[VHSt02] *Claus Vielhauer, Michael Haisch, Ralf Steinmetz;* **Schlüsselmanagement in biometrischen Systemen - Sicherung von Referenzdaten auf mobilen Computern am Beispiel der Handschriftverifikation;** Enterprise Security, Klagenfurt, März 2002, S. 284 - 295.

Schlüsselmanagement in biometrischen Systemen

Sicherung von Referenzdaten auf mobilen Computern am Beispiel der Handschriftverifikation

Claus Vielhauer[1,2] · Michael Haisch[1] · Ralf Steinmetz[1]

[1] Technische Universität Darmstadt
{claus.vielhauer | ralf.steinmetz} @kom.tu-darmstadt.de

[2] Platanista GmbH
claus.vielhauer@platanista.com

Zusammenfassung

Mobile Endgeräte spielen in der Unternehmenskommunikation eine immer wichtigere Rolle und sind nicht mehr nur isoliert einem Benutzer zugeordnet, sondern sind Bestandteil einer offenen verteilten Umgebung. Dies führt zu einer Vielzahl von Sicherheitsbedrohungen, denen mobile Endgeräte und damit Ihre Nutzer und ganze Unternehmen ausgesetzt sind. Die Möglichkeit einer gesicherten Benutzerauthentifizierung und des Zugiffschutzes sind neben Datenauthentizität und –integrität sowie Verfügbarkeit wichtige Sicherheitsaspekte. In unserem Beitrag beschäftigen wir uns mit biometrischen Authentifizierungsmöglichkeiten. Ein Problem bei biometrischen Authentifizierungssystemen ist die Absicherung der biometrischen Referenzdaten auf dem mobilen Endgerät selbst oder die gesicherte Übertragung bei einer serverbasierten Authentifizierung. Wir diskutieren den Schutzbedarf und zeigen generelle Absicherungsmethoden für gespeicherte und zu übertragende biometrische Merkmale auf. Darüber hinaus entwickeln wir für handschriftliche Merkmale ein Konzept zur Schlüsselerzeugung, um die Referenzdaten lokal auf einem PDA verschlüsselt zu hinterlegen. Die Schlüsselerzeugung ist dabei gleichzeitig ein biometrisches Authentifizierungssystem, basierend auf 24 ausgewählten handschriftlichen Merkmalen. Tests zeigen, daß das Vorgehen weitgehend gegen zufällige und gezielte Angriffe von Unbefugten fälschungssicher ist. Weiterhin stellen wir ein Konzept zur Übertragung von biometrischen Merkmalen bei einer serverbasierten biometrischen Authentifizierung vor. Abschließend diskutieren wir das erreichte Sicherheitsniveau und den weiteren Forschungsbedarf.

1 Motivation

Mobile persönliche Endgeräte wie PDAs, Organizer oder Handys sind bereits heute ein wichtiger Bestandteil mobiler und verteilter Unternehmensinfrastrukturen. Über lokale Funknetze, über Satelliten-Netzwerke, Telefonnetze oder über stationäre LANs und WANs können derartige Geräte mit anderen Komponenten einer verteilten Umgebung kommunizieren. Durch den technologischen Fortschritt verbessern sich die Fähigkeiten mobiler Endgeräte in einem rasan-

ten Tempo. Daher können sie in zunehmendem Maße für mobiles und ubiquitäres Computing eingesetzt werden. Entwicklungen, wie das Wireless Application Protocol – kurz WAP – ermöglichen den Zugriff auf Internet-Dienste auch bereits für sehr kleine mobile Endgeräte. Dies alles hat zur Konsequenz, dass mobile Endgeräte in zunehmendem Maße auch im Bereich des E-Commerce, des M-Commerce, des Homebanking über das Internet und auch des E-Business eingesetzt werden. Das bedeutet, dass die beteiligten mobilen Endgeräte nicht mehr nur isoliert einem Benutzer zugeordnet sind, sondern Bestandteil einer offenen verteilten Umgebung sind. Dies führt zu einer Vielzahl von Sicherheitsbedrohungen, denen mobile Endgeräte und damit Ihre Nutzer ausgesetzt sind [Hors01]. Daher gewinnt die Möglichkeit einer gesicherten Authentifizierung gerade auch bei der Nutzung von mobilen Endgeräten eine immer größere Bedeutung. Als Zugangskennung werden hier oft immer noch einfache Zahlenkombinationen oder Passwörter, welche eine Kombination aus Zahlen, Buchstaben und Sonderzeichen darstellen. Beide sind meist wenig einprägsam. Dies führt dazu, dass die Kennwörter vom Benutzer oftmals an einem scheinbar sicheren Ort aufgeschrieben werden oder dass Namen von Verwandten, Geburtsdaten und Kontonummern verwendet werden. Diese Vorgehensweise senkt die Sicherheit beträchtlich. Die Verwendung von digitalen Signaturen erweist sich auch oft als nicht sehr anwenderfreundlich, da sich hier das Problem der Sicherung der Schlüssel stellt, welches letztendlich in ähnliche Probleme, wie die bei der Verwendung von Kennwörtern schon erwähnten, mündet.

Biometrische Merkmale geben hier einen sehr viel anwenderfreundlicheren Ansatz. Sie haben nicht nur die Eigenschaft, dass sie einem Benutzer fest zugeordnet sind, sondern auch die, dass sie nicht vergessen werden und daher nirgends aufgeschrieben werden müssen. Besonders die Handschrift verfügt über viele weitere wünschenswerte Eigenschaften. Sie ist ein erlerntes biometrisches Merkmal, welches schon seit Jahrhunderten eine große Verbreitung und Akzeptanz erlangt hat – also schon seit langem zur Authentifizierung verwendet wird. Da zunehmend auch mobile Endgeräte und Computer mit der Möglichkeit der stiftbasierten Eingabe Verwendung finden, wird es zunehmend leichter möglich, handschriftliche Daten zu erfassen und auszuwerten.

Biometrische Merkmale sind oftmals gar nicht oder nur sehr schwer änderbar, darum wirft die Speicherung derselben oder der von Ihnen abgeleiteten Referenzdatensätze wiederum ein Sicherheitsproblem auf, da Sie auf keinen Fall in falsche Hände geraten dürfen. Wenn sie ausgespäht sind, können sie von einem Angreifer benutzt werden, um die fremde Identität vorzutäuschen mittels „Reply"-Attacken [Tele01]. Sie müssen in einem solchen Fall wie auch ein ausgespähtes Kennwort geändert werden. Ein Kennwort lässt sich jedoch sehr viel einfacher ändern, als eine Handschrift. Daher sind handschriftliche Daten besonders schützenswert. Einmal ausgespäht, sind insbesondere passive Merkmale wie z.B. der Fingerabdruck nicht mehr einsetzbar, da es durch den jeweiligen Anwender nur sehr schwer verändert werden kann. Etwas günstiger stellen sich in einer solchen Situation die aktiven Merkmale wie z.B. die Handschrift dar, da der Anwender sein Verhalten gegebenenfalls verändern kann (z.B. durch Training einer neuen Unterschrift).

Um dieser Sicherheitsproblematik gerecht zu werden, ist stets die verschlüsselte Speicherung und Übertragung von biometrischen Kenndaten erforderlich. Bei der Verschlüsselung werden jedoch Schlüssel benötigt, die geheim gehalten werden müssen. In vielen Anwendungsdomänen, beispielsweise bei Smartcards, wird dies durch PIN-Aktivierung erzielt. Will man aber gerade die PIN-Problematik mit biometrischen Verfahren lösen, ist eine PIN-Eingabe nicht

akzeptabel, da diese das Konzept der einfachen und sicheren Handhabung der Biometrie ad absurdum führen würde. Gefordert werden Alternativen für ein sicheres Schlüsselmanagement.

In unserem Beitrag werden wir im folgenden zuerst auf den generellen Schutzbedarf von biometrischen Merkmalen bei der Benutzerauthentifizierung eingehen. Aufbauend auf dieser Einführung diskutieren wir im Kapitel 3 grundlegende Sicherungskonzepte für biometrische Kenndaten bei der Nutzung von mobilen Endgeräten in unternehmensweiten IT-Infrastrukturen. Wir entwickeln weiterhin in den Abschnitten 3.1 bis 3.3 ein Konzept Bio-Key für handschriftliche Merkmale und stellen in Abschnitt 3.4 Testergebnisse vor. Abschließend diskutieren wir das erzielte Sicherheitsniveau und den weiteren Forschungsbedarf.

2 PDA-basierte biometrische Systeme

In diesem Kapitel werden die wesentlichen Komponenten biometrischer Systeme aufgezeigt, für welche Schutzbedarf beim Einsatz von mobilen Endgeräten existieren. Hierzu werden zunächst anhand des allgemeinen Phasenmodells biometrischer Systeme sensible Abschnitte dargelegt.

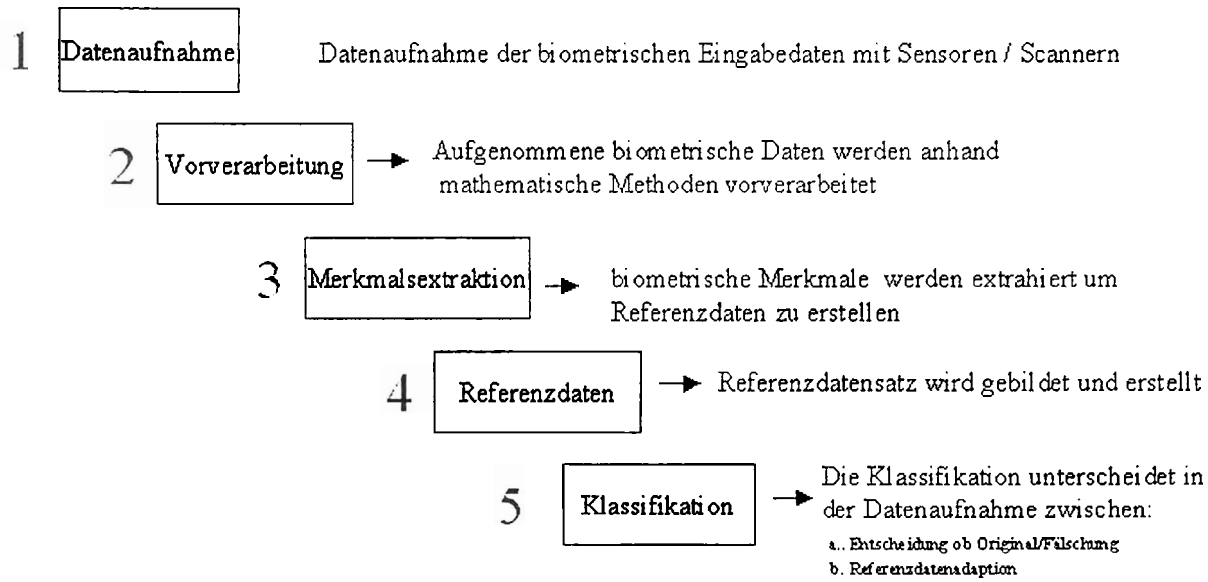

Abb. 1: Allgemeines Phasenmodell biometrischer Systeme

Bei der Verifikation oder Identifizierung der Benutzer wird eine aktuell aufgenommen Probe gegen die Referenzdatensätze verglichen. Aus diesem Grund sind die Schritte 1 (Datenaufnahme) und 4 (Referenzdaten) als sicherheitskritisch einzustufen. Während bei der Datenaufnahme das System vor verdeckten Aufzeichnungen geschützt werden muss, welche später für Wiedereinspiel-Attacken eingesetzt werden können, gilt es die Referenzdaten so zu speichern, dass sie für Unbefugte nicht lesbar sind.

Lokale Authentifikation ist dann gegeben, wenn der Vergleich der Schriftprobe mit den Referenzdaten und der Entscheidungsprozeß auf demselben Medium stattfindet, auf dem sich das physikalische Eingabegerät befindet (vgl. On-Card Matching). Hier muss sichergestellt sein,

dass diese Daten verschlüsselt hinterlegt werden und nur während des Verifikationsprozesses kurzzeitig entschlüsselt im Arbeitsspeicher gehalten werden.

Im Gegensatz zur lokalen wird bei einer serverbasierten Authentifikation die aktuelle Schriftprobe auf dem Eingabegerät erfasst, zur Verifikationsentscheidung jedoch zusammen mit einer vorgegebenen Identität an den Server übermittelt. Es ist hier zu beachten, dass neben einer sicheren Referenzdatenhaltung auf dem Server zusätzlich die Übertragungsstrecke zwischen beiden Geräten zu sichern ist.

3 Diskussion von Ansätzen

Zur Sicherung oder Übertragung gespeicherter vertraulicher Daten bieten sich kryptographische Verfahren an, welche in großer Zahl veröffentlicht sind und als sicher gelten [Schn96]. In der Regel handelt es sich entweder um symmetrische oder asymmetrische Verfahren, welche mit zunehmender Schlüssellänge stärkere Sicherheit gewährleisten. Da es jedoch für den Anwender oft nicht akzeptabel und praktikabel ist, sich einen solchen langen Schlüssel zu merken und vor jeder Ver- oder Entschlüsselung einzugeben, werden solche Schlüssel bisher mittels PIN oder Passwörtern chiffriert gespeichert. Vorschläge zur Lösung der Schlüsselproblematik durch biometrische Verfahren finden sich in [Nich99], wo vier Ansätze zur biometrischen Absicherung von Schlüsseln skizziert werden, die alle auf dem passiven biometrischen Merkmal Fingerabdruck basieren. Idee dabei ist, einen Schlüssel zur Verschlüsselung der biometrischen Merkmale (die erfassten Referenzdaten) aus dem biometrischen Merkmal selbst abzuleiten. Somit muss der Benutzer sich den Schlüssel nicht merken, sondern wird aus seiner aktuellen Eingabe (in der Verifikation) ermittelt. Folgende vier Strategien werden nach [Nich99] verfolgt:

- Referenzspeicherung und Verifikation auf vertrauenswürdigem Server:

  Hier erfolgt sowohl die Referenzdatenhaltung als auch der Authentifizierungsprozeß auf einem vertrauenswürdigem Server. Wenn Datenerfassung und Verifikation auf unterschiedlichen Rechnern erfolgt, ist eine Sicherung der Übertragungsstrecken erforderlich.

- Einbettung des Schlüssels in die Referenzdaten mittels Bit-Replacement:

  Dieser Ansatz verwendet einen geheimen Bit-Ersetzungsalgorithmus um den Schlüssel an definierten Positionen der Referenzdaten einzubetten. Problematisch ist hierbei, dass bei Kenntnis des Algorithmus ein Angreifer die Schlüssel aller verifizierten Anwender ermitteln kann.

- Direkte Ableitung des Schlüssels aus dem biometrischen Merkmal:

  Hierbei wird aus den abgegebenen biometrischen Merkmalen, ohne Vergleich mit einer Referenz, ein Schlüssel ermittelt. Insbesondere bei passiven Merkmalen stellt sich das Problem, dass bei Bekannt werden des individuellen Schlüssels das zugrunde liegende Merkmal verloren ist, da es vom Anwender nicht modifiziert werden kann.

- Verknüpfung von biometrischen Merkmalen und Schlüsseln während des Enrollments:

  Hier wird während des Enrollments das biometrische Merkmal mit dem individuellen Schlüssel so verknüpft, dass bei späterer Verifikation des Anwenders, die Antwort des biometrischen Systems nicht auf einer Ja/Nein-Entscheidung beruht, sondern bei Erfolg direkt den Schlüssel zurück liefert.

In Erweiterung zu den vorgestellten vier Strategien stellen wir ein neues Konzept zur sicheren Referenzdatenhaltung und Benutzerauthentifizierung auf Basis von handschriftlichen Merkmalen vor, welches aus zwei Abschnitten besteht:

1. Im ersten Abschnitt werden die biometrischen Merkmale erfasst.

   Das heißt, dass zunächst die Schriftprobe auf dem PDA erfasst wird. Es werden hierbei mehrere Schriftproben aufgenommen. Die dabei gewonnenen Daten werden dann mittels verschiedener Funktionen aufbereitet, um zum einen einen Referenzdatensatz zu erhalten und zum anderen die unterschiedlichen Merkmale zu extrahieren, aus denen mit der im folgenden Abschnitt beschriebenen Heuristik ein Schlüssel gebildet wird.

   Dieser Schlüssel wird im folgenden Bio-Key genannt. Zu den Referenzdaten wird dann ein Hashwert ihrer selbst hinzugefügt. Die erhaltenen Daten werden schließlich mit dem Bio-Key verschlüsselt. Die so verschlüsselten Daten werden dann als verschlüsselte Referenz abgespeichert. Der Vorgang der Erfassung der biometrischen Daten wird als Enrollment bezeichnet.

2. Der zweite Abschnitt beinhaltet die Authentifizierung.

   Hierbei wird eine Schriftprobe auf dem PDA eingegeben. Daraus wird zunächst der Bio-Key extrahiert und danach die verschlüsselte Referenz mit dem gewonnenen Bio-Key entschlüsselt.

   Wenn der Hashwert der Referenzdaten nicht mit dem gespeicherten Hashwert übereinstimmt, wird die Authentifizierung abgebrochen, der Benutzer kann nicht authentifiziert werden.

   Bei korrektem Hashwert folgt die zweite Stufe der Authentifizierung. Hierbei werden die aus der Unterschrift extrahierten Merkmalsdaten mit den Referenzdaten abgeglichen. Wenn nun die Identität eines Benutzers vorgegeben ist und vom System überprüft wird, spricht man von einer Verifikation. Bei ausreichender Übereinstimmung bzw. Ähnlichkeit der Merkmale ist die Authentifizierung erfolgreich, ansonsten ist sie misslungen. Für die Authentifizierung gibt es zwei unterschiedliche Konzepte:

   - Es besteht die Möglichkeit die Authentifizierung vollständig lokal auf dem PDA vorzunehmen
   - Die Authentifizierung erfolgt auf einem Server, der Referenzdaten enthält, so dass auf dem PDA nur die Eingabe der zu überprüfenden Unterschrift erfolgt; die Daten werden dann an den Server weitergegeben, der sie mit den Referenzdaten vergleicht.

Wir werden in den nächsten Abschnitten darstellen, wie der Bio-Key bestimmt wird und dieser für lokale und serverbasierte Authentifizierung eingesetzt werden kann.

3.1 Schlüsselgenerierung (Bio-Key)

Für jede handschriftliche Eingabe wird ein 24-dimensionaler Merkmalsvektor bestimmt, welcher aus den in der Tabelle 1 aufgeführten statistischen Größen besteht.

Für jedes Merkmal wird ein ganzzahliger Wert berechnet. Die Werte aller Schlüsselmerkmale ergeben den Schlüsselvektor.

Tab. 1: Merkmale des 24-dimensionalen Merkmalsvektors

Merkmalnummer	Beschreibung des Merkmals
1.	Anzahl der Segmente N_S
2.	Dauer T
3.	Anzahl Punkte N_P
4.	Anzahl Extrema
5.	Verhältnis der maximalen Ausdehnung Y:X
6.	Verhältnis TDown zu Tup
7.	FlächeX
8.	FlächeY
9.	Durchschnittliche Horizontalgeschwindigkeit V_X
10.	Durchschnittliche Vertikalgeschwindigkeit V_Y
11.	Durchschnittliche Horizontalbeschleunigung A_X
12.	Durchschnittliche Vertikalbeschleunigung A_Y
13.	(Max-Min)/T für X
14.	(Max-Min)/T für Y
15.-19.	FlächeX_1-X_5 (für 5 äquidistante Zeitabschnitte)
20.-24.	FlächeY_1-Y_5 (für 5 äquidistante Zeitabschnitte)

Dieser Zahlenvektor wird als Schlüssel bzw. Initialisierungsvektor für eine symmetrische Verschlüsselung verwendet. Da die aus den Schriftproben abgeleiteten Merkmalswerte nicht konstant sind, muss der entstehende Wertebereich jedes einzelnen Merkmals auf einen ganzzahligen Wert abgebildet werden. Dies geschieht nach folgendem von uns entwickelten Verfahren:

Es werden zunächst für jedes Merkmal x_j die beiden Intervallgrenzen, innerhalb derer die Werte der beim Enrollment eingegebenen Schriftproben einer Person liegen, ermittelt. Es werden also die Werte für das Maximum der beim Enrollment erfassten Werte und das Minimum der beim Enrollment erfassten Werte für jedes Merkmal bestimmt. Damit ergibt sich das Intervall:

$$I_{j,0} = \{ I_{min,j,0}, I_{max,j,0} \}$$

in dem alle Werte eines Merkmals liegen sollen. Es handelt sich hierbei immer um ganze Zahlen.

Da bei nur vier Enrollmentwerten nicht erwartet werden kann, dass jeder weitere Wert eines Merkmals einer weiteren Schriftprobe innerhalb des Intervalles $I_{j,0}$ liegt, werden die Werte $I_{min,j,0}$ und $I_{max,j,0}$ prozentual erniedrigt bzw. erhöht. Man gibt hierzu Toleranzwerte vor, die merkmalsspezifisch aus Feldversuchen über eine große Zahl von Anwendern und Semantiken

ermittelt werden, Details hierzu finden sich in [Hais01]. Es ergibt sich dann das folgende erweiterte Intervall:

$$I_j = \{ I_{min,j}, I_{max,j} \} = \{ I_{min,j,0} * (1 - Toleranz_{unten}), I_{max,j,0} * (1 + Toleranz_{oben}) \}$$

Die Breite dieses Intervalls I_j wird für jedes Merkmal χ_j bestimmt. Sie ist als die Einheit, mit welcher das Merkmal „gemessen" wird, definiert. Dieser Vorgang wird im weiteren als Normierung bezeichnet. Da die Werte $I_{min,j}$ und $I_{max,j}$ ganzzahlig sind, repräsentieren sie einen Wertebereich von $I_{min,j}$- *0,5 bis* $I_{max,j}$ *+0,5*, d.h. die Intervallbreite und somit die Maßeinheit eines Merkmals ist :

$$\Delta I_j = I_{max,j} + 0{,}5 - (I_{min,j} - 0{,}5) = I_{max,j} - I_{min,j} + 1$$

Man erhält mit der Intervallbreite als Maßeinheit damit folgende normierte Intervallgrenzen für jedes Merkmal :

$$I_{\min,j,normiert} = \left[\frac{I_{\min,j}}{\Delta I_j} \right] + \frac{I_{\min,j} \bmod \Delta I_j}{\Delta I_j}$$

und

$$I_{\max,j,normiert} = \left[\frac{I_{\max,j}}{\Delta I_j} \right] + \frac{I_{\max,j} \bmod \Delta I_j}{\Delta I_j}$$

Die Funktion $f(\chi)=[\chi]$ bedeutet hier die Entier- oder Ganzzahligkeitsfunktion, die den ganzzahligen Wert $\chi_0<x$ liefert. Weiter ist die Funktion $f(\chi,y) = y \bmod \chi = y - \chi * [y/\chi]$ der Divisionsrest. Durch diese Normierung gilt für jedes Intervall $I_{max,j,normiert} = I_{min,j,normiert} + 1$. Das normierte Intervall hat also immer die Größe Eins.

Das Intervall $\{ I_{min,j}, I_{max,j} \}$ ist so zu verschieben, dass alle Werte des Intervalls, nachdem man sie durch die Intervallbreite ΔI dividiert hat und das Ergebnis gemäß der Ganzzahligkeitsfunktion abgerundet hat, immer den gleichen ganzzahligen Wert liefern. Hierzu wird zunächst eine neue untere Intervallgrenze festgelegt. Im Normalfall ergibt sich als Verschiebungswert V_j:

$$V_j = I_{min,j} \bmod \Delta I_j ,$$

der zum Intervall $I_{j,verschoben} = \{ I_{min,j} - V_j, I_{max,j} - V_j \}$ führt. Alle Werte aus I_j nehmen nun, wenn man sie durch ΔI dividiert und auf das Ergebnis die Entierfunktion anwendet, denselben ganzzahligen Wert an. Dieser Wert entspricht im Normalfall $[I_{min,normiert}]$.

In dem seltenen Fall, dass der Nullpunkt sich im Intervall befindet und nicht der Minimalwert ist, ist aus Konsistenzgründen das Intervall so zu verschieben, dass die untere Intervallgrenze auf den Nullpunkt fällt. Der Wert für die Verschiebung berechnet sich dann einfach zu $V_j = -I_{min,j}$. Es ergibt sich das Intervall $I_{j,verschoben} = \{ 0, (I_{max,j} - I_{min,j}) \}$ für diesen Sonderfall.

Alle erhaltenen ganzzahligen Werte aller Merkmale werden in einen Vektor zusammengefasst, den Schlüsselvektor. Dieser handschriftliche Fingerabdruck kann gleichzeitig direkt als Schlüssel verwendet werden. Je nach gewünschter Schlüssellänge kann der Vektor stattdessen auch mit einer entsprechenden Hashfunktion angepasst werden. So kann das Ergebnis der Anwendung der Hashfunktion auf den Vektor als Schlüssel für eine symmetrische Verschlüsselung oder auch als Initialisierungsvektor für die Erzeugung des ersten Rundenschlüssels eingesetzt werden, je nach angewandtem Verschlüsselungsverfahren.

Zur Prüfung, ob ein Merkmal x einer weiteren Schriftprobe innerhalb des oben beschriebenen Intervalls liegt, benötigt man die oben beschriebenen Werte V und ΔI. Sie werden benötigt, um einen erhaltenen Merkmalswert auf den entsprechenden skalaren Parameter abzubilden. Daher wird ein weiterer Vektor, im folgenden SP-Vektor genannt, erzeugt. Er enthält für jedes Merkmal ein 2-Tupel, welches aus der entsprechenden Intervallänge ΔI und dem zugehörigen Verschiebungswert V besteht. Der SP-Vektor muss beim Enrollment ermittelt und gespeichert werden. Aus diesem Vektor kann man nur ersehen, wie groß der Bereich ist, in dem die einzelnen Werte liegen, jedoch nicht direkt wo dieser Bereich liegt. Man kann somit keine Rückschlüsse auf den genauen Wertebereich oder die zugehörigen Parameter ziehen.

Nachdem nun der Schlüssel erzeugt ist, wird er mittels einer Hashfunktion auf die gewünschte Größe gebracht. Als Ergebnis der auf den Schlüsselvektor angewandten Hashfunktion erhält man einen Schlüssel, den Bio-Key. Nachdem an die Referenz der Hashwert ihrer selbst angefügt wurde, wird das Ergebnis dieses Vorgangs mit einem symmetrischen Verschlüsselungsverfahren unter Benutzung des Bio-Key als Schlüssel verschlüsselt. Nachdem diese verschlüsselte Referenz sowie der SP-Vektor gespeichert wurden, ist das Enrollment beendet.

3.2 Lokale Referenzverschlüsselung und Authentifizierung

Zur lokalen Authentifizierung wird ein zweistufiges Konzept benutzt, welches zunächst die lokal gespeicherte und mit dem Bio-Key verschlüsselte Referenz entschlüsselt und bei erfolgreicher Authentizitäts- und Integritätsprüfung die Referenzdaten einer Vergleichsfunktion zur Verifikation zuführt, siehe folgende Abbildung:

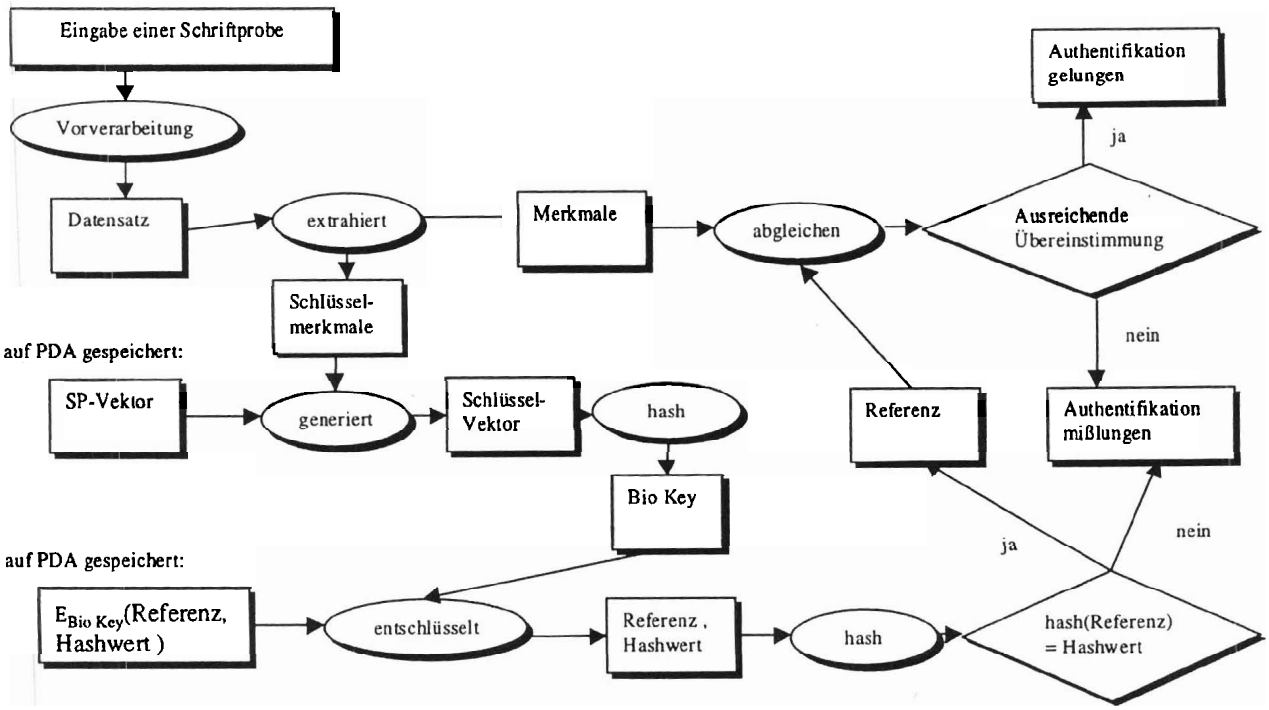

Abb. 2: Ablauf der lokalen Verifikation

Durch die verschlüsselte Speicherung sowohl der Referenzdaten als auch eines über die Referenzdaten gebildeten Hashwertes kann bei der Verifikation nach der Entschlüsselung bereits

eine Integritätsprüfung erfolgen. Ist der über die entschlüsselten Referenzdaten ermittelte Hashwert nicht gleich dem aus dem entschlüsselten Datensatz, so ist mit sehr großer Wahrscheinlichkeit der eingesetzte Bio-Key nicht authentisch, somit ist die Authentifizierung des Anwenders abzuweisen. Der vorgestellte Bio-Key kann somit sowohl zur Verschlüsselung der Referenzdaten, als auf zur Benutzerauthentifizierung eingesetzt werden.

3.3 Sichere serverbasierte Authentifizierung

Zur sicheren serverseitigen Authentifizierung handschriftlicher Eingaben von Anwendern auf einem PDA gehen wir wie in Abbildung 3 vor: der Bio-Key wird vom PDA zum Server übermittelt, auf welchem die verschlüsselte Referenz hinterlegt ist. Der Server entschlüsselt diese in der Folge und kann dann mittels Authentizitäts- und Integritätsprüfung bestimmen, ob erfolgreich entschlüsselt wurde.

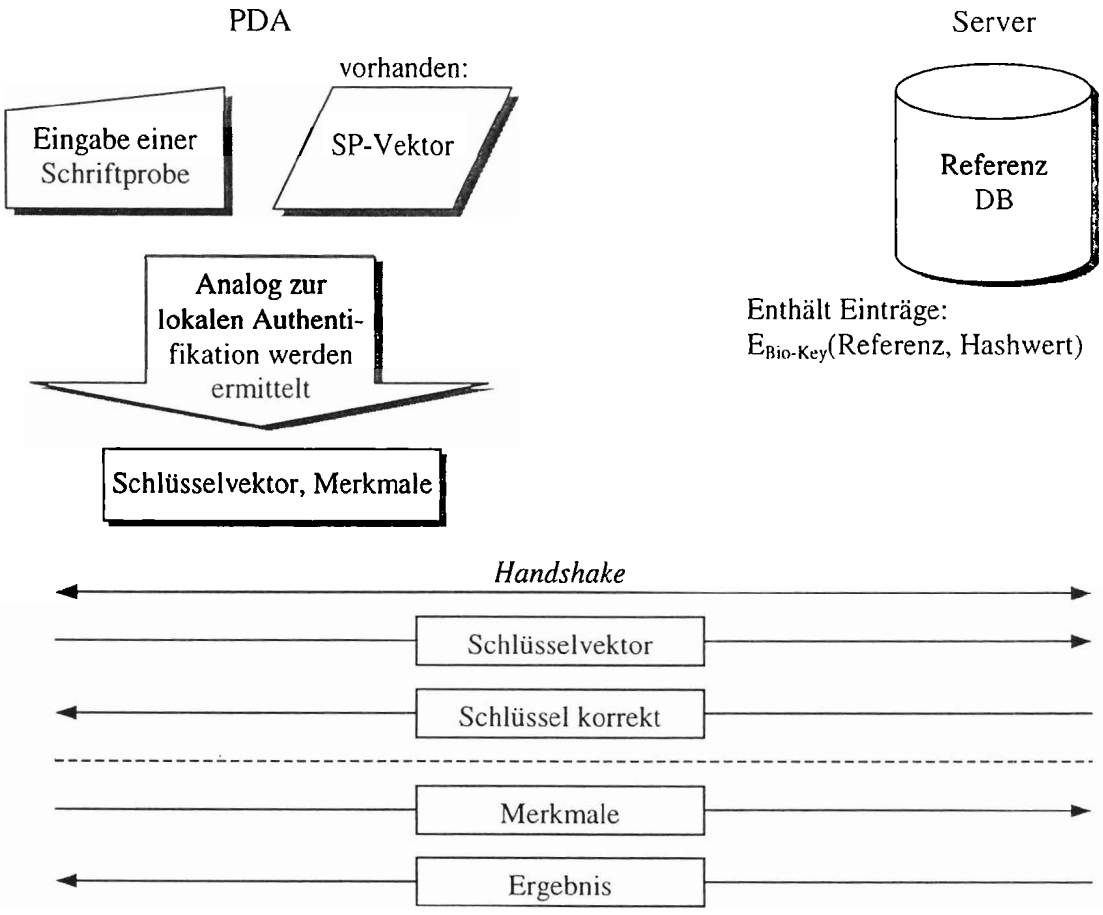

Abb. 3: Ablauf der Globalen Authentifizierung

Zur Sicherstellung der sicheren und vertraulichen Kommunikationsstrecke wird das SSL 3.0 Protokoll [SSL01] eingesetzt.

3.4 Evaluation und Testergebnisse

Zur Abschätzung des mit dem vorgestellten Verfahren erreichbaren Schlüsselraums wurde das Verfahren mit 11 Anwendern und 5 verschiedenen Semantiken (Unterschrift, Symbol, Zahl, Wort, Passphrase, vgl. [Viel00]) getestet.

Es ergaben sich Schlüsselraumgrößen im Bereich von 6*1022 (Semantiken Zahl und Symbol) bis 5.1*1024 (Semantik Wort). Diese Größenordnung lassen auf einen hinreichend großen Schlüsselraum der Bio-Keys schließen.

In Tests wurden sowohl die Fehlerraten für Falschabweisung (False Rejection Rate, FRR) als auch für Falschakzeptanz (False Acceptance Rate, FAR) für die Generierung der Bio-Keys bestimmt.

Ein Verifikationsversuch eines authentischen Anwenders wurde dabei der FRR-Fehlerklasse zugeordnet, wenn der aus der Eingabe generierte Bio-Key nicht dem in den Referenzdaten hinterlegten entspricht. Falschakzeptanz liegt dann vor, wenn ein Fälscher einen Bio-Key eines anderen Anwenders generieren kann.

Nach der Klassifikation der Angriffstärke in [Vist01] wurden Low-Force Angriffe durchgeführt, wobei jedem Fälscher der Schriftzug des Originalschreibers vorlag. Es wurde mit 10 Anwendern getestet, wobei ein Verifikationsversuch direkt nach dem Enrollment erfolgte und ein zweiter eine Woche später. Die Ergebnisse sind in den folgenden beiden Tabellen dargestellt.

Tab. 2: False Rejection Rates (FRR)

Person Semantik	Unterschrift	Symbol	Zahl	Wort	Passphrase	Durchschnitt
AL	8 %	4 %	6 %	0 %	4 %	4 %
AM	9 %	2 %	8 %	4 %	12 %	5 %
MM	21 %	14 %	29 %	6 %	27 %	19 %
FR	4 %	2 %	18 %	6 %	8 %	8 %
EH	6 %	20 %	6 %	6 %	6 %	9 %
YS	10 %	12 %	8 %	6 %	12 %	10 %
JD	6 %	0 %	6 %	10 %	8 %	6 %
EF	10 %	0 %	16 %	4 %	21 %	10 %
MH	4 %	2 %	2 %	0 %	10 %	4 %
ST	8 %	4 %	10 %	2 %	10 %	7 %
LF	2 %	2 %	2 %	0 %	4 %	2 %
Durchschnitt	7 %	6 %	10 %	4 %	11 %	8 %

Tab. 3: False Accepteance Rates (FAR)

Person Semantik	Unterschrift	Symbol	Zahl	Wort	Passphrase	Durchschnitt
AL	0 %	50 %	0 %	0 %	0 %	10 %
AM	0 %	20 %	0 %	0 %	0 %	4 %
MM	0 %	0 %	0 %	0 %	0 %	0 %
FR	0 %	20 %	0 %	0 %	0 %	4 %
EH	0 %	0 %	0 %	0 %	0 %	0 %
YS	0 %	0 %	0 %	0 %	0 %	0 %
JD	0 %	0 %	0 %	0 %	20 %	4 %
EF	0 %	40 %	0 %	0 %	0 %	8 %
ST	0 %	0 %	0 %	0 %	0 %	0 %
LF	0 %	20 %	0 %	0 %	0 %	4 %
Durchschnitt	0 %	15 %	0 %	0 %	2 %	3 %

4 Ausblick

Zusammenfassend kann man sagen, dass die Werte der Fehlerraten des vorgestellten Verfahrens sehr gering sind. In [BSI00] ist für die Bewertung von Fehlerraten eine vierstufige Skala definiert. Sie enthält die Bewertungen „schwach",„mittel", „stark" und „sehr stark", wobei „schwach" die ungünstigste Kategorie darstellt und „sehr stark" die günstigste.

Die FAR über alle Personen und Semantiken beträgt nur 3% bei geübten Fälschungen. Dies wird nach [BSI00] als „stark" bewertet. Bei zufälligen Fälschungen wird ein Wert von unter 0,3 % erreicht, was nach [BSI00] als „sehr stark" bewertet wird. Die FRR beträgt 8 %, das ist nach [BSI00] „schwach". Erweiterungen des Verfahrens unter Einbeziehung von statistischen Ausreißertests haben in ersten Versuchen bereits zu deutlichen Verbesserungen dieser Fehlerrate geführt. Der Vergleich der Semantiken zeigt, dass die Unterschrift besser geeignet scheint, als die übrigen Semantiken, wobei alle Semantiken grundsätzlich zur Generierung von Bio-Keys geeignet sind.

Die Probandenzahl von 10 läßt noch keine statistisch signifikanten Aussagen zu. Hier sind weitere Tests mit einer größeren Anzahl von Benutzern notwendig, um die Stabilität des Bio-Keys zu bestätigen. Es muß ferner die Entropie der mit dem dargestellten Verfahren generierten Schlüssel untersucht werden, d.h. welche Wertbereiche im Schlüsselraum tatsächlich ausgenutzt werden. Dies läßt dann Rückschlüsse auf mögliche Mehrfachabbildung unterschiedlicher Anwender auf identische Hash-Werte zu.

Eine weitere Verbesserung der Fehlerraten kann durch Dynamisierung der Toleranzwerte erzielt werden, bei der mit jedem Authentifizierungsversuch die Toleranzwerte der Schlüsselintervalle im Rahmen eines dynamischen Enrollments oder nach anderen zu findenden Kriterien neu berechnet werden.

Des weiteren können noch weitere andere als die in dieser Beitrag vorgestellte Merkmale zur Schlüsselerzeugung gefunden werden, mit dem Ziel ein Verfahren zu erhalten, welches noch bessere Fehlerraten aufweist. Bei einer Umsetzung des Verfahrens auf geeignetem Aufnahmegerät lässt sich auch der Schreibdruck messen. Dieser gilt als ein charakteristisches Merkmal der Handschriftenerkennung [Pllo87]. Daher ist zu untersuchen, inwieweit sich aus den Druckwerten Parameter ableiten lassen, die sich zur Erzeugung eines Schlüssels eignen.

Neben der Betrachtung der Stabilität des Bio-Keys sind jedoch auch Aspekte der Hinterlegung der verschlüsselten Referenzdaten zu beachten. Gelingt es einem Angreifer seine Referenzdaten auf dem mobilen Endgerät oder auf dem Server zu hinterlegen, kann er sich wie ein rechtmäßiger Benutzer gegenüber dem Endgerät authentifizieren.

Literatur

[BSI00] Bundesamt für Sicherheit und Informationstechnik: Technische Evaluierungskriterien zur Bewertung und Klassifizierung biometrischer Systeme. http://www.bsi.de

[Hais01] M. Haisch: Konzeption und Entwicklung von Verfahren zur Absicherung handschriftlicher Merkmale bei der Benutzerauthentifikation auf mobilen Endgeräten, Diplomarbeit am Lehrstuhl für Industrielle Prozess- und Systemkommunikation (KOM) der TU Darmstadt, 2001.

[Hors01] P. Horster: Kommunikationssicherheit im Zeichen des Internets, Vieweg Verlag, 2001, ISBN 3-528-05763-7

[Nich99] R. K. Nichols: ICSA Guide To Cryptography, McGraw-Hill, 1999, ISBN 0-07-913759-8

[Pllo87] R. Plamondon, G. Lorette: Automatic Signature Verification and Writer Identification – the State of the Art, Pergamon Press plc., Pattern Recognition, 22, 2:107-131, 1987

[Schn96] B. Schneier: Angewandte Kryptographie, Addison-Wesley, 1996, ISBN 3-89319-854-7

[SSL01] http://home.netscape.com/eng/ssl3/

[Tele01] TeleTrust Deutschland e.V., Arbeitsgruppe 6: Biometrische Identifikationsverfahren. Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren. Kriterienkatalog Version 1.0, www.teletrust.de, 1998

[Viel00] C. Vielhauer: Handschriftliche Authentifikation für digitale Wasserzeichenverfahren, In: M. Schumacher, R. Steinmetz: Sicherheit in Netzen und Medienströmen, Springer Verlag, 2000, ISBN 3-540-67926-X

[Vist01] C. Vielhauer, R. Steinmetz: Sicherheitsaspekte biometrischer Verfahren: Klassifizierung von sicherheitsrelevanten Vorfällen und wesentlicher Größen zur Beurteilung der Funktionssicherheit. In: Tagungsband 7. Deutscher IT-Sicherheitskongress des BSI, SecuMedia Verlag, 2001, ISBN 3-922746-36-5