Der Landesbeauftragte
für den Datenschutz Rheinland-Pfalz

Hintere Bleiche 34 | 55116 Mainz
Postfach 30 40 | 55020 Mainz
Telefon +49 (0) 6131 208-2449
Telefax +49 (0) 6131 208-2497
poststelle@datenschutz.rlp.de
www.datenschutz.rlp.de

Orientierungshilfe „Biometrische Authentisierung – Möglichkeiten und Grenzen“

Herausgegeben vom
Arbeitskreis „Technische und organisatorische Datenschutzfragen“
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Stand 2. November 2009

erarbeitet unter Federführung des Berliner Beauftragten für Datenschutz und Informationsfreiheit

Die Authentisierung von Personen mit bestimmten körperlichen Merkmalen wie z. B. Fingerabdrücken, Gesichtsgeometrie oder Irismuster wird gelegentlich als Alternative zu den Authentisierungsverfahren durch Besitz und/oder Wissen angesehen. In diesem Papier geht es nicht um die spezifischen Datenschutzfragen beim Einsatz biometrischer Verfahren, sondern um die Möglichkeiten und Grenzen dieser Verfahren bei der Authentisierung.

Die biometrische Authentisierung setzt zunächst die Erfassung eines biometrischen Merkmals einer Person mittels optischer, thermischer, chemosensorischer, akustischer oder drucksensitiver Verfahren für spätere Vergleichszwecke voraus. Aus den erfassten Rohdaten wird mittels geeigneter Algorithmen ein sog. Template (Muster) berechnet und zentral oder dezentral für spätere Vergleiche (z. B. auf einer Chipkarte) abgespeichert. Dabei ist sicher zu stellen, dass eine Rekonstruktion des biometrischen Merkmals durch Rückrechnung aus dem Template ausgeschlossen ist.

Beim eigentlichen Authentisierungsvorgang wird mit den gleichen Erfassungssystemen das biometrische Merkmal erfasst und ebenfalls mit den gleichen geeigneten Algorithmen aus dem aktuellen Merkmal die sog. biometrische Signatur berechnet. Die biometrische Signatur wird dann mit dem hinterlegten Template computergestützt verglichen. Das Ergebnis dieses Vergleichs führt dann zur automatisierten Entscheidung, ob die Authentisierung zum Erfolg führt oder nicht.

Die wichtigsten Erkennungsarten bei der Überprüfung sind die biometrische Verifikation (1:1-Vergleich) und die biometrische Identifikation (1:n-Vergleich). Bei der Verifikation wird die Identität durch den Vergleich der biometrischen Signatur mit genau einem Template geprüft, das dezentral, zum Beispiel auf einem bei der zu verifizierenden Person befindlichen Chip gespeichert werden kann. Bei der Identifikation wird die biometrische Signatur mit einer Vielzahl von Templates verglichen, die zentral in einer Datenbank gespeichert sind.

Aus datenschutzrechtlicher Sicht ist wegen der Datensparsamkeit und –vermeidung der biometrischen Verifikation eindeutig der Vorzug vor der biometrischen Identifikation zu geben. Dies gilt insbesondere bei einer dezentralen Speicherung der Referenzdaten.

Die Treffsicherheit biometrischer Verfahren folgt im Gegensatz zu den kausalen Verfahren der Authentisierung durch Besitz und/oder Wissen Gesetzen der Wahrscheinlichkeit. Es ist stets davon auszugehen, dass die biometrische Signatur und das Template nie ganz gleich sein werden. Der Vergleich zwischen Signatur und Template kann daher nur einen Grad von Ähnlichkeit ermitteln.
Je nach den Anforderungen an die Treffsicherheit des biometrischen Erkennungssystems muss ein Schwellenwert für die Ähnlichkeit festgelegt werden, über dem die Berechtigung vergeben (Acceptance) und unter dem sie verweigert (Rejection) wird. Je höher (*oder geringer*) der Schwellenwert gewählt wird, desto geringer (*oder höher*) ist die Wahrscheinlichkeit, dass eine Berechtigung unzutreffend erteilt wird. Andererseits steigt (*sinkt*) mit dem Schwellenwert die Wahrscheinlichkeit, dass jemand unberechtigt abgewiesen wird.

Die Wahrscheinlichkeit, dass jemand unrichtigerweise zurückgewiesen wird, wird als „False Rejection Rate“ (FRR) bezeichnet; die Wahrscheinlichkeit, dass jemand unberechtigterweise eine Berechtigung erteilt bekommt, wird als „False Acceptance Rate“ (FAR) bezeichnet. Unter Kalibrierung versteht man die für eine konkrete Anwendung sinnvolle Vergabe von FRR bzw. FAR. Wenn eine der beiden Größen festgelegt bzw. beschränkt wird, ergibt sich die Festlegung bzw. Beschränkung für die andere wegen der wechselseitigen Abhängigkeit aus dem jeweiligen konkreten biometrischen Verfahren.

Die „Equal Error Rate“ ist der Wert, für den FRR=FAR gilt. Sie kann ein sinnvoller Kompromiss hinsichtlich der Sicherheitskalibrierung sein. Es gibt jedoch Anwendungs-Szenarien, bei denen die FAR im Vergleich zur FRR sehr niedrig sein muss, z. B. beim Zutritt/Zugang zum Hochsicherheitsbereich eines Kernkraftwerkes. Und es gibt Anwendungen, bei denen die FRR beispielsweise aus Performancegründen sehr niedrig sein muss und man eine höhere FAR gerne in Kauf nimmt. Das wäre bei der Zugangskontrolle für Besucher eines großen Fußballspiels der Fall, wenn wenige unberechtigt eingelassene Besucher akzeptiert werden.

Von den vielen übrigen „Rates“, die etwas über das biometrische System aussagen, sei noch die „Failure to Enroll Rate“ (FTE) erwähnt, die die Wahrscheinlichkeit benennt, dass von einer Person aus medizinischen Gründen kein brauchbares Template zu späteren Vergleichszwecken gewonnen werden kann. Dies gilt vor allem für Fingerabdrücke, bei denen FTEs von ca. 2 % der Gesamtbevölkerung ermittelt worden sind.

FRR und FAR sind abhängig von der Qualität des biometrischen Systems hinsichtlich der Genauigkeit der Erfassung, der Qualität der Template- und Signatur-Berechnung und der Genauigkeit des Vergleichs, von der Kalibrierung des biometrischen Systems, also der Wahl der Schwellenwerte und der Kooperation der Betroffenen.

Bei allzu kleiner FAR wird die FRR zu groß, d. h. z. B., bei einem Zutrittskontrollsystem bleiben zu viele Berechtigte vor der Tür. Dagegen führt eine allzu kleine FRR zu einer großen FAR, d. h. zu viele Unberechtigte können die Tür durchschreiten.

1. <u>Die kausalen Verfahren der Authentisierung mit Besitz und/oder Wissen</u>
   Beim kausalen Authentifizierungsvorgang, d. h. der Prüfung, ob der Besitz vorhanden und das Wissen korrekt wiedergegeben wurde, ist eine Ja-Nein Entscheidung möglich. Diese Verfahren treffen aber keine 100-prozentige, eindeutige und zutreffende Entscheidung, ob die zu authentifizierende Person wirklich anwesend ist oder nicht. Vielmehr wird unterstellt bzw. angenommen, dass wenn Besitz und Wissen im Authentisierungsverfahren mit dem der zu authentifizierenden Person übereinstimmen, [nur] diese Person anwesend ist. Es kann keine Wahrscheinlichkeit dafür berechnet, hergeleitet oder angegeben werden, dass diese Annahme oder Unterstellung zutrifft. Auch eine Lebenderkennung ist damit nicht verbunden.

   Es gibt eine Fülle von Beispielen, die belegen, dass ein korrekter Ablauf des Authentisierungsverfahrens nicht sicherstellt, dass auch die richtige Person das System nutzt.

So können die Authentisierungsmittel beispielsweise

- weitergegeben sein,
- gestohlen (Besitz) oder erpresst (Wissen) sein,
- der Besitz technisch dupliziert und das Wissen durch technische Manipulation ganz oder teilweise in falsche Hände gekommen sein (vgl. hierzu u. a. die vielfältigen Manipulationen an Geldausgabeautomaten),
- der richtige Benutzer zwar anwesend sein und das Authentisierungsverfahren bedienen, die anschließende Nutzung des Systems aber mit oder ohne Anwendung von Gewalt ausschließlich durch Dritte erfolgen etc.

2. Biometrische Authentisierung

Bei der biometrischen Authentisierung kann immerhin mit einer berechenbaren bzw. hohen Wahrscheinlichkeit davon ausgegangen werden, dass die richtige Person anwesend ist, wenn das biometrische Merkmal dauerhaft und direkt mit ihr verbunden ist. Dies gilt insbesondere für biometrische Merkmale, die nicht wie der Fingerabdruck an vielen Orten ständig hinterlassen werden. Hierbei ist natürlich auch zu berücksichtigen, ob das Verfahren eine Lebenderkennung beinhaltet.

Die tatsächliche Bindung des biometrischen Merkmals an die Person ist als echter Vorteil gegenüber personenbezogenen Merkmalen wie Besitz und Wissen zu werten, bei denen die Anwesenheit der Person nur angenommen werden kann.

3. Besondere Vorkehrungen bei biometrischer Authentisierung

Die biometrischen Daten sind – im Gegensatz zu UserID und Passwort und zu Verfahren von Besitz und Wissen – eindeutig und potenziell lebenslang mit der Betroffenen verbunden.

Deshalb sind für biometrische Authentisierungsverfahren - unabhängig vom verwendeten biometrischen Verfahren - besondere Vorkehrungen zu treffen:

a. Die Verbindung zwischen biometrischen und anderen Identitätsdaten muss sicher geschützt werden.

b. Der Schutz des Speichersystems der biometrischen Referenzdaten ist für Datensicherheit und Datenschutz des Verfahrens von grundlegender Bedeutung. Dabei sollte keine zentrale, sondern eine dezentrale Speicherung der Referenzdaten, z. B. auf einer Chipkarte, realisiert werden.

c. Speicherung und Übertragung der biometrischen Daten müssen gegen Abhören, unbefugte Offenbarung und Modifikation geschützt werden. Dies erfordert den Einsatz kryptografischer Verfahren.

Die biometrischen Daten sind nicht geheim und sie können nach Bekanntwerden oder Missbrauch nicht verändert oder gesperrt werden. Deshalb ist folgendes wichtig:

d. Die biometrischen Daten dürfen nicht allein zur Authentisierung herangezogen werden, sondern sie sind mit sperr- und veränderbaren Daten wie Besitz und Wissen wirksam zu koppeln.

Die Stärke biometrischer Verfahren kann sich bei der biometrischen Authentisierung wegen der Nicht-Änderbarkeit und Nicht-Sperrbarkeit biometrischer Merkmale nur entfalten, wenn die genannten Anforderungen erfüllt sind und die mit der Verarbeitung der biometrischen Daten verbundenen Risiken insgesamt wirksam beherrscht werden. Wenn eine Methode mit Besitz und Wissen durch die biometrische Authentisierung ergänzt wird, verleiht dies damit dem kausalen Verfahren höhere Sicherheit vor Kompromittierung.