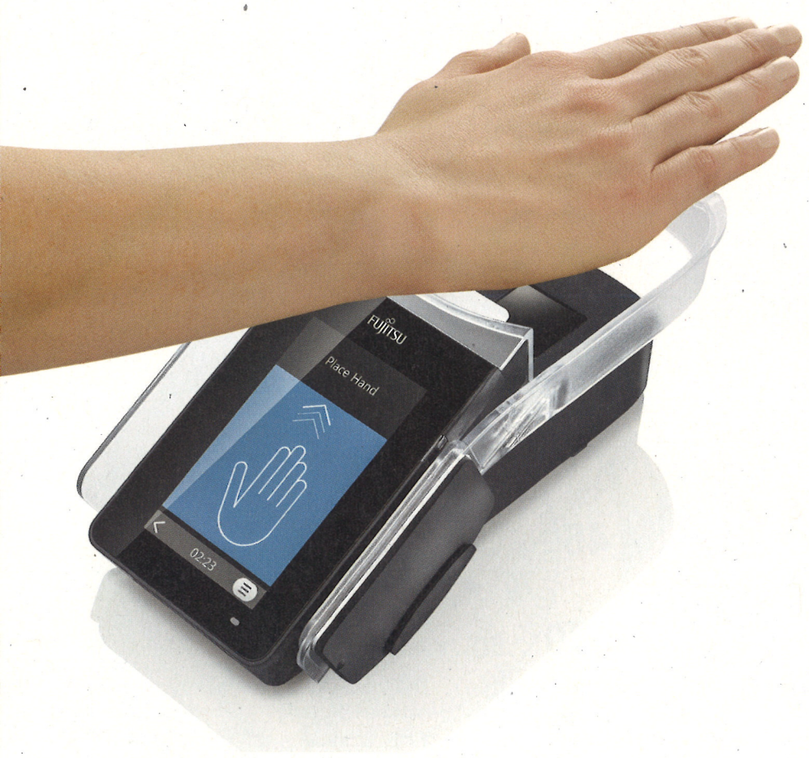

BILD: FUJITSU

Handlesen ohne Hokuspokus

Identifikation, Authentifizierung und danach die entsprechende Autorisierung sind Kernpunkte jeder Sicherheitsstrategie. Die aktuell modernste, genaueste und damit sicherste Methode dafür ist das Scannen von Venenmustern der Hand.

→ VON WILHELM PETERSMANN

Biometrie gilt heute als der wichtigste Ansatz, um die IT-Sicherheit in Bezug auf Identifikation, Authentifizierung und Autorisierung von Personen signifikant zu erhöhen. Das Scannen von Venenmustern ist eine solche biometrische Erkennungsmethode, genauso wie zum Beispiel Gesichtserkennung, Stimmerkennung, Fingerabdruck oder Iris-Scan. Bei all diesen Methoden werden biologische Charakteristika gemessen und ausgewertet.

Das wesentliche Qualitäts- und Sicherheitsmerkmal in der Biometrie ist die sogenannte FAR (false acceptance rate) bzw. Falschakzeptanzrate. Sie beschreibt die relative Häufigkeit, mit der ein Sicherheitssystem Zugang gewährt, obwohl keine Zugangsberechtigung besteht. Man kann vereinfacht auch von der Authentifizierungsgenauigkeit sprechen. Beim Handvenen-Scan ist die FAR kleiner als 0,00008 Prozent. Zum Vergleich: Beim Iris-Scan liegt dieser Wert bei rund 0,0001 Prozent, bei der Gesichtserkennung sogar bei etwa 1,3 Prozent.

Die Ansprüche an funktionierende Sicherheitskonzepte sind hoch. Die Lösung muss langfristig ohne wesentliche Veränderungen einsetzbar (Investitionsschutz) und ihre Leistung muss qualitativ mess- und vergleichbar sein; sie muss maximale Genauigkeit bei hoher Performance bieten, für jedermann zugänglich sein und gleichzeitig jedes Individuum vom anderen abgrenzen können; sie muss einfach angewendet werden können, plattform- und systemunabhängig sein, also leicht implementierbar, und akzeptiert werden (Benutzerfreundlichkeit).

WIE ES FUNKTIONIERT

Das Handvenen-Scanning erfüllt alle diese Voraussetzungen. Die Technologie von Fujitsu dafür heisst PalmSecure. Der Benutzer positioniert seine Hand kurz über einem Sensor. Via Infrarot wird die Hand gescannt (ohne Hautkontakt und damit absolut hygienisch) und das Venenmuster erkannt und aufgezeichnet. Damit das funktioniert, nutzt die Technologie zwei Eigenschaften des menschlichen Blutkreislaufs: Blut zirkuliert, und sauerstoffarmes (venöses) Blut absorbiert Nah-Infrarot-Strahlung. Für die im Gerät enthaltene Weitwinkel-Nah-Infrarot-Kamera wird dadurch das komplexe Handvenenmuster sichtbar. Dieses Muster ist bei jedem Menschen einmalig und damit unterscheidbar, selbst bei eineiigen Zwillingen. Auf der Hand werden über 5 Millionen Referenzpunkte identifiziert. Diese Identifikation ist subkutan (bezieht sich also auf das Gewebe unter der Haut), weshalb kleinere Verletzungen oder Verschmutzungen der Hautoberfläche das Ergebnis nicht beeinträchtigen. Auch dadurch ist diese Methode weitaus zuverlässiger und sicherer als andere biometrische Prüfverfahren.

VERSCHLÜSSELTE SPEICHERUNG

Das gewonnene Bild wird zunächst als sogenanntes Raw-Image innerhalb des Sensorgeräts gespeichert und hat eine Grösse von rund 5 MB. Raw ist ein Rohdatenformat, bei dem die Kamera die Daten nach der Digitalisierung weitgehend ohne Bearbeitung auf ein Speichermedium schreibt. Dieses Format wird gelegentlich auch als «digitales Negativ» bezeichnet. Ebenfalls noch innerhalb des Sensorgeräts wird das Raw-Image mit 128 oder 256 Bit AES verschlüsselt und zusätzlich einem Zufallsalgorithmus zugeordnet. Anschliessend erfolgt die Übertragung via USB-Schnittstelle zu einem Server/PC/Notebook. Hier ist die zum Sensor gehörende Authentifizierungsbibliothek hinterlegt und erst hier erfolgt die Umwandlung des Raw-Images in ein biometrisches Template. Bei der Umwandlung werden die Daten von 5 MB auf eine Grösse von 1 bis 3 KB komprimiert. Das komprimierte biometrische Template wird erneut mittels 128 oder 256 Bit AES verschlüsselt und in einer zentralen Datenbank hinterlegt. Die Authentifizierungsbibliothek schützt die abgelegten biometrischen Templates, indem sie diese mit einem zusätzlichen individuellen Schlüssel versieht, der nur einem Administrator oder CIO bekannt ist. Ohne diesen Schlüssel sind die Daten auch bei einem Diebstahl nicht verwendbar.

In der Praxis läuft jeder einzelne Authentifizierungsvorgang nach dem gleichen Muster ab: Der Benutzer hält seine Hand über den Infrarotsensor, das Handvenenmuster wird erfasst, an die Authentifizierungsbibliothek geschickt und mit den dort hinterlegten Daten verglichen. Gibt es beim Vergleich des hinterlegten biometrischen Musters 100 Prozent Übereinstimmung mit dem für den Authentifizierungsvorgang gesandten Muster, wird der Zugang gewährt – ansonsten wird der Benutzer abgewiesen. Passwort oder PIN sind nun für eine einfache, schnelle und sichere Identifikation, Authentifizierung und Autorisierung nicht mehr nötig.

KEINE ZENTRALE DATENBANK NÖTIG

Die PalmSecure-Standardsensoren lassen sich sowohl als USB-Geräte für Login- oder Single-Sign-on-Lösungen verwenden oder als OEM-Sensoren in jede Art von Terminal-Lösung integrieren. Die aktuellste Entwicklung der PalmSecure-Familie eröffnet eine neue Dimension von Sicherheit durch einen Zwei-Faktor-Abgleich ohne Speicherung personenbezogener Daten in einer zentralen Datenbank. Beim sogenannten ID-Match-Verfahren wird das Sensor- mit einem Kartenlesegerät kombiniert. Das ermöglicht den biometrischen Abgleich direkt im Gerät. Dabei wird das Handvenenmuster auf dem Chip einer Smartcard gespeichert und bei einer Verifikation mit dem eingelesenen Handvenenabdruck verglichen.

«Venenscanner sind weitaus zuverlässiger und sicherer als andere biometrische Prüfverfahren»

Wilhelm Petersmann

BESSER ALS PASSWÖRTER

Für Benutzer ist das Scannen der Handvene eine sehr einfache und schnelle Sache. Der vor dem ersten Gebrauch notwendige Registrierungsprozess dauert etwa 10 Sekunden, die normale Authentifizierung weniger als eine. Das ist schneller erledigt, als man ein Passwort eingibt. Weil die Lösung ausserdem extrem sicher ist, wird sie auf dem Markt und von Unternehmen der unterschiedlichsten Branchen hervorragend akzeptiert. PalmSecure, als weltweit erste und einzige Lösung dieser Art, ist mittlerweile in über 50 000 Geschäftsfällen in fast 40 Ländern mit rund 200 Millionen Anwendern im Einsatz. Die Nutzungsmöglichkeiten sind vielfältig. Beispielsweise ersetzt der Venen-Scanner als integrierte Lösung bei einigen Notebooks (oder als USB-Sensor am Desktop-PC) die Eingabe von Benutzername und Passwort. Das System wird für die Zeiterfassung von Arbeitnehmern oder die Patientenregistrierung in Krankenhäusern eingesetzt. Banken sichern damit die Benutzung von Geldautomaten. In öffentlichen Gebäuden, in Grossunternehmen, Rechenzentren und an Flughäfen wird der Venen-Scan als Methode für die Zugangsberechtigung benutzt. Auch in der Schweiz ist PalmSecure im Einsatz – beispielsweise setzt ein namhafter IT-Distributor die Lösung als Zutrittskontrolle ein. Der Nutzen: optimierte Sicherheit beim Zugang zum Gebäude, keine Schlüsselverwaltung mehr und dadurch reduzierter Administrationsaufwand. Passwörter oder PIN zu merken, ist Vergangenheit. ←

Wilhelm Petersmann ist Managing Director von Fujitsu Schweiz → **www.fujitsu.ch**