Biometrische Nachrichten-Authentisierung

Christoph Busch[1,2], Daniel Hartung[2]

[1] Hochschule Darmstadt - CASED
[2] Norwegian Information Security Laboratory (NISlab)
Teknologiveien 22, 2821 Gjøvik, Norwegen
christoph.busch@hig.no
daniel.hartung@hig.no

Abstract: Bei vielen Anwendungen ist die Integrität und Authentizität übertragener Nachrichten von Interesse. So sind zum Beispiel im Online-Banking sind die relevanten Informationen i) welches Empfänger–Konto eine Gutschrift erhält, ii) welcher Betrag dem Empfänger gutgeschrieben werden soll, iii)) welches Sender-Konto eine Belastung erhält und schließlich iv) welche natürliche Person die Transaktion initiiert und die Transaktionsdaten bestätigt hat. In derzeitig eingesetzten Protokollen sind die Informationen i), ii) und iii) vielfach nur ungenügend geschützt. In keinem der derzeitigen Protokolle wird die Information iv) ausreichend gesichert. Das hier vorgestellte Protokoll zur Biometrischen Nachrichten-Authentisierung realisiert eine Daten-Authentisierung und gleichzeitig eine Personen-Authentisierung. Damit wird eine starke Bindung zwischen einer natürlichen Person und den anderen relevanten Informationen hergestellt und somit für den Ausführenden der Transaktion gesichert nachgewiesen, dass tatsächlich eine berechtigte natürliche Person die Transaktion initiiert und bestätigt hat.

1 Bedrohungen und Vorfälle mit Identitätsmissbrauch

Ein Identitätsmissbrauch ist definierbar als Nutzung des Identitätsdiebstahls zum Schaden der betroffenen Person, wobei das vorrangige Interesse des Angreifers in aller Regel eine finanzielle Bereicherung ist. Das Risiko, Opfer eines solchen Ereignisses zu werden, ist in den vergangenen Jahren dramatisch gestiegen. Das Identity Theft Resource Center berichtet für das Jahr 2008 eine Zunahme von 47% im Vergleich zum Vorjahr [Idtc2009a]. Die Liste der Einzelvorfälle dokumentiert zum Beispiel Kreditkartenbetrug, Kontenraub und Bankbetrug und zeigt die zur Beschaffung der notwendigen Informationen eingesetzte Spannbreite von Angriffen. Diese reichen von manipulierten Kartenlesern über Phishing-Angriffe bis hin zu ausgefeilten Social-Engineering-Angriffen, die zur unbedachten Preisgabe von sensitiven Daten motivieren. Diese Gefahren sind auch für Deutschland ein größer werdendes Problem, wie die Statistiken des Bundeskriminalamtes belegen [Bka2008]. Eine Studie des Bundesamtes für Sicherheit in der Informationstechnik prognostiziert, dass die Angriffsszenarien in Zukunft deutlich vielfältiger werden [Bsi2010]. Das Potential für Angriffe steigt durch die zunehmende Nutzung von Online-Banking-Diensten. In Deutschland gab es beispielsweise in den letzten Jahren eine Steigerung von 15 Millionen Online-Konten im Jahr 2000 auf 39 Millionen Online-Konten im Jahr 2008 [Bdb2006], [Grud2009]. Nach einer Studie des BITKOM haben sieben Prozent aller Internet-Nutzer über 14 Jahren

bereits einen finanziellen Schaden beispielsweise durch Viren, bei Online-Auktionen oder Online-Banking erlitten [Bit2008]. Neben Online-Banking Transaktionen sind auch andere sicherheitskritische Anwendungen bedroht, wie beispielsweise die authentische Kommunikation zwischen Einsatzeinheiten eines Krisenstabes im Katastrophenmanagement. Insbesondere bei der Koordination von Einheiten, die ad hoc an einem Katastrophenort zusammengezogen werden wie etwa bei einer terroristisch bedingten Katastrophe ist es essentiell, dass die Authentizität von Nachrichten für den Empfänger einer Handlungsanweisung nachweisbar wird.

Nach dem letzten Lagebericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) geht die Bedrohung weniger von Phishing-Angriffen aus [Bsi2009]. Die Bedrohung wächst vielmehr durch die immer ausgereifteren Mechanismen von bösartiger Software (Malicious Software – Malware), die über verschiedenste Kanäle auf privaten Rechnern installiert wird und dort - ohne Kenntnis des Endanwender - Informationen über verwendete Programme und Nutzdaten wie etwa Finanz-Transaktionen aufzeichnet und an einen entfernten Steuerrechner über das Internet weiterleitet. Zu diesen Malware-Arten zählen Computer-Viren und Trojanische Pferde. Die dabei zum Einsatz kommende Malware ist für das Opfer nur in seltenen Fällen erkennbar. Dies liegt einerseits daran, dass sie ausgefeilte Mechanismen wie Selbstverschlüsselung und Mutation verwenden und somit beim Abgleich mit den Virenmustern in Datenbanken der Anti-Virenhersteller unerkannt bleiben. Andererseits werden Mechanismen wie Rootkits eingesetzt, die das Betriebssystem selbst unterwandern und mit heutigen Methoden kaum zu detektieren sind [Rut2006].

2 Biometrische Authentisierung

Unter Biometrie versteht man ein Messverfahren zur Wiedererkennung von Personen. Die Internationale Standardisierung definiert den Begriff *biometrics* wie folgt: "*automated recognition of individuals based on their behavioural and biological characteristics*" [Iso-sc37]. Biometrische Verfahren analysieren demnach das Verhalten des Menschen und/oder eine Eigenschaft der biologischen Charakteristika. Die biologischen Charakteristika gliedern sich einerseits in anatomische Charakteristika, die geprägt werden durch Strukturen des Körpers und andererseits in physiologische Charakteristika, die geprägt werden durch Funktionen des Körpers wie beispielsweise die Erkennung der Stimme. Der Vorgang der biometrischen Authentisierung bedingt, dass grundsätzlich eine Person vorab eingelernt wurde (Enrolment), um die notwendigen Referenzdaten zu bilden. Biometrische Authentisierungsverfahren werden in sicherheitsrelevanten Anwendungen substituierend oder ergänzend zu anderen Authentisierungsfaktoren wie Wissens-Authentisierung (Passwort) oder Besitz-Authentisierung über Token (Schlüssel) eingesetzt, um deren Nachteile zu kompensieren. Passworte und Token können – meist unter Missachtung einer Sicherheitsrichtlinie – weitergeben werden, sie werden vergessen oder verloren. Um bei der ansteigenden Zahl der logischen und physikalischen Zugangskontrollen dem Verlust vorzubeugen, werden oft ungeeignete Speicherorte oder identische Passworte verwendet. Im Gegensatz dazu können biometrische Charakteristika nicht vergessen gehen und naturgemäß ist keine Delegation möglich.

2.1 Sicherheit biometrischer Systeme

Die Bedrohungen der Sicherheit biometrischer Systeme und geeignete Schutzmaßnahmen sind aus der Literatur hinreichend bekannt. Mögliche Angriffe sind denkbar auf den biometrischen Sensor und auf die gespeicherten Referenzdaten [Iso-sc27]. Die Robustheit des Sensors ist vor allem in einem nicht-überwachten Anwendungsumfeld von Bedeutung; die Sicherheit des Gesamtsystems erfordert, dass von einem Angreifer präsentierte Plagiate (z.B. Gummifinger) einer biometrischen Charakteristik zuverlässig als solche erkannt werden. Alternativ können biometrische Modalitäten wie etwa die Venenerkennung zum Einsatz kommen, bei denen die erfolgreiche Produktion eines Plagiates als unwahrscheinlich eingestuft werden kann.

Aus der Sicht einer Betroffenen Person ist die Sicherheit eines biometrischen Systems jedoch auch verbunden mit den Maßnahmen zum Schutz der biometrischen Referenzdaten. Erwartet werden technische Maßnahmen, die es ermöglichen, Referenzdaten zurückzurufen, einen Querbezug zwischen verschiedenen Anwendungen zu verhindern und potentiell in der biometrischen Charakteristik enthaltene Zusatzinformationen nicht zugänglich werden zu lassen. Zur Lösung dieser Anforderungen gibt es verschiedene Ansätze des *Biometric Template Protection* [Bre2008], die das Speichern von Bild- oder Templatedaten in einer Datenbank entbehrlich machen. Ein bereits kommerziell eingesetztes Verfahren ist das *Helper-Data-Schema* [Tak05], das im Folgenden skizziert wird.

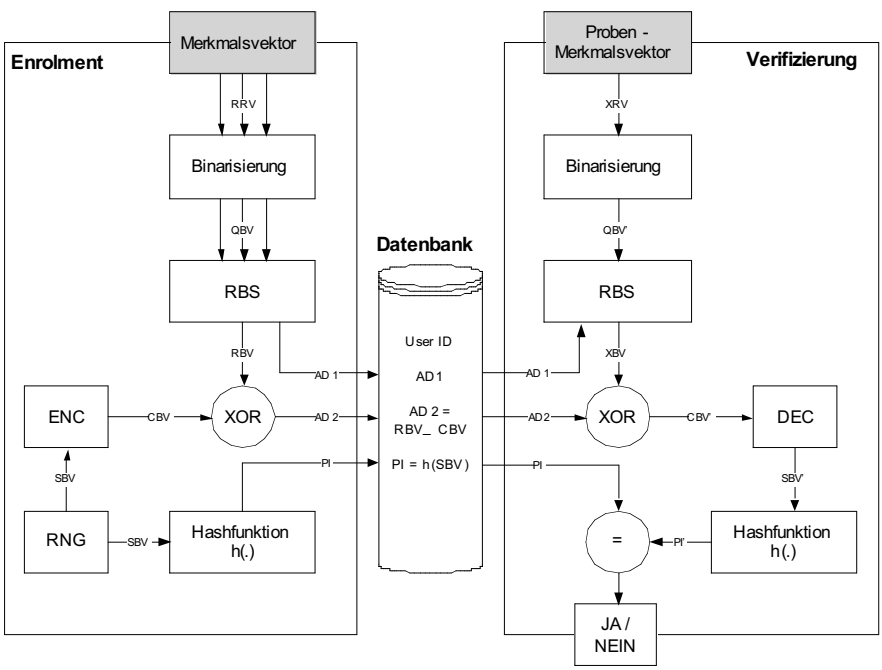

Abbildung 1: Helper-Data-Schema zum Schutz biometrischer Referenzdaten

Um die biometrische Erkennungsleistung zu steigern, wird im Helper-Data-Schema ein Reliable-Bit-Selector (RBS) verwendet. Ein biometrischer Enrolment- und Verifikationsprozess kann in der Folge durch folgende Funktionsblöcke und Variablen beschrieben werden:

2.2 Funktionsblöcke

- Binarisierung – transformiert realwertigen Merkmalsvektor in binäre Form
- RBS – Reliable-Bit-Selector (Analysiert Binärvektor nach stabilen Elementen)
- ECC (ENC/DEC) – Fehlerkorrektur-Block (z.B. BCH-Code) Encoding/Decoding
- XOR – XOR-Operation auf Binärvektoren
- Hashfunktion $h(.)$ – Funktion zur Erzeugung von Hashwerten

2.3 Variablen

- RRV / XRV – realwertiger Merkmalsvektor (Referenz / Probe)
- QBV / QBV‘ – quantisierter Merkmalsvektor
- RBV / XBV – binärer Merkmalsvektor bestehend aus geeigneten Komponenten
- SBV – binärer Zufalls-Geheimnisvektor
- CBV – binärer Codevektor (um Fehlerkorrektur erweitertes SBV)
- AD1 – Auxilliary Data 1: Datensubjekt-spezifischer Indexvektor der geeigneten Komponenten (Reliable Bit Indizes) generiert in RBS
- AD2 – Auxiliary Data 2: berechnet aus Geheimnis SBV und biometrischen Daten (AD2 = RBV XOR CBV)
- PI – Pseudo-Identifikator berechnet aus dem Hashwert $h(.)$ über dem subjekt- und applikations-spezifischem Geheimnisvektor SBV
- Anmerkung: Ein Hochkomma‘ deutet veränderte Version einer Variable an (hervorgerufen durch biometrisches oder sensorbedingtes Rauschen)

Wie in klassischen biometrischen Systemen unterscheiden wir zwei Phasen: Die Registrierungsphase (Enrolment) und die eigentliche Verifikationsphase.

Zum biometrischen Enrolment sind für das Helper-Data-Schema (HDS) mehrere Präsentationen einer biometrischen Charakteristik erforderlich, so dass Merkmalvektoren gleicher Länge gebildet werden können und als Eingabe für das HDS dienen. Im HDS wird eine binäre Repräsentation durch Quantisierung der biometrischen Daten erzeugt. Die entstandenen quantisierten Binärvektoren werden im Reliable-Bit-Selector-Block (RBS) analysiert, diesmal um Positionen in den Vektoren zu identifizieren, an denen sich Bits befinden, die sich einerseits vom Mittel aller Vektoren der Population unterscheiden aber auch stabil und somit reproduzierbar für ein Subjekt in den Merkmalen vorkamen. Der Binärvektor RBV der die |AD1| stabilsten Komponenten enthält, wird nun mit einem Binärvektor CBV gleicher Länger kombiniert, der im zweiten Prozess generiert wird.

In einem parallelen zweiten Prozess wird ein Zufallszahlengenerator (RNG) genutzt um einen binären Geheimnis-Vektor SBV zu erzeugen. Der Hashwert $h(.)$ dieses Vektors wird in der Datenbank gespeichert, ein Berechnen von SBV aus h(SBV) ist somit nicht möglich ohne die Hashfunktion zu brechen. Dieser Wert kann als Pseudo-Identifikator (PI) betrachtet werden. SBV wird nun zusätzlich mit dem Binärvektor aus dem ersten Prozess wie folgt verknüpft: Ein Fehlerkorrekturverfahren (ECC-Encoder ENC, z.B. BCH-Codes) wird genutzt um SBV resistent gegen Einzelbitfehler zu machen, die durch die Variation in der biometrischen Probe verursacht werden. Die Kapazität lässt sich leicht variieren, je mehr Fehler korrigiert werden können sollen, desto niedriger ist der Anteil von SBV in dem entstehenden Codewort CBV. Der Fehlerkorrekturcode wird so gewählt, dass CBV und der Binärvektor RBV die gleiche Länge haben. Eine XOR-Verknüpfung dieser beiden Vektoren sorgt dafür, dass ohne das Wissen eines der beiden Eingaben kein Rückschluss auf die andere Eingabe gemacht werden kann.

Soll eine Verifikation stattfinden, wird der Datensatz eines Nutzers (AD1, AD2, PI=h(SBV)) geladen und ein frischer Probenvektor XRV verarbeitet. Der Binarisierungs -Block erzeugt daraus den Binärvektor QBV‘. Die Bits an den Positionen die in AD1 gespeichert sind werden durch den RBS-Block extrahiert, so entsteht der Binärvektor XBV. Dieser Vektor sollte bei gleichem Datensubjekt dem Vektor RBV aus der Registrierungsphase sehr ähnlich sein. Durch die erneute XOR-Operation auf AD2 und XBV entsteht CBV‘. Wenn die Hamming-Distanz der Codeworte CBV und CBV‘ kleiner ist als die Kapazität des Fehlerkorrekturverfahrens und wenn die Fehler Einzelbitfehler sind, kann SBV‘=SBV im Fehlerkorrektur-Block (DEC) rekonstruiert werden. Die Entscheidung, ob die Verifikation positiv ist, ergibt der Vergleich von PI‘=h(SBV‘) und dem gespeicherten Wert PI=h(SBV).

Um eine Revokation einer biometrischen Referenz durchzuführen, muss ein neuer Geheimnis-Vektor SBV generiert werden, der mit einem frischen Merkmalsvektor (nach Binarisierung und RBS) kombiniert wird. Lediglich AD2 und PI müssen erneut in der Datenbank als Referenz gespeichert werden.

3 Transaktions-Absicherung

Bisher werden für Online-Transaktionen eine Reihe von Verfahren eingesetzt, die als nicht ausreichend sicher eingestuft werden müssen bzw. ungewollt eine Delegation der Authentisierungsfaktoren erlauben. Dieser Abschnitt liefert eine Übersicht bekannter Verfahren. Eine vertiefte Diskussion und Sicherheitsanalyse der gegenwärtig eingesetzten Authentisierungsverfahren im Online-Banking findet sich in [Asit08].

PIN/TAN: *Zwei-Faktoren-Authentisierung* mit Persönlicher Identifikationsnummer (PIN) und Transaktionsnummer (TAN), wobei sich die zu verwendenden TAN’s im Besitz des Bank-Kunden befinden sollen und nach Verwendung (d.h. einer Transkation / Buchung) aus einer Papierliste ausgestrichen werden.

PIN/iTAN: Um die Gefahr durch Phishing Angriffe zu reduzieren, wird seit 2006 eine indizierte TAN-Liste verwendet, so dass der Bank-Kunde vom Bank-Server in der Online-Sitzung aufgefordert wird zur Autorisierung einer gewünschten Transaktion eine bestimmte TAN zu verwenden, deren Index (Position) in einer nummerierten Liste von TANs dem Bank-Kunden mitgeteilt wird.

Mobile TAN (mTAN): Über einen zweiten Kommunikationskanal werden die relevanten Transaktionsdaten, welche bei der Bank eingetroffen sind per *Short Message Service* (SMS) Nachricht zum Mobiltelefon des Bank-Kunden übertragen und von ihm durch visuellen Vergleich mit der intendierten Transaktion geprüft. Die Autorisierung der Transaktion geschieht durch Eingabe einer ebenfalls übermittelten *mTAN,* die nur in einem kurzen Zeitfenster Gültigkeit hat und transaktionsspezifisch ist.

TAN-Generatoren: Beim TAN-Generatoren-Verfahren werden mobile Token verwendet, die sequentiell eine TAN elektronisch erzeugen können. Einige TAN-Generatoren wie der RSA-Token arbeiten zeitgesteuert. Die Ausprägungsformen sind *sm@rt-TAN, eTAN-Generator, chipTAN manuell* und *chipTAN comfort.* Die TAN Generatoren sind dann besonders komfortabel, wenn sie über eine optische Schnittstelle HHD 1.3.2 mit dem Client-PC kommunizieren [Zka2009].

Digitale Signatur / HBCI: Die Digitale Signatur wurde mit dem *Homebanking Computer Interface* (HBCI) seit 1996 entwickelt und standardisiert[1]. Damit steht eine Schnittstelle für ein Chipkarten-basiertes Online-Transaktionsprotokoll zur Verfügung. Das Protokoll wurde als *Financial Transaction Services* (FinTS) vom ZKA weiterentwickelt [Zka2009].

Online-Banking mit USB-Stick: Im Jahr 2009 wurde von IBM mit *Zone Trusted Information Channel* (ZTIC) ein USB-Stick-Verfahren vorgestellt, dass speziell für sicheres Online-Banking auf Malware-betroffenen Client-Rechnern konzipiert wurde [Wei2008]. Ähnliche Produkte gibt es von den Unternehmen KOBIL und Novosec.

4 Biometrische Transaktions-Authentisierung

Vorgestellt wird in diesem Beitrag ein Protokoll zur biometrischen Nachrichten-Authentisierung, exemplarisch dargestellt für die Absicherung von Online-Banking-Diensten. Das Protokoll erfüllt die beiden folgenden wesentlichen Anforderungen:

1.) Eine zuverlässige *Personen-Authentisierung*.
Nur die registrierte natürliche Person hat die Transaktion durchgeführt. Das Abstreiten einer tatsächlich durchgeführten Transaktion durch den registrierten Endkunden wird damit unmöglich.

[1] HBCI als solches ist kein Sicherheitsverfahren per se sondern ein Standard des ZKA zur Abwicklung von Online-Banking-Transaktionen

2.) Eine zuverlässige *Daten-Authentisierung*.
Die registrierte natürliche Person hat die Transaktionsdaten in einer vertrauenswürdigen Umgebung kontrolliert, diese Transaktion autorisiert und die Autorisierung über einen unabhängigen zweiten Kommunikationskanal zum Bank-Server übertragen.

4.1 Annahmen

Auf einem potentiell unsicheren Kundenrechner wird eine Online-Banking-Software (BSW) betrieben, die mit dem Online-Banking-Server (OBS) in der Bank kommuniziert. Die Online-Banking-Software überträgt Transaktionsdaten an den OBS und an das sichere Biometric-Transaction-Device (BTD), auf dem die Bestätigung der Transaktion durch den Endkunden erfolgt. Auf dem BTD wird ein Siegel erzeugt, das als Transaction-Order-Seal (TOS), die Transaktionsdaten mit den biometrischen Daten des Endkunden verknüpft. Für das Biometrische-Nachrichten-Authentisierungs-Protokoll wird von einer Bedrohungs-Situation ausgegangen, die in Abbildung 2 illustriert und im folgenden Abschnitt erläutert wird.

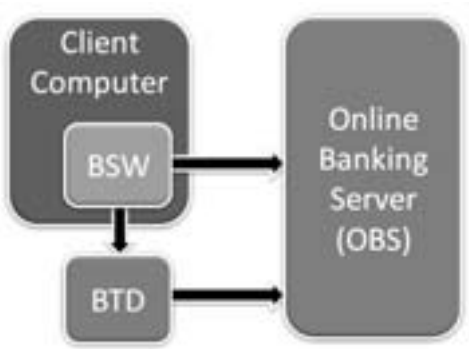

Abbildung 2: Bedrohungs-Situation und Kommunikationswege zwischen Online-Banking-Software (BSW), Online-Banking-Server (OBS) und Biometric-Transaction-Device (BTD).
Die Online-Banking-Software wird auf einem unsicheren Client-Computer betrieben, der Server OBS und das Device BTD werden als sicher eingestuft.

4.2 Komponenten

Zur Umsetzung biometrisch sicherer Online-Transaktionen interagieren die folgenden Komponenten, die sich in Bezug auf die Bedrohungssituation unterscheiden:

1.) Ein sicherer *Online-Banking-Server* (OBS), der folgende Eigenschaften aufweist:
- hat Zugriff auf Kundendaten.
- etabliert eine Kommunikation mit der Online-Banking-Software (BSW), die auf dem unsicheren Rechner des Kunden betrieben wird.
- führt Transaktionen aus.

- kann mit einem *Biometric-Transaction-Device* (BTD) eine Verbindung aufbauen.

2.) Eine *Online-Banking-Software* (BSW) auf einem **unsicherem** Kunden-Rechner (Client-Rechner). Die BSW:
- wird ausgeführt auf einem Kunden-Rechner, der durch Trojanische Pferde, Root-Kits etc. beliebig gefährdet sein kann.
- kann als browserbasierte Applikation ausgeprägt sein.
- kommuniziert mit Online-Banking-Server (OBS) und transferiert Aufträge in Form eines Transaction-Order-Record (TOR). Ein TOR beinhaltet: i) Transaktionsidentifikator (TID), ii) Sender-Account-Number (SAN), iii) Receiver-Account-Number (RAN), iv) Ordered Amount (ORA).
- Verbunden mit dem Kunden-Rechner ist ein vertrauenswürdiges Biometric-Transaction-Device (BTD).

3.) Ein **sicheres** *Biometric-Transaction-Device* (BTD), das mit Kunden-Rechner verbunden ist. Das BTD:
- ist eine vertrauenswürdige Hardware, die idealer Weise sicherheitsgeprüft wurde (z.B. nach Common Criteria). Die Hardware kann eine dedizierte Komponente, wie etwa ein biometrisch erweiterter Secoder nach ZKA-Anforderungen sein.
- kann nicht durch Malware manipuliert werden.
- kann eine biometrische Charakteristik erfassen. Dabei wird als Biometric-Capture-Device (BCD) ein Sensor eingesetzt, der als überwindungssicher eingestuft werden kann und somit für den nicht-überwachten Betrieb im Heimbereich oder Bürobereich geeignet ist.
- kann mit einem Online-Banking-Server (OBS) als Kommunikationspartner eine Verbindung aufbauen.
- kann eine Transaction-Order (TRO) von BSW als Transaction-Order-Record (TOR) empfangen und darstellen.
- Die Kommunikation zwischen BSW und BTD kann in verschiedenen Optionen ausgeprägt sein. Es kann eine kontaktlose Datenanbindung oder eine optische Schnittstelle (z.B. Flicker-Code) sein.

4.3 Enrolment

Zum Enrolment für das Biometrische-Transaktions-Authentisierungs-Protokoll wird das bekannte Helper-Data-Schema wie folgt erweitert (siehe Abbildung 3):

1.) Enrolment-Schritte im Biometric-Transaction-Device (BTD):
- Die selbe biometrische Charakteristik des Bank-Kunden wird mit dem BCD erfasst und in Merkmalsvektoren umgewandelt.
- Das Hilfsdatum AD1 wird aus Enrolment Samples abgeleitet, wobei charakterisierende Daten zur Verteilung über die Population ebenfalls erforderlich sind.
- Ein binarisierter Merkmalsvektor RBV ergibt sich aus den Enrolment-Samples QBV und AD1.
- Der Kunde gibt ein Geheimnis SBV ein, das er zusammen mit der ebenfalls vom Server erzeugten Account-Number auf dem Postwege vom OBS erhalten hat.
- Der Fehlerkorrektur-Codebookvektor CBV ergibt sich aus: CBV = ENC(SBV)
- Die Auxilliary Data AD2 ergibt sich aus CBV und dem binarisierten Referenz-Merkmalsvektor RBV: AD2 = CBV XOR RBV

- AD1 und AD2 sind nicht sonderlich schützenswert und werden im BTD oder auf der persönlichen Chipkarte gespeichert

2.) Enrolment-Schritte des Online-Banking-Server (OBS):
- Generiert und sendet pre-shared secret (Geheimnis SBV)
- Legt Kundenrecord mit den folgenden Daten an: Account-Nummer (AN) und biometrischer Pseudo Identifikator PI = h(SBV) (Hashfunktion h, z.B RIPEMD-160, das bereits in der FinTS-Spezifikation genutzt wird)
- Sendet SBV samt AN zum Kunden (Postweg)

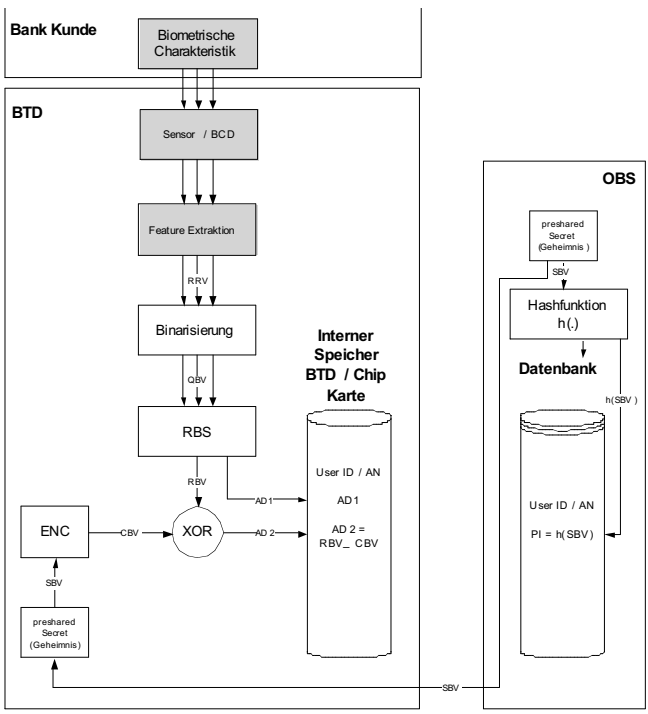

Abbildung 3: Erweitertes Enrolment

4.4 Prüfung der biometrischen Transaktions-Authentisierung

Zur Bestätigung einer vom Bank-Kunden gewünschten Transaktion wird für das Biometrische Nachrichten-Authentisierungs-Protokoll die klassische biometrische Verifikation erweitert. Zur Bestätigung der Transaktion wird lokal, d.h. im Home- oder Office-Umfeld des Bank-Kunden ein Transaction-Order-Seal (TOS‘) berechnet, der dann statt einer TAN an den Bank-Server übertragen wird. Die Arbeitsschritte sind wie folgt (siehe Abbildung 4):

1.) Operationen, die in der unsicheren Online-Banking-Software (BSW) durchgeführt werden sind:
   - Der Kunde erstellt durch Interaktion mit der BSW-Software einen Transaction-Order-Record (TOR).
   - Der BSW überträgt den TOR an den Online-Banking-Server (OBS)
   - Der BSW überträgt den TOR an das Biometric-Transaction-Device (BTD).

2.) Operationen, die im Biometric-Transaction-Device (BTD) durchgeführt werden:
   - Die relevante Information aus dem Transaction-Order-Record (TOR) wird im Display des BTD angezeigt: Receiver-Account-Number (RAN), Ordered-Amount (ORA). Die Ausprägung der Darstellung kann ähnlich wie mit den bereits am Markt erhältlichen chipTAN comfort Token erfolgen.
   - Zur Bestätigung der gewünschten Transaktion präsentiert der Initiator seine nicht-replizierbare biometrische Charakteristik dem Biometric-Capture-Device. Durch diesen Schritt wird ein Probe Image Sample mit dem BCD erfasst.
   - Die Auxilliary Data AD1 wird aus dem BTD-Speicher abgerufen
   - Ein binarisierter Probe-Merkmalsvektor XBV ergibt sich aus dem Probe-Sample QBV‘ und AD1
   - Ein Codebookvektor CBV‘ wird rekonstruiert aus im BTD gespeicherter Auxilliary Data AD2 und dem binarisierten Probe-Merkmalsvektor XBV: CBV‘ = AD2 XOR XBV
   - Das Secret SBV‘ wird aus CBV‘ berechnet: SBV‘ = DEC(CBV‘)
   - Die Pseudo-Identifikator PI‘ wird aus SBV‘ berechnet: PI‘=h(SBV‘)
   - Es wird ein Transaction-Order-Seal (TOS‘) berechnet aus Transaction-Order-Record TOR und rekonstruiertem PI‘: TOS‘ = MAC(h(TOR), PI‘)
   - Das TOS‘ verknüpft als Siegel die Daten eindeutig mit der bestätigenden natürlichen Person. Der berechnete Transaction-Order-Seal kann auch als Message Authentication Code (MAC) bezeichnet werden. Als MAC-Verfahren kann beispielsweise ein HMAC-Verfahren eingesetzt werden, das auf der Hashfunktion h aufbaut. Die Eingabevektoren TOR und PI‘ entsprechen der Nachricht und dem Schlüssel im HMAC-Verfahren. Der Wert TOS‘ lässt sich nach [Rfc2104] z.B. mit RIPEMD-160 als Hashfunktion wie folgt berechnen:
   - TOS‘ = h(PI‘ XOR OPAD, h(PI’ XOR IPAD, TOR))
   - Das Transaction-Order-Seal (TOS‘) wird zum Online-Banking-Server übertragen und gegebenenfalls vorab mit asymmetrischer Kryptographie verschlüsselt. Die Übertragung kann über den unsicheren Client-Rechner getunnelt werden oder alternativ (und bevorzugt) über einen zweiten unabhängigen Kanal. Dieser zweite unabhängige Kanal kann beispielsweise über das GSM-Netz realisiert werden. Diese Variante wird insbesondere dann bevorzugt werden, wenn das BTD in einem marktüblichen Mobiltelefon / Smartphone hardwaretechnisch integriert wird.

3.) Operationen, die im Online-Banking-Server (OBS) durchgeführt werden. Der OBS:
   - hat den Transaction-Order-Record (TOR) von der Banking-Software (BSW) erhalten.
   - hat den Transaction-Order-Seal (TOS‘) von dem Biometric-Transaction-Device (BTD) erhalten
   - hat den PI zum Kunden vorliegen PI=*h*(SBV)
   - rekonstruiert den TOS: TOS = MAC(*h*(TOR), PI)

- vergleicht den rekonstruierten TOS mit dem vom BTD gelieferten TOS‘:
- TOS = = TOS‘?

Die Transaktion ist personen- **und** datenauthentisch, wenn TOS und TOS‘ identisch sind. In diesem Fall und nur in diesem Fall gilt der im Transaktions-Record kodierte Auftrag als authentisch **und** bestätigt und wird vom OBS ausgeführt.

Die notwendigen Verifikations-Schritte im BTD und auf dem OBS zur Bestätigung der Transaktion und zur gleichzeitigen Prüfung von Personen-Authentizität **und** Daten-Authentizität werden in der folgenden Abbildung dargestellt.

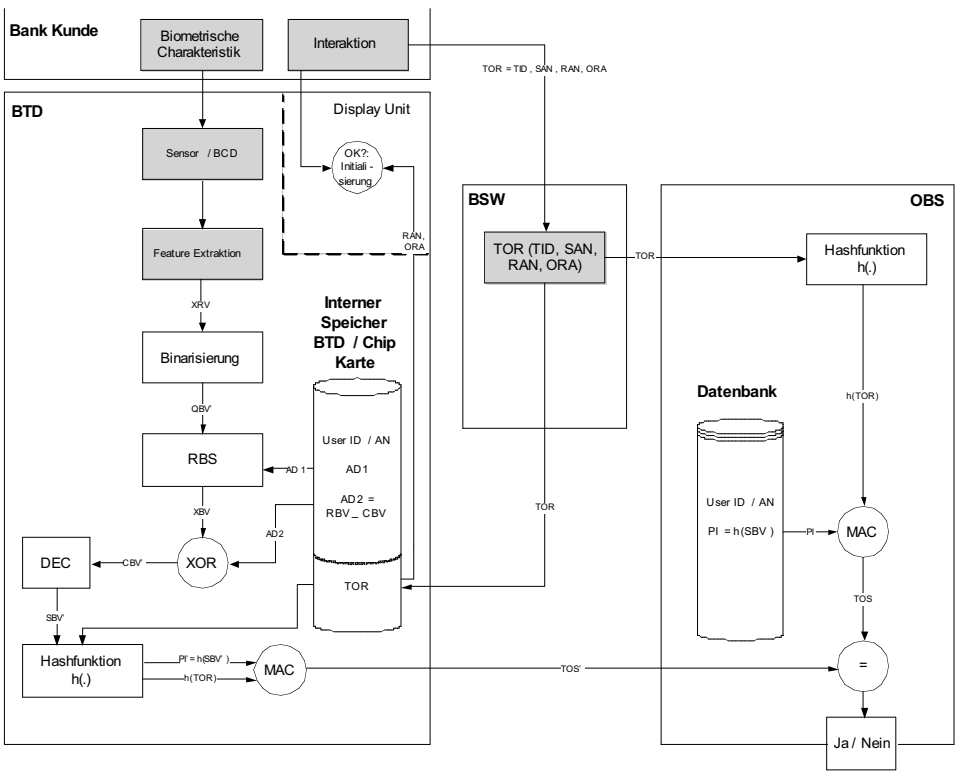

Abbildung 4: Prüfschritte einer biometrischen Transaktions-Authentisierung

5 Zusammenfassung und Ausblick

Durch das hier vorgelegte Transaktionsprotokoll wird die Personen-Authentisierung mit der Daten-Authentisierung verknüpft und damit die Forderung des Bundesverbandes Deutscher Banken erfüllt, dass durch die Nutzung der Biometrie im Online-Banking „eine Bindung des eineindeutigen biometrischen Merkmals des Kunden an seine gewollte Transaktion“ erreicht wird [Grud2009]. Sicherheitsrelevante Funktionalität

wird in einem Biometric-Transaction-Device gekapselt, das auch als biometrischer *Secoder* verstanden werden kann. Der wesentliche Sicherheitsgewinn im Vergleich zu existierenden Protokollen besteht darin, dass eine unerlaubte Delegation von Authentisierungsfaktoren ausgeschlossen werden kann. Weitere Anwendungsfelder ergeben sich z.B. in der Nachrichtenkommunikation im KRITIS- und Katastrophenmanagement. Durch den geringen Funktionsumfang des BTD ist eine Ausprägung in Hardware leicht realisierbar und eine Common-Criteria-konforme Sicherheitsprüfung dieser Komponente möglich.

Literaturverzeichnis

[Asit08] A-SIT: Secure Information Technology Center Austria, Österreichische Nationalbank. Risikoanalyse – E-Banking Angebote Österreichischer Kreditinstitute, 2008

[Bdb2006] Bundesverband Deutscher Banken: „Anzahl der Online-Konten“, http://www.bankenverband.de/downloads/112007/1ta0711-pr-onlinekonten.pdf

[Bit2008] Branchenverband BITKOM: „Fast 4 Millionen Opfer von Computer- und Internet-Kriminalität“, http://www.bitkom.org/de/presse/56204_53100.aspx

[Bka2008] Bundeskriminalamt: „Aktuelle Herausforderungen in der Kriminalitätsbekämpfung“, http://www.bka.de/pressemitteilungen/2008/pm080328.html, März 2008

[Bre2008] J. Breebaart, C. Busch, J. Grave, E. Kindt: „A Reference Architecture for Biometric Template Protection based on Pseudo Identities“, in Proceedings BIOSIG2008, pages 25-37, GI-LNI, (2008)

[Bsi2009] Bundesamt für Sicherheit in der Informationstechnik: „Die Lage der IT-Sicherheit in Deutschland 2009“, https://www.bsi.bund.de/Lageberichte

[Bsi2010] Bundesamt für Sicherheit in der Informationstechnik: „Identitätsdiebstahl und Identitätsmissbrauch im Internet “, https://www.bsi.bund.de/Studien

[Grud2009] W. Grudzien: „Sicherheit in der Kreditwirtschaft“, Vortrag auf der Fachtagung für FinanzDL am 22.09.2009

[Iso-sc37] ISO/IEC JTC1 SC37 SD2 Harmonized Biometric Vocabulary, September 2009 http://www.3dface.org/media/vocabulary.html

[Iso-sc27] ISO/IEC JTC1 2ndCD 24745: Biometric Template Protection, Januar 2010

[Idtc2009a] Identity Theft Resource Center: Security Breaches 2008, http://www.idtheftcenter.org/artman2/publish/lib_survey/Breaches_2008.shtml

[Rfc2104] H. Krawczyk, M. Bellare, R. Canetti. “RFC2104 - HMAC: Keyed-Hashing for Message Authentication”, 1997, http://www.faqs.org/rfcs/rfc2104.html

[Rut2006] J. Rutkowska: „Introducing Stealth Malware Taxonomy“, http://www.invisiblethings.org/papers/malware-taxonomy.pdf

[Tak05] P. Tuyls, A. H. M. Akkermans, T. A. M. Kevenaar, G. J. Schrijen, A. M. Bazen, and R. N. J. Veldhuis. “Practical biometric authentication with template protection.” In Audio and video-based biometric person authentication, pages 436–446. Springer, Berlin, Germany, 2005.

[Wei2008] T. Weigold et al.: „The Zurich Trusted Information Channel – An Efficient Defence against Man-in-the-Middle and Malicious Software Attacks“, in : TRUST 2008, LNCS 4968, pp. 75–91, http://www.zurich.ibm.com/pdf/csc/ZTIC-Trust-2008-final.pdf

[Zka2009] Zentraler Kreditausschuss: „FinTS Spezifikation“, Version vom 02.02.2009, http://www.hbci-zka.de/dokumente/aenderungen/V3.0/HKTAN-4_zur_Unterstuetzung_von_HHD_UC.pdf