MICROSESAME CUBE

FUNKTIONSBESCHREIBUNG

Version 2025.1 – März 2025

TIL TECHNOLOGIES by HIRSCH

1. INHALTSVERZEICHNIS

2. MICROSESAME IN WENIGEN WORTEN

MICROSESAME CUBE

MICROSESAME ist ein integriertes System für das zentrale Sicherheitsmanagement (Zutrittskontrolle, Einbruchmeldetechnik, Videoüberwachung) sowie für das technische Gebäudemanagement.
Es ermöglicht die einheitliche Überwachung aller elektronischen Informationen des Gebäudes.
Die Steuerung der verschiedenen Funktionen über eine gemeinsame grafische Benutzeroberfläche macht die Bedienung deutlich einfacher und Eingriffe effizienter.
Da die Interaktionen zwischen den verschiedenen Systemen vollständig automatisiert werden können (Ereignisgesteuerte Aktionen), ist auch eine schnelle Verarbeitung gewährleistet.
Das System besteht aus einer Softwarekomponente und IP-basierten Automatisierungseinheiten, an die alle Arten von Endgeräten angeschlossen werden können.

MS ENTRY

MS PRIME

MS HIGH SECURE

Diese Architektur basiert auf Standards, die sowohl ihre Zukunftssicherheit als auch ihre Weiterentwicklungsfähigkeit bei minimalen Kosten gewährleisten.

Durch die Integration von SDKs oder IT-Protokollen (z. B. MODBUS) kann MICROSESAME Informationen aus externen Systemen (wie etwa Brandmeldesystemen) überwachen und als übergeordnetes System (Hypervisor) für digitale VMS-Videosysteme fungieren.
Es kommuniziert zudem direkt mit speicherprogrammierbaren Steuerungen (SPS) und anderen Sicherheits- bzw. Sicherheitssystemen über Gateways (z. B. OPC, Textschnittstellen).

Über die funktionale Beschreibung von MICROSESAME CUBE hinaus zeigen wir am Ende dieses Dokuments das Software-/Hardware-Angebot CUBE in drei Ausprägungen (ENTRY, PRIME, HIGH SECURE), basierend auf dem Konzept der „Beherrschung von Vertraulichkeit“. Diese CUBE-Baureihe ist:

- Einfacher & umfassender: Gesamter Funktionsumfang der TIL-Software bereits ab der Basisversion und dem ersten Leser. Es gibt nur einen Automatisierungscontroller – in voller Kapazität und mit allen Optionen.
- Sicherer: Native Cybersicherheit mit umfassendem Schutz des Systems, konform mit den ANSSI-Vorgaben.
- Flexibler: Die Sicherheitsstufe kann durch einfaches Software-Update erhöht werden , ohne Hardware-Austausch

3. ZERTIFIZIERTE ARCHITEKTUR

CYBERSICHERE HARD- UND SOFTWARE-ARCHITEKTUR

Eine MICROSESAME-Architektur besteht aus folgenden Komponenten:

► Einem Server, der sowohl zur Parametrierung als auch zum Betrieb dient und unter einer Standard-Windows-Umgebung läuft. Die Inbetriebnahme ist einfach und benutzerfreundlich.

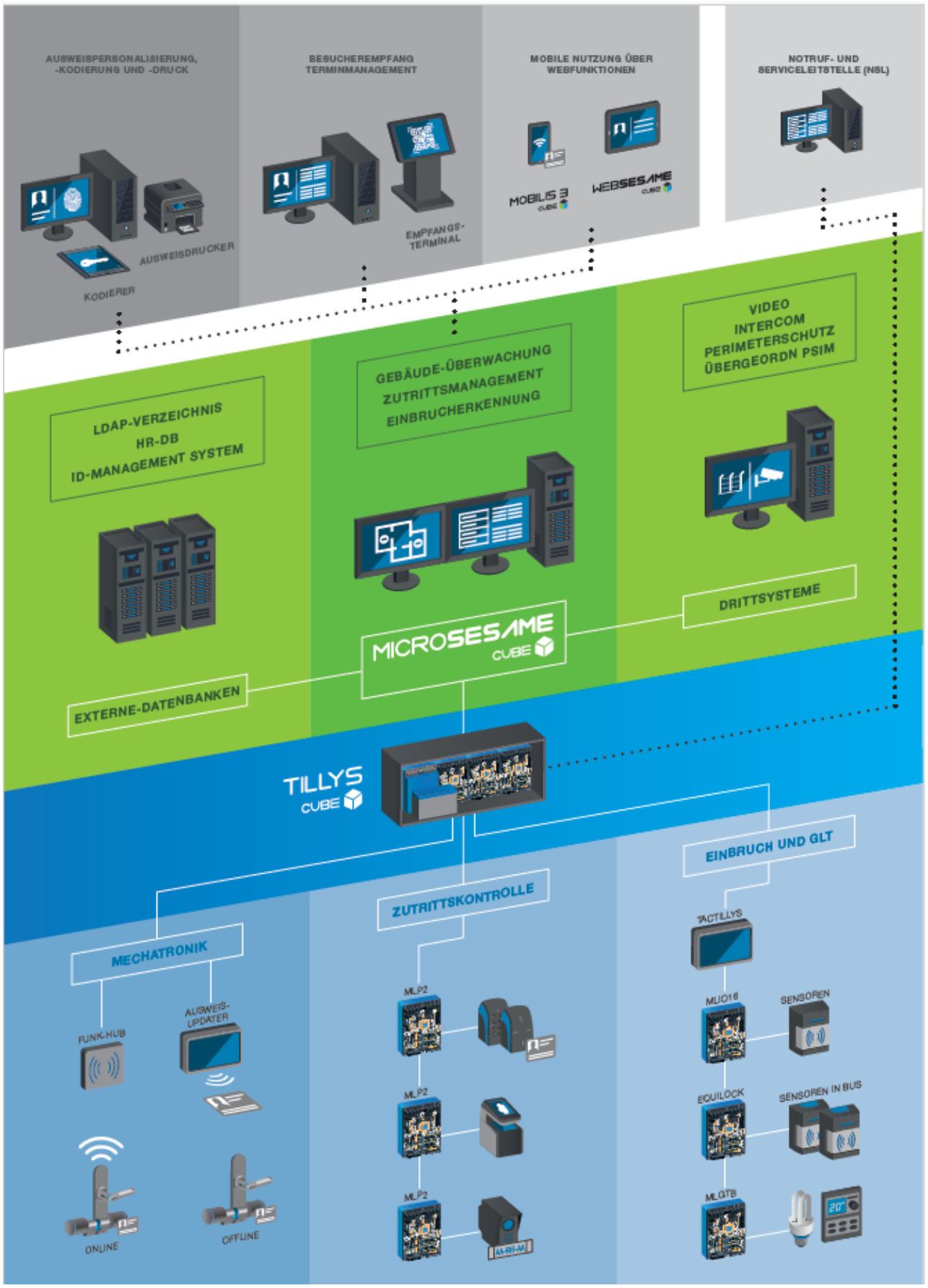
► Einem IP-Ethernet-Netzwerk (verkabelt oder WLAN), über das der Server mit Bedienstationen verbunden ist: lokalen MICROSESAME- und VISIOSESAME-Clients (Fat Clients), Thin Clients via RDP/TSE/Citrix, WEBSESAME-Webclients auf PC, Smartphone oder Tablet, mit TIL-Automaten (LVE) sowie mit mobilen Geräten (z. B. MOBILIS-Leser über WLAN).

► Das Ethernet-Netzwerk ermöglicht außerdem die Anbindung der MICROSESAME-Lösung an Systeme des Endkunden (z. B. Active Directory, IT-Supervisor via SNMP, HR-Datenbanken …) sowie an Drittanwendungen (z. B. VMS-Server und Videorekorder, OPC-Hypervisor, Automatisierungssysteme via MODBUS …).

► Autonomen und multifunktionalen TIL-Automaten (LVE) im IP-Netzwerk, die die Steuerung von Zutrittskontrolle, Einbruchmeldung und technischem Gebäudemanagement übernehmen.

► Einbruchmeldebedienteile, onlinefähige mechatronische Lösungen, spezialisierte dezentrale Elektronikmodule (z. B. Türmodule, Ein-/Ausgangsmodule), die über sekundäre Busleitungen mit den Automaten verbunden sind – für eine wahlweise verteilte oder zentrale Architektur.

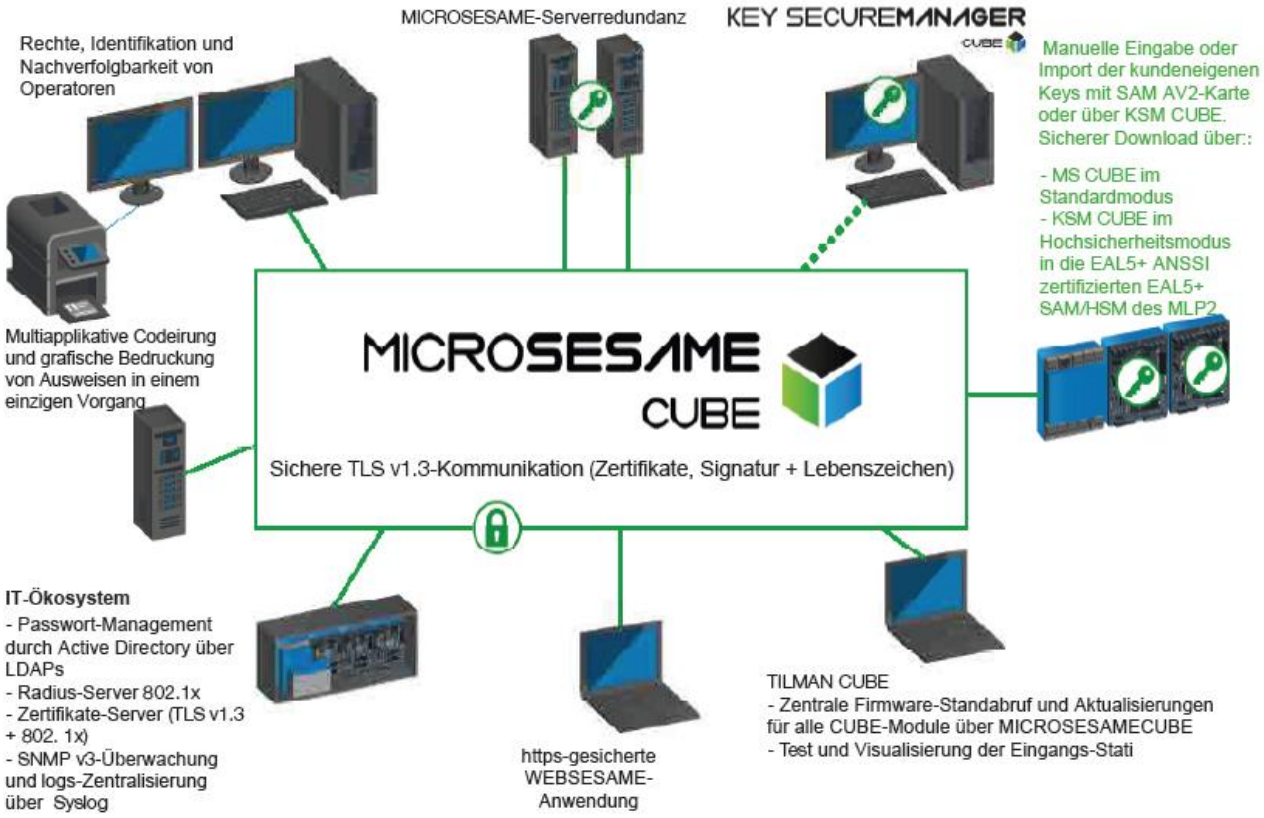
► Leser, Zutrittskontrolltastaturen, Sensoren (z. B. Kontakte, Einbruchmelder), gesteuerte Zugänge (z. B. Schlösser, Schranken, Drehkreuze) und Aktoren (z. B. Sirenen, Beleuchtung …), die mit diesen spezialisierten Modulen verbunden sind.


AUSWEISPERSONALISIERUNG, -KODIERUNG UND -DRUCK
BESUCHEREMPFANG TERMINMANAGEMENT
MOBILE NUTZUNG ÜBER WEBFUNKTIONEN
NOTRUF- UND SERVICELEITSTELLE (NSL)
AUSWEISDRUCKER
KODIERER
EMPFANGS-TERMINAL
MOBILIS 3
WEBSESAME
LDAP-VERZEICHNIS
HR-DB
ID-MANAGEMENT SYSTEM
GEBÄUDE-ÜBERWACHUNG
ZUTRITTSMANAGEMENT
EINBRUCHERKENNUNG
VIDEO
INTERCOM
PERIMETERSCHUTZ
ÜBERGEORDN PSIM
MICROSESAME CUBE
EXTERNE-DATENBANKEN
DRITTSYSTEME
TILLYS CUBE
MECHATRONIK
FUNK-HUB
AUSWEIS-UPDATER
ONLINE
OFFLINE
ZUTRITTSKONTROLLE
MLP2
MLP2
MLP2
EINBRUCH UND GLT
TACTILLYS
MUO16
SENSOREN
ECUILOCK
SENSOREN IN BUS
MLGTB

CSPN-ZERTIFIZIERTE CYBERSICHERE GESAMTLÖSUNG

Es reicht heute nicht mehr aus, bloß Standorte zu schützen. Ebenso wichtig ist es, Mechanismen zu implementieren, die das Sicherheitssystem selbst vor internen und externen Bedrohungen absichern.
In der gesamten MICROSESAME-Architektur – vom Ausweis bis zum Server – kommen elektronische und IT-Schutzmaßnahmen zum Einsatz, um Manipulationen oder Hackerangriffe zu verhindern.

Um Ihnen höchste Sicherheits- und Cybersicherheitsstandards zu gewährleisten, ist die Lösung von der ANSSI nach der von ihr empfohlenen Architektur 1 („transparenter Leser“) zertifiziert.



MICROSESAME CUBE, die CUBE-Hardwarefamilie (TILLYS CUBE, externes Modul ML) sowie die „transparenten“ EVOLUTION-Leser bieten Ihnen insbesondere folgende Eigenschaften und Fähigkeiten im Bereich Cybersicherheit:

- Eine offizielle ANSSI-Zertifizierung – empfohlen für alle sicherheitskritischen Einrichtungen.
- Eine durchgängige, sichere Lösung – vom Ausweis bis zum Server.
- Sämtliche IP-Netzwerkkommunikation ist mittels TLS v1.3 und Zertifikaten abgesichert – sowohl zwischen dem Server und den UTLs als auch zwischen dem Server und den Client-Arbeitsplätzen.

CUBE WANDSCHRÄNKE :

- Verwaltung von Störungs- und Sabotageinformationen: Abreißen, Öffnen von Gehäusen, Kommunikations- und Stromversorgungsfehler (Netzausfall, schwache Batterie, Ladegerät).
- Schutz vor Fehlfunktionen und Sabotage durch überwachte Eingänge.
- Schutz vor Kurzschlüssen, Überspannungen und Verpolung an Ausgängen und RS485-Bussen.

TILLYS CUBE AUTOMATEN/LVE MIT:

- Integrierter HTTPS-Webserver zur lokalen Konfiguration.
- Kompatibilität mit 802.1X (Radius) und SNMPv3 zur Überwachung von Systemzuständen und sicherheitsrelevanten Alarmen durch die IT-Abteilung des Endkunden.
- Modulare Architektur mit drei ANSSI-zertifizierten RS485-Feldbussen, gesichert mit AES 128 Bit, an die dezentrale Zutritts- und Einbruchstechnik angeschlossen wird. Dies ermöglicht:
  - Kostensenkung durch optimale Nutzung vorhandener Verkabelung
  - Flexible Wahl zwischen verteilter oder zentralisierter Architektur
- Schutz vor Denial-of-Service-Angriffen (DoS) durch integrierte Firewall.

MLP-TÜRMODULE MIT:

- AES-128-bit-gesicherte RS485-Kommunikation mit transparenten Lesern.
- Nativ integrierte HSM-Komponente (Hardware Security Module), ANSSI EAL5+-zertifiziert – fungiert als Kryptoprozessor und sicheres Schlüsseldepot für die Anwendung „Zutrittskontrolle“ auf den Ausweisen.
- Applets (Konfigurationsmodule), um sich an das Ausweiskonzept des Kunden anzupassen und LEDs sowie Summer der transparenten Leser zu steuern.
- Gesicherte Operatorrechte schützen den Zugriff auf die Konfiguration der Applets MLP / MLD

RFID-LESER:

- Tastaturleser, ANSSI-zertifiziert gemäß Architektur 1 („transparente Leser“), bei denen keine Ausweisschlüssel im Leser gespeichert werden – ideal zur Verwaltung von DESFIRE-Hochsicherheitsausweisen.
- Transparente biometrische EVOLUTION-Leser, die über die Protokolle SCCPv1 und SCCPv2 gesteuert werden – ANSSI-zertifiziert – und über die MLP-Module verwaltet werden. Diese erkennen neue Zustände wie „Ausweis OK, aber Fingerabdruck fehlt“, „Zeitüberschreitung“ sowie „Fingerabdruck unter Zwang“.

SCHLÜSSEL AUSSCHLIESSLICH DEM ENDKUNDEN BEKANNT:

- Für alle Ausweisanwendungen (Zutritt, Kantine usw.), die über eine dedizierte Benutzeroberfläche – KSM – erfasst oder generiert werden (Schlüsselgenerierung), erfolgt die Verwaltung zentral. Diese Schlüssel werden in einem sicheren digitalen Container mit AES-256-Bit-Verschlüsselung gespeichert, der in MICROSESAME eingebettet ist.
  Alle Schlüssel bleiben für Dritte, die das System konzipieren, integrieren oder warten, vollständig unsichtbar. Für den Integrator und den Endkunden ist nur **ein einziger Schlüsselgenerierungsvorgang** erforderlich.

SCHLÜSSEL & APPLETS :

- Der Download von Schlüsseln und Applets erfolgt gesichert und zentralisiert – vom Server bzw. KSM bis zu den HSM-Modulen der MLPs. Dies erleichtert die Verteilung der Schlüssel und ermöglicht deren zentrale Aktualisierung in allen Modulen, wie von der ANSSI gefordert.

- Ein Schlüsseldiversifizierungsprinzip gemäß dem Standard AN10922 ermöglicht es dem Endkunden, unterschiedliche Schlüssel pro Ausweis zu verwenden und sein Sicherheitsniveau durch individuell anpassbares Padding selbst festzulegen.

CUBE-ARCHITEKTUR:

- **TILMAN CUBE**, das dedizierte Dienstprogramm von MICROSESAME, bietet eine zentrale Übersicht über den gesamten Bestand an CUBE-Automaten (UTL, Module). Es ermöglicht das Auslesen und Aktualisieren der Firmware-Versionen über globale Downloads. So lässt sich die Wartung – sowohl korrektiv als auch evolutiv – bequem von einer zentralen Stelle aus durchführen. Zusätzlich unterstützt das Tool bei der Inbetriebnahme durch Tests und Diagnosefunktionen für die Verkabelung der Detektoreingänge.

- **Die** für die Zutrittskontrolle zertifizierte Sicherheit der TILLYS CUBE ist auch im Modus Einbruchmeldeanlage aktiv – und macht daraus eine cybersichere Einbruchmeldezentrale.

- Die Firmware der Automaten der CUBE-Serie ist digital signiert, um ihre Integrität zuverlässig zu gewährleisten.

VERSTÄRKTE SICHERHEIT

- Stärkung der Sicherheit durch Entfernen des Reverse-DNS-Codes (Auswirkungen auf den Inhalt von Zertifikaten).
- Operator-Passwörter sind in der Datenbank geschützt – mit SHA-512-Hashing und einem 512 Zeichen langen zufälligen Salt.
- Das WEBSESAME-Portal **ist gegen** CSRF-Angriffe (Cross-Site Request Forgery) abgesichert.
- Ein **Web-Abfragewerkzeug** mit einer Bibliothek vordefinierter Abfragen für verdächtiges Verhalten (z. B. wiederholte Versuche, auf gesperrte Zonen zuzugreifen). Die Abfrageliste ist editierbar und ermöglicht automatisierte Berichte.

HOCH ANPASSUNGSFÄHIG AN VORHANDENE IT-UMGEBUNG

Je nach Größe Ihres Systems werden spezifische Hardware- und Softwareempfehlungen ausgesprochen. MICROSESAME passt sich kontinuierlich an neue Versionen von Betriebssystemen und Datenbanken an, um mit den neuesten IT-Umgebungen kompatibel zu bleiben.
Vor jeder Systeminstallation oder Migration können Sie auf regelmäßig aktualisierte Dokumente zurückgreifen, die über Ihren gewohnten TIL-Ansprechpartner erhältlich sind.

KOMPATIBEL MIT DEN AKTUELLEN BETRIEBSSYSTEMEN UND DATENBANKEN :

- Windows 10 oder 11 Pro bzw. Enterprise (64 Bit) für kleinere Systeme, bis hin zu Windows Server 2019 oder 2022 Standard bzw. Essential (64 Bit).
- Fat Clients: Windows 10 oder 11 Pro bzw. Enterprise (64 Bit).
- Datenbank: Microsoft SQL Server 2017 bis 2019 (64 Bit).

FÜR THINK-CLIENT-INFRASTRUKTUREN OPTIMIERT:

- Kompatibel mit RDS-Lösungen (ehemals Terminal Server – TSE)
- Keine MICROSESAME-Softwareinstallation auf den Arbeitsplätzen erforderlich.
- Zugriff von jedem beliebigen Rechner im Netzwerk möglich.
- Betrieb mit Floating-Lizenzen / gleichzeitige Verbindungen sind möglich.

Windows **RDS**

WEBSESAME-WEBPORTAL FÜR DEN ZUGRIFF ÜBER DAS KUNDENEIGENE INTRANET:

- **Responsives Design**: Bildschirminhalte passen sich automatisch an Auflösung und Ausrichtung auf Smartphones, Tablets und PCs an.
- **Optimierte Benutzerführung** für die mobile Nutzung: Auto-Vervollständigung von Feldern, Fotodarstellung, Checkboxen zur einfachen Bedienung).
- Verfügbare Funktionen für eine breite Nutzerbasis:
  - Verwaltung von Terminen, Besuchen und Besuchern
  - Verwaltung identifizierter Personen
  - Erstellen und Exportieren vordefinierter Berichte und Abfragen
  - Ereignishistorie zu Zutrittskontrolle und Technik
  - Übersicht aktueller Alarme
  - Live-Überwachung von Zutritts-, Technik- und Systemereignissen. Klick auf ein Ereignis zeigt die zugehörige Benutzerkarteikarte. Vereinfachter Ereignismonitor.
  - Anzeige der identifizierten Personen + Anzahl der Anwesenden in einer Zone
  - Hinzufügen und Einsehen von Tickets/Kommentaren aktiver, quittierbarer Alarme. Einfache oder filterbasierte Suche.
  - Berichte & grafische Auswertungen über erlaubte/verweigerte Zutritte an allen vom Operator überwachten Standorten
  - Diagnosehilfe zur Installation: Anzeige aller Zustände/Eigenschaften (z. B. Tür offen) eines überwachbaren Objekts, Filter- und Suchfunktionen, Fernsteuerung, Eigenschafts-Inhibierung für Wartungszwecke.

WEBSESAME CUBE

KOMPATIBEL MIT VIRTUELLEN UMGEBUNGEN WIE VMWARE:

- Server-Virtualisierung für Ressourcenteilung und Energieeinsparung.
- Softwarelizenz kompatibel mit virtuellen Umgebungen.
- Betrieb auf dedizierter physischer Maschine oder im Rechenzentrum möglich.
- Redundanz über virtuelle Umgebung (VM) mit HA-Modul (High Availability) realisierbar.

vmware

Microsoft Azure

OFFEN FÜR IHRE ARCHITEKTUR- UND NETZWAUSWAHL:

- Drittarchitektur möglich (Datenbank, Applikationsserver, Webserver getrennt).
- Kompatibel mit VPN, VLAN.
- E-Mail-/SMTP-Kommunikation integrierbar.
- TILLYS-CUBE LVE: kompatibel mit 802.1x, SNMPv3, IPv6-ready, Hostname-fähig.

HARDWARE- UND SYSTEMREDUNDANZ:

- Kompatibilität mit der Hot-Redundanzlösung SAFEKIT.
- orkonfigurierte Schnittstelle für MICROSESAME.

EVIDIAN
A Bull Group Company

INSTALLATIONS- , MIGRATIONS- UND WIEDERHERSTELLUNGSPAKET – INTEGRIERT UND EINFACH:

- Einfache Installation von MICROSESAME-Server und -Clients mit allen notwendigen Komponenten im Installationspaket enthalten.
- Tools zur Migration von Server und Clients verfügbar.
- Halbautomatische Aktualisierung der Fat Clients nach Server-Update.
- Alle „System“-Anwendungen laufen als Dienste.
- Automatische Datenbanksicherung gemäß vordefiniertem Pfad, inkl. Wiederherstellungstool.

BEDIENRECHTEVERWALTUNG ÜBER DAS KUNDENEIGENE ACTIVE DIRECTORY VIA LDAP

Siehe entsprechendes Kapitel.

SYSTEM-EVENTS PER SYSLOG-SCHNITTSTELLE

Die Syslog-Schnittstelle sendet Systemereignisse zu Sicherheit, Stabilität und Performance an die IT-Abteilung (SI). Ereignisse aus dem Bereich Gebäudesicherheit (wie Zutrittskontrolle oder Einbruch) werden nicht übermittelt. So kann die IT-Abteilung MICROSESAME zusätzlich zu den üblichen Betriebssystemüberwachungen (RAM, CPU usw.) gezielt mitverfolgen. Jedes Ereignis ist im Syslog-Modul aktivier- oder deaktivierbar und wird parallel im System-Ereignisprotokoll gespeichert.
Ereignisbeispiele:

- Sicherheitsereignisse - Bediener
  - Erfolgreiche / fehlgeschlagene Authentifizierungen
  - Passwortänderungen
  - Nicht autorisierte Aktionen (z. B. fehlgeschlagene Rechteerhöhung)
- Sicherheitsereignisse – Netzwerk / System
  - Ablauf von Kommunikationszertifikaten auf verschiedenen Ebenen der Architektur
- Stabilitätsereignisse
  - Unerwarteter Stopp eines Automats
- Leistungsereignisse
  - Lange Downloadzeiten bei der Aktualisierung von Zutrittsrechten

HOHE VERFÜGBARKEIT UND LEISTUNGEN

Die Architektur wurde entwickelt, um höchste Verfügbarkeit und Leistung bereitzustellen:

- Autonomer Betrieb jeder TILLYS CUBE mit ihren Erweiterungsmodulen und Peripheriegeräten – auch ohne Ethernet-Netzwerk und/oder Server. Bei Verbindungsverlust zu MICROSESAME speichert jede Einheit lokal die letzten 10.000 Ereignisse und lädt diese automatisch hoch, sobald die Verbindung wiederhergestellt ist.
- Direkte Kommunikation zwischen den TILLYS CUBE UTLs über IP (z. B. für Antipassback), ohne Server erforderlich.
- Schnelle parallele Verarbeitung zahlreicher Ausweislesungen – jeweils in unter 500 ms, selbst bei transparenten Lesern und Hochsicherheitsausweisen. Ermöglicht durch den integrierten HSM-Kryptoprozessor in allen Modulen, die diese Leser steuern und entschlüsseln.

- Server-Redundanz möglich über die virtuelle Infrastruktur des Kunden oder mittels der von TIL validierten und bereitgestellten SAFEKIT-Lösung.
- Drittarchitektur möglich zur Lastverteilung auf mehrere leistungsfähigen Maschinen.
- 24/7-Webportal für die Bereitstellung temporärer Lizenzen bei Serverausfällen.
- Industriell konzipierte CUBE-Automaten mit einem MTBF (Mean Time Between Failures) von 20 Jahren und einem MTTR (Mean Time To Repair) von nur 5 Minuten.
- Paralleler Download aller Konfigurationen zu allen UTILs vom Server aus.

UNTERSTÜTZUNG UND ANPASSUNGSFÄHIGKEIT AN AUSWEIS-CODIERUNGSRICHTLINIEN

Die TIL-Lösung ermöglicht höchste Sicherheit und eine große Projektflexibilität durch die zentrale Verwaltung von Schlüsseln und das individuelle Mapping des Ausweises gemäß der Encodierungsrichtlinie des Endkunden. TIL TECHNOLOGIES bietet dem Endkunden einen dedizierten Supportservice, um bei der Erstellung einer mehranwendungsfähigen, ANSSI-konformen, hochsicheren und zugleich flexiblen Ausweis-Encodierungsrichtlinie zu unterstützen. Damit kann der Ausweis optimal für bestehende und zukünftige Anwendungen genutzt werden

.

4. FUNKTIONSREICHTUM FÜR SICHERHEIT & SMART BUILDING

MICROSESAME ist ein offenes und skalierbares System. Es überwacht sowohl die eigenen Automatisierungseinheiten als auch die daran angeschlossenen Peripheriegeräte, Sensoren und Aktoren. Darüber hinaus kann es auch Fremdsysteme oder -produkte (wie industrielle Automatisierungsanlagen, Klimatisierung, Heizung, Brandmeldesysteme usw.) verwalten, sofern diese über unterstützte Protokolle wie MODBUS IP, OPC UA u. a. angebunden sind).

MICROSESAME vereint einen umfangreichen Funktionsumfang im Bereich **Sicherheit und Gebäudetechnik (GTB)**, da es mehrere Fachbereiche (Zutrittskontrolle, Einbruchmeldetechnik, Überwachung usw.) sowie verschiedene Marktsegmente (Industrie, Dienstleistungssektor, sicherheitskritische Anlagen, Infrastrukturen, öffentliche Einrichtungen usw.) abdeckt. Das System lässt sich exakt an die Anforderungen des Endanwenders anpassen und ist bei Bedarf jederzeit erweiterbar.

NUTZER- UND BEDIENERVERWALTUNG

VERWALTUNG DER IDENTIFIZIERTEN PERSONEN

Verwaltung von Personen, Besuchern und Operatoren sowie deren persönlichen Daten:

- Standardisierte und individuell anpassbare Felder (z. B. Name, Vorname)
- Vordefinierte Dropdown-Listen
- Gültigkeitsdauer der Identitäten
- Möglichkeit zur Zuordnung von Anhängen (z. B. Dokumente, Genehmigungen)
- Anzeige des letzten Badge-Vorgangs
- Zuweisung von Status-Tags wie „VIP“ usw.

ZUWEISUNG MEHRFACHER ID-MEDIENT JE PERSON MÖGLICH wie Ausweis (Badge), Kfz-Kennzeichen, virtuelle ID, QR-Code etc. Unterstützung von bis zu 4 ID-Technologien pro Nutzer. Pro Technologie bis zu 99 ID unterstützt (Bsp. 2 Badges + 3 Kfz-Kennzeichen).

INTEGRIERTER BADGE-DESIGNER: Gestaltung von Vorder- und Rückseite, Verwendung von fixen und variablen Textfeldern. Integration von Bildern, QR-Codes, Logos oder anderem Grafikmaterial.

VERWALTUNG VIELFÄLTIGER MAPPINGS UND ENCODIERUNGEN : Hochgradig personalisierbare und sichere Badge-Konfigurationen, mehranwendungsfähige und sichere Encodierung für verschiedene Anwendungen (Zutritt, Kantine, Zeiterfassung etc.). Badge-Ausgabe und Enrolment in einem einzigen Vorgang direkt über den Drucker, schnell, einfach und sicher. Vollständig integrierter Editor für Badge-Layout un Encodierung.

AUTOMATISCHE SYNCHRONISATION der erstellten personen und der in MICROSESAME codierten Multi-Anwendungs-Badges mit externen Anwendungen, wie Kantine, Zeiterfassung usw. möglich.

ZUTRITTSKONTROLLE

- Verwaltung individueller Zutrittsrechte nach Profil, mit Start- und Enddatum. Die Rechte werden den identifizierten **Personen** zugewiesen – **unabhängig** von ihren ID-Medien.

- Gruppenweise Änderung der Zutrittsrechte für Personen aus einer Mehrfachkriterien-Suche

- Automatische Zuweisung von Zutrittsrechten für Personen, die aus einer HR-Datenbank importiert wurden – basierend auf vordefinierten Regeln für alle Felder der Identitäten (z. B. Profil 1 für Abteilung 1)

- **Automatischer Download** der Liste der berechtigten Personen an die UTLs nach Validierung

- **Aufzugssteuerung mit Etagenfilter** je Person, Zeitfenster und Krisenstufe. Vorrangiger Aufzugsaufruf für berechtigtes Personal (z. B. in Krankenhäusern)

- **Kompatibilität mit verschiedenen Technologien** und allen Arten von Zutrittslesern:
  - Proximity-Leser 125 kHz und 13,56 MHz (MIFARE, DESFIRE, ICLASS usw.)
  - MOBILIS-Mobilgeräte-Leser 13,56 MHz (MIFARE, DESFIRE)
  - UHF-Weitbereichsleser, aktive Badges oder Fernbedienung
  - Leser für Kfz-Kennzeichen, biometrische Leser oder QR-Codes auf dem Smartphone
  - Digitale Zylinder und Drücker (online und offline)
  - Online-Lösung TIL + STid + HID für virtuelle Ausweise auf dem Smartphone mit:
    - EVOLUTION Bi-Techno-Lesern (Bluetooth / 13,56 MHz) oder HID-Leser
    - Onlineplattform in der Cloud

- **Steuerung verschiedener kontrollierter Zugänge oder Aktoren** (z. B. Schranken, elektrische Schlösser, Drehkreuze, Anzeigen, Sirenen, Beleuchtung usw.)

- **Hohe Flexibilität bei der Zutrittslogik**:
  Schleusen mit 2, 3 oder x-Türen, ein- oder Zwei-Wege-Zutritt, Leser oder Leser mit Tastatur (Badge + Code), Mobile Leser, einfaches oder doppeltes Badging für Risikozonen mit unterschiedlichen Personenkategorien.

- **Erweiterte Funktionen mit kumulativer Wirkung auf die Zutrittsrechte**:
  Kontrolle der Ruhezeiten, Personen- und zugangsbezogene Berechtigungen (z. B. elektrische, medizinische) mit Gültigkeitszeitraum, Krisenstufenverwaltung: 7 mögliche Stufen, individuell zuweisbar pro Person, Zugang und Etage, aktiviert über Bedienerschnittstelle oder Automatik. Wählbare Zutrittslogiken je nach Krise: Badge → Badge, Badge + Code, Doppel-Badge, Räumlicher & zeitlicher Rückkehrschutz (Anti-Passback), lokal oder global, mit Ausnahmeregelung, Zutritt unter Zwang mit Badge + speziellem Code, Abhängigkeitslogik: Badge-Vorgang an Leser X ist Voraussetzung für den an Leser Y

BESONDERE FUNKTIONEN IN DER ZUTRITTSKONTROLLE

BESUCHERMANAGEMENT mit einem vollständigen Workflow – von der Erstellung von Besuchen und Besucherdaten, über die Besuchsfreigabe bis hin zur Begrüßung am Standort.

PARKPLATZ- UND SICHERHEITSZONEN-VERWALTUNG mit Zählung der Anwesenden pro Zone und Zutrittsbeschränkung je nach Personenkategorie

EVAKUIERUNGSPLAN (Übung oder Ernstfall) mit dedizierter Benutzeroberfläche zur Anzeige von Anwesenheitslisten, Zählern, Standorten der anwesenden Personen je Sicherheits- bzw. Risikozone. Inklusive Fotos als Listen mit Ausdruckmöglichkeiten für Einsatzkräfte.

VERWALTUNG MEHRERER STANDORTE UND MANDANTEN unter Berücksichtigung von Standorten (Hardware, Überwachungsobjekte), Entitäten (Personen), Klassifikation (Leser) Perimeter (Schlüsselbereiche) sowie gezielte Anwenderverwaltung.

PCVA Video-Zutrittskontrolle durch einen Operator, der nach dem Badge-Vorgang den Zutritt entweder aktiv freigibt oder passiv überwacht – je nach zugewiesenem Zutrittsrecht.

BEFÄHIGUNG (Elektrik, Gefahrgut…) nach person und Zutrittspunkt mit Gültigkeitszeitraum.

KONTROLLE DER RUHEZEITEN, um die Einhaltung arbeitsrechtlicher Vorschriften zu gewährleisten.

KONTROLLRUNDGANG-MANAGEMENT mit zentral gesteuerten Rundgängen auf Basis von Lesepunkten und Badges.

QUARANTÄNENVERWALTUNG mit TILLYS CUBE – inklusive konfigurierbarer Wegeführung und Aufenthaltsdauer zwischen definierten Zonen.

AKTIVIERUNG DER BADGES AM TERMINAL durch die Nutzer selbst – über Eingabe eines persönlichen Aktivierungscodes am CARDIGO-Terminal.

EINBRUCHMELDETECHNIK

VERWALTUNG ALLER MELDEINFORMATION vom Typ Kontakt (z. B. Radare, Detektoren), angeschlossen an:

- Die überwachten Eingänge unserer Module
- Die EQUILOCK-Transponder über den Bus mit unserem EQUILOCK-Modul
- Fremde Automatisierungssysteme, die über MODBUS, OPC etc. mit unserem System verbunden sind
- Oder aus SORHEA-Lösungen über deren MAXIBUS-Schnittstelle mit unserem System oder aus Videoanalysen (VMS) über deren SDK-Schnittstelle.

ZENTRALE VERWALTUNG UND ZUWEISUNG DER EINBRUCHÜBERWACHUNGSBEREICHE aller TILLYS-Zentralen über MICROSESAME: Einfachheit, Schnelligkeit, Flexibilität. So können Benutzer mehrere Überwachungsbereiche über verschiedene Zentralen verwalten – jedoch nur die, für die sie berechtigt sind.

SCHARF-/UNSCHARFSCHLATUNG DER ÜBERWACHUNGSBEREICHE nach Zeitplan über das **TACTILLYS CUBE-Multizonen-Bedienteil**, mit automatischem, manuellem oder verbotenem Maskieren, Zählung, Zutrittsfreigabe, kombinatorischen oder sequentiellen Abhängigkeiten gemäß Projektvorgabe (z. B. dreifaches Badging auf einem Leser aktiviert die Überwachung

VOLLE UND NATIV INTEGRIERTE INTERAKTION MIT DER ZUTRITTSKONTROLLE da sie von der selben **TILLYS LVE** gesteuert wird**.**

AUTOMATISMEN UND AKTIONEN mit anderen Systemen (Video, Sirenen, Beleuchtung usw.)

ALARMFERNÜBERTRAGUNG (einschließlich Zutrittskontrolle und Gebäudetechnik) an eine Notruf- und Serviceleitstelle (NSL) per IP über das standardisierte „TIP“-Protokoll von TIL – qualifiziert bei ESI und Azur Sof oder mit dem SIA-Protokoll.

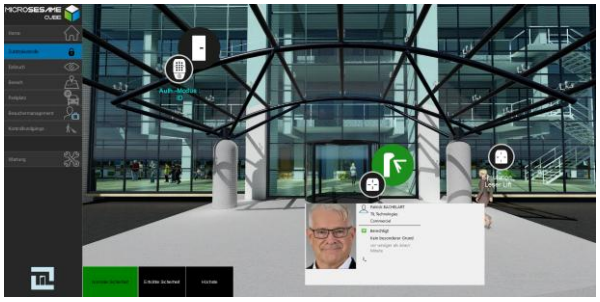
ÜBERWACHUNG & HYPERVISION - SICHERHEIT & SMART BUILDING

ALLGEMEINE ERGONOMIE DER BENUTZER-OBERFLÄCHEN so konzipiert, dass sie eine besonders einfache und intuitive Bedienung ermöglicht.

EREIGNISMONITOR UND ALARMÜBERWACHUNG in Echtzeit mit schneller Suchfunktion und Mehrfachfilterung.

INTEGRIERTER EDITOR FÜR ÜBERWACHUNGSGRAFIK nativ eingebunden, schnell konfigurierbar und hochgradig anpassbar mit: Objektlogik, Objektbibliotheken, Zoomfunktionen der Gebäudepläne unter Anderem.

ÜBERWACHUNG MIT GRAFISCHER PLANANIMATION mit animierten Symbolen für eine visuelle und dynamische Darstellung.



ECHTZEIT-ÜBERWACHUNG VON ALARMEN aus den Bereichen Zutrittskontrolle, Einbruch, Brand und Technik (z. B. Aufzugsstörung, Klimaanlage, Schutzschalter), inkl. Quittierung und hinterlegbaren Instruktionen, individuell pro Alarm und angepasst an das Anwenderprofil

BEREICHSÜBERWACHUNG MIT ZÄHLFUNKTION mit spezieller Benutzeroberfläche zur Anzeige von Listen, Zählern und der genauen Position der Anwesenden in jeder Zone.

SCHNITTSTELLEN ZWISCHEN MICROSESAME UND MARKTGÄNGIGEN VMS (z. B. MILESTONE, GEUTEBRUCK usw.), wobei die integrierte Komponente **VISIOSESAME** folgende Funktionen bietet::

- Parallele Überwachung mehrerer VMS-Videoströme gleichzeitig.
- Live-Videoanzeige durch Auswahl von Symbolen in den Plänen oder auf Basis von Alarmen. Steuerung von PTZ-Kameras und Videowänden.
- **Automatische Videoaufzeichnung** durch das VMS bei Einbruchsalarmen, Zutrittsversuchen usw
- **Wiedergabe von Videoaufzeichnungen** in VISIOSESAME, verknüpft mit den im MICROSESAME-Ereignisprotokoll gefundenen Alarmen.
- **Integration von Videoalarmen** (z. B. Bildanalyse) und **Kamerafehlermeldungen** (oder sonstiger VMS-Störungen).
- **Dashboard für die IT-Abteilung / CIO**, zur Überwachung von Systemprozessen (z. B. manuelles Starten/Stoppen von Diensten)

UMFASSENDE SCHNITTSTELLENOPTIONEN, HARD- UND SOFTWARE-GATEWAYS

OPTIONEN FÜR DATENAUSTAUSCH MIT MICROSESAME:

- Benutzerdatenbank & Besuchermanagement: Webservice via REST API, CSV-Dateien
- Anwenderverwaltung via Active Directory: LDAPs, Authentifizierung über Windows-Konto (SSO ⇒ Fat Client: NTLM, Web: SAMLv2)Superviseur I.T : SNMPv3 (Von TILLYS CUBE LVE aus)
- IT-Supervision: SNMPv3 (über UTL TILLYS CUBE)
- Hypervisor-Schnittstellen (Übergeordnete Überwachungsplattform, GMA): OPC UA, MODBUS IP
- Automatisierungssysteme und Fremdsysteme: MODBUS IP
- Video-Managementsysteme über VMS-SDK, TEXT/ASCII-Gateway
- Projektspezifische und/oder produktspezifische Gateways (z. B. Verzeichnisse, Drittsysteme, diverse SDKs)

Siehe auch Kapitel: GATEWAYS UND KONNEKTOREN

ENERGIEEINSPARUNG

- Überwachung der Verbrauchswerte
- Visualisierung der Gesamt- oder Teil-Leistungen
- Zonenfreigabe nach Prioritätsstufe je nach vertraglich festgelegter Leistung
- Jahresprogrammierung der Betriebszyklen gesteuerter Zonen (bis zu 3 Jahresprogramme)

STEUERUNG VON BELEUCHTUNG UND ANDEREN AKTOREN

- Ein-/Ausschaltsteuerung mit Zeitsteuerung
- Nachlauf- oder Ausnahmefunktion per parametrierbare Zeitschaltuhr (z. B. bei unregelmäßiger Raumnutzung)

STEUERUNG VON HEIZUNG, LÜFTUNG, KLIMA

- Ein-/Ausschalten von Reglern mit Zeitsteuerung
- Vorgabe von Temperaturwerten und Betriebsmodi: Frostschutz, Reduziert, Wirtschaftlich, Komfort
- Überwachung oberer und unterer Temperaturschwellen

STEUERUNG DER WARMWASSERVERSORGUNG

- Ein-/Ausschalten mit programmierbarem Zeitplan
- Betriebsarten programmierbar: Automatik, manuelles oder programmiertes Nachheizen

5. SYSTEMLEISTUNG

Konfiguration der Hardware	
Gleichzeitig verbundene Client-Workstations	499
Anzahl der Controller je Server (TILLYS CUBE LVE)	10 000
Controller je IP-Linie	255
Unterstützte Drivers (Linien)	128
Leser	20 000
Video-Rekorder	256

Konfiguration der Zutrittskontrolle	
Identifizierte Personen (Stammnutzer, Operatoren, Besucher)	unbegrenzt
ID-Medien (Zutrittskarte, Kfz-Kennzeichen…)	unbegrenzt
Standorte	2048
Entitäten	2048
Lesergruppen	Illimité
Leser je Gruppe	1 024
Zutrittsbereiche	128
Befähigungen	256
Video-Zutrittskontrolle	256
Kontrollrundgänge	64

Konfiguration der Überwachung	
Pfade, Eigenschaften insgesamt	40 960
Pfade, Eigenschaften je Linie	8 192
Eigenschaftskategorien	64
Zähler	2 048
Eigenschaften in einer Formatzeichenfolge	16

Konfiguration des Betriebs	
Operatoren (zentralisiert)	unbegrenzt
Einbruchberechtigte TILLYS V2 / CUBE / NG (local)	150

Zutrittskontrolle (Karteikarte Nutzer/ID-Medien)	
Verfügbare Lesetechnologien je Nutzer	4
ID-Medien je Lesetechnologie	99
Länge des Ausweis-Codes (an LVE-Treiber anzupassen)	32 Zeichen
Länge des Standort-Codes (an LVE-Treiber anpassen)	32 Zeichen
Definierbare Felder (Größe, Groß-/Kleinschreibung, Länge, Freitext, Pflichtfeld…)	16
Herunterladbare Felder in eine TILLYS CUBE LVE (nicht über 20 Zeichen)	Name, Vorname + 6 erste

Zeitpläne und Feiertage	
Zeitpläne je Standort (1 TILLYS CUBE LVE = 1 Einzelstandort, 1 Standort = x-LVE)	256
Zeitpläne insgesamt auf einem Zentralserver für mehrere Standorte	256 x Standorte
Tage je Zeitplan	9 (Wochen + Feiert. + Sondertage)
Zeitfenster je Tag	4
Zeitfenster-Mindestdauer	1 Min
Sondertage	32

Verlauf und Abfragen	
Ereignisse im Verlauf	unbegrenzt (gemäß DB)
Ereignisse je Verlaufabfrage	unbegrenzt
Aufbewahrungsdauer (konfigurierbar, z. B. zur Einhaltung einer Pflichtfrist)	30 Tage standard

Controller-Leistung	
Lokal gespeicherte Ereignisverlauf auf TILLYS CUBE LVE	10 000
Herunterladbare ID-Medien – TILLYS CUBE LVE	Bis 600 000 nativ
Leser je LVE – TILLYS CUBE LVE	24 natif
Anzahl der Meldergruppen – TILLYS CUBE LVE	32
Anzahl der Melder je TILLYS CUBE LVE im Intrusion CUBE-Modus	624

6. DSGVO-KONFORMITÄT

FEINGRANULARE VERWALTUNG DER NUTZUNGSRECHTE

MICROSESAME IST KONFORM MIT DEN DATENSCHUTZVORSCHRIFTEN DER DSGVO durch die nachfolgenden Funktionen, die in jedem der Hauptthemen der DSGVO verfügbar sind. Es obliegt dem Endkunden:

- Die nachstehenden in MICROSESAME verfügbaren Funktionen anzuwenden und umzusetzen**.**
- Festzulegen, welche Daten in den Freifeldern der Identitätsdatenblätter gespeichert werden sollen (für permanente, temporäre oder Besucherdaten).
- Die Operatoren und deren Zugriffsrechte auf die Daten zu definieren.
- Den Speicherort der SQL-Datenbank sowie die zugriffsberechtigten Personen zu benennen.

ZUTRITTSKONTROLLE FÜR NUTZER (EINSCHLIESSLICH ANWENDERRECHTE FÜR DIE VERWALTUNG VON BESUCHERDATEN)

- Der Zugriff auf personenbezogene Daten in den Identitätsdatenblättern ist durch Operatorrechte eingeschränkt – nach Feldern und nach autorisierten Einheiten (z. B. Personenkategorien oder Standorte.
- Der Zugriff auf freigegebene Daten kann schreibgeschützt und/oder bearbeitbar sein.
- Es lässt sich definieren, welche Felder bei der Erstellung von Besucherdaten verpflichtend sind (abweichend von den Feldern bei permanenten Identitäten).
- Ohne das Operatorrecht „Profil GESTION-RDV“ für Besucher kann ein Operator:
  - Über die Autovervollständigung nach bestehenden Besuchern in der Besucherdatenbank suchen, um Dubletten zu vermeiden, und dabei nur Name, Vorname und Firma einsehen.
  - Einen neuen Besucher vollständig mit allen Feldern (z. B. Geburtsdatum) erfassen, falls er noch nicht existiert.
  - In beiden Fällen kann der Operator keine weiteren Informationen in der Besucherdatenmaske einsehen, bearbeiten oder ändern.
    → Ist das entsprechende Recht aktiviert, kann der Operator alle Informationen der Besucherdaten einsehen, bearbeiten und ändern.

NACHVERFOLGBARKEIT: ART DER PROTOKOLLE, GESPEICHERTE DATEN UND AUFBEWAHRUNGSDAUER

- Alle Änderungen, Abfragen und Löschvorgänge von Personendaten werden protokolliert – ein Handeln in MICROSESAME ohne Protokollspur ist nicht möglich.
- Die Aufbewahrungsdauer der Daten ist konfigurierbar.
- Manuelles Löschen von Daten ehemaliger Mitarbeiter möglich.
- Import von Benutzerdaten aus HR-Datenbanken automatisch möglich, um manuelle Eingriffe zu minimieren.

DATENSICHERUNG

- Automatische, regelmäßige Sicherung der Datenbank auf Festplatte ohne manuelles Eingreifen.
- Regelmäßige Archivierung der Verlaufsdaten möglich.

DATENVERSCHLÜSSELUNG

- Absicherung der Zugriffsdatenströme: Fat Clients über TLSv1.3, Thin Clients über HTTPS.
- Anwender-Passwörter in der Datenbank geschützt durch SHA-512-Hashing plus 512 zufällig generierte Zeichen als Salt.
- WEBSESAME-Portal geschützt gegen "CSRF"-Angriffe.
- MICROSESAME ermöglicht die Anonymisierung der Datenbankdaten vor einer Weitergabe an Dritte zu Debugging- oder Migrationszwecken.

SCHUTZMASSNAHMEN FÜR SOFTWARE & AUFRECHTERHALTUNG DER SICHERHEIT

- Updates und Sicherheitspatches werden über das AMCO PREMIUM-Paket von TIL bereitgestellt, zertifiziert durch die ANSSI.

ANALYSE D'IMPACT AIPD (DATA PROTECTION IMPACT ASSESSMENT) / PIA (PRIVACY IMPACT ASSESSMENT)

- Für die Implementierung eines Sicherheitskonzepts mit Badges ohne biometrische Daten ist keine Auswirkungsanalyse erforderlich.

ZUTRITTSKONTROLLE UND BIOMETRIE

TIL TECHNOLOGIES und die Lösung MICROSESAME verarbeiten keine biometrischen Daten (Fingerabdrücke, Minuten usw.) direkt).

Die Lösung MICROSESAME integriert marktübliche biometrische Lesegeräte, z.B. von IDEMIA und STID. Unsere Steuerungen lesen ausschließlich die vom Lesegerät übermittelte Kennung (z.B. von einem Badge oder einer lokalen Datenbank) und niemals den Fingerabdruck selbst. Nur die Hersteller der Lesegeräte verwalten die biometrischen Daten. Sie bieten eigene gesetzkonforme Tools zur biometrischen Registrierung an (z.B. SECARD BIO, MORPHOMANAGER.

7. BENUTZERVERWALTUNG

FEINGLIEDRIGE UND SICHERE VERWALTUNG DER NUTZUNGSRECHTE VON MICROSESAME

Ein Benutzer ist eine natürliche Person, die zur Nutzung der Überwachungsoberfläche von MICROSESAME berechtigt ist. Je nach Funktion, Hierarchieebene oder geografischer Lage kann dieser Benutzer auf alle oder nur auf bestimmte Teile der in MICROSESAME verfügbaren Funktionen und Daten zugreifen.



Um jedem Benutzer ausschließlich die für ihn notwendigen Rechte zuzuweisen – und dies schnell und effizient nach Operator-Typ – beinhaltet MICROSESAME das Konzept der **„Benutzerprofile“**. Diese Profile werden durch ein System von Auswahlkästchen definiert, das einen feingliedrigen Zugriff auf die einzelnen Hauptfunktionen ermöglicht – jeweils in den Modi *Anzeigen*, *Erstellen*, *Bearbeiten* und *Löschen*:

- Rechte im Zusammenhang mit der Zutrittskontrolle.
- Rechte im Zusammenhang mit der Systemnutzung.
- Rechte im Zusammenhang mit dem Verlauf.
- Rechte im Zusammenhang mit Identitäten (einschl. Personenbezogener Daten).
- Rechte im Zusammenhang mit Besuchen.
- Rechte im Zusammenhang mit der Überwachung (einschließlich Kategorien von Eigenschaften wie z. B. Zutritt, Einbruch, Brand usw.; Anzeige / Bestätigungsstufe von Alarmen).
- Rechte im Zusammenhang mit den Einstellungen (einschließlich Filterung bei Multi-Site-Projekten nach Leserstandorten, Standorten von grafischen Objekten, identifizierten Einheiten, Klassifizierung jedes Zugangs – mit einer Granularität, die über das einfache Standortkonzept hinausgeht).
- Rechte im Zusammenhang mit der Sicherheit.

Aufgrund der Vielzahl und Differenziertheit der Benutzerprofile und Rechte gibt es regelmäßig aktualisierte, spezifische Dokumente, auf die Sie sich beziehen können und die über Ihren gewohnten TIL-Ansprechpartner erhältlich sind.

Für jeden neu angelegten Benutzer genügt es anschließend, ihm eines oder mehrere dieser vordefinierten Operatorprofile zuzuweisen.

Die Rechteverwaltung ist gesichert, benutzerfreundlich gestaltet und systemseitig vorgesehen.

Die Rechteverwaltung ist sicher, benutzerfreundlich, für große anwenderzahlen ausgelegt und vereinfacht Nutzung, Wartung und Implementierung:

- Eine Änderung der Benutzerprofile wirkt sich automatisch auf alle zugewiesenen Benutzer aus.
- Ein Benutzer kann mit einem oder mehreren Profilen verknüpft werden, sodass er z. B. in die gleiche Rolle schlüpfen kann wie ein Kollege, dem er helfen möchte.
- Ein Benutzer ist zunächst eine identifizierte Person, also eine Person mit physischer Zutrittsberechtigung, die zusätzlich als Benutzer in der Software MICROSESAME deklariert wurde. Dadurch entfällt eine doppelte Eingabe personenbezogener Daten und Datensätze.
- Hierarchie zwischen Benutzern: Um Benutzerrechte zu ändern, muss der ausführende Benutzer eine höhere Hierarchiestufe als die betroffenen besitzen (bezogen auf Hierarchiestufe und Profil).
- Benutzer-Passwörter werden in der Datenbank durch einen SHA-512-Hash mit einem 512 Zeichen langen zufälligen Salt geschützt.
- Nachvollziehbarkeit und Historie der Benutzeraktionen (einschließlich geänderter Felder/Werte) – eine gesetzliche Anforderung in vielen Branchen (Lebensmittelindustrie, Pharma, Transport, Kernenergie usw.).
- Zentrale Verwaltung der Benutzerrechte in MICROSESAME für alle Client-Typen (Fat Client, Thin Client, Web).
- Jedem Benutzer wird ein Standard-Login und -Passwort zugewiesen, das beim ersten Login geändert werden muss – nur der Benutzer kennt es danach.
- Automatische Abmeldung von WEBSESAME-Benutzern nach längerer Inaktivität oder beim Neustart des Apache-Webserver.
- Rechte zur Durchführung von Änderungen können gezielt vergeben werden, abhängig von verschiedenen Kriterien und dem Profil des Mitarbeiters.
- Mitarbeiter können Änderungen durchführen, ohne dass dabei eine Löschung erforderlich ist
- Erweiterung der Benutzerrechte möglich, z. B. um das Kommentarfeld bearbeiten zu können, ohne andere Felder zu beeinflussen

LDAP/Active Directory-Verzeichnisdienst

Die Benutzerverwaltung kann entweder direkt in MICROSESAME oder über ein zentrales Active Directory (A.D.) des Endkunden erfolgen. Dieses wird von dessen IT-Abteilung verwaltet und über eine LDAP-Schnittstelle mit MICROSESAME verbunden. Vorteile:

- Zentrales Referenzverzeichnis für alle Nutzer der Unternehmensanwendungen, was die Erstellung, Änderung und Löschung von Benutzern vereinfacht. Aktualisierungen erfolgen automatisch.
- Zuweisung von in MICROSESAME definierten Benutzerprofilen direkt im A.D., inklusive Unterstützung von Mehrfachprofilen und Authentifizierung via LDAP.
- Verwaltung komplexer Passwörter und Timeouts (automatische Abmeldung) durch die Leistungsfähigkeit des A.D.
- Sichere Benutzerverwaltung über LDAPs (verschlüsselte LDAP-Verbindung).

8. VERWALTUNG MEHRERER STANDORTE/MANDANTEN

GEOGRAFISCHE ODER ORGANISATORISCHE NUTZUNG

MICROSESAME ermöglicht die Verwaltung zahlreicher, voneinander unabhängiger Standorte über ein und dasselbe System. Diese Funktion ist in verschiedenen Szenarien besonders nützlich:

- Verwaltung geografisch verteilter Gebäude, z. B. Filialnetze, kommunale Einrichtungen oder Produktionsstandorte – zentral gesteuert über einen einzigen Server.
- Bedarf an unterschiedlichen Rechteverwaltungen innerhalb eines einzelnen Standorts, etwa auf Abteilungsebene.
- Nutzung eines Gebäudes oder eines Turms durch mehrere Firmen oder Mieter, mit Unterscheidung zwischen gemeinsamen und eigenen Zugängen.
- **Flexible Serverwahl**: entweder ein zentraler nationaler Server für alle Standorte oder ein Server pro Standort – je nach Netzwerkqualität und gewünschter Organisationsstruktur (zentralisiert, dezentralisiert etc.)
- **Flexible Badge-Administration**, mit folgenden Optionen:
  - Zentrale Personalisierung und Codierung in der Hauptverwaltung.
  - Zentrale Codierung mit dezentraler Personalisierung vor Ort.
  - Lokale Personalisierung und Codierung an jedem Standort.

Die Nutzung der Multisite-Funktion erfordert einen zentralen Administrator, um:

- Die zentrale, einheitliche Datenbank zu verwalten.
- Die Standorte zu definieren, wobei der kleinste verwaltete Standort eine sogenannte LVE ist (lokale Verarbeitungseinheit). Dabei ist zu beachten: Die LVE ist architekturbedingt einzelstandortbezogen, daher sind Auswahl, Positionierung und Verkabelungsaufwand bei LVEs sorgfältig zu planen.
- Die Zuweisungseinheiten für Personen festzulegen.
- Benutzerrechte sowie die Benutzer pro Standort gemäß der Organisationsstruktur und den internen Abläufen zu definieren.
- Standort-, Abteilungs- oder unternehmensbezogene Administratoren zu benennen, die mittels Operator-Hierarchie gezielt Befugnisse erhalten. Sie können u. a. verwalten:
  - Die Zutrittsrechte ihres Personals auf die Lesegeräte ihres Standorts sowie – sofern vorhanden – auf gemeinsam genutzte Geräte (Empfang, Parkplätze, Aufzüge etc.).
  - Die Einsicht in die Verläufe und Bewegungsdaten ihres eigenen Personals
  - Diese Administratoren haben keinen Zugriff auf Lesegeräte oder Rechte **anderer** Standorte und sehen auch keine personenbezogenen Daten oder Historien anderer Organisationseinheiten.

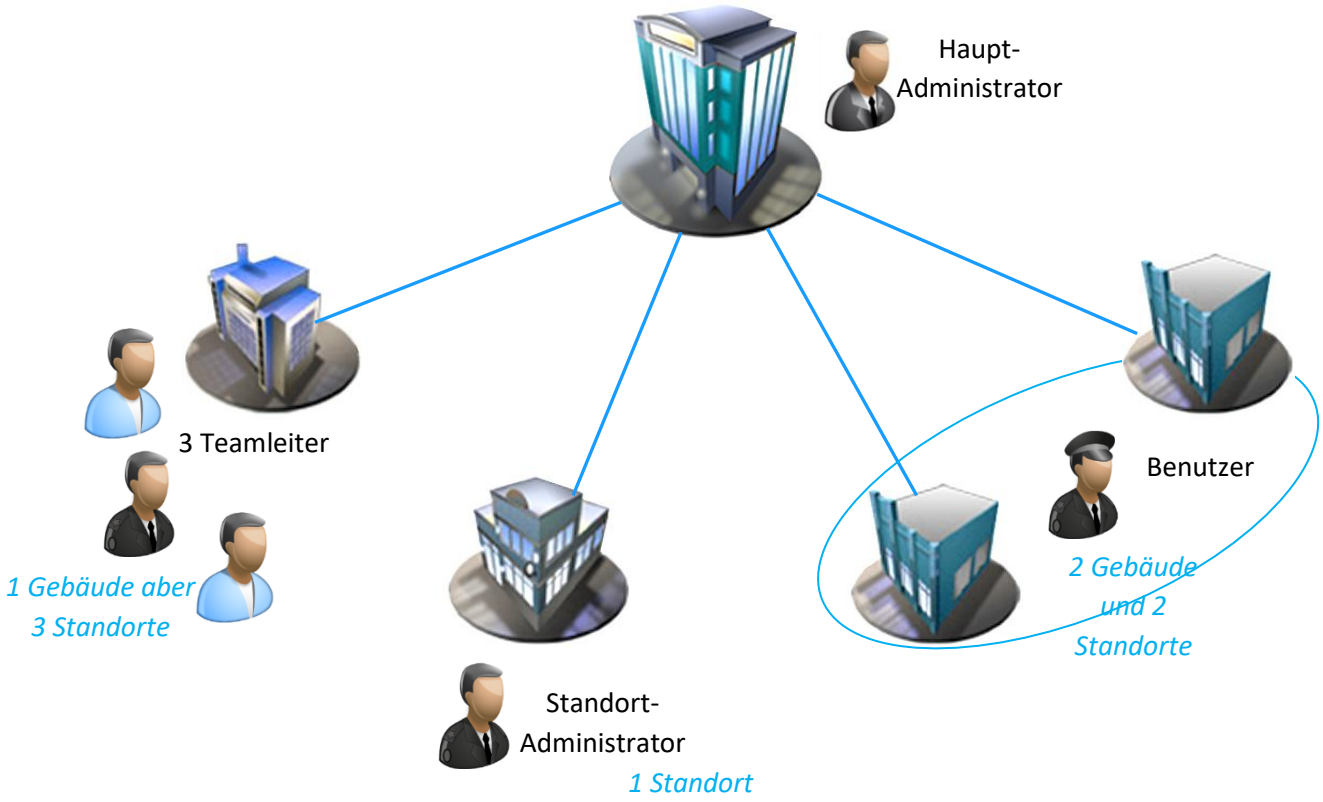
Jeder Standort verfügt über 256 unabhängige Zeitpläne, die für verschiedene Zwecke genutzt werden können – etwa für die Zutrittskontrolle, Einbruchmeldetechnik oder das technische Gebäudemanagement (z. B. Alarmsysteme, automatische Bewässerung usw.).

Das zentrale System kann bis zu 256 Standorte verwalten und insgesamt 256 x 256 Zeitpläne für alle Standorte bereitstellen.

Für die Sicherheit der Badge-Schlüssel ermöglichen das Tool *KSM*, die Codiertools und die CUBE-LVE dem zentralen Sicherheitsbeauftragten die Verwaltung unterschiedlicher Schlüssel pro Standort. Dies geschieht mithilfe des Perimeterkonzepts, wie es im ANSSI-Leitfaden (BSI anerkanntes zertifizierungsstelle für die Cybersicherheit von IT-Systemen) gefordert wird.

Ein spezifisches Dokument zu möglichen Multisite-Architekturen ist über Ihren gewohnten TIL-Ansprechpartner erhältlich

.



9. VERWALTUNG DER ZUTRITTSPUNKTE

PROFILE, ZEITPLÄNE, BEFÄHIGUNGEN, LESER, BEREICHE...

Die Karteikarte Benutzer/ID-Medien fasst zusammen und definiert:

INFORMATIONEN ÜBER DIE IDENTIFIZIERTE PERSON: Gültigkeitsdaten, Unternehmen, Abteilung, Kontaktdaten sowie 16 zusätzlich frei definierbare Bezeichnungsfelder. Anhänge wie z. B. Arbeitsvertrag, Foto etc. können ebenfalls zugeordnet werden).

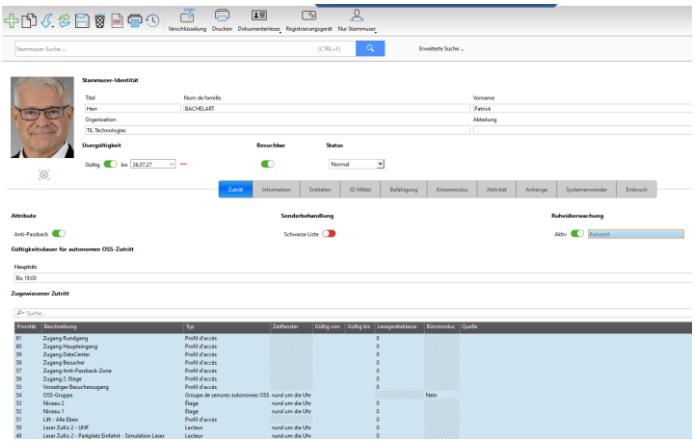
SEINE ID-MEDIEN: Bis zu 4 unterschiedliche Identifikationstechnologien sind möglich (z. B. 13,56 MHz-Badge, 125 kHz-Badge, Tastaturcode, KFZ-Kennzeichen, QR-Code…). Für jede Person können bis zu 99 ID-Medien pro Technologie gespeichert werden. ID-Medien können verschiedene Status haben: defekt, verloren, gestohlen, nicht zurückgegeben – zur Angabe des Sperrgrundes. So wird für eine Person nur ein einziger Datensatz erstellt, selbst wenn sie mehrere ID-Medien besitzt.

SPEZIFISCHE ATTRIBUTE: Anti-Passback, schwarze Liste (für gezielte Überwachung), Akkreditierungsstufe (im Krisenmodus), Besuchserlaubnis, Begleitfunktion u. v. m.

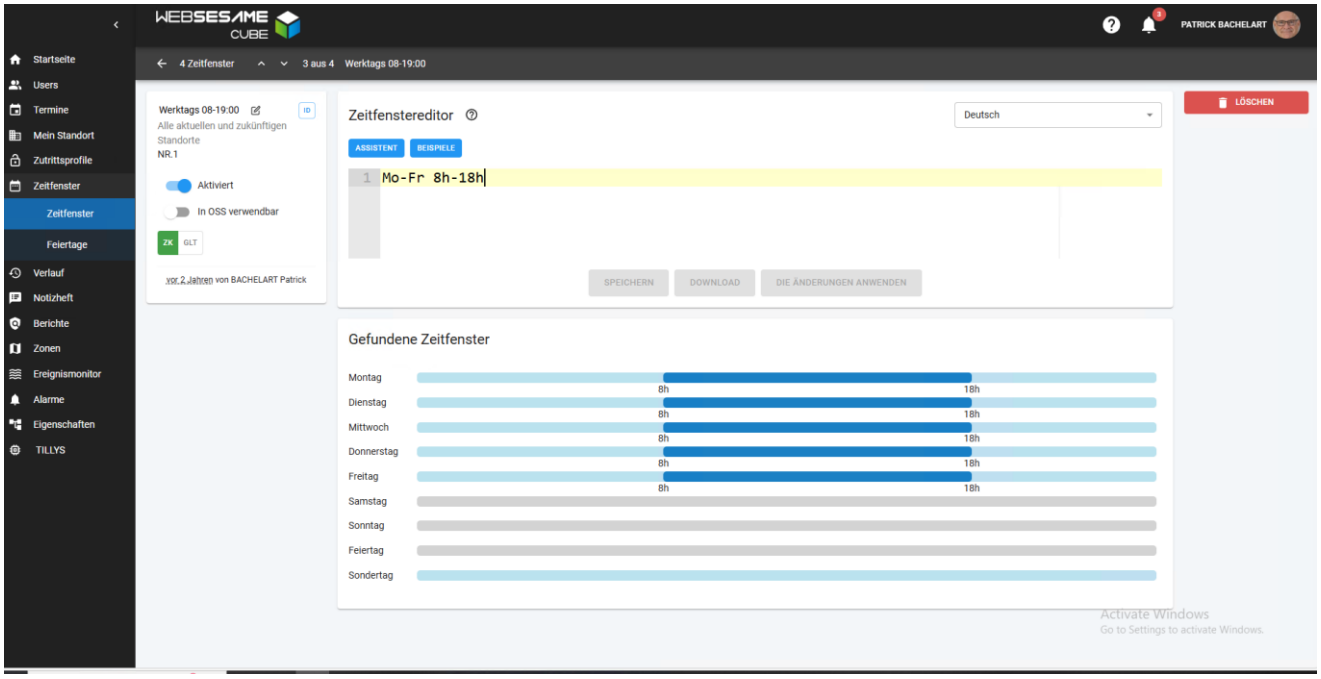
EINE GÜLTIGKEITSPERIODE: Diese ist jeder identifizierten Person zugeordnet und erlaubt eine schnelle, temporäre Deaktivierung (oder Reaktivierung) eines ID-Mediums, ohne die komplette Rechtevergabe zu löschen

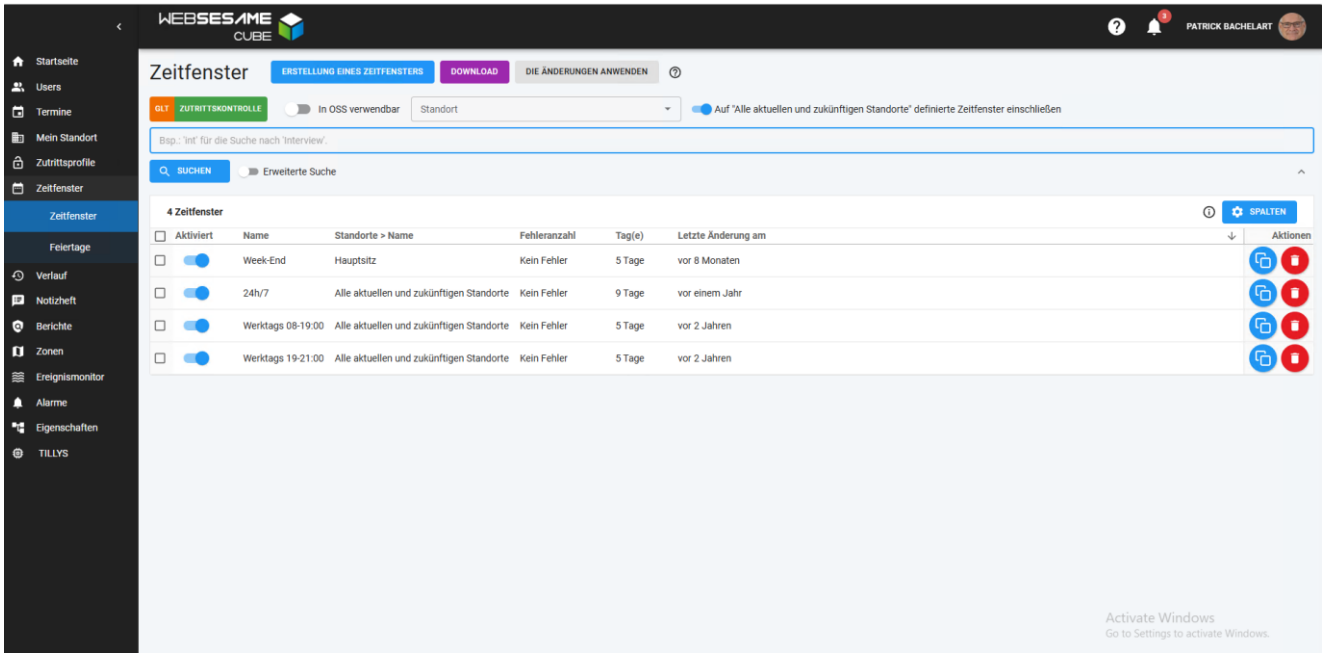
DIE VERWALTUNG DER ZUTRITTSRECHTE, DIE EINE FLEXIBLE ANSICHT UND SCHNELLE RECHTEZUWEISUNG ERMÖGLICHT: Gemeinsame Ansicht, Textfilter, Mehrfachauswahl von Rechten aus einer Liste mit Profilen, Online-/Offline-Lesern, Lesergruppen, Aufzugsetagen, Schlüsseln & Schlüsselgruppen vernetzter Schlüsselschränke. Die Zutrittsrechte werden der Person zugewiesen – **nicht** den ID-Medien (z. B. Badges). Daher ändert sich beim Verlust eines Badges und Zuweisung eines neuen **nichts** an den Zutrittsrechten.

VERWALTUNG INDIVIDUELLER ZUTRITTSPUNKTE



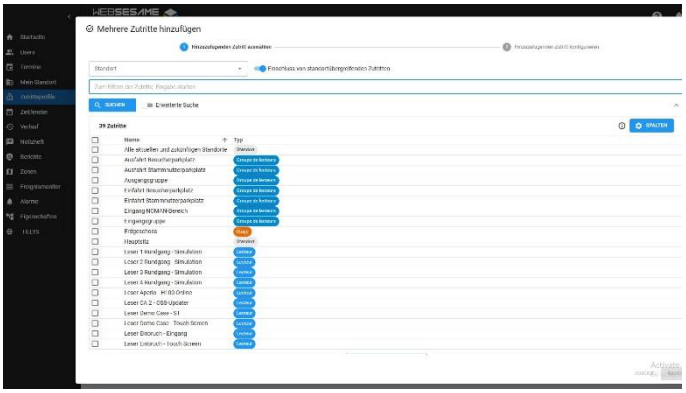
Die Zuweisung einer Zutrittsberechtigung ermöglicht einem identifizierten Nutzer den Durchgang an einem Leser oder einer Lesergruppe, entsprechend einem definierten Zeitplan (128 Zeitpläne verfügbar). Die **LVE TILLYS CUBE** werden regelmäßig durch MICROSESAME – den „Zeitgeber“ – synchronisiert, um sicherzustellen, dass keine zeitliche Abweichung zwischen LVE und Server entsteht und die Zeitpläne korrekt eingehalten werden.





ZUTRITTSVERWALTUNG ÜBER PROFILE

Ein Zutrittsprofil ermöglicht die vordefinierte Zuweisung von Zutrittsrechten für eine bestimmte Kategorie von Identifizierten – standortübergreifend oder standortspezifisch.



Ein Profil besteht aus einer Liste von:

- Online-/Offline-Lesern und/oder
- Lesergruppen und/oder
- Schlüsseln von vernetzten Schlüsselschränken und/oder
- Schlüsselgruppen und/oder
- Aufzugsetagen

Jedem Leser oder jeder Gruppe kann dabei ein eigener Zeitplan zugewiesen werden.

Jedem Identifizierten können ein oder mehrere Zutrittsprofile zugewiesen werden. Ausnahmen für einzelne Personen lassen sich über die individuelle Zugangsverwaltung auf Leser- und/oder Gruppenebene definieren.

Beispiel:
Ein „Allgemeines“ Profil für gemeinsame Zutrittspunkte,
ein „Abteilungs“-Profil für bereichsspezifische Zutrittspunkte
und zusätzliche Rechte, die mit der Funktion oder Hierarchieebene einer Person zusammenhängen.

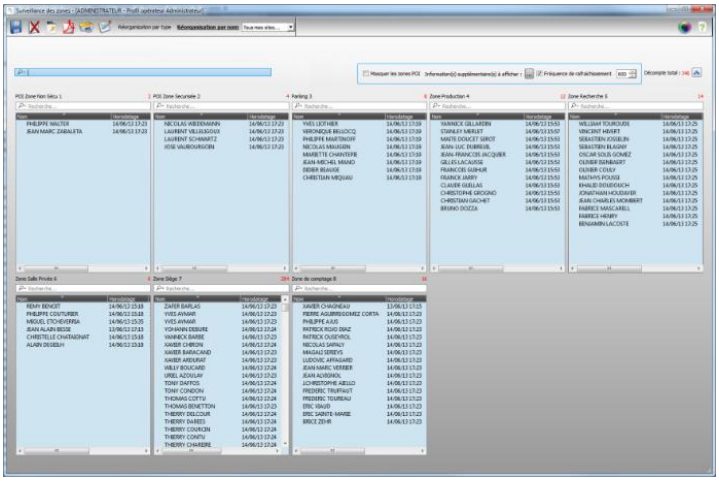
MICROSESAME bietet auch ein spezielles „Alle Leser“-Profil pro Standort, das alle aktuellen und zukünftigen Leser des Standorts umfasst. Dieses Profil ist besonders praktisch, wenn man einem Identifizierten uneingeschränkten Zugang zu allen Lesern eines Standorts gewähren möchte, ohne das Profil bei jeder neuen Installation aktualisieren zu müssen.

Die Verwaltung der Zugangsrechte für Identifizierte ist äußerst flexibel. Sie ermöglicht eine schnelle Übersicht und Zuweisung von Rechten, wie Gesamtansicht aller Zugänge, Textbasierter Filter, Mehrfachauswahl in einer Liste, die Profile, Leser, Lesergruppen und Aufzugsetagen zusammenfasst

Eine spezielle Funktion in der Verwaltung von Identifizierten zeigt permanent die „resultierenden Zugänge“ an, also die Gesamtheit aller aktiven Zutrittsrechte, die dem Identifizierten durch die ihm zugewiesenen Profile gewährt werden.

.

VERWALTUNG VON BEREICHEN (ZONEN)



MICROSESAME unterstützt die Verwaltung von Bereichen oder Zonen.

Ein Bereich wird definiert durch zwei Gruppen von Lesern:
– eine Gruppe für den Eingang in die Zone
– eine Gruppe für den Ausgang aus der Zone

Eine Lesergruppe kann eine beliebige Anzahl von Lesern innerhalb einer Anlage enthalten

Es ist möglich, genau zu ermitteln, wie viele Personen sich in jeder Zone befinden, und eine Liste der Anwesenden zu erstellen – sortiert nach Alphabet, nach chronologischer Ankunft oder nach anderen Kriterien wie Unternehmen usw.

Diese Zonenverwaltung wird besonders häufig in SEVESO-klassifizierten Einrichtungen eingesetzt und ist unerlässlich für die Umsetzung der spezifischen Anwendung, die von TIL zur Unterstützung des Interner Einsatzplans entwickelt wurde.

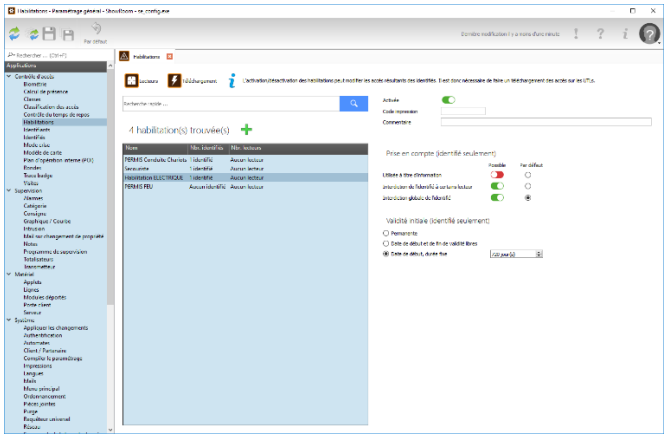
Im Falle der Auslösung eines Einsatzplans kann die Liste der in einer Zone anwesenden Personen automatisch per E-Mail versendet werden.

Die Zonenverwaltung ermöglicht außerdem eine präzise Kontrolle der Bewegungen innerhalb einer Anlage.

MICROSESAME erlaubt es zudem,

- Zonen ineinander zu verschachteln und
- Leser nur dann zu aktivieren, wenn zuvor eine andere Zone verlassen wurde – was einen verpflichtenden Durchgang erzeugt, auch bekannt als Abhängigkeitskonzept in MICROSESAME**.**

VERWALTUNG VON BEFÄHIGUNGEN



Die Zutrittsberechtigungen eines Nutzers zu bestimmten Zonen oder Lesern können von einer gültigen Qualifikation abhängig gemacht werden, die außerhalb der klassischen Zutrittskontrolle liegt, wie z. B.:

– Elektrofachkraft-Zulassung
– ATEX-Zertifizierung
– Berechtigung zum Führen von Maschinen
– Erste-Hilfe-Ausbildung
– Zeitlich befristeter Arbeitsvertrag
– Medizinische Tauglichkeit usw..

Diese Gültigkeitsvoraussetzung kann von verschiedenen Personen verwaltet werden, etwa vom HR-Bereich oder von der jeweils zuständigen Fachabteilung.

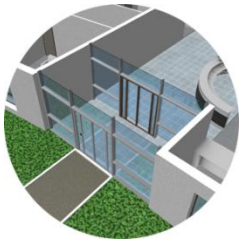
Diese Funktionalität erlaubt die Verwaltung von bis zu 256 verschiedenen Habilitationen (Berechtigungen / Qualifikationen.

Jeder Nutzer kann mehrere Habilitationen (Berechtigungen) besitzen**,** wobei jede einzelne ihre eigene Gültigkeitsdauer hat**.**
Der Zutritt zu einem bestimmten Leser kann an die Gültigkeit einer oder mehrerer dieser Habilitationen geknüpft werden**.**

ERWEITERTE SICHERHEITSFUNKTIONEN

ANTI-PASSBACK : Bei Zutrittsbereichen mit Lesern am Ein- und Ausgang ermöglicht die Zonenverwaltung die Umsetzung eines Anti-Passback-Mechanismus. Dieser verhindert, dass sich eine identifizierte Person mehrfach hintereinander in eine Zone einbucht, ohne diese zuvor verlassen zu haben.

SCHLEUSENSTEUERUNG: Die leistungsfähige Programmierung des Systems erlaubt eine projektspezifische Kopplung mehrerer Türen. Dabei können verschiedene Technologien kombiniert werden:
Bodenkontaktmatten,
Vereinzelungsmatten,
Videokameras,
biometrische Leser usw.



MEHRFAKTOR-IDENTIFIKATION: MICROSESAME bietet die Möglichkeit, bestimmte Leser mit einer Doppelkontrolle auszustatten: Durchziehen eines autorisierten Ausweises und Eingabe eines persönlichen Codes über eine Tastatur. Diese verstärkte Kontrolle gewährleistet eine starke Authentifizierung des Ausweisträgers für besonders sensible Bereiche.
Der geheime Code kann entweder für alle Identifizierten gleich oder individuell vergeben werden.

CODE UNTER ZWANG : MICROSESAME erkennt auch die Eingabe eines unter Zwang eingegebenen Codes. In diesem Fall wird am Bedienplatz sofort ein stiller Alarm ausgelöst, während der Zutritt ohne akustisches Signal freigegeben wird.

ÜBERWACHUNG DER "SCHWARZEN LISTE": Diese Funktion ermöglicht die sofortige Alarmierung, sobald ein auf der „Schwarzen Liste“ verzeichneter Ausweis an einem der Leser im System präsentiert wird. Dies erlaubt ein schnelles Eingreifen im Falle eines Missbrauchsversuchs mit einem verlorenen oder gestohlenen Ausweis.

KRISENMODUS: MICROSESAME ermöglicht die Verwaltung von Krisenschwellen. Basierend auf standortspezifischen Kriterien können bis zu 7 Krisenstufen definiert und sowohl Personen (nach Hierarchie, Berechtigungen usw.) als auch Lesern (nach Zonen, Alarmtypen usw.) zugewiesen werden.

VIGIPIRATE
SECURITE RENFORCEE
RISQUE ATTENTAT

Wird ein Krisenmodus ausgelöst, erhält jede LVE im System den Befehl zur Anpassung der Schwelle und steuert automatisch die Zuordnung zwischen den Akkreditierungsstufen der Personen und den Sicherheitsniveaus der Leser. Eine Person mit einer niedrigeren Stufe als die eines Lesers erhält keinen Zutritt mehr und kann auch keine Etagen mehr per Aufzug erreichen. Der Krisenmodus wirkt sich auf sämtliche Zutrittsrechte von Online-Lesern aus – einschließlich der Kabinenleser zur Etagensteuerung.

Mehrere Krisenszenarien können ausgelöst werden durch:

- Automatische Kopplungen auf Basis definierter Eingangskombinationen
- Manuelle Bedienaktionen durch autorisierte Operatoren über Schaltflächen in zuvor vom Integrator konfigurierten Übersichtsplänen: Ein Szenario X versetzt die definierten Leser in die gewünschte Krisenstufe

QUARANTÄNE

MICROSESAME verfügt über eine hochgradig konfigurierbare Verwaltung von Quarantänezeiten (ab Firmware TILLYS NGv2.3).

Es wird empfohlen, pro Quarantänezone eine eigene LVE zu verwenden.
Für jeden Zutrittspunkt über einen bestimmten Leser durch eine Person X (Quarantäne-auslösender Leser) können individuelle Quarantänezeiten für nachgelagerte, von der Quarantäne betroffene Leser definiert werden – spezifisch für die Person X (z. B. 2 Stunden für Leser 1, 5 Tage für Leser 2 usw.)

Wird versucht, auf einen von der Quarantäne betroffenen Leser zuzugreifen, ohne dass die Quarantänezeit abgelaufen ist, erscheint eine Alarmmeldung im Ereignismonitor.
In diesem Fall, also bei Zugriffsverweigerung aufgrund einer nicht eingehaltenen Quarantänezeit, informiert die Meldung darüber, ab wann (in Tagen/Stunden) die betroffene Person X den Zutritt an den entsprechenden Lesern wieder erlangt.

Die LVE arbeiten völlig autonom, da sie direkt miteinander kommunizieren.
Bei einem Netzwerkausfall speichert jede LVE die Nachrichten und die genaue Uhrzeit des Ausweisvorgangs. Nach Wiederherstellung der Verbindung erfolgt die automatische Übertragung dieser Informationen an die anderen LVE.

FAHRSTUHLVERWALTUNG

Die Installation von Ausweislesern in den Aufzügen eines Gebäudes ermöglicht es, den Zugang zu bestimmten Etagen abhängig von individuellen Rechten, Personalprofilen oder der Zugehörigkeit zu Unternehmen einzuschränken, insbesondere in einem Mehrmietergebäude.

MICROSESAME verwaltet diese Funktionalität standardmäßig direkt innerhalb der Zutrittsrechte der Nutzer. Etagen oder Etagen-Gruppen werden dabei wie Ausweisleser des Gebäudes behandelt und können daher in Lesergruppen oder Zugangsprofile integriert werden.

Die Multisite-Verwaltung in einem Gebäude mit mehreren Mietern ermöglicht es, zu steuern, welche Etage von welchem Verwalter verwaltet wird, wobei zu beachten ist, dass eine LVE nur einen Standort verwaltet. Die Etagen können zum Beispiel wie folgt organisiert werden:

- Der Hauptverwalter (Vermieter) kann die Zugangsrechte für alle Etagen verwalten.
- Jeder Mieter verwaltet die Zutrittsrechte ausschließlich für die von ihm gemieteten Etagen sowie für die gemeinsam genutzten Bereiche (Erdgeschoss/Empfang, Parkplätze, Kantine usw.) – und dies nur für das eigene Personal, mithilfe von Entitäten.

Ein Mieter kann somit Zutritte zu seinen eigenen Etagen sowie zu den Gemeinschaftsbereichen gewähren. Die Kontrolle über die Zeitpläne der gemeinschaftlich genutzten Etagen bleibt jedoch beim Hauptverwalter des Gebäudes.
Für die Nutzung dieser Funktionalität ist eine eigene LVE für die Aufzugssteuerung erforderlich.

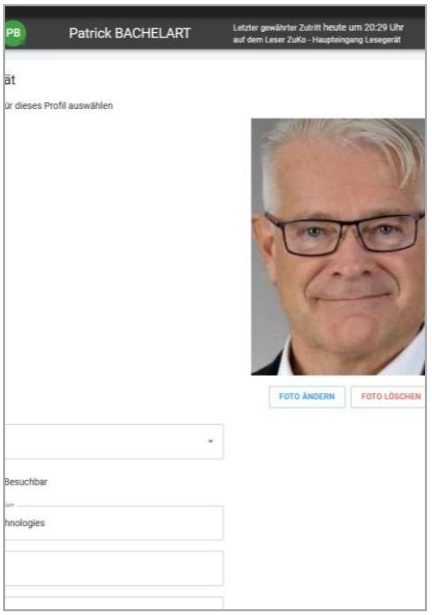
FAHRZEUGZUFAHRT UND PARKPLATZVERWALTUNG

MICROSESAME kann spezielle Leser für die Fahrzeugzufahrt überwachen, wie z. B. Weitbereichleser (mit Fernbedienung oder aktiven Ausweisen), Kennzeichenerkennungssysteme oder QR-Code-Leser.
Diese Geräte erleichtern die Steuerung des Fahrzeugflusses – insbesondere zu Stoßzeiten – und erhöhen den Komfort für die Nutzer.
Die Integration in MICROSESAME erfolgt nahtlos: Fernbedienungen oder Weitbereichausweisen (sog. Tags) senden eine Identifikationsnummer wie jeder andere Ausweis, und Kennzeichen werden direkt im Datensatz des Nutzers verwaltet (bis zu 99 Kennzeichen pro Person).

Diese integrierte Verwaltung der ID-Medien erlaubt mehr als nur die Zufahrtkontrolle – beispielsweise kann ermittelt werden:

- Die Gesamtzahl der Fahrzeuge.
- ie Auslastung je nach Personaltyp, Abteilung oder Unternehmen (bei gemeinsam genutztem Parkplatz).
- Belegungsvolumen und -dauer für Kostenstellenzuweisungen oder Weiterverrechnungen

WEBGESTÜTZTE VERWALTUNG DER NUTZER



Zur vereinfachten Nutzung der Zutrittskontrolle stehen neben den klassischen Server- und Fat-Client-Oberflächen (siehe „Kartei-karten“-Maske auf Seite 11) auch „leichte“ Web-Oberflächen für die Verwaltung von Nutzern und Besuchern zur Verfügung.
Über jeden beliebigen PC oder ein mobiles Gerät mit Internetbrowser und -verbindung erlaubt die neue Oberfläche WEBSESAME:

- Das Suchen und Anzeigen von „Nutzer“-Datensätzen nach verschiedenen Kriterien.
- das Erstellen oder Bearbeiten von Datensätzen, einschließlich der Zuordnung eines Fotos (z. B. per Smartphone oder Tablet schnell aufgenommen)
- Die Zuweisung von Zutrittsprofilen und bestehenden ID-Medien.
- den Import/Export von Identifizierten/Identifikatoren

Diese Funktionen stehen auch für die Verwaltung von Besucherdaten (externe Personen) zur Verfügung.
Weitere Web-Oberflächen für die Zutrittskontrolle sind ebenfalls verfügbar, z. B. für die Verwaltung von Besuchsterminen (externe Besucher) oder zur Einsicht in das Zutrittsprotokol.

10. BESUCHERVERWALTUNG

TERMINPLANUNG UND BESUCHEREMPFANG

Auf einem Gelände mit Zutrittskontrollsystem müssen externe Personen erfasst, begleitet und ggf. mit einem Identifikationsmittel ausgestattet werden, um sich in den für sie freigegebenen Bereichen bewegen zu dürfen. Dieses Ziel ergibt sich aus der Sicherheitsrichtlinie des Endkunden.

Die Besucherverwaltung von MICROSESAME ermöglicht die Terminplanung, die Steuerung der Besucherströme sowie eine Optimierung der Empfangsprozesse – bei gleichzeitiger Gewährleistung von Flexibilität und Sicherheit.
Um sich bestmöglich an die Bedürfnisse, Abläufe und Organisation des Endkunden anzupassen, bietet die Lösung allgemeine vordefinierbare Parameter (z. B. Standarddauer eines Termins begrenzen) sowie funktionale Einschränkungen je nach Benutzerprofil (Anfragender, Genehmigender, Empfangspersonal.

Diese Softwareoption von MICROSESAME wird über drei dedizierte Schnittstellen bereitgestellt:

- Die Weboberfläche **WEBSESAME**
- Empfangsarbeitsplätze (Fat Client)
- Digitales Empfangsterminals

Die Benutzeroberfläche dieser Schnittstellen wurde so konzipiert, dass sie eine klare Struktur und eine beschleunigte Bearbeitung ermöglichen durch:

- Zugriff auf funktionsspezifische Registerkarten, gefiltert nach Operatorrechten, mit voreingestellten oder verbindlichen Standardwerten
- Besuchererfassung und -suche mit Autovervollständigung.
- Fotoaufnahme direkt über Webcam, Tablet oder Smartphone.

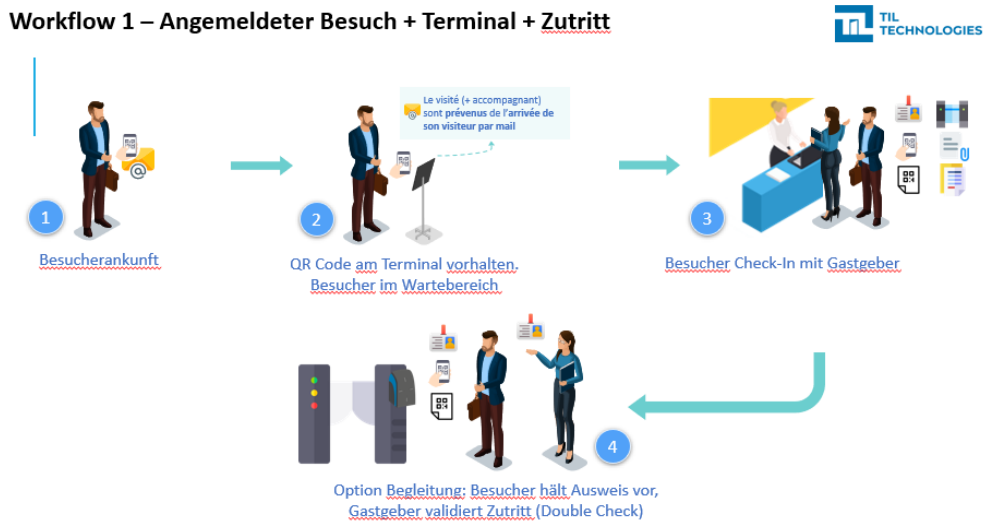
Die WEBSESAME-Oberfläche ist für alle autorisierten Benutzer über ihre Büro-PCs mit Webbrowser über das Intranet des Unternehmens zugänglich.
Sie erlaubt die Erstellung von Besuchereinträgen, die Terminplanung und/oder -freigabe sowie die Ergänzung aller erforderlichen Informationen (Zeitpläne, Zutrittsprofil, Begleitperson, Besucherdatenblatt usw.)

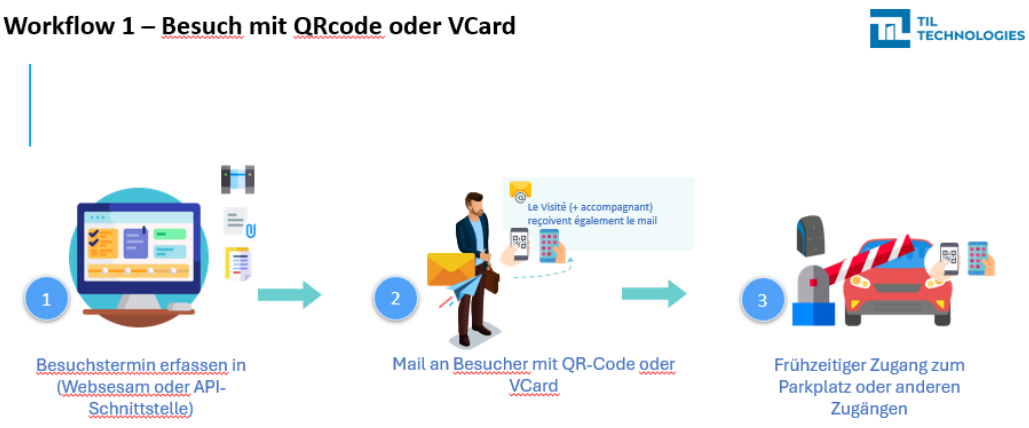
Der Besucherempfang, eingerichtet als Fat-Client-Arbeitsplatz am physischen Eingang des Gebäudes, ermöglicht einen reibungslosen Ablauf und umfassende Vorgänge – von der Ausgabe bis zur Rückgabe der Besucherausweise, der Erfassung unangekündigter Besuche, dem Scannen von Ausweisdokumenten bis hin zum Druck personalisierter Ausweise oder Besucherkarten.
Die „Fat-Client“-Arbeitsplätze müssen über das Netzwerk mit dem MICROSESAME-Anwendungsserver verbunden sein:

- Für den erwarteten Besucher, der seinen per E-Mail erhaltenen QR-Code scannt.
- Für den unangekündigten Besucher, der sein Formular ausfüllt und einen Besuch beantragt.

Ein spezielles Dokument zur Besucherverwaltung ist über Ihren gewohnten Ansprechpartner bei TIL erhältlich.

VEREINFACHTER WORKFLOW DER BESUCHERVERWALTUNG





DETAILIERTER WORKFLOW BEI DER BESUCHERVERWALTUNG

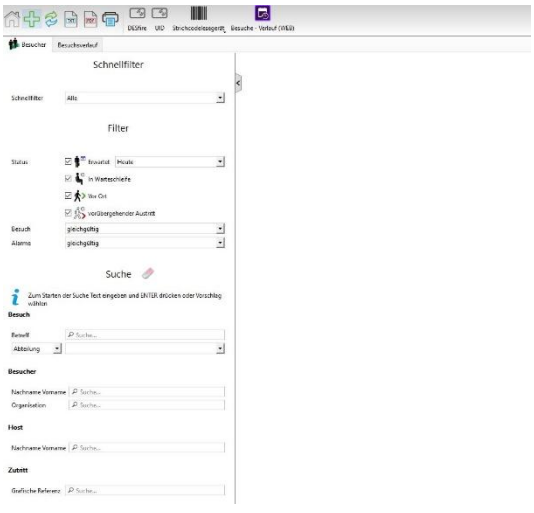
Diese Lösung bietet folgende Vorteile:

- Besucher über einen vollständigen und in die Zutrittsverwaltung integrierten Workflow verwalten.
- Den Empfang und Zugang von Besuchern optimieren, vereinfachen und absichern.
- Freie oder begleitete/eskortierte Besuche ermöglichen – mit Doppel-Ausweiskontrolle.
- Termine anhand kundenspezifischer Kriterien validieren:
  - Automatische E-Mail-Benachrichtigungen mit angehängter ICS-Datei an Besuchte, Besucher und Begleitpersonen – zur Eintragung des Termins in Outlook mit nur einem Klick
- Besuchern frühzeitigen Zugang zu bestimmten Bereichen gewähren (z. B. Parkplätze).
- Besuchsanfragen durch berechtigte Mitarbeitende direkt vom Büro-PC aus erstellen.
- Einhaltung der Anforderungen der ANSSI (Leitfaden für kontaktlose Systeme).
- Zwei Arten des Besucherempfangs anbieten (mit Empfangspersonal und/oder über Terminal) zur Berücksichtigung unterschiedlicher Anforderungen (Sicherheit, Kosten).
- Erstellung personalisierter Besucherausweise nach Kundenvorgaben (Designrichtlinien, Name, Farbcode usw).
- Möglichkeit zur Erstellung unangekündigter Besuchstermine.

WEBSESAME zeigt zwei Symbole zur Besucherverwaltung: „Besucher“ und „Termine“.

DIE BESUCHERVERWALTUNG ermöglicht die Erfassung aller erforderlichen Informationen, um Besucherprofile zu erstellen – je nach Bedarf mit oder ohne Begleitung auf dem Gelände. Die Pflichtfelder, die durch den Nutzer auszufüllen sind, lassen sich durch MICROSESAME-Benutzer konfigurieren. Die Möglichkeiten zur Zutrittsverwaltung sind im Vergleich zur MICROSESAME-Fat-Client-Oberfläche bewusst eingeschränkt – angepasst an die Anforderungen des Empfangs- und Verwaltungspersonals (außerhalb von Sicherheitsdiensten):

- Auswahl aus vordefinierten Besucher-Zutrittsprofilen.
- Vergabe eines freien Besucherausweises aus dem dafür vorgesehenen Pool.
- Parameter wie Gültigkeit, Anti-Passback, Generalschlüssel, Schwarze Liste usw…
- Besucherstatus, der optional nur bestimmten Benutzern angezeigt wird.

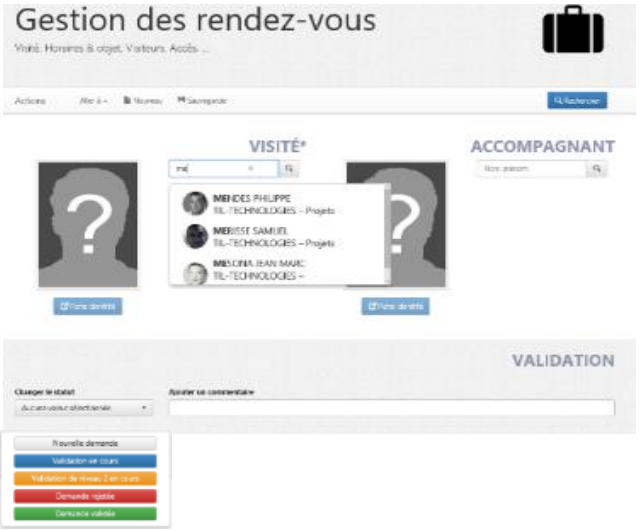


Dies ermöglicht die Vergabe zeitlich begrenzter und gezielter Zugangsrechte

DIE BESUCHERVERWALTUNG ermöglicht die Suche und Erstellung von Besuchsterminen mit:

- der besuchten Person, ausgewählt aus autorisierten Personen mit dem Status „besuchbar“

- Datum, Uhrzeit und ergänzenden Informationen (z. B. Besuchsgrund)
- dem oder den Besuchern, ausgewählt über eine Suchfunktion zur Vermeidung von Dubletten, oder falls nicht vorhanden, direkt neu angelegt über ein vereinfachtes Pop-up-Fenster.
- Zuweisung von Zugangsprofilen aus einer Liste von Profilen, die sowohl für Besucher als auch für den Operator (z. B. bei Multisite-Verwaltung, Klassifizierung) freigegeben sind).
- Angabe des Besuchsortes über ein vordefiniertes Dropdown-Feld – für Multisite-Projekte geeignet, mit E-Mail-Benachrichtigung an die zuständigen Genehmiger der betreffenden Standort.
- Vergabe eines vorgezogenen Zugangs (z. B. vom Parkplatz zum Empfang), über QR-Code-Leser. Ein QR-Code (oder ein PIN-Code) wird dem Besucher des Termins per E-Mail zugesandt.
- Auswahl einer möglichen Begleitperson aus einer Liste zulässiger Begleiter. In diesem Fall erfolgt der Zugang über ein Doppel-Badge-Verfahren: zuerst durch den Besucher, danach innerhalb eines definierten Zeitfensters durch eine beliebige autorisierte Begleitperson – beide müssen gültige Zutrittsprofile besitzen.



- Möglichkeit, spezifische Hinweise oder Anweisungen als Kommentar zu hinterlegen.

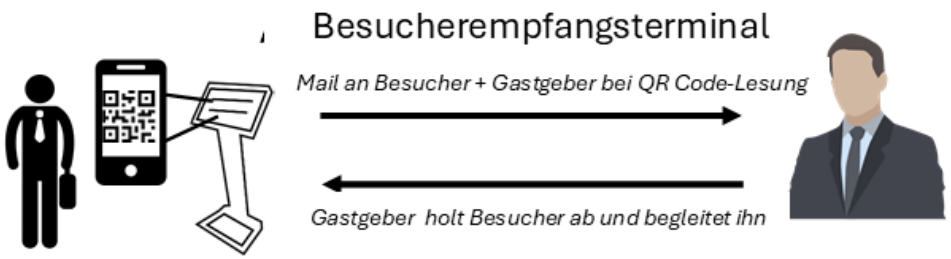
EINE FUNKTION „TERMINVALIDIERUNG“ ist ebenfalls in dieser Oberfläche verfügbar, wenn interne Prozesse des Unternehmens eine Genehmigung durch eine oder zwei weitere Personen (z. B. Sicherheitsbeauftragter, Abteilungsleiter …) vorschreiben:

- Es können bis zu zwei Validierungsstufen verwaltet werden (Operatoren der Stufe 1 & 2).
- Die Validierungskriterien für jeden Termin, die eine automatische Freigabe durch einen oder zwei Benutzer ermöglichen, sind pro Endkunde konfigurierbar. Sie basieren auf Abfragen, die sich auf Daten des Antragstellers (Abteilung, Status …), des Besuchs (Datum, Ort …) oder des Besuchers (Nationalität, Firma …) stützen.
- Personalisierbare E-Mail-Benachrichtigungen können automatisch an alle Beteiligten versendet werden (Besucher, Besuchte, Begleitpersonen, Validierer), um über den Ablauf der Validierung und den Status des Besuchs (z. B. in Prüfung, zu validieren, akzeptiert, abgelehnt …) zu informieren

Nach erfolgter Validierung (automatisch oder manuell durch einen Benutzer) kann der Besuchstermin nicht mehr geändert werden – er kann jedoch dupliziert werden

BESUCHEREMPFANG

AM BESUCHEREMPFANGSTERMINAL:



Touch-Empfangssäule mit integriertem QR-Code-Scanner und zwei Auswahlmöglichkeiten auf dem Startbildschirm:

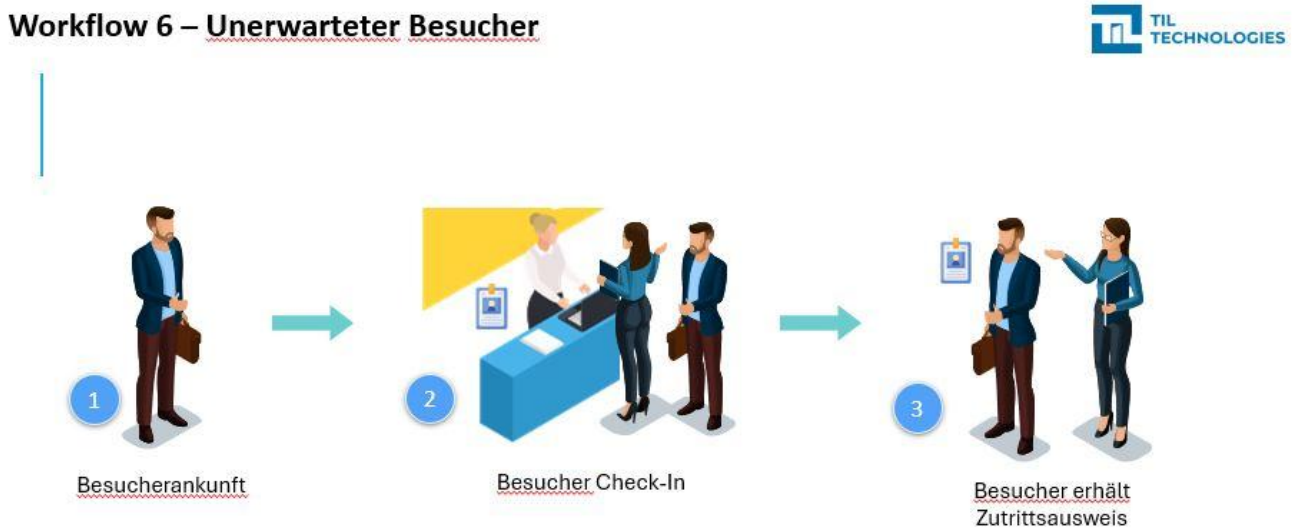
1. Für den erwarteten Besucher, der seinen QR-Code scannt

2. Für den unangekündigten Besucher, der seine Besucheranfrage und sein Profil erstellt

Die spezifischen Vorteile dieser Besuchsempfangslösung über eine Empfangssäule:

- Einfache Besucherabwicklung über einen vereinfachten Workflow.
- Kostenreduktion (Empfangspersonal, Besucherausweise usw.).
- Besucher werden durch die besuchten Personen begleitet – diese verfügen als Einzige über einen Ausweis und ein Zutrittsrecht.
- Lückenlose Nachverfolgung der Besuche und Zutritte über das MICROSESAME-Historienprotokol**.**

EMPFANG DER BESUCHER DURCH EINE EMPFANGSPERSON AM EMPFANGSPLATZ:



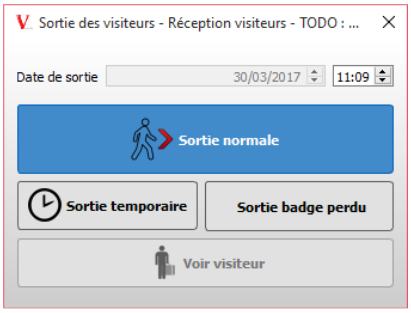
VORTEILE DIESER LÖSUNG :

- ► Zuweisung eines Besucherausweises und Herunterladen der Zutrittsrechte in weniger als 10 Sekunden.
- ► Auflistung und Lokalisierung der anwesenden Besucher auf dem Gelände sowie Anzeige ihres Status (wartend, im Besuch, ausgecheckt usw.)
- ► Lückenlose Nachverfolgung aller Besuche und Bewegungen der Besucher im MICROSESAME-Historienprotokoll**.**
- ► Verschiedene Arten der Besucherabmeldung möglich.

VORTEILE FÜR DAS EMPFANGSPERSONAL:

- Schneller Empfang und einfache Suche nach Besuchern:
  - • Suche nach Name des Besuchten oder des Besuchers
  - • Scan des per E-Mail erhaltenen QR-Codes des Besuchers über Handscanner
  - • Möglichkeit, unangekündigte Besuche ohne vorherige Terminvereinbarung zu erfassen (sofern erlaubt):
  - – mit Zuweisung von speziell für Besucher vorgesehenen Zugangsprofilen (z. B. Besucherparkplatz)
  - – mit Gültigkeitsdauer (auch über mehrere Tage und für temporäre Abwesenheiten)
  - – mit oder ohne Begleitperson mit entsprechender Berechtigung (Doppelbadge erforderlich)
  - – Anschlussmöglichkeit eines OCR-Lesers zur automatischen Übernahme von Ausweisdaten (Personalausweis, Reisepass) in die Benutzeroberfläche.

- ► Attribution d'un badge visiteur disponible par simple badgeage sur lecteur de table.
- ► Mettre à jour l'état du visiteur : Faire entrer le visiteur ou placer le visiteur en attente (Visiteur enregistré mais en attente dans l'accueil visiteur du site).
- ► Mehrere anpassbare Dokumente können für eintreffende Besucher erstellt und ausgedruckt werden (Besucherkarte, Besucherschein, Lageplan, Fahrzeugpassierschein – jeweils mit Besuchsgrund und Gastgeber) auf Karton-Badges oder Plastikkarten.
- ► Schnittstellen zu Drittanwendungen (z. B. für Meetings, Schulungen etc.) für Besucher sind möglich.
- ► Besucher auschecken und Besuch beenden. Nach dem Besuch muss der Besucher als ausgecheckt erfasst werden. Es sind mehrere Arten des Auscheckens möglich:
  - Normales Auschecken: Beendigung des aktuellen Besuchs. Der Besucher wird aus der Liste der registrierten Besucher entfernt. Der Besucherausweis wird wieder freigegeben und ist erneut für andere Personen verwendbar.
  - Temporäres Auschecken: Sobald der Besucher das Gelände vorübergehend verlassen hat, werden seine Zutrittsrechte deaktiviert. Bei seiner Rückkehr muss er erneut registriert werden.
  - Auschecken bei verlorenem Ausweis: Der Besucher beendet seinen Besuch auf dem Gelände, gibt jedoch den Ausweis nicht zurück (oder dieser ist beschädigt). Der laufende Besuch wird beendet, der Besucher aus der Liste der registrierten Besucher entfernt. Der nicht zurückgegebene Ausweis kann nicht erneut vergeben werden.



Lesegeräte mit automatischer Auscheck-Funktion (Leser mit Einzugsvorrichtung) sind erhältlich und ermöglichen, dass der Besucher danach nicht mehr zur Rezeption zurückkehren muss.

Anzeige der Besucherübersicht mit verschiedenen Status:

- Erwartete Besucher: Der Besucher ist vorregistriert, hat sich aber noch nicht an der Rezeption gemeldet.
- Besucher in Warteschleife.
- Eingetretene Besucher: Der Besucher ist registriert und hat das Gelände betreten und es noch nicht wieder verlassen.
- Ausgecheckte Besucher.
- Abgelaufene Besuche: Wenn die geplante Besuchszeit überschritten ist und der Besucher das Gelände nicht verlassen hat, erscheint eine Warnmeldung und ein Symbol weist auf die Überschreitung hin.

► Erstellung von Besuchshistorien oder Besucherlisten (erwartet, in Warteschleife, temporär ausgecheckt etc.) zur Ausgabe über Drucker oder als exportierbare Excel-kompatible Dateien.

► Mögliche Synchronisation mit Outlook-Kalendern über eine ICalendar-Datei (ICS), die den beteiligten Personen per E-Mail zugesendet wird.

► Löschung von Besucherdaten möglich, wenn Besucher nicht zum vereinbarten Termin erscheinen.

11. OSS OFFLINE-ZUTRITTSPUNKTE

VERWALTUNG DIGITALER ZYLINDER UND BESCHLÄGE MIT OSS STANDARD OFFLINE

MICROSESAME verwaltet nativ die Logik der Offline-Zutrittsrechtevergabe, also auf autonomen digitalen Schlössern (Zylinder, Beschläge, Türgriffe usw.), die nicht in Echtzeit mit dem System verbunden sind.
In diesem Konzept werden die Zutrittsrechte direkt auf den Benutzerausweis codiert – mit einer konfigurierbaren Gültigkeitsdauer (vorzugsweise kurz, Bsp. 24 Stunden**)**.

Die digitalen Schlösser verfügen über eine integrierte Intelligenz und speichern Daten wie z. B. Zutrittsgruppen und Uhrzeit. Sie entriegeln sich, sobald die auf dem Badge gespeicherten Zutrittsrechte von der Schlosslogik erkannt und validiert werden.
.

Der regelmäßige Refresh der Zutrittsrechte auf den Benutzerausweis kann auf verschiedene Weise erfolgen:

- Über mit MICROSESAME verbundene Badge-Encoder (PRIME/HIGH SECURE): für die Erstcodierung und das Re-Encodieren der Rechte.
- Über Ladestationen für Zutrittsrechte (alle Baureihen): ebenfalls für Erstcodierung und Re-Encodierung.
- Über kabelgebundene Leser am Standort (alle Baureihen), sofern diese kompatibel sind und an entsprechende MLP2-OSS-Module angeschlossen sind: hier ist nur das zeitverzögerte Nachladen der Rechte möglich

Für den Betreiber erfolgt die Rechtevergabe auf diese nicht-vernetzten Zutrittspunkte völlig transparent über die gewohnte Benutzeroberfläche „Benutzer/ID-Meiden“, über die auch die vernetzten Leser verwaltet werden.
Diese Systemflexibilität macht es überflüssig, zwei Benutzeroberflächen zu bedienen oder Datenbanken miteinander zu synchronisieren. Gleichzeitig profitieren die Offline-Zutrittspunkte – wie auch alle vernetzten Leser – von MICROSESAME-Funktionen wie Multi-Site-Verwaltung und der Zuweisung von Zutrittsprofilen.

Die zentrale Verwaltung digitaler Offline-Komponenten bietet darüber hinaus Vorteile bei der Rückmeldung von Informationen.
Bei jedem Kontakt eines Badges mit einer Rechteladestation (Updater) werden folgende Informationen an MICROSESAME übertragen:

- Die Zutrittshistorie der Ausweise.
- Die Batterie-Warnmeldungen (niedriger Stand).

Der Offline-Standard OSS (Open Security Standards Association) und seine Vorteile

- Entwickelt von einem Zusammenschluss führender Hersteller mechatronischer Systeme, darunter:
  - ASSA ABLOY, DEISTER, UZ, DORMA KABA, Zugang GmbH...
- Die auf den Badges gespeicherten Daten (z. B. Zutrittsrechte) folgen einem gemeinsamen Format für alle Hersteller, die den Offline-Standard OSS einhalten
- OSS-kompatible Schlösser verschiedener Marken können die auf den Badges gespeicherten Rechte und Daten auf identische Weise auslesen. Der Endkunde ist somit frei in der Wahl des Herstellers.

12. CLIQ OFFLINE-ZUTRITTSPUNKTE

VERWALTUNG VON ZYLINDERN UND ELEKTRONISCHEN SCHLÜSSELN

MICROSESAME verfügt über einen nativen Konnektor zur Anbindung an die elektronische Schließtechnologie CLIQ von ASSA ABLOY.

Bei diesem „Offline“-Zutrittskontrollsystem werden die Benutzerrechte in einem „aktiven“ Schlüssel gespeichert. Im Gegensatz zu Offline-OSS-Lösungen benötigen die CLIQ-Schließzylinder, in die diese Schlüssel eingeführt werden, weder Stromversorgung noch Batterie – die Energie für die Prüfung der Berechtigungen und das Öffnen des Zylinders oder Vorhängeschlosses liefert ausschließlich der Schlüssel selbst.

Wie bei jedem Offline-System ist eine regelmäßige Aktualisierung der gespeicherten Rechte auf dem Schlüssel erforderlich:

- Entweder über eine CLIQ-Ladestation.
- Oder über das Smartphone mittels der mobilen App **CLIQ CONNECT**.

Die Integration in MICROSESAME ist einfach: Die Konfiguration ist in nur fünf Minuten abgeschlossen, da Schlüssel, Zylinder und Ladestationen direkt aus dem CLIQ WEB MANAGER importiert werden können:

- CLIQ-Schlüssel werden in MICROSESAME als ID-Medien importiert.
- Die Zylinder und Zylindergruppen werden als zuweisbare Zutrittselemente übernommen.
- Die Rechtevergabe zu diesen Zylindern/Zylindergruppen erfolgt genau wie bei herkömmlichen Lesern – über die MICROSESAME- und WEBSAME-Oberflächen „Benutzer“ und „Zutrittsprofile“.
- Die Ladestation (Updater) wird als überwachbares Element geführt: Ein „Überwachungsobjekt“ steht zur Verfügung, inklusive Status- und Fehlermeldungen.

13. AUSWEISCODIERUNG

ELEKTRISCHE PERSONALISIERUNG

Die elektrische Personalisierung von Badges oder Zutrittsausweisen (MS-ENCODBADGE) ist eine Softwareoption von MICROSESAME, mit der Daten in Badges der MIFARE-Familie geschrieben werden können.
Die Software unterstützt das Encodieren der meisten Formate wie MIFARE Classic sowie MIFARE Desfire EV1/EV2/EV3, wobei unter anderem der Speicherort (z. B. Sektor bei MIFARE Classic oder Applikationen und Dateien bei MIFARE Desfire) sowie das Format der Identifikatoren (dezimal, hexadezimal, alphanumerisch etc.) definiert werden können.

Mehrere Anwendungen mit jeweils eigenen Identifikatoren können in einem einzigen Vorgang auf den Badge geschrieben werden.
Der Identifikator kann entweder direkt von MICROSESAME generiert oder von einer Drittanwendung bereitgestellt werden.

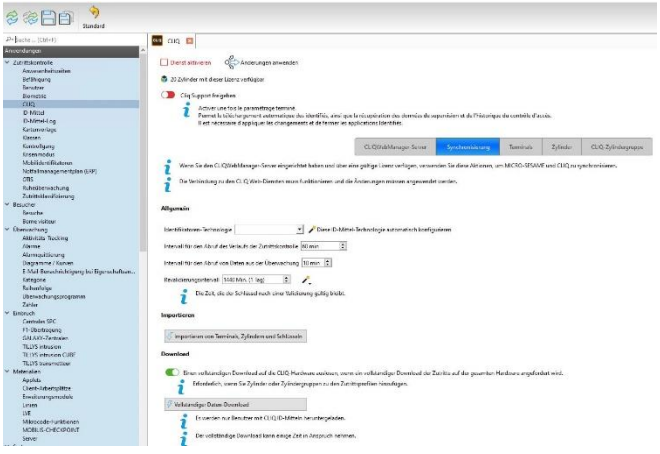
Die physische Codierung kann entweder einzeln oder im Batchverfahren erfolgen – entweder über einen Tisch-Encoder oder direkt über einen Zutrittskartendrucker mit integriertem Encoder.
In letzterem Fall ist es möglich, eine ganze Personengruppe automatisch und gleichzeitig zu personalisieren

- Die grafische Darstellung der Zutrittskarte
- Die Multi-Anwendungs-Encodierung
- Die Zuweisung jedes Badges zur zugehörigen Person (Enrolment)

Diese Lösung bietet Schnelligkeit, Einfachheit und Sicherheit

VERWALTUNG DER BADGE-SCHLÜSSEL MIT KSM

MICROSESAME unterstützt die Verwaltung von Schlüsseln (Keys) für MIFARE-Badges über ein **Key Secure Management (KSM)**-System. Damit wird gewährleistet, dass alle kryptographischen Elemente zentral und sicher verwaltet, gespeichert und verwendet werden.
Dies erhöht die Sicherheit beim Einsatz von MIFARE Desfire EV1/EV2/EV3 und stellt die Integrität der Off- und Online-Zutrittskontrolle sicher:



- Konfiguration der Schlüssel (abhängig von den Formaten und Schlüsselt-Typen) für die Badges.
- Erzeugung der Schlüssel und zugehöriger Sicherungsdateien
- Erstellung der Datei, die für MS-ENCODBADGE benötigt wird, um das physische Encodieren bzw. Registrierung des Ausweise über einen transparenten Leser an einem MICROSESAME-Client-PC

14. AUSWEISPERSONALISIERUNG

Die Personalisierung von Badges ist eine integrierte Standardfunktion von MICROSESAME. Sie ermöglicht die grafische Gestaltung (z. B. personalisierter Text aus den Personendaten, statischer Text, Logo, Foto, Piktogramme, QR-Code etc.) sowie den Thermodruck.

Für jede Person kann ein Bild gespeichert werden – entweder aus einer bestehenden Datei, über einen Scanner, eine Videokamera oder eine beliebige Webcam.

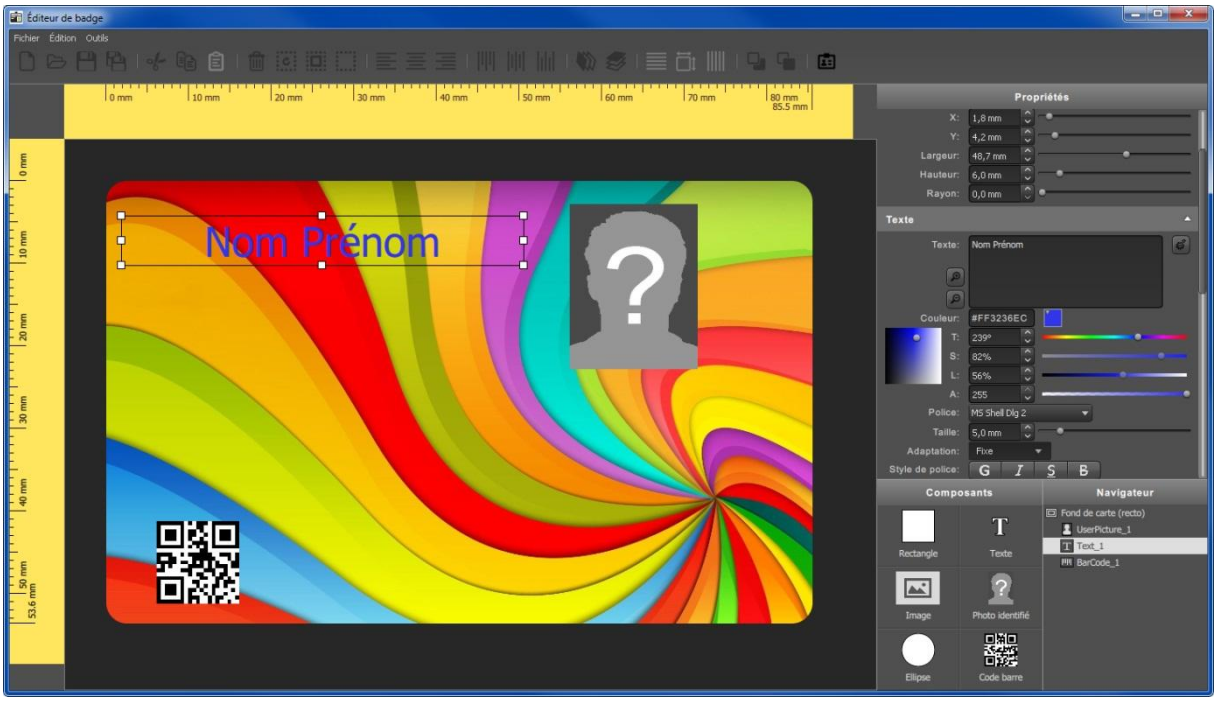
Der grafische Editor von MICROSESAME erlaubt die Gestaltung von Kartenlayouts, einseitig oder zweiseitig, und die Konfiguration der zu druckenden Inhalte (z. B. Name, Abteilung, Berechtigung...). Dabei können sämtliche internationale Schriftsysteme verwendet werden, einschließlich arabischer Zeichen.

Beispielsweise lassen sich Piktogramme ergänzen, die spezielle Berechtigungen des Karteninhabers darstellen (z. B. Elektrobefähigung, explosionsgefährdete Bereiche, spezielle Genehmigungen...).

Der Badge-Layout-Editor erlaubt auch den Export bereits erstellter Layouts, sodass diese auf anderen Standorten desselben Kunden wiederverwendet werden können.

Die Lösung bietet die Möglichkeit, mehrere Kartenlayouts zu definieren (z. B. dauerhaft, temporär, Besucher...) – jeweils mit unterschiedlichen Eigenschaften. Vor dem Seriendruck kann für jede Person das passende Layout ausgewählt werden.

.



15. MONITORING & ÜBERWACHUNG

EREIGNISMONITORING IN ECHTZEIT, GRAFISCHE ÜBERSICHT, ZONENÜBERWACHUNG

MICROSESAME ermöglicht die Überwachung von Ereignissen, Alarmen und Störungen im Zusammenhang mit der Zutrittskontrolle, Einbruchmeldetechnik, Systemstatus sowie technischen Anlagen – und das Auslösen zugehöriger Aktionen (z. B. Quittierung, Steuerbefehle, Video-Streams aufrufen…) über folgende Funktionen:

- Übersichtsanimation
- Echtzeit-Ereignisticker
- Zonenüberwachung
- Zonen mit Zählfunktion

ALLGMEINEN ERGONOMIE

- Die Benutzeroberflächen (HMI) sind so konzipiert, dass sie eine einfache und schnelle Bedienung ermöglichen, mit folgenden Merkmalen:
  - Eine einheitliche Oberfläche zur Verwaltung aller Sicherheitsfunktionen
  - Der Operator sieht nur die Funktionen und Daten, für die er berechtigt ist
  - Mehrsprachige Benutzeroberflächen
  - Jede Oberfläche ist spezifisch für bestimmte Funktionen vorgesehen (z. B. Benutzer, Monitoring, Synoptik…)
  - Webzugriff für Funktionen, die von einer großen Nutzergruppe verwendet werden (z. B. Terminvereinbarung)
  - Klare visuelle Trennung der Anwendungsbereiche durch Navigation und Farbschema: **Benutzung** – **Einstellungen** – **Wartung**
  - Un champ de recherche du Menu permet de retrouver facilement les fonctions disponibles

  Affichage de l'opérateur connecté sur la barre du haut

- Favoriten, Schnellzugriffe und Liste zuletzt geöffneter Anwendungen im Hauptmenü für den schnellen Zugriff auf häufig verwendete Funktionen

- Autovervollständigungsfunktion, die dem Benutzer Eingabevorschläge macht, um die Tastatureingabe zu minimieren – basierend auf den bereits eingegebenen Zeichen
- Kohärenzprüfung der eingegebenen Daten entsprechend dem jeweiligen Eingabefeld
- Benachrichtigung von Bedienern bei Eingabefehlern oder fehlenden Angaben
- Anpassung der meisten Spalten in Ergebnisformularen möglich:
  - Auswahl der anzuzeigenden Felder und Daten
  - Speichern der Spaltenpositionen
  - Flexible Änderung durch den Anwender jederzeit

INTERAKTIVER EREIGNIS- UND ALARMMONITOR

Der interaktive Ereignismonitor zentralisiert die Überwachung aller von MICROSESAME empfangenen Ereignisse, Alarme und Störungen. Er zeigt diese fortlaufend in Echtzeit an und ermöglicht die Quittierung von Alarmen, das Ausführen von Aktionen und Fernsteuerbefehlen sowie das Erzwingen von Eigenschaftszuständen.

Jeder Bediener sieht nur die Standorte, Ereigniskategorien usw., für die er autorisiert ist. In jedem Fall werden alle Ereignisse – Auftreten, Quittierung und Löschung von Alarmen – mit Zeitstempel versehen und in der Datenbank archiviert, sodass sie später eingesehen werden können (siehe Kapitel Historie & Bediener.

EREIGNISMONITOR

EREIGNISMONITOR

Der Reiter **Ereignismonitor** zeigt in Echtzeit alle Ereignisse chronologisch an, basierend auf einer dynamischen Filterung.
Es ist möglich, das automatische Scrollen der Ereignisliste zu deaktivieren, um dem Benutzer Zeit zu geben, die vor oder nach einem bestimmten Ereignis aufgetretenen Einträge in Ruhe zu betrachten.

Unabhängig von der Anzahl der erfassten Ereignisse kann die Liste jederzeit dynamisch gefiltert werden, z. B. nach:

- Standort (bei Multi-Site-Verwaltung)
- Ereignistyp (erlaubter oder verweigerter Zutritt, Alarme, Fernsteuerungen, Systemereignisse, letzter Zutritt einer identifizierten Person)
- Stichwort in der Schnellsuche (z. B. Name)

DETAILS

Bei Auswahl eines Ereignisses im Reiter „Fil de l'eau" zeigt der Bereich **„Details"** zusätzliche Informationen zum jeweiligen Ereignis sowie die verfügbaren zugehörigen Aktionen:

- Alarm quittieren: Das Quittieren einer Alarmmeldung stellt sicher, dass der Operator sie zur Kenntnis genommen hat. Ob eine Quittierung erforderlich ist, kann je nach Alarmtyp individuell festgelegt werden.
  - Einzeln oder mehrfach quittierbar – je nach Alarmkategorie (z. B. CA, AI ...) und den konfigurierten Quittierungsstufen („Maske"). Eine Alarmmeldung kann z. B. von mehreren berechtigten Operatoren bestätigt werden müssen.
    - Optional kann ein Blinken der zu quittierenden Alarme aktiviert werden.
- Anzeigen einer Anweisung oder Handlungsanleitung,
- Livebild einer zugeordneten Kamera anzeigen
- Videoaufzeichnung eines Alarms oder Badge-Durchgangs wiedergeben
- Den mit dem Alarm verknüpften Gebäudeplan anzeigen
- Bei einem Badge-Durchgang direkt auf die Personendaten zugreifen, z. B. um eine temporäre Entsperrung bei Anti-Passback/Anti-Retour-Alarmen durchzuführen
- Bei einer Zustandsänderung: aktuellen Zustand einsehen, Zustand erzwingen oder eine Fernsteuerung auslösen...
- Anzeigen des Fotos, das mit dem letzten Badge-Durchgang verknüpft ist
- Öffnen einer Notizfunktion (frei oder ereignisbezogen)

Man kann Alarme anhand eines Schweregrads von 0 (am wenigsten kritisch) bis 512 (am kritischsten) unterscheiden:

- Roter Hintergrund mit weißem Text: aktiver, nicht quittierter Alarm (Standardfarbe, anpassbar). Diese quittierungspflichtigen Alarme können je nach Schweregrad 0 individuell unterschieden werden durch:
  • Frei wählbare Text- und Hintergrundfarben
  • Akustische Signale oder Sprachausgabe (Windows-Sprachausgabe, Audiodateien)
- Weißer Hintergrund mit schwarzem Text: aktiver, nicht quittierbarer Alarm
- Weißer Hintergrund mit rotem Text: quittierter, aber weiterhin aktiver Alarm

REITER ALARME

- Gibt eine vollständige Übersicht über alle aktiven oder noch nicht quittierten Alarme. Bereits quittierte und nicht mehr aktive Alarme verschwinden automatisch.

  Die Alarme sind standardmäßig nach Schweregrad sortiert. Die meisten im „Energiemonitor“ verfügbaren Aktionen zu Alarmen sind auch in dieser Ansicht verfügbar, zusätzlich:
- Anzeigen des Kurvenfensters zur Alarmhistorie (siehe Kapitel Grafik / Kurve)
- Schneller Zugriff auf die Konfiguration einer mit dem Alarm verknüpften Eigenschaft

REITER EIGENSCHAFTEN:

Ermöglicht die Überwachung und Suche nach verschiedenen Eigenschaftstypen, die Anzeige ihrer Zustände (z. B. Benachrichtigung bei geöffneter Tür), deren Bearbeitung und Interaktion.
Ein Objekt stellt ein am Standort installiertes Element dar, das Informationen liefert (z. B. eine Tür). Überwachungseigenschaften sind die verschiedenen Zustände und Fernsteuerungen, die zu einem Objekt gehören (z. B. bei einer Tür: Taster, Haftmagnet, Türkontakt, Einbruch, Öffnungsbefehl) und die in MICROSESAME gesteuert werden können.
Diese Ansicht ist sowohl für den Betreiber als auch für den Errichter bei der Einrichtung eines Standorts nützlich, da sie die Diagnose der Installation ermöglicht (z. B. Fernbefehl auslösen, Zustand prüfen, weiteren Befehl senden, Übersicht öffnen...).

Die möglichen Aktionen auf diese Eigenschaften, je nach Typ, sind:

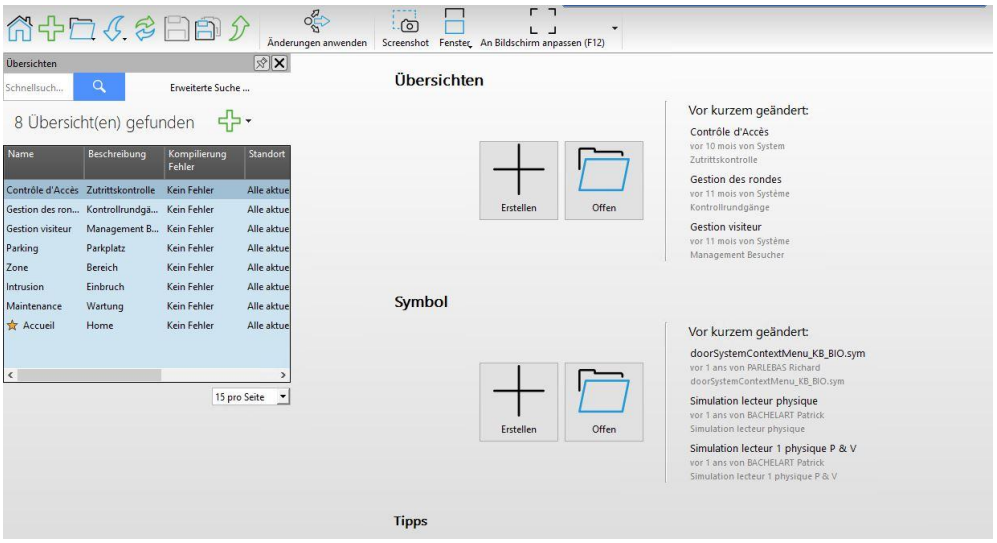
- Erzwingen: Ermöglicht das Deaktivieren von Eigenschaften, z. B. vorübergehend im Fall von Wartungsarbeiten oder einem defekten Detektor...,
- Befehl oder Impuls senden,
- Zugehörige Kurve anzeigen
- Zugehörige Übersichtsplan anzeigen
- Eigenschaft bearbeiten

Eigenschaften können mit unterschiedlichen Farben angezeigt werden:
Gelber Hintergrund mit braunem Text, wenn der Zustand einer Eigenschaft erzwungen wurde.

ANIMATION GRAFISCHER ÜBERSICHTSPLÄNE

Die Übersichtsanimation von MICROSESAME ermöglicht die individuelle Anpassung der Mensch-Maschine-Oberfläche je nach Standort für Überwachungsfunktionen (Anzeige von Alarmen, logischen Zuständen und numerischen Werten) sowie für eine schnelle Reaktion der Bediener (Alarmbearbeitung gemäß Anweisungen, Auslösen von Fernsteuerungen und Aktionen).

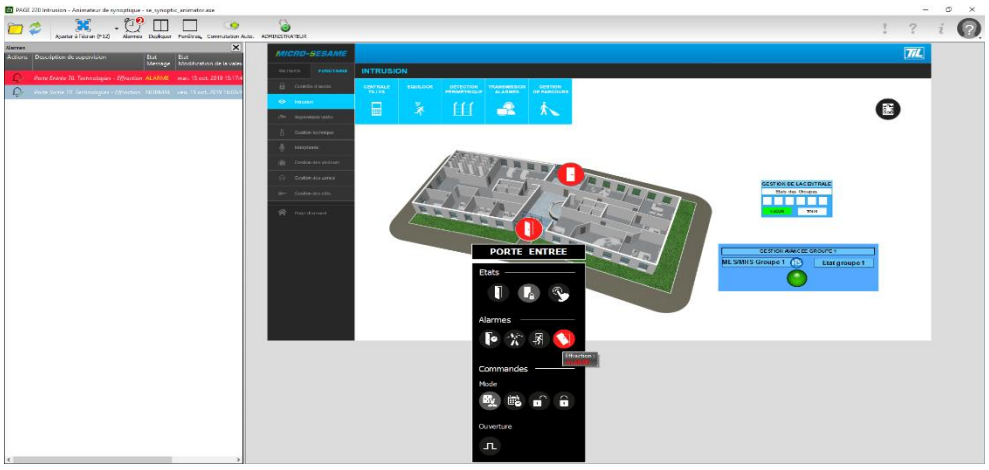
Ein Übersichtsplan ist eine grafische Darstellung der zu überwachenden Anlage und besteht aus einer Sammlung grafischer Objekte auf einem Hintergrundplan.



Die mit den Plänen verbundenen Funktionen umfassen insbesondere:

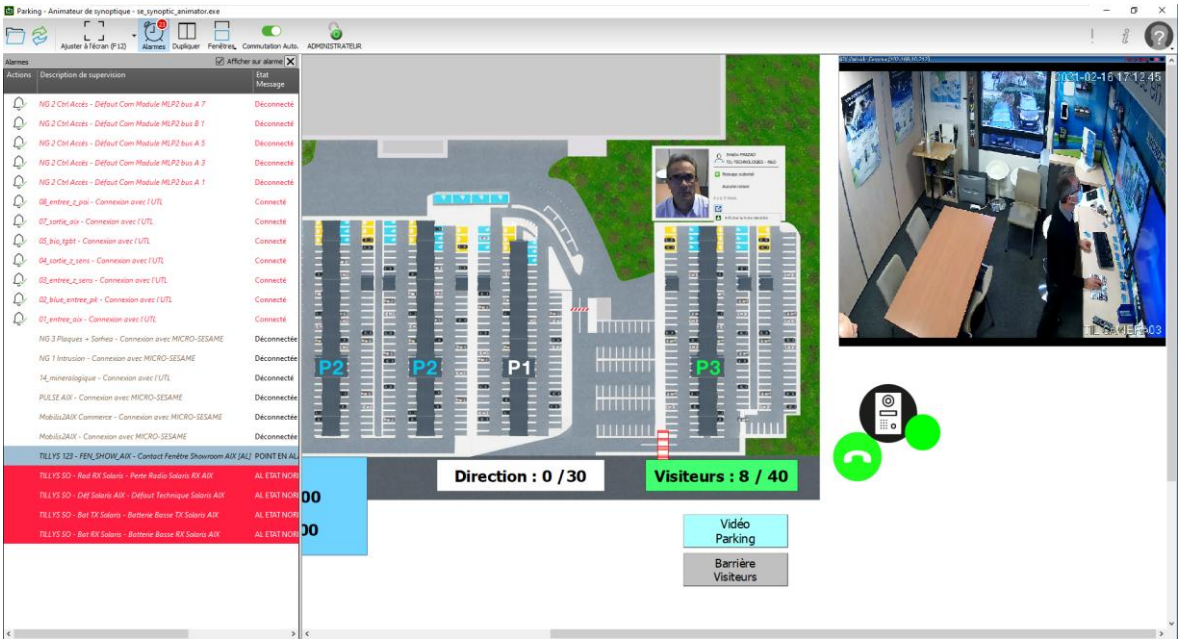
INTEGRIERTER SYNOPTIK-EDITOR UND -ANIMATOR, SCHNELL KONFIGURIERBAR UND HOCHGRADIG ANPASSBAR DANK:

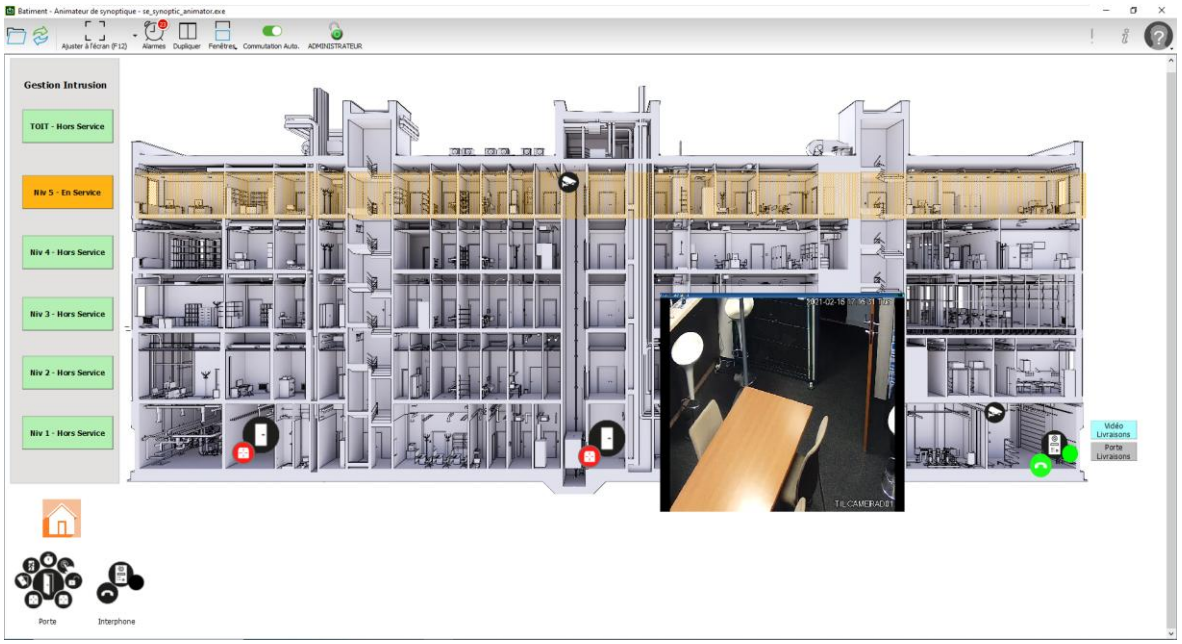
- Der Objektlogik mit zugehörigen Eigenschaften (Informationen, Zustände, Steuerbefehle)
- Einer Bibliothek mit vordefinierten Objektvorlagen, die mit MICROSESAME ausgeliefert wird (UTL, Tür, MAXIRIS usw.) und sowohl fachliche als auch überwachungstechnische Konfigurationen integriert:
    - Einfache, schnelle Konfiguration durch Drag & Drop eines Objekts aus der Vorlage
    - Automatische Zuweisung von Automatisierungen, Ein- und Ausgängen gemäß Standardschaltplan – Auswahlmöglichkeiten per einfachem Klick
    - Möglichkeit, das Bild des Objekts zu ändern, ohne die hinterlegte Konfiguration zu verlieren
    - Beispiel Objekt „Standardtür“: Auswahl aktivierbarer Eingänge wie Türstellungskontakt, Steuerbefehl, BBG-Kontakt oder Verriegelungskontakt
- Möglichkeit zur Erstellung, zum Import und Kopieren projektbezogener, benutzerdefinierter Objekte/Eigenschaften
- Unterstützung des .SVG-Formats zur einfachen Übernahme und Weitergabe von Bauplänen,



- Objekte je nach Gerätezustand animieren (Farbe, Blinken, Sprachausgabe usw.
- Fernsteuerungen und verschiedene Aktionen direkt über Objekte oder Schaltflächen durch den Operator auslösen
- Mit dem Grafikfenster zwischen mehreren, baumartig aufgebauten Gebäudeplänen navigieren (z. B. Gesamtübersicht des Standorts → Klick für Zoom auf Gebäude → Ansicht pro Etage usw.)
- Zoomfunktionen innerhalb eines Plans (Vergrößern/Verkleinern)
- Schnelles Anpassen des Plans an die Bildschirmgröße oder Umschalten in den Vollbildmodus über zwei Tastenkombinationen
- Alarme direkt aus den Grafiken heraus verwalten und überwachen dank:

- Möglichkeit, Alarme direkt aus dem Übersichtsplan heraus zu quittieren
- Öffnen der Eigenschaften eines Objekts
- Anzeigen der zugehörigen Kurvendiagramme
- Abtrennbares Alarmfenster mit Widget/Anzeigezähler und Alarmliste (wie im Ereignismonitor), mit farblicher Darstellung je nach Zustand und Quittierung
- Beispiel: Widgets und Objekte (z. B. Tür, Gegensprechanlage, Kamera…) mit Foto und Echtzeitinformationen zur Person, die gerade ihren Ausweis verwendet…
-





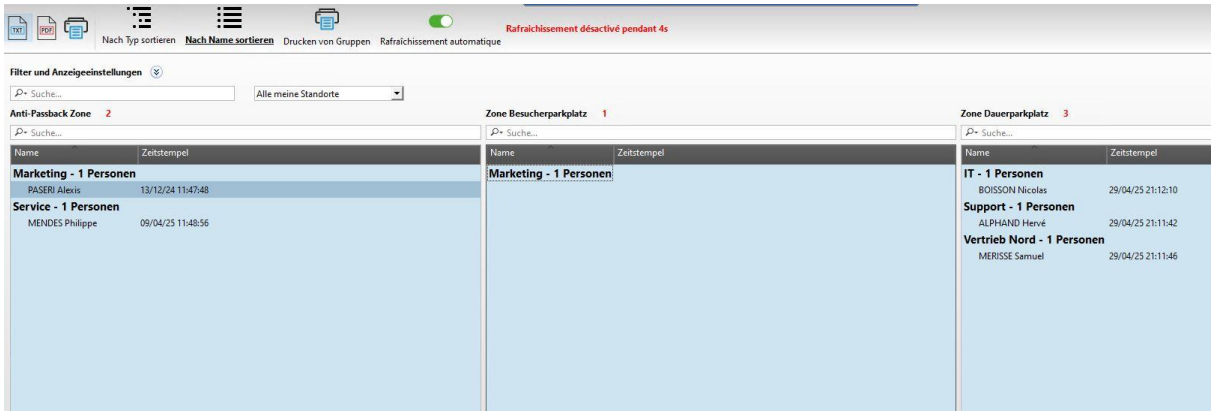
BEREICHS-/ZONENÜBERWACHUNG

EINE ZONE IST EIN GESCHLOSSENER BEREICH (BÜRO, ETAGE, GEBÄUDE), DER BESTIMMTEN REGELN UNTERLIEGT:

- Sie muss über eine Gruppe von Lesern für den Eingang verfügen
- Sie muss über eine Gruppe von Lesern für den Ausgang verfügen
- Ihre physische Abgeschlossenheit (z. B. durch Wände) gewährleistet die korrekte Funktion, da ein Betreten oder Verlassen der Zone nur kontrolliert möglich ist
- Eine Mechanik zur **Einmaligkeit des Zutritts** ist erforderlich, um eine zuverlässige Zählung zu gewährleisten

ES GIBT VERSCHIEDENE ZONENARTEN MIT IHRER JEWEILS SPEZIFISCHEN VERWALTUNG:

- Zählung / Abzählung der anwesenden Identifizierten basierend auf Ein- und Ausgängen
- Anti-Passback (standort- oder zeitabhängig)
- Evakuierungsplan
- Weitere Zonentypen (z. B. zur Verwaltung spezieller Identifizierter wie Personen auf einer Blacklist))



DIE ÜBERWACHUNG DER ZONEN ÜBER IHR DEDIZIERTES FENSTER ERMÖGLICHT:

- Echtzeit-Anzeige der Liste und Zählung der Personen pro Zone und Zonentyp
- Drucken und Exportieren dieser Listen im TXT- und PDF-Format
- Angebot verschiedener Anzeigeoptionen und Filtermöglichkeiten

16. VIDEO-ÜBERWACHUNG

VISIOSESAME

Die Softwarefunktion **VISIOSESAME** von **MICROSESAME CUBE** ermöglicht:

- Zweirichtungs-Kommunikation mit zahlreichen VMS-Softwarelösungen und Video-Rekordern wie **MILESTONE**, **GEUTEBRUCK**, **GENETEC** – über integrierte und optionale Konnektoren in MICROSESAME CUBE
- Zentrale Steuerung aller Sicherheitsfunktionen über eine einheitliche Überwachungsplattform für sämtliche Systeme im Gebäude (Zutrittskontrolle, Einbruchmeldung, Brandmeldung, Gebäudetechnik)
- Durchführung der wichtigsten Videoüberwachungsfunktionen von jedem MICROSESAME-CUBE-Client-Arbeitsplatz aus – mit einem oder mehreren VMS gleichzeitig:
  - Livebildanzeige
  - Starten von Aufzeichnungen
  - Empfangen und Auslösen von Ereignissen & Alarmen
  - Abruf von gespeicherten Aufnahmen
  - Steuerung von Dome-Kameras

Die Integration der Videoüberwachung in MICROSESAME CUBE erleichtert die Bedienung für den Nutzer erheblich. Da die Interaktionen zwischen Videosystem und den anderen Sicherheitsanwendungen vollständig automatisiert werden können (z. B. Aktionen bei Alarmen oder Ereignissen), sind Schnelligkeit und Effizienz der Abläufe gewährleistet. Für den optimalen Betrieb sollte der Client-Arbeitsplatz mit zwei Bildschirmen ausgestattet sein

Beispiel für einen typischen Datenfluss zwischen dem VMS und MICROSESAME:

- Die Überwachungskamera erkennt aufzuzeichnende Bilder
- Der digitale Rekorder speichert die erkannten Bilder
- Der VISIOSESAME-Client greift direkt auf Livebilder oder aufgezeichnete Bilder vom Rekorder zu, ohne über den MICROSESAME-Server zu gehen, abhängig von der Konfiguration des Servers, auf den der Client zugreift
- Die Videobilder werden nicht auf dem MICROSESAME-Server oder -Client gespeichert, sondern ausschließlich auf den Rekordern der VMS

VISIOSESAME-FUNKTIONEN SIND:

EMPFANG UND SENDEN VON EREIGNISSEN, MIT MEHREREN VMS GLEICHZEITIG:

- MICROSESAME → VMS: Start/Stopp der Aufzeichnung, Steuerung des Domes mit Auswahl von Presets und Zoom...
- VMS → MICROSESAME: Detektionsalarm, Kamerafehler, Aufzeichnungsfehler, Rekorder verbunden, Kamera verbunden...

MINIMALER ZEITAUFWAND BEI PARAMETRIERUNG

- Die integrierten und optionalen Konnektoren in MICROSESAME CUBE verwenden die SDKs der VMS sowie native TIL-Objekte/-Eigenschaften für eine schnelle und einfache Konfiguration
- Das Objekt „Kamera“ im Synoptik-Editor
- Der Import der Kamerabezeichnungen aus den VMS

ÜBERWACHUNG DER BETRIEBSALARMEN (Erkennung von Aktivitäten per Video) und Betriebsalarme (Verlust von Videosignalen oder andere Störungen) von den Rekordern über den Ereignismonitor, die Alarmleiste – in Echtzeit wie alle anderen auch

EIN FENSTER FÜR DIE HARDWARE-ARCHITEKTUR kann bei Bedarf angezeigt werden

STEUERUNG DER KAMERAS (Zoom, Auswahl einer vordefinierten Kameraposition – über ein dediziertes Fenster)

VOLLSTÄNDIG ANPASSBARE KAMERA-VISUALISIERUNGSZONE gemäß vordefinierter Szenarien, die einen oder mehrere Monitore in verschiedenen Positionen und Größen (3 x 3, 2 x 2 usw.) anordnen. Es können beliebig viele Monitore entsprechend der Anzahl der Quellen hinzugefügt werden. Die Farben der Titelleiste des Monitors geben Auskunft über dessen Inhalt und Zustand.

ANZEIGE VON LIVE-VIDEOFLÜSSEN mehrerer VMS-Systeme gleichzeitig, über die Auswahl von Symbolen auf Grafikübersichten oder über Alarme

AUTOMATISCHES AUSLÖSEN VON AUFNAHMEN, das durch ein Ereignis (z. B. das Vorzeigen einer Zutrittskarte an einem bestimmten Leser), durch einen Alarm, durch eine komplexe Steuerung, durch eine manuelle Bedieneraktion auf grafischen Schnittstelle (durch Klicken auf einen Button oder ein grafisches Objekt) oder über den Ereignismonitor ausgelöst werden kann

STEUERUNG DER VIDEOWAND (Matrixfunktion), die es ermöglicht, eine Videowand aus mehreren Bildschirmen zu verwalten und eine Kamera in einem bestimmten Bereich (einer sogenannten „Kachel“) anzuzeigen

DIE ANIMIERTE GRAFIKSCHNITTSTELLE ermöglicht es, durch einfaches Klicken auf ein Objekt:

- Die Live-Anzeige einer oder mehrerer Kameras zu starten
- Eine aufgezeichnete Sequenz einer bestimmten Quelle anzusehen
- Automatisch vordefinierte Anzeigeeinstellungen zuzuordnen (Auswahl einer Monitorgruppe, der gewählten Voreinstellung, der Videoquelle unter anderem.

VERKNÜPFUNG EINER VIDEOAKTION mit einem Ereignis oder einer Fernbedienung durch den Bediener. Zum Beispiel: automatische Vorausrichtung einer Dome-Kamera bei der Erkennung eines nicht zugelassenen Ausweises.

WIEDERGABE AUFGEZEICHNETER VIDEOSEQUENZEN, die mit einem Alarm verknüpft sind, direkt über die Funktion „Verlauf“ von MICROSESAME. Diese gewährleistet die Synchronisation der Informationen (ein gemeinsames Protokolldokument für Zutrittskontrolle, Einbruchmeldungen und Video) und erleichtert somit erheblich die Suche nach einer Videoaufzeichnung. Es ist nicht erforderlich, die Quelle, den Kameranamen oder die genaue Uhrzeit zu kennen – ein Klick auf das mit dem Alarm verknüpfte Videosymbol genügt und zeigt an, dass eine zugehörige Aufzeichnung existiert

EINE SCHNELLAKTIONSLEISTE, am unteren Bildschirmrand bietet, zusätzlich zu den klassischen Steuerungstasten für Aufzeichnungen (wie bei einem Videorekorder), aktive Direktbefehle je nach Rekorder, wie z. B. einen Screenshot der aktuellen Anzeige erstellen, eine Aufzeichnung starten, Wechsel des Wiedergabemodus (Live-/Aufzeichnungsmodus), einen Monitor freigeben

VMS-SCHNITTSTELLEN ZU MICROSESAME ÜBER KONNEKTOREN

Die Liste der unterstützten Lösungen, kompatiblen Versionen und verfügbaren Funktionen entwickelt sich ständig weiter – mit integrierten Konnektoren und deren nativen TIL-Objekten/-Eigenschaften sowie optionalen, über MICROSESAME angebundenen Gateways. Ein spezieller Leitfaden zu VISIOSESAME, der die unterstützten VMS-Lösungen und deren kompatible Funktionen im Detail beschreibt, ist über Ihren Ansprechpartner bei TIL TECHNOLOGIES erhältlich.
Je nach VMS werden nicht alle SDK-Versionen unterstützt und nicht alle Funktionen sind verfügbar. Vor jeder Installation wird empfohlen, die Kompatibilität mit TIL TECHNOLOGIES abzuklären.

Ebenso wird empfohlen, die Systemvoraussetzungen für die Videoleitstände (Bildschirmauflösung, Betriebssystem, Grafikkarte, Netzwerkkarte usw.) sowie die Anforderungen an das Netzwerk (Bandbreite, Latenz usw.) zu berücksichtigen, wie sie vom Hersteller des verwendeten Videorekorders angegeben sind, auf den die VISIOSESAME-Clients zugreifen werden.

Zur Information eine Liste der VMS-Lösungen, die aktuell in MICROSESAME integriert sind:

- MILESTONE X-PROTECT (CORPORATE /EXPERT /PROFESSIONAL)
- GEUTEBRUCK G-Scope
- GENETEC Security Center

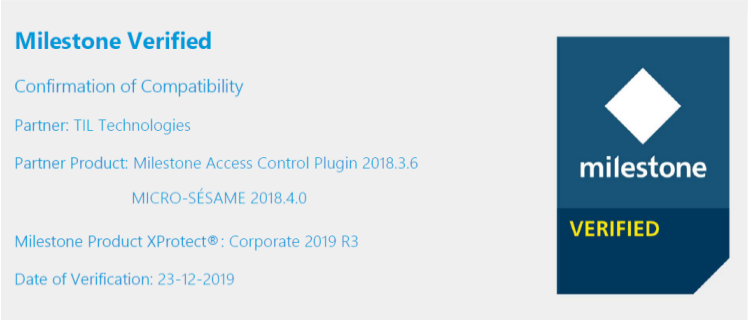
Hinweis: Eine generische ASCII-Textschnittstelle zu VMS-Systemen ist in MICROSESAME CUBE verfügbar (Option LIC-GENERIC-TEXT). Diese funktioniert ohne VISIOSESAME und ohne Video-Streaming in MICROSESAME. Sie wird unter anderem mit **VIVOTEK**, **AVIGILON** und **ARGOS** eingesetzt.

MILESTONE PLUG-IN

Für Kunden, die den Schwerpunkt auf Videoüberwachung legen und eine vereinheitlichte Überwachung wünschen, bietet MICROSESAME CUBE die Option LIC-MILESTONE-PAC an.
Diese integriert das MILESTONE ACCESS CONTROL Plug-in, um die Zutrittskontrolle von TIL direkt über die X-PROTECT-Überwachungsoberfläche von MILESTONE zu steuern.

Diese Schnittstelle, von MILESTONE zertifiziert, ermöglicht es dem X-PROTECT-VMS-Operator:

► Alarme von TIL zu verwalten (MICROSESAME → X-PROTECT)
► Badge-Durchgänge mit Fotoanzeige zu verwalten (MICROSESAME → X-PROTECT)
► Öffnungskommandos für über MICROSESAME verwaltete Zutrittspunkte auszulösen (MICROSESAME ← X-PROTECT)



VISUELLE ZUTRITTSKONTROLLPUNKTE

An einem Zutrittspunkt, der mit einem Ausweisleser und einer Videokamera ausgestattet ist, ermöglicht die Option **MS-CVA**, dass beim Vorhalten eines Ausweises gleichzeitig das Foto des Ausweisinhabers sowie das Live-Video des Zugangs angezeigt werden.
Ein über dem Foto eingeblendete Symbol zeigt den Status des Ausweises an (erlaubt, verweigert, unbekannt).
Das Öffnen der Tür kann je nach Sicherheitsstufe manuell, automatisch oder optional erfolgen. Weitere Aktionen können ebenfalls konfiguriert werden, beispielsweise das Einschalten der Beleuchtung, das Anzeigen einer Nachricht oder die Deaktivierung der Einbruchserkennung in der entsprechenden Zone.

17. EINBRUCHMELDETECHNIK

Eine gesonderte Dokumentation zum Thema Einbruchmeldetechnik **ist über Ihren gewohnten** Ansprechpartner bei TIL erhältlich (z. B. Leitfaden zur Parametrierung der Einbruchmeldetechnik, Verdrahtungsprinzipien für Einbruchmelder, Leitfaden zur Übertragungseinrichtung usw.)

DIE NEUE CUBE INTRUSTION (EINBRUCH CUBE)

Die neue Intrusion Cube 2024 stellt eine bedeutende Weiterentwicklung dar, um den neuen Bedrohungsszenarien und den gestiegenen Sicherheitsanforderungen gerecht zu werden. Diese Version basiert auf vier Verbesserungsachsen: Cybersicherheit, Integration, Benutzerfreundlichkeit und erweiterte Funktionalität.

VERBESSERTE CYBERSICHERHEIT

Zur optimalen Abwehr von Cyberangriffen übernimmt Intrusion Cube die gleiche technische Architektur wie die TIL-Zutrittskontrolle, die ANSSI-zertifiziert ist. Alle Kommunikationen sind verschlüsselt, und sowohl die Hardware als auch die Firmware sind gegen Sabotage geschützt. Darüber hinaus wird ein strenges Management von Schwachstellen und CVE-Patches gewährleistet, um die Systemsicherheit kontinuierlich aktuell zu halten.

INTEGRIERTE ÜBERWACHUNG

Intrusion Cube erleichtert das Systemmanagement durch die Vereinheitlichung von Operatorprofilen für Einbruchmeldungen und Zutrittskontrolle. Die Integration von Endgeräten (Detektoren, Detektorgruppen, Sirenen) wurde vereinfacht, und über Webservices wird eine bessere Interoperabilität mit Drittanwendungen ermöglicht. Eine Identifikation ausschließlich per PIN-Code (ohne Badge) ist ebenfalls möglich

OPTIMIERTE ERGONOMIE

Die Benutzererfahrung wurde durch das neue Touch-Display TACTILLYS-IP das eine einfachere Überwachung und Bedienung ermöglicht, deutlich verbessert. Das Monitoring ist dank animierter Widgets, die eine visuelle Interaktion mit aktuellen Ereignissen bieten, intuitiver**.**

ERWEITERTE FUNKTIONALE LEISTUNG

Zur Unterstützung großer Infrastrukturen ermöglicht Intrusion Cube jetzt den Betrieb über mehrere Zentralen und unterstützt sowohl physische als auch virtuelle Detektoren.
Die Alarmübertragung wurde durch die Einführung des Protokolls SIA DC-09 optimiert, um eine zuverlässige Kommunikation mit Leitstellen zu gewährleisten. Neue integrierte Test- und Diagnosetools erleichtern die Wartung und Optimierung des Systems.

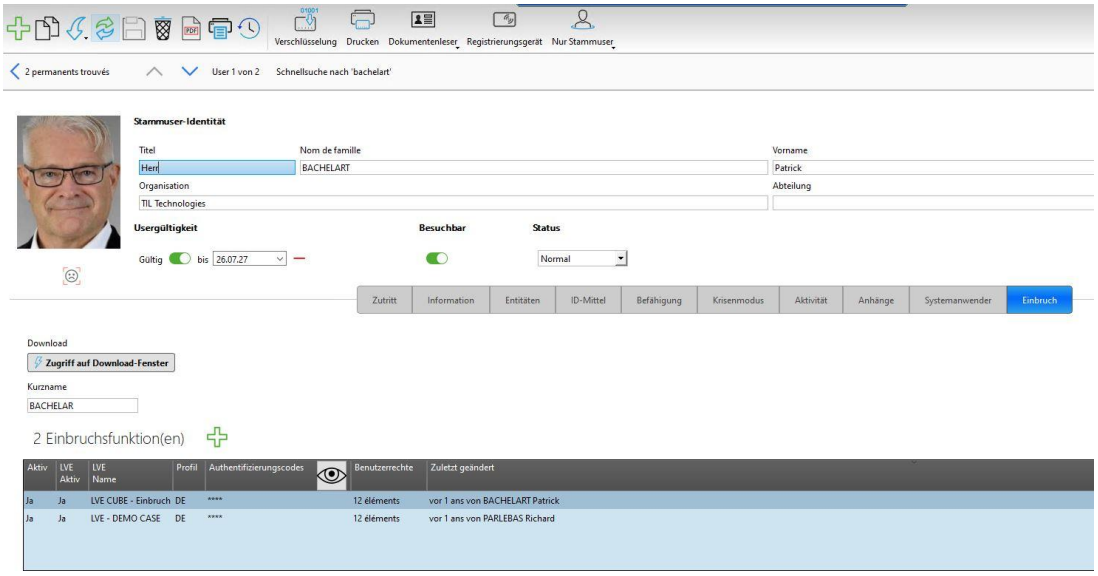
NATIV INTEGRIERTE EINBRUCHMELDETECHNIK

Der MICROSESAME-SERVER VERWALTET ZENTRAL ALLE BENUTZER-NUTZUNGSRECHTE.

Ein Benutzer und sein ID-Code werden nur einmal erstellt und können für mehrere Zentralen verwendet werden:

EIN TILLYS-BENUTZER ist eine Person, die berechtigt ist, sich über Einbruch-Bedienteil der TILLYS-Zentrale zu identifizieren. Jeder Benutzer ist einem Einbruchprofil, entsprechenden Nutzungsrechten sowie einem automatisch generierten PIN-Code für die Einbruchmeldetechnik zugeordnet. Es können Einbruchsnutzungsprofile dupliziert werden.

NUTZUNGSRECHTE: Die Nutzungsrechte definieren die Aktionen, die ein Benutzer über die Bedienteil durchführen darf (z. B. Zugriff auf das Menü, Scharf-/Unscharfschaltung einer Gruppe, Auslösen einer Ausnahmegenehmigung usw.). Jedem Benutzer können individuelle Rechte zugewiesen werden



DIE TILLYS CUBE ZENTRALEN arbeiten eigenständig auf Basis ihrer zuvor in MICROSESAME konfigurierten und heruntergeladenen Betriebsmodi. Jede TILLYS CUBE bietet folgende Kapazitäten:

- ► 32 Gruppen von Melder/Punkten
- ► 624 Melder/Punkte
- ► Unbegrenzte Anzahl an Benutzern
- ► 8 Bedienteile pro Bus, 16 Sirenenfunktionen
- ► Integrierte IP-Übertragungsfunktion „TIP“

BEDIENTEILE TACTILLYS CUBE, angeschlossen an die RS485-Busse der TILLYS-Zentralen, ermöglichen den lokalen und autonomen Betrieb einer Einbruchmeldezentrale mit nur wenigen Klicks. Jedes Bedienteil kann einer Liste von Gruppen zugeordnet werden, um die Bedienmöglichkeiten auf einen eingeschränkten Bereich der Installation zu begrenzen

Die Bedienmöglichkeiten können auf einen eingeschränkten Bereich der Installation begrenzt werden:

► Neues, modernes und ergonomisches Bedienterminal mit 7-Zoll-Touchscreen, installierbar im Hoch- oder Querformat, optional mit Ausweisleser, dessen Schlüssel durch einen HSM-Sicherheitsspeicher EAL5+ geschützt werden

I/O ERWEITERUNGSMODULE für überwachte Ein-/Ausgänge angeschlossen an die Busse der TILLYS-Zentralen, an die Bewegungsmelder, Detektoren und Aktoren (z. B. Sirenen, Lichtsteuerungen) angebunden sind

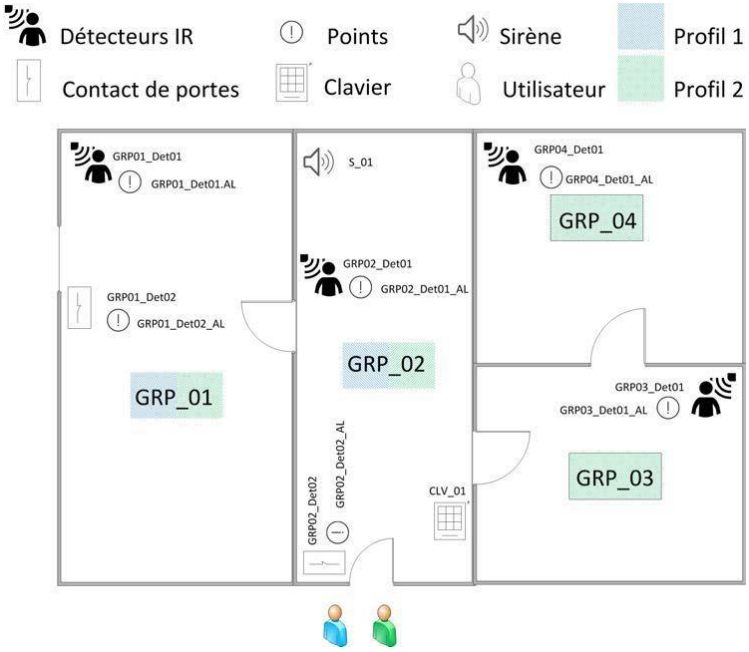
SPEZIFISCHE HOCHSICHERHEITSMODULE FÜR DIE EINBRUCHMELDETECHNIK EQUILOCK, mit jeweils zwei gesicherten Bussen für je 32 kompakte, adressierbare Transponder, die in die Detektoren integriert werden.

DIE LÖSUNG BIETET EINE GROSSE FUNKTIONSVIELFALT UND ANPASSUNGSFÄHIGKEIT, UNTER ANDEREM DANK FOLGENDER FUNKTIONEN:

► Jeder Punkt/Detektor wird einem Punktetyp zugeordnet, der das Auslösen einer Alarmmeldung steuert.
Mögliche Typen sind:
- Einbruchalarm
- 24/24-Alarm
- Stiller Einbruchalarm
- Technischer Alarm
- Stiller Systemfehler
- Notruf
- Feueralarm

► Detektorgruppen definieren eine Sammlung von Detektoren/Punkten, die inhaltlich zusammengehören (z. B. Gebäude, Etage, Abteilung, Perimeter, Zone) und gemeinsam verwaltet werden.
Mögliche gemeinsame Verwaltungsfunktionen sind:
- Scharf-/Unscharfschalten
- Übermittlung von Alarmcodes an eine externe Leitstelle
- Steuerung einer oder mehrerer Sirenen
- Einleitung einer Voralarmphase oder eines Ausnahmemechanismus

Bedienteil TACTILLYS CUBE



Beispiel:
Profil 1 kann die Gruppen **GRP_01** und **GRP_02** scharf- und unscharfschalten.
Profil 2 kann **alle Gruppen** scharf- und unscharfschalten

IN STÖRUNG: Ein Punkt in Störung ist ein Punkt, der den Benutzer in bestimmten Situationen behindern könnte (z. B. bei Bauarbeiten)

MASKIEREN : Funktion, die es ermöglicht, einen Punkt entweder dauerhaft oder vorübergehend von der Überwachung auszuschließen, um die Aktivierung eines Gruppenalarms zu ermöglichen und das unnötige Auslösen von Alarmen oder Maßnahmen durch die Leitstelle zu vermeiden – insbesondere wenn der Punkt beispielsweise gestört oder unwichtig ist.
Es gibt verschiedene Maskierungsmodi:

- Maskieren verboten
- Manuelles Maskieren
- Automatisches Maskieren
- Maksieren mit automatischer Wiedereinbindung
- Permanentes Maskieren

Eine „Wiedereinbindung“ beendet den Ausschluss eines Punktes.

VOR-ALARM : Dies entspricht einer einstellbaren Verzögerung, die durch einen kurzen Sirenenton die Anwesenden auf die bevorstehende Scharfschaltung der Überwachung hinweist und ihnen noch ermöglicht, eine Ausnahmegenehmigung (Verzögerung der Schaftschaltung) zu beantragen.

AUSNAHMEGENEHMIGUNG : Funktion, die es ermöglicht, auf ausdrücklichen Wunsch die automatische Scharfschaltung der Alarmanalge (Trigger) um eine einstellbare Dauer zu verschieben. Die Anforderung kann über das Bedienteil durch einen TILLYS-Benutzer oder durch ein Microcode-Skript oder per Fernbedienung vom MICROSESAME-Server aus erfolgen.

AUTOMATISCHE SCHARFSCHALTUNG MIT TRIGGER : Ermöglicht die automatische Aktivierung der Überwachung (Scharfschaltung) einer Gruppe der Zentrale (z. B. zu festgelegten Zeitfenstern). Automatische Deaktivierungen der Überwachung (Unscharfschaltungen) sind möglich, werden jedoch aus offensichtlichen Sicherheitsgründen nicht empfohlen.

VERZÖGERUNG : Eine Gruppe von Punkten kann beim Eintritt und/oder Austritt mit einer einstellbaren Verzögerungsdauer versehen werden, um dem Benutzer das Erreichen der Ein-/Ausgangstastatur zu ermöglichen, wenn diese sich innerhalb eines überwachten Bereichs befindet. Die Verzögerungszeiten werden auf Gruppenebene definiert, und es wird individuell festgelegt, ob eine Verzögerung beim Eintritt und/oder Austritt für die betreffenden Punkte gilt.

SCHARF-/UNSCHAFRFSCHALTUNG: Die Scharfschaltung eines oder mehrerer Gruppen aktiviert die Überwachung der dem/den Gruppen zugeordneten Einbruchmeldepunkte. Die Scharfschaltung kann auf verschiedene Arten erfolgen:

- Durch eine Benutzeraktion am Bedienteil TACTILLYS CUBE
- Über einen definierten Zeitplan
- Durch andere Aktionen, wie konfigurierte Verknüpfungen mit Eingängen oder Ereignissen aus verschiedenen Bereichen (Bsp. Zutrittskontrolle, Einbruchmeldetechnik, Gebäudetechnik, Brandschutz)

QUITTIERUNG eines Alarmpunktes über die Leitstellen-Software (siehe Kapitel "Überwachung").

INHIBITION eines Punktes oder einer Gruppe von Punkten, die über die Leitstellen-Software vorübergehend deaktiviert werden (siehe Kapitel "Überwachung"

INTEGRIERTE IP-ÜBERTRAGUNGSFUNKTION „TIP“ DER TILLYS CUBE-ZENTRALE:

Die TILLYS CUBE-Zentrale verfügt über eine integrierte IP-Übertragungsfunktion namens „TIP“. Diese ermöglicht die Übertragung von Einbruchalarmen (sowie Zutritts- und Technikmeldungen) über IP an eine Leitstelle, basierend auf den Protokollstandards ID-Contact oder CESA 200, qualifiziert bei ESI und Azur Soft oder SIA.

Die wichtigsten Funktionen dieser Übertragungslösung bieten eine große Funktionsvielfalt und Flexibilität:

LEISTUNGEN JEDER ÜBETRAGUNGS- UND LEITSTELLENEINHEIT (LVE) :

- Bis zu 4 Empfänger/Nutzer für den Empfang von Alarmen (z. B. Leitstellen), die auch Befehle an die Zentrale senden können
- 8 Alarmübertragungsprofile zur Definition, welcher Empfänger kontaktiert wird und in welcher Reihenfolge
- 32 Fernbedienungsbefehle, die von Benutzern ausgelöst werden können

POLLING : Ermöglicht es dem Empfänger, die Zentrale regelmäßig zu überprüfen, um sicherzustellen, dass sie weiterhin im Netzwerk erreichbar ist.

ZYKLISCHER TEST: Die Zentrale sendet regelmäßig eine Testnachricht an den Empfänger, um die Kommunikationsverbindung zu überprüfen. Der Testintervall ist einstellbar (zu einer bestimmten Uhrzeit, abhängig von der Scharfschaltung von Gruppen, individuell pro Empfänger

CODIERUNGSTABELLE: Eine Codierungstabelle legt für jede Alarmart (z. B. Einbruch, Zugang, Brand usw.) einen spezifischen Ereigniscode fest, der an die Leitstelle übermittelt wird. Diese Codes werden in Abstimmung mit der jeweiligen Leitstelle definiert

ÜBERWACHUNG VON EINBRUCHSSYSTEMEN DRITTER:

Dank der Anbindung an Fremdsysteme (z. B. GALAXY NFA2P-Zentralen und Vanderbilt (ACRE) über IP oder SORHEA-Perimetersicherungssysteme mit dem MAXIBUS-Protokoll) ermöglicht MICROSESAME auch die Überwachung von Einbruchalarmen dieser Systeme. Weitere Informationen und Beispiele finden Sie in den speziellen Kapiteln: **Passerellen und Konnektoren**, **Monitoring & Überwachung**, **Videoüberwachung**

18. NOTIZHEFT

Die Funktion „Notizheft“ ermöglicht es, während der Bearbeitung einer Alarmmeldung Kommentare hinzuzufügen – unabhängig von der Art des Alarms (z. B. Einbruchsensor, unerwartetes Türöffnen usw.). Sie kann auf drei Arten verwendet werden:

- Direkt beim Quittieren eines Alarms, sowohl in der Desktop-Oberfläche (Fat Client) als auch in der Weboberfläche WEBSESAME.
- Im Ereignismonitor und im Verlauf (Desktop-Client) durch Klicken auf die betroffene Alarmmeldung.
- In einem speziellen WEBSESAME-Tab, der dem Verfolgen aller „Notizheft-Tickets“ gewidmet ist.

QUITTIERUNG VON ALARMEN

Beim Quittieren eines Alarms kann der Bediener ein Feld „Kommentar“ neben der Schaltfläche „Quittieren“ ausfüllen. Dieses Prinzip gilt sowohl im Desktop-Client als auch in WEBSESAME.

NOTIZHEFT-TICKETS

Im Ereignismonitor oder im Verlauf wird beim Anklicken eines ausgewählten Alarms ein sogenanntes „Notizheft-Tickets“ angezeigt. Es listet in chronologischer Reihenfolge alle Ereignisse im Zusammenhang mit dem Alarm auf (Auslösung, Quittierung, Unscharfschaltung) sowie alle von den Bedienern eingegebenen Kommentare.

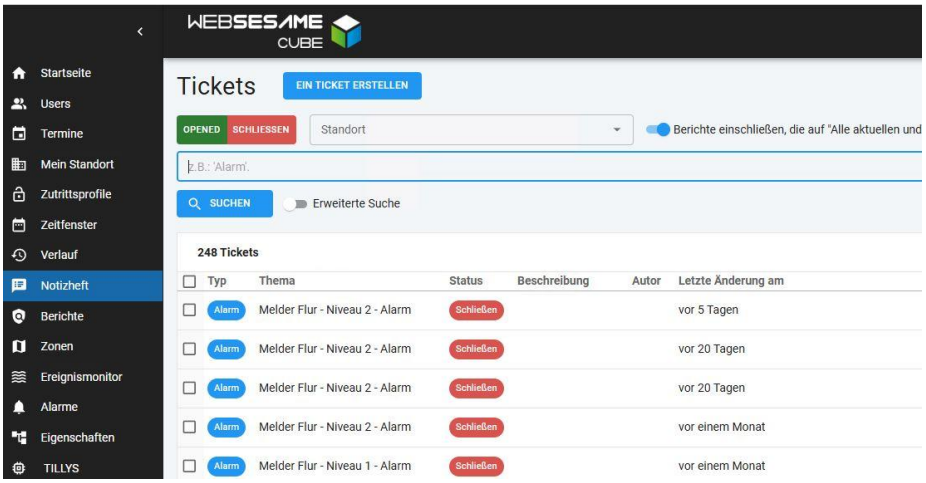
Der Bediener hat außerdem die Möglichkeit:

- Freie Tickets zu erstellen, die nicht mit einem Alarm verknüpft sind,
- Neue Kommentare zu bestehenden vorliegenden Ereignissen einzugeben.

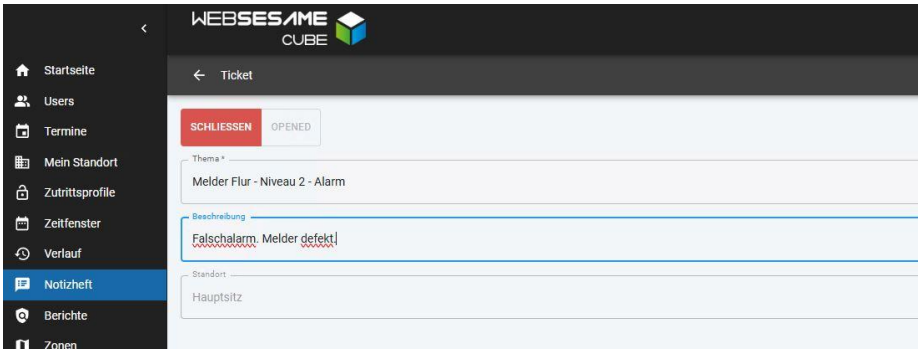
Jeder Bediener kann beliebig viele Kommentare ergänzen, insbesondere wenn die Bearbeitung eines Ereignisses mehrere Schritte umfasste (z. B. Vor-Ort-Kontrolle, Information der Führungsebene, ergriffene Maßnahmen.

WEBSESAME-TAB FÜR NOTIZHEFT

Im speziellen WEBSESAME-Tab für das NOTIZHEFT werden alle Tickets, die mit Alarmen verbunden sind, als Liste angezeigt. Diese kann chronologisch oder nach anderen Kriterien (Bsp. Standort, Alarmname, Status) sortiert werden. Sie kann auch im CSV-Format exportiert werden.



Wie im Desktop-Client kann jedes Ticket aufgeklappt werden, um die chronologische Abfolge der Maßnahmen und Kommentare anzuzeigen. Jeder Bediener kann auch beliebig viele Kommentare hinzuzufügen.



In Web-Oberfläche ist es zudem möglich, den chronologischen Verlauf eines Tickets auszudrucken, auf Papier oder als PDF-Datei.

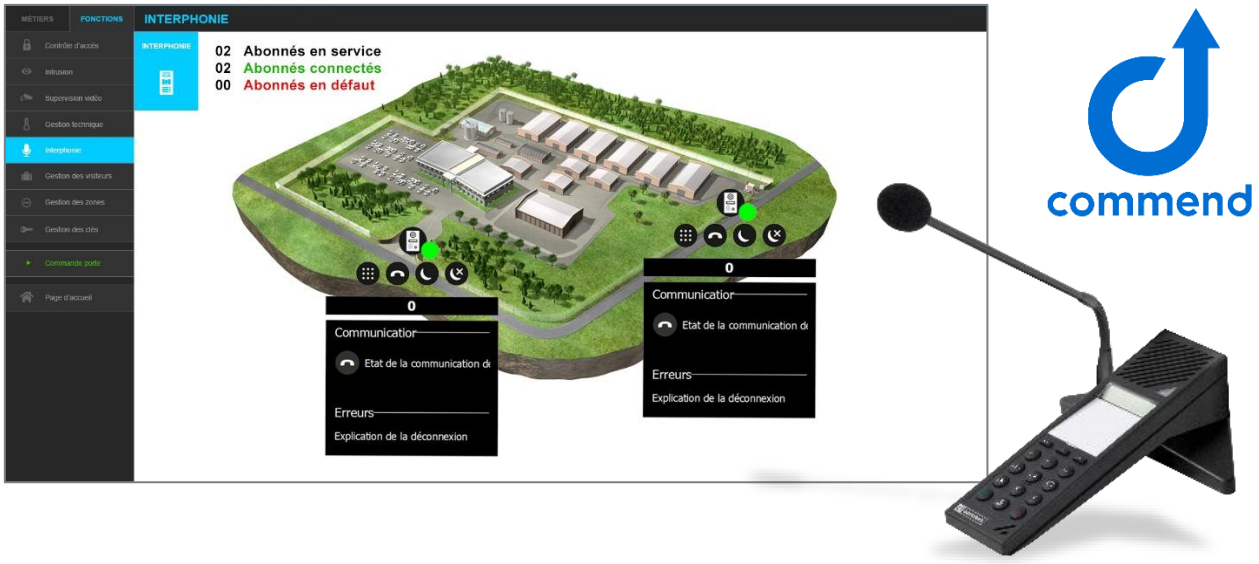
19. SPRECHANLAGEN

SPRECHANLAGEN-NUTZUNG ÜBER MICROSESAME

Durch die Integration von Sprechanlagen in das MICROSESAME-Sicherheitssystem können die Kommunikationsfunktionen über dieselbe grafische Benutzeroberfläche gesteuert werden wie die anderen Sicherheitssysteme im Gebäude (Zutrittskontrolle, Videoüberwachung, Einbruchmeldetechnik, Gebäudetechnik usw.). Dadurch können Ereignis-Folgeaktionen vollständig automatisiert werden. Die Bedienung wird für den Nutzer deutlich vereinfacht und die Reaktionsgeschwindigkeit optimiert.

Es gibt zahlreiche Anwendungsbeispiele:

- Eingehende Sprechanlagen-Anrufe können Videoaufschaltungen auslösen, um eine effektivere visuelle Kontrolle zu ermöglichen, ebenso wie das Einschalten der Beleuchtung oder die Steuerung anderer Automatismen.
- Nach einem Anruf kann die Fernöffnung einer Tür gleichzeitig die Unscharfschaltung der Einbruchüberwachung veranlassen.
- Umgekehrt kann das Verwenden eines verbotenen Ausweises an einem Leser die Wiedergabe einer vorab aufgezeichneten Nachricht über die Sprechanlage auslösen.



Ein weiterer Vorteil dieser Integration ist, dass die Nutzung der Sprechanlagen von allen Informationsfunktionen profitiert, die MICROSESAME bietet gemeinsame Historien, erweiterte Suchfunktionen, Erstellung von Berichten zur Analyse und zur Nutzungsauswertung.

INTERAKTION MIT COMMEND-LÖSUNGEN

MICROSESAME ermöglicht die Kommunikation mit den IP-Sprechanlagenzentralen COMMEND von Schneider Intercom (GE800, GE300, IS300, VIRTUOSIS).

Die Mehrheit der gängigen Kommunikationsvorgänge kann von jedem beliebigen Bedienplatz in MICROSESAME aus durchgeführt werden:

- Vollständige Virtualisierung des Hauptbedienplatzes (Mikrofon und Lautsprecher direkt am Bedienplatz angeschlossen)
- Anzeige und Status der Sprechanlagen-Anrufe (Teilnehmer) zum Hauptbedienplatz sowie der Status der Teilnehmer (in Kommunikation usw.)
- Differenzierte Behandlung auf zwei Ebenen: normale Kommunikation oder Notfall
- Anrufannahme, Unterbrechung oder Abbruch
- Aktivierung/Deaktivierung eine Sprechanlage
- Anzeige der Verbindungszustände eines Teilnehmers/MICROSESAME zum Sprechanlagenserver und der Ursachen: Stromausfall, Sabotage, Kurzschluss usw.
- Aufbau und/oder Beenden einer Kommunikation zwischen zwei Stellen (Direkttaste in der grafischen Oberfläche oder über die Tastatur des virtuellen Hauptbedienplatzes)
- Nachtschaltung: Weiterleitung der Anrufe vom Hauptbedienplatz auf einen anderen Bedienplatz je nach Tag-/Nachtmodus
- Fernlauschen
- Verbreitung von vorab aufgenommenen Audiomeldungen über die Sprechanlage von COMMEND bei Alarmen zum Beispiel
- Steuerung von COMMEND-Relais auf Sprechanlagen oder virtuellen Relais (z. B. Beleuchtung)
- Öffnen einer Tür, die auf einem TIL-Modul verdrahtet ist, durch Drücken einer Taste an einer Sprechanlage von COMMEND

VEREINFACHTE PARAMETRIERUNG UND INTEGRATION

NATIVE INTEGRATION MIT SPEZIFISCHEN „OBJEKTEN UND EIGENSCHAFTEN“

Die Integration der Sprechanlagen von COMMEND wurde so konzipiert, dass eine Zeitersparnis bei der Parametrierung erreicht wird, dank der Definition von Objekten „Server“ und „Teilnehmer“. Es genügt, den Sprechanlagenserver zu deklarieren und die bereits mit den Tools von COMMEND erstellte Teilnehmerliste zu importieren. Die Überwachungselemente für Server und Teilnehmer werden dann automatisch in MICROSESAME erstellt. MICROSESAME kann gleichzeitig mit mehreren COMMEND-Servern verbunden werden. Einige spezielle Funktionen sind nicht nativ integriert, können aber durch zusätzliche Parametrierung entweder auf Seite von MICROSESAME oder des COMMEND-Servers umgesetzt werden. Beispiel: die Befehlsauslösung einer Evakuierungsnachricht an alle Sprechanlagen gleichzeitig (anstatt einzeln).

GRAFISCHE ÜBERWACHUNG

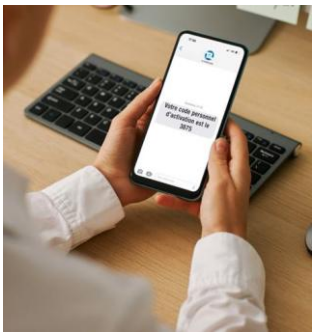
Für die grafische Überwachung beinhalten die Objekte vorkonfigurierte Symbole (Icons) für eine direkte Integration in die synoptischen Bildschirme von MICROSESAME. Diese Symbole enthalten nicht alle Eigenschaften der Objekte, können aber je nach MICROSESAME-Versionen ergänzt werden. Natürlich besteht auch die Möglichkeit, eigene Sprechanlagensymbole zu erstellen und die gewünschten Eigenschaften in die Übersichtsbildschirme zu integrieren.

20.ON-BOARDING MIT CARDIGO CUBE

CARDIGO ermöglicht die frühzeitige Ausgabe und Verteilung neuer Zutrittsausweise ohne jegliches Risiko bis zu ihrer ersten tatsächlichen Nutzung. Für die Nutzer wird der Empfang im Unternehmen erleichtert, da ihnen der Ausweis bereits vor ihrem Eintritt übergeben wird (Bsp. persönlich, per Postweg).
Für den Sicherheitsdienst besteht kein Risiko mehr einer missbräuchlichen Verwendung durch Verlust oder Dritte, da die Zutrittsausweise solange inaktiv bleiben, bis sie auf einem CARDIGO-Terminal authentifiziert werden.

Um einen Ausweis im System zu aktivieren, authentifiziert sich jeder Nutzer eigenständig mit einem PIN-Code, der separat vom Ausweis übermittelt wird. Ohne geografische oder zeitliche Einschränkungen ist diese Lösung für die gesamte Organisation praktischer. Es besteht keine Verpflichtung mehr, sich zu einem bestimmten Zeitpunkt an einem festgelegten Sicherheitsposten einzufinden.

PRINZIP DES AKTIVIERUNGSCODES



- Erstellung persönlicher PIN-Codes in einer externen CSV-Datei, Import in MICROSESAME
- Versand der persönlichen PIN-Codes getrennt von der Übergabe der Badges
- Per Post, E-Mail oder SMS… Die Verteilungsmethode wird vom Kunden festgelegt

ZUORDNUNG BADGE / CODE AM CARDIGO

- Auflegen des Badges und anschließende Eingabe des PIN-Codes über die Touchscreen-Oberfläche
- Bei Übereinstimmung > Systemaktivierung und Übertragung der Rechte in die Steuerungseinheiten (Controller)
- Bei keiner Übereinstimmung > Keine Anzeige von Informationen über den Ausweisinhaber und der Ausweis bleibt inaktiv, ohne jeglichen Zugang

21. TRAGBARES LESEGERÄT MOBILIS CUBE 2024

NEUE METHODE ZUR DATENBANKSYNCHRONISATION

- Bis zu 50.000 Identifizierungen in weniger als 10 Minuten heruntergeladen

VEREINFACHTE PARAMETRIERUNG UND INBETRIEBNAHME

- Verwaltung von Checkpoint-Parameterprofilen direkt in MICROSESAME
- Funktionen und Informationen, die den Bedienern am Terminal zugänglich sind, können wesentlich präziser zugewiesen werden

VERBESSERTE ERGONOMIE

- Neues, vereinfachtes Layout verfügbar für die automatische Zutrittskontrolle: Auf Wunsch Anzeige von Bild, ID und einem grünen oder roten Hintergrund je nach Entscheidung (zusätzlich zum Standardthema)
- Ausweis- oder auf Wunsch QR-Code-Lesung per einfachem Klick

CYBERSICHERHEIT & MILITÄRISCHES HARDENING

- Passwörter werden signiert gespeichert, mit Hashing und Salting
- Automatische Löschung offline gespeicherter Daten im MOBILIS nach einer konfigurierbaren Anzahl von Stunden ohne Serververbindung sowie nach einer bestimmten Anzahl fehlgeschlagener Authentifizierungsversuche
- Verschlüsselung der SQL-Lite-Datenbank
- Keine Speicherung von Ausweis-Schlüsseln, da nur das CSN (Card Serial Number) ausgelesen wird
- Verwaltung eines internen Anti-Time-Back-Mechanismus im MOBILIS.

22. DIGITALE SCHLÜSSELSCHRÄNKE

MICROSESAME integriert Konnektoren für Schlüsselschränke von TRAKA (ASSA ABLOY) und PROXSAFE (DEISTER). Diese lizenzpflichtigen Konnektoren ermöglichen folgende Vorgänge direkt von einem MICROSESAME-Client oder -Server aus:

► Zuweisung von Zugriffsrechten auf Schlüssel/Keytags und Schlüsselgruppen/Keytagsgruppen
► Überwachung von Ereignissen im Zusammenhang mit Schränken und Schlüsseln (Überwachungsobjekte)
► Ausführen von Fernsteuerbefehlen an die Schränke (Überwachungsobjekte).

ÜBERWACHUNG DER TRAKA- UND DEISTER-SCHRÄNKE

Die Integration in MICROSESAME ist einfach und die Parametrierung erfolgt in wenigen Minuten durch den Import aller Informationen zu Schlüsseln, Schlüsselgruppen und Schränken aus den TRAKA- oder PROXSAFE-Softwares in einem einzigen Vorgang. Die Zuweisung der Zugriffsrechte auf diese Schlüssel oder Schlüsselgruppen erfolgt anschließend transparent: direkt in den Interfaces „Benutzer“ und „Zutrittsprofile“ von MICROSESAME und WEBSESAME. Somit profitiert die Schlüsselverwaltung von der Präzision der klassischen Zutrittsrechte (Zugehörigkeit zu Profilen, Zeitpläne usw.) und von allen erweiterten Funktionen wie Betreiberfilterung, Mehrfachänderungen, Suchfunktionen und Identifikatoren-Gateways…

ÜBERWACHUNG DER DIGITALENSCHLÜSSELSCHRÄNKE VON TRAKA & DEISTER

Der Import der Konfiguration der Schlüsselschränke ermöglicht die automatische Erstellung der zugehörigen Überwachungsobjekte für die TRAKA- und PROXSAFE-Geräte:

• Bei den Schränken: Verbindungsstatus, Batteriestatus, Fehler, Türöffnungen usw.
• Bei den Schlüsseln/Keytags oder Schlüsselgruppen/Keytagsgruppen: Entnahme-/Rückgabestatus, betroffener Benutzer, Rückgabezeit, Verspätungen, Position im Schrank usw.

Die Eigenschaften dieser Überwachungsobjekte werden entsprechend den von den TRAKA- oder PROXSAFE-Servern gemeldeten Ereignissen aktualisiert. Die mit den Schränken verbundenen Steuerbefehle können genutzt werden, um Zustandsänderungen direkt an die Server zu übermitteln. Das Zugriffsprotokoll der Schlüssel ist über das technische Ereignisprotokoll (der Überwachungsobjekte) verfügbar. Außerdem können diese Eigenschaften in der grafischen Überwachungsschnittstelle verwendet und ihre Zustände im Ereignismonitor angezeigt werden.

Hier ist die Liste der verfügbaren Eigenschaften für jedes Überwachungsobjekt:

proxSafe®

Objekt PROXSAFE-Schlüsselschrank:

- Stromausfall
- Niedriger Batteriestand
- Verbindung zum COMMANDER-Server
- Datum/Uhrzeit des letzten Ereignisses
- Öffnung des Schranks
- Tür zu lange geöffnet
- Wartungstür geöffnet
- Diebstahlalarm
- Diebstahlalarm im Wartungsfach
- Dreimal falscher Code
- Unerwartete Öffnung
- Unbekannter KeyTag zurückgegeben
- Unbekannter KeyTag entnommen
- Keine Bewegung von KeyTags (Tür geöffnet und wieder geschlossen ohne KeyTag-Entnahme oder -Rückgabe)

Objekt PROXSAFE-Keytag:

- Datum/Uhrzeit letzter Ereignisse
- Vom Nutzer entnommener Schlüssel
- Unerwartete Entnahme
- Schon zu lange entommen
- Keytag vom Nutzer wieder gefunden
- Inkorrekte Rückgabe
- Gesicherte Rückgabe vermieden (Rückgabeprotokoll n. eingehalten)
- Überschrittene Rückgabefrist
- Zur Rückgabe an Nutzer entriegeln

Objekt PROXSAFE- Keytags-Gruppe:

- Datum/Uhrzeit letzt. Ereignisse
- Unvollständige Gruppenentnahme
- Unvollständige Gruppenrückgabe

traka
ASSA ABLOY

Objekt TRAKA-Schlüsselschrank:

- Stromversorgung
- Batterie verbunden
- Batteriestatus (3 Stufen)
- Verbindung zum TRAKA-Server
- Angemeldeter Benutzer
- Verbindungsdauer
- Öffnung des Schranks
- Öffnungsdauer
- Tür zu lange geöffnet
- Wartungstür geöffnet
- Diebstahlalarm
- Unerwartete Öffnung

Objekt TRAKA-Schlüssel:

- Position
- Schlüssel entnommen/verfügbar
- Schlüssel vom Identifizierten entnommen
- Datum/Uhrzeit der Entnahme
- Schlüssel vom Identifizierten zurückgegeben
- Datum/Uhrzeit der Rückgabe
- Überschrittene Rückgabezeit
- Falsche Rückgabe (falscher Steckplatz)
- Unerwartete Entnahme

23. NOTFALLMANAGEMENT

UNTERSTÜTZUNG BEI EVAKUIERUNGEN UND RETTUNGSEINSÄTZEN

Notfallmanagement beschreibt die organisatorischen Maßnahmen, die Einsatzmethoden und die erforderlichen Mittel, die der Betreiber einsetzen muss, um sein Personal, die Bevölkerung und die Umwelt zu schützen. Er wird insbesondere für Anlagen mit erhöhtem Risiko verlangt, insbesondere für Anlagen, die einem besonderen Einsatzplan verpflichtet sind.

INTEGRATION IN MICROSESAME

Die in MICROSESAME integrierte POI-Unterstützungsanwendung greift in den Schutzprozess des Personals über benutzerfreundliche Bedienoberflächen und spezielle Fenster sowie folgende Funktionen ein:

- ► Parametrierung der POI-Zonen in zwei Kategorien: gesicherte und ungesicherte Zonen
  - • Gesicherte Zonen sind die Sammelbereiche für das Personal, die Schutz vor Gefahren bieten
  - • Ungesicherte Zonen umfassen den übrigen Bereich der Anlage
- ► Echtzeitbereitstellung der Liste und der Anzahl der auf dem Gelände anwesenden Personen, aufgeschlüsselt nach Zonen, mit Anzeige ihrer Qualifikationen (sofern verwendet), basierend auf ihren Ausweis-Lesevorgängen
- ► Echtzeitüberwachung von Personalfluss von den Arbeitsbereichen in die gesicherten Bereiche nach Auslösung des Notfallplans, bei Übungen oder realen Vorfällen
- ► Suche nach einer Person zur Lokalisierung (in gesicherter oder ungesicherter Zone)
- ► Erstellung einer Namensliste der Personen mit Fotoübersicht für ausgewählte Zonen
- ► Möglichkeit des Exports der Personenliste im PDF-Format in ein definiertes Verzeichnis
- ► Start der Nutzung und Anzeige der POI-Zonen direkt über eine Grafikübersicht oder das Hauptmenü

Um die Erfassung an Sammelpunkten (gesicherte Zonen) zu erleichtern, ist der tragbare Ausweisleser MOBILIS besonders praktisch, da er für den Außeneinsatz geeignet ist. Es ist keine Verkabelung von fest installierten Lesern mehr nötig, da die Ausweislesung durch die Evakuierungs-verantwortlichen vorgenommen wird.

24. RUHEZEIT-ÜBERWACHUNG

EINHALTUNGS VON ARBEITSZEITVORSCHRIFTEN

MICROSESAME ermöglicht es Ihnen mit der Funktion „Ruhezeit-Überwachung“, die Einhaltung des Arbeitszeitgesetzes einfach über die Zutrittskontrolle des Gebäudes sicherzustellen. Durch die automatische Analyse der Nutzerdurchgänge wird geprüft, ob die gesetzlichen Ruhezeiten oder andere vom Unternehmen festgelegte Pausen eingehalten wurden. Diese Funktion bietet mehrere Optionen:

UTOMATISCHES BLOCKIEREN DER ZUGÄNGE für Mitarbeiter, die die vorgeschriebenen Ruhezeiten zwischen dem Verlassen und Betreten des Standorts nicht eingehalten haben, bis zum nächstmöglichen erlaubten Zeitpunkt.

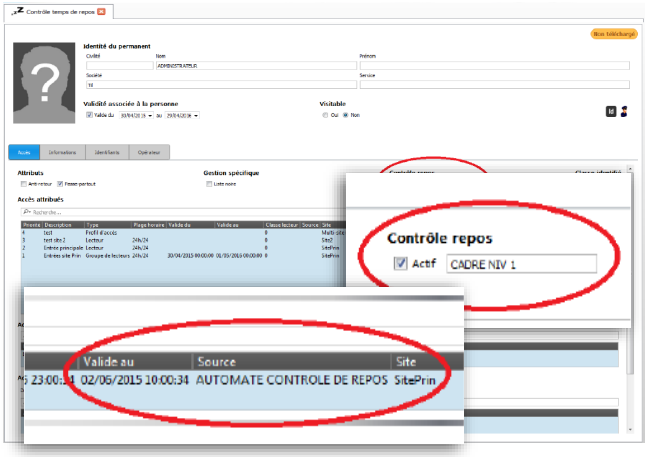
MELDUNG DER TEMPORÄREN ZUGANGSVERWEIGERUNG an die Betreiber mit Angabe von Datum und Uhrzeit der nächsten erlaubten Zutrittsmöglichkeit in der Nutzerkarteikarte – wahlweise mit oder ohne Zutrittssperre.

MANUELLE AUFHEBUNG DER TEMPORÄREN BLOCKIERUNG durch einen autorisierten Bediener.

ERSTELLUNG VON BERICHTEN zur Anzeige der Abweichungen bei den Ruhezeiten.

AUSNAHMESITUATIONEN: Möglichkeit, die Kontrolle der Ruhezeiten für alle Mitarbeiter zu deaktivieren.

Um eine große Anzahl von Personen effizient zu verwalten, basiert die Funktion „Ruhezeit-Überwachung“ auf dem Konzept der „Ruhezeitregime“. Für jedes „Ruhezeitregime“ müssen Ein- und Ausgangsleser definiert, die Ruhezeiten und Wochentage sowie der Beginn der wöchentlichen und täglichen Berechnungszeiträume festgelegt werden. Es können mehrere „Ruhezeitregime“ erstellt werden, sodass jeder Nutzer nach den für ihn geltenden Regeln und über die entsprechenden Leser überwacht wird. Die Zuordnung kann direkt in MICROSESAME oder über eine Schnittstelle mit der HR-Datenbank des Unternehmens erfolgen.



Wird diese Option für einen Mitarbeiter aktiviert, werden verweigerte Lesedurchgänge im Ereignismonitor und im MICROSESAME-Verlauf als „außerhalb der zulässigen Zeiten“ gekennzeichnet.

Beim Öffnen der Nutzerkarteikarte kann die temporäre Zutrittssperre sowie das Datum und die Uhrzeit der nächsten erlaubten Zutrittsmöglichkeit eingesehen werden.

Falls erforderlich, kann diese Sperre manuell von einem autorisierten Bediener aufgehoben werden.

Abschließend ermöglicht der Universelle Abfragegenerator von MICROSESAME eine umfassendere Überwachung durch die HR- und Sicherheitsdienste, indem wöchentliche Auswertungen durchgeführt werden können, um eine Datei mit allen „außerhalb der zulässigen Zeiten“ verweigerten Zutritten zu erstellen.

25. KONTROLLGANGS-MANAGEMENT

UNTERSTÜTZUNG FÜR KONTROLLGELÄNDE AUF DEM GELÄNDE

Die Verwaltung der Kontrollgänge, ehemals eine optionale Softwareerweiterung und jetzt standardmäßig in MICROSESAME CUBE enthalten, ermöglicht das Erstellen von Rundgängen sowie die Echtzeitüberwachung der Sicherheitsagenten, die die Rundgänge auf dem Gelände durchführen.
Ein Kontrollgang entspricht einer vordefinierte Route von Lesern, an denen die für die Runde verantwortlichen Mitarbeiter nacheinander ihren Ausweis vorhalten müssen.
Diese Option ermöglicht die Überwachung Fortgangs mehrerer Sicherheitsagenten auf bis zu 64 verschiedenen Kontrollgängen (jeweils ein Agent pro Kontrollgang).

DIE VERWALTUNG DER KONTROLLGÄNGE kann die bereits auf Ihrer Anlage installierten Leser nutzen, ohne dass extra für Kontrollgänge dedizierte Geräte erforderlich sind.

DER KONTROLLANG kann auch ohne Zutrittsrechte an den betreffenden Lesern durchgeführt werden, jedoch dann ohne tatsächlichen Zutritt. Der Sicherheitsagent kann dabei seinen regulären Zutrittsausweis zur Durchführung der Runde verwenden.

ES EXISTIEREN SPEZIFISCHE BEDIENRECHTE für die Verwaltung der Kontrollgänge (Zugriff auf die Anwendung und Verwaltung der Kontrollgänge ohne notwendige Zutrittsrechte), beispielsweise für speziell eingeschränkte Bedienerprofile.

Zum Starten einer Runde wählen Sie einen Rundgang aus der Liste aus und bestimmen den Sicherheitsagenten, der die Runde im Gelände ausführt. Die vorgegebene Zeit zwischen zwei Lesern muss eingehalten werden. Bei Überschreitung der zulässigen Zeit zwischen zwei Lesern wird automatisch ein Ereignis oder Alarm im Ereignismonitor ausgelöst, der den betreffenden Sicherheitsagenten und Kontrollgang angibt. Im Alarmfall stehen folgende Aktionen zur Verfügung: Quittieren, Anzeige des zugehörigen Grafikoberfläche, Visualisierung der zugehörigen Kamera in VISIOSESAME

Eine spezielle Tabelle zeigt in Echtzeit die verschiedenen Informationen und Zustände der Rundgänge an:
► Der aktuell durchgeführte Rundgang und der zugewiesene Sicherheitsagenten
► Die seit dem Start des Rundgangs vergangene Zeit
► Die verbleibende Zeit, die der Agent hat, um seinen Ausweis am nächsten Leser vorzuhalten, mit einer farbcodierten Fortschrittsanzeige (grün, gelb, orange, rot) je nach verbleibender Zeit
► Die Gesamtdauer für jede Etappe
► Die Gesamtanzahl der Etappen
► Die aktuelle Etappe
► Der letzte Leser, an dem der Ausweis des Agenten erkannt wurde
► Der Punkt, an dem der Identifikator des Agenten als nächstes präsentiert werden muss

Der Bediener kann außerdem jederzeit eine zusätzliche Frist für den nächsten Lesedurchgang gewähren oder den Kontrollgang abbrechen.

26. VERLAUF, REQUESTER, BERICHTE & JOURNALS

Diese Funktionen sind nativ in die MICROSESAME-Lösung integriert

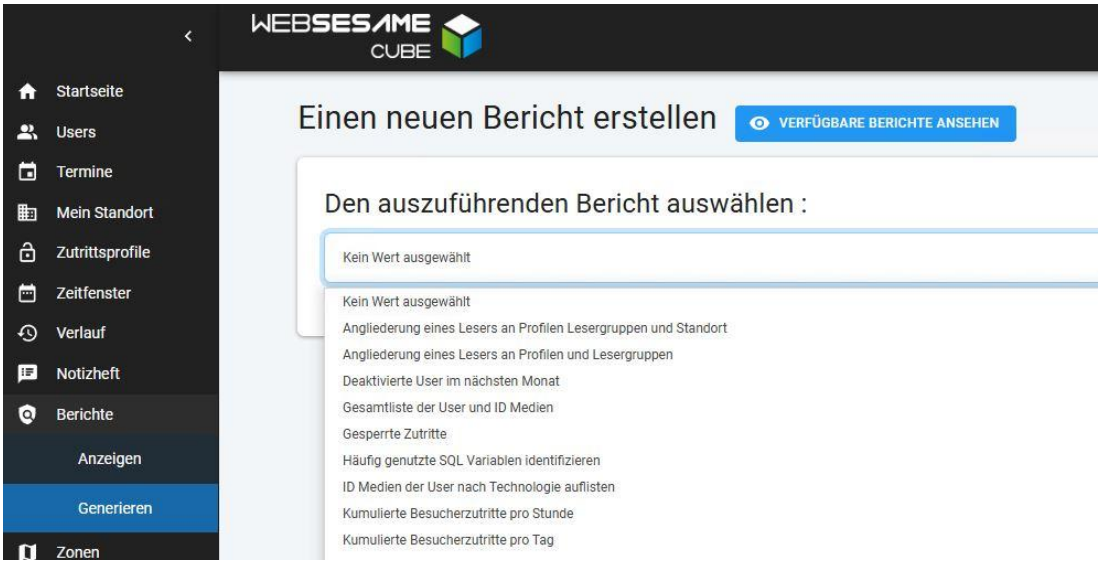
VERLAUF

Die Funktion „Verlauf“ ermöglicht es vom Desktop-Client aus, alle in der Datenbank gespeicherten Ereignisse einzusehen. Sie protokolliert sowohl die Nutzung des Gebäudes (Ausweislesungen, technische Alarme usw.), die Systemaktivitäten als auch die Aktionen der Bediener. Die Speicherkapazität ist unbegrenzt. Standardmäßig beträgt die Ereignisaufbewahrungsdauer 30 Tage, diese kann jedoch angepasst werden, zum Beispiel auf 3 Monate.

Die Such- und Anzeigeoptionen für Ereignisse, Alarme und Bewegungen werden in einer globalen Ansicht mit gemeinsamen Suchkriterien und den folgenden Reitern angeboten, die jeweils bestimmten Ereignistypen entsprechen:

- Zutrittskontrolle
- Technische Ereignisse
- Systemereignisse
- Audit der Änderungen (Bedieneraktionen)
- Zusammenführung aller Ereignisse

Die angezeigten Felder unterscheiden sich je nach Reiter. Standardmäßig ist die Suchperiode auf die aktuelle Stunde und die letzten 7 Tage eingestellt.



Die Funktion Verlauf bietet dem Kunden Präzision, Personalisierung und Geschwindigkeit durch:

FILTER FÜR BESTIMMTE DATEN (FELDER) Sie ermöglichen eine sehr genaue Ausgabe der gesuchten Ereignisse. Um schnelle und relevante Filterauswahlen zu ermöglichen, können diese in vordefinierten Dropdown-Listen erscheinen, je nach Parametrierung des Systems. Bsp: Auswahl des Standorts (bei Multi-Site-Management), Typ des Identifizierten (Besucher oder festangestellter Mitarbeiter), Status des Identifikators (verloren, gestohlen, aktiv)

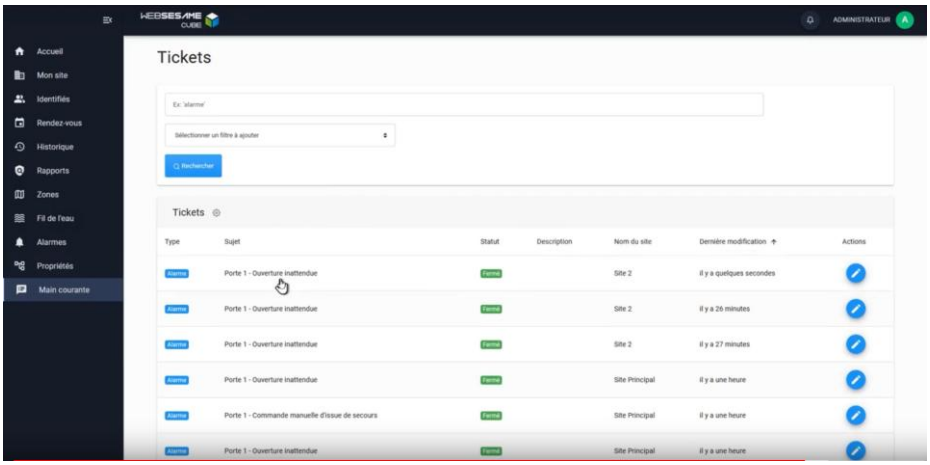
SPEICHERUNG UND BENENNUNG: Um wiederkehrende Anforderungen zu vereinfachen, kann jeder Bediener Suchvorgänge mit den verwendeten Parametern und Filtern speichern und benennen. Diese gespeicherten Suchvorgänge erscheinen im Fenster „vordefinierte Filter“, wobei zwischen privater Speicherung (nur sichtbar für den Bediener, der sie erstellt hat) oder öffentlicher Speicherung (für andere Bediener verfügbar) gewählt werden kann. So entfällt die wiederholte Neueingabe der gleichen Suchkriterien und es wird erheblich Zeit gespart

FILTERUNG der Sichtbarkeit von Eigenschaften je nach Rechtekategorie des Bedieners.

HINZUFÜGEN VON DETAILS BEI VERWEIGERTEN DURCHGÄNGEN: Anzeige von Standort, unbekanntem Identifikator, verstärkter Kontrolle, kontrolliertem Durchgang oder Zugang verweigert

WEBSESAME

Das WEBSESAME-Portal bietet unter anderem folgende Anwendungen im Bereich Historie, Berichte usw.:
• Erstellung und Export von Berichten, vordefinierte Abfragen
• Historie von Ereignissen im Zusammenhang mit Zutrittskontrolle und Technik
• Übersicht der aktuellen Alarme
• Echtzeit-Überwachung von Zutritts-, Technik- und Systemereignissen. Durch Klick kann die Identifikator-Karte des Ereignisses aufgerufen werden. Vereinfachter Ereignismonitor
• Hinzufügen und Anzeigen von offenen Tickets/Kommentaren zu quittierbaren Alarmen. Einfache oder gefilterte Suche
• Erstellen von Berichten und grafischen Zusammenfassungen zu genehmigten und verweigerten Durchgängen an den vom Bediener überwachten Standorten
• Unterstützung bei der Diagnose der Installation: Anzeige der Status-/Eigenschaftenliste (z. B. geöffnete Tür) eines Überwachungsobjekts, Filterung, Interaktion mit diesen Zuständen (z. B. Fernsteuerbefehle), Inhibierung einer Eigenschaft bei Wartungsarbeiten

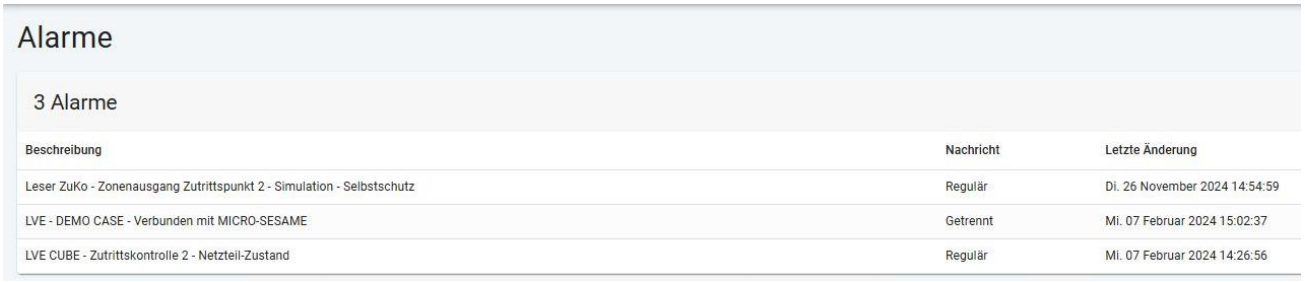


WEBSESAME VERLAUF FÜR ZUTRITTSKONTROLLE

Die Web-Oberfläche von MICROSESAME beinhaltet einen Reiter, der eine einfache Ansicht der Zutrittskontrollhistorie ermöglicht, um Ausweislesungen zu recherchieren.
Verschiedene Parameter und Filter wie Datum oder Ereignistyp (erlaubte oder verweigerte Ausweise usw.) können angewendet werden, um die Datenabfrage zu erleichtern.
Die anzuzeigenden Ergebnisfelder sind vollständig konfigurierbar (Anrede, Name, ID-Medium…)

WEBSESAME VERLAUF FÜR TECHNISCHE EREIGNISSE

Die Anwendung „Verlauf der Variablen (Eigenschaften)“ ermöglicht die Recherche technischer Ereignisse im Zusammenhang mit dem Zutrittskontrollsystem.



WEBSESAME ALARME

Der Bediener kann die aktuellen Alarme der von ihm überwachten Standorte einsehen. Die im Anzeigefenster dargestellten Informationen werden in Echtzeit aktualisiert. Eine Farbkennzeichnung ermöglicht es, quittierbare und nicht quittierbare Alarme leicht zu unterscheiden.

WEBSESAME – BERICHTE, UNIVERSELLER ABFRAGEGENERATOR

Ebenfalls über das WEBSESAME-Portal zugänglich ist der Universelle Requester (Abfragegenerator) – ein Tool zur Extraktion aller Arten von Informationen aus der MICROSESAME-Datenbank durch Ausführung einer SQL-Abfrage und die Erstellung eines Berichts bzw. Ergebnisses.

Der universelle Web-Abfragegenerator bietet folgende Möglichkeiten:

ABFRAGEN : Es sind bereits native Abfragen im Produkt enthalten (siehe Liste unten), die Ihnen die gängigsten Suchen ermöglichen. Die Bibliothek der verfügbaren Abfragen befindet sich unter: Server\ScriptsSql\SqlServer\Requestor

ERGEBNIS, BERICHT: Das Ergebnis wird direkt in der Benutzeroberfläche nach Ausführung der gewünschten Abfrage angezeigt. Es besteht die Möglichkeit, das Ergebnis in eine CSV- oder PDF-Datei zu exportieren. Die CSV-Datei kann anschließend in einer Tabellenkalkulation wie Excel oder in einem Texteditor genutzt werden, um Grafiken zu erstellen oder Statistiken auszuwerte

AUSFÜHRUNG EINES BERICHTS: Berichtsausführung bei Änderung einer Eigenschaft und automatischer Versand per E-Mai.

ERSTELLUNG VON EIGENEN ABFRAGEN MÖGLICH:

- Durch den Errichter oder Endkunden, sofern ausreichende Kenntnisse in SQL-Skripting vorhanden sind, für einfache Abfragen basierend auf bestehenden Beispielen,
- Durch TIL TECHNOLOGIES im Rahmen eines Projekts für komplexere Abfragen, da das Datenbankschema und die Tabelleninhalte (MCD) nicht dokumentiert sind.

IMPORT UND EXPORT VON ABFRAGEN im Format „.json“-Datei: Es ist möglich, eine zuvor aus einem anderen MICROSESAME-System exportierte Abfrage zu importieren.

FILTER : Die Abfrage kann Parameter enthalten, um die Ergebnisse gezielt zu filtern, z. B. nach Datum, Uhrzeit, Auswahl in Dropdown-Listen (Firma, Abteilung, Leser usw.), Person usw. Wird ein Filterfeld nicht ausgefüllt, bezieht sich die Suche auf „alle“ Einträge des betreffenden Feldes.

TOOL „EXTRAKTOR“: Dieses in der Lösung enthaltene Tool ermöglicht die Erstellung automatischer und periodischer Berichte gewünschter Abfragen in vordefinierten Verzeichnissen und erleichtert so wiederkehrende Aufgaben erheblich.

BEISPEILABFRAGEN:

► „Ruhezeiten-Abfrage“: Liste der Identifizierten, die ihre Ruhezeiten nicht eingehalten haben

► „Abfrage Nutzer, die im nächsten Monat ungültig werden“: Liste der Personen, deren Gültigkeit zu einem bestimmten Datum abläuft. In der Benutzeroberfläche dieser Abfrage finden sich folgende Filter: Startdatum-Enddatum, Personalnummer, Name, Vorname

DIAGRAMME UND KURVENDARSTELLUNGEN IN MICROSESAME

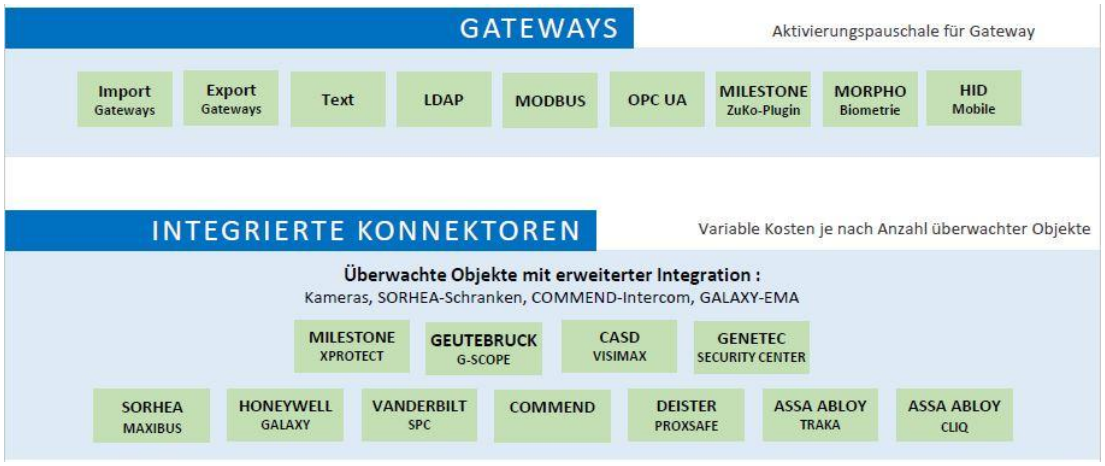
MICROSESAME integriert eine Anwendung für Diagramme/Kurven, die es ermöglicht, die Entwicklung numerischer oder logischer Variablen über einen definierten Zeitraum hinweg grafisch darzustellen. Diese Anwendung bietet folgende Funktionen: ► Eine spezifische Suchperiode zur Filterung der angezeigten Daten

► Die erzeugten Kurven/Daten können im PDF-Format oder als .JSON-Datei an einem frei wählbaren Speicherort exportiert werden. JSON-Dateien können ebenfalls für den Import externer Parameter verwendet werden.

- ► Mehrere Kurven können in einem einzigen Diagramm zusammengefasst werden
- ► Folgende Anzeigeeigenschaften der Kurven sind parametrierbar
    - o Farben der Kurven, Hintergrund, Achsen, Texte, Schwellenwerte
    - o Titel des Diagramms
    - o Beschriftung der X- und Y-Achse
    - o Auswahl des Kurvendarstellungstyps aus drei verfügbaren Typen:
        - Liniengrafik: genutzt für „Eigenschaften“ in MICROSESAME (mit Möglichkeit von 3 definierten Schwellenwerten, jeweils mit Bezeichnung und Wert)
        - Balkendiagramm: erstellt auf Basis einer SQL-Abfrage
        - Kreisdiagramm (Tortendiagramm): erstellt auf Basis einer SQL-Abfrage

27. GATEWAYS & KONNEKTOREN

MICROSESAME CUBE ist ein Sicherheits-Hypervisor (Überwachungssoftware), der sich mit einer Vielzahl von Softwarelösungen, Hardware, Systemen und Verzeichnissen integriert und verbindet, um eine umfassende zentrale Lösung, größtmögliche Offenheit und einfache Anpassungsfähigkeit an zukünftige Anforderungen zu bieten. MICROSESAME CUBE ermöglicht es somit, ein großes Ökosystem an Funktionen und Bereichen zu verwalten und Alarme sowie Störungen dieser Systeme mit den in den entsprechenden Kapiteln beschriebenen Möglichkeiten der Lösung zu überwachen: MONITORING & ÜBERWACHUNG, VIDEOÜBERWACHUNG, EINBRUCHMELDETECHNIK



MÖGLICHE CONNECTOREN UNSERES SYSTEMS MICROSESAME:

- Benutzer- und Besucherdatenbanken: Web Services API REST, TXT/CSV-D
- nOperatorenverwaltung A.D: LDAP, Windows-Authentifizierung (SSO => Desktop: NTLM, Web: SAMLv2)
- I.T-Supervisoren: SNMPv3 (über TILLYS CUBE UTL)
- Hypervisoren / Gebäudeleittechnik (GLT): OPC UA, MODBUS IP
- Automaten, Fremdsysteme (Brandschutz usw.), UGIS: MODBUS IP
- Videomanagementsysteme (VMS): VMS-SDK, TEXT-/ASCII-Gateway

BEISPIELE REALISIERTER SCHNITTSTELLEN

- Building-Managementsystem : PRYSM, PC VUE, PANORAMA,….
- Raum- und Ressourcenreservierung: ASW, Planitec usw.
- Lkw-Logistikmanagement: EASYPROG, STACKR
- Videomanagement: MILESTONE, GEUTEBRUCK, GENETEC (siehe Kapitel VIDEOÜBERWACHUNG)
- Integration des MILESTONE ACCESS CONTROL Plug-ins zur Überwachung der TIL-Zutrittskontrolle in der X-PROTECT-Oberfläche von MILESTONE (siehe Kapitel VIDEOÜBERWACHUNG)

- ► Sprechanlagen: COMMEND über IP / Import der Teilnehmer, Anrufe, Anrufbenachrichtigungen (mit Unterscheidung zwischen normal und dringend), Nachtanrufweiterleitung, Möglichkeit zur Serververbindung (siehe Kapitel INTERPHONIE)
- ► DEISTER-Schlüsselschränke: Synchronisation der Identifizierten, Import der Zustände über die Software COMMANDER 4
- ► Perimetersicherung: SORHEA über das MAXIBUS-Protokoll von SORHEA
- ► Brandmeldezentralen über MODBUS-Protokoll
- ► Videomatrizen und Multiplexer: AVIGILON, Sprechanlagen STENTOFON über ASCII-, TXT-Protokolle
- ► Biometriesysteme: MORPHO von IDEMIA (siehe Kapitel BIOMETRIE)
- ► Aufzugssteuerungen: SCHINDLER, KONE, OTIS (native Konnektoren) Bereitschaftsmanagement: ME
- ► MOGUARD
- ► Telekommunikationssysteme: AASTRAAlleinarbeiterschutzsysteme
- ► HR-Verzeichnisse: CANIF der SNCF, BDRS der Société Générale, STITCH der DGAC usw.
- ► SMTP-Mailserver für E-Mail-Versand

BIOMETRIE

- ► MICROSESAME ist in der Lage, biometrische Leser verschiedener Marken und Serien zu verwalten: EVOLUTION CUBE, IDEMIA, STID.
- ► Für die Marken EVOLUTION CUBE TIL und STID:
  - Leser der Serien EVOLUTION CUBE TIL und ARCHITECT
  - TIL hat die biometrischen Leser im transparenten Modus mit einem von der ANSSI zertifizierten Protokoll integriert.
- ► Biometrische Lösung mit Badge + Biometrie (1:1: Die Fingerabdrücke befinden sich auf dem Ausweis jeder Person und nicht in einer zentralisierten Datenbank. In diesem Fall erfolgt die Erfassung der Fingerabdrücke über die Software STID SECARD BIO, die diese in den Badge beschreibt.

Für den Hersteller IDEMIA (ex MORPHO) :

Leser der Serien SIGMA (Fingerabdruckleser) und MORPHOWAVE COMPACT (kontaktlose Fingerabdruckerfassung im Vorbeigehen)

► Die biometrische Erfassung erfolgt über die Software MORPHOMANAGER von IDEMIA, die direkt über einen Favoriten-Link in der Benutzerkarteikarte von MICROSESAME aufgerufen werden kann.

► TIL hat die Schnittstelle MORPHO-BRIDGE von MORPHOMANAGER integriert, um die in MICROSESAME erstellten Personendatensätze und IDs automatisch an MORPHOMANAGER zu übermitteln und eine doppelte Dateneingabe zu vermeiden.

► Biometrische Lösung mit:

- Badge + Biometrie (1:1), konform mit der Empfehlung CNIL AU52: Die Fingerabdrücke werden auf dem persönlichen Badge gespeichert und nicht in einer zentralen Datenbank. Die Erfassung erfolgt über MORPHOMANAGER, das die Daten in den Ausweisen schreibt.
- Nur Biometrie (1:N), unterliegt strengeren Vorgaben gemäß CNIL AU53, da die Fingerabdrücke in einer zentralen, besonders geschützten Datenbank gespeichert werden müssen (gemäß DSGVO). In diesem Fall werden die Fingerabdrücke über MORPHOMANAGER direkt an die biometrischen Leser übertragen

STANDARDISIERTE IT-PROTOKOLLE

Es ist möglich, industrielle Automatisierungsgeräte oder Gebäudeleittechniksysteme über das Protokoll MODBUS IP (Master oder Slave) zu integrieren. MICROSESAME unterstützt zudem das sichere OPC UA-Protokoll (nur Servermodus). Diese Protokolle sind weit verbreitet in der Automatisierungswelt und ermöglichen die Anbindung an GTC- oder GLT-Systeme.

Beispielkompatibilität:

ÜBERGEORDNEDETE SYSTEMÜBERWACHUNG

- Prysm Appvision
- Codra Panorama
- Wonderware
- PCVUE

AUTOMATEN UND BRANDMELDEZENTRALEN, DIE MIT MODBUS IP ODER OPC KOMPA

- Schneider
- DIRIS…

API REST & WEBSERVICES

TIL stellt seinen Kunden und Technologiepartnern eine API (Application Programming Interface) zur Verfügung.

Diese API ermöglicht es, auf einfache Weise Schnittstellen zwischen MICROSESAME und anderen Anwendungen zu entwickeln, indem Daten aus der Datenbank des TIL-Überwachungssystems (Supervisors) ausgetauscht werden.

Die API definiert genau die Methoden, mit denen Softwareentwickler Programme erstellen können, die in ihren eigenen Anwendungen mit MICROSESAME interagieren (Aufruf von Funktionen oder Daten).

Die Kommunikation zwischen MICROSESAME und Drittanwendungen erfolgt über das Netzwerk mittels Web Services. Das bedeutet, dass die API das HTTPS-Protokoll verwendet, das am häufigsten verwendete Kommunikationsprotokoll.

Hinweis: Der Zugriff auf die MICROSESAME-API ist an die Unterzeichnung einer Geheimhaltungsvereinbarung (NDA) gebunden).

BEISPIELE FÜR DATENAUSTAUSCH PER REST-API MIT ANDEREN FACHANWENDUNGEN:

- Die bereits umgesetzten Schnittstellen betreffen sowohl bestehende und kommerzialisierte Softwarelösungen als auch speziell von unseren Kunden entwickelte Anwendungen:
- Softwarelösungen zur spezifischen Besucherverwaltung (QR-Code usw.) oder personalisierte Intranets mit Terminverwaltungsoberfläche (Identifizierte und Identifikatoren)
- Software zur Buchung von Besprechungsräumen ASW (Identifizierte)
- Anwendung zur Buchung von Zimmern (Identifizierte und Identifikatoren)
- Anwendung zur Berechnung der Anwesenheitszeiten (Benutzer und Historie der Ausweislesungen)
- Anwendung zur Konferenzempfangsverwaltung (Identifizierte und Historie der Ausweislesungen an mobilen Lesern)
- Software zur Abrechnung von Kantinennutzung (Identifizierte und Historie der Ausweislesungen)
- Software zur Nachverfolgung von Logistikvorgängen eGestrack (von STACKR) für Logistikplattformen (Identifizierte, Identifikatoren und Historie der Ausweislesungen)
- Anwendung zur Verwaltung einer Rail/Road-Transferplattform (Identifizierte und Historie der Lesung von Kfz-Kennzeichen)
- Schnittstelle zwischen MICROSESAME und den Aufzügen von KONE (Identifizierte und Identifikatoren)
- Schnittstelle zwischen MICROSESAME und der Videomanagement-Software TEB

SCHNITTSTELLEN ZU MANAGEMENT-, PERSONAL- UND VERZEICHNISANWENDUNGEN…

In vielen Fällen ist es sinnvoll, Daten zwischen MICROSESAME und Datenbanken auszutauschen, die Mitarbeiter oder Benutzer des Unternehmens verwalten (HR-Datenbanken, Verzeichnisse usw.Automatiser Die Automatisierung der Synchronisation dieser Datenbanken mit dem Zutrittskontrollsystem ist umso nützlicher, je mehr Badges im Umlauf sind, denn sie ermöglicht:

- Die Vermeidung doppelter Eingaben (erhebliche Zeitersparnis und höhere Genauigkeit)
- Die automatische Zuweisung von Zugangsrechten an Personen anhand von Regeln (Aliasnamen), die projektbezogen definiert werden (z. B. basierend auf Abteilung, Funktion usw.)
- Die sofortige und automatische Berücksichtigung von Personalbewegungen (Eintritte und Austritte), was die Sicherheit erheblich erhöht.

Mit den von TIL angebotenen Schnittstellen, WEB SERVICES API REST oder MS-SYNCH (CSV), kann die automatische Aktualisierung der Daten so parametriert werden, dass sie zu festen Zeiten oder bei jeder Änderung der Quelldatei erfolgt.
Selbstverständlich bleibt auch eine manuelle Synchronisierung auf Anfrage möglich.

MICROSESAME unterstützt die Synchronisation mit mehreren unterschiedlichen Quellen, wobei jede Quelle eine eigene spezifische Synchronisationskonfiguration haben kann.

MICROSESAME kann sich auch in einen Datenlieferanten verwandeln, um anderen Systemen (z. B. Catering, Druckdienste, Schlüsselschrankverwaltung usw.) die von der Zutrittskontrolle und der Mehrfachanwendungscodierung erzeugten Personaldaten zur Verfügung zu stellen – über WEB SERVICES oder MS_RSYNC (CSV).
MICROSESAME ist in der Lage, verschiedene Systeme mit jeweils angepassten Daten für jede Drittanwendung zu versorgen.

Dadurch können die Datenbanken der Drittsysteme automatisch aktualisiert werden und es entfällt die Notwendigkeit für Benutzer, sich bei jedem System separat zu registrieren und ihre Badges einzeln einpflegen zu lassen (keine doppelten Eingaben mehr)

NACHRICHTENFUNKTION

MICROSESAME verfügt über eine integrierte Funktion zum Versand von E-Mails bei Alarmen über ein SMTP-Nachrichtensystem. Wird im System ein Alarm (Einbruch, Zutrittskontrolle, technische Alarme) erkannt, kann automatisch eine E-Mail an definierte Empfänger versendet werden.
Außerdem ist es möglich, nach der Ausführung eines Berichts mit dem universellen Abfragewerkzeug dessen automatischen Versand per E-Mail auszulösen. Hinweis: Der Versand von SMS ist in MICROSESAME nicht direkt integriert und erfordert den Einsatz einer Drittanbieterlösung.

INTER-SYSTEM-KOMMUNIKATION

MICROSESAME bietet eine Schnittstelle (ISMS), die den Datenaustausch zwischen mehreren unabhängigen MICROSESAME-Systemen über ein IP-Netzwerk (UDP-Protokoll) ermöglicht. Der Datenaustausch basiert auf Eigenschaftsnamen. MICROSESAME bietet eine Schnittstelle (ISMS), die den Datenaustausch zwischen mehreren unabhängigen MICROSESAME-Systemen über ein IP-Netzwerk (UDP-Protokoll) ermöglicht. Der Datenaustausch basiert auf Eigenschaftsnamen.

Anwendungsbeispiel: Ein Kunde betreibt mehrere Standorte, von denen jeder über einen eigenen Server und einen Sicherheitsarbeitsplatz (PCS) verfügt. Über ein standortübergreifendes IP-Netzwerk kann:

- ein Standort die Rolle der zentralen Alarmzusammenfassung (zum Beispiel am Wochenende) übernehmen,
- ein Client-PC betrieben werden, der sich (jeweils einzeln) mit allen Servern der verschiedenen Standorte verbinden kann

Wenn also ein wichtiger Sammelalarm vom Server X an den zentralen Server gesendet wird, erhält der zentrale Operator diesen Alarm auf seinem Arbeitsplatz am Standort.
Er wird dann die Anweisung haben, sich über einen allgemeinen Client-PC mit dem Server X zu verbinden und den Alarm unter Zugriff auf alle verfügbaren Details zu bearbeiten.

28. BANKING

Die Absicherung einer Bankfiliale muss klar definierten Prozessen folgen und spezielle Zutrittskontrollfunktionen nutzen. Angesichts der Risiken von Überfällen, erzwungenem Zutritt oder interner Sabotage müssen der Zugang zu Sicherheitsbereichen und das Öffnen der Tresore durch starke Authentifizierungslösungen (z. B. doppelte Identifikation) und anhand vordefinierter Szenarien (Zeitverzögerungen, Aktionssequenzen usw.) abgesichert werden.
Die eingesetzten Lösungen müssen es ermöglichen, komplexe Automatismen einfach, flexibel und skalierbar zu konfigurieren.

Komplette lokale Konfiguration einer Bankfiliale ohne Server, mit Export der Konfiguration zur späteren Übernahme in den Zentralserver und zur Vervielfältigung auf X weitere Filialen.

- Ausstattung der Filialen mit speziellen und vereinfachten Benutzeroberflächen: LED-Farben der Leser anpassbar je nach Status, Ausweisleser mit Display für Zeitverzögerungsanzeige und farblicher Anzeige des Zustands „scharf“/„unscharf“ der Einbruchmeldeanlage.
- SAS-Steuerung und Zutrittseinheitlichkeit zur ETS (gesicherter Technikraum)
  - Es darf jeweils nur eine Tür zwischen einem Tresorraum und der ETS geöffnet sein.
  - Der Zutritt zur ETS ist verboten, wenn ein Tresor geöffnet ist und/oder sich bereits eine Person im Bereich befindet.
  - Mehrere Personen sind erlaubt, jedoch jeweils nur Angehörige einer einzigen Benutzergruppe (Einheitlichkeit der Benutzerpopulation).
    - Verwaltung und Steuerung der Tresorzugriffe über das 7’’ VAULTYS-Farb-Touchdisplay:
  - Identifikation per Code, Ausweis oder Ausweis + Code.
  - Zulassung der Öffnung jeweils nur eines Tresors gleichzeitig.
  - Anzeige der laufenden Zeitverzögerung.
  - Filterung der zugänglichen Tresore und Anpassung der Zeitverzögerungen je nach Benutzer, Zeitfenster oder anderen Bedingungen.
  - Individuell konfigurierbare bedingte oder sequentielle Verknüpfungen:
  - Kombination von Aktionen wie Zutrittsausweisprüfung, Scharf-/Unscharfschaltung der Einbruchmeldeanlage, „Alles in Ordnung“-Taste usw.
  - Unterschiedliche Abläufe je nach Art des Zutrittsberechtigten (z. B. Werttransportunternehmen, Mitarbeiter, Vorgesetzter)

29. CUBE SOFTWARE- UND HARDWAREPRODUKTE

CUBE: ZUKUNFTSSICHERE LÖSUNG FÜR DIE ZUTRITTSKONTROLLE