ZUTRITTSKONTROLLSYSTEME VON conus

Zutrittskontrolle

+

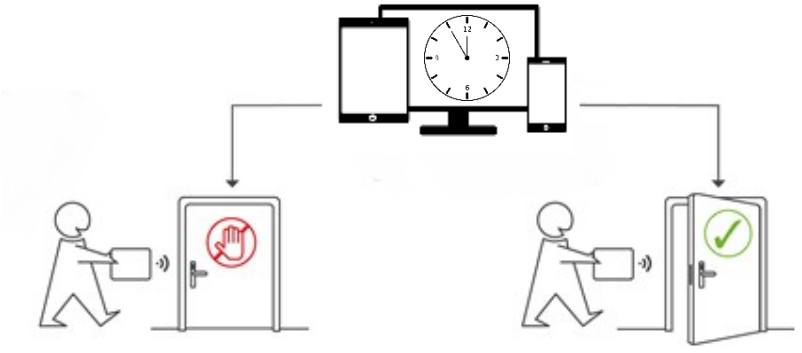
Schließsystem

=

Zutrittskontrollsystem

+

=




Elevator Control
Easy System Connectivity
& Easy Maintenance
Access Control and Time &
Attendance Management
Outstanding Performance &
Contactless Authentication

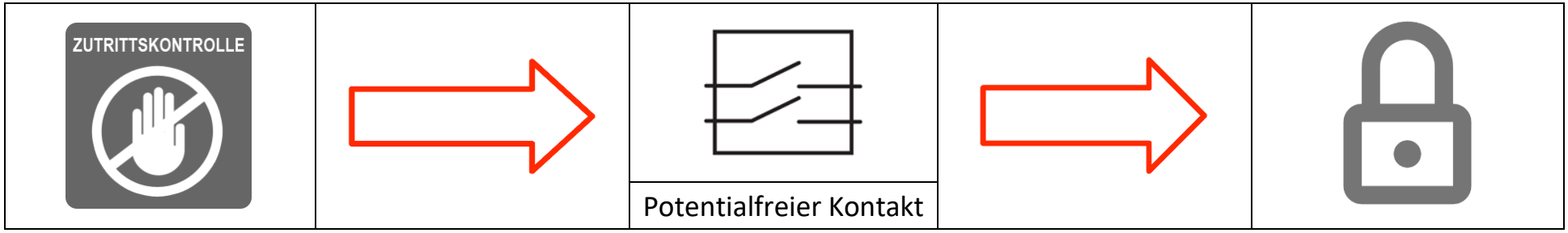
Zutrittskontrolle vs. Schließsystem – eine Begriffserklärung

Zutrittskontrollsysteme *steuern konfigurierbar über ein vom Betreiber definiertes Regelwerk den Zugang zu Bereichen, Gebäuden und Arealen, und sind eine Kombination aus der Zutrittskontrolle und dem Schließsystem.*

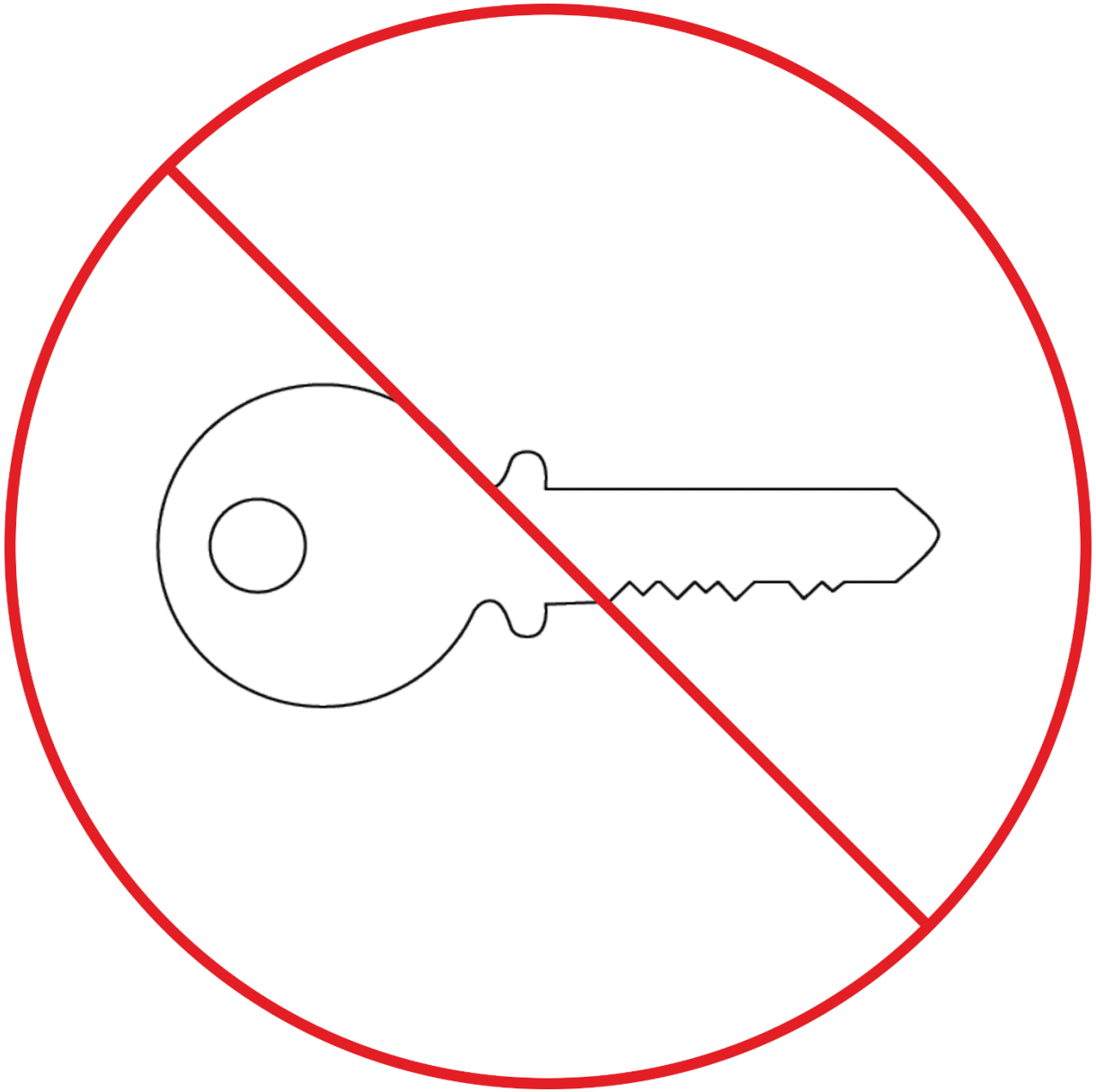
Die Zutrittskontrolle steuert das Schließsystem. Allgemein wird dafür der „potentialfreie Kontakt" genutzt. Dies bedeutet, das Zutrittskontrollsystem schließt bei gewährtem Zugang elektronisch einen Kontakt, wobei die Schließanlage darauf reagiert, und zum Beispiel eine Türe öffnet. Der „potentialfreie Kontakt" kann mit einem Türöffnertaster verglichen werden, mit welchem man eine Türe, ein Tor, einen Schranken öffnen kann, und dies gänzlich **ohne** Einsatz eines Zutrittskontrollsystems.

Ein Schließsystem ist eine aus mehreren Türschließern bestehende Anlage, die in funktionalem Bezug zueinander stehen. Türschließer können mechanisch für die manuelle Bedienung (zum Beispiel bestehend aus Schloss – Schlüssel) oder elektromechanisch (zum Beispiel mit automatischer Verriegelung und/oder Entriegelung) ausgeführt werden.

Die Zutrittskontrolle und das Schließsystem haben grundsätzlich **nichts** miteinander zu tun und sind als vollkommen getrennte Themen zu betrachten.



Als Folge kann jede Zutrittskontrolle mit jedem elektromechanischem Schließsystem kombiniert oder ergänzt werden. Dies hat nicht zuletzt deshalb große Bedeutung, da an jede Türe, Tor, Schranken (etc.) verschiedene Anforderungen hinsichtlich Sicherheit und Einbaumöglichkeit gestellt werden. Dies schlägt sich ebenfalls in finanzieller Hinsicht nieder.

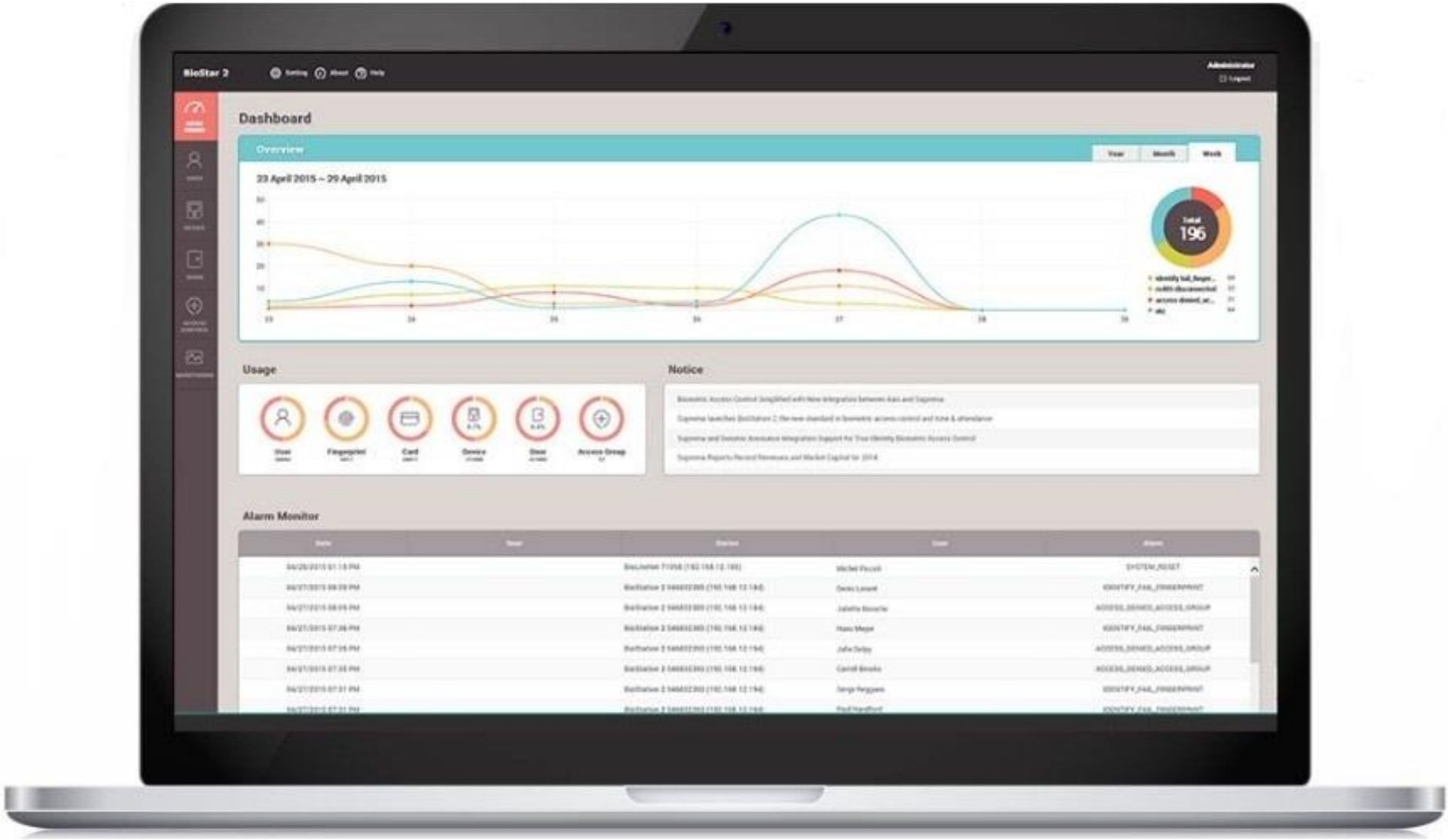


Die Zutrittskontrolle ist eine aus Software und Hardware bestehende Kombination, mittels welcher über eine zentrale Oberfläche oder ein zentrales Bauteil Benutzer und Zutrittsrechte konfiguriert und gesteuert werden.

Zutrittskontrollsysteme unterscheiden sich untereinander durch eine Vielzahl von Faktoren. Diese betreffen die Bedienbarkeit, die Administrierbarkeit, die Möglichkeiten der Identifikation der Benutzer, die Möglichkeiten der Erweiterung, die Integrierbarkeit in andere Systeme, die notwendigen Vorarbeiten (zum Beispiel Verkabelung), die Art der Datenübertragung, die Sicherheit und Verschlüsselung der Daten und deren Übertragung und nicht zuletzt durch die Anschaffungskosten.

Übersicht	
Zutrittskontrolle	Betrieb auf einem eigenen Server
	Betrieb im eigenen Netzwerk (on premise) bzw. Intranet
	Betrieb im Internet (Cloud)
	Betrieb in einer elektronischen Blackbox (Steuerungseinheit)
Bedienung und Administration	Administration durch ein eigenes zu installierendes Programm (Client)
	Administration durch eine standardisierte html- bzw. Weboberfläche
	Administration über ein eigenes Bauteil durch z.B. eine Menüoberfläche

Eine Zutrittskontrolle besteht aus Terminals und der Software, welche die Zutrittsmedien und die Benutzer sowie damit verbunden – Rechte wie Zutrittszeiten, Türen und Zutrittsbereiche, normal oder hochgesichert, konfiguriert, verwaltet und protokolliert. Die Zutrittsmedien können physische Medien, Codes oder biometrische Erkennungsmerkmale sein. Diese Mittel dienen der Zutrittsidentifikation und nennen sich „credentials“.


BioStar 2
Administrator
Dashboard
Overview
Year
Month
Week
23 April 2015 ~ 29 April 2015
Total
196
Usage
Notice
Alarm Monitor

*Im Allgemeinen unterteilen sich **Credentials** (= Identifikationsmedien) in drei wesentliche Gruppen: physische Zutrittsmedien, den biometrischen Zutritts und mobile Zutrittsmedien. In Bereichen höherer Sicherheitsanforderung werden auch Kombinationen dieser Gruppen eingesetzt. Bei der **Two-Factor-Authentification** ist zumindest eine positiv erkannte Kombination aus zwei Komponenten -zum Beispiel- Transponder & Fingerabdruck oder mobile-credential & FaceScan, erforderlich.*

Physische Zutrittsmedien

Physische Medien basieren vor Allem auf **RFID** Anwendungen. Die Technologie RFID ist sehr weit verbreitet, steht für **R**adio **F**requenzy **Id**entification, und wird unter anderem für Zutrittsidentifikation genutzt. Weitere Anwendungen sind Zeiterfassung, Warenerkennung, Diebstahlserkennung, Prozessautomatisation, Fahrzeugidentifikation, Zahlungsablauf und viele mehr.

Ein, auf einem **Medium (= „Transponder“ oder „TAG“)** gespeicherter Code wird auf Basis eines eingehenden Signals (=Anfrage) drahtlos, also über Funk (=radio) auf einen Leser übertragen. Die Anfrage wird durch den Leser gesendet. Dieser Code wird mit dem bestehenden Eintrag in einer Datenbank verglichen, wonach die Aktion ausgelöst wird. Im Falle der Anwendung der Zutrittskontrolle wird ein physisches Medium und somit ein darauf gespeicherter Code einem Benutzer zugeordnet.

Im Bereich der Zutrittskontrolle werden vorwiegend „**passive Transponder**“ eingesetzt. Die zur Kommunikation benötigte Energie wird ausschließlich aus dem Feld der Sende-/Empfangseinheit bezogen. Passive Transponder benötigen somit **keine eigene Stromversorgung**, können aber nur auf kurze Distanzen arbeiten.

Die **Sicherheit** dieser Identifikationsweise wird bestimmt durch die Übertragungsfrequenz (= die Wellenlänge des Funksignals innerhalb einer Sekunde), die Art und die Technologie des zu übertragenden Codes, sowie einer möglichen zusätzlichen Übertragungsverschlüsselung. Somit bestimmt die Sensibilität der Anwendung die Wahl der möglichen Technologie. Diese Parameter sind in Normen definiert.

Sollte ein Transponder verloren werden, wird dieser einfach im System gesperrt, und mit dem Benutzer wird ein neuer Transponder verknüpft. Abgesehen von der Sicherheit der Gesamtanlage, senkt dies die Kosten vor Allem in großen Schließanlagen bzw. Zutrittskontrollsystemen erheblich, da keine Schlüssel mehr ausgegeben werden.

Frequenz	Erlaubte Frequenzen (ISM-Band)	Typische Anwendungen	Typische Reichweite für TAGs
Langwellen-Frequenzen (LF)	9…135 kHz	Tier-Identifizierung, Geldkarten,	0,5 m (passiv)
Kurzwellen-Frequenzen (HF)	6,78 MHz, 13,56 MHz, 27,125 MHz, 40,680 MHz	Zugangskontrolle, Personenidentifikation	0,5 m (passiv)
Dezimeterwellen (UHF)	433,920 MHz, 868 MHz, 915 MHz, 2,45 GHz	Lager und Logistikbereich (Paletten)	5 m (passiv)
Mikrowellen (SHF)	5,8 GHz, 24,125 GHz	Fahrzeug-Identifizierung	10m (aktiv)


NFC
02762
SYN
ACCESS CONTROL
SYS
conus
www.conus.at
6752449892

Biometrische Erkennungsmethoden haben in den letzten Jahren einen enormen Aufschwung erlebt. Der technologische Fortschritt erlaubt in zunehmendem Maße die rasche Messung **biologischer Charakteristika** und deren Auswertung mit vertretbarem Aufwand und hoher Qualität. Wie verbindet man Identitäten und die dazugehörigen Rechte mit den die richtige Identität aufweisenden physischen Personen?

Im Bereich Zutrittskontrolle werden **biometrische Merkmale des Benutzers** durch einen Leser gelesen und in einer Datenbank gespeichert. Möchte sich der Benutzer nun Zutritt verschaffen, wird -zum Beispiel- der **Fingerabdruck** mit dem bestehenden Eintrag in der Datenbank verglichen, wonach die **Aktion** ausgelöst wird. Die Aktionen können je nach Konfiguration und Anwendung vielfältig sein. Das Ziel sollte die **Zutrittsgewährung** sein, doch auch ein Alarm oder eine fotographische Aufnahme können im Falle eines potentiellen Missbrauchs ausgelöst werden. Bei vielen Verfahren werden nur die **wichtigsten Charakteristika** der biometrischen Aufnahme gespeichert. So sind im **Rückverfahren** das ursprüngliche Bild bzw. Profil **nicht reproduzierbar**! Weiters verfügen moderne Leser über vielfältige Technologien, welche die **Sicherheit** im Missbrauchsfall gewährleisten. So werden -zum Beispiel- durch Mikrowellen, elektromagnetische Felder oder Infrarotstrahlungen erfasst, ob die biometrische Komponente lebt.

Beim Einsatz der **Biometrie** zur automatisierten **Personenerkennung** kommt es darauf an, individuelle biometrische **Verhaltens- oder Körpercharakteristika** zu finden, die sich -zum Beispiel- durch folgende Eigenschaften auszeichnen:

Einmaligkeit	Der Messwert des Charakteristikums ist für möglichst alle Personen unterschiedlich
Konstanz	Der Messwert hängt nicht vom Alter der Person oder dem Messzeitpunkt ab
Messbarkeit	Es sollte eine gut definierbare Messgröße existieren, für die es geeignete Sensoren gibt
Universalität	Das Charakteristikum kommt bei möglichst vielen Personen vor

Als biometrische Charakteristika können eine Vielzahl von Komponenten verwendet werden, wie -zum Beispiel- DNA, Handgeometrie, Stimmerkennung, Ohrform, Nagelbettmuster und viele mehr, im Bereich der Zutrittskontrolle werden hauptsächlich Fingerabdruck, Gesichtserkennung, Iris-Erkennung, Handvenenstruktur oder die Handlinienstruktur eingesetzt.


09:15 AM
04
03/24 FRI
20170519 Irina Kalentyeva
suprema


suprema
SECURITY & BIOMETRICS


suprema
PM
05:28
07/29
MON
F1
F2
ESC
OK

*Ein **Schließsystem** wird ganz allgemein eingesetzt, um dem **Zutritt** oder Zugang für Personen zu unterbinden, oder zu gewähren. Dies können - zum Beispiel - Türen oder Kästen, aber auch Schleusen, Vereinzelungs- oder Schrankenanlagen sein.*

Konventionelle Schließsysteme bestehen aus **Schlössern** und **Schlüsseln**, stellen im Verlustfall von Schlüsseln ein erhebliches **Sicherheitsrisiko** dar, welches je nach Größe der Anlage nur mit hohem **Kostenaufwand** behoben werden kann, und ist außerdem aufwändig zu verwalten.

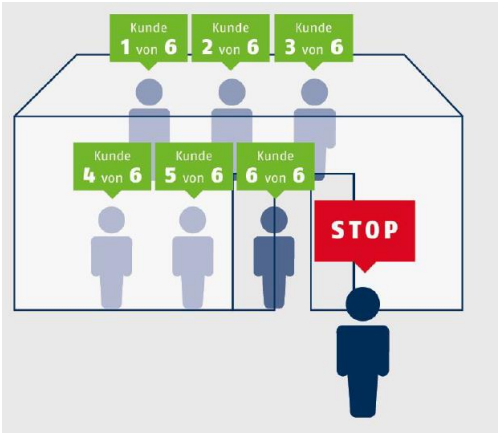
Elektromechanische Schließsysteme werden in Zutrittskontrollen eingebunden. Sie verfügen über elektr(on)ische und mechanische Bauteile, wobei der elektr(on)ische Bauteil eine Aktion des mechanischen Bauteils auslöst oder antreibt. Sofern diese auch über Schlüssel verfügen, werden diese nicht ausgegeben, sondern nur für den Notfall eingesetzt. Diese können voll- oder halbautomatisch agieren, und unterscheiden sich weiters durch verschiedene Eigenschaften, wie -zum Beispiel- Verriegelungseigenschaften. Die elektromechanischen Schließsysteme werden durch die Zutrittskontrolle angesteuert.

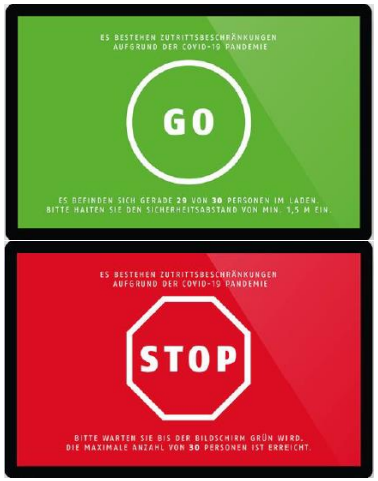
Konventionelle Schließsysteme	Einbauschlösser			
	Riegel			
	Mechanische Codeschlösser			
Elektromechanische Schließsysteme	Motorschlösser mit Verriegelung			
	Türöffner ohne Verriegelung			
	Magnetschlösser			
	Schiebetüren			
	Aufzugsanlagen			
	Bolzenschlösser			

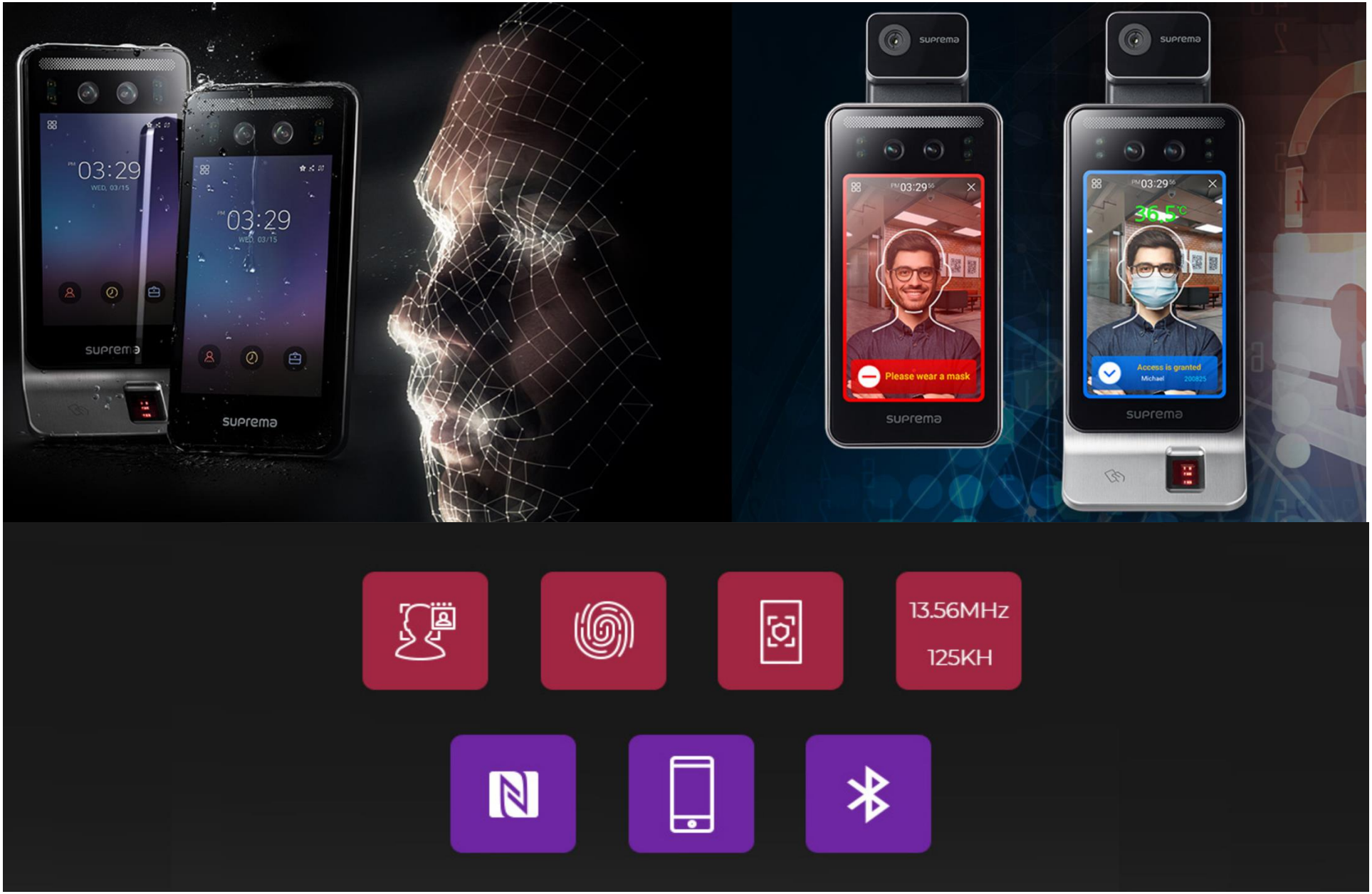
Als Zusatz lassen sich Zutrittskontrollsysteme mit anderen Gegebenheiten und Variablen aus der Umgebung verknüpfen. Dies bedeutet, dass Zutritt unter Beachtung weiterer Bedingungen gewährt oder verhindert wird.

Fever Screening steuert den Zutritt auf Basis der Temperatur der Benutzer. Dabei wird zusätzlich Fieber oder erhöhte Temperatur genmessen, bzw. das Tragen von Masken erkannt. Dies stellt eine *zusätzliche* Bedingung dar, um Zutritt zu erhalten, wodurch. Risiko, eine Krankheit zu übertragen, massiv reduziert wird. Diese Komponenten sind in vernetzte Zutrittssysteme integrierbar, können aber auch als *alleinstehende Systeme* ausgeführt werden.

People Counting stellt die Möglichkeit zur Verfügung, Zutritt auf Basis der Anzahl bereits anwesender Personen zu erlauben, oder zu verhindern. Es werden ein- und ausgehende Personen erfasst, wobei ab einer definierten Zahl gleichzeitig anwesender Personen der Zutritt verhindert wird. Dies findet Anwendung in sensiblen oder speziell geschützten Bereichen (z.B. gefährlichen Laborumgebungen, Umgebungen mit Wertgegenständen etc), in Bereichen, wo Krankheitsübertragungen eingeschränkt werden müssen, oder um Vorschriften zu erfüllen.



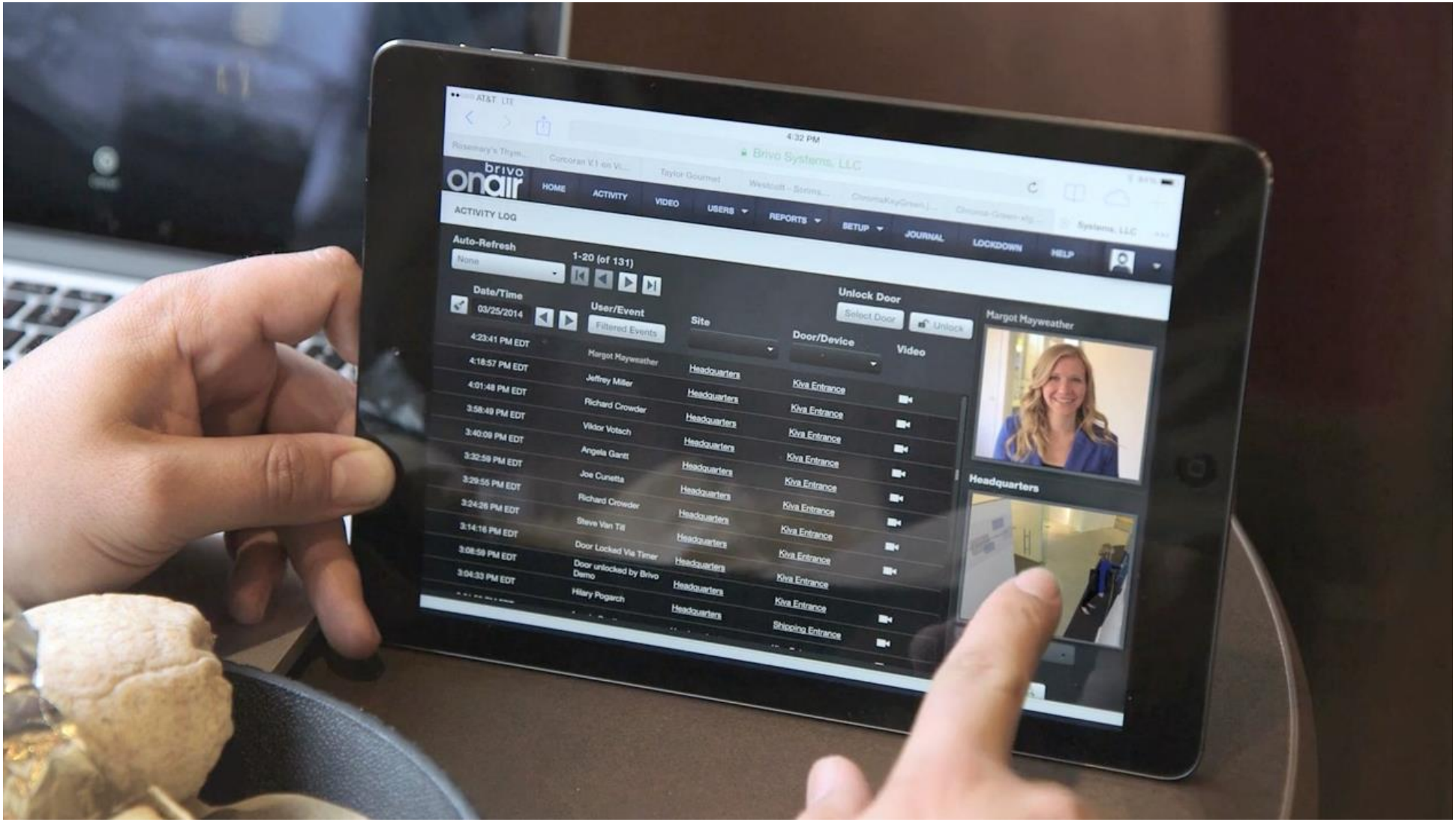



03:29
WED, 03/15
suprema
Please wear a mask
36.5℃
Access is granted
Michael
13.56MHz
125KH

Unsere Technologiepartner

www.supremainc.at [powered by CONUS GmbH.]

Unsere Technologiepartner



***Wir** installieren **national** und **international** seit Jahrzehnten Zutrittskontrollsysteme aller Dimensionen. Durch unsere direkten Partnerschaften mit Herstellern lassen sich auch neben den Standardfunktionen nahezu alle **Vorstellungen** im Software- und Hardwarebereich umsetzen.*

Wir konzipieren, installieren und betreuen sehr gerne **Ihr** Zutrittskontrollsystem

conus

CONUS GmbH.

Kirchstetterngasse 47

A – 1160 Wien

M: info@conus.at

W: www.conus.at

T: +43 1 617 51 44

Hier ist Platz für Ihre Notizen