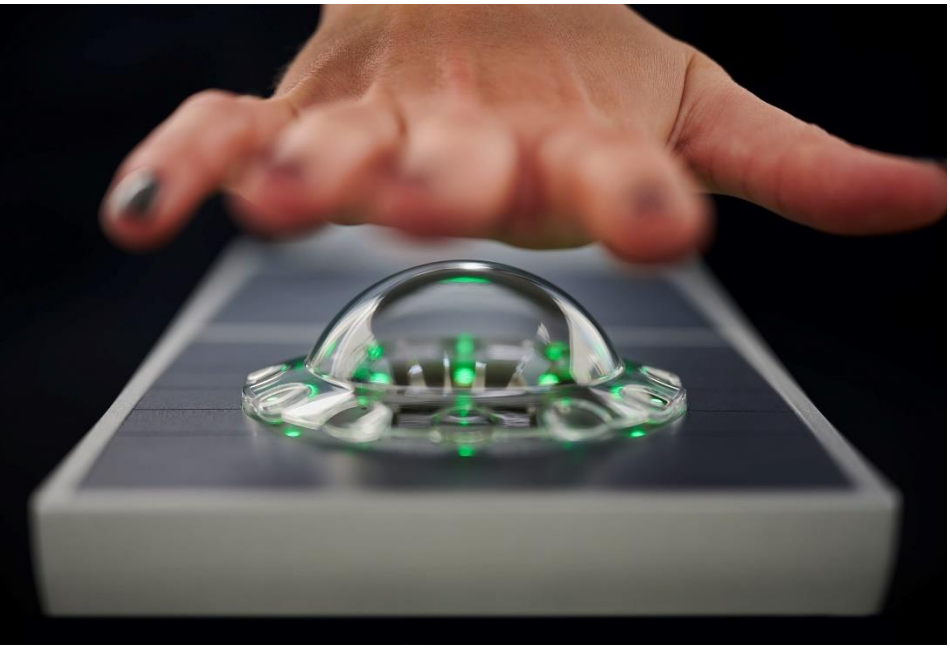


WHITE PAPER

Handvenenerkennung

Komfortabel wie Fingerprint,
hochsicher wie Retinaerkennung.
Die Quadratur des biometrischen Kreises?

Stand: Juli 2019

Inhalt

Die Informationen dieses WhitePapers wurden mit größter Sorgfalt zusammengestellt. PCS kann jedoch keine Gewährleistung dafür übernehmen, dass dieses Dokument frei von Fehlern ist. Verbindlich sind technische Daten ausschließlich, wenn sie im Rahmen eines Auftrages vom technischen Support der PCS geprüft und freigegeben wurden.

Marken: PCS, INTUS, DEXICON, „The terminal people.“ und „INTUS. The terminal.“ sind eingetragene Marken der PCS Systemtechnik GmbH. PalmSecure™ ist eine Marke der Fujitsu Ltd. Alle anderen Marken oder Produktnamen sind Marken oder eingetragene Marken der jeweiligen Firmen und Organisationen.

Copyright © 2019 PCS Systemtechnik GmbH

1 Biometrische Zutrittssysteme: Überflüssige Spielerei?

Schon seit vielen Jahren haben sich elektronische Zutrittssysteme bei großen und kleinen Unternehmen durchgesetzt. Kein Wunder, bieten Sie doch zahlreiche Vorteile. Sie arbeiten 24 Stunden lang, rund um die Uhr, kennen keine Feiertage oder Wochenenden, können gezielt Personengruppen eingeschränkte Rechte zuweisen („nur werktags“, „nicht nachts“,…) und protokollieren automatisch mit, was am Eingang zu einem Firmengelände passiert – gegebenenfalls kombiniert mit einer Videodokumentation.

Ein wichtiger Grund für die zunehmende Verbreitung von elektronischen Zutrittssystemen ist neben dem geschärften Sicherheitsbewusstsein in den Führungsebenen zweifellos auch das erhöhte Gefahrenpotential z. B. in Form von Industriespionage. Der Diebstahl von geistigem oder materiellem Eigentum als Folge eines unzureichenden Zutrittssystems kann Unternehmen Millionen Euro kosten, ganz abgesehen von der Rufschädigung, falls derartige Vorfälle an die Öffentlichkeit dringen. Die klassischen Sicherheitsmechanismen mit Schlüsselverteilung an Mitarbeiter reichen hier nicht mehr aus.

1.1 Trügerische Sicherheit durch Beschränkung auf ein Medium

Diese komfortable Technik kann aber auch ein falsches Sicherheitsgefühl hervorrufen. Üblicherweise werden heute RFID-Zutrittsmedien eingesetzt. Aus Gründen der Bequemlichkeit verzichtet man oft auf zusätzliche Identifikationsmerkmale wie PIN und ermöglicht Mitarbeitern den Zutritt zu einem Gebäude ausschließlich per Karte. Diese RFID-Ausweise können jedoch verloren gehen, sie können bewusst an nicht-autorisierte Personen weitergegeben oder gestohlen werden.

Durch den gleichzeitigen Einsatz einer PIN lässt sich zwar der Missbrauch von gestohlenen oder verloren gegangene Karten vermeiden. Die gezielte Weitergabe einer PIN zusammen mit einem Ausweis ist aber weiterhin möglich.

Die wirksame Lösung zur Vermeidung dieses Problems ist die Authentifikation von Personen mit Hilfe von biometrischen Merkmalen. Am weitesten verbreitet ist dabei der Fingerabdrucksensor, mit dem beispielsweise vermieden werden kann, dass sich gelernte Arbeitskräfte durch nicht-qualifiziertes Personal vertreten lassen.

Dabei ist das Fingerprint-Verfahren nicht ganz unproblematisch. Fingerabdrücke können mit moderatem Aufwand nachgemacht werden und das Sicherheitsniveau der Technologie (konkret: die Falsch-Akzeptanz-Rate FAR) ist mittelmäßig. Zusätzlich gibt es hygienische Bedenken durch die kontaktbehaftete Nutzung.

1.2 Bedrohungsspezifisches Sicherheitskonzept

Viele Firmen setzen auf ein bedrohungsspezifisches Sicherheitskonzept, das verschiedene Gefährdungsbereich definiert. Für den Zutritt zu normalen Firmengebäuden oder Geländen reicht eine übliche Zutrittskarte allein aus. Für den Zutritt zu sensibleren Bereichen oder am Wochenende muss zusätzlich eine PIN eingegeben werden. Und in den absoluten Hochsicherheitsbereich (Rechenzentrum, Research & Development, Vorstandsetage, etc.) kommt nur, wer sich zusätzlich mit einem biometrischen Merkmal ausgewiesen hat. Auf diese Weise werden unnötig komplizierte und zeitaufwändige Zutrittsprozeduren für die Mehrzahl der Mitarbeiter vermieden und wirklich sicherheitskritische Bereiche trotzdem sicher vor unberechtigten Zutritten geschützt. Dadurch werden zudem Kosten optimiert, da die Mehrzahl der Zutrittsleser preiswerte RFID-Leser sind, nur ein kleinerer Teil davon ist mit der zusätzlichen PIN-Tastatur ausgestattet und die teureren biometrischen Leser sind nur bei den wirklich kritischen Türen installiert.

1.3 Positionierung der biometrischen Verfahren

Neben der schon erwähnten Fingerabdrucktechnologie, die einen Marktanteil von über 50 Prozent aufweist, gibt es weitere biometrische Lösungen wie Handgeometrie, Iriserkennung, Retinaerkennung, Gesichtserkennung und Sprachmustererkennung um nur einige zu nennen. Jedes dieser Systeme hat eigene Vor- und Nachteile. Häufig muss sich der Anwender entscheiden, was er möchte: Komfort oder Sicherheit. Die wenigsten Systeme bieten beides gleichermaßen. Eine willkommene Ausnahme stellt die Handvenenerkennung dar. Einfach und komfortabel wie der Fingerprint und zugleich hochsicher. Die folgende Grafik zeigt eine Gegenüberstellung der verbreitetsten Technologien hinsichtlich der relevanten Eigenschaften bei biometrischer Zutrittskontrolle.

Forderung	Begründung	Handvenenmuster	Iriserkennung	Fingerprint	Face Recognition
Einzigartigkeit	Unterschiedlich für jede Person	👍	👍	👍	👎
Universalität	Kommt bei jeder Person vor	👍	👍	👎	👍
Konstanz	Ändert sich temporär und zeitlebens nicht	👍	👍	👎	👍
Benutzerakzeptanz	Einfache, bequeme Handhabung	👍	👎	👍	👍
Sicherheit	Hoher Aufwand bei Fälschung, datenschutzgerecht	👍	👎	👎	👎
Anwendbarkeit	Ohne Einschränkung bei jeder Person	👍	👍	👎	👍

Abbildung 1: Merkmale biometrischer Verfahren im Vergleich

Relevant ist zudem der Vergleich der verschiedenen Erkennungssysteme zueinander bezüglich Komfort und Sicherheit. Die Gesichtserkennung ist bequem für den Anwender, aber wie der Fingerprint vergleichsweise einfach zu überlisten. Die Retinaerkennung wiederum ist dagegen hochsicher, doch haben die wenigsten Menschen ein gutes Gefühl dabei, wenn ihnen ein

Infrarotlaser auf den Augenhintergrund leuchtet. Zudem muss über einen Zeitraum von mehreren Sekunden ein Punkt mit dem Auge fixiert und der Kopf ruhig gehalten werden – die Benutzerakzeptanz ist entsprechend niedrig.

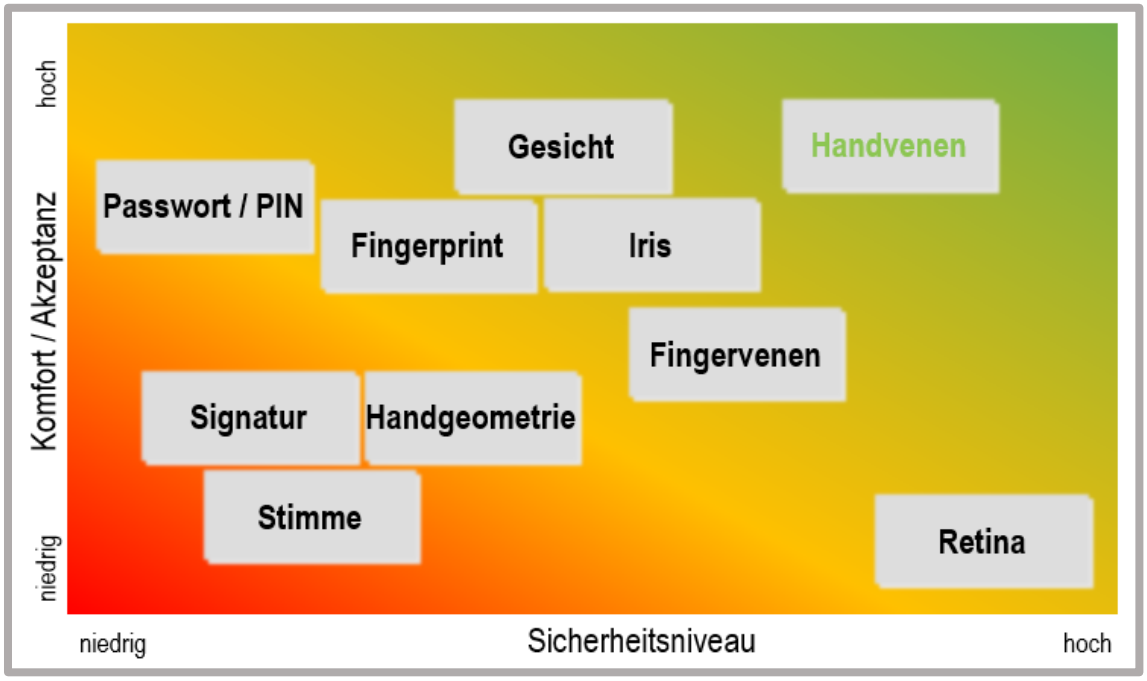


Abbildung 2: Positionierung von Sicherheitssystemen nach Komfort und Sicherheitsniveau

Es reicht folglich nicht aus, nur ein maximal hohes Sicherheitsniveau zu bieten. Genauso wichtig ist eine gute Ergonomie, damit die Biometrie vom Anwender akzeptiert wird. Das Ideal ist ein System, das hochsicher und trotzdem einfach zu bedienen ist.

Die Venenerkennung kommt diesem Ideal einen großen Schritt näher. Besonders die Handinnenflächen-Venenmustererkennung zählt zu den sichersten und trotzdem komfortabelsten biometrischen Verfahren. Sie ist hochsicher wie eine Retinaerkennung und dabei einfach in der Anwendung wie ein Fingerprintleser.

2 Venenerkennungssysteme im Vergleich

Neben der im Folgenden ausführlicher beschriebenen *Handinnenflächen-Venenmustererkennung* (im Folgenden Handvenenerkennung genannt) gibt es noch die Möglichkeit der *Fingervenen-Erkennung*, bei der die viel kleineren Venen in einem Finger gescannt werden. Wie weiter unten in diesem Dokument erläutert, unterscheiden sich die Verfahren wesentlich bezüglich Sicherheit, Komfort, Abweisungsraten oder Hygiene von der Handvenenerkennung.

2.1 Fingervenenerkennung

Bei der Fingervenenerkennung wird ein Finger in oder auf einen Sensor gehalten, der das Venenmuster des Fingers auswertet. Dazu wird er entweder von oben oder von der Seite beleuchtet und von unten gescannt.

Gegenüber der herkömmlichen Fingerabdruckerkennung hat die Venenerkennung den Vorteil, dass sich die erforderlichen Informationen nicht von jedem Gegenstand abnehmen und so potenziell fälschen lassen, wie bei einem Fingerabdruck-Leser.

Im Vergleich zu den nachfolgend beschriebenen Verfahren ist das Venenmuster eines Fingers um den Faktor 10 kleiner und damit entsprechend weniger komplex als das Venenmuster innerhalb einer Handfläche. Daraus resultiert eine entsprechend geringere Genauigkeit bei der Erkennung. Ein weiterer Nachteil: Die Venen in einem Finger sind empfindlich bei Kälte; Kapillar-Venen können sich bei kalten Fingern komplett zusammenziehen, so dass sie nicht mehr erkannt werden können.

2.2 Handrückenvenenerkennung

Bei der Handrückenvenenerkennung wird das Muster des Verlaufs der Venen im Handrücken ausgewertet. Dieser muss dafür auf die Sensorfläche gedrückt werden – das Verfahren ist also kontaktbehaftet. Bei der Erfassung kann starke Behaarung und Pigmentflecken die Aufnahme stören. Aufgrund dieser Schwächen, die die Handvenenerkennung nicht teilt, konnte sich die Handrückenvenen-Erkennung nicht am Markt durchsetzen und spielt heute keine Rolle mehr.

2.3 Funktionsweise und Sicherheitsmerkmale der Handvenenerkennung

Bei der Handvenenerkennung wird das Muster des Verlaufs der Handvenen in der Handinnenfläche mit einer Kamera aufgenommen und ähnlich wie bei einem Fingerabdruck mit einem Referenzmuster verglichen.

Das physikalische Prinzip der Handvenenerkennung beruht auf der verstärkten Absorption von Infrarotstrahlen im sauerstoffarmen venösen Blut. Der PalmSecure™-Sensor von Fujitsu enthält unter anderem eine kleine Kamera, die Infrarotbilder aufnehmen kann, und Infrarot-LEDs, wie man sie beispielsweise von Fernbedienungen für Fernsehgeräte kennt. Hält man seine Hand vor den Sensor, sendet dieser über die Infrarot-LEDs Nah-Infrarotstrahlung in Richtung der Handfläche aus und führt eine Fake-Object-Detection durch. Ist diese erfolgreich abgeschlossen, wird mittels der eingebauten Nahinfrarot-LEDs Infrarotlicht mit einer Wellenlänge von 750nm an die Handfläche gesendet. Das sauerstoffreduzierte Blut in den Venen absorbiert diese Infrarotstrahlung. Damit kann ein eindeutiges Bild der Venen innerhalb der Hand aufgenommen und für die Erkennung verwendet werden.

Sobald sich die eingebaute Weitwinkel Nah-Infrarotlicht-Kamera fokussiert hat, erfasst sie etwa **5 Millionen Referenzpunkte** des Handflächenvenenmusters und erstellt zunächst ein RAW-Image, das eine Größe von etwa 5 MB hat. Die Venen sind auf diesem Bild wegen der erhöhten Lichtabsorption als dunkle Linien zu erkennen. Dieses RAW-Image wird innerhalb des PalmSecure-Sensors nach AES 128 Bit oder **AES 256 Bit verschlüsselt.** Die so verschlüsselten Rohdaten werden zusätzlich mit einem Zufallsalgorithmus versehen und über die USB-Schnittstelle zur weiteren Verarbeitung und Templategenerierung an den INTUS PS Controller oder die Einlernsoftware übergeben.

Die in der Einlernsoftware integrierte Authentication Library wandelt die Bilddaten in ein biometrisches Template um. Bei der Generierung des Templates wird dieses nochmals mit **AES 128 Bit oder AES 256 Bit verschlüsselt.** Abhängig davon, ob das Template in der Datenbank oder auf einer RFID-Karte gespeichert werden soll, ist es 3 kByte (Template-On-System) oder 0,8 kByte (Template-On-Card) groß. Die Verschlüsselung erfolgt im Standard mit einem PCS-spezifischen AES-Schlüssel. Optional können Kunden die Verschlüsselung mit einem eigenen Schlüssel vornehmen.

Bei Template-On-System wird die Templatedatenbank von der Software an die INTUS PS Controller verteilt und ist so dezentral verfügbar. Bei Template-On-Card liegt das Template nur auf der RFID-Karte. Die biometrischen Daten liegen an **keiner Stelle** unverschlüsselt vor. Selbstverständlich kann aus dem Template, analog zu Fingerprint-Templates, auch kein Bild des originalen Handvenenmusters errechnet werden.

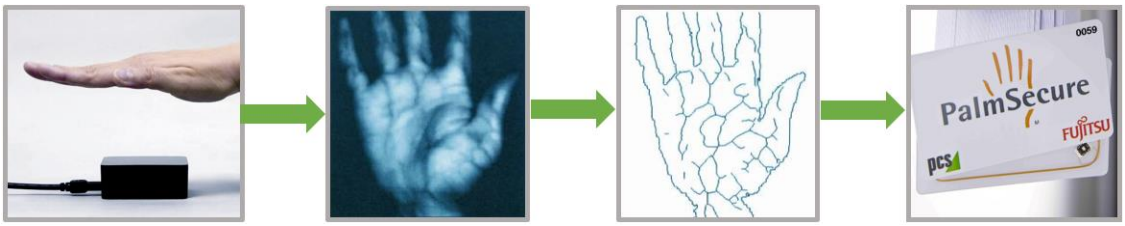


Abbildung 3: Ablauf der Handvenenerkennung

Das menschliche Handvenenmuster ist äußerst komplex und befindet sich innerhalb des Körpers, vor Missbrauch und Manipulationen bestens beschützt. Die Position der Venen bleibt zeitlebens unverändert und ist bei jedem Menschen unterschiedlich. Die FAR (Falsch-Akzeptanz-Rate) liegt bei der Handvenenerkennung bei 0,000.08%.

Die Handvenenerkennung ist in der Anwendung unproblematisch und unbedenklich. Das Verfahren ist unempfindlich gegenüber Hautverunreinigungen, Hautfarbe, Haaren, Muttermalen oder oberflächliche Verletzungen. Das Handvenenmuster verändert sich weder bei Wärme noch bei Kälte. Ein wichtiger Pluspunkt dieses biometrischen Verfahrens ist die Tatsache, dass die Identifizierung völlig berührungslos erfolgt, was für maximale Hygiene sorgt.

In zahlreichen Projekten hat sich die Handvenenerkennung bereits als zuverlässige und sichere Biometrielösung erwiesen. Außerdem kann das Erkennungssystem, ähnlich einem Fingerabdrucksensor, gut in Automaten, Geräten, Säulen oder Gehäusen von Gegensprechanlagen integriert werden. Noch wertvoller wird der Einsatz in Unternehmen, die Venenerkennung nicht nur für den physischen Zutritt zu Gebäuden oder Räumen einsetzen, sondern parallel für die Zugangskontrolle zu Rechnern und/oder Maschinen nutzen wollen.

2.4 Gefährliche Strahlung?

Bei jedem System mit „Strahlung“ wird sehr schnell die Frage nach der Gefährlichkeit gestellt. Bei der Handvenenerkennung wird Nahinfrarotstrahlung im Wellenbereich von $7{,}6 \cdot 10^{-7}$ mm genutzt. Das ist eine vergleichbare Strahlung, wie sie beispielsweise auch bei handelsüblichen Infrarot-Fernbedienungen von Fernsehern verwendet wird. Im Vergleich zu den Fernbedienungen ist die ausgesandte Strahlung beim PalmSecure-Sensor jedoch um den Faktor 10 geringer. Alle wichtigen Sicherheitsstandards in Europa und USA (UL, CSA, TÜV) werden eingehalten. So wird der Sensor in den USA verstärkt im Gesundheitswesen eingesetzt, in dem bekanntlich sehr hohe Sicherheitsanforderungen gestellt werden. Es lässt sich also guten Gewissens sagen, dass die Strahlung bei der Handvenenerkennung nachgewiesen im unkritischen Bereich liegt.

3 Die INTUS PS Handvenenerkennung und ihre Systembestandteile

PCS Systemtechnik GmbH vertreibt die Handvenenerkennung als Zutrittskontrollsystem. Um den biometrischen Leser als hochsicheres Zutrittssystem zu betreiben, gehören weitere Steuereinheiten zum INTUS Handvenenerkennungssystem. In der Betriebsart „Standalone“ genügt ein INTUS PS Leser und ein INTUS PS Controller. Die Zutrittsentscheidung und die Steuerung der Türen direkt durch den Controller. Bei größeren Installationen wird das Handvenenerkennungssystem über die OSDP-, LBus oder Wiegand-Schnittstelle an einen Zutrittskontrollmanager angeschlossen, welcher von einem übergeordneten Leitsystem gesteuert wird.

3.1 INTUS PS Handvenenleser-Modelle

PCS Systemtechnik vertreibt Zutrittskontroll-Leser mit Handvenenerkennung unter dem Namen **INTUS PS**. Der INTUS 1600PS-II wird für die Aufputzmontage verwendet, die INTUS PS Head Unit-3 für den Einbau in Säulen, Drehkreuze und Panels. Bei beiden Modellen stellt der PalmSecure-Sensor die Kernkomponente dar. Der Sensor wird von einem robusten Glasdom geschützt, umschlossen von der ‚MagicEye‘ genannten LED-Anzeige. Das MagicEye signalisiert den Status des INTUS PS Lesers über wechselnde Farben bei der Bedienung. Dazu können bis zu 200 verschiedene Farben genutzt werden. Der INTUS 1600PS-II kombiniert den Handvenensensor optional mit einem RFID-Leser und/oder einer PIN-Tastatur. Der RFID-Leser liest die Handvenen-Templates von der Zutrittskarte (Template on Card) oder dient als normaler RFID-Leser. Der INTUS PS Leser wird über zwei USB-Leitungen bzw. über eine Cat-5-Leitung per USB-Extender mit dem INTUS PS-Controller verbunden. Über diese Leitungen erfolgt auch die Spannungsversorgung des Lesers.

3.2 INTUS PS Controller

Als Steuereinheit dient der **INTUS PS Controller**, eine leistungsfähige Rechnereinheit mit Industrie-PC-Board, ausgelegt für 24/7-Betrieb, die primär die Aufgabe hat, die erfassten Templates mit den gespeicherten Templates zu vergleichen. Als Betriebssystem enthält der INTUS PS Controller ein embedded Linux-Kernel mit Realtime-Erweiterungen. Über zwei USB-Schnittstellen bzw. die Cat-5-Schnittstelle verbindet er sich mit dem INTUS PS-Leser. Eine Ethernet-Schnittstelle dient zum Anschluss an den übergeordneten Leitrechner, von dem der Controller u.a. die Templates erhält. Eine LBus-, OSDP- oder Wiegand-Schnittstelle dient zum Anschluss von Zutrittskontrollmanagern (wie INTUS ACM40e oder andere Fabrikate).

3.3 INTUS ACM

Der **INTUS ACM**, (auch Zutrittsmanager, Zutrittskontrollmanager oder Zutrittskontrollzentrale genannt) trifft im Rahmen der definierten Raum- und Zeitprofile autonom die Entscheidungen über Zutritt oder Zurückweisung, steuert die angeschlossenen Leser, die Türen, Schranken oder Drehsperren mit sei-

nen Überwachungskontakten (DI Digitaler Eingang, DO Digitaler Ausgang), sowie die angeschlossene Videoüberwachung für neuralgische Zutrittspunkte. Der Zutrittskontrollmanager ist mit dem Leitsystem über eine Ethernet-Schnittstelle verbunden.

3.4 Leitsystem

Das **übergeordnete Leitsystem** kontrolliert alle in einem Gebäude vorhandenen Zutrittskontrollmanager und versorgt sie mit den Stammdaten, wie „wer darf zu welchen Zeitpunkten welche Bereiche betreten“, „welche Räume dürfen nur von mehreren Mitarbeitern gleichzeitig betreten werden“ oder „wie lange darf sich eine Person maximal in einem Raum aufhalten“. Daneben verteilt sie die Handvenentemplates an die INTUS PS Controller.

4 Systemarchitektur - Beispiele

Die folgenden zwei Beispiele zeigen Möglichkeiten auf, die INTUS PS Handvenenerkennung in unterschiedlichen Situationen in ein Gesamtsystem einzubinden.

4.1 Einzeltür direkt gesteuert von INTUS PS als Standalone Lösung

Die Tür wird ohne Zutrittskontrollmanager direkt über die Relais-Schnittstelle des INTUS PS Controllers geöffnet. Die Lösung ist nicht eingebunden in eine übergeordnete Zutrittskontroll-Lösung, sondern wird mit der Software INTUS PS Small Enterprise administriert. So lassen sich Standalone-Lösungen schnell und einfach realisieren.

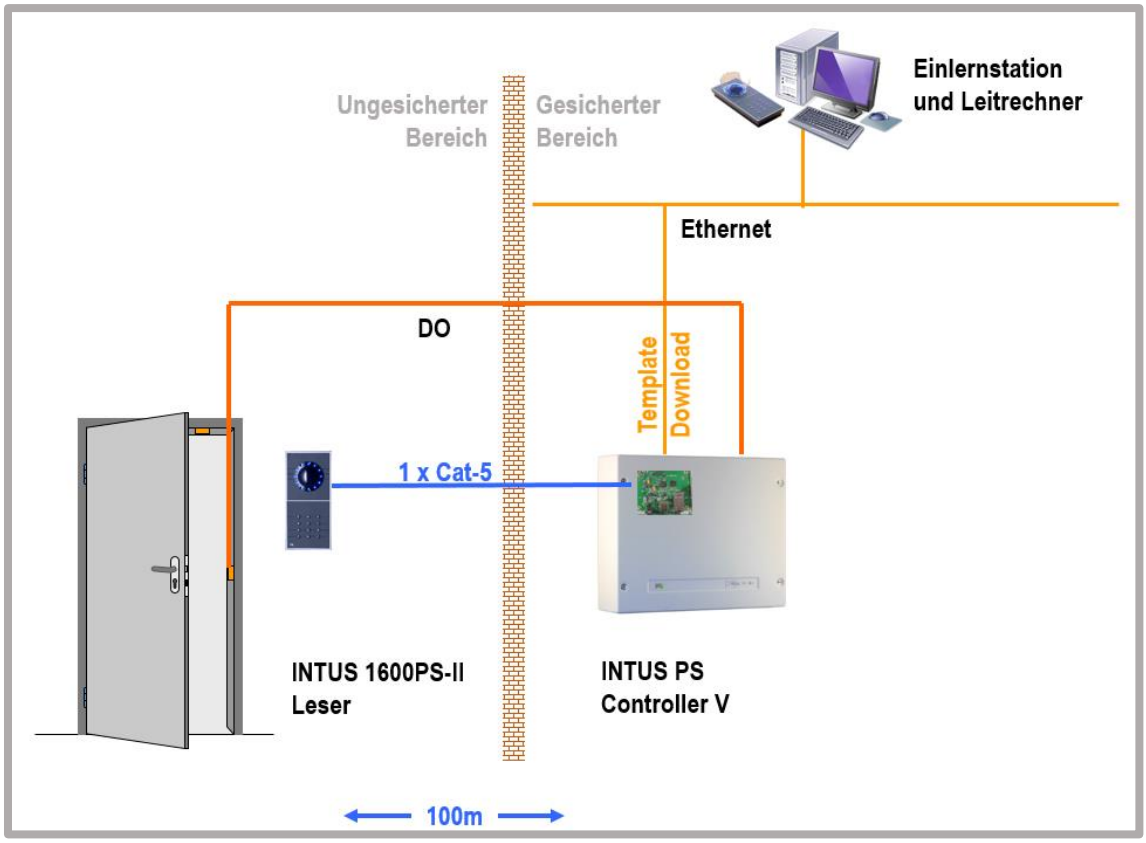


Abbildung 4: Konfiguration Handvenenerkennung für eine Tür

4.2 Vier Türen gesteuert über einen Zutrittskontrollmanager

An einen Zutrittskontrollmanager INTUS ACM40e können per LBus bis zu vier INTUS PS Systeme angeschlossen werden, das heißt zwei PS-Controller mit jeweils zwei INTUS PS-Lesern.

Für die Identifikation, bei der Betriebsart ‚Template On System', werden die Templates im System gespeichert und aus dem Leitrechner über die Ethernet-Schnittstelle in den INTUS PS-Controller herunter geladen, damit dort das aufgenommene Handvenenmuster im Controller mit dem Template der Person verglichen werden kann. Das Ergebnis wird an den Zutrittskontrollmanager übermittelt, der anhand des Raum-Zeitprofils die finale Zutrittsentscheidung trifft und die Tür öffnet, sofern die Person berechtigt ist. Die Anbindung an den Zutrittskontrollmanager erfolgt über LBus, OSDP oder Wiegand.

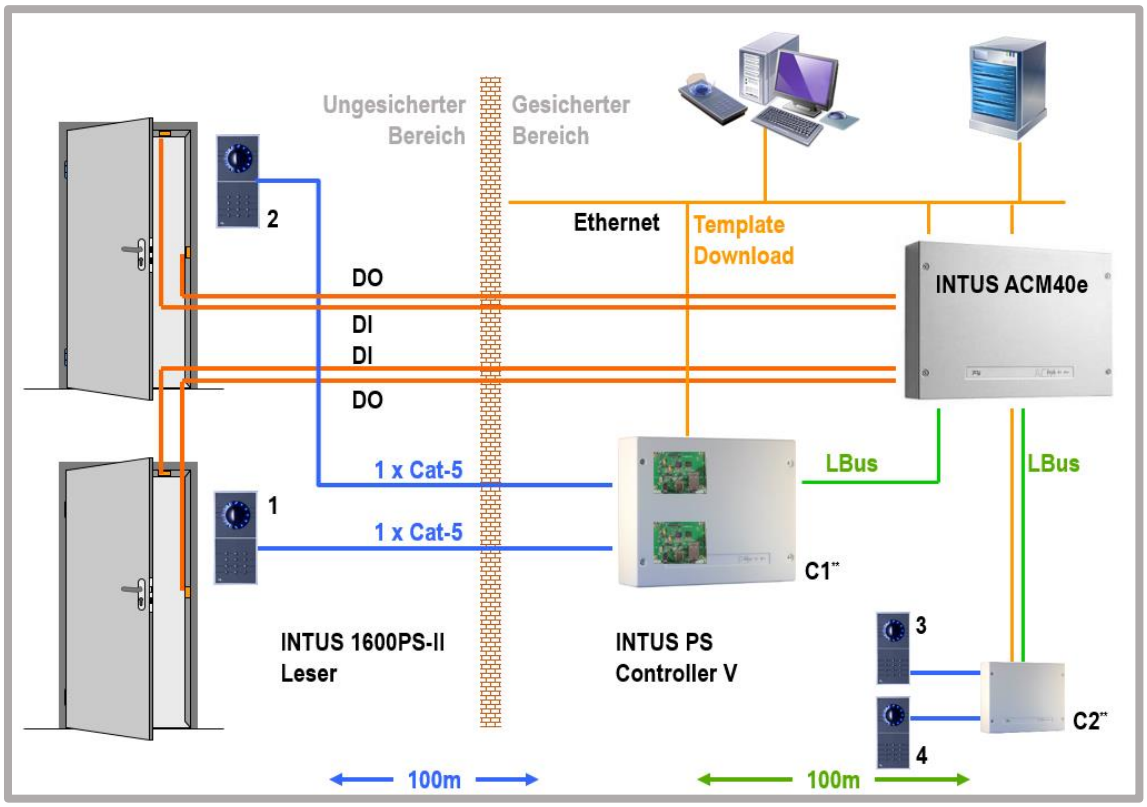


Abbildung 5: Konfiguration Handvenenerkennung für vier Türen mit Cat-5-Anschluss

5 Systemsicherheit

5.1 INTUS PS Leser

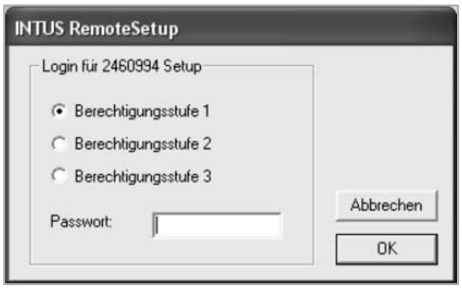
Der INTUS PS Handvenenleser kann im ungesicherten Bereich installiert werden, da die Sensoreinheit keine sicherheitskritische Komponente darstellt. Ein gewaltsames Aufbrechen des Gehäuses ermöglicht weder den Zugriff auf biometrische Daten, noch auf die elektrischen Elemente (wie Relais-Ansteuerung), die zum Öffnen einer Tür führen könnten. Alle sicherheitsrelevanten Entscheidungen werden auf Controller-Eben getroffen.

5.2 INTUS PS Controller

Im INTUS PS Controller werden die Templates verglichen und abhängig vom Betriebsmodus auch gespeichert. Es ist deshalb erforderlich, dass der INTUS PS Controller im gesicherten Bereich installiert wird. Das gilt insbesondere auch für Kleininstallationen, bei denen auf Zutrittskontrollmanager verzichtet wird. Der INTUS PS Controller ist mit einem Linux Betriebssystem ausgestattet. Der Anschluss des Controllers an einen Zutrittskontrollmanager erfolgt verschlüsselt per RS485 über die LBus bzw. OSDP Schnittstelle oder alternativ über Wiegand.

5.3 INTUS ACM

In größeren Installationen steuert der INTUS ACM die Zutrittsfreigabe des INTUS PS Handvenenerkennungssystems. Alle Zutrittskontrollmanager von PCS sind mit einem dreistufigen Sicherheitspaket ausgestattet, bestehend aus mehrstufigem Passwortsystem, integrierter Firewall und Verschlüsselung. Das dreistufige hierarchische Passwortsystem sorgt dafür, dass bestimmte Einstellungen nur von den jeweils autorisierten Personen vorgenommen werden können.



In der Berechtigungsstufe 1 kann der Haustechniker das Kommunikationsprotokoll konfigurieren und die IP-Adresse bei Ethernet-Anschluss bzw. die Betriebsparameter bei seriellem Leitsystem-Anschluss einstellen. Der Ethernet-Anschluss wird immer für die Wartung verwendet.

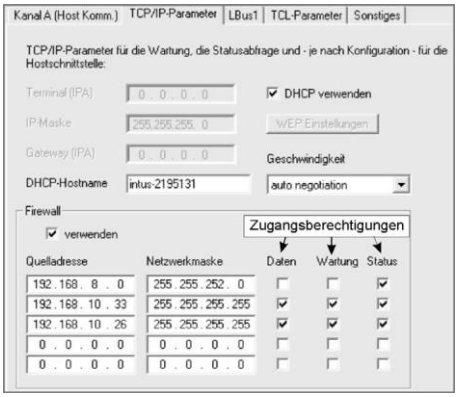
In der Berechtigungsstufe 2 werden Betriebsparameter vom Betreuer/Partner eingestellt oder verändert wie Host-Kommunikation (Verbindung zum Leitsystem, Ethernet oder serielle Schnittstelle), TCP/IP-Parameter (IP-Adresse und IP-Maske), Firewall-Einstellungen, oder Betriebsparameter für den TCL-Interpreter, Verschlüsselung der Hostschnittstelle und Passwörter der Hostschnittstelle.

Die Berechtigungsstufe 3 des Setup-Modus ist bei der Einstellung der Betriebsparameter mit der Ebene 2 identisch. Zusätzlich kann der Systemverwalter die Kommunikation im INTUS LBus zwischen dem INTUS ACM und einem geeigneten Leser verschlüsseln, den Zugang zur Hostschnittstelle verschlüsseln, die Setup Einstellung in einer Datei auf dem PC speichern und auf die voreingestellten Parameter zurücksetzen.

Mit Hilfe einer integrierten Firewall können für den INTUS ACM Operationen freigeschaltet werden, wie Daten und Programme ändern, Wartung und Anzeige des Status für Netzwerkteilnehmer.

Die Quelladresse in Verbindung mit der Netzwerkmaske legt fest, wie viele und welche Netzwerkteilnehmer Zugangsberechtigungen für die jeweiligen Dienste erhalten. Die Anzahl der Netzwerkteilnehmer wird dabei von der Netzwerkmaske vorgegeben.

Die Firewall muss so konfiguriert werden, dass das INTUS ACM Setup auf das Netzwerk zugreifen darf.



5.4 Verschlüsselung

Sowohl die Daten der Rechnerschnittstelle als auch die der Leserschnittstellen vom INTUS ACM können verschlüsselt werden. Für die Verschlüsselung der Kommunikation sowohl zwischen INTUS PS-Leser und INTUS ACM, als auch zwischen INTUS ACM und Host, kann eine Passphrase (Verschlüsselungstext) mit max. 512 Zeichen eingegeben werden.

Für den PalmSecure-Sensor ist optional ein „Application Key“ erhältlich, mit der eine kundenspezifische Verschlüsselung möglich ist. Beim Einsatz der Standard-PCS-Verschlüsselung (über den PCS-SDK) werden die Templates alle gleich verschlüsselt. Theoretisch wäre es damit möglich, ein PalmSecure-Template vom Leitsystem der Firma A zu entwenden und heimlich auf das Leitsystem der Firma B einzuschleusen. Voraussetzung dafür ist, dass in beiden Firmen die Leitsysteme so schlecht abgesichert sind, dass fremde Personen die Systeme hacken und darauf zugreifen können.

Wir empfehlen bei Hochsicherheitsanwendungen einen eigenen Application Key zu erwerben und die Templates mit diesem firmeneigenen Application Key zu verschlüsseln. Damit ist sichergestellt, dass selbst beim Hacken eines Leitsystems PalmSecure-Templates einer anderen Firma nicht für den Zutritt verwendet werden können.

Der PalmSecure Sensor ist vom BSI zertifiziert für Common Criteria Level 2 (https://www.bsi.bund.de/cae/servlet/contentblob/480424/publicationFile/29460/0511a_pdf.pdf).

6 Anwendungsbeispiele für Handvenenerkennung

Da die Handvenenerkennung sowohl hochsicher als auch bequem in der Anwendung ist, erstrecken sich die Anwendungsfälle über ein breites Spektrum. Dabei kommt im Hochsicherheitsbereich üblicherweise die Verifikation zum Einsatz, während die Identifikation das bevorzugte Verfahren für Komfortanwendungen ist.

Abbildung 6: INTUS PS im Rechenzentrum

INTUS PS wird heute in hunderten Projekten und zahlreichen Szenarien eingesetzt:

- Zutritt zu hochsicheren Firmenbereichen wie
  Rechenzentrum, Tresorraum, Vorstands-Etage, Entwicklungsabteilung,
  Intensivstation, Lager
- Zutritt mit eindeutiger Personen-Identifikation
  wie Spielkasino, Flughafen, Grenzverkehr, Freizeitpark
- Integration in andere Geräte
  wie Geldautomat, Getränkeautomat, Medizintechnik, Schließfachanlage
- Zutritt (zum Gebäude) kombiniert mit Zugang (zum Rechnersystem – Login)

Weiterführende Informationen finden Sie unter

- www.pcs.com/ps