Integration biometrischer Anwendungen in Sicherheitsinfrastrukturen

Dr. Norbert Pohlmann

UTIMACO Safeware AG

Germanusstr. 4

52080 Aachen

norbert.pohlmann@utimaco.de

Zusammenfassung

Für Organisationen und Unternehmen ist es wichtig festzustellen, welche Gefahren durch die Nutzung der neuen Technologien entstehen. Sind die Risiken bekannt, wird eine Einschätzung darüber möglich, welche Angriffe und Gefahren relevant sind und welche vernachlässigt werden können. Mit Hilfe geeigneter Sicherheitsmaßnahmen kann die globale Informationsgesellschaft ihre Verwundbarkeit reduzieren. Die verwendeten Sicherheitsmechanismen müssen aber auch einfach und bequem genutzt werden können, damit sie eine breite Akzeptanz finden.

Neue Technologien, wie Biometrie, sind einerseits attraktiv und können helfen, die Sicherheit weiter zu erhöhen, andererseits sind diese Technologien auch immer im Kreuzfeuer der Kritik.

Anhand der folgenden Skizze werden die Anforderungen und die Realisierung anhand eines ausgewählten Projektes mit integrierten biometrischen Lösungen dargestellt und speziell auf die aktuelle Kritik an dieser Technologie eingegangen. Des Weiteren werden allgemeine, vom konkreten Projekt unabhängige Einsatzgebiete biometrischer Sicherheitslösungen für wesentliche Mechanismen, wie Authentikation, Dateiverschlüsselung und digitale Signatur vorgestellt.

Das Projekt ROBIN verdeutlicht, dass Benutzerkomfort und Bequemlichkeit in Verbindung mit Sicherheitsfunktionen wichtige Erfolgsfaktoren für die Verwendung von Sicherheitsmechanismen sind. Biometriefähige Sicherheitsanwendungen und Smartcards sowie eine PKI-basierte Sicherheitsinfrastruktur sind die Grundlagen dieses Konzepts. Die hier vorgestellte Lösung hat sich in der Praxis bewährt und kann auf alle Bereiche übertragen werden, in denen Aktionen mit weitreichenden Konsequenzen auf elektronischem Weg getätigt werden, deren Urheberschaft eindeutig und beweisbar sein muss.

1 Biometrie und IT-Sicherheit

Die meisten Geschäftsprozesse wurden in der Vergangenheit persönlich oder – mit Hilfe der Post – papiergebunden abgewickelt. Solche Abläufe können heute durch eine gemeinsame globale IT-Infrastruktur weitaus rationeller gestaltet werden. Die elektronischen Daten können direkt und ohne Medienbruch in die Arbeitsprozesse einbezogen werden. Dieser Trend zum Re-Engineering der Geschäftsprozesse in allen Bereichen geht einher mit der Internationalisierung und Globalisierung. Das bedeutet auch eine immense Zeit- und Kostenersparnis.

Im Rahmen des Projekts ROBIN wird ein Best Practice Beispiel vorgestellt, bei dem biometrische Technik großflächig zur Absicherung von IT-Systemen in der öffentlichen Verwaltung zum Einsatz kommt. Kern des Projekts, das vom niederländischen Justizministerium in Auftrag gegeben wurde, ist die Bereitstellung einer sicheren IT-Umgebung für die "Richterlichen Organisationen“ der Niederlande.

Verwaltungsprozesse, die bislang auf dem herkömmlichen Weg abgewickelt wurden, sollen künftig auf elektronischem Weg durchgeführt werden und dabei eine dem bisherigen Stand äquivalente Sicherheit bieten. Um die Verbindlichkeit und Vertraulichkeit sämtlicher elektronischer Prozesse mit der notwendigen Sicherheit zu gewährleisten, werden Mechanismen wie Identifikation und Authentisierung, Ver- und Entschlüsselung oder die digitale Signatur mit Hilfe biometrischer Verfahren eindeutig an den einzelnen Nutzer gebunden.

Biometrische Identifikationsverfahren, die Körpermerkmale mittels biologischer Charakteristika – zum Beispiel einen Fingerabdruck, die Stimme oder Gesichtszüge – zur eindeutigen Identifikation von Personen nutzen, sind sicherer als ein Passwort. Denn im Gegensatz zu einem Passwort kann ein solches Merkmal nicht gestohlen, verloren, vergessen oder weitergegeben werden. 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 Netzhaut-musters, 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.

Biometrieverfahren stellen neben der hohen Sicherheit auch eine starke Vereinfachung für den Benutzer dar. Da diese Verfahren zudem auf die Zukunft ausgerichtet sind, bieten sie dem Anwender eine hohe Investitionssicherheit.

Bei der Authentisierung gibt es unterschiedliche Methoden wie „What you know“ (Passwort), „What you have“ (SmartCard) und „What you are“ (Biometrik). Um eine hohe Sicherheit gewährleisten zu können, wird gefordert, dass bei einer Authentisierung mindestens zwei dieser drei Verfahren gleichzeitig eingesetzt werden.

2 Wie sicher ist die Biometrie?

Frühere biometrische Verfahren waren bei weitem nicht so genau. Die Fingerabdrücke wurden an mehreren Punkten auf Übereinstimmung geprüft. Eine Ungenauigkeitsrate musste in Kauf genommen werden [Pohl3/01].

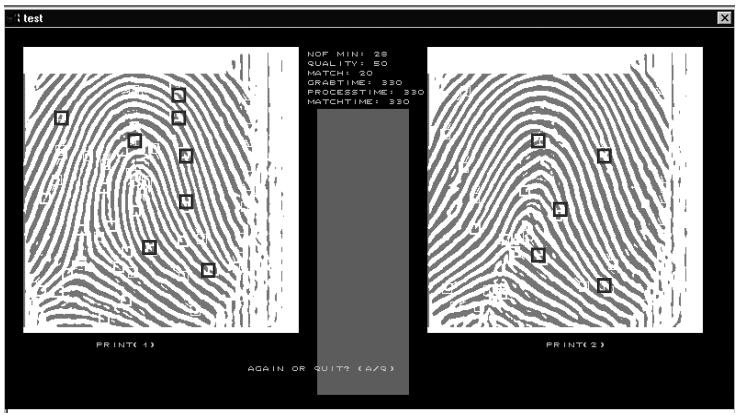

Bild 1: Übereinstimmung der Ausschnitte bei unterschiedlichen Abdrücken

Im sogenannten „Minutien-Verfahren“ wurden nur kleine Ausschnitte gemessen, so dass die Gefahr bestand, dass die gemessenen fünf Ausschnitte passen, aber der sechste oder siebente hätte nicht mehr gepasst. Das heißt, es bestand die große Gefahr, dass Leute als berechtigt anerkannt worden sind, obwohl sie es gar nicht waren.

Heutige biometrische Verfahren sind sehr genau und daher sicherer. Mit der Möglichkeit des präzisen Mustervergleichs (Pattern Matching) lässt sich eine hohe Genauigkeit erzielen. Dieses Verfahren beinhaltet mehr Informationen als das minutien-basierte Verfahren und ist für schnelle 1:1 Vergleiche für 8 Bit SmartCard Prozessoren optimiert. Die Prüfung des Fingerabdrucks wird dadurch so schnell, dass die Verzögerung kaum noch wahrnehmbar ist. Das Pattern Matching ist optimal für kleine Leseeinheiten und daher sehr geeignet für Applikationen wie das tägliche mehrmalige Einloggen in den Arbeitsrechner.

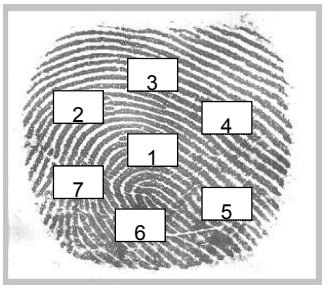

Bild 2: Pattern Matching

Mit einem Sensor wird der Abstand zwischen der Hautoberfläche des Fingers und den Kondensatoren (C1, C2, C3 ..) gemessen. Das Ergebnis der Messungen ist ein '3D' Bild. Da sehr viele Messungen hintereinander durchgeführt werden, ist die Wahrscheinlichkeit der falschen Akzeptanz äußerst gering.

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 oder Fett auf der Haut berücksichtigt werden.

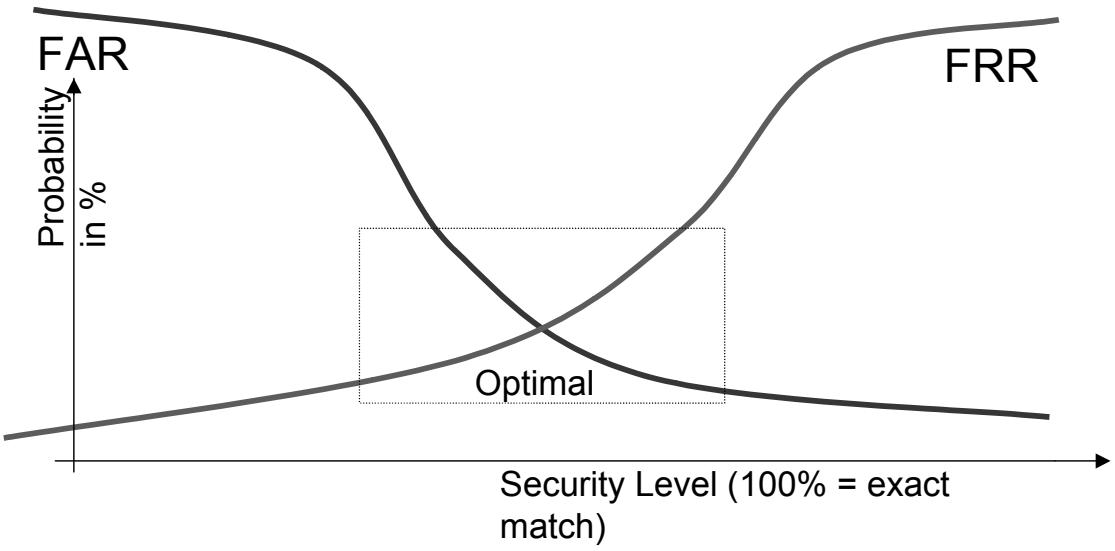

Bild 3: Wahrscheinlichkeit der Falschakzeptanz und Falschrückweisung

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

3 SmartCards, die mit Fingerabdruck aktiviert werden

Welchen Nutzen hat die Integration von biometrischen Verfahren für SmartCards?

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. Hier ist keine Weitergabe der Authentisierungsinformation möglich.

Ein Beispiel für die Übertragung einer Vollmacht ist die Großmutter, die ihren Enkeln ihre PIN gibt, damit sie in ihrem Namen Prozesse abwickeln. Die Weitergabe von Authentisierungsinformationen ist bei biometrischen Verfahren nicht gegeben. Das bedeutet ganz eindeutig ein wesentlich höheres Maß an Sicherheit.

Geringere Kosten

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.

4 Das Projekt ROBIN

Im Rahmen des Projekts ROBIN wird zum weltweit ersten Mal biometrische Technik großflächig zur Absicherung von IT-Systemen in der öffentlichen Verwaltung eingesetzt. Kern des Projekts ist die Bereitstellung einer sicheren IT-Umgebung für die "Richterlichen Organisationen“ der Niederlande.

Verwaltungsprozesse, die bislang auf dem herkömmlichen Weg abgewickelt wurden, sollen künftig auf elektronischem Weg durchgeführt werden und dabei eine dem bisherigen Stand äquivalente Sicherheit bieten. Um die Verbindlichkeit und Vertraulichkeit sämtlicher elektronischer Prozesse mit höchster Sicherheit zu gewährleisten, werden Mechanismen wie Identifikation und Authentisierung, Ver- und Entschlüsselung oder die digitale Signatur mit Hilfe biometrischer Verfahren eindeutig an den einzelnen Nutzer gebunden.

Im ersten Schritt werden 12.500 Arbeitsplätze abgesichert. In Bezug auf Verbindlichkeit und Vertraulichkeit stehen folgende Anforderungen im Mittelpunkt:

- Alle wichtigen Informationen, die über das Justiznetz übertragen oder auf den Rechnersystemen der Justizbehörden gespeichert werden, müssen vor Manipulationen geschützt werden können.
- Bestimmte Informationen (Berichte, Dateien, ...) dürfen nur von autorisierten Personen oder Personengruppen gelesen werden.
- Urheber von Dokumenten sowie Absender von Nachrichten müssen eindeutig identifizierbar sein.
- Bestimmte Kompetenzen dürfen nicht delegiert werden (z.B. Einlieferung, richterliche Entscheidungen über Abhörmaßnahmen, etc.).
- Erfolgreiche Angriffe von Hackern müssen verhindert werden.

4.1 Die Umsetzung

Die benötigten Sicherheitsmechanismen werden in die vorhandene IT-Infrastruktur eingebunden. Um ein dem Verwendungszweck angemessenes Sicherheitsniveau zu erreichen, ist eine Kombination mehrerer Mechanismen erforderlich:

- starke Authentikation mit biometrischen Verfahren
- Dateiverschlüsselung
- E-Mail-Sicherheit durch Verschlüsselung und digitale Signatur
- Public-Key-Infrastruktur (PKI)
- eindeutige Koppelung der digitalen Identität (des Zertifikats) an die 'natürliche' Person; hierzu dienen personengebundene Smartcards mit Fingerabdruckvergleich (biometrische Identitätskontrolle) [Pohl5/02].

Als zentrales Sicherheits-Token dient die persönliche Smartcard. Sie speichert das Zertifikat des jeweiligen Nutzers, seine Passworte für sämtliche Netz-Ressourcen sowie seine persönlichen Schlüssel (Private Keys). Sie wird zur Authentisierung an PCs, Servern und

Host-Systemen, zur Verschlüsselung von Dateien und E-Mails sowie für digitale Signaturen verwendet. Die Sicherheitsinfrastruktur basiert auf einer PKI, in der die Registrierung der Nutzer, die Schlüsselerzeugung, die Ausgabe von Zertifikaten und Smartcards sowie die Bereitstellung von Verzeichnisdiensten und Sperrlisten organisiert sind [Pohl2/02].

4.2 Angriffe auf die Fingerabdruckleser

In der letzten Zeit wurde in der Presse und anderen Medien diskutiert, wie Systeme zur Anmeldung mittels Fingerabdruck teilweise "überlistet" werden können. Bei diesen Angriffen wird versucht, sich über einen nachgemachten Fingerabdruck unerlaubt Zugang zu einem Computersystem zu verschaffen.

Grundsätzlich gibt es zwei Möglichkeiten:

1. Der autorisierte Benutzer stellt seinen Finger für das Anfertigen einer Kopie zur Verfügung.

2. Mit kriminaltechnischen Verfahren wird ein Fingerabdruck ohne das Einverständnis eines autorisierten Benutzers, z.B. von einem benutzten Glas, abgenommen und über mehrere Arbeitsschritte ein Duplikat des Fingerabdrucks erstellt.

Beide Verfahren waren nur deshalb erfolgreich, weil der Zugang zum Computersystem ausschließlich durch das biometrische Verfahren geschützt war. Nicht zuletzt deshalb werden auch in diesem Projekt biometrische Anmeldeverfahren ausschließlich in Kombination mit fälschungssicheren Smartcards verwendet. Damit sind die oben beschriebenen Szenarien wirkungslos, da nur die Kombination von Fingerabdruck und Smartcard den Zugang zu einem Computersystem ermöglicht.

Wer nicht die SmartCard besitzt, kann mit einem gefälschten Fingerabdruck alleine nichts anfangen, da dieser nur dazu verwendet wird, die SmartCard direkt aufzusperren. Die SmartCard vergleicht bei jeder Anmeldung den Fingerabdruck mit einem in der Karte gespeicherten Referenzabdruck.

Deshalb ist in der Sicherheitspolitik (Security Policy) festgelegt, dass beim Verlassen des Arbeitsplatzes der Benutzer die Smartcard mitnehmen muss. Durch die Entfernung der Smartcard wird zudem die Arbeitsstation automatisch gesperrt und ein Angriff mit einem gefälschten Fingerabdruck ist nicht mehr möglich [Pohl9/01].

Die Verwendung biometrischer Verfahren in Kombination mit einer biometriefähigen Smartcard hat weitere Vorteile: Weil der Referenzabdruck des Fingers auf der Karte gespeichert ist, kann auf zentrale und angreifbare Referenz-Datenbanken verzichtet werden.

Im Folgenden werden die PKI-/Smartcard-basierten Dienste Authentikation, E-Mail-Sicherheit und Dateiverschlüsselung vorgestellt.

4.3 Biometriegestützte Authentikation

Die prinzipielle Funktionsweise einer biometriegestützten Authentikation wird durch das folgende Beispiel verdeutlicht:

4.3.1 Sicherer Zugriff auf den Arbeitsplatzrechner

Der Benutzer möchte auf seinen Arbeitsplatzrechner (PC mit Windows) zugreifen. Die Sicherheitssoftware fordert den Benutzer auf, seine Smartcard einzulegen und mit Hilfe seines Fingerabdrucks freizuschalten. Nach erfolgreicher Aktivierung der Smartcard wird damit ein "Advanced Security Log-On" durchgeführt. Anschließend kann der Benutzer die ihm erlaubten Aktionen auf dem PC durchführen.

Das folgende Bild zeigt ein Anwendungsbeispiel für die biometriegestützte Anmeldung eines Benutzers im Netzwerk:

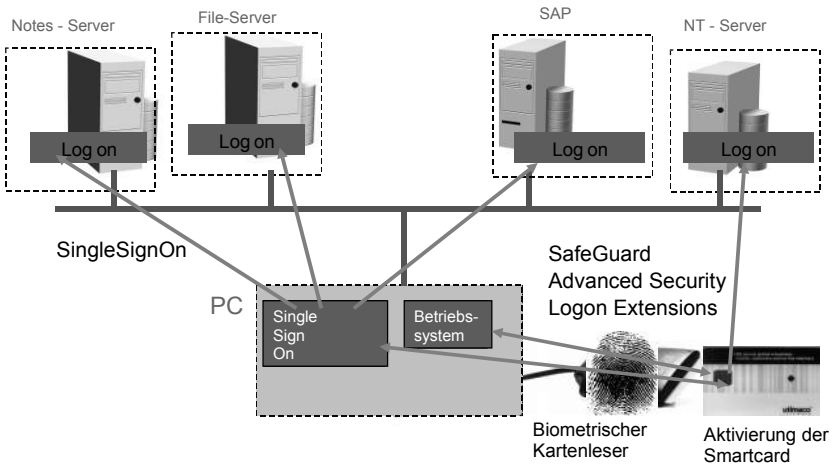

Bild 4: Anmeldung des Benutzers im Netzwerk

Möchte er zum Beispiel auf dem entfernten NT-Server weitere Dienste durchführen, wird zuerst zwischen der Security Software auf dem NT-Server und der SmartCard eine kryptographische Authentisierung durchgeführt.

4.3.2 Sicherer Zugriff auf ein Server-System

Möchte der Nutzer beispielsweise auf einem entfernten NT-Server weitere authentisierungspflichtige Dienste durchführen, wird zuvor zwischen der Security Software auf dem Server und der SmartCard eine kryptographische Authentisierung durchgeführt.

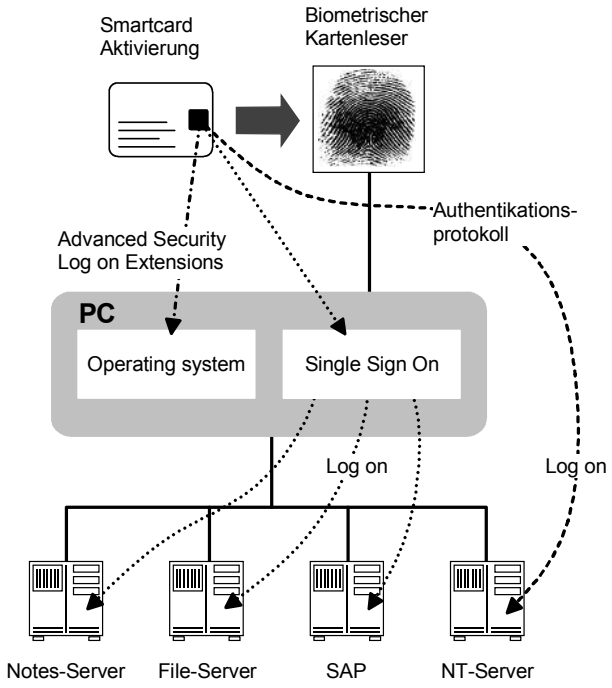

Bild 5: Anmeldung des Benutzers im Netzwerk

4.3.3 SingleSignOn-System

Möchte der Benutzer eine andere Anwendung nutzen, zum Beispiel Lotus Notes oder SAP, organisiert das SingleSignOn-System (SSO) der Sicherheitssoftware auf dem PC den Log-On für den Benutzer. Das SSO erkennt die Aufforderung, ein Passwort einzugeben, entnimmt dieses Passwort der Smartcard und führt für den Benutzer den Log-On aus. Falls die Anwendung einen Passwortwechsel verlangt, wird dieser vom SSO gemäß den Passwortregeln realisiert und das neue Passwort wieder auf der Smartcard gespeichert. Durch dieses Verfahren wird ein Höchstmaß an Benutzerkomfort erreicht.

4.4 Aktivierung der elektronischen Signatur

Zur Erzeugung seiner elektronischen Signatur unter einer E-Mail legt der Nutzer seine Smartcard ein und authentisiert sich per Fingerabdruck. Wenn er sich bereits mit Smartcard und Fingerabdruck eingeloggt hat, kann er die gleiche Smartcard für die Digitale Signatur und Verschlüsselung von E-Mails nutzen. Die dafür benötigten Schlüssel sind ebenfalls auf der Karte gespeichert.

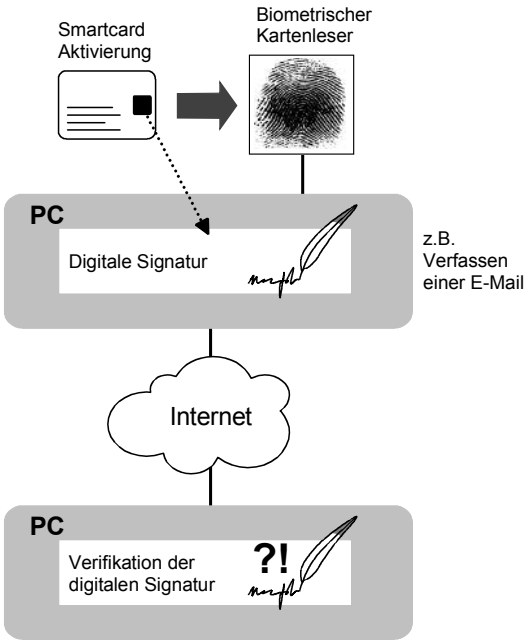

Bild 6: Aktivierung der elektronischen Signatur

4.5 Aktivierung der Dateiverschlüsselung für Benutzergruppen

Dateiverschlüsselung sorgt in einem Unternehmensnetz dafür, dass berechtigte Mitarbeiter bestimmter Nutzergruppen Dokumente über das Netzwerk austauschen bzw. im Netzwerk ablegen können, ohne dass diese von Unbefugten gelesen oder bearbeitet werden könnten. Die Benutzergruppen werden so eingerichtet, dass nur bestimmte Benutzer eine Zugangsberechtigung und damit einen Schlüssel für die sensiblen Dokumente besitzen.

Auch hier ist die Authentisierung mit Smartcard und Fingerabdruck der sicherste und einfachste Weg für die Benutzer. Um Zugriff auf die Daten zu bekommen, wird das Dateiverschlüsselungssystem auf dem PC durch den Fingerabdruck aktiviert. Dieses System verwendet den auf der Smartcard gespeicherten Schlüssel, um die Daten zu entschlüsseln. Für die befugten Nutzer läuft dieser Vorgang transparent, d.h. ohne ihr Zutun ab. Für alle anderen bleiben die Daten unlesbar, weil sie nicht über den Schlüssel verfügen. Die Daten

werden in verschlüsselter Form vom Fileserver über das Netzwerk auf den Computer des Anwenders übertragen und erst dort entschlüsselt.

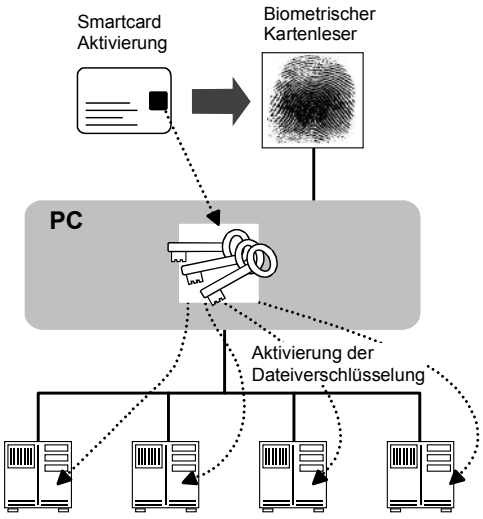

Bild 7: Aktivierung der File-Verschlüsselung

5 Erfahrungen einer Anwendung

Durch das biometriebasierte Sicherheitssystem ergeben sich für die niederländischen Justizbehörden folgende Vorteile:

Wichtige Informationen im behördeneigenen Computernetzwerk (E-Mails, Daten auf PCs und Servern) bleiben vertraulich und können nur von berechtigten Personen gelesen oder bearbeitet werden. Außerdem ist die Verbindlichkeit der auf elektronischem Weg durchgeführten Verwaltungsakte gewährleistet. Bei dieser Lösung lassen sich Verwaltungsstrukturen exakt abbilden, Kompetenzen und Rechte der Benutzer können klar zugeordnet werden. Mittels biometrischer Identifikation und Authentisierung sind Sicherheitsmechanismen wie Dateiverschlüsselung, E-Mail-Sicherheit und elektronische Signatur für jeden Nutzer verfügbar. Somit dient die Smartcard mit digitaler Signatur für die Nutzer als 'Ausweis für die elektronische Welt'. Sie brauchen sich keine Passworte zu merken – ihr Fingerabdruck genügt.

Die Wahrung des Datenschutzes ist im Zusammenhang mit dem Einsatz biometrischer Funktionen von besonderer Bedeutung. Die personenbezogenen biometrischen Daten sind sicher auf der Smartcard gespeichert, es gibt keine zentrale Speicherung. Die Anforderungen des Datenschutzes bleiben dadurch gewahrt.

Für den Einsatz von Sicherheitsmechanismen in der Praxis sind die Komplexität der Lösungen in Bezug auf die Integration in die bestehenden Strukturen und der Bedienkomfort für den Anwender von entscheidender Bedeutung. Die hier vorgestellten Sicherheitsfunktionen lassen sich leicht in bestehende Abläufe integrieren und können von den Benutzern einfach und komfortabel genutzt werden. Die Nutzerakzeptanz ist

entsprechend hoch. Darüber hinaus ist der Schulungs- und Administrationsaufwand vergleichsweise gering, Einsätze des Helpdesk wegen vergessener Passworte entfallen. Dadurch bleiben die Betriebskosten gering.

Als 'Nachteil' des biometriegestützten Sicherheitssystems muss dagegen in Kauf genommen werden, dass personengebundene Prozesse nicht mehr an andere Mitarbeiter delegiert werden können.

6 Fazit

Viele Organisationen und Unternehmen wollen eine höhere Sicherheit für die neuen Geschäftsprozesse. Das Einleiten von Aktionen mit schwerwiegenden Konsequenzen muss eindeutig und beweisbar sein, damit auch kritische Geschäftsprozesse abgewickelt werden können. Eine sichere und beherrschbare Informationstechnik muss realisiert werden.

Benutzerkomfort und Bequemlichkeit in Verbindung mit wirksamen Sicherheitsfunktionen sind wesentliche Erfolgsfaktoren für die Anwendung von Sicherheitsmechanismen. Mit biometrischen Verfahren kann man nicht nur die Bequemlichkeit und den Komfort erhöhen, sondern gleichzeitig ein wesentlich höheres Maß an benutzergebundener Sicherheit erreichen. Die Nachteile und Risiken der Verwendung von Passworten müssen nicht mehr in Kauf genommen werden; sie können mit Hilfe von SingleSignOn-Verfahren einfach umgangen werden. Die Nutzung von Biometrie anstelle eines Passworts oder einer PIN vereinfacht den Prozess für den Nutzer noch weiter und erhöht damit den Sicherheitslevel von E-Government- und E-Business-Implementierung weiter.

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

Literatur

[Pohl3/01] N. Pohlmann: ”Aktivierung von Smartcards durch Biometrie", KES - Kommunikations- und EDV-Sicherheit, SecMedia Verlag, 3/2001

[Pohl9/01] N. Pohlmann: "Trusted IT-Infrastructures: Not only a Technical Approch", DuD Datenschutz und Datensicherheit - Recht und Sicherheit in Informationsverarbeitung und Kommunikation, Vieweg Verlag, 09/2001

[Pohl2/02] N. Pohlmann: „Nutzen und Chancen von Public-Key-Infrastrukturen", in "Sicherheitsinfrastrukturen in Wirtschaft und Verwaltung", Hrsg.: Patrick Horster, IT Verlag, 2002

[Pohl5/02] N. Pohlmann: „Weil der Fingerabdruck einmalig ist“, Die Sparkassenzeitung – Nachrichten für die Sparkassen – Finanzgruppe, Deutscher Sparkassenverlag, 24.05.02