuard Sign&Crypt von Utimaco Safeware
- Integration in SAP-Anwendungen und interoperable Public-Key-Infrastrukturen für sicheren elektronischen Geschäftsverkehr
- Sekundenschnelles Desktopswitching mit Smartcard und Fingerprint in großen Unternehmen und Institutionen wie Krankenhäusern, in denen verschiedene Personen am gleichen PC arbeiten
- Zeit- und Kostenersparnis durch SingleSignOn-Prinzip mit biometrischem Sensor auf der Chipkarte selbst

Kasten 2: Fingerprint Verfahren nach Minutien und Pattern Matching

Minutien	**Pattern Matching**
Prüfung der Fingerabdrücke auf Übereinstimmung: Vergleich mehrerer Ausschnitte	Sensor misst den Abstand zwischen der Hautoberfläche des Fingers und den Kondensatoren (C1, C2, C3 ..); Ergebnis der Messungen ist ein ‘3D’ Bild.
nicht sehr genau, da möglicherweise 5 Ausschnitte als übereinstimmend erkannt werden, der 6. oder 7. hätten nicht übereingestimmt	sehr genau, da sehr viele Messungen hintereinander durchgeführt werden