Elektronische Zugangssysteme

Biometrisch bequem und sicher ins Haus

Die meisten von uns benutzen heute noch den guten alten Sicherheitsschlüssel, um ins Haus zu gelangen. Aber die Garage öffnet man bequem mit einem Funkbefehl, das Auto sowieso. Weshalb nicht auch den Zugang ins Haus in moderner Technik ausführen? Wir zeigen und diskutieren zeitgemäße Technik für diese komfortable Art der Türöffnung. Im zweiten und abschließenden Teil geht es vor allem um biometrische Systeme, aber auch um Versicherungsfragen.

Finger, Auge, Gesicht oder Hand?

Neben den „technischen" Zugangssystemen spielen die biometrischen Systeme eine stetig wachsende Rolle, gelten sie doch als besonders sicher, und man benötigt für den Zugang nichts als „sich selbst". Jeder Mensch verfügt über zahlreiche, mit geeigneter Sensortechnik sehr zuverlässig auswertbare Merkmale. An erster Stelle der entsprechenden Zugangstechnik stehen hier die schon seit geraumer Zeit sehr ausgereiften Fingerabdruckscanner, die einen oder mehrere Fingerabdrücke nach bestimmten Kriterien identifizieren können.

Wahrscheinlich auch aufgrund der Verkaufspreise folgen erst mit Abstand die Erkennungssysteme für die Augeniris, das Handvenenmuster und die Gesichtserkennung. Letztere, ebenso wie Fingerabdruckscanner und Irisdetektoren, kennen viele von uns ja bereits aus der Computer- bzw. Arbeitswelt oder gar vom eigenen Smartphone. Hier haben sich diese Systeme bereits bewährt, sie erfordern zum Teil aber tatsächlich auch die erst heute zur Verfügung stehende hohe Rechenleistung moderner Smartphones.

Nach und nach ziehen alle diese Techniken in die Welt der privaten Zugangssysteme ein – im professionellen und Hochsicherheitsbereich sind sie bereits seit Langem eingeführt.

All diese genannten Systeme basieren immer auf den Komponenten Sensor – einer Auswerteelektronik, die die geforderten Sicherheitsmerkmale bzw. Referenzmuster (darauf kommen wir noch jeweils) über Algorithmen ausfiltert und speichert sowie ggf. nicht erfassbare biometrische Merkmale abweist – und Vergleichsalgorithmus, der die Übereinstimmung oder eben Nichtübereinstimmung der gespeicherten Merkmale mit der aktuellen Sensoreingabe feststellt. Dabei sind, je nach technischem Verfahren, sehr komplexe Rechenkapazitäten erforderlich, vor allem, um eine möglichst sichere Übereinstimmung zwischen hinterlegter Referenz und aktueller Erfassung zu gewährleisten. Um das jeweilige System auch bedienfreundlich und zuverlässig zu gestalten, muss es gleichzeitig eine hohe Rate der schnellen Erkennung Berechtigter (Falschabweisungsrate FRR) und eine möglichst geringe Rate der Zugangsgewährung Unberechtigter (Falschakzeptanzrate FAR) realisieren. Ein technischer Spagat für Entwickler wie verantwortliche Betreiber gleichzeitig, der allerdings auch in einer Norm, der ISO/IEC 19795, in eindeutige Grenzen gefasst ist.

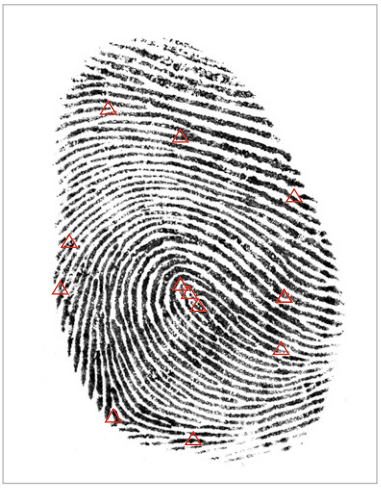

Bild 1: Zur Identifizierung eines Fingerabdrucks wird eine Reihe bestimmter Merkmale (Minuzien, rot markiert) erfasst und als individuelles Muster gespeichert.

Den Finger, bitte!

Der Fingerabdruckscanner ist auch im Privatbereich auf dem Sprung, andere Systeme großflächig abzulösen, besticht er doch durch einfache Handhabung und hohe Zugangssicherheit. Jeder Mensch hat auf seinen Fingerkuppen einmalige Papillarlinienmuster, -endungen, -verzweigungen (Minuzien, siehe Bild 1), anhand derer man ihn eindeutig identifizieren kann. Diese sind ein Leben lang weitgehend konstant, lediglich bestimmte Verletzungen, starke Alterungserscheinungen oder noch stark im Wachstum befindliche Finger von Kindern bis sechs Jahre können eine Wiedererkennung einschränken. Zu den unveränderlichen Merkmalen zählen dabei Breite und Verlauf der Papillarlinien, Schleifen, Wirbel, Gabelungen, Linienenden usw.

Betrachten wir das Verfahren anhand des optischen Sensors einmal kurz. Ein Sensor nimmt zunächst nach unterschiedlichen Verfahren das gesamte Bild der von einer integrierten Lichtquelle angestrahlten Fingerkuppenfläche als stark kontrastiertes Graustufenbild auf, sodass schließlich ein detailliertes Schwarz-Weiß-Bild entsteht. Jetzt treten die Algorithmen in Aktion, indem die eben erwähnten Minuzien erfasst und im Bild markiert werden (Bild 1). Nach Norm reichen dazu tatsächlich zwölf dieser Merkmale aus, um einen Abdruck eindeutig zu identifizieren. Allerdings gehen die technisch hochwertigeren Systeme deutlich weiter, 50 und mehr Minuzien sind ein deutliches Qualitätsmerkmal. Deren Lage im Bild wird nun abgespeichert und durch die eindeutige geometrische Lage zueinander erfolgt später der Vergleich und die Wiedererkennung oder Abweisung, auch wieder anhand sogenannter Matching-Algorithmen.

Bild 2: Weit verbreiteter Vertreter der optischen Fingerabdruckscanner mit Flächensensor – der Sebury F007-2

Für die Sensoren kommen hier mehrere technische Verfahren zum Einsatz, so optische Sensoren (Bild 2), HF-Sensoren, thermische und kapazitive (besonders in Smartphones und Laptops verbreitete) Sensoren. Sie werden je nach Systemaufwand ergänzt durch weitere 3D-, HF-, Infrarot- und Ultraschallsensoren, die ein besonderes Merkmal guter Fingerabdruckscanner möglich machen, die Lebenderkennung. Hier werden z. B. Porentiefe, Puls, Durchblutung, Körperwärme oder HF-Leitfähigkeit des Fingers registriert, so kann es nicht zu den in den Anfangszeiten des Verfahrens kritisierten Manipulationsversuchen etwa durch abgeformte Fingerabdrücke oder gar Leichenfinger kommen. Auch kann man so einen verschmutzten Empfänger bzw. einen Finger auf einer verschmutzen Sensorabdeckung schneller erkennen. Optische Sensoren arbeiten mit einem Bild-/Zeilensensor, kapazitive mit Kondensator-Arrays, die bei Auflegen des Fingers ein komplexes Ladungsbild der Papillarlinien erzeugen.

In der Gerätepraxis unterscheidet man im Wesentlichen zwischen dem „halbautomatischen" Scanner, bei dem man den Finger über eine schmale Sensorfläche (Zeilensensor) zieht (Bild 3), und dem „automatischen" Scanner, der den Fingerabdruck durch einfaches Auflegen auf die

Bild 3: Der Fingerabdruckscanner Idencom BioKey Gate arbeitet mit einem robusten Zeilensensor. Bild: Idencom

Bild 4: Automatischer Scanner, hier der SF300, im Einsatz an einem elektrischen Hoftor. Er ist als IP66-Gerät für den harten Außeneinsatz geeignet und verfügt zusätzlich über einen RFID-Leser.

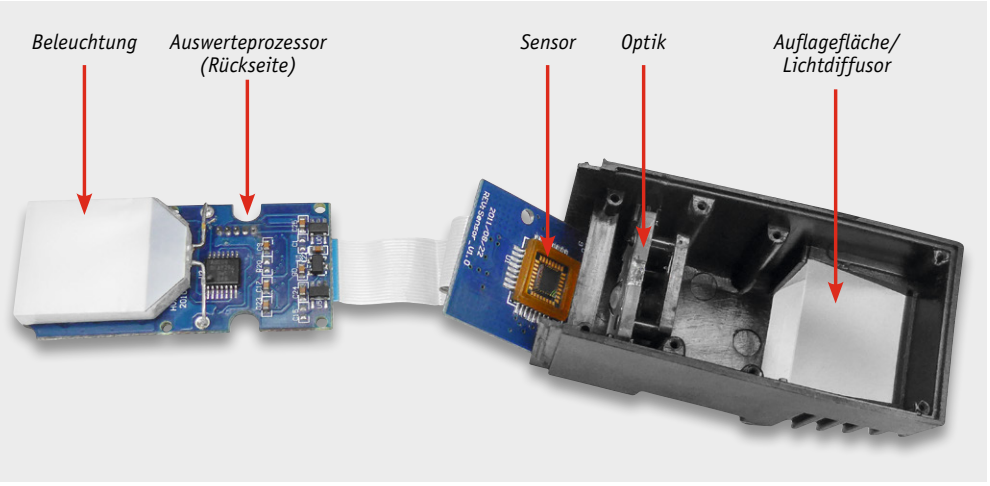

Bild 5: Ein zerlegter Flächenscanner, man erkennt deutlich die Baugruppen Auflagefläche/Lichtdiffusor, Optik, Sensor und Elektronik/Beleuchtungseinheit.

größere Sensorfläche erfasst (Bild 4). Blickt man einmal ins Innere eines solchen Sensors (Bild 5), kann man die wesentlichen Bauteile gut identifizieren: die Auflagefläche, die Optik zur Bildfokussierung, den Flächen-Bildsensor und die Auswerteelektronik, die schließlich weitere Baugruppen wie Relaissteuerungen, Wiegandcoder oder Funkbaugruppen zur Ausgabe ansteuert.

Bild 6: Der BioKey-Scanner von Idencom ist so kompakt und komfortabel, dass er sogar direkt in kompakte Türbeschläge integriert werden kann, hier in einen Beschlag der Firma Hoppe. Bild: Idencom

Bild 7: Geeignet für hochwertige Selbstbauprojekte – der Fingerabdrucksensor ZFM-708

Beide Scannerarten haben ihre Vorteile. Wesentliche Vorteile des halbautomatischen Scanners sind der Wegfall einer Sensorfläche, auf der ein kompletter Fingerabdruck hinterlassen werden kann, die geringere Schmutzanfälligkeit, die einfachere Beheizbarkeit für die Lebenderkennung und allgemein die robuste Ausführung aufgrund der schmalen Sensorfläche. Der frühere Nachteil des schlechteren Einlesens ist längst beseitigt, hochwertige und moderne Scanner, die man sogar in kompakte Türgriffe (Bild 6) integrieren kann, registrieren einen Fingerabdruck durch sehr schnelles Abtasten aus der Bewegung heraus.

Die automatischen Scanner hingegen können auch Verschmutzungen des Fingers gut kompensieren, ihre Handhabung wird von manchen Benutzern als praktischer empfunden, sie sind allerdings auch anfälliger für Manipulation in der Weise, dass man durchaus Fingerabdrücke von der Scanneroberfläche generieren kann. Auch sind sie bei Fremdlichteinfall, im ungünstigsten Fall noch verbunden mit Schmutz auf der Scannerfläche, fehleranfälliger. Dies kommt allerdings stark auf den eingesetzten technischen Aufwand an. Es gibt Scanner für um die 15 Euro, wie sie etwa auf chinesischen Handelsplattformen angeboten werden, die auf entsprechend billiger Technik basieren und allenfalls im unteren Sicherheitslevel bei Inkaufnahme hoher Fehlerraten einsetzbar sind. Hochwertigere Scannerbaugruppen für die Selbstbauelektronik wie der in Bild 7 gezeigte Scanner stechen nicht nur mit einer schnellen Erfassungsrate, geringer Falschakzeptanzrate und hoher Falschabweisungsrate hervor, sie erkennen auch nasse und schmutzige Finger, kompensieren etwa einen Kondensatfilm und sind mit einer speziellen Hintergrundbeleuchtung versehen, die Falschlicht kompensiert. Auch das Anlernen erfolgt hier schneller als beim Billig-Scanner, da die eingesetzte Rechentechnik bzw. Software leistungsfähiger ist. Die in Bild 7 gezeigte Scannerbaugruppe findet auch ihren Einsatz in vielen Fingerabdruckscannern der unteren und mittleren Preisklasse.

Ein großes Thema ist aber hier neben der eigentlichen Sensor- und Sicherheitstechnik ein robuster Aufbau, eine hohe Manipulationssicherheit und bei Außeneinsatz eine hohe Witterungsbeständigkeit und Zuverlässigkeit unter verschiedenen klimatischen Bedingungen.

Die nächste Entscheidung für den Einsatz eines solchen Türöffnungssystems muss man auf der Ausgabenseite treffen. Es gibt Standalone-Geräte, die bis hin zum auslösenden Relaiskontakt oder auch integriertem Motorschloss (siehe dazu auch Teil 1 des Artikels, Bild 5) sämtliche Technik beherbergen, auch erfolgt das Anlernen hier direkt am Gerät. Die zweite Klasse sind die in Sensor und Controller unterteilten Geräte. Hier findet man lediglich den eigentlichen Sensor samt seiner Peripherie im Außengerät, die Auswertung und Schlossansteuerung übernimmt ein sicher im Innenbereich untergebrachter Controller. Die Übertragung erfolgt hier codiert per Kabel oder Funk. Natürlich eignen

sich besonders diese Scanner sehr gut für die Anbindung an die weitere Haustechnik – so kann ein Funk-Interface sehr einfach mit untergebracht bzw. angesteuert werden.

Weitere Kriterien, die beim Kauf bedacht werden müssen, sind Stromausfallsicherheit (also Abwägen zwischen Batterie- und Netzbetrieb bzw. verfügbare Notstromfunktion), einfaches Anlernen und die individuell zu planenden Installations- und Integrationsmöglichkeiten in die eigene Türanlage. Auch eine Notschlossfunktion sollte hier immer einkalkuliert werden. Ein letztes Wort noch zu den Fingerprintscannern. Wem die Sicherheitsstufe hier noch zu gering ist: Es gibt auch Scanner, die die Eingabe mehrerer Fingerprints in bestimmter Reihenfolge erfordern. Systeme im professionellen Bereich können sogar das gleichzeitige Auflegen von mehreren Fingern anfordern.

Durch das Auge ...

Neben dem Fingerabdruck verfügen wir über weitere unverwechselbare Merkmale, die eine einzigartige Zuordnung zu einem Menschen möglich machen, so das Muster der Iris (Regenbogenhaut) des Auges, das ebenfalls lebenslang erhalten bleibt (Bild 8).

Der sogenannte Iris-Scanner setzt dazu im Wesentlichen eine hoch auflösende Kamera und Infrarotlicht ein. Auch hier wird, wie beim Fingerabdruck, das individuelle Irismuster erfasst, hier sind es allerdings bis zu mehrere Hundert optische Besonderheiten, die erfasst, gespeichert und ausgewertet werden. Der Iris-Scanner weist aufgrund dieser detaillierten Erfassung ein extremes Verhältnis zwischen Falschakzeptanzrate (quasi null Prozent) und Falschabweisungsrate (nahe 100 Prozent) auf.

Im Consumerbereich finden wir heute Iris-Scanner vor allem in einigen Smartphone- und Tablet-Modellen, die von der technischen Ausstattung her bereits prädestiniert sind. Hier ist der Knackpunkt allein die Softwareseite, die entsprechende Rechentechnik erfordert.

Aber auch in der Türöffnungstechnik ziehen diese Geräte sukzessive ein. So bietet z. B. EyeLock einen einfach installierbaren Iris-Scanner an, der bei einer Erfassung von mehr als 240 Irismerkmalen eine Akzeptanz-Fehlerquote von eins zu 1,5 Mio. aufweist, die noch durch Einbeziehung des zweiten Auges erhöht werden kann. Verbunden ist die eigentliche Scannertechnik mit dem Controller über eine hochsichere AES256-Verschlüsselung, und es stehen verschiedene Interfacesysteme wie Wiegand, F2F, OSDP und PAC zur Verfügung. Das Nano-System von EyeLock steht sowohl für den Innen- als auch für den Außenbereich zur Verfügung. Alternativ zur Scanner-Hardware an der Tür gibt es auch zahlreiche Lösungen, die auf der Iriserkennung per Smartphone basieren und dann mit entsprechenden Embedded-Systemen in Gebäuden, Fahrzeugen oder Maschinen oder sogar Bezahlsystemen zusammenwirken. Zu überlisten ist diese Technik kaum, denn bereits kurze Zeit nach Unterbrechung des Blutkreislaufs zerfallen die Irisstrukturen, trotzdem verfügen auch Iris-Scanner über Algorithmen zur Lebenderkennung.

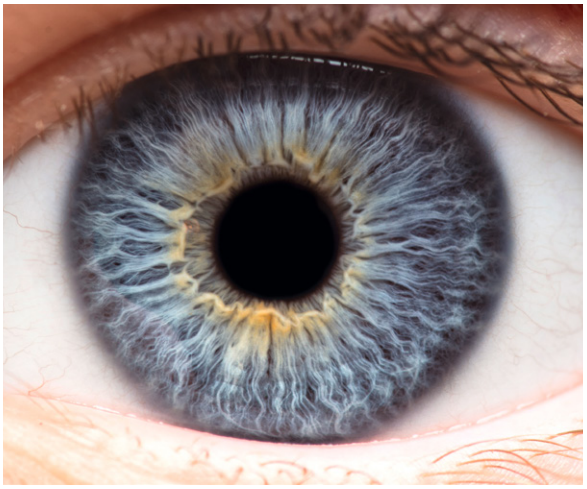

Bild 8: Einmalig: die Regenbogenhaut (Iris) jedes Menschen

Gesicht zeigen!

Die Technik der Gesichtserkennung (engl. Facial Recognition) ist eine weitere Technologie zur Erfassung und Auswertung biometrischer Merkmale. Hier wird das Gesicht mit einer Infrarot-Kamera aufgenommen, und die Software setzt je nach Aufwand bis zu 100 Markierungspunkte, um eine wirklich eindeutige Erkennung zu ermöglichen. Wie sich leicht nachvollziehen lässt, ist das menschliche Gesicht im Lauf des Lebens zahlreichen Veränderungen unterworfen, dazu kommen unterschiedliche Merkmale wie Bärte, kosmetische Operationen, Brillen usw. Deshalb wird hier auch ein dreidimensionales Bild erstellt, das typische, unveränderliche Merkmale (Nodes) wie etwa Augenabstand, Abstand und Lage der Backenknochen und andere Strukturmerkmale erfasst und auswertet. Die dahinter stehende Rechentechnik ist sehr komplex, dazu kommen auch hier weitere Erkennungsalgorithmen, um nicht etwa mit Fotos oder einem Video das System zu überlisten. Deshalb verfügen Iris-Scanner nicht nur über hochwertige Spezialkameras, der Fokus liegt hier auf der zugehörigen, äußerst komplexen Software, die derzeit noch entwicklungsbedürftig ist. Wohl auch der Grund dafür, dass diese Technik bisher außer bei einer Smartphone-Anwendung (Apple-Face-ID-Technik im iPhone X) kaum Einsatz im Consumerbereich findet, da sie enorme Rechnerressourcen bindet.

Bild 9: Installationsbeispiele für hochwertige Handvenenleser. Hier muss man die Hand nicht einmal auflegen, einige Zentimeter Abstand genügen.
Bilder: Frank Türen AG

Bild 10: Einfach das Smartphone darunter halten – der QR-Codescanner, links in das Außengehäuse integriert, bietet sich besonders für temporäre Zugänge an. Bild: I-Keys

Hand auflegen

Nein, nicht wie auf dem Jahrmarkt – die sogenannten Handvenenleser sind deutlich dichter an der Wahrheit. Auch diese Sensoren werten biometrische Merkmale aus, nämlich das ebenfalls einmalige Muster der Venen in der Hand. Auch hier gibt es absolut individuelle Verteilungen, Abstände, Verästelungen. Dazu wird der Blutfluss in den Venen erfasst. Eine Weitwinkelkamera und ein Infrarot-Scanner erfassen diese Merkmale, die als hoch fälschungssicher gelten, da sie im Körper liegen, somit optisch nicht fälschbar sind. Auch die Lebenderkennung ist hier anhand des Durchblutungsstatus prinzipbedingt hochsicher. Dementsprechend gering geben die Hersteller die Fehlerquoten an. Gegenüber dem Fingerabdruckscan gilt das Verfahren u. a. als hygienischer, da die Erkennung auch berührungslos erfolgen kann. In Bild 9 auf der vorherigen Seite sind Installationsbeispiele für diese Technik zu sehen.

Von der Interface- und Verschlüsselungstechnik sowie der technischen Einbindung her ist auch diese Technik ähnlich ausgeführt wie die bisher diskutierten Systeme.

Damit wollen wir unseren Streifzug durch die biometrischen Zugangssysteme beenden und uns am Schluss noch kurz einem recht neuen und immer mehr Verbreitung findenden Zugangsverfahren sowie einigen versicherungstechnischen Aspekten widmen.

Ich schicke Ihnen den Code ...

Im Zeitalter des Smartphones ermöglicht die mobile Technik ganz neue Aspekte unseres Themas, so z. B. den Zugang über QR-Codes. Der ist zunehmend vor allem dort verbreitet, wo es gilt, fremden Personen zeitweise Zugang zu gewähren – von der Reinigungskolonne über den Parkhauszugang bis zum Ferienhausaufenthalt. Man generiert einen QR-Code, hinterlegt diesen per Netzwerk in einem Controller im Gebäude. Der Berechtigte bekommt den QR-Code auf sein Smartphone gesendet und muss dieses dann nur noch unter den QR-Code-Leser (Bild 10) halten, um Zugang zu bekommen. Das ist dann insgesamt noch sicherer als beispielsweise der Zugang über Magnetstreifenkarten, wie man sie aus Hotels kennt.

Und was sagen die Versicherer?

Ein elektrisches Zugangssystem wird grundsätzlich von den meisten Versicherern, z. B. in der Hausratversicherung, genauso bewertet wie ein mechanisches System. Die Bedingung ist allerdings, dass die elektrischen Systeme die Tür genauso sicher verriegeln, wie dies mit einem mechanischen Schloss und Schlüssel erfolgt. Das heißt, dass ein Verriegeln mit dem elektrischen System möglich sein muss und die Tür grundsätzlich nach einem Öffnen wieder verschlossen wird. Ein normales Ins-Schloss-Fallen („Zuhaltung") wird bei einfachen Wohnungstüren (anders als bei entsprechend ausgerüsteten Gebäudetüren mit Selbstverriegelung beim Zufallen) auch versicherungstechnisch genauso bewertet – der Versicherer stellt sich meist leistungsfrei oder haftet eingeschränkt. Die sichere Lösung ist hier das im ersten Teil des Artikels bereits angesprochene selbstverriegelnde Elektroschloss, das sich jedes Mal nach Schließen der Tür wieder verriegelt. Und natürlich sind die dort genannten Grundregeln der Installation zu beachten, beispielsweise zur Verkabelung und deren Zugänglichkeit.

Ein herkömmlicher Schlüssel wird von vielen Versicherern sogar als unsicherer betrachtet als z. B. ein Fingerprint. Da dies jedoch keinesfalls auf alle Produkte im Bereich der elektrisch-elektronischen Zugangssysteme zutrifft, sollte man vor der Anschaffung eines solchen Systems Rücksprache mit seinem Hausratversicherer halten. Hier muss man auch mit dem Versicherer den Aspekt besprechen, was passiert, wenn es keine Einbruchspuren gibt. Bei herkömmlichen Schlüsseln kann man weitgehend plausibel erklären, ob alle Schlüssel vorhanden sind, der Täter also illegale Öffnungsmittel/Nachschlüssel verwendet haben muss. Bei einem elektronischen Zugangssystem wird das schwieriger, es sei denn, das System erfüllt bestimmte Bedingungen, die besonderen VdS-Kriterien folgen. Solch ein Kriterium ist z. B. der Nachweis über die letzten Öffnungsversuche mit einem internen Speicher des Systems. Deshalb verfügen gute Systeme über einen solchen Speicher mit Zeitstempel. Ebenso speichern hochsichere Systeme keine kompletten Bilder z. B. des Fingerabdrucks, sondern nur das ermittelte Koordinatengerüst des Abdrucks, das einem Datendieb nichts nutzt. Auch weitere Kriterien, die wir bereits bei den Zugangssystemen im ersten Teil des Artikels diskutiert haben wie Sperrung nach mehreren Fehlversuchen, getrennte Innen- und Außeneinheit usw., sollte man hier beachten und sich explizit von seinem Versicherer bestätigen lassen, dass er bei ordnungsgemäßem Einbau des Systems im Schadensfall eintritt.

Unter [1] hat der Anbieter des weit verbreiteten BioKey-Systems einige dieser Kriterien übersichtlich zusammengefasst.

Dazu kommt noch ein weiterer Aspekt: Wenn man eine Video-Türsprechanlage mit automatischer Aufzeichnung betreibt, sind dadurch alle Besucher optisch erfasst. ELV

Weitere Infos:

[1] www.idencom.com/versicherungsschutz/sicherheitskriterien/

Informationen zu Fingerabdruckscannern im ELV Shop finden Sie unter www.elv.de ...at ...ch: Webcode #10243