Biometrische Template-Protection-Verfahren und Interoperabilitätsstrategien

Christoph Busch [1], Sebastian Abt [1], Claudia Nickel [1], Ulrike Korte [2], Xuebing Zhou [3]

1: Hochschule Darmstadt / CASED
Haardtring 100, 64295 Darmstadt
christoph.busch@h-da.de
2: Bundesamt für Sicherheit in der Informationstechnik (BSI)
3: Fraunhofer-Institut für Graphische Datenverarbeitung (IGD)

Abstract: Biometrische Authentisierung wird häufig zur Verbesserung der Identitätsverifikation eingesetzt. Durch die Nutzung biometrischer Verfahren entstehen neue Herausforderungen an den Schutz der Privatsphäre betroffener Personen. In biometrischen Systemen gespeicherte Referenzdaten enthalten Informationen, die aus den biometrischen Charakteristika einer Person abgeleitet wurden. Das Speichern von Abbildern einer biometrischen Charakteristik (z.B. Fingerbilder) in einer Datenbank ist aus Datenschutzsicht ungeeignet, da die Charakteristik selbst nach einer etwaigen Korrumpierung der Datenbank nicht ersetzt werden kann. Des Weiteren ist die Anzahl der biometrischen Charakteristika eines Nutzers begrenzt. Biometrische Merkmale werden z.B. aus einem Fingerbild extrahiert und in einem Template gespeichert. Eine Mehrfachnutzung von Templates in verschiedenen Anwendungen kann zu sog. Cross-Matching-Problemen führen, wenn Anwendungen miteinander verknüpft werden. Darüber hinaus können Referenzdaten für die Authentisierung irrelevante Informationen enthalten (z.B. ethnische Zugehörigkeit, Krankheiten). Zur Lösung dieser Herausforderungen hat sich mit den Template-Protection-Verfahren eine Technologie entwickelt, die den Anforderungen des Datenschutzes gerecht wird. Offene Systeme erfordern jedoch die Möglichkeit zum Austausch von interoperablen Referenzdatensätzen. Dieser Beitrag betrachtet daher Sicherheitsanforderungen an biometrische Systeme, behandelt die aktuellen Standardisierungsbemühungen zu Biometric-Template-Protection und schlägt eine weitere Vorgehensweise vor.

1 Einführung

Die steigende Nachfrage an Verbesserungen der Sicherheit in der Grenzkontrolle und die zunehmende Anzahl elektronischer Transaktionen, die über kabelgebundene und drahtlose Netzwerke getätigt werden, haben einen starken Bedarf an einem zuverlässigeren Identitätsmanagement erweckt. Existierende, besitzbasierte Identifikationsmethoden (zum Beispiel eine ID Karte) oder wissensbasierte Methoden (z.B. PIN oder Passwort) sind mit Nachteilen verbunden: Diese Authentisierungsfaktoren können vergessen, verloren, verteilt oder gestohlen werden. Biometrie als ergänzender oder ersetzender Faktor kann zu einer höheren Zuverlässigkeit der Verifikation von Identitätsbehauptungen beitragen und im gleichen Zuge einen

höheren Nutzerkomfort bedeuten, da biometrische Charakteristika nur schwer vergessen werden oder verloren gehen können.

Die Nutzung von Biometrie zur Identitätsverifikation hat jedoch auch Bedenken aufgeworfen. Die enge Verbindung biometrischer Verifikationsmethoden zu physikalischen, anatomischen Eigenschaften der betroffenen Personen ermöglicht die Nutzung biometrischer Messdaten für andere als die beabsichtigten Verwendungszwecke und kann somit eine Gefährdung der Privatsphäre darstellen, die sich in die folgenden vier Kategorien unterteilen lässt:

Nichtauthorisierte Erfassung: Erfassung biometrischer Samples ohne das Wissen der betroffenen Person, zum Beispiel durch Verwendung versteckter Kameras.

Unnötige Erfassung: Anwendung biometrischer Methoden ohne oder mit nur wenig zusätzlichem Nutzen im Vergleich zu gewöhnlicher Nutzerverifikation.

Nichtauthorisierte Verwendung und Preisgabe: Nutzung biometrischer Verfahren für andere als die von der betroffenen Person genehmigten Zwecke.

Schleichende Erweiterung des Verwendungsrahmens: Erweiterung eines Systems in Bereiche, in denen die Verwendung ursprünglich nicht vorgesehen war.

Die für das Verarbeiten biometrischer Daten zu beachtende Direktive 95/46/EC über den Schutz personenbezogener Daten und über die freie Verfügbarkeit derartiger Daten gibt keine eindeutige Vorgabe zum Einsatz von biometrischen Verfahren. Der Artikel 29 EU Beratungsausschuss für Datenschutz und Privatsphäre hat daher in seinem im Jahre 2003 veröffentlichten Arbeitspapier über Biometrie [Par03] die Bedeutung von den Schutz der Privatsphäre verbessernden Technologien hervorgehoben, um hierdurch biometrische Systeme zu fördern, die eine dem Schutz der Privatsphäre und dem Schutz der Daten freundliche Architektur aufweisen und übermäßiges Sammeln von Daten und einen ungesetzmäßigen Umgang mit diesen Daten erschweren bzw. verhindern.

Dieser Beitrag widmet sich dem Schutz von biometrischen Referenzdaten und daraus abgeleiteten Interoperabilitätsstrategien. Dazu werden zunächst in Kapitel 2 die Sicherheitseigenschaften biometrischer Systeme betrachtet. In Kapitel 3 wird die für ein offenes, interoperables System notwendige Standardisierung zusammengefasst und in Kapitel 4 besondere Fragen im Zusammenhang mit dem Schutz von Referenzdaten diskutiert. Das Kapitel 5 gibt einen Ausblick auf die weitere Vorgehensweise in der Standardisierung.

2 Sicherheitsaspekte biometrischer Systeme

Die primäre Motivation beim Einsatz biometrischer Verfahren ist die Steigerung der Sicherheit einer Anwendung durch genauere und zuverlässigere Identifikation. Ein möglicher Vorbehalt gegen die Verwendung biometrischer Verfahren ist, dass die erreichte erhöhte Sicherheit mit einem verminderten Schutz der Privatsphäre

einhergehen kann [CS07]. Die Einbeziehung biometrischer Verfahren kann jedoch darüber hinaus in neuen Schwachstellen resultieren. Nach Jain [Jain08] kann das Sicherheitsrisiko eines biometrischen Systems in vier Kategorien unterteilt werden:

- Immanente biometrische Fehler, die häufig durch Wahrscheinlichkeitswerte für Falsch-Akzeptanz und/oder Falsch-Rückweisung ausgedrückt werden.
- Angriff auf die Systemverwaltung.
- Unzulänglich geschützte Infrastruktur, resultierend in Schwachstellen im Zusammenhang mit nicht hinreichend gesicherter Hardware, Software oder Kommunikationskanälen.
- Öffentlichkeit von biometrischen Charakteristika, die versteckte Gewinnung biometrischer Samples und die Erzeugung von Plagiaten ermöglicht.

Die Beständigkeit biometrischer Charakteristika ist eine für die Erkennungsleistung erstrebenswerte Eigenschaft, hat aber auch Auswirkungen auf die eingeschränkten Möglichkeiten der Risikominimierung in Bezug auf einen Identitätsmissbrauch. Sobald ein biometrisches Charakteristikum einem Diebstahl zum Opfer gefallen ist und einem potentiellen Angreifer in Form eines Plagiates zur Verfügung steht, ist es so gut wie unmöglich, dieses Charakteristikum zu erneuern. Eine Verminderung der einhergehenden Risiken kann jedoch dadurch erreicht werden, dass die Erneuerbarkeit biometrischer Templates[1] in einem Identitätsverifikationssystem, sichergestellt wird. Durch die Erneuerbarkeit wird das Risiko einer unzulänglich geschützten Infrastruktur / Systemverwaltung minimiert und damit auch mittelbar das Risiko einer Plagiat-Erzeugung reduziert.

2.1 Sicherheitsanforderungen

Zur Analyse möglicher Angriffsvektoren auf biometrische Systeme sind zunächst grundlegende Sicherheitsanforderungen zu betrachten. Die Sicherheitsanforderungen lassen sich in die Teilaspekte Vertraulichkeit, Integrität, Verfügbarkeit sowie Erneuerbarkeit und Widerrufbarkeit unterteilen.

Vertraulichkeit ist die Eigenschaft, die den Schutz von Informationen vor nicht autorisiertem Zugriff und unerlaubter Veröffentlichung beschreibt.

Integrität ist die Eigenschaft, die die Unversehrtheit und Korrektheit von Daten und Verfahren sicherstellt. Durch die Überprüfung der Integrität wird eine beabsichtigte oder unbeabsichtigte Modifikation einer biometrischen Referenz oder das Ersetzen einer gespeicherten biometrischen Referenz zum Zwecke eines Angriffs ausgeschlossen.

Verfügbarkeit ist die Eigenschaft eines Systems, bei Bedarf zugänglich und funktionsfähig zu sein. Eine Beeinträchtigung der Funktionsfähigkeit eines

[1] ISO/IEC SC37 Harmonized Biometric Vocabulary: http://www.3dface.org/media/vocabulary.html

biometrischen Systems kann z.B. durch von einem Angreifer vorgenommenes Löschen notwendiger, in einer biometrischen Referenzdatenbank gespeicherter, biometrischer Daten erfolgen.

Erneuerbarkeit und Widerrufbarkeit von biometrischen Referenzen bietet einen Schutz bei einer Kompromittierung des biometrischen Datenspeichers.

2.2 Erzeugung von geschützten biometrischen Referenzen

Bei Erneuerbarkeit und Widerrufbarkeit biometrischer Referenzen handelt es sich um bedeutende Maßnahmen zur Wahrung der Privatsphäre eines Individuums durch Vermeidung unerwünschter Verknüpfungen über Datenbanken hinweg. Erneuerbare biometrische Referenzen werden durch Diversifikation im Erstellungsprozess erzeugt und erlauben das Generieren mehrerer unterschiedlicher biometrischer Referenzen, die sämtlich aus einem Charakteristikum abgeleitet wurden [Bre08]. Dazu werden sogenannte Template-Protection-Verfahren eingesetzt. Die Transformation von biometrischen Templates in geschützte Templates (Referenzen) erfolgt mittels einer Einweg-Funktion, sodass eine Rekonstruktion des ursprünglichen Samples unmöglich wird. Somit erlauben Referenzen, die in unterschiedlichen Anwendungen für eine betroffene Person gespeichert werden, keinerlei Querbezüge zwischen den Anwendungen und geben keine unerwünschte Information über die betroffene Person preis.

3 Standardisierung biometrischer Systeme

Bei der gegebenen großen Bandbreite biometrischer Modalitäten, Sensortypen, Merkmalsextraktionsverfahren und Templateformaten ist für große offene Anwendungen (wie zum Beispiel biometrische Reisepässe, Bürgerkarten oder biometrische Bankkarten) die Interoperabilität gleichzeitig eine große Herausforderung und zwingend erforderlich.

Durch den Einsatz standardisierter Technologien reduziert sich für den Betreiber das Risiko einer sich einstellenden Herstellerabhängigkeit. Bei einem ggf. notwendigen Wechsel eines Herstellers kann der Betreiber des biometrischen Systems daher beträchtliche Migrationskosten sparen, wenn etablierte Standards bei der Einrichtung des Systems berücksichtigt wurden.

3.1 Zusammenwirken der Standardisierungsgremien

Die Standardisierung im Bereich der Informationstechnologie wird von einem Joint Technical Committee (JTC) zwischen der International Organization for Standardization (ISO) und der International Electrotechnical Commission (IEC) erarbeitet. Mit der Biometriestandardisierung beauftragt wurde das im Jahr 2002 etablierte Subcommittee SC37. Parallel dazu werden im Subcommittee SC27 die Sicherheitsverfahren sowie im Subcommittee SC17 SmartCards und deren Kommunikationsprotokollen bearbeitet.

Das SC37 formuliert Datenaustauschformate, nach denen die Repräsentation einer biometrischen Charakteristik, z.B. eines Gesichtsbilds, in einem spezifizierten Datensatz kodiert werden kann. Für den Bereich Biometrische Systeme ist die wichtigste Tätigkeit des SC17 die Bearbeitung des On-Card-Comparison Standards ISO/IEC 24787, der für Token-basierte Systeme relevant ist. Das SC27 beschäftigt sich in der Working Group 5 mit Identity Management Systemen und Privacy-Enhancing-Technologies und behandelt in diesem Kontext auch biometrische Verfahren und den Schutz von biometrischen Referenzdaten im Rahmen der Standardentwicklung des ISO/IEC 24745 „Information technology – Security techniques – Biometric template protection“ [ISOtp]. Mit beiden Standards werden wesentliche Grundlagen für die Sicherheitseigenschaften eines biometrischen Systems definiert.

4 Biometrische Systeme nach ISO/IEC 24745

Biometrische Systeme werden im Wesentlichen zur Authentisierung und Identifikation eines Individuums eingesetzt. Hierzu vergleicht ein biometrisches System eine vom Individuum genommene Probe mit einer oder mehreren gespeicherten biometrischen Referenzen. Bei einer biometrischen Referenz (BR) handelt es sich um ein biometrisches Sample, ein biometrisches Template oder ein biometrisches Modell, das ein Individuum eindeutig innerhalb eines bestimmten Kontextes identifizieren kann.

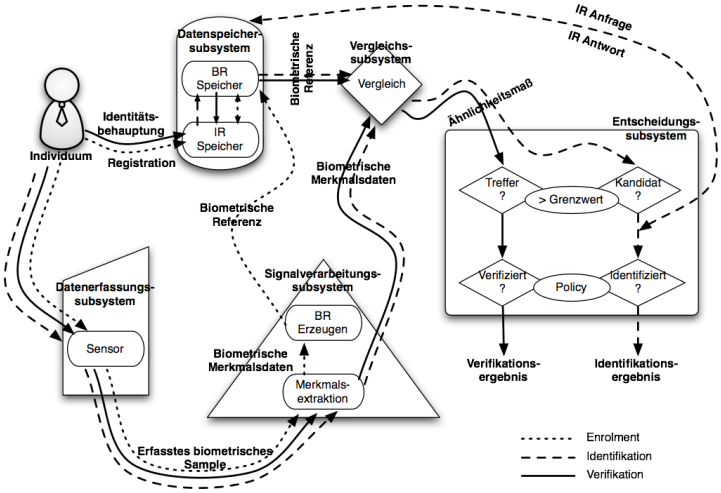

Abbildung 1: Struktur eines biometrischen Systems

Die Architektur eines biometrischen Systems gliedert sich nach [ISOtp] in die folgenden fünf Subsysteme, die in Abbildung 1 dargestellt sind:

Biometrisches Erfassungssubsystem: Beinhaltet Sensoren und bildet die erfassten biometrischen Charakteristika auf biometrische Samples ab.

Signalverarbeitungssubsystem: Extrahiert biometrische Merkmalsdaten aus biometrischen Samples.

Datenspeichersubsystem: Dient zur Speicherung erfasster biometrischer Referenzen und Identitätsreferenzen, meist in separaten Datenbanken.

Vergleichssubsystem: Vergleicht erfasste biometrische Samples mit gespeicherten biometrischen Referenzen und liefert ein Ähnlichkeitsmaß (Vergleichswert).

Entscheidungssubsystem: Entscheidet auf Grund des Ähnlichkeitsmaßes über die Identität des zum erfassten biometrischen Sample gehörenden Individuums.

Biometrische Referenzen stellen sensible personenbezogene Daten dar, die entweder unmittelbar (z.B. Gesichtsfoto) oder indirekt (z.B. Fingerabdruck-Minutien) zur Identifizierung einer Person und auf Grund deren Eindeutigkeit potenziell als eindeutiger Identifikator (Universal Unique Identifier - UUID) zur datenbankübergreifenden Verknüpfung von Daten genutzt werden können. Dies stellt eine Gefährdung der Privatsphäre des Individuums dar. Insbesondere sollten biometrische Daten im Besitz und unter Kontrolle der betroffenen Person bleiben und biometrische Samples von biometrischen Systemen nur gespeichert werden, wenn dies dringend erforderlich ist. Weiterhin sollte ein biometrisches System Mechanismen zum Erzeugen diversifizierbarer Referenzen zur Verfügung stellen, um das Widerrufen und Erneuern biometrischer Referenzen zu ermöglichen.

4.1 Sicherheitsgefährdungen und Gegenmaßnahmen

Jedes der im vorigen Abschnitt beschriebenen Subsysteme (Datenerfassungssubsystem, Signalverarbeitungssubsystem, Datenspeichersubsystem, Vergleichssubsystem, Entscheidungssubsystem) sowie die zwischen den Subsystemen liegenden Kommunikationskanäle besitzen eigene Angriffsvektoren. Tabelle 1 gibt eine Übersicht über Gefährdungen der Subsysteme und die in ISO/IEC 24745 vorgeschlagenen Gegenmaßnahmen.

Subsystem	***Gefährdungen***	***Gegenmaßnahmen***
Erfassungssubsystem	Sensor Spoofing mit Plagiaten	- Lebenderkennung - Multimodale Biometrie - Challenge/Response
Signalverarbeitungs-subsystem	Einfügen gefälschter Daten	- Verwendung geprüfter und freigegebener Algorithmen
Vergleichs-subsystem	Manipulation von Ähnlichkeitsmaßen (berechneten Vergleichswerten)	- Sicherung des Servers und/oder Clients - Geschützte Implementierung (z.B. On- Card-Comparison)
Datenspeicher-subsystem	Kompromittierung der Datenbank	- Verwendung erneuerbarer biometrischer Referenzen

Subsystem	*Gefährdungen*	*Gegenmaßnahmen*
		- Datenseparation - Zugriffskontrolle
	- Unautorisierte Veröffentlichung personenbezogener Daten - Unautorisiertes Austauschen von gespeicherten Daten (BR, IR) - Unautorisierte Modifikation von BR, IR	- Zugriffskontrollen - Sicherung von BR, IR durch elektronische Signaturen - Sicherung von BR, IR durch Verschlüsselung
Entscheidungs-subsystem	Kontinuierliche Modifikation eines biometrischen Samples zur Erreichung der notwendigen Entscheidungsgrenzwerte (Hill-Climbing Attacke)	- Verwendung grob quantisierter Vergleichswerte - Sichere Kommunikationskanäle

Tabelle 1: Gefährdungen biometrischer Subsysteme und Gegenmaßnahmen.

Oft sind biometrische Systeme als verteilte Implementierungen realisiert, so dass sensible Daten zwischen den Subsystemen ausgetauscht werden. Tabelle 2 beschreibt während der Datenübertragung entstehende Gefährdungen und Gegenmaßnahmen.

Kommunikations-verbindung(en)	*Übertragene Daten*	*Gefährdungen*	*Gegenmaßnahmen*
Datenerfassungs-subsystem ↔ Signalverarbeitungs-subsystem ↔ Vergleichs-subsystem	Biometrisches Sample und Merkmalsdaten	Abhören der Daten	Einsatz einer verschlüsselten Kommunikationsverbindung
		Wiederholung (Replay-Attacke)	Einsatz von Challenge-Response-Verfahren
		Brute Force	Fehlbedienungszähler
Datenspeicher-subsystem ↔ Vergleichs-subsystem	Biometrische Referenz	Abhören der Daten	Einsatz einer verschlüsselten Kommunikationsverbindung
		Wiederholte Datenübermittlung (Replay-Attacke)	Einsatz von Challenge-Response-Verfahren
		Man-in-the-middle Angriff	Einsatz einer Ende-zu-Ende verschlüsselten Kommunikationsverbindung und Authentifikation der Teilnehmer
		Hill-Climbing Attacke	Verwendung grob dargestellter Vergleichswerte
Vergleichs-subsystem ↔ Entscheidungs-subsystem	Vergleichswert	Manipulation des Vergleichswertes	Einsatz einer verschlüsselten Kommunikationsverbindung

Tabelle 2: Durch Datenübertragung auftretende Gefährdungen und Gegenmaßnahmen.

Zusätzlich zu den in Tabelle 1 und 2 dargestellten technischen Gegenmaßnahmen existieren weitere administrative Gegenmaßnahmen zum Schutz biometrischer Systeme und Daten. Siehe hierzu ITU-T X.tpp-1 [ISOe] und ISO 19092:2008 [ISOf].

4.2 Erneuerbare biometrische Referenzen

Erneuerbare biometrische Referenzen bestehen aus einem pseudonymen Identifikator (PI) sowie dazugehörenden unterstützenden Daten (Auxilliary Data - AD), die während des Enrolmentprozesses aus einem oder mehreren biometrischen Samples erzeugt werden.

Pseudonyme Identifikatoren (PI) sind diversifizierbare, geschützte binäre Strings. Ein pseudonymer Identifikator gibt keine Informationen preis, die Aufschluss über die ursprünglich erhobenen Daten, das zu Grunde liegende biometrische Template oder die wahre Identität dessen Besitzers geben. Der Prozess zur Erzeugung pseudonymer Identifikatoren wird in Abbildung 2 dargestellt. Während einer Enrolmentphase wird für ein Individuum eine biometrische Referenz generiert. Innerhalb dieses Prozesses werden von einem Sensor ein oder mehrere biometrische Samples erzeugt und im Anschluss von einem Feature-Extraktor zur Erzeugung biometrischer Merkmale verwendet. Abschließend werden von einem Pseudonymous-Identifikator-Encoder (PIE) ein pseudonymer Identifikator sowie möglicherweise benötigte unterstützende Daten erzeugt.

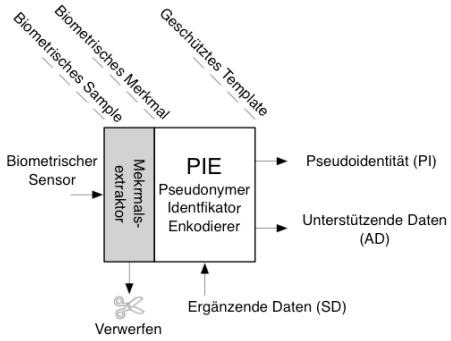

Abbildung 2: Erzeugung geschützter Templates

In den Prozess einfließende ergänzende Daten (Supplementary Data - SD) können Sicherheitsverbesserungen durch besitz- oder wissensbasierte Schlüssel bewirken, die vom Enrollee eingegeben werden müssen (z.B. biometrisch gehärtete Kennwörter). Alternativ können benutzer-spezifische Parameter als SD gespeichert werden.

Die Kombination von pseudonymem Identifikator und unterstützenden Daten wird als ein geschütztes Template bezeichnet. Sowohl der pseudonyme Identifikator, als auch die unterstützenden Daten werden nach deren Erzeugung gespeichert, wohingegen die

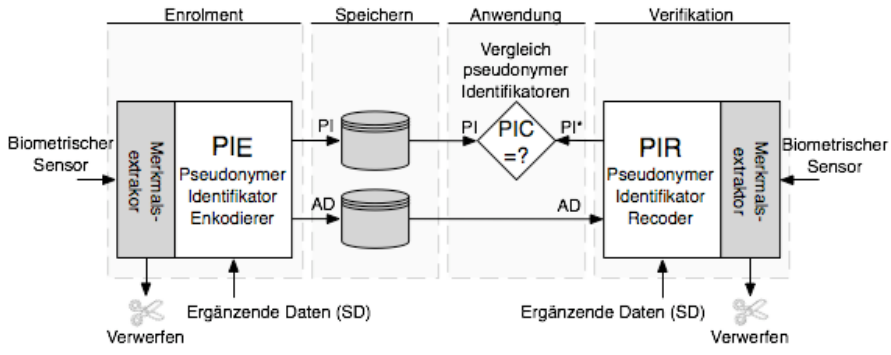

Abbildung 3: Referenzarchitektur eines Systems zum Schutz biometrischer Templates.

erfassten biometrischen Merkmale zerstört werden.

Für die Verifikation wird ein pseudonymer Identifikator neu erzeugt, der dann mit dem während des Enrolments erzeugten PI verglichen wird. Dazu wurden in den letzten zehn Jahren etliche Verfahren vorgeschlagenz.B. [SRS+98], [JW99], [DRS04], [TAK+05], [ST06], [NJP07], [RCCB07]. Die Verifikation wird hierbei durch die Transformation eines Proben-Samples in einen neuen pseudonymen Identifikator PI* unter Verwendung der bereitgestellten unterstützenden Daten erreicht. Ergänzende Daten aus der Enrolmentphase müssen auch dem Pseudonymer-Identifikator-Recoder (PIR) während des Erzeugens des rekonstruierten PI* zur Verfügung gestellt werden. Nach dem Erzeugen von PI* durch den PIR werden alle Eingabedaten, d.h. das biometrische Sample, die Merkmalsdaten und die ergänzenden Daten gelöscht und PI* wird an den Pseudonymen Identifikator-Comparator (PIC) übergeben, der PI mit PI* vergleicht. Abbildung 3 gibt einen Überblick über die Gesamtarchitektur zum Erstellen, Speichern und Verifizieren von pseudonymen Identifikatoren. Der pseudonyme Identifikator und die unterstützenden Daten werden auf einem passenden Medium oder auf unterschiedlichen Medien, wie zum Beispiel Datenbanken, Smartcards, Barcodes, etc., gespeichert.

4.3 Anwendungsmodelle biometrischer Systeme

Das Speichern von PI und AD kann auf unterschiedlichen Wegen stattfinden, die sich wie folgt in drei Kategorien einteilen lassen: zentrales Speichern (sowohl PI, als auch AD werden in einer Datenbank gespeichert), lokales Speichern (PI und AD werden gemeinsam auf einem Token gespeichert) und hybrides Speichern durch Separierung von PI und AD (zum Beispiel durch Speichern der unterstützenden Daten auf einem Token und des pseudonymen Identifikators in einer Datenbank). Vorteile des zentralen Speicherns zumindest einer der beiden Datenelemente liegen in der Möglichkeit des Erstellens einer schwarzen Liste, des Realisierens von Prüf-Funktionalitäten (Audits) und des Ermöglichens eines simplen Widerruf-Prozesses. Die Vorteile des lokalen Speicherns sind das Nichtvorhandensein von für zentrale Datenbanken spezifischen Sicherheitsrisiken sowie der vollständige Besitz der Kontrolle über Referenzdaten bei der betroffenen Person. Das hybride Speichern zeichnet sich dadurch aus, dass sowohl die betroffene Person, als auch der Anbieter Kontrolle über die Nutzung der Templatedaten besitzt und die durch eine zentrale Datenspeicherung potentiell entstehenden Sicherheitsrisiken reduziert werden können.)

Notwendige Schutzmaßnahmen für ein biometrisches System können oft erst in der Analyse des Anwendungskontextes ausgewählt werden. Zu diesem Zweck beschreibt ISO/IEC 24745 verschiedene Anwendungsmodelle und unterscheidet diese auf Basis des Speicherortes der Referenzdaten sowie des Vergleichsortes. Die hierbei verwendeten Standorte lassen sich wie folgt beschreiben:

Client: Bei einem Client handelt es sich um einen Arbeitsplatzrechner oder ein äquivalentes Endgerät (z.B. PDA, Smartphone) und angeschlossene Sensoren.

Server: Ein Server ist ein System, das über ein Netzwerk mit einem Client kommuniziert und Daten zur Verfügung stellt bzw. Operationen ausführt.

Token: Ein Token (z.B. SmartCard) kann biometrische Daten speichern und in manchen Fällen auch vergleichen (z.B. On-Card-Comparison).

Die in ISO/IEC 24745 beschriebenen Modelle A bis F sind anwendbar auf erneuerbare biometrische Referenzen unter der Annahme, dass PI und AD am gleichen Ort gespeichert werden. Die Modelle G und H hingegen sind ausschließlich für den Einsatz mit erneuerbaren biometrischen Referenzen anwendbar und beschreiben Modelle der Separation von PI und AD.

Modell A – Speichern und Vergleich auf Server
Modell B – Speichern auf Token, Vergleich auf Server
Modell C – Speichern auf Server, Vergleich auf Client
Modell D – Speichern und Vergleich auf Client
Modell E – Speichern auf Token, Vergleich auf Client
Modell F – Speichern und Vergleich auf Token
Modell G – Verteiltes Speichern auf Token und Server, Vergleich auf Server
Modell H – Verteiltes Speichern auf Token und Client, Vergleich auf Client

Die Modelle G und H beziehen sich ausschließlich auf erneuerbare biometrische Referenzen. Das Konzept der Datenseparierung wird durch verteiltes Speichern der Komponenten erneuerbarer biometrischer Referenzen (IR, PI, AD) umgesetzt. Nach diesem Modell wird ein pseudonymer Identifikator in einem Server-seitigen Datenspeicher hinterlegt. Die hierzu gehörenden unterstützenden Daten (AD) werden jedoch zusammen mit der Identitätsreferenz (IR) auf einem benutzerspezifischen Token gespeichert. Durch die Verteilung der erneuerbaren biometrischen Referenz auf unterschiedliche Systeme wird bei der Durchführung einer Verifikation zwingend das Vorliegen korrekter Daten von beiden Systemen notwendig. Diese Vorgehensweise setzt zur Authentisierung immer die Zustimmung der betroffenen Person voraus. Darüber hinaus ermöglicht dieses Modell ein serverseitiges Widerrufen biometrischer Referenzdaten (PI), ohne hierzu Zugriff auf das Token zu benötigen.

5 Interoperabilität von erneuerbaren Referenzen

Durch die bisherigen Standardisierungsaktivitäten im Rahmen von ISO/IEC 24745 wurde ein Rahmen für ein biometrisches System mit Mechanismen zum Erzeugen diversifizierbarer Referenzen definiert. Dieser Architekturrahmen ist ein normativer Bestandteil von ISO/IEC 24745 geworden. Konforme Implementierungen müssen daher die beschriebenen Anforderungen zum Widerrufen und Erneuern biometrischer Referenzen erfüllen. Damit ist jedoch nicht sichergestellt, dass Referenzdaten auch zwischen unterschiedlichen Anwendungen ausgetauscht werden können. Die Vielfalt heute angebotener Template-Protection-Verfahren ist per se nicht interoperabel. Um eine Interoperabilität wie bei bildbasierten Referenzen zu erreichen, sollte für die zukünftige Standardisierungsarbeit ein zwei-stufiger Ansatz verfolgt werden.

In der ersten Stufe sollte mittelfristig ein Datenaustauschformat als Element des ISO/IEC 19794 Multipart-Standards definiert werden, der die relevanten Datenelemente PI und AD kodiert, wobei für herstellereigene Kodierungen der beiden Elemente entsprechende dynamische Datenfelder vorgesehen werden sollten, wie dies auch bei ISO/IEC 19794-2 definiert wurde. Eine Interoperabilität kann erreicht werden, wenn der Record zusätzlich eine registrierte Hersteller-Identifikationsnummer enthält, so dass ein Verifikationssystem den zum PIE korrespondierenden PIR auswählen und den PI* an den Comparator übergeben kann. Ein entsprechender pragmatischer Ansatz wurde von SC37 bereits für die Kodierung von Bildqualitätswerten unterschiedlicher Hersteller eingesetzt.

In einer zweiten Stufe sollte langfristig ein Auswahl-Wettbewerb zu einem standardisierten Verfahren gestartet werden, wie er ähnlich in der Vergangenheit mit dem Advanced Encryption Standard (AES) durchgeführt wurde und derzeit mit der Cryptographic Hash Algorithm Competition durchgeführt wird. Ein solcher Auswahl-Wettbewerb verlangt transparente Algorithmen, die eine Sicherheitsevaluierung des Template-Protection-Verfahrens ermöglichen. In der Evaluierung sollte der Nachweis der Einweg-Eigenschaft (ENW) geprüft werden, um eine Rekonstruktion des Samples auszuschließen. In einer vergleichenden Evaluierung sollten mindestens die Kriterien Entropie (ENT) des erzeugten Referenzdatensatzes, die Diversifikationseigenschaft (DIV) sowie die Undichtigkeit (DIC) geprüft und bewertetet werden. Darüber hinaus ist eine Evaluierung der Erkennungsleistung nach ISO/IEC 19795-1 erforderlich, um die Performanz (PER) zu bewerten. Ein Ranking von Kandidaten kann erfolgen, in dem die Systemgüte durch

$$\text{Score} = 0{,}5\ \text{PER} + 0{,}2\ \text{ENT} + 0{,}2\ \text{DIV} + 0{,}1\ \text{DIC}$$

gewichtet bewertet wird. Erkennungsleistung und Sicherheitseigenschaften eines Verfahrens werden dabei gleichgewichtet gefordert. Dieses Maß für die Systemgüte verfolgt den Zweck, einen Zugewinn an Template-Sicherheit nicht auf Kosten der Erkennungsleistung zu bewerten.

6 Zusammenfassung

Mit der Standardisierung in ISO/IEC 24745 wurde ein einheitliches Verständnis für Sicherheitsanforderungen an biometrische Systeme sowie für Risiken und empfohlene Gegenmaßnahmen erreicht. Mit der Integration der normativen Anforderung von erneuerbaren biometrischen Referenzen wurden wesentliche Datenschutzmechanismen im Standard verankert.

Für System-Betreiber ist neben der Sicherheit aber auch die Interoperabilität von Austauschformaten und damit die Reduzierung von Hersteller-Abhängigkeiten ein wichtiges Ziel. Durch den vorgeschlagenen Auswahl-Wettbewerb kann dieses Ziel langfristig verfolgt und sichere, datenschutzfreundliche und performante biometrische Systeme ermöglicht werden.

7 Danksagung

Diese Arbeit wurde durchgeführt im Rahmen des Projekts "BioKeyS- Pilot-DB" des Bundesamtes für Sicherheit in der Informationstechnik.

Literaturverzeichnis

[Bre08] J. Breebaart, C. Busch, J. Grave, E. Kindt: A Reference Architecture for Biometric Template Protection based on Pseudo Identities, in Proceedings BIOSIG 2008

[CS07] A. Cavoukian und A. Stoianov: Biometric encryption: a positive-sum technology that achieves strong authentication, security and privacy. Whitepaper information and Privacy Commissioner/Ontario, 2007. available from www.ipc.on.ca.

[DRS04] Yevgeniy Dodis, Leonid Reyzin, Adam Smith: Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In EUROCRYPT, pages 523–540, 2004.

[ISOe] ISO/IEC 9594-2, ITU-T X.tpp-1 (Telebiometric Protection Procedure-Part1): A guideline of technical and managerial countermeasures for biometric data security

[ISOf] ISO 19092:2008, Financial Services – Biometrics – Security framework

[ISOtp] ISO/IEC CD 24745 Information technology - Security techniques - Biometric template protection

[Jain08] A. Jain, K. Nandakumar, A. Nagar: Biometric Template Security, EURASIP Journal on Advances in Signal Processing, Volume 2008

[JW99] A. Juels und M. Wattenberg: A fuzzy commitment scheme. In Proc. 6th ACMCCCS, pages 28–36, 1999.

[NJP07] K. Nandakumar, A.K. Jain, S. Pankanti: Fingerprint-based fuzzy vault: Implementation and performance. Information Forensics and Security, IEEE Transactions on, 2(4):744–757, Dec. 2007.

[Par03] ARTICLE 29 Data Protection Working Party. Working document on biometrics working document on biometrics. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_en.pdf, 2003. Last visited: November 26, 2009

[RCCB07] N. K. Ratha, S. Chikkerur, J. H. Connell, R. M. Bolle: Generating cancelable fingerprint templates. IEEE Trans. pattern analysis and machine intelligence, 29(4):561–572, 2007.

[SRS+98] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, B. V. K. Vijaya Kumar: In R. L. van Renesse, editor, Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series, volume 3314 of Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series, pages 178–188, April 1998.

[ST06] Berry Schoenmakers, Pim Tuyls: Efficient binary conversion for paillier encrypted values. In EUROCRYPT, pages 522–537, 2006.

[TAK+05] P. Tuyls, A. H. M. Akkermans, T. A. M. Kevenaar, G. J. Schrijen, A. M. Bazen, R. N. J. Veldhuis: Practical biometric authentication with template protection. In Audio and video-based biometric person authentication, pages 436–446.