Der Großteil der Zutrittssysteme sind nach wie vor Karten- und Ausweislösungen.

Zutritt gesichert

Karten, Codes, Finger, Augen, Nasen, Mundpartien – um sicherzugehen, dass nur Berechtigte ein Gebäude oder einen Gebäudebereich betreten, ist eine ganze Reihe von Möglichkeiten am Markt.

Jedes bluetoothfähige Mobiltelefon der Welt – und das sind derzeit rund zwei Milliarden Stück – kann, wie es aus der Verpackung genommen wird, als elektronischer Schlüssel verwendet werden," sagt Christian Csank, Geschäftsführer von *Sorex Wireless* in Wiener Neustadt, der das System entwickelt hat.

Sorex Wireless Key ist für Privatanwender und Unternehmen einsetzbar. Konsumenten können mit der Basisversion ihre Eingangstür oder ihr Garagentor steuern. Nähert sich der Besitzer mit seinem Handy der Tür, öffnet sich diese automatisch. Die Distanz, innerhalb derer das System anspricht, kann zwischen wenigen Zentimetern und mehreren Metern programmiert werden. Das ist einer der Vorteile gegenüber der ebenfalls in Österreich entwickelten *Nearfield Communication (NFC),* die nur auf Distanzen von ein paar Zentimetern funktioniert. NFC benötigt eine spezielle Hardware im Handy.

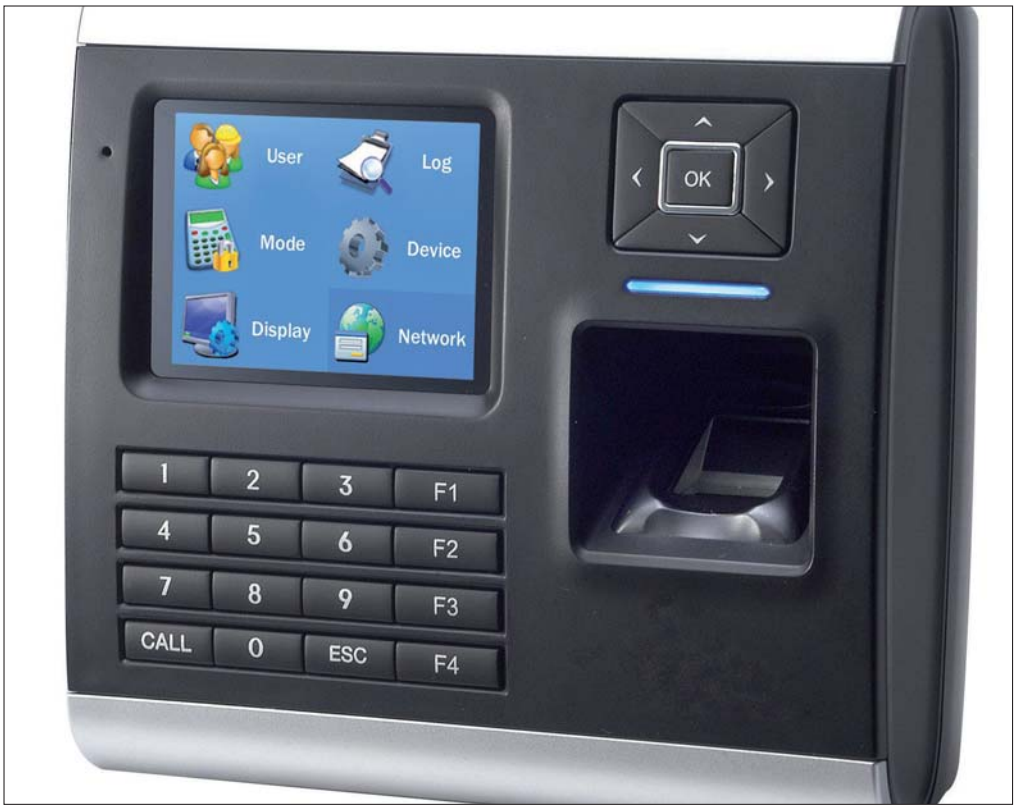
Bei der *Sorex*-Lösung wird an der Innenseite der Tür ein zwölf mal fünf Zentimeter großes Modul angebracht, das die nötige Technik enthält. Die Aktivierung oder Deaktivierung des Handys erfolgt bei der Basisversion direkt am Modul. Jedes Modul hat eine eigene Internet-Adresse (IP-Adresse), so dass es weltweit über Internet angesteuert werden kann. Ist der Besitzer beispielsweise im Urlaub und jemand anderer Berechtigter muss dringend ins Haus, so weist das System einen Code auf sein Handys zu und gewährt ihm einmalig Zutritt.

Für Hotels eröffnet die *Sorex*-Lösung die Möglichkeit, dem Gast bei Buchung seinen Zimmercode über Internet zuzusenden, etwa bei Vorausbezahlung per Kreditkarte. Kommt der Gast bei der Ankunft zur Tür, erkennt das Modul sein Handy und öffnet. Am Ende des Aufenthaltes endet die Berechtigung des Handys automatisch.

Neben der Produktvariante *Basic* stehen die Versionen *Advanced* und *Professional* zur Verfügung. Der Unterschied zur Basisversion: Bei *Advanced* können 50, bei *Professional* 65.000 Nutzer pro Modul angemeldet werden. Die Steuerung erfolgt nicht mehr direkt am Modul sondern zentral über das Computer-Netzwerk.

Bei der *Professional*-Version kann das System in die zentrale Datenbank des Unternehmens integriert werden. Für Unternehmen bietet das unter anderem den Vorteil, dass Authentifizierungen von Mitarbeiter-Handys jederzeit per Mausklick hinzugefügt oder

FOTO: KABA



„BioStation“: Fingerprint-Zeiterfassungssystem für gewerbliche und industrielle Anwendungen mit Zutrittskontrollfunktion.

gelöscht werden können. Die Sicherheit des Systems wird durch mehrere Faktoren gewährleistet: Das industrielle Bluetooth der Klasse I wechselt 1.700-mal pro Sekunde die Frequenz, so dass Frequenzstörungen ausgeschlossen sind. Der Code zur Autorisierung ist mit einer 128-Bit-Verschlüsselung ausgestattet. Der Code wird nur einmal ausgetauscht, nämlich bei der ersten Anmeldung. Ab diesem Zeitpunkt ist er im Modul gespeichert.

Bei jeder Annäherung eines Bluetooth-Handys wird die Autorisierung überprüft; dabei werden keine Daten übertragen. Geht das Handy verloren, kann das System deaktiviert werden. Das Steuerungsmodul an der Tür befindet sich von außen unerreichbar im Innenraum, anders als beispielsweise NFC-Sensoren, Fingerprintsysteme oder Tastaturen von Codeschlössern.

Der Mobilfunkbetreiber *T-Mobile* hat die Entwicklung in den eigenen Vertrieb aufgenommen und bietet sie seinen Business-Kunden an. Das auf Telekommunikation spezialisierte Unternehmen *M-Line* ist Vertriebspartner von *Sorex-Wireless* für die Betreuung des Einzelhandels.

Sorex Wireless, gegründet im Jahr 2004, hat sich auf die Entwicklung kabelloser Datenübertragungslösungen spezialisiert.

Die Produktpalette umfasst bluetooth-gesteuerte Zutrittssysteme sowie Lösungen zur Diebstahlsicherung, Alarmanlagensteuerung und Fernsteuerung von Haustechnikgeräten. Zu den Kunden zählen die *Telekom Austria, Philips, Würth* und *Forstinger*.

Der Großteil der Zutrittssysteme erfolgt nach wie vor über Karten- und Ausweislösungen. Chipkarten als „intelligente“ Speicherkarten können mit einer PIN (persönliche Identifikationsnummer) kombiniert werden. Ausgeführt als „Smart-Card“, kann die Karte mit Rechenleistungen verbunden werden, was vor allem die Programmierung von Verschlüsselungssystemen ermöglicht. An den Terminals erfolgt die Überprüfung über Kartenlesegeräte, die häufig berührungslos erfolgt.

Bei den biometrischen Zutrittsverfahren ist der Fingerprint nach wie vor – wie in der Kriminalistik – die sicherste Lösung. Biometrische Verfahren haben den Vorteil, dass die Zutrittsmerkmale nicht verloren werden können, wie etwa eine Code-Karte; sie können nicht vergessen werden, wie etwa ein Zahlen-Code; sie können nicht gefälscht werden.

Fingerprint-Zutrittssysteme sind meist entweder mit einer PIN kombiniert oder mit einer Chipkarte. Beim erstmaligen Speichervorgang liest ein Gerät einen Fingerabdruck direkt vom betreffenden Finger ab und speichert die jeweiligen Parameter in Form eines mathematischen Abbilds. Dieser Vorgang dauert etwa zwei Minuten. Das Auslesen beim Zutritt dauert in der Regel etwa drei Sekunden.

Beim Zutritt tippt der Betroffene einen Code ein und legt den „gespeicherten“ Finger auf ein Lesegerät. Das System nimmt die Daten auf, vergleicht sie mit den gespeicherten und gibt den Zutritt frei. Bei Lösungen, die mit einer Chipkarte kombiniert sind, drückt der Betroffene seinen „gespeicherten“ Finger auf das Lesegerät und lässt zusätzlich seine Zutrittskarte auslesen; zusätzlich kann der Vorgang mit der Eingabe einer PIN abgesichert werden. Es ist auch möglich, mehrere Finger abzuspeichern.

Ähnliches ist mit dem Handballen möglich: Statt eines Fingers wird das Papillarmuster des Handballens in mathematische Daten umgesetzt. Bei einem anderen System wird das Schattenbild der Handfläche vermessen. Die geometrischen Eigenschaften der Handfläche werden dann in mathematische Daten übersetzt und gespeichert. Andere Lösungen machen sich die Einzigartigkeit der Blutgefäßverteilung am Handrücken zunutze. Auch sie werden elektronisch vermessen und gespeichert.

Die Augensignatur basiert entweder auf einer Vermessung der Regenbogenhaut (Iris) im Auge oder der Netzhaut (Retina). Wie die Papillarlinien auf den Fingern des Menschen ist die Struktur der Iris jedes Menschen einzigartig, genauso wie die Gefäßstruktur auf der Netzhaut. Ein Sensor tastet dabei die Iris oder die Retina kreisförmig ab und speichert die Daten, um

FOTO: BIOMETRIX

Bluetoothfähiges Handy: Als elektronischer Schlüssel verwendbar.

sie beim Zutritt mit den neuen Daten vergleichen zu können. Immer wieder gibt es Diskussionen über eine eventuelle Gesundheitsschädigung am Auge.

Beim Passbildvergleich werden drei Kameras miteinander kombiniert: Eine Kamera nimmt ein Bild vom Foto auf der Zutrittskarte auf; eine weitere fotografiert den Betroffenen selbst; eine dritte nimmt die Umgebung des Betroffenen auf, um diese Daten vom neuen Bild abzuziehen und zwei vergleichbare Bilder zu produzieren. Das System erkennt nur, ob das Bild auf der Zutrittskarte mit dem Bild des Betroffenen übereinstimmt. Es erkennt nicht, ob die Karte zum Beispiel gefälscht ist. Daher muss der Zutritt personell kontrolliert werden.

Bei der Gesichtserkennung werden die Konturen des Gesichts vermessen, meist vorwiegend jene der Augen-, Nasen- und Mundpartien. Wie bei Fingerprint-Systemen werden die Daten meist auf einer Chipkarte gespeichert und beim Zutritt verglichen.

Bei der ersten Speicherung nimmt das System ein Foto des Betroffenen auf, speichert es, berechnet die Daten des Gesichts und speichert sie. Zusätzlich wird nach ähnlichen, gespeicherten Gesichtern gesucht, was im Trefferfall einen Alarm auslöst, um spätere, falsche Zutritte zu vermeiden.

Bei jedem Zutritt nimmt das System ein neues Bild des Betroffenen auf, ruft anhand einer zusätzlich ausgelesenen Karte das bei der Aufnahme gespeicherte Bild auf und vergleicht die Daten. Zusätzlich hat das Wachpersonal am Terminal die Möglichkeit, die beiden Bilder zu vergleichen. Auf diese Weise überwacht der Faktor Mensch das System.

Zutrittssysteme können auf Stand-alone-Basis eingerichtet werden, zentral oder dezentral. Bei der „Stand-alone“-Lösung erfolgen Datenaufnahme, Überprüfung und Steuerung am Ort des Zutritts.

Bei der „zentralen“ Lösung werden die Daten der Zutrittsberechtigten in einer Zentrale gespeichert. Die aus der Karte gelesenen Zutrittsdaten werden vom Zutrittspunkt an die Zentrale weitergeleitet, überprüft und der Zutritt wird bei Übereinstimmung direkt von der Zentrale freigeschaltet. Auch das Türmanagement wird von der Zentrale überwacht. Jeder Vorgang wird zentral protokolliert.

Die Zahl der „Leser“ und damit Zutrittsmöglichkeiten, die an eine Zentrale angeschlossen sind, ist praktisch unbegrenzt. Ähnlich bei „dezentralen“ Lösungen: Im Unterschied zur „zentralen“ Lösung werden die Daten Zutrittsberechtigter in der Zentrale gespeichert; die Zutrittsentscheidung fällt aber am Ort des Zutritts, entweder durch automatische Freigabe der Tür oder durch händisches Öffnen. Häufig sind dezentrale Lösungen mit Wach- oder Portierpersonal kombiniert, das eine zusätzliche Überprüfung vornimmt. *G. B.*

Foto: Sorex