

Dr. jur. Astrid Albrecht

Biometrische Authentifizierungsverfahren

Einleitung

Mit zunehmender elektronischer Abwicklung wichtiger Transaktionen wächst das Bedürfnis nach Vertraulichkeit und Verbindlichkeit. Im informationstechnologischen Zusammenhang ist Authentizität und damit die Übereinstimmung einer behaupteten mit der tatsächlichen Identität neben Vertraulichkeit, Integrität und Verfügbarkeit eines der herausragenden Sicherheitsziele. Durch hinreichend sichere Authentifizierung mittels Biometrie können elektronische Transaktionen bestimmten Personen verlässlich zugeordnet werden. Hier wird zunächst die grundsätzliche Funktionsweise biometrischer Verfahren vorgestellt. Diese können vor allem zur Kontrolle des Zutritts zu und der Verweildauer in Gebäuden/Räumen sowie des Zugangs zu und des Zugriffs auf Daten in der elektronischen Datenverarbeitung sowie allgemein zur Überprüfung von Berechtigungen eingesetzt werden.

Biometrische Erkennung erfolgt anhand messbarer, individueller Körpermerkmale. Sie verfolgt das Ziel, eine mittels automatisierter Messung durch ein spezifisches Merkmal bestimmte Person von anderen unterscheidbar zu machen. Definitionsgemäß muss es sich um die automatische Erkennung eines lebenden Individuums in Echt-Zeit handeln. Dabei kann ein biometrisches Verfahren auf jedem menschlichen Merkmal basieren, das einigen Basisanforderungen wie Universalität, Einzigartigkeit, Dauerhaftigkeit/Permanenz sowie Erfassbarkeit/Messbarkeit genügen muss.

Sowohl Wissens- als auch Besitzelemente (also z. B. Geheimzahlen und Karten) werden einer Per-

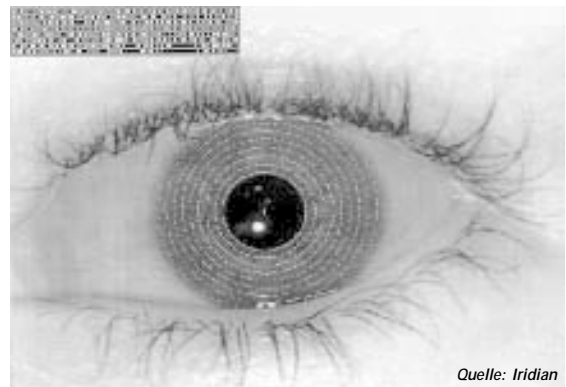
son indirekt und künstlich zugeordnet. Geheimnisse knüpfen an das Erinnern an und können daher vergessen werden. Sie können ausgespäht oder entschlüsselt werden. Besitzelemente können verloren gehen oder gestohlen werden. Sie können (freiwillig oder erzwungen) weitergegeben werden. Bei wissensbasierten Verfahren kommt es also vornehmlich auf die Geheimhaltung des Codes an, hinsichtlich des Besitzelements darauf, dass ein Dritter keinen Zugriff auf dieses erlangt. Schließlich kann anhand von Besitz und Wissen nur überprüft werden, ob das Besitzelement gültig ist und der richtige Code verwendet wird. Ob der aktuelle Benutzer auch der Berechtigte ist, kann dagegen nicht festgestellt werden.

Körperliche Merkmale sind dagegen in der Regel untrennbar mit dem Körper der Person verbunden und müssen nicht erst dem Berechtigten künstlich zugeordnet werden. Im Gegensatz zu lediglich auf die Person bezogenen Merkmalen sind diese also direkt und nicht nur abgeleitet unmittelbar an die Person gebunden. Sie sind grundsätzlich auch nicht wie lediglich einer Person künstlich zugeordnete Besitzelemente verlierbar. An ein körperliches Merkmal muss sich der Merkmalsträger nicht erinnern, er trägt es untrennbar stets bei sich. Es muss auch nicht geheim gehalten werden. Im Gegenteil liegen viele der für eine biometrische Erkennung verwendeten körperlichen Merkmale wie Gesicht und Finger offen, wovon in der Folge auch abhängt, dass die Sicherheit eines

biometrischen Systems nicht auf Geheimhaltung beruhen darf. Biometrische Merkmale können schließlich nicht übertragen oder weitergegeben werden. Wenn die Zuordnung des körperlichen Merkmals zu einer Person korrekt erfolgt, kann mit dessen Verwendung somit sichergestellt werden, dass es sich um die tatsächlich berechtigte Person handelt.

Grundlagen biometrischer Verfahren

Unterschieden werden biometrische Verfahren, die mit physiologischen Merkmalen arbeiten, und solche, die verhaltensbezogene Merkmale verwenden. Erstgenannte beruhen in der Regel auf der Verwendung passiver Merkmale wie Gesicht, Iris, Finger oder Hand. Verhaltensbezogene Merkmale beruhen dagegen grundsätz-



Bei der Iserkennung wird ein sog. Iriscode aus bestimmten Regionen der Iris berechnet.

lich auf einem aktiven Tun wie Unterschrift, Stimme oder Anschlagrhythmus an einer Tastatur.

Ablauf einer biometrischen Authentifikation

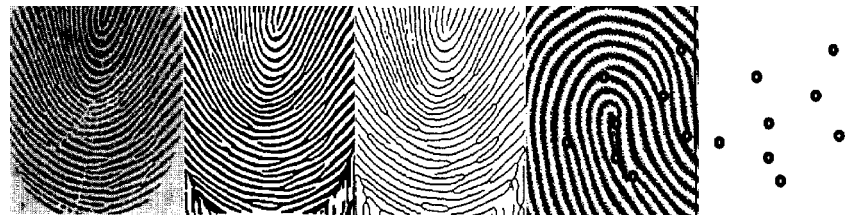
Das Grundprinzip der biometrischen Erkennung ist bei allen Systemen gleich. Diese enthalten unabhängig von ihrem oft sehr in-

dividuellen technologischen Aufbau die Schlüsselemente der Personalisierung oder Registrierung des Nutzers im System (Enrolment), die Erstellung von Datensätzen (Templates) und den Vergleich der aktuell präsentierten mit den zuvor abgespeicherten Daten (Matching). Die Erfassung biometrischer Merkmale erfolgt sowohl bei der erstmaligen Erfassung zur Erstellung des sog. Referenzdatensatzes als auch bei der späteren Erfassung zur Wiedererkennung durch Sensoren wie Kamera, Mikrofon oder Druckpad.

Zur Erfassung einer Person in einem biometrischen System wird beim Enrolment zunächst von dem Originalmerkmal ein Bild oder eine Aufzeichnung erzeugt, die sog. Rohdaten. Mittels eines Algorithmus wird dieses Original in einen Datensatz umgewandelt, in das sog. Template. Dieses enthält einen extrahierten Datensatz aus den aufgenommenen Daten, und kein genaues Abbild des verwendeten körperlichen Merkmals. Wenn Personen vom System nicht registriert werden können, wird deren Anteil in der sog. „False-Enrolment-Rate“ angegeben. Diese gibt also den Prozentsatz der Personen an, die nicht in das System eingelesen werden können. Dies kann zum einen darauf beruhen, dass das körperliche Merkmal zu gering ausgeprägt ist, mit der Folge, dass das System nicht die erforderliche Menge einzelner Merkmale zur Erstellung eines Datensatzes erfassen kann. Zum anderen kommt es vor, dass Personen das verwendete Merkmal überhaupt nicht besitzen, sei es aufgrund von Erkrankungen, Behinderungen oder einer anderen biologischen Besonderheit.

Beim sog. Matching wird ein Vergleich zwischen dem gespeicherten Template und dem Datensatz, der bei der erneuten Präsentation des Merkmals gegenüber dem biometrischen System erstellt wird, vorgenommen. Die Erfassung und

Auswertung biometrischer Merkmale ist naturgemäß mit Messfehlern behaftet, da sich die verwendeten Merkmale im Lauf der Zeit



Bei der Fingererkennung werden bestimmte Merkmale der Fingerkuppe zu einigen charakteristischen Punkten reduziert.
Quelle: Behrens/Roth 2001

verändern. Dies kann auf natürlichen, etwa altersbedingten Änderungen aber auch auf äußeren Einflüssen wie Verletzungen oder Krankheiten beruhen, oder auf äußerlichen Veränderungen wie Änderung der Haartracht (Frisur,



Bei der Gesichtserkennung werden markante Bereiche des Gesichts vermessen.
Quelle: cognittec

Bart). Zudem wird das Merkmal dem System niemals in der gleichen Art und Weise vom Nutzer dargeboten. Die Position des Fingers z. B. auf einem Fingerabdrucksensor oder der Blickwinkel des Gesichts ändern sich bei jeder Nutzung geringfügig. Dies hat zur Folge, dass zwei digitale Abbilder eines biometrischen Merkmals niemals identisch sind. Daher kann es zu den sog. Fehlerraten kommen, die entweder das fälschliche Erkennen einer Person für eine andere („False Accep-

tance“) oder das fälschliche Zurückweisen der berechtigten Person („False Rejection“) darstellen. Ein exakter Abgleich der Daten

kann daher nicht erreicht werden. Dieser beruht vielmehr auf einem zuvor eingestellten Parameter, dem sog. Schwellwert oder Toleranzbereich, in dem biometrische Daten vom System als „gleich“ erkannt werden. Die biometrischen Merkmale werden also nicht auf Gleichheit, sondern nur auf „hinreichende Ähnlichkeit“ getestet.

Während daher geringe Änderungen des Merkmals durch die Einstellung der Toleranzschwelle ausgeglichen werden können und dennoch eine korrekte Erkennung erfolgt, kann zu einem bestimmten Zeitpunkt die Veränderung so groß sein, dass das Merkmal im Vergleich zum gespeicherten Referenzdatum für eine Erkennung nicht mehr ähnlich genug ist. Um zu vermeiden, dass bei derartigen Änderungen des verwendeten Merkmals der Nutzer neu personalisiert werden muss, können durch den Einsatz von Lernmodulen bei sog. adaptiven Verfahren die Referenzdaten bei jeder neuen positiven Erkennung aktualisiert werden (Referenzdatenadaptation).

Betriebsarten biometrischer Systeme

Biometrische Erkennung kann grundsätzlich zwei Zwecke verfolgen. Bei der Verifikation erfolgt die Bestätigung der Identität auf die Frage, ob es sich bei einer Person um diejenige handelt, für die sie sich ausgibt. Es wird also eine

Vorgabe überprüft. Der Abgleich der aktuell präsentierten Daten erfolgt mit einem zuvor abgelegten Datensatz (1:1-Vergleich). Gespeichert sein kann dieser Datensatz in einem Datenverarbeitungssystem wie in einer zentralen Datenbank. Hier ist dann erforderlich, dass die Person sich dem System gegenüber als diejenige zu erkennen gibt, für die sie vom System zugelassen wird, z. B. über eine PIN oder ein Passwort. Der Datensatz kann aber auch für jeden Erkennungsvorgang aus einem externen Speichermedium wie z. B. einer Chipkarte oder einem anderen Token vom biometrischen System eingelesen werden. Der biometrische Erkennungsvorgang kann auch vollständig in diesem externen Speichermedium durchgeführt werden. In diesem Fall wird nur die Meldung „erkannt“ oder „abgewiesen“ an das System weitergegeben.

ler im System erfassten Nutzer verglichen. Als Ergebnis der Identifikation werden eine Nutzerkennung sowie eine Identitätsnummer desjenigen Benutzers aus dem Datenbestand geliefert, dessen Template am besten mit dem des aktuellen Benutzers übereinstimmt. Das System muss daher auf alle Templates aller eingelernten Benutzer zurückgreifen können, so dass eine zentrale Datenablage erforderlich ist.

Sicherheit

Biometrische Verfahren bieten somit generell die Chance, die informationstechnologische Sicherheit zu verbessern. Während jedoch der Einsatz eines biometrischen Systems die Authentizität in elektronischen Anwendungen grundsätzlich besser gewährleisten kann als die herkömmlichen Methoden, bedürfen biometrische

Integrität, d. h. ihre Unverfälschtheit, beim Einlernen, aber auch anschließend stets gewährleistet sein. Schließlich dürfen die Eingabedaten, die die Sensoren aus den biometrischen Merkmalen gewinnen, nicht abgehört und wiedereingespielt, aber auch nicht mit oder ohne Mitwirkung des Nutzers einfach reproduziert werden können.

Ausblick

Der Einsatz biometrischer Verfahren bietet somit eine potenzielle Verbesserung der Authentizitätsprüfung sowohl im privaten als auch im hoheitlichen Bereich in verschiedenen Anwendungsszenarien. Die dabei zu beachtenden Rahmenbedingungen auch rechtlicher Natur müssen nicht zuletzt mit Blick auf den notwendigen Persönlichkeitsschutz der Nutzer dabei angemessen Berücksichtigung finden. Den in diesem Zusammenhang grundlegenden Rechtsfragen wird sich ein weiterer Beitrag in einer der nächsten Ausgaben der AWV-Informationen widmen.

Weiterführende Literatur:

Albrecht, Astrid, *Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz*, Dissertation 2003, i. E. bei Nomos Baden-Baden in der Reihe Frankfurter Studien zum Datenschutz, hrsg. von Prof. Dr. Dr. hc. Spiros Simitis;

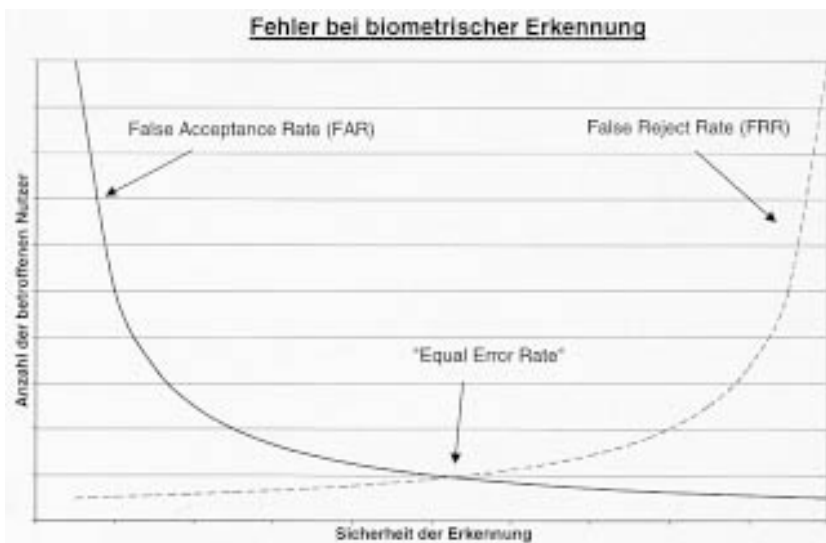
Behrens, Michael/Roth, Richard (Hrsg.), *Biometrische Identifikation – Grundlage, Verfahren, Perspektiven*, Vieweg 2001;

Gundermann, Lukas/Probst, Thomas, *Brennpunkte des Datenschutzrechts*, Kap. 9 in: Roßnagel, A. (Hrsg.): *Handbuch Datenschutzrecht*, C.H. Beck München 2003;

Leger, Lothar/Nolde, Veronika (Hrsg.), *Biometrische Verfahren, Körpermerkmale als Passwort, Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation*, Deutscher Wirtschaftsdienst 2002;

TeleTrust e. V.: *Kriterienkatalog zur Vergleichbarkeit biometrischer Verfahren*, vollständig überarbeitete Auflage vom 10.07.2002, download unter <http://www.teletrust.de/publikat.asp?id=40600>.

Dr. jur. Astrid Albrecht, Referentin beim Bundesamt für Sicherheit in der Informationstechnik, Leiterin der AG 6 Biometrische Identifikationsverfahren des TeleTrust e. V., Email: aalbrechtlaw@aol.com



Bei der Identifikation wird dagegen die Identität der Person festgestellt, und zwar auf die Frage, um welche Person es sich handelt (1:n-Vergleich). Die Person wird als das Individuum identifiziert, dessen biometrische Referenzdaten mit dem aktuellen biometrischen Datensatz der Person übereinstimmen. Im Gegensatz zur Verifikation wird hier das Template des aktuellen Benutzers mit allen gespeicherten Templates al-

len Daten selbst eines entsprechenden Schutzes. Denn hier werden in aller Regel personenbezogene Daten verwendet. Die Sicherheit biometrischer Systeme hängt besonders vom Schutz der Referenzdaten und den Vergleichsmechanismen ab. Insbesondere drei Aspekte stehen dabei im Vordergrund. Zunächst müssen diese tatsächlich von den Merkmalen der Person stammen, der sie zugeordnet sind. Zudem muss ihre