Vertrauenswürdige Chipkartenbasierte Biometrische Authentifikation[1]

Gunter Lassmann, Matthias Schwan

T-Systems International GmbH,
ICT Security,
Goslarer Ufer 35, 10589 Berlin
gunter.lassmann@t-systems.com
matthias.schwan@t-systems.com

Abstract: In dieser Arbeit stellen wir das Chipkartenbasierte Biometrische Identifikationssystem (CBI-System) vor. Dieses Template-On-Card System vereint die Vorteile von Chipkarten mit den Vorteilen der Biometrie, um eine höhere Überwindungssicherheit des Gesamtsystems zu gewährleisten. Ausgehend von den Sicherheitsanforderungen führen wir ein Protokoll ein, welches u.a. abgestufte Fehlbedienungszähler benutzt, um den Sicherheitsbedürfnissen der Chipkarte und des korrespondierenden Hostsystems Rechnung zu tragen. In einer Analyse des Systems zeigen wir dessen Stärken und Schwächen.

1 Einleitung

Biometrische Systeme erlauben das Erkennen von Personen anhand physiologischer oder verhaltenstypischer Merkmale. Damit ist im Grunde die unbefugte Weitergabe des Authentifikationsmittels wie bei wissens- oder besitzbasierten Verfahren nicht möglich. Dieser Vorteil kann die Sicherheit eines Systems sowie die Benutzerfreundlichkeit erhöhen. Andererseits bieten biometrische Systeme neue Angriffsmöglichkeiten, wie z.B. auf die Referenzdaten [BEM02, Ma03]. Weiterhin stellen die zugrunde liegenden biometrischen Erkennungsverfahren eine physikalische Messung am lebenden Objekt dar und sind somit immer mit einem Messfehler behaftet. Dadurch ist z.B. das Nichterkennen eines Berechtigten ein normaler „Betriebsfall“, der diskret und doch sicher gehandhabt werden muss [La02a, NL02]. Chipkarten haben sich seit langer Zeit als sichere Speichermedien und als besitzbasierte Authentifikationsmittel bewährt. Häufig werden sie in Kombination mit wissensbasierten Verfahren (PIN) benutzt, wobei das Problem der willentlichen oder unwillentlichen Weitergabe des Wissens oder Besitzes besteht. Die Idee der Kombination von biometrischen und besitzbasierten Verfahren wird schon seit langem diskutiert [SCA02]. Weiterhin wurde in diesen auch Zweifaktor Authentifikation genannten Systemen die Kombination von biometrischen und wissensbasierten Verfahren vorgestellt [BA03]. Beim *System-on-Card* wird die gesamte biometrische Erkennung von der Karte ausgeführt. Die Karte arbeitet unbeeinflußt und die Referenzdaten verlas-

[1] Diese Arbeit entstand im Rahmen des vom BMBF geförderten Projektes „Verisoft – Beweisen als Ingenieurwissenschaft“ – http://www.verisoft.de

sen nie die Karte, leider ist dies zurzeit aus Platz- und Rechenkapazitätsgründen nur selten realisiert worden [Br05][BAI05], wenn dann als einfache Fingerprinterkennung. Beim *Matching-On-Card* werden die letzten Schritte der biometrischen Erkennung auf der Karte ausgeführt, d.h. die Aufbereitung der aktuellen Messdaten findet außerhalb der Karte statt, die Referenzdaten verlassen nie die Karte. Matching-On-Card Systeme wurden schon für komplexere Merkmale wie Gesichtserkennung vorgestellt [G&D05]. Beim *Template-on-Card* rechnet die Karte nicht selbst, sondern die Referenzdaten werden zum Vergleich temporär ausgelesen. Die biometrische Erkennung findet außerhalb der Karte statt. Die Realisierung eines kombinierten Verfahrens, das mehrere biometrische Verfahren sowie Chipkarten benutzt ist lediglich über ein Template-On-Card System realisierbar. Eine Veröffentlichung der gewählten Schutzmassnahmen sowie Sicherheitsanalysen dieser Systeme sind den Autoren nicht bekannt. Wir stellen ein Template-On-Card System vor, das die Vorteile einer kryptographischen Chipkarte und der biometrischen Verifikation kombiniert. Wir betrachten nicht nur das Sicherheitsbedürfnis des eigentlichen Zugangssystems, sondern aus Datenschutzgründen auch das Sicherheitsbedürfnis der Chipkarte als Träger der biometrischen Referenzdaten [La02b]. Dazu formulieren wir in Kapitel 2 zunächst die Sicherheitsanforderungen und erarbeiten in Kapitel 3 mögliche Sicherheitsmassnahmen, die in einem konkreten Protokoll umgesetzt werden. Eine ausführliche informelle Analyse zeigt in Kapitel 4 die Stärken und Schwächen des Systems. Die Verifikation der propagierten Sicherheitseigenschaften des CBI-Systems in einem formalen Modell wird derzeit im Rahmen des Forschungsprojekts Verisoft [CLRS05], [Ver05] durchgeführt, die aber im Rahmen dieser Arbeit nicht behandelt werden können. Abschließend geben wir in Kapitel 5 mögliche Weiterentwicklungen des Systems an.

2 Sicherheitsziele und -anforderungen

Das Chipkartenbasierte Biometrische Identifikationssystem (kurz: CBI-System) ist für eine Zugangskontrolle zu Rechnern und Rechenressourcen sowie für eine Zutrittskontrolle zu Räumen und Gebäuden nutzbar. Es identifiziert und authentifiziert einen Nutzer durch Besitz sowie biometrische Merkmale, um einem nachgeordneten System die überprüfte Identität des Nutzers zu übermitteln. Dazu werden biometrische Referenzdaten eines Nutzers auf einer ihm zugeordneten Chipkarte gespeichert, wobei die Speicherung mehrerer Referenzdatensätze unterschiedlicher biometrischer Merkmale möglich ist. Damit kann sich ein Nutzer an unterschiedlichen Systemen mit unterschiedlichen biometrischen Merkmalen anmelden. Das CBI-System verfolgt zwei Hauptziele:

- Dezentrale Speicherung der biometrischen Referenzdaten zum Zweck des Datenschutzes
- Erhöhung des Schwierigkeitsgrades zur Überwindung des Zugangssystems

Um die beiden Sicherheitsziele zu erfüllen stellen wir folgende 10 Sicherheitsanforderungen an das CBI-System. Ein Nutzer gilt gegenüber dem System als authentifiziert, wenn

a. der Nutzer eine zugelassene Chipkarte besitzt und

b. der Host, auf dem sich das Zugangssystem befindet, zugelassen ist und
c. die Chipkarte eine gültige Identität enthält und
d. die Chipkarte gültige biometrische Referenzdaten präsentiert und
e. der Nutzer seine aktuellen biometrischen Daten präsentiert und
f. die biometrischen Daten und die Referenzdaten hinreichend ähnlich sind.

Zusätzlich darf das System die aktuellen biometrischen Daten sowie Referenzdaten nicht speichern oder in anderer Weise weitergeben. Nach erfolgtem Vergleich beider Datensätze sind die Datensätze verlässlich zu löschen. Erst nach der Löschung wird dem nachgeordneten System die überprüfte Identität des Nutzers übermittelt. Weiterhin sind fehlgeschlagene Authentifizierungsversuche zwischen Chipkarte und Host sowie fehlgeschlagene biometrische Verifikationsversuche auf der Chipkarte zu registrieren. Die so eingeführten Fehlbedienungszähler können in Abhängigkeit der Sicherheitsstrategie vom Zugangssystem ausgewertet und eine Authentifizierung abgelehnt werden. Es besteht damit die Möglichkeit, das in Abschnitt 4 genannte Restrisiko zu vermindern. Es gelten folgende zusätzlichen Sicherheitsanforderungen.

g. Die biometrischen Daten und Referenzdaten sind vertrauliche Daten und nach dem Vergleich sind beide Datensätze zu löschen.
h. Fehlgeschlagene Authentifizierungsversuche des Hosts (Zugangssystem) gegenüber der Chipkarte sind zu registrieren und auswertbar
i. Fehlgeschlagene biometrische Verifizierungsversuche sind zu registrieren und auswertbar
j. Die Übermittlung der überprüften Identität des Nutzers an das nachgeordnete System erfolgt nach Erfüllung aller anderen Ziele.

3 Sicherheitsmassnahmen

3.1 Architektur und allgemeiner Ablauf

Das CBI-System besteht aus vier Hauptkomponenten: a) dem *Zugangssystem*, das als Anwendung auf einem Betriebssystem aufsetzt (Host Software), b) einem *Chipkartenterminal* für die Kommunikation zwischen Zugangssystem und Chipkarte, c) einer *Chipkarte* (Smartcard), und d) einem *biometrischen Sensor* für die Aufnahme der aktuellen biometrischen Daten. Anweisungen an den Nutzer und der Erfolg oder Misserfolg einer biometrischen Verifikation werden über ein Display angezeigt.

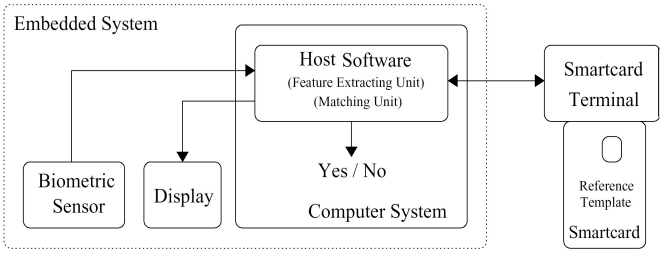

Abbildung 1: Architektur des CBI-Systems

Ablauf: Die Chipkarte und der Host authentifizieren sich gegenseitig nach ISO 9798 mittels eines beiden bekannten symmetrischen Schlüssels und vereinbaren einen Sitzungsschlüssel. Der Zähler für fehlgeschlagene Authentifizierungsversuche (FBZ1) wird geprüft. Der Host prüft und vermindert den biometrischen Fehlbedienungszähler (FBZ2), schreibt ihn in die Karte, liest die signierten Referenzdaten von der Chipkarte und verifiziert deren Authentizität durch Prüfung der Signatur. Der Host liest die aktuellen biometrischen Daten vom biometrischen Sensor und vergleicht beide Datensätze. Bei einem positiven Ergebnis wird der FBZ2 neu in die Karte geschrieben, bei negativem Ergebnis wird der Nutzer über das Display aufgefordert seine biometrischen Daten erneut dem Sensor zu präsentieren. Dieser Vorgang wird höchstens zweimal wiederholt, danach wird der Nutzer im negativen Fall abgewiesen. Der Host löscht dauerhaft die aktuellen biometrischen Daten und die Referenzdaten. Erst nach erfolgreicher Löschung (z.B. Überschreiben) gibt er das Ergebnis an das nachgeordnete System weiter.

3.2 Protokollablauf (Sequenzdiagramm)

Nach der Personalisierung befinden sich neben anderen beliebigen Anwendungen auf der Chipkarte ein File mit der Kartennummer (Card_ID) und ein Verzeichnis für die Hostapplikation. Im Applikationsverzeichnis werden ein Geheimnisfile, ein File mit dem biometrischen Fehlbedienungszähler (FBZ2) und ein File mit den Referenzdaten und der elektronischen Signatur angelegt. Das Geheimnisfile enthält den symmetrischen Schlüssel für die Hostapplikation und kann weder gelesen noch manipuliert werden. Auf die Files FBZ2 und die Referenzdaten mit der Signatur kann nur nach einer erfolgreichen Authentifikation im Modus Secure Messaging zugegriffen werden. Das Protokoll ist in Abbildung 2 und 3 als Sequenzdiagramm in der UML1.0 gegeben und wird im Folgenden informell beschrieben.

1. Wird die Chipkarte in den aktiven Kartenleser gesteckt, läuft gemäß ISO 7816 ein ATR Protokoll (answer to reset) ab, welches den Controller auf der Karte rücksetzt und ein Übertragungsprotokoll aushandelt. Damit kann TCOS2.0 Kommandos entgegennehmen und bearbeiten.

2. Die Hostapplikation liest die Card_ID ID_{icc} aus der Karte und fordert von der Chipkarte eine Zufallszahl R_{icc} an, welche neu in der Karte generiert wird.

3. Im Kommando „(mutual) external Authenticate“ übergibt die Hostapplikation der Chipkarte ein 32 Byte langes mit dem gemeinsamen Geheimnis k_{auth} verschlüsseltes Kryptogramm, das die 8 Byte Zufallszahl R_{icc}, 8 Byte Card-ID ID_{icc} , 8 Byte Host-ID ID_{Host} und eine von der Hostapplikation generierte Zufallszahl R_{Host} enthält.

4. Die Chipkarte entschlüsselt das Kryptogramm und erkennt die ursprünglich gesendete Zufallszahl und die Kartennummer und kann somit der Hostapplikation vertrauen. Als Antwort wird ein neues Paket verschlüsselt, das die 8 Byte Zufallszahl der Hostapplikation R_{Host} , die 8 Byte Host-ID ID_{Host} und eine neue Zufallszahl R''_{icc} enthält. Die Hostapplikation kann nach der erfolgreichen Entschlüsselung dieser Daten seine Zufallszahl und ID erkennen und vertraut seinerseits der Chipkarte. Die Kommandofolge, Anfordern einer Zufallszahl „ask random“ und „external Authen-

ticate“, ist zwingend vorgeschrieben. Der Authentikations-Fehlbedienungszähler (FBZ1) wird vor jeder Authentifikation dekrementiert und nur nach erfolgreichem Abschluss auf seinen Ursprungswert zurückgesetzt. Somit ist nur eine begrenzte Anzahl von Versuchen möglich. Der FBZ1 wird vom Chipkartenbetriebssystem verwaltet.

5. Mittels Secure Messaging wird ein Sitzungsschlüssel k_s von der Karte angefordert, der mit k_{enc} verschlüsselt sowie mit k_{mac} integritätsgeschützt ist und für die nachfolgende sichere Kommunikation benutzt wird.

6. Nach einer erfolgreichen Authentifikation ist der Zugriff auf die Files FBZ2 und die Referenzdaten mit Signatur möglich. Beide, Chipkarte und Hostapplikation, besitzen den gleichen Sitzungsschlüssel. Der Datenaustausch erfolgt mit dem Sicherheitsmechanismus „Secure Messaging“. Die Datenobjekte zum Lesen und schreiben der Files werden verschlüsselt und/oder authentisch übertragen (siehe unten).

7. Die Hostapplikation liest den FBZ2, prüft seinen Stand, dekrementiert den Wert und schreibt ihn zurück. Der FBZ2 regelt ausschließlich den Zugriff auf die biometrischen Daten, er wird nur durch die Hostapplikation gelesen und geschrieben und kann durch die Chipkarte nicht ausgewertet werden. Ist er abgelaufen muss die Hostapplikation den weiteren Prozess abbrechen. Um das Speichern zu überprüfen wird der FBZ2 nochmals gelesen und sein Wert mit dem aktuellen Stand der Hostapplikation verglichen. Dies ist erforderlich, da von der Chipkarte nur eine ungesicherte Kommandobestätigung kommt, die von einem Angreifer manipuliert werden kann, wogegen ein Lesebefehl die integritätsgeschützte Information zurückgibt.

8. Die Hostapplikation liest die Referenzdaten einschließlich der Signatur und prüft über die Signatur die Authentizität der Referenzdaten sowie die Zugehörigkeit der Referenzdaten zur Card_ID.

9. Nun fordert die Hostapplikation über das Display den Nutzer auf, seine biometrischen Daten zu präsentieren und liest die aktuellen Daten vom Biosensor. Aus den Rohdaten wird ein biometrisches Template generiert. Die Hostapplikation vergleicht das Referenztemplate mit dem aktuellen biometrischen Template und kann bei einem fehlgeschlagenen Matching diesen Vorgang noch zweimal wiederholen lassen. Er fordert erneut aktuelle Daten vom Biosensor an, generiert ein neues Template und vergleicht dieses mit dem Referenztemplate. Dadurch bekommt der Anwender die Möglichkeit, seine biometrischen Daten besser zu präsentieren.

10. Nach drei fehlgeschlagenen Versuchen löscht die Hostapplikation in seinem Applikationsspeicher alle biometrischen Daten und zeigt den fehlgeschlagenen Versuch an. Weitere Versuche sind vom Startpunkt aus möglich, bis der FBZ2 keine weiteren Versuche zulässt.

11. Bei einem erfolgreichen Match wird der FBZ2 wieder auf die maximal mögliche Anzahl biometrischer Verifikationsversuche gesetzt. Die Hostapplikation löscht alle biometrischen Daten und zeigt das positive Ergebnis an und gibt es an die rufende Anwendung zurück.

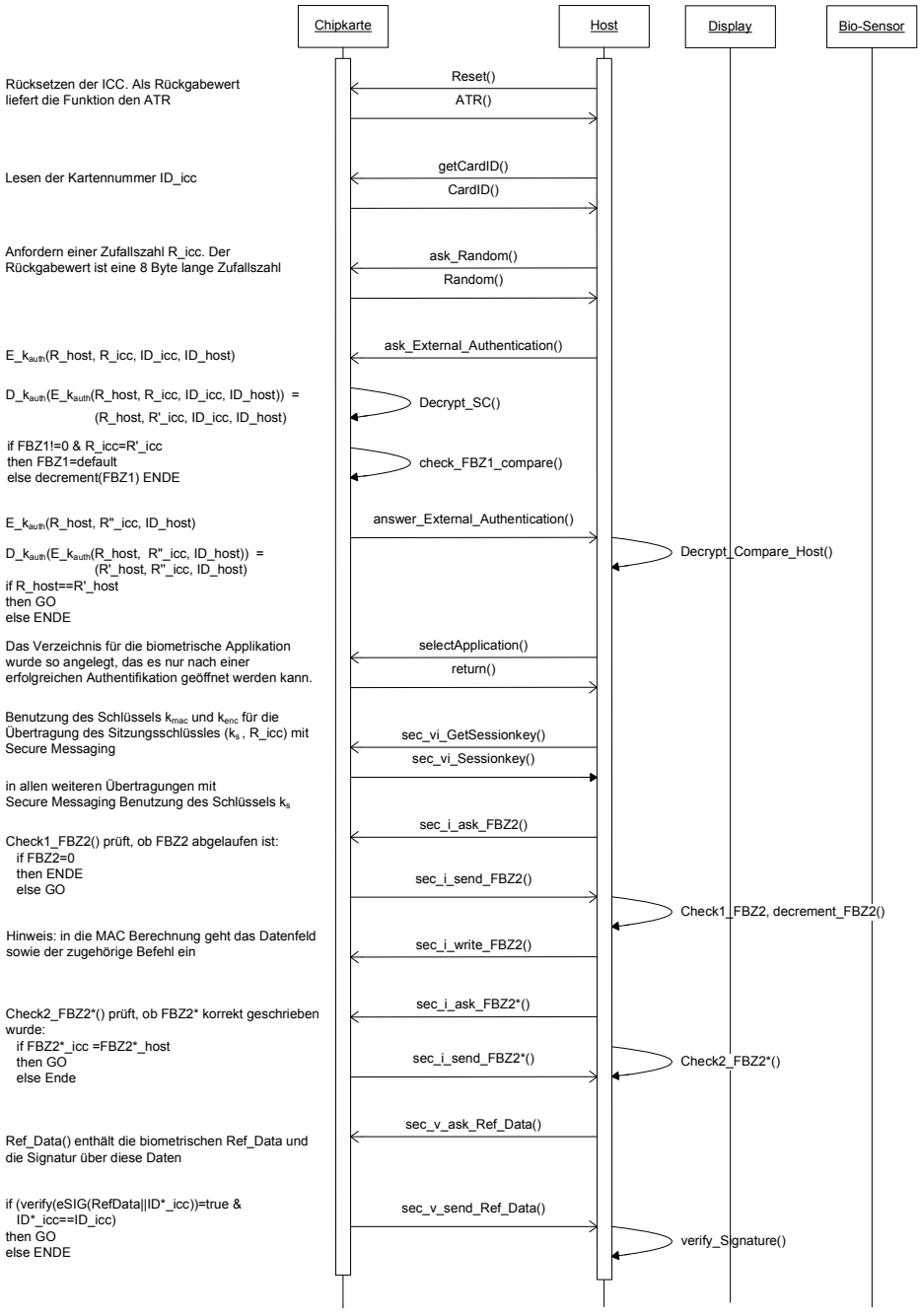

Abbildung 2: Sequenzdiagramm CBI-System (Teil 1)

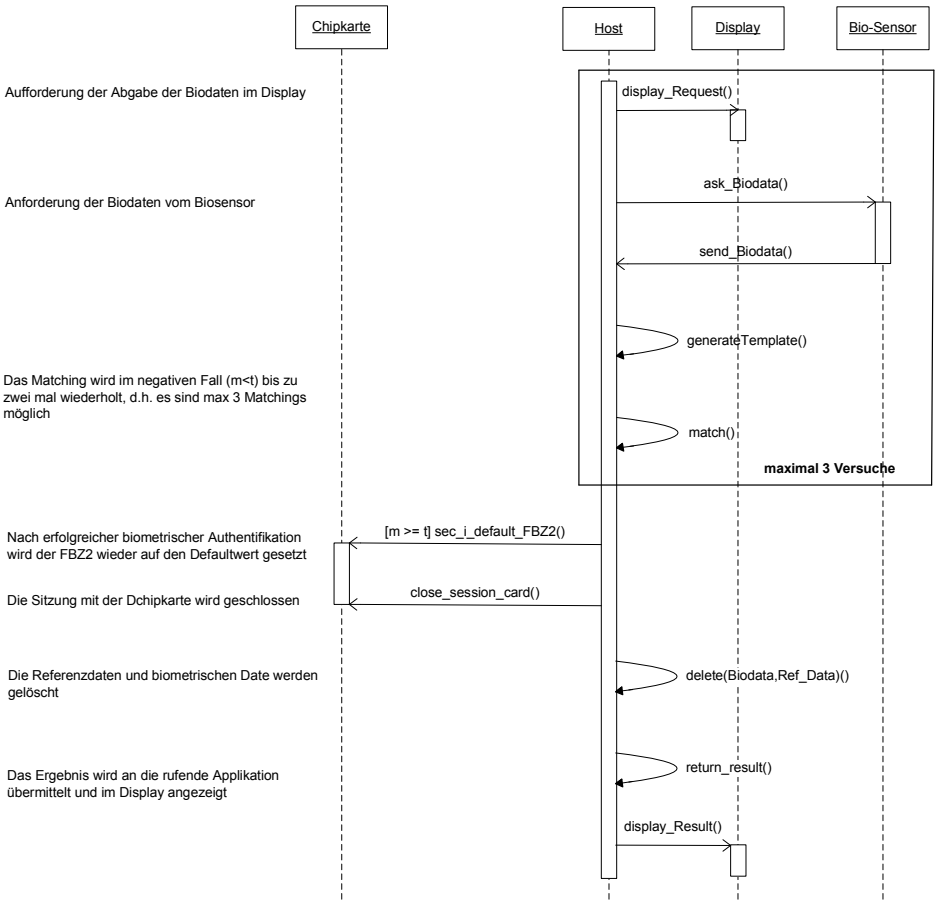

Abbildung 3: Sequenzdigramm CBI-System (Teil 2)

Der FBZ1 wird durch das Betriebssystem TCOS2.0 auf der Chipkarte verwaltet. Er kann durch die Applikation nicht beeinflusst werden. Ist dieser FBZ1 abgelaufen, ist kein Zugriff auf die Applikationsdaten mehr möglich. Lediglich ein Administrator kann nach Präsentation der Administrator-PIN den FBZ1 auf eine Defaultwert zurücksetzen. Der FBZ2 wird durch die Hostapplikation verwaltet. Über den Stand und Status (z.B. abgelaufen) und die Reaktion darauf entscheidet ausschließlich die Hostanwendung. Das File mit dem Referenzdaten und der Signatur wird als nur lesbares File implementiert. Durch Präsentieren weiterer Geheimnisse z.B. einer PIN (Administrator) kann es während einer Personalisierungsphase auch neu beschrieben werden. Der Modus „Secure Messaging“ nach ISO 7816-4 hat zum Ziel, die Kommunikation zwischen Hostapplikation und Chipkarte mit Hilfe der Sicherheitsmechanismen *Verschlüsselung* und *Message Authentication Code (MAC)* zu schützen. Damit können die Schutzziele Vertraulichkeit und Integrität erreicht werden. Im Sequenzdiagramm ist dieser Modus mit sec_... gekennzeichnet.

Für die zu übertragenden Daten im CBI-System sind unterschiedliche Sicherheitsanforderungen zu unterscheiden. Der FBZ2 ist kein vertrauliches Datum. Es genügt die Forderung der Integrität, was das Datum selbst sowie den zugehörigen Befehl (read, write) umfasst. Im Sequenzdiagramm wird die Notation sec_i_... gewählt. Die Referenzdaten sind dagegen gemäß den formulierten Sicherheitsanforderungen vertrauliche Daten, weshalb eine verschlüsselte Übertragung notwendig ist. Da die Daten bereits eine elektronische Signatur besitzen, kann auf einen Integritätsschutz verzichtet werden. Im Sequenzdiagramm wird dazu die Notation sec_v_... gewählt. Die Übertragung des Sitzungsschlüssels k_s wiederum erfordert eine vertrauliche sowie integritätsgeschützte Kommunikation, die mit sec_vi_... bezeichnet wird. Es ist zu beachten, dass die Chipkarte und der Host als gemeinsames Geheimnis drei symmetrische Schlüssel teilen, einen Authentisierungsschlüssel k_{auth}, einen Verschlüsselungsschlüssel k_{enc} und einen MAC-Schlüssel k_{mac}. Der Schlüssel k_{auth} dient der gegenseitigen Authentifizierung und die Schlüssel k_{enc} und k_{mac} der vertraulichen und integeren Übertragung des Sitzungsschlüssels. Hierbei geht in die Verschlüsselung und MAC Bildung des Sitzungsschlüssels k_s zusätzlich die von der Chipkarte bereits am Protokollanfang benutzte Zufallszahl aus der Authentifizierung ein. Dadurch wird die Bindung des Sitzungsschlüssels an die aktuelle Sitzung erreicht. Nach der Übertragung des Sitzungsschlüssels wird in den folgenden Schritten im Modus Secure Messaging ausschließlich der Sitzungsschlüssel benutzt.

4 Überwindungsszenarien / Restrisiko

In diesem Kapitel werden verschiedene Überwindungsszenarien betrachtet, um ein größeres Verständnis für die gewählten Sicherheitsanforderungen und –maßnahmen zu vermitteln. Es gibt zwei Sicherheitsbedürfnisse zu unterscheiden. Ein Host will lediglich berechtigten Nutzern Zugang gewähren, und eine Chipkarte will lediglich berechtigten Hosts den Zugriff auf die Referenzdaten gewähren. Es werden im Folgenden erst die Bedrohungen beschrieben und anschließend die entgegenwirkenden Maßnahmen des CBI-Systems diskutiert.

A.1. Ein Angreifer präsentiert einem beliebigen CBI-System seine biometrischen Daten über den biometrischen Sensor.

A.2. Ein Angreifer kommt in den Besitz einer Chipkarte. Es ist weiterhin vorausgesetzt, dass der Angreifer den Eigentümer sowie die für die Chipkarte zugelassenen Rechner kennt. Der Angreifer wird nun versuchen, biometrische Daten dem CBI-System zu präsentieren. Zu dieser Art Angriff gehört auch der Typus “Innentäter bei günstiger Gelegenheit“: Der Eigentümer hat eine gültige Karten gesteckt, wird abgelenkt und der Angreifer präsentiert seine eigenen biometrischen Daten.

A.3. Ein Angreifer kommt in den Besitz einer Chipkarte. Es ist weiterhin vorausgesetzt, dass der Angreifer den Eigentümer kennt, ihm jedoch die für die Chipkarte zugelassenen Rechner unbekannt sind. Der Angreifer kann nun versuchen, biometrische Daten dem CBI-System eines beliebigen Rechners zu präsentieren.

A.4. Ein Angreifer kommt in den Besitz einer Chipkarte. Er schafft es weiterhin, den auf der Karte gespeicherten geheimen Schlüssel zu ermitteln. Er könnte somit eine neue gültige Chipkarte generieren, auf die er sein eigenes Referenztemplate einspielt. Der Angreifer präsentiert diese Karte und seine eigenen Biometrischen Daten dem Zielrechner.

A.5. Ein Angreifer kommt in den Besitz einer Chipkarte. Es ist weiterhin vorausgesetzt, dass der Angreifer den Eigentümer sowie die für die Chipkarte zugelassenen Rechner kennt. Nun klemmt der Angreifer den biometrischen Sensor ab und überspielt an dessen Stelle die biometrischen Daten, die je nach Aufwand mehr oder weniger ähnlich mit den Daten des Eigentümers sind oder aus einer vorangegangenen Session abgelauscht wurden. Damit könnte eine vom biometrischen Sensor umgesetzte Lebenderkennung umgangen werden. Diese Angriffe werden auch Replay-Angriffe genannt.

A.6. Der Angreifer unterdrückt die Meldung des Prüfergebnisses des CBI-Systems und meldet selbst positive Authentifikation. Er umgeht den gesamten Authentifikationsprozess.

A.7. Der Angreifer versucht, einen Nutzer mit ihm ähnlichen biometrischen Daten zu finden. Dazu zapft er die Leitung zum Biosensor an. Bei einem Authentifizierungsversuch eines berechtigten Nutzers präsentiert er nichtdeterministisch die eigenen biometrischen Daten dem Host. Führt die zu einer erfolgreichen Authentifikation, versucht der Angreifer die entsprechende Karte zu identifizieren und später zu entwenden.

Die genannten Überwindungsszenarien werden teilweise durch die im CBI-System umgesetzten Sicherheitsmaßnahmen verhindert oder erschwert. Das Szenario A.1 wird verhindert, da keine notwendige Chipkarte vorhanden ist. Die Szenarien A.2, A.3, A.4 und A.5 sind lediglich möglich, wenn der Angreifer im Besitz einer gültigen Chipkarte ist. Eine gültige Chipkarte kann durch Sperrung des zugehörigen geheimen Schlüssels zurückgezogen werden. Damit sind die genannten Szenarien nicht durchführbar. Für den Fall, dass ein Angreifer in den Besitz einer gültigen Chipkarte gelangt, sind für den biometrischen Verifikationsprozess drei Fälle zu unterscheiden:

- Der Angreifer hat eine durchschnittliche FAR.
- Der Angreifer hat rein zufällig die 10-fache FAR.
- Der Angreifer betreibt mittleren Aufwand beim Nachmachen der biometrischen Daten vom berechtigten Nutzer.

Die *False Acceptance Rate* ist der empirische Wert, dass ein unberechtigter Nutzer als berechtigter Nutzer erkannt wird, d.h. seine biometrischen Daten hinreichend mit den Referenzdaten übereinstimmen. Dieser Wert bezieht sich auf einen einzelnen Versuch. Die Mehrzahl der biometrischen Systeme räumt den Nutzern mehrere oder sogar beliebig viele Versuche ein. Die FAR ein und desselben biometrischen Systems ändert sich jedoch mit der Anzahl der Versuche vorausgesetzt, mit jedem Versuch werden statistisch unabhängige Merkmale verwendet. Die Änderung der *FAR* für *n* Versuche kann wie

folgt angegeben werden: $FAR_n = 1-(1-FAR)^n$. D.h. sind bei einem biometrischen System mehrere Versuche zugelassen, so steigt mit jedem weiteren zugelassenen Versuch die FAR bei gleichzeitiger Verminderung der *False Rejection Rate (FRR)*. Es fällt also die Sicherheit und es steigt der Komfort. Wird kein biometrischer Fehlbedienungszähler eingesetzt, wird zwar irgendwann jeder berechtigte Nutzer erkannt, aber auch viele unberechtigte Nutzer. Im CBI-System steht einem Angreifer nur eine endliche Anzahl von Versuchen zur Verfügung. Die Anzahl ergibt sich aus der Höhe des biometrischen Fehlbedienungszählers (z.B. 5) und den dreimaligen biometrischen Verifikationsversuchen je Authentifikation. Im genannten Beispiel würden dem Angreifer in den Szenarien A.2 und A.3 demnach maximal 15 Verifikationsversuche erlaubt sein. Danach führen der Host und alle anderen berechtigten Hosts für die Chipkarte keine Verifikationen mehr durch. Unberechtigte Hosts werden von der Chipkarte bereits bei der gegenseitigen Authentifizierung abgewiesen (siehe unten). Damit ergibt sich für das CBI-System mit z.B. einem biometrischen Fehlbedienungszähler von 5 und einer *FAR* von 0.1% eine absolute FAR_{15} von 1.49%. Es ist zu beachten, dass sich diese Zahlen auf einen Angreifer mit durchschnittlicher FAR beziehen. Sie können sich erheblich erhöhen, wenn der Angreifer eine überdurchschnittliche FAR besitzt. Mit dem biometrischen Fehlbedienungszähler kann allerdings eine absolute FAR für ein konkretes System angegeben werden.

Wenn der gewählte Rechner nicht zu denen für die Chipkarte berechtigten Hosts gehört, wird ein fehlgeschlagener Authentifizierungsversuch von der Chipkarte registriert, der zur Sperrung der Chipkarte führen kann. Die Auswertung dieses Authentikations-Fehlbedienungszählers der Chipkarte ist optional und wird von der Sicherheitsstrategie festgelegt. Der FBZ1 dient dem Vereiteln des „Ausprobierens“ eines Zugangs zu einem nichtberechtigten Rechner durch den berechtigten sowie unberechtigten Nutzer. Ist der FBZ1 z.B. auf 10 gesetzt, so hat der Angreifer aus A.3 genau 10 Versuche einen berechtigten Rechner zu finden. Der Angreifer muss mit Szenario A.2 fortfahren. Bei dem Zugangsversuch A.4 würde das selbstgenerierte Referenztemplate aufgrund der fehlenden Signatur vom Host abgewiesen werden. Weiterhin dient die Signatur der Bindung der Nutzeridentität und der Chipkarten-ID an das Referenztemplate. Damit kann verhindert werden, dass ein zugelassener Nutzer mit einer gültigen Chipkarte mit geringen Zugangsrechten seine darauf befindlichen signierten Referenzdaten ausliest und auf eine Chipkarte mit hohen Zugangsrechten einspielt. Das bedarf zusätzlich der Simulierung eines Hosts, um in den Besitz gültiger Referenzdaten zu kommen, was mit der Voraussetzung einer kompromittierten Chipkarte möglich ist. Dieser Angriff ist ein Spezialfall von A.4. Im Szenario A.5 hat der Angreifer Zugang zur Verbindung zwischen dem biometrischen Sensor und dem Host. Im CBI-System sind keine Sicherheitsmaßnahmen für diese Verbindung entwickelt worden. Damit ist ein solcher Angriff möglich mit der Voraussetzung, dass die Chipkarte noch nicht als ungültig markiert wurde. Auch der Angriff A.6 wird durch das CBI-System nicht abgewehrt. Hier sind Maßnahmen auf dem Zugangsrechner zu treffen. Weiterhin nutzt der Angriff A.7 die Ablauschmöglichkeit an der genannten Verbindung und ist als Vorbereitung für Angriff A.2 zu sehen. Dieser Gruppe von Angriffen kann durch bauliche Maßnahmen begegnet werden. Für das Beispiel einer Zutrittskontrolle sind mindestens der Host und der biometrische Sensor in einer Tamper-Proofed Box zu integrieren.

5 Schlussfolgerungen

Mit der Einführung des biometrischen Fehlbedienungszählers wird der klassische Hauptangriff, d.h. der Angreifer „findet“ eine Karte und probiert in das System zu kommen, zu einem sehr hohen Risiko für den Angreifer. Trotzdem wird der Normalnutzer, der ab und zu nicht erkannt wird, nicht stärker belästigt als in einem reinen biometrischen System. Zusätzlich werden die Datenschutzbestimmungen auf hohem Niveau eingehalten: Nur wenn sowohl Host und als auch Karte Ihre Vertrauenswürdigkeit bewiesen haben., werden die biometrischen Daten freigegeben und unter dem Schutz der Verschlüsselung ausgetauscht. Wenn der Nutzer die Nachricht der erfolgreichen Authentifikation erhält, kann er sicher sein, dass seine Biometriedaten im Host schon wieder gelöscht sind.

6 Zusammenfassung und Ausblick

Ein biometrisches Erkennungsverfahren allein ist nichtdeterministisch und nicht stärker als etwa ein Passwortverfahren (Anwendung des Bewertungsschemas nach E-Governmenthandbuch des BSI [BSI05]). Dagegen leidet ein Chipkartenverfahren darunter, dass immer die Chipkarte und nicht deren Besitzer Endpunkt der Authentifikation ist. Diese spezifischen Schwächen der Einzelverfahren können mit dem vorgelegten Protokoll nicht nur ausgeglichen werden, sondern durch das verschachtelte Zusammenspiel wird ein höheres Sicherheitsniveau und die strikte Einhaltung des Datenschutzes sowie ein besserer Komfort erreicht.

In der Zukunft werden wir im Alltag von verschiedenen Chipkarte-Biometrie-Systemen umgeben sein. Deutschland beginnt die Ausgabe der neuen biometriegestützten Reisepässe ab dem 1. November 2005. Im Chip der Reisepässe wird zunächst ein digitales Foto gespeichert. Ab März 2007 werden in den neuen Pässen zusätzlich zwei Fingerabdrücke gespeichert. Dabei wird die Biometrie zwar, wie in dieser Arbeit, dezentral auf dem Chip als Template-On-Card System gespeichert, die Protokolle sind aber mehr auf die staatlichen Belange ausgerichtet. Dabei haben wir mit dieser Arbeit gezeigt, dass es kaum einen Mehraufwand erfordert, auch die Chipkarte die Prüfumgebung prüfen zu lassen und die Biometriedaten erst in bewiesen sicherer Umgebung freizugeben. Hoffnung macht, dass vor Jahren auch die zentrale Speicherung als „technisch zwingend“ angesehen wurde und diese Ansicht inzwischen obsolet ist [ICAO03, ICAO04, KK05]. Die natürliche Weiterentwicklung unseres Systems wäre der verstärkte Einsatz von asymmetrischen Verfahren, Einführung einer Authentifizierung des Biosensors sowie die gesicherte Übertragung der aktuellen biometrischen Daten [WSE04][RS05].

Literaturverzeichnis

[BA03] Brömme, A.; Al-Zubi, S.: Multifactor Biometric Sketch Authentication. GI BIOSIG 2003, Darmstadt, Germany, Juli 2003.

[BAI05] Biometric Associates Inc., Self-Authenticating Biometric SmartCard, http://www.biometricassociates.com (Abruf 10.09.2005)

[BEM02] The Biometric Evaluation Methodology Working Group: Common Methodology for Information Technology Security Evaluation. Version 1.0, August 2002.

[Br05] Bromba, M: Examples for Prototyping, http://www.bromba.com/protoe.htm#Karte (Abruf 10.09.2005)

[BSI05] Bundesamt für Sicherheit in der Informationstechnik (BSI): E-Government-Handbuch, 4. Ergänzungslieferung, Bundesanzeiger Verlag, Köln, 2005.

[CLRS05] Cheikhrouhou, L., Lassmann, G., Rock, G.; Schwan, M.: Verisoft – Beweisen als Ingenieurwissenschaft. T-Systems International University Conference, Düsseldorf, 10.-11.10.2005, Tagungsband wird in Buchform erscheinen.

[G&D05] Giesecke&Devrient, Whitepaper on smart cards and biometrics, Februar 2003. http://www.gi-de.com (Abruf 10.09.2005)

[ICAO03] International Civil Aviation Organisation (ICAO): PKI Digital Signatures for Machine Readable Travel Documents. Version 4.0, 2003.

[ICAO04] International Civil Aviation Organisation (ICAO): Biometric Deployment of Machine Readable Travel Documents. Version 2.0, 2004.

[KK05] Kügler, D., Kelter, H.: Risiko Reisepass? Schutz der biometrischen Daten im RF-Chip. c't 05/05, Heise Verlag, pp 84ff, 2005.

[La02a] Lassmann, G.: Some results on robustness, security and usability of biometric systems. IEEE International Conference on Multimedia and Expo, Lausanne, 26-29.8. 2002.

[La02b] Lassmann, G. (Hrsg.): Bewertungskriterien zur Bewertung und Vergleichbarkeit biometrischer Verfahren. TeleTrusT Deutschland e.V., Arbeitsgruppe 6, Version 2.0, 2002.

[Ma03] Maltoni, D.; Maio D.; Jain A.; Prahbaker S.: Handbook of Fingerprint Recognition. Springer-Verlag New York, 2003.

[NL02] Nolde, V.; Leger, L. (Hrsg.): Biometische Verfahren,. Kapitel: Erfahrungen mit Biometrischen Systemen, Giesecke/Kalo/Laßmann, Dt. Wirtschaftsdienst, Köln, 2002.

[RS05] Reiner-SCT, cyberJack® biometric, Standards: HBCI, Digitale Signatur, Sicherheitsklasse 3,http://www.reiner-sct.de/produkte/biometric.php (Abruf 10.09.2005)

[SCA02] Smart Cards Alliance: Smart Cards and Biometrics in Privacy-Sensitiv Secure Personal Identification System. White Paper, May 2002.

[WSE04] Waldmann, U.; Scheuermann, D.; Eckert, C.: Protected transmission of biometric user authentication data for oncard-matching. Proceedings of the 2004 ACM symposium on Applied computing, ACM Press New York, pp425-430, 2004.

[Ver05] Verisoft Teilprojekt 4: Biometrisches Identifikationssystem, http://www.verisoft.de/TeilProjekt4.html (Abruf 10.09.2005)