Biometrie

Bessere Identifizierung, sichere Authentisierung

Dr. Norbert Pohlmann

Vorstandsmitglied der Utimaco Safeware AG

Kontakt: Dr. Norbert Pohlmann
Fon: + 49 (0) 241 / 1696 150
Fax: + 49 (0) 241 / 1696 199
E-Mail norbert.pohlmann@utimaco.de

Inhaltsverzeichnis

1. Einleitung 2
2. Identifizierung und Authentisierung 3
3. Passwortverfahren 3
4. SmartCard 4
5. Biometrische Verfahren 6
5.1. Was ist Biometrie ? 6
5.2. Eigenschaften des verwendeten biometrischen Merkmals 6
5.3. Benutzerakzeptanz 7
5.4. Vergleich der verschiedenen Verfahren 8
6. Verfahren der Fingerabdruck 8
7. SmartCard Anwendungen im e-Business 11
7.1. Biometriegestützte Anmeldung eines Benutzers im Netzwerk 11
7.2. Aktivierung der elektronischen Signatur 12
7.3. Authentisierung von Virtual Private Networks (VPN) 13
7.4. Aktivierung der Dateiverschlüsselung für Benutzergruppen 14
7.5. Integration in SAP 15
8. Vorteile bei der Verwendung von SmartCards, die mit Fingerabdruck aktiviert werden 16
9. Zusammenfassung 17
10. Literatur 17
11. Autor 18

1. Einleitung

Die meisten Geschäftsprozesse wurden in der Vergangenheit schriftlich auf Papier mit Hilfe der Post oder persönlich abgewickelt. Solche Abläufe werden heute durch eine gemeinsame globale IT-Infrastruktur, das Internet, weitaus rationeller gestaltet.

Die elektronischen Informationen und Daten können direkt und ohne Medienbruch in die Businessprozesse einbezogen werden. Dieser Trend des Reengineerings der Geschäftsprozesse in allen Bereichen geht einher mit der Internationalisierung und Globalisierung. Das bedeutet auch eine immense Zeit- und Kostenersparnis.

Sowohl für die „Old Economy“ als auch für die „New Economy“ ist es wichtig festzustellen, welche neuen Gefahren darin liegen. Wenn man die Gefahren kennt, kann man einschätzen, welche Angriffe relevant sind und welche vernachlässigt werden können, um sicher in die Zukunft zu gehen.

Mit Hilfe von geeigneten Sicherheitsmaßnahmen ist die globale Informationsgesellschaft in der Lage, die eigene Verwundbarkeit durch Angriffe zu reduzieren. Die verwendeten

Sicherheitsmechanismen müssen aber auch einfach und bequem genutzt werden können, damit sie eine breite Akzeptanz finden.

2. Identifizierung und Authentisierung

Die Nutzung der innovativen Geschäftsprozesse ist in vieler Hinsicht attraktiv. Ein gravierende Bedrohung ist die Sicherheitsfrage. Damit der Benutzer die IT-Dienstleistungen sicher nutzen kann, muss eine Vielzahl an Sicherheitsmechanismen bereit gestellt werden. Einer der Hauptaspekte ist dabei die Identifikation und Authentisierung der Nutzer.

Identifikation und Authentisierung

Woher weiß ein Internet-Dienstleister, zum Beispiel eine Bank, dass der Kunde A, der eine Kommunikationsbeziehung aufbauen möchte, tatsächlich Kunde A ist?

Zum Aufbau einer Kommunikationsverbindung muss er sich gegenüber dem Partner identifizieren und authentisieren.

Die **Identifikation** ist die Überprüfung eines vorgelegten, kennzeichnenden Merkmals, zum Beispiel des Benutzernamens. Eine Person wird eindeutig durch die Angabe von Vorname, Nachname, Geburtsort und Geburtstag identifiziert. In den meisten Ländern wird die Eindeutigkeit der Identifikation von den Standesämtern garantiert.

Eine Identifikation muss innerhalb eines Systems (Organisation) abgesprochen sein, damit sie eindeutig ist. Damit eine solche Absprache mit verschiedenen Benutzern zustande kommt, müssen klar definierte Regeln eingehalten werden.

Ein Beispiel für ein Konzept eindeutiger, kennzeichnender Namen oder „distinguishing identifier“ sind die “directory names“ aus der CCITT “Recommendation“ X.509 beziehungsweise ISO 9594-8 /CCITT/.

Authentisierung bezeichnet einen Prozess, in dem überprüft wird, ob „jemand“ oder „etwas“ echt oder berechtigt ist. Authentisierung bedeutet die Verifizierung (Überprüfung) der Echtheit beziehungsweise der Identität. Die Überprüfung des Personalausweises einer Person ist eine solche Authentisierung.

Authentisierungsverfahren

Für die Authentisierung von Benutzern sind unterschiedliche Authentisierungsverfahren möglich: Einfache Passwortverfahren, Einmal-Passwort und Challenge-Response-Verfahren, aber auch kryptographische Verfahren , die mit der Hilfe von SmartCards arbeiten.

3. Passwortverfahren

Das einfachste Authentisierungsverfahren ist das Passwort-Verfahren. Es wirft eine Vielzahl von Problemen auf:

- Falls das Passwort im Klartext über das Internet übertragen wird, kann es von einem Angreifer mitgelesen werden.
- Außerdem hängt die Sicherheit bei Passwort-Verfahren von der Qualität des Passwortes ab. Die Umsetzung der notwendigen Passwortregeln (Nicht notieren, Mindestlänge von x-Stellen, keine Trivialpassworte, in angemessenen Zeitabständen ändern, ...) werden von den meisten Unternehmen beziehungsweise den Usern nicht eingehalten.

- Ein weiteres Problem mit Passworten tritt dann auf, wenn die Benutzer sich viele Passworte für die unterschiedlichen Anwendungen (Windows2000, LotusNotes, SAP usw.) merken müssen.

Hohe Kosten durch vergessene Passworte

In verschiedenen Studien (zum Beispiel Morgan Keegan&Co., Gartner Group) wird aufgezeigt, dass zwischen 30 und 40 Prozent aller Helpdesk Calls in einer Organisation durch vergessene Passworte anfallen und die Kosten pro User in der Regel zwischen US$ 100-200 im Jahr liegen.

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. Daher muss ein Sicherheitssystem eingesetzt werden, dass die höchsten Sicherheitsanforderungen erfüllt und gleichzeitig so bequem zu handhaben ist, dass die Benutzer es auch immer verwenden und dabei die Vorschriften der Sicherheitspolitik einhalten.

4. SmartCard

Weitaus sicherer und komfortabler für die Benutzer ist die Authentisierung mit der SmartCard. Auf der SmartCard können alle Schlüssel gespeichert werden, die ein Benutzer für die verschiedenen Anwendungen braucht. Auf der SmartCard ist genügend Platz für alle Informationen. Technisch ist es möglich, Personen mit einer SmartCard für sämtliche Anwendungen auszustatten.

Eine „intelligente SmartCard“ ist ein Rechnersystem in der genormten Größe einer Kreditkarte (86 x 54 x 0,76 mm), das dem Benutzer verschiedene Sicherheitsdienstleistungen zur Verfügung stellt.

Eine SmartCard enthält:

- eine CPU
- RAM- und ROM-Speicher
- ein „schlankes“ Betriebssystem im ROM
- eine I/O-Schnittstelle, über die die gesamte Kommunikation stattfindet (Kontaktflächen oder kontaktloses Interface)
- ein EEPROM, auf dem die geheimen Schlüssel - zum Beispiel ein privater RSA-Schlüssel oder andere symmetrische Schlüssel - sowie persönliche Daten (Passworte etc.) sicher gespeichert sind
- sonstiges, beispielsweise einen Co-Prozessor, der symmetrische oder asymmetrische Verschlüsselung sehr schnell durchführt (Krypto-Prozessor)

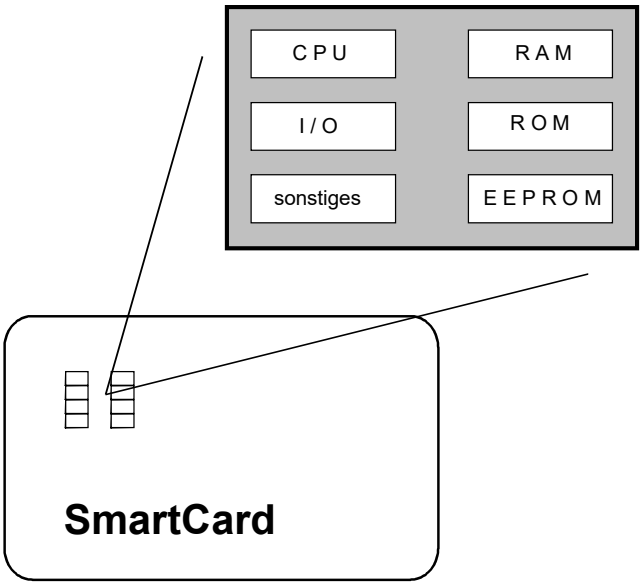

Bild 1: Intelligente SmartCard

Dieses „smarte Rechnersystem“ stellt dem Benutzer in der Regel folgende Sicherheitsdienstleistungen zur Verfügung :

- Identifikation/Authentisierung des Benutzers (Aktivieren der SmartCard)
- SingleSignOn-Anwendungen (zum Beispiel Passwort und PIN von unterschiedlichen Anwendungen werden auf einer SmartCard gespeichert)
- Sicheres Speichern von Daten auf der SmartCard
- Lesen gespeicherter Servicedaten
- Kryptographische Anwendungen wie Digitale Signaturen usw.
- Laden und Entladen von Werteinheiten für elektronisches Bezahlen
- Ausführen sonstiger Rechenoperationen

Warum brauchen wir SmartCards ?

Eine SmartCard kann alle oben aufgeführten Dienstleistungen bereit stellen. Der Vorteil für den Benutzer liegt auf der Hand: Er kann alle Operationen mit einem einzigen Multi-Device – der SmartCard – ausführen, beispielsweise die Speicherung eines 1024 Bit langen RSA-Schlüssels oder die Berechnung des RSA-Verfahrens.

Die SmartCard ist für den User somit Tresor und Rechnersystem in einem.

Aktivierung der SmartCard

Grundsätzlich existieren zwei Verfahren zur Aktivierung der SmartCard und ihrer Sicherheitsfunktionen:

- Passwort und
- Biometrie

Die weitverbreitetste Aktivierungsart ist der Passwortschutz.

Falls ein Benutzer des Systems Sicherheitsfunktionen in Anspruch nehmen will, muss er seine SmartCard mit Hilfe seines persönlichen Passwortes aktivieren. Verliert der Benutzer seine SmartCard, kann ein Finder diese nicht verwenden, da er das Passwort nicht kennt. Kennt jemand das individuelle Passwort eines anderen Benutzers, kann er keinen Nutzen daraus ziehen, wenn er nicht auch die SmartCard besitzt. Außerdem kann ein Benutzer sein Passwort jederzeit ändern.

Sicherer als ein Passwort sind biometrische Identifikationsverfahren, die Körpermerkmale – zum Beispiel einen Fingerabdruck, die Stimme oder Gesichtszüge – zur eindeutigen Identifikation von Personen nutzen. Im Gegensatz zu einem Passwort kann ein solches Merkmal nicht gestohlen, verloren, vergessen oder weitergegeben werden.

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.

5. Biometrische Verfahren

5.1. Was ist Biometrie ?

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.

5.2. 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.

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.

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.

5.3. 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.

5.4. Vergleich der verschiedenen 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.

6. Verfahren der Fingerabdruckmessung

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.

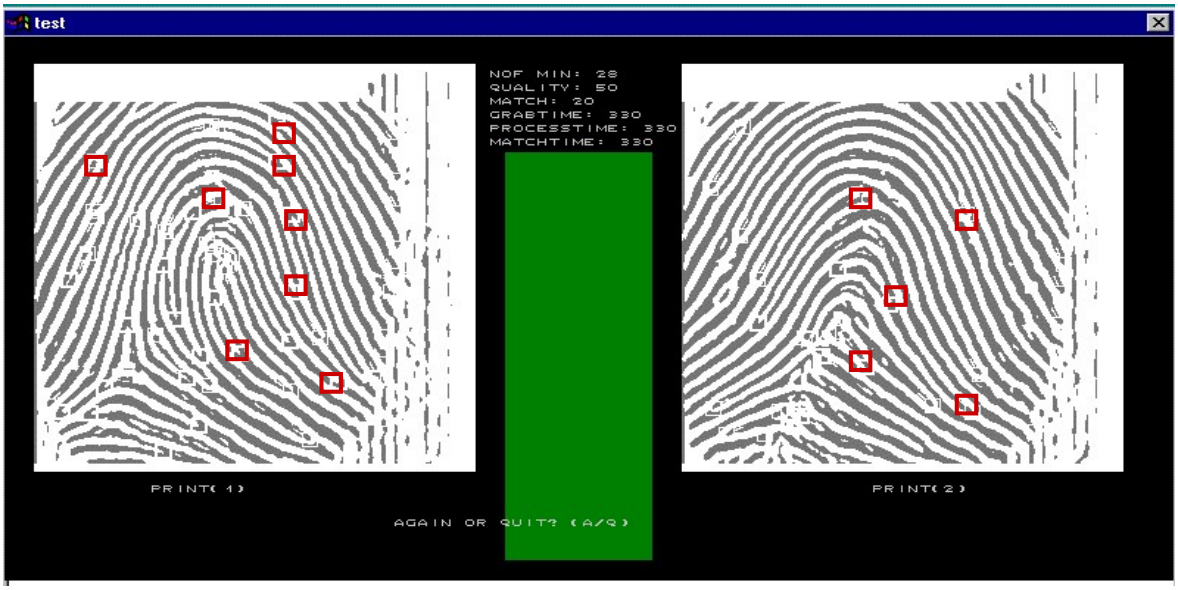

Bild 2: Übereinstimmung der Ausschnitte bei unterschiedlichen Abdrücken

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 (Precise 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 Precise Pattern Matching ist optimal für kleine Leseeinheiten und daher sehr geeignet für Applikationen wie das tägliche mehrmalige Einloggen in den Arbeitsrechner.

Bild 3: Precise 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, 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.

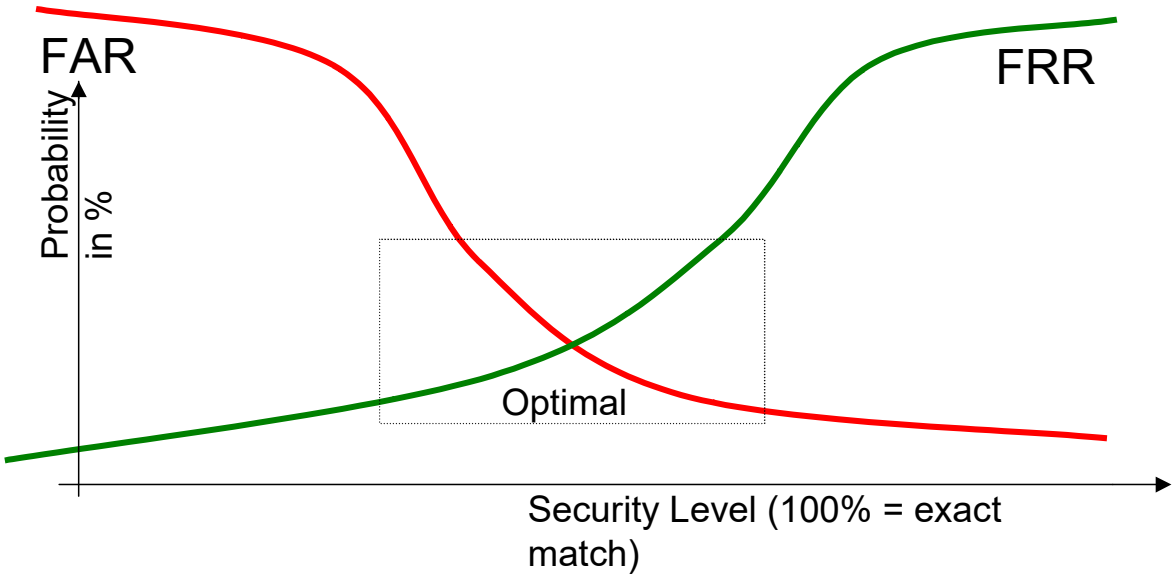

Bild 4: Wahrscheinlichkeit der Falschakzeptanz und Falschrückweisung

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.

7. SmartCard Anwendungen im e-Business

Mit Hilfe der SmartCard kann mehr Vertrauenswürdigkeit in die elektronischen Geschäftsprozesse integriert werden. Die SmartCard arbeitet mit einem RSA-Schlüssel (1024 Bit) und enthält die Fingerabdruckprüfung (Fingerprint). Zur Sicherheit sind immer vier Fingerabdrücke auf der SmartCard abgebildet. Wenn der Benutzer zum Beispiel eine Verletzung am Zeigefinger hat, wählt er einen der drei anderen Finger.

Ein PKI-System stellt SmartCards und Zertifikate im kundeneigenen oder einem öffentlichen Trustcenter bereit.

7.1. Biometriegestützte Anmeldung eines Benutzers im Netzwerk

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

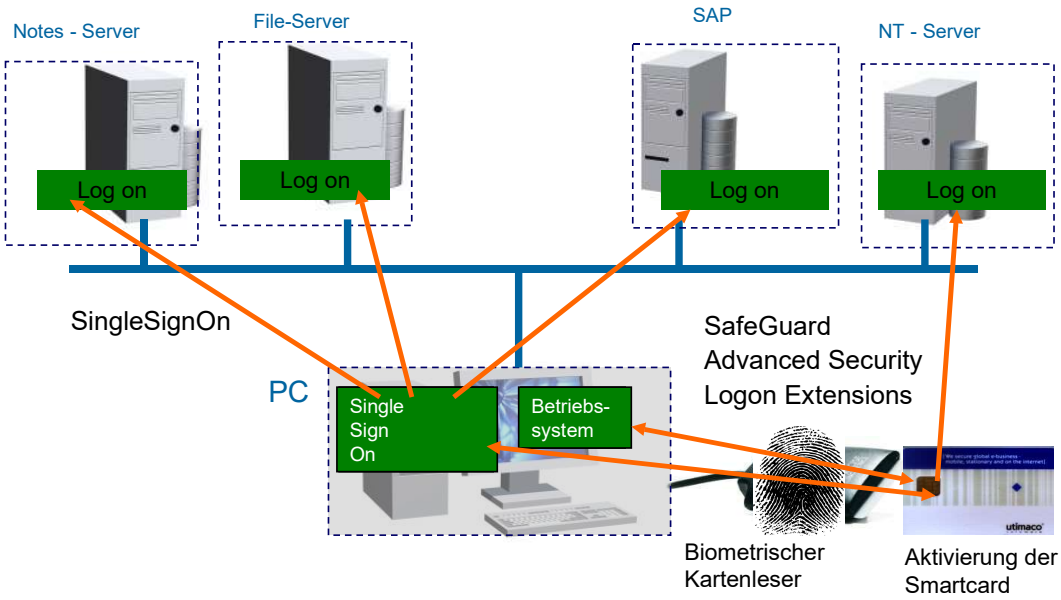

Bild 5: Anmeldung des Benutzers im Netzwerk

Der Benutzer möchte auf seinen Arbeitsplatzrechner zugreifen. Auf dem PC mit Windows NT oder Windows2000 ist eine entsprechende Sicherheitssoftware installiert, die den Benutzer auffordert, seine SmartCard einzulegen und mit Hilfe seines Passwortes oder seines Fingerabdruckes die SmartCard zu aktivieren. Nach erfolgreicher Aktivierung der SmartCard findet ein „Advanced Security Logon" mit der SmartCard statt. Anschließend kann der Benutzer die ihm erlaubten Aktionen auf dem PC durchführen. 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.

7.2. Aktivierung der elektronischen Signatur

Möchte der Benutzer eine andere Anwendung nutzen, zum Beispiel Lotus Notes oder SAP, organisiert das SingleSignOn-System (SSO) der Sicherheitssoftware auf dem PC den Logon für den Benutzer. Das SSO erkennt die Aufforderung, ein Passwort einzugeben, nimmt dieses Passwort aus der SmartCard und führt für den Benutzer das Logon aus. Falls die Anwendung einen Passwortwechsel verlangt, wird dieser von SSO nach den Passwortregeln realisiert und das neue Passwort wieder auf die SmartCard gespeichert. Dieses Verfahren stellt für den Benutzer ein Höchstmaß an Benutzerkomfort da.

Die gleiche SmartCard wird auch für die Digitale Signatur und Verschlüsselung von E-Mails, die Authentisierung eines VPN-Systems und für eine File-Verschlüsselung verwendet. Die SmartCard wird von der eigenen oder einer fremden PKI ausgestellt.

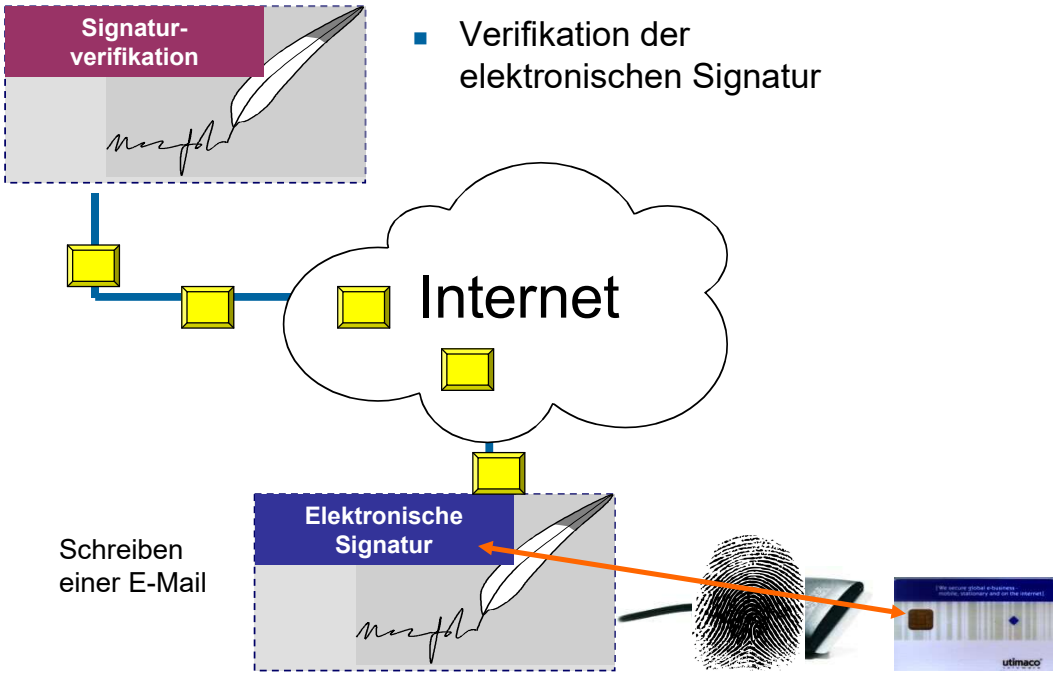

Bild 6: Aktivierung der elektronischen Signatur

Zur Erzeugung seiner elektronischen Signatur unter einer E-Mail legt der Nutzer seine SmartCard ein und authentisiert sich per Fingerabdruck. Wenn er bereits mit SmartCard und Fingerprint eingeloggt ist, kann er die gleiche SmartCard für die Digitale Signatur und Verschlüsselung von E-Mails nutzen. Auf der SmartCard sind auch die Schlüssel für seine Digitale Signatur und Objektverschlüsselung gespeichert.

7.3. Authentisierung von Virtual Private Networks (VPN)

In einem Virtual Private Network läuft die Kommunikation zwischen Servern und Clients verschlüsselt ab. Der berechtigte Nutzer kann sich mit seiner SmartCard und dem Fingerprint bequem ins VPN einloggen, alle angebotenen Dienste sicher nutzen und verschlüsselt mit den anderen Mitgliedern des Systems kommunizieren.

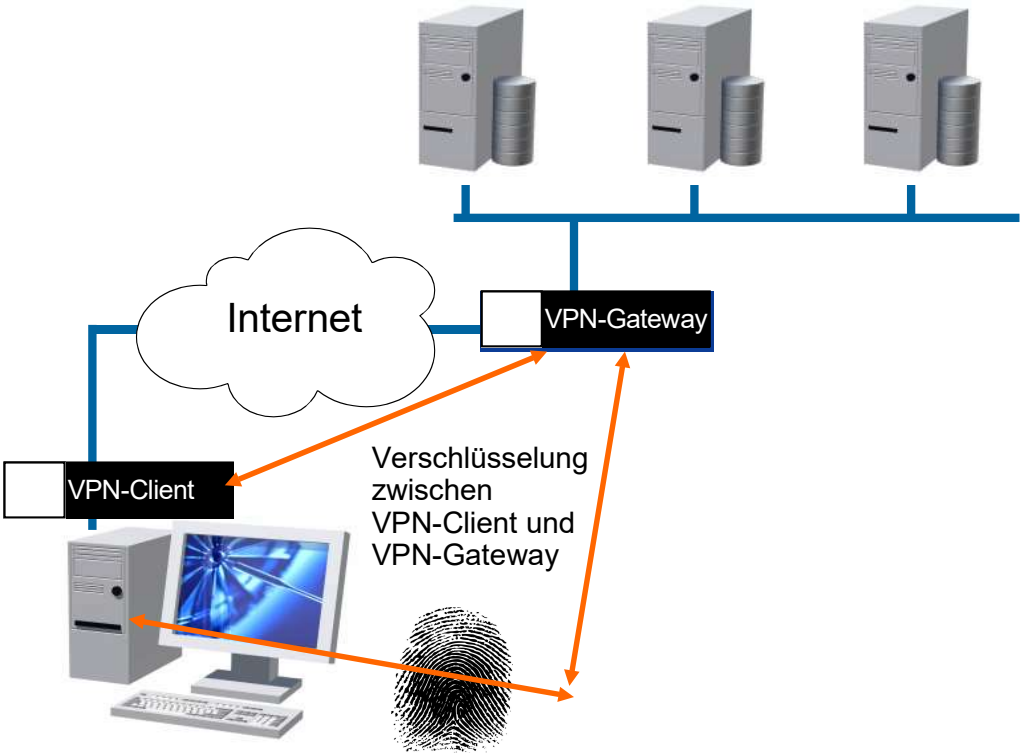

Bild 7: Authentisierung von Virtual Private Networks

Der Benutzer arbeitet zum Beispiel von seinem Heimarbeitsplatz aus. Über das Internet ist er an die Serversysteme seines Unternehmens angeschlossen und will neue Informationen bekommen oder Daten ablegen. Auf Serverseite ist ein VPN Gateway eingerichtet, das parallel hochperformant die IPsec Verschlüsselung durchführt, und auf dem Heimarbeitsrechner ist ein VPN Client. Als erstes muss der Benutzer mit seinem Fingerabdruck die SmartCard aktivieren und die SmartCard führt dann zertifikatsbasiert die starke Authentisierung mit dem VPN Gateway durch.

Und nur wenn diese starke Authentisierung erfolgreich durchgeführt wird, kann die eigentliche Kommunikation durchgeführt werden, die dann zwischen dem VPN Gateway und dem VPN Client realisiert wird

7.4. Aktivierung der Dateiverschlüsselung für Benutzergruppen

Eine Dateiverschlüsselung sorgt in einem Unternehmensnetz dafür, dass berechtigte Mitarbeiter bestimmter Nutzergruppen auf dem Netz Dokumente austauschen beziehungsweise ablegen können, ohne dass diese von unberechtigten Mitarbeitern gelesen oder bearbeitet werden könnten. Alle Dokumente werden nur verschlüsselt auf den Servern abgelegt und können von Unberechtigten nicht geöffnet werden, da diese den Schlüssel nicht besitzen. Die Benutzergruppen werden so eingerichtet, dass nur bestimmte Benutzer eine Zugangsberechtigung und damit einen Schlüssel für die sensiblen Dokumente besitzen.

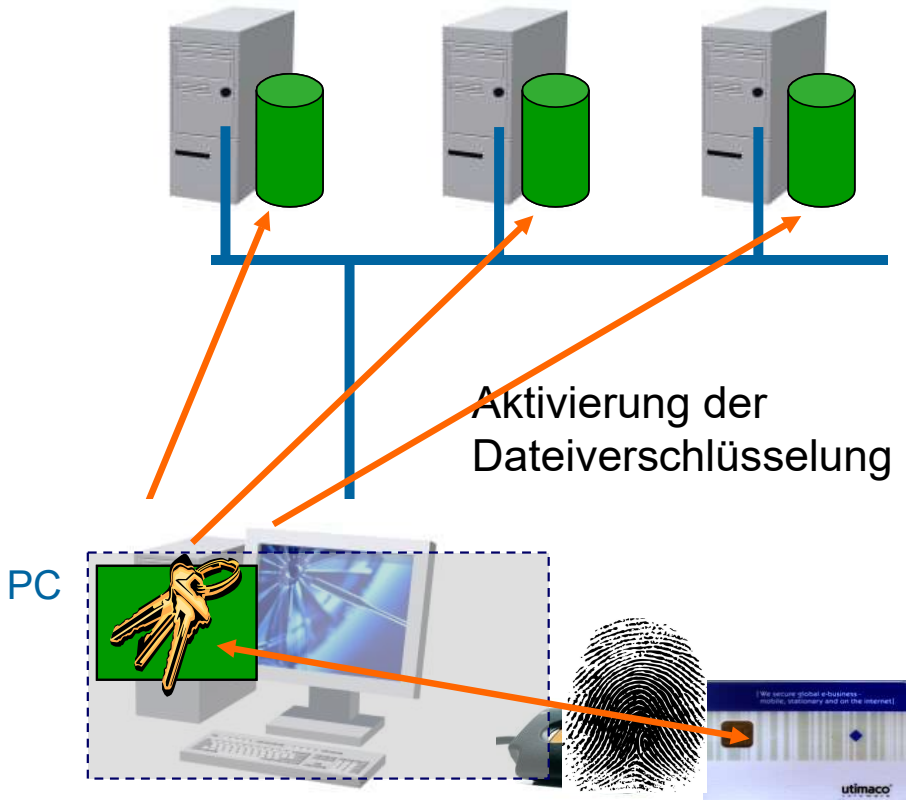

Bild 8: Aktivierung der File-Verschlüsselung

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 ihr File-Verschlüsselungssystem auf dem PC durch den Fingerabdruck aktiviert. Von der SmartCard wird der Schlüssel genommen und dem File-Verschlüsselungssystem zur Verfügung gestellt und dann können die Benutzer transparent die Daten auf den Fileservern im Klartext lesen. Für alle anderen bleiben diese verschlüsselt, weil sie nicht über den Schlüssel verfügen. Auch die Daten werden verschlüsselt von den Fileservern über das lokale oder andere Netze auf den eigenen Computer gespielt und erst auf dem Rechner entschlüsselt.

7.5. Integration in SAP

Digitale Signaturen und Verschlüsselung ermöglichen es, dass auch sicherheitskritische Produktions- und Geschäftsprozesse elektronisch abgebildet werden können. Dazu gehören beispielsweise Freigaben, Genehmigungen und Abnahmen im Qualitätsmanagement, die im Rahmen der Produkthaftung brisant werden können. Hier bietet die Digitale Signatur eines elektronischen Dokumentes ein rechtsverbindliches Äquivalent zur handschriftlichen Unterschrift auf Papier.

Digitale Signaturen und Verschlüsselung ermöglichen es, zukünftig betriebswirtschaftliche Internetsoftware auch verstärkt zur Vernetzung von Geschäftspartnern zu nutzen. Kunden, Lieferanten und externe Dienstleister können auf dieser Grundlage sicher an das Firmennetz angebunden werden, um Geschäftsprozesse zu optimieren. Die verstärkte Nachfrage nach Sicherheitserweiterungen bei Unternehmen, die den Einsatz von betriebswirtschaftlicher Internetsoftware im Rahmen von E-Business erweitern wollen verlangt eine Integration der Sicherheitsfunktionalitäten in verbreitete Applikationen wie SAP.

Daten und Dokumente können direkt aus mySAP.com-Applikationen, die die BC-SSF-Schnittstelle von SAP unterstützen, digital signiert und verschlüsselt werden. Die Sicherheitsapplikation verwendet standardisierte X.509v3-Zertifikate und bietet somit die Basis für eine zukünftige Einbindung in interoperable Public Key-Infrastrukturen (PKI). Optional können SmartCards zur Erhöhung der Sicherung beim Key Management genutzt werden.

Das Sicherheitssystem wird über die SAP SSF-Schnittstelle (Secure Store & Forward Mechanism) nahtlos mit der jeweiligen mySAP.com-Applikation verzahnt. Die verschlüsselten und signierten Daten können nicht nur innerhalb von SAP verwendet werden, sondern lassen sich auch auf beliebigen Datenträgern (tapes/disks/server) speichern und mit beliebigen Kommunikationsdiensten (zum Beispiel E-Mail, EDI, HTTP, FTP) gesichert übertragen.

Die Sicherheitseinstellungen (Security Policy) werden in der SAP-Administration zentral festgelegt. Verschlüsselungen und Digitale Signaturen lassen sich somit in Arbeitsprozesse integrieren und unternehmensweit durchsetzen. Die Akzeptanz der Sicherheitsfunktionen bei den Benutzern ist durch die Zeit und Kostenersparnis, die die biometrische Authentisierung bietet, sehr hoch.

In großen Unternehmen und Institutionen wie Krankenhäusern, in denen schichtweise verschiedene Personen am gleichen PC arbeiten, ist das sichere Desktop-Switching eine große Arbeitserleichterung. Die Mitarbeiter authentisieren sich sekundenschnell mit SmartCard und Fingerprint und haben Zugriff auf die Daten und Dienste, zu denen sie berechtigt sind. Das SingleSignOn-Prinzip bewirkt, dass keine Wartezeiten durch erneute Passworteingabe für weitere Dienste entstehen. Sobald der Benutzer sich eingeloggt hat, steht ihm sein persönliches Desktop mit seiner zuletzt genutzten Applikation zur Verfügung.

8. Vorteile bei der Verwendung von SmartCards, die mit Fingerabdruck aktiviert werden

Welchen Nutzen hat die Integration von biometrischen Verfahren ?

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.

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.

9. 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 Biometrieleser 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.

10. Literatur

/CCITT/ CCITT: „The Directory – Authentication Framework“, Draft Recommendation X.509.- Gloucester: 11 (1987).

/Chau87/ D. Chaum:
„Security without Identification: Transaction Systems to Make Big Brother Obsolete“.- Comm. ACM 28, 10 (1985), S. 1030–1044.

Deutsche Übersetzung in: „Sicherheit ohne Identifizierung“.- Informatik-Spektrum 10 (1987), S. 262–277.

/Pohl01/ Norbert Pohlmann: „Firewall Systeme – Sicherheit für Internet und Intranet; E-Mail-Security, Virtual Private Networks; Intrusion Detection-Systeme, Personal Firewall“. 4. aktualisierte und erweiterte Auflage.- Bonn:MITP-Verlag 2001.

11. Autor

Dr. Norbert Pohlmann

Mitglied des Vorstandes der Utimaco Safeware AG

Vorstandsvorsitzender des TeleTrusT e.V.

Vorsitzender des Programm Komitees der ISSE 2000

Zahlreiche Publikationen, Vorträge und Seminare zu Themen der IT-Sicherheit dokumentieren seine Erfahrung und Kompetenz auf diesem Gebiet.