MICROSESAME CUBE

SYSTEM-DETAILBESCHREIBUNG

Version 2023.1 – 21. März 2023

TIL TECHNOLOGIES
by HIRSCH

INHALTSVERZEICHNIS

MICROSESAME IN ALLER KÜRZE	3
BSI-ANERKANNTE ANSSI-ZERTIFIZIERTE ARCHITEKTUR	4
HOHE FUNKTIONALITÄT FÜR GEBÄUDESICHERHEIT UND TECHNIK	12
SYSTEMLEISTUNGEN	17
DSGVO	19
USER-VERWALTUNG	21
MEHRFACHSTANDORTE UND -MANDANTEN	23
ZUTRITTSKONTROLLE	25
BESUCHERVERWALTUNG	31
„OSS“-OFFLINE-ZUTRITTSKONTROLLE	39
„CLIQ“OFFLINE-ZUTRITTSKONTROLLE	41
AUSWEISKODIERUNG	42
AUSWEISPERSONALISIERUNG	43
MONITORING UND ÜBERWACHUNG	44
VIDEOÜBERWACHUNG	52
EINBRUCHMELDETECHNIK	56
GEGENSPRECHANLAGEN	60
NOTFALLMANAGEMENT-UNTERSTÜTZUNG (NOMAN)	62
RUHEZEITENKONTROLLE	63
STRECKENMANAGEMENT	64
VERLÄUFE, SUCHEN, BERICHTE UND PROTOKOLLIERUNGEN	66
GATEWAYS UND KONNEKTOREN	71
BANKING	77
CUBE SOFT- UND HARDWARE-SORTIMENT	78

MICROSESAME IN ALLER KÜRZE

MICROSESAME CUBE

MICROSESAME integriert als zentrale Managementlösung alle Gewerken der **Gebäudesicherheit und -technik** (ZuKo, EMT, Video, GLT…)
Es ermöglicht eine einheitliche Überwachung aller elektronischen Gebäudeinformationen.

Die Steuerung der verschiedenen Funktionen über eine gemeinsame Grafikschnittstelle erleichtert die Nutzung und sorgt für effizientes Eingreifen.
Da die Interaktionen zwischen verschiedenen Systemen vollständig automatisiert werden können (Aktionen bei Ereignis), wird eine hohe Verarbeitungsgeschwindigkeit erreicht.

Das System besteht aus einer Software einerseits und IP-Zentralen andererseits, an welchen alle Arten von Endgeräten angeschlossen sind.

MS ENTRY

MS PRIME

MS HIGH SECURE

Die Systemarchitektur basiert auf marktüblichen Standards, die Langlebigkeit und -skalierbarkeit zu geringen Kosten garantieren.

Durch die Integration von SDKs oder IT-Protokollen (MODBUS und andere...), kann **MICROSESAME** Informationen aus fremden Systemen (Bsp. Galaxy-EMZ) überwachen und als Hypervisor von digitalen Video Management System beispielsweise agieren.
Es kommuniziert auch direkt mit industriellen speicherprogrammierbaren Steuerungen (API) und anderen Sicherheitseinrichtungen über Gateways (OPC, Text...).

Über die Leistungsbeschreibung von MICRO-SESAME CUBE hinaus wird am Ende dieses Dokuments auf das in 3 Geheimhaltungsstufen einsortierte CUBE Soft- und Hardwareangebot eingegangen. Dieses als „ENTRY“, „PRIME“ und „HIGH SECURE“ genannte CUBE-Produktangebot bietet erhöhte

- Einfachheit und Leistung: Der gesamte Softwareumfang von TIL ist ab der Basislizenz mit dem ersten Leser bereits erhältlich. Es gibt nur ein Zentralenmodell für alle Funktionen und alle Optionen,
- Sicherheit: Native ANSSI-konforme Cybersicherheit mit vollständigem Systemschutz,
- Skalierbarkeit: Sicherheitsstufe durch einfaches Software-Upgrade erhöht, ohne notwendigen Hardwarewechsel.

BSI-ANERKANNTE ANSSI-ZERTIFIZIERTE ARCHITEKTUR

CYBERSICHERE HARD- UND SOFTWARE-ARCHITEKTUR

Der Aufbau der **MICROSESAME**-Architektur besteht aus folgenden Bestandteilen:

- Einem Server, der sowohl als Konfigurations- wie auch als Systemanwender-Arbeitsplatz dient und in einer Standard-Windows-Umgebung läuft. Die Implementierung ist einfach und benutzerfreundlich.

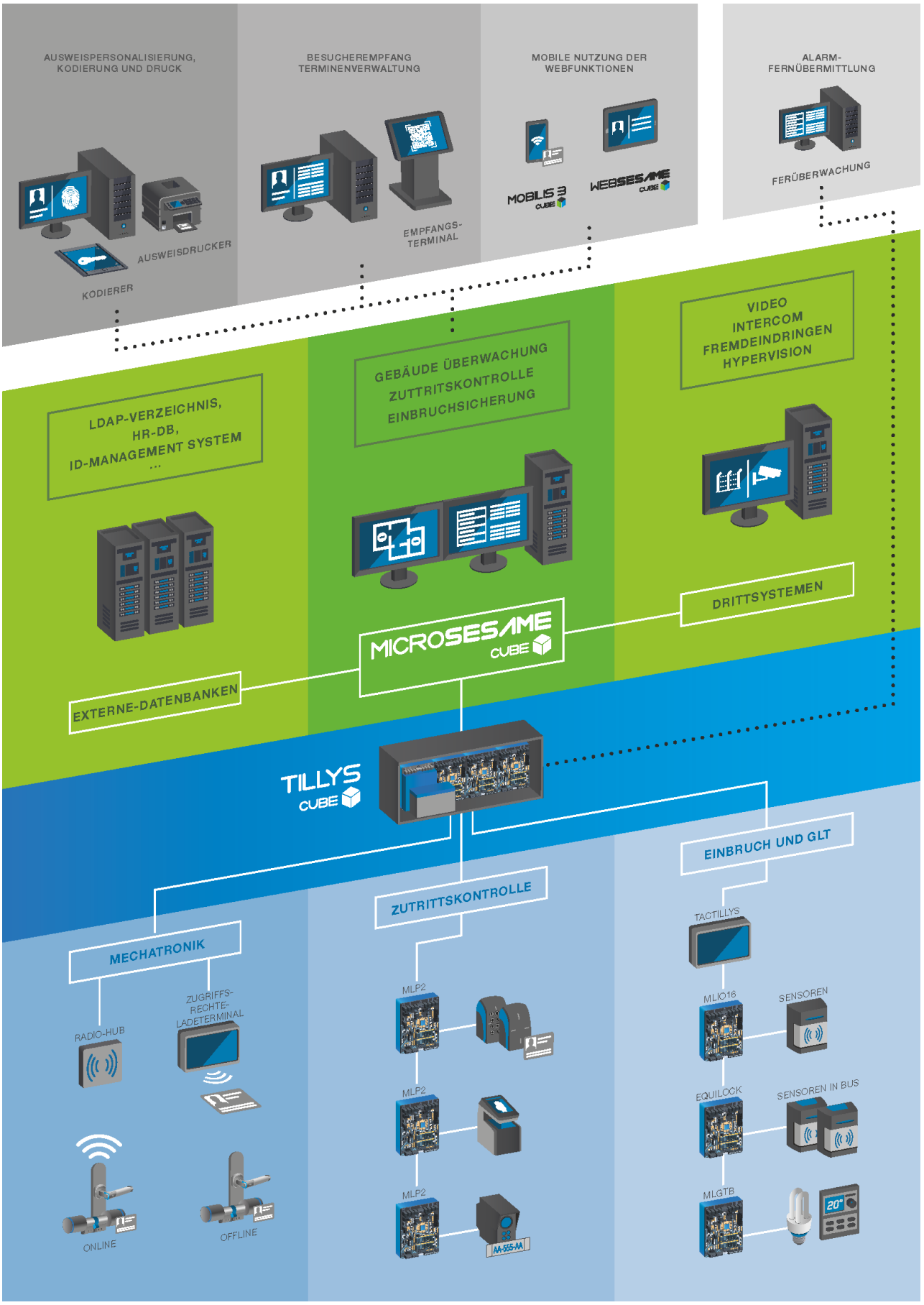
- Einem IP-Netzwerk (LAN oder WLAN), in dem der Server mit Benutzer-Arbeitsplätzen (**MICROSESAME-** und **VISIOSESAME**-Heavy-Clients, Thin-Clients via RDP/Citrix oder **WEBSESAME-**WEB-Clients auf PCs, Smartphones bzw. Tablets), und schließlich TIL-Zentralen (ZuKo, EMT, GLT) sowie mobilen Handgeräten (MOBILIS-Leseeinheitenüber WLAN) in Verbindung steht.

    - Über Netzwerk kann die **MICROSESAME**-Lösung auch mit kundeneigenen Fremdsystemen (Active Directory, I.T SNMP-Supervisor, HR-Datenbank…) oder Drittanwendungen (VMS-Server, Videorekorder, OPC-Hypervisor, Automaten via MODBUS…) kommunizieren.

- Autonomen und multifunktionalen TIL-Zentralen) in einem IP-Netzwerk zur Steuerung von Zutrittskontrolle, Einbruch und Gebäudetechnik

- Alarm-Schalteinrichtungen, mechatronischen Online-Lösungen, Erweiterungsmodulen (Türmodulen, Ein-/Ausgangsmodulen...), die an die sekundären Busse der Zentrale nach Wahl als dezentrale oder zentrale Installation angeschlossen sind

- Leseeinheiten, Tastaturen für Zutrittskontrolle, Sensoren (Kontakten, Einbruchmeldern...), kontrollierten Zutrittseinrichtungen (Schlössern, Schranken, Drehkreuzen…), Aktoren (Sirenen, Beleuchtung...), die mit diesen Erweiterungsmodulen verbunden sind

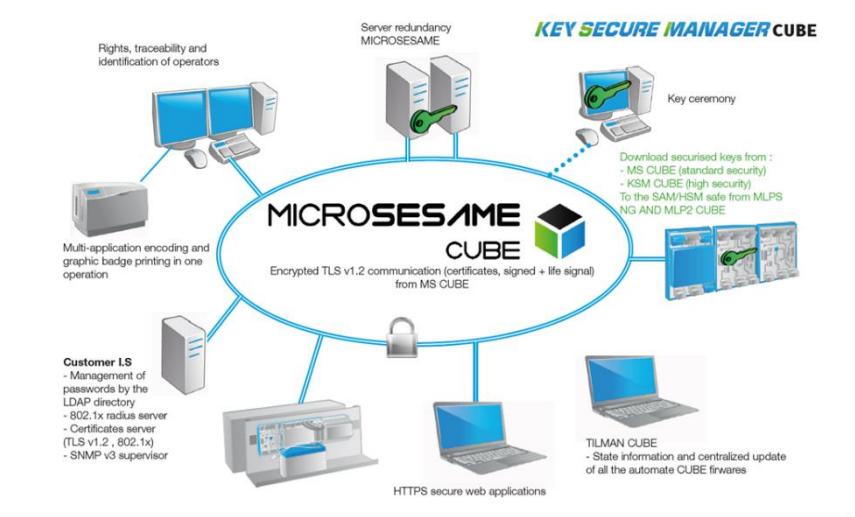

AUSWEISPERSONALISIERUNG, KODIERUNG UND DRUCK
KODIERER
AUSWEISDRUCKER
BESUCHEREMPFANG TERMINENVERWALTUNG
EMPFANGS-TERMINAL
MOBILE NUTZUNG DER WEBFUNKTIONEN
MOBILIS 3.0 CUBE
WEBSESAME CUBE
ALARM-FERNÜBERMITTLUNG
FERÜBERWACHUNG
LDAP-VERZEICHNIS, HR-DB, ID-MANAGEMENT SYSTEM ...
GEBÄUDE ÜBERWACHUNG ZUTTRITSKONTROLLE EINBRUCHSICHERUNG
VIDEO INTERCOM FREMDEINDRINGEN HYPERVISION
DRITTSYSTEMEN
EXTERNE-DATENBANKEN
MICROSESAME CUBE
TILLYS CUBE
MECHATRONIK
RADIO-HUB
ZUGRIFFS-RECHTE-LADETERMINAL
ONLINE
OFFLINE
ZUTRITTSKONTROLLE
MLP2
MLP2
MLP2
EINBRUCH UND GLT
TACTILLYS
MLIO16
SENSOREN
EQUILOCK
SENSOREN IN BUS
MLGTB

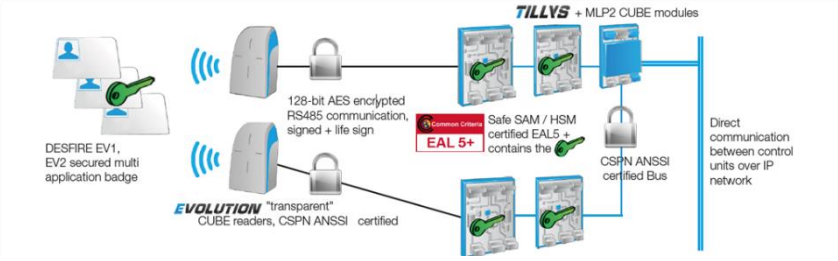
CYBERSICHERE LÖSUNG DURCH ANSSI-ZERTIFIZIERTE UND QUALIFIZIERTE CSPN-ARCHITEKTUR 1

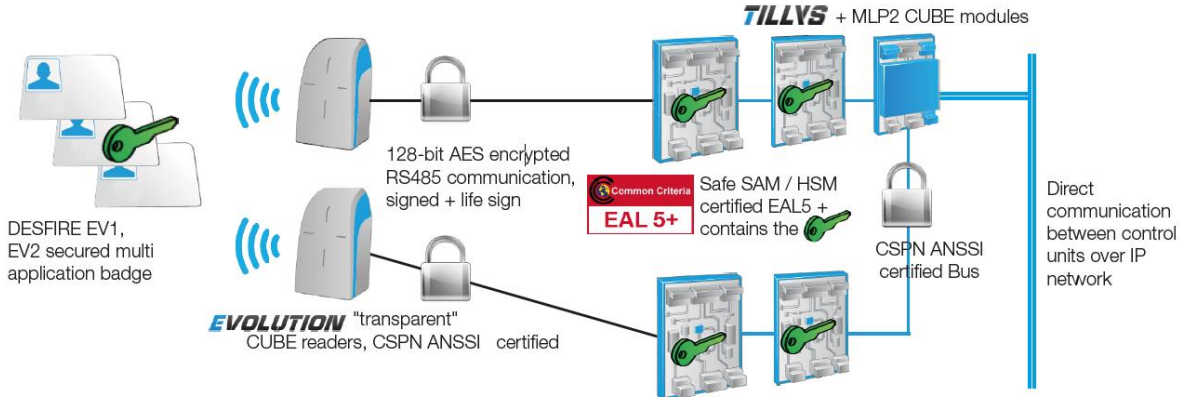
Standorte schützen, reicht nicht mehr aus. Ebenso wichtig ist die Einrichtung von Schutzmechanismen gegen externe und interne Bedrohungen für das Sicherheitssystem selbst.

An der gesamten **MICROSESAME**-Architektur – vom Ausweis bis zum Server - wurden elektronische und IT-Schutzvorrichtungen implementiert, die einem Missbrauch oder einem unerlaubten Zutritt vorbeugen.

Um die oberste Stufe der Sicherheit und Cybersicherheit zu garantieren, wurde unsere Lösung ANSSI-zertifiziert und nach der von ANSSI empfohlenen Architektur 1 (transparente Leseeinheite) qualifiziert.







MICROSESAME-CUBE, Hardware der CUBE-Serie (**TILLYS CUBE**, **ML-**Erweiterungsmodule) und **die „transparenten“ EVOLUTION-Leseeinheiten**besitzen folgende Cybersicherheitseigenschaften und -Leistungsmerkmale:

- Eine offizielle ANSSI-Zertifizierung und -Qualifizierung, die für bestimmte regulierte Standorte (wichtige, essenzielle Infrastrukturen...) gemäß geltenden Richtlinien Pflicht und für alle sensiblen Standorte dringend empfohlen sind
- Eine ANSSI-Qualifikation, welche die Aufrechterhaltung dieser Sicherheitsstufe im Laufe der Zeit weitersichert (TIL TECHNOLOGIES-Verpflichtung gegenüber ANSSI)
- Eine End-to-End- sichere Lösung, vom Ausweis bis zum Server
- Die gesamte Kommunikation in einem gesicherten TLS v1.3 IP-Netzwerk mit Zertifikaten zwischen Server und Zentralen einerseits und Client-Arbeitsplätzen andererseits

CUBE-WANDGEHÄUSE FÜR EINE GESCHÜTZTE ELEKTRONIK:

- Fehler- und Manipulationsschutz: Kabeltrennung, Schranköffnung, Kommunikations- und Spannungsfehler (Netzausfall, Batterieschwäche, Ladegerät); Fehler- und Sabotageschutz dank symmetrischer Eingänge, Ausgänge und RS485-Bus; Kurzschluss-, Überspannungs- und Verpolungsschutz

AUTOMATISIERTE TILLYS CUBE-ZENTRALEN MIT:

- Eingebettetem HTTPS-Webserver zur lokalen Konfiguration
- 802.1X (Radius) und SNMPv3-Kompatibilität zur Überwachung von Systemzuständen und Tätigkeitsalarmen über die IT-Abteilung des Endkunden
- Modulare 3er RS485-Feldbus-Architektur, ANSSI-zertifiziert und AES 128 Bit-gesichert, an denen die Erweiterungsmodule für Zutrittskontrolle- sowie Einbruchschutz angeschlossen sind und folgende Vorteile bringt:
  - Kostensenkung durch bestmögliche Wiederverwendung der vorhandenen Verkabelung
  - Zertifizierung der vorhandene Verkabelung
  - Wahl zwischen einer zentralen oder dezentralen Modularchitektur
- Schutz vor Denial-of-Service (DoS)-Angriffen durch die Firewall

MLP-TÜRMODULE MIT:

- Gesicherter RS485-AES128-Bit-Kommunikation bei transparenten Leseeinheiten
- Nativ integrierter ANSSI EAL5 + zertifizierter HSM-Komponente, die als Krypto-Prozessor und Safe dient und die Ausweisschlüssel für „Zutrittskontrolle“ sicher aufbewahrt
- Applets (Konfiguration) zur Anpassung an die Ausweis-Charta des Kunden und zur Steuerung der LEDs und Summer von transparenten Leseeinheiten. Benutzerberechtigungen sichern den Zugriff auf die Konfiguration der MLP-Applets

RFID-LESEEINHEITE:

- ANSSI-zertifizierte TastaturLeseeinheitennach Architektur 1, die als „transparente Leseeinheite“ bezeichnet werden (kein Ausweisschlüssel im Leseeinheit selbst gespeichert) zur Verwaltung von hochsicherer DESFIRE-Ausweise
- In ANSSI-zertifizierten SCCPv1-Protokollen verwaltete transparente biometrische EVOLUTION Leseeinheiten(ab MLP-Modulen SCCPv2 ANSSI-zertifiziert), welche neue Zustände (Ausweis OK, Fingerabdruck jedoch nicht, Zeitüberschreitung) und den Fingerabdruck unter Zwang verwalten

AUSSCHLIESSLICH DER ENDKUNDE BEHÄLT DIE KONTROLLE ÜBER SEINE SCHLÜSSEL:

- Für alle Ausweisanwendungen (Zutritt, Kantine...), die mit Hilfe einer speziell dafür vorgesehene HMI (Mensch-Maschine-Schnittstelle) eingegeben oder erstellt werden – dem sogenannten **KSM** -und einfach in einem digital gesicherten AES256 Bit-Behälter in **MICROSESAME** gespeichert werden (Schlüsselzeremonie). Keiner dieser Schlüssel ist für Dritte, die entweder das System entwerfen, integrieren oder warten jemals sichtbar. Für den Integrator und den Endkunden ist nur 1 Schlüsselzeremonie notwendig

SCHLÜSSEL UND APPLETS:

- Gesicherter, zentralisierter Schlüssel- und Applets-Download vom Server oder **KSM** auf die HSM-Module der MLP, damit die Schlüssel verteilt und gemäß ANSSI-Vorschrift in allen Modulen über das Zentralsystem ausgetauscht werden
- Durch das Prinzip der Schlüsseldiversifikation nach AN10922-Standard kann der Endkunde unterschiedliche Schlüssel für einen Ausweis haben und dessen Verhalten über ein anpassbares Padding definieren

CUBE-ARCHITEKTUR:

- **TILMAN-CUBE**, das dedizierte Programm für **MICROSESAME**, bietet eine zentralisierte Ansicht des Zentralen-Parks der CUBE-Baureihe (Zentralen, Module), um Firmware-Versionen über globale Downloads auszulesen und zu aktualisieren. So können problemlos von einer zentralen Arbeitsplatz aus nicht nur korrektive- und entwicklungstechnische Wartungen durchgeführt, sondern auch die Inbetriebnahme durch Tests und Diagnosen der Verkabelung und Meldereingänge unterstützt werden
- Die Sicherheit des für die Zutrittskontrolle zertifizierten TILLYS CUBE ist auch bei Einbruch aktiv und dient als cybersichere Einbruchmeldezentrale
- Die Firmware der Zentrale der CUBE-Reihe ist signiert und seine Integrität somit gewährleistet.

ERHÖHTE SICHERHEIT

- Durch Entfernen des Reverse-DNS-Codes (Auswirkung auf den Inhalt von Zertifikaten)
- Durch in der Datenbank mit einem gesalzenen SHA-512-Hash aus 512 zufälligen Zeichen geschützte Benutzerpasswörter
- Durch das gegen CSRF-Angriffe geschützte **WEBSESAME**-Portal
- Durch Web-Requester mit Bibliothekanfragen zu verdächtigem Verhalten (Mehrfachversuche, Zugriff auf verbotene Bereiche...). Liste mit automatischem Bericht editierbar.

ANPASSUNG AN IT-UMGEBUNG

Je nach Systemgröße gelten bestimmte Maschinen- und Softwareempfehlungen.
MICROSESAME hält mit Fortentwicklungen der Betriebssystem- und Datenbankversionen Schritt und bleibt mit den neuesten IT-Umgebungen kompatibel.
Vor jeder Systeminstallation oder -migration kann auf spezifische, regelmäßig aktualisierte und bei Ihrem bekannten TIL-Ansprechpartner erhältliche Dokumentation zurückgegriffen werden.

KOMPATIBEL MIT DEN NEUESTEN BETRIEBSSYSTEMEN UND DATENBANKEN:

- Server: von Windows 10 PRO oder Enterprise (64-Bit) für kleine Systeme auf Windows Server 2019 Standard oder Essential Edition (64-Bit)
- Heavy-Client: Windows 10 Pro oder Enterprise 64-Bit
- Datenbank: SQL-Server 2016 bis 2019 (64 Bit)

FÜR „THIN-CLIENT"-INFRASTRUKTUR GEEIGNET:

- Kompatibilität mit RDS (ex TSE)/Citrix-Lösungen
- Keine Installation der **MICROSESAME**-Anwendung auf Arbeitsplätzen nötig
- Verbindung von jeder Arbeitsplatz im Netzwerk aus
- Floating-Lizenz-Betrieb / gleichzeitige Verbindungen

Windows **RDS**

WEBSESAME-WEBPORTAL FÜR ZUGELASSENE FUNKTIONEN IM KUNDENINTRANET:

- Je nach Format (Smartphone, Tablet, PC) selbstadaptive Bildschirme (Auflösung und Ausrichtung)
- Zur vereinfachten Nutzung auf Tablets und Smartphones optimierte Ergonomie (Auto-Ausfüllen von Feldern, Bildanzeige, Check-Buttons)
- Für breite Populationen verfügbare WEB-Funktionen:
  - WEB-TERMINE: Terminen- und Besucherverwaltung
  - WEB-BENUTZER: Benutzer-Verwaltung
  - WEB-BERICHTE: Berichterstellung, Status-/Alarmverlauf
  - WEB-ALARME: Gesamtübersicht aktueller Alarme
  - WEB-EREIGNISTICKER: Ereignisliste von Zutrittskontrolle, Technik und Systemmanagement
  - WEB-BEREICHE: Identifikation und Anzahl der sich in einem Bereich befindlichen Personen

WEBSESAME CUBE

KOMPATIBEL MIT KLASSISCHER VIRTUELLER VMWARE-UMGEBUNG:

- Serverbündelung, Energieeinsparungen
- Softwarelizenz mit dieser Umgebung kompatibel
- Auf einem bestimmten physischen Computer oder im Rechenzentrum
- Redundanz durch der VM-Umgebung möglich

vmware

Microsoft Azure

FÜR BELIEBIGE ARCHITEKTURTYPEN UND NETZWERKE OFFEN:

- Architektur von Drittanbietern (Datenbanken, Anwendungsserver, WEB-Server)
- VPN, VLAN-kompatibel
- E-Mail/SMTP-Übertragungen,
- TILLYS-CUBE Zentrale kompatibel mit 802.1x, SNMPv3, IPv6-ready, Hostname

HARDWARE- / SYSTEMREDUNDANZ:

- Mit der Redundanzlösung SAFEKIT kompatibel (Hot Spare)
- Vorkonfigurierte **MICROSESAME**-Schnittstelle

VEREINFACHTES UND INTEGRIERTES INSTALLATIONS-, MIGRATIONS-, WIEDERHERSTELLUNGSPAKET:

- Einfache Installation von MICROSESAME Server- und Client-Arbeitsplätzen mit allen im vorgesehenen Komponenten
- Migrationstools für Server und Client-Arbeitsplätze erhältlich
- Halbautomatisches Updaten von Heavy-Client-Arbeitsplätzen vom Server aus
- Sämtliche Systemanwendungen betriebsbereit
- Speichern, automatisches Datenbank-Backup nach vordefiniertem Pfad. Wiederherstellungstool

BENUTZERRECHTEVERWALTUNG IN CLIENTANSICHT ÜBER LDAP

- Siehe entsprechendes Kapitel

HOHE VERFÜGBARKEIT UND STARKE LEISTUNGEN

Die MICROSESAME-Architektur ist so konzipiert, dass sie eine stets hohe Verfügbarkeit und starke Leistungen garantiert:

- Autonomer Betrieb ohne Ethernet-Netzwerk und/oder Server jeder **TILLYS CUBE** Zentrale einschließlich ihrer Erweiterungsmodulen und Peripherien. Dadurch bleibt bei Netzverbindungsabbruch zu **MICROSESAME** der Verlauf der letzten 10.000 Ereignisse gespeichert und wird nach Wiederherstellung der Verbindung automatisch hochgeladen.
- Direkte serverunabhängige **TILLYS CUBE**-Zentralen-Interkommunikation mittels IP (Anti-Passback auch dann gewährleistet)
- Die **TILLYS CUBE** Zentrale verarbeitet zahlreiche Ausweisprüfungen zeitgleich in weniger als 500 mS. Dies gilt sogar mit transparenten Leseeinheiten und Hochsicherheitsausweisen dank des in allen Modulen befindlichen HSM-Kryptoprozessors, das eine blitzschnelle Entschlüsselung ermöglicht
- Serverredundanz mit der virtuellen Umgebung des Kunden oder der von TIL validierten und angebotenen SAFEKIT-Lösung möglich
- Drittanbieter-IT-Architektur zur Steigerung der Rechnerleistung möglich
- 24/7-Webseite zur Wiederherstellung vorläufiger Lizenzen bei Serverausfall
- CUBE-Zentrale im Industriedesign mit einer MTBF von 20 Jahren und einer MTTR von 5 Mio
- Paralleler Download auf alle Zentralen vom Server aus

UNTERSTÜTZUNG UND ANPASSUNGSFÄHIGKEIT AN VORGABEN FÜR EINE ANSSI-KONFORME AUSWEISPROGRAMMIERUNG

Die TIL-Lösung bietet eine hohe Sicherheit und große Projektanpassungsfähigkeit bei der Schlüsselverwaltung und beim Ausweis-Mapping nach Kodierungsvorgabe des Endkunden.

Das Unternehmen TIL TECHNOLOGIES unterstützt Kunden bei der Definition einer ANSSI-konformen Ausweisprogrammierung mit hochsicherer und flexibler Ausweiskodierung für vielfältige Anwendungen. Dadurch wird eine optimale Nutzung vorgesehener und zukünftiger Anwendungen auf dem Ausweis ermöglicht.

HOHE FUNKTIONALITÄT FÜR GEBÄUDESICHERHEIT UND -TECHNIK

MICROSESAME ist ein offenes skalierbares System. Es überwacht die eigenen Zentralen und daran angeschlossene Peripherien, Sensoren und Aktoren sowie Drittsysteme oder -Produkte (Industrie-SPS, Klima, Heizung...), die über verschiedenen frei erhältlichen Standardprotokollen (MODBUS IP, OPC UA usw.) eingebunden werden können.

MICROSESAME besitzt eine große Funktionsvielfalt für die Sicherheits- und Gebäudetechnik, da es verschiedene Gewerken (Zutrittskontrolle, Einbruch, Video...) für spezifische Branchen (Industrie, Dienstleistungen, sicherheitssensible Standorte, Infrastruktur, Behörden...) abdeckt. Die Systemkonfiguration kann an die Bedürfnisse des Endnutzers genau angepasst und bei Bedarf sicherheitstechnisch auch nachträglich höhergestuft werden. Nachstehend folgt eine nicht erschöpfende Liste der Hauptfunktionen:

PERSONEN- UND BENUTZERVERWALTUNG

BENUTZERVERWALTUNG (Personen, Besucher, Benutzer) mit personenbezogenen Daten mit bereits festgelegten (Nachname, Vorname...) und kundeneigenen Feldern oder über vordefinierten Drop-Down-Listen, Gültigkeitsdauer, zugeordnete Dateien und Dokumente, Informationen zur letzten Ausweisprüfung, Benutzerstatus („VIP“...)

ZUWEISUNG MEHRERER ID-MITTEL (Ausweis, Kfz-Kennzeichen, virtueller Ausweis, QR-Code...) pro Person, bis zu 4 Technologien pro Server, und 99 ID-Mittel pro Technologie (Bsp.:2 Ausweise, 3 Autos)

INTEGRIERTER EDITOR FÜR AUSWEIS-HINTERGRUNDGRAPHIK: feste und variable Texte, Bild, QR-Code, festes Bild wie Logo…), Vorder-/Rückseite, Farbe usw. zur Ausweispersonalisierung

VERWALTUNG VON MULTI-MAPPING/KODIERUNG für hochgradig personalisierbare und sichere Ausweise

GRAFISCHE PERSONALISIERUNG, MULTI-ANWENDUNGSKODIERUNG gesichert (Zutritt, Restaurant, Zeiterfassung...) mit Ausweisregistrierung in einem einzigen Druckervorgang zur schnellen, einfachen und sicheren Ausweiserstellung. Integrierter Editor für Ausweishintergrund und -kodierung

AUTOMATISCHE SYNCHRONISATION mit in **MICROSESAME** erstellten Personen und kodierte Multi-Anwendungsausweisen Kantine-, Zeiterfassung oder andere…

SIEHE KAPITEL BENUTZERVERWALTUNG, DSGVO, AUSWEISKODIERUNG UND AUSWEISPERSONALISIERUNG

ON- UND OFFLINE-ZUTRITTSKONTROLLE

- Verwaltung individueller Zutrittsberechtigungen, nach Profil, mit Anfangs- und Ablaufdatum. Zutrittsberechtigungen werden den Benutzer unabhängig von ID-Mittel oder On-/Offline-Leseeinheiten zugewiesen

- Sammeländerung von Zutrittsberechtigungen für Personen, die aus einer Suche nach mehreren Kriterien resultieren

- Automatische Zuweisung von Zutrittsberechtigungen für Personen, die aus einer HR-Datenbank nach vordefinierten Regeln der Benutzereingabefelder importiert wurden (Bsp.: Profil 1 in Betrieb 1)

- Nach Validierung automatischer Download der Liste autorisierter Personen an die Zentralen

- Aufzugsverwaltung mit Filterung der zugänglichen Etagen je Person, Zeitfenster, Krisenstufe. Vorrangiger Aufzugsruf für Vorzugspersonal (Bsp.: KKH)

- Kompatibilität mit diversen Technologien und allen Arten von Zutrittskontroll-Leseeinheiten:
    - 125 kHz und 13,56 MHz Proximity Leseeinheit (MIFARE, DESFIRE, ICLASS usw.)
    - 13,56 MHz (MIFARE, DESFIRE) mobile MOBILIS-Leseeinheit
    - Fernleseeinheiten, aktive Ausweise oder Fernbedienung
    - Kfz-Kennzeichen-, biometrische oder QR-Code-Leseeinheiten auf Smartphone
    - Mechatronische Zylinder und Türdrücker (on- und offline)
    - TIL + STid Online-Lösung für virtuelle Ausweise auf Smartphones mit:
        - Bi-Techno-Bluetooth/13,56 MHz auf EVOLUTION-Leseeinheiten
        - Cloud-Online-STid-Plattform

- Steuerungen für verschiedene kontrollierte Zutritte oder Auslöser (Schranke, Elektroschloss, Drehkreuze, Displays, Sirenen, Beleuchtung...)

- Große Anpassungsfähigkeit der Zutrittsbetriebsart: Schleuse mit 2/3/X-Türen, ein- oder beidseitig, Leseeinheit oder Leseeinheit mit Tastatur (Ausweis + PIN), mobile Leseeinheite, einfache oder Mehrfachauthentifizierung für Risikobereiche bei Nutzern unterschiedlicher Sicherheitseinstufung…

- Erweiterte Funktionen, die sich kumulativ auf die Zutrittsberechtigungen auswirken:
    - Ruhezeitenüberwachung
    - Befähigung (elektrische, medizinische...) pro Person und Zutrittsstelle, mit Anfangs-/ Ablaufdatum
    - Krisenstufe (Antiterrorplan) 7 pro Person, Zutrittspunkt und Etagen über Systemanwenderbefehl zuweisbare Stufe. Authentifizierungsmodus für jede Krisenstufe individuell wählbar: Ausweis + Ausweis, Ausweis + PIN, Mehrfachauthentifizierung
    - Unterstützung Zonen- und zeitabhängiger, lokaler oder globaler Rückkehrsperre je nach Ausnahmeregelung
    - Erzwungener Zutritt mit Ausweis + spezifischem PIN erkennbar
    - Bedingte Authentifizierung: Obligatorische Ausweisprüfung erst an Leseeinheit X und dann an Leseeinheit Y

SPEZIAL FUNKTIONEN IN DER ZUTRITTSKONTROLLE

BESUCHERVERWALTUNG mit komplettem Workflow von der Termin- und Besuchererfassung über die Genehmigung der Besuche bis hin zum Besucherempfang am Standort.

VERWALTUNG VON PARKPLÄTZEN und sensiblen Bereichen mit zonenspezifischer Zählung, zulässiger Zufahrt-/Zutrittsschwelle je nach Nutzerkategorie

UNTERSTÜTZUNG FÜR NOTFALLPLAN (Übung oder real) mit spezifischer Benutzeroberfläche, die die Liste, die Anzahl, den Aufenthaltsort der in jeder sicheren/unsicheren Zone anwesenden Personen mit Bild, Mitarbeiterliste und Ausdruck für das Rettungspersonal bekanntgibt

MULTISTANDORT- und MULTIMANDANTEN-VERWALTUNG mit Standort (Ausrüstung, Überwachungsobjekt), Einheit (Personen), Klassifizierung (Leseeinheit), Perimeter (Schlüssel) und Benutzerverwaltung

PCVA: Zutrittspunkt-Videokontrolle durch einen Systemanwender, der nach der Ausweisprüfung den Zutritt erlaubt oder nur informiert wird und den Zutritt gemäß Zutrittsberechtigung gewährt

BEFÄHIGUNG: (elektrische, medizinische usw.) pro Person und Zutritt, mit Anfangs- und Ablaufdatum

RUHEZEITKONTROLLE

UNTERTÜTZUNG VON KONTROLLGÄNGEN: Zentralisierte Streckenüberwachung mit Ausweisen und Ausweis-Leseeinheiten

QUARANTÄNENVERWALTUNG mit **TILLYS CUBE** (Pfad und Dauer zwischen definierbaren Zonen)

EINBRUCH

VERWALTUNG ALLER ORTUNGSINFORMATIONEN des Typs Kontakt (Radar, Melder), verbunden mit:
- symmetrischen, diskreten Eingängen unserer Zentralen

- **EQUILOCK**-Transpondern im Bus mit dem **EQUILOCK**-Modul

- Zentralen, Drittsystemen, die über MODBUS, OPC usw. am System angeschlossen sind oder aus **SORHEA**-Lösungen über die **MAXIBUS**-Schnittstelle mit unserem System oder aus der VMS-Bildanalyse über eine SDK-Schnittstelle zu unserem System

ZENTRALE VERWALTUNG DER RECHTEZUWEISUNG Eingreifen auf allen **TILLYS**-Zentralen über **MICROSESAME**: Einfach, schnell, flexibel. Somit können Benutzer mehrere Einbruchzonen in mehreren Einbruchmeldezentralen verwalten, jedoch ausschließlich solche, die freigegeben sind

ZONENÜBERWACHUNG

SCHÄRFEN/ENTSCHÄRFEN Umschaltung über Zeitpläne, Multizonen- **TACTILLYS-CUBE**-Tastatur mit automatischem/manuellem/verbotenem Ausschluss, Zählung, autorisiertem Zutritt, projektweise festgelegten Steuerungen (kombinatorisch und sequenziell). Beispiel: Dreifachauthentifizierung an der Leseeinheit für Überwachung erwirkt Scharfschaltung.

NATIVE und VOLLSTÄNDIGE INTERAKTION mit Zutrittskontrollanlage, da von einer und derselben **TILLYS-**Zentrale verwaltet

AUTOMATISMEN bei Interaktionen mit anderen Systemen (Video, Sirene, Beleuchtung...)

ÜBERTRAGUNG VON EINBRUCHALARMEN (einschließlich Zutrittskontrolle und Gebäudemanagement) an eine IP-Fernüberwachungsstation mit standardisiertem ESI qualifizierten - Azur soft - "TIP"-Protokoll von TIL

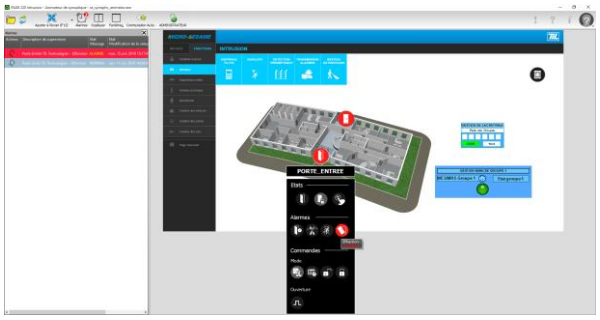
SICHERHEITSSUPER- UND HYPERVISION, SMART BUILDING

ALLGEMEINE ERGONOMIE DER BENUTZEROBERFÄCHE für ein erleichterte intuitive Systembedienung konzipiert

EREIGNISMONITOR, Echtzeitalarme mit Schnellsuche und Mehrfachkriterien-Eingabeoption

GRAFIKÜBERSICHTSEDITOR und -ANIMATION nativ integriert, schnell konfigurierbar und hochgradig individualisierbar mit Objekte, Objektbezeichnungen, Übersichtszoom...

ÜBERWACHUNG MIT GRAFISCHER ANIMATION VON GEBÄUDEPLÄNEN und Übersichten mit animierten Status-Icons



ECHTZEITÜBERWACHUNG VON ZUTRITTSKONTROLLALARMEN bei Einbruch, Brand, Technik (Aufzugsfehler, Klimaanlagenfehler, Leistungsschalterfehler...) mit Qualifizierung und zugehörigen alarm- und benutzerprofilabhängig konfigurierbaren Hinweisen

ZONENÜBERWACHUNG MIT ZÄHLER, NOMAN über dedizierte Benutzeroberfläche, die die Liste, den Zählerstand und den Aufenthaltsort der in jedem Bereich anwesenden Personen anzeigt

SCHNITTSTELLEN ZWISCHEN MICROSESAME und marktüblichen VMS (MILESTONE, GEUTEBRUCK, HIKVISION...). Die integrierte **VISIOSESAME**-Funktion bietet:

- ► Die parallele Überwachung der Videostreams mehrerer VMS gleichzeitig
- ► Die Visualisierung von Live-Bildern durch deinen Klick auf einen Icon in der Benutzerübersicht für Alarme zur Steuerung von Videokuppeln und -Wänden
- ► Automatische Videoaufzeichnungen an VMS bei Einbruch, unerlaubtem Zutrittsversuch...
- ► Die Wiedergabe von Videoaufzeichnungen auf VISIOSESAME, die mit den im MICROSESAME-Verlauf gesuchten Alarmen im Zusammenhang stehen
- ► Die Einbindung von Videoalarmen (Bildanalyse) und Fehlern (Kamerafehler usw.) aus den VMS
- ► Ein Dashboard zur Systemprozessüberwachung durch die IT-Abteilung (Steuerungen und Dienste manuell starten/stoppen, Abfragestatistiken...)

BREITE KOMPATIBILITÄT ÜBER HARD-/SOFTWAREGATEWAYS

FÜR UNSER **MICROSESAME**-SYSTEM SIND FOLGENDE KONNEKTOREN VERFÜGBAR:

- Benutzer- und Besucherverwaltung: REST-API-Webdienst, CSV-Dateien
- AD-Benutzerverwaltung: LDAPs, Authentifizierung über Windows-Account (SSO NTLM)
- IT-Supervisor: SNMPv3 (TILLYS CUBE)
- Hypervisor: OPC UA, MODBUS IP
- Zentrale, Drittsystem: MODBUS IP
- VMS-Videosystem: VMS SDK, TEXT/ASCII-Gateway
- Projekt- und/oder produktspezifische Gateways (Verzeichnisse, Drittprodukte, diverse SDKs...)

Weitere Informationen und Beispiele in den entsprechenden Kapiteln: GATEWAYS UND KONNEKTOREN, VIDEOÜBERWACHUNG, GEGENSPRECHANLAGE

STROMVERWALTUNG

- Verbrauchsüberwachung
- Visualisierung der verbrauchten Gesamt- oder Teilenergieleistungen
- Bereichsausnahme nach Prioritätsstufe entsprechend der vertraglich vereinbarten Leistung
- Jahresprogrammierung der Betriebsrhythmen von kontrollierten Bereichen (bis zu 3 Jahresprogramme)

BELEUCHTUNGSSTEUERUNG UND ANDERE SCHALTUNGEN

- Ein-/Ausschaltung mit Zeitprogrammierungsoption
- Neustart oder Ausnahme durch konfigurierbare Dauer über Timer (Räume mit unregelmäßiger Belegung)

STEUERUNG VON HEIZUNG, MECHANISCHER BELÜFTUNG, KLIMAANLAGE

- Ein-/Ausschaltung der Regler mit Zeitprogrammierungsoption
- Definition von Temperatursollwerten und Betriebsarten: frostfrei, reduziert, energiesparend, komfortabel usw.
- Messwerte für hohe und niedrige Temperaturen

STEUERUNG VON WARMWASSER WW

- Ein-/Ausschaltung mit Zeitprogrammierungsoption
- Programmierung der Betriebsarten: Automatischer, manueller oder programmierter Neustart

SYSTEMLEISTUNGEN

Hardware-Parametrierung	
Gleichzeitig verbundene Client-Arbeitsplätze	499
Programmierbare Steuerungen (TILLYS CUBE)	10.000
Zentrale auf derselben IP-Leitung	255
Unterstützte Treiber (Leitungen)	128
Ausweis-Leseeinheiten	20.000
Videorekorder	256

Parametrierung der Zutrittskontrolle	
Systemnutzer (Benutzer, Besucher)	unbeschränkt
ID-Mittel (Ausweis, Kfz-Kennzeichen usw.)	unbeschränkt
Standorte	256
Einheiten	256
Leseeinheitengruppen	unbeschränkt
Leseeinheiten je Gruppe	1.024
Zutrittszonen	128
Befähigungen	256
Visuelle Zutrittskontrollpunkte	256
Kontrollgänge	64

Überwachungsparametrierung	
Wege, Gesamteigenschaften	40.960
Wege, Eigenschaften je Leitung	8.192
Eigenschaftskategorien	64
Zähler	2.048
Eigenschaften in einer Formatzeichenfolge	16

Betriebsparametrierung	
Benutzer (zentralisiert)	unbeschränkt
TILLYS CUBE Systemanwender (lokal)	150

Zutrittskontrolle (Benutzer/ID-Karteien)	
Mit der Benutzer-kartei verknüpfte Lesetechnologien	4
Anzahl der ID-Mittel pro Lesetechnologie	99
Länge des Ausweiscodes (mit den Zentrale-Steuerungen harmonisiert)	32 Zeichen
Länge des Standortcodes (mit den Zentrale-Steuerungen harmonisiert)	32 Zeichen
Definierbare Felder (Größe, Gehäuse, Länge, freie Eingabe, verpflichtend, assistiert usw.)	16
Herunterladbare Felder in einer Zentrale (höchstens 20 Zeichen)	Nachname, Vorname + 6 erste

Zeitpläneund Feiertage	
Zeitpläne pro Standort / Zentrale (Zentrale gilt als ein Einzelstandort, doch kann ein Standort X Zentralen haben)	128
Gesamt Anzahl von Zeitplänen auf zentralem Multistandort-Server	256
Tage pro Zeitfenster	9 (Woche + Feiertage + Sondertage)
Slots pro Tag	4
Mini-Slot	1 Min
Sondertage	32

Ereignisverlauf	
Ereignisse im Verlauf	Unbegrenzt (je nach Datenbank)
Maximale Anzahl von Ereignissen je Verlaufsabfrage	unbeschränkt
Aufbewahrungsfrist (konfigurierbar, um beispielsweise eine 3-Monate-Regel einzuhalten)	Standardmäßig 30 Tage

Hardwareleistungen der Zentrale	
Herunterladbare ID-Mittel - TILLYS CUBE	Bis zu 600.000 native
Leseeinheiten zur Zentrale- TILLYS CUBE	nativ 24

DSGVO

FEINSTEUERUNG DER BERECHTIGUNGEN IN MICROSESAME

Mit folgenden Funktionen entspricht **MICROSESAME** der DSGVO in jedem der Hauptthemenbereiche.

Es liegt dann am Datenschutzbeauftragten (DSB) des Endkunden:

- Die unten verfügbaren Funktionen in **MICROSESAME** anzuwenden und zu aktivieren
- Festzulegen, welche Daten in den freien Feldern der User-Karteien erfasst werden sollen (Dauerbenutzer, temporärer Benutzer, Besucher)
- User und ihre Datenzugriffsrechte festzulegen
- Wo die SQL-Datenbank installiert wird, in der diese User-Daten gespeichert sind und wer Zugriff auf die SQL-Datenbank hat
- DSGVO-Verfahren einzuhalten (zum Beispiel für die Bekanntgabe einer Zutrittskontrolle am Standort und insbesondere für die Biometriedaten)

BENUTZERZUTRITTSKONTROLLE (INKLUSIVE GÜLTIGKEITSABLAUF)

- Zugriff auf personenbezogene Daten in den User-Karteien, gemäß Benutzerberechtigungen nach autorisierten Feldern und Einheiten (Personenkategorie oder -standort)
- Zugriff auf autorisierte Daten mit ausschließlich Lese- oder/und Schreibrecht
- Eingabefelder bei Besucherkartei-Erstellung als obligatorisch definierbar (≠ permanente Karteien)
- Ohne Benutzerrecht von Besuchern mit „TERMINMANAGEMENT“-Profil kann der Benutzer:
  - Um Dubletten zu vermeiden, in der Datenbank bekannter Besucher mit der automatischen Vervollständigung nach einem Besucher suchen und dabei nur Nachnamen, Vornamen, Firma von Besuchern sehen
  - Wenn dieser nicht vorhanden ist, einen neuen Besucher mit allen Feldern (Geburtsdatum usw.) vollständig erstellen,
  - In beiden Fällen die übrigen Informationen der Besucherkartei weder bearbeiten, noch ändern oder einsehen.

Bei entsprechender Berechtigung können alle Informationen in der Besucherkartei bearbeitet, geändert und angezeigt werden

RÜCKVERFOLGBARKEIT: ART DER RÜCKVERFOLGUNG, DER AUFGEZEICHNETEN DATEN UND AUFBEWAHRUNGSDAUER

- Alle Änderungen, Abfragen, Löschungen von personenbezogenen Daten sind rückverfolgbar. In MICROSESAME ist ein Agieren ohne Rückverfolgbarkeit nicht möglich
- Die Datenaufbewahrungsdauer ist frei einstellbar
- Die manuelle Datenlöschung von nicht mehr dem Unternehmen zugehörigen Personen ist möglich
- Benutzerimport mit automatischer HR-Datenbank zur Minimierung menschlicher Eingriffe ist möglich

DATENSPEICHERUNG

- Periodische, automatische Datenbanksicherung ohne menschlichen Eingriff auf Festplatte
- Periodische Archivierung der Verläufe möglich

DATENVERSCHLÜSSELUNG

- Datenfluss-Schutz: Heavy-Client-Arbeitsplätze in TLSv1.3, Thin-Clients in Https
- In der Datenbank durch einen gesalzenen SHA-512-Hash aus 512 zufälligen Zeichen geschützte Benutzerpasswörter
- Gegen CSRF-Angriffe geschütztes **WEBSESAME**-Portal
- **MICROSESAME** unterstützt die Datenbank-Anonymisierung vor Übertragung an Dritte für Debugging, Testmigration

SOFTWARESCHUTZ UND ERHALTUNG DER SICHERHEITSUMGEBUNG

- ANSSI-qualifiziertes AMCO PREMIUM-Paket: von TIL bereitgestellte Updates und Sicherheitspatches

DPIA (DATA PROTECTION IMPACT ASSESSMENT) / PIA (PRIVACY IMPACT ASSESSMENT) - DATENSCHUTZ-FOLGENABSCHÄTZUNG

Nicht erforderlich für die Implementierung einer Sicherheitseinrichtung per Ausweis ohne Biometrie. Gemäß PDF-Datei „Liste der Arten von Verarbeitungsvorgängen“, für die keine Datenschutz-Folgenabschätzung erforderlich ist.

ERKLÄRUNG FÜR DIE ZUTRITTSKONTROLLE UND INSBESONDERE DIE BIOMETRIE

TIL TECHNOLOGIES und deren **MICROSESAME**-Lösung verwalten direkt kein biometrisches Element (Fingerabdruck, Details...) und sind von den Biometrie-Nutzungserklärungen AU52 (1:1) und AU53 (1:N) nicht betroffen.

Die **MICROSESAME**-Lösung integriert marktübliche biometrische Leseeinheiten beispielweise von IDEMIA und STid. Unsere Automaten lesen nur die von der Leseeinheit gesendete ID (des Ausweises oder der lokalen Datenbank) und auf keinen Fall den Fingerabdruck. Ausschließlich die Leseeinheitenhersteller verwalten die biometrischen Elemente. Sie verfügen über eigene biometrische Erfassungstools (SECARD BIO, MORPHOMANAGER) und müssen die technischen Anforderungen der Biometrie-Nutzungserklärung AU52 (1:1) und AU53 (1:N) erfüllen.

Zur Erinnerung stehen hier die Verfahren, die vom Endkunden eingerichtet und befolgt werden müssen:

- Zutrittskontrollerklärung, ohne Biometrie, vereinfachter Standard NS-42
    - Identifikationselemente: 5 Jahre nach dem Ausscheiden des Arbeitnehmers: Manuelles Löschen von Nutzern auf **MICROSESAME**
    - Elemente des Personenverkehrs (3 Monate): Auf **MICROSESAME:** konfigurierbare Verlaufstiefe: 3 Monate oder andere
- Biometrie-Nutzungserklärung AU52 (1:1) und AU53 (1:N). Das Fingerabdruckmanagement muss insbesondere hinsichtlich der anspruchsvolleren AU53 im Vergleich zu der simplen und einfachen AU52 konform sein

USER-VERWALTUNG

DETAILLIERTES UND SICHERES MANAGEMENT VON USER-RECHTEN IN MICROSESAME

Ein User ist eine natürliche Person, die berechtigt ist, die **MICROSESAME**-Überwachungsschnittstelle zu verwenden. Dieser User kann je nach Funktion, hierarchischer Ebene oder geografischem Standort auf alle oder einen Teil der verschiedenen Funktionen, verfügbaren Daten in **MICROSESAME** zugreifen.

Um jedem User nur die Rechte zuzuweisen, die er schnell je nach User-Typ benötigt, hält **MICROSESAME** „Userprofile“ bereit. Diese Profile werden mit Hilfe von Kontrollkästchen präzise definiert, um den Grad der zugänglichen Rechte bei Visualisierung, Erstellung, Änderung, Löschung und in jeder der folgenden Hauptfunktionen darzustellen:

- Zutrittskontrollrechte
- Nutzungsrechte
- Verlaufsrechte
- User-Rechte (einschließlich welche personenbezogenen Daten)
- Besuchsrechte
- Überwachungsrechte (einschließlich Kategorien von Eigenschaften, zum Beispiel: Zutritt, Einbruch, Brand usw., Maske / Alarmverifikationsebene)
- Rechte in Verbindung mit der Parametrierung (einschließlich Filtern für Multistandort-Projekte nach Leseeinheit-Standorten, Standorten von Übersichtsobjekten, Entitäten von Benutzern, Klassifizierung jedes Zutritts, dessen Einstufung höher ist als die Standorteinstufung)
- Sicherheitsrelevante Rechte

Angesichts der Reichweite und der Präzision dieser Userprofile/-Rechte werden spezifische Dokumente regelmäßig aktualisiert, auf die Sie verweisen können. Sie sind bei Ihrem bekannten TIL-Ansprechpartner erhältlich.

Für jeden angelegten User genügt es dann, ihm eines oder mehrere vordefinierte User-Profile zuzuweisen.

Die Rechteverwaltung ist sicher, einfach und für eine große Population gedacht. Sie vereinfacht die Nutzung, Wartung und Implementierung, da:

- Eine Änderung der Userprofile von allen ihnen zugeordneten User automatisch übernommen wird
- Dem User ein oder mehrere Profile zugeordnet werden können, damit sich dieser in die gleichen Bedingungen wie ein anderer User versetzen kann, dem er beispielsweise aushelfen möchte
- Ein User zunächst einmal ein „Benutzer“ ist, der über physische Zutrittsberechtigungen verfügt und als Benutzer der **MICROSESAME**-Software gilt. Dadurch wird eine doppelte Eingabe von personenbezogenen Daten und Karteien vermieden
- Eine Hierarchie zwischen Usern besteht: Damit Benutzerrechte geändert werden dürfen, muss die Hierarchieebene des Users, der die Änderung durchführt, höher sein als die der geänderten Users (Hierarchieebene und Profil)
- User-Passwörter in BDD HASH SHA-512 + SEL aus 512 zufälligen Zeichen geschützt sind
- Rückverfolgbarkeit und Verlauf von User-Aktionen (mit geänderten Werten/Feldern), wie in vielen Wirtschaftsbereichen (Agro-Food, Pharma, Logistik, Kernenergie) regulatorisch vorgeschrieben gesichert sind
- User-Rechte in **MICROSESAME** für alle Arten von Client-Arbeitsplätzen (Heavy, Thin, WEB) zentral verwaltet werden
- Jedem User ein Standard-Login und ein Standardpasswort zugeteilt werden, die er bei seiner Erstanmeldung ändern muss und daher nur ihm bekannt sind
- **WEBSESAME**-Benutzer nach zu langer Inaktivität oder Neustart des Apache Webservers sicherheitshalber automatisch getrennt werden

LDAP-Verzeichnis/Active Directory

Das User-Verwaltung erfolgt entweder auf dem **MICROSESAME**-System oder von einem zentralen Verzeichnis Active Directory (AD), das von der IT-Abteilung verwaltet wird und über eine Gateway mit LDAP-Protokoll an **MICROSESAME** angebunden ist. Dies ermöglicht, dass

- Ein einziges Referenzverzeichnis für alle Benutzer der Anwendungen eines Unternehmens gepflegt wird, was das Erstellen, Ändern und Löschen von Usern erleichtert, da die Aktualisierung einfach und automatisch synchronisiert wird
- Das oder die in **MICROSESAME** vordefinierte/n User-Profil/e für diese Tätigkeit in diesem Active Directory zugewiesen wird/werden. Das User-Multiprofil wird mit der LDAP-Authentifizierung berücksichtigt
- Komplexe Passwörter mit der Active Directory-Funktion verwaltet werden
- User im sicheren Modus mit LDAPs verwaltet werden

MEHRFACHSTANDORTE- UND -MANDANTEN

STANDORT- ODER ORGANISATIONSORIENTIERTER BETRIEB

MICROSESAME ermöglicht die Verwaltung von bis zu 256 verschiedenen Standorten mit einem einzigen System aus. Diese Funktionalität ist in vielen Fällen vorteilhaft:

- Zum Verwalten geografisch verteilter Gebäude: Netzwerk aus Behörden, Ämtern, Produktionsstandorten über einen einzigen Zentralserver.
- Zum Verwalten unterschiedlicher Rechte auf jeder Dienstebene an einem Standort.
- Bei einer gemeinschaftlichen Nutzung desselben Gebäudes oder Büroturms durch mehrere Unternehmen, Mieter, bei der zwischen gemeinsamen und eigenen Zugängen unterschieden wird.
- Bei einer individuellen Serverstruktur: 1 x nationalen Server für alle Standorte oder je nach Einschränkungen (Netzwerkqualität) und geplanter Organisation (zentral, dezentral...) 1 x Server je Standort
- Bei einer kundeneigenen Ausweisverwaltung mit:
  - Zentralisierter Personalisierung und Kodierung zentral am Sitz
  - Zentralisierter generischer Kodierung zentral am Sitz und Personalisierung dezentral an jedem Standort
  - Personalisierung und Kodierung dezentral an jedem Standort

Die Nutzung der Multistandort-Funktion setzt einen Systemverwalter voraus, der

- Die alleinige Zentraldatenbank verwaltet
- Standorte definiert, wobei eine Zentrale als kleinster Standort gilt:
  Die Zentrale stellt ein Einzelstandort in der Systemarchitektur dar. Zu beachten ist die Wahl eines optimalen Anbringungsorts, der die nötige Kabelverlegung erheblich reduzieren kann.
- Personen Entitäten zuweist
- Userrechte und User pro Standort gemäß Organisation und Verfahren definiert
- Standort-, Abteilungs- und Unternehmensverwalter erstellt, die gemäß der User-Hierarche als Delegierte fungieren können, um eine präzise jedes Standorts zu ermöglichen, einschließlich:
  - Personalzutrittsberechtigungen / Einheit an den Standort-Leseeinheiten und ggf. gemeinschaftlich genutzte Leseeinheiten (Empfang, Parkplätze, Aufzüge...)
  - Einsicht in den Verlauf und die Mitarbeiterbewegungen

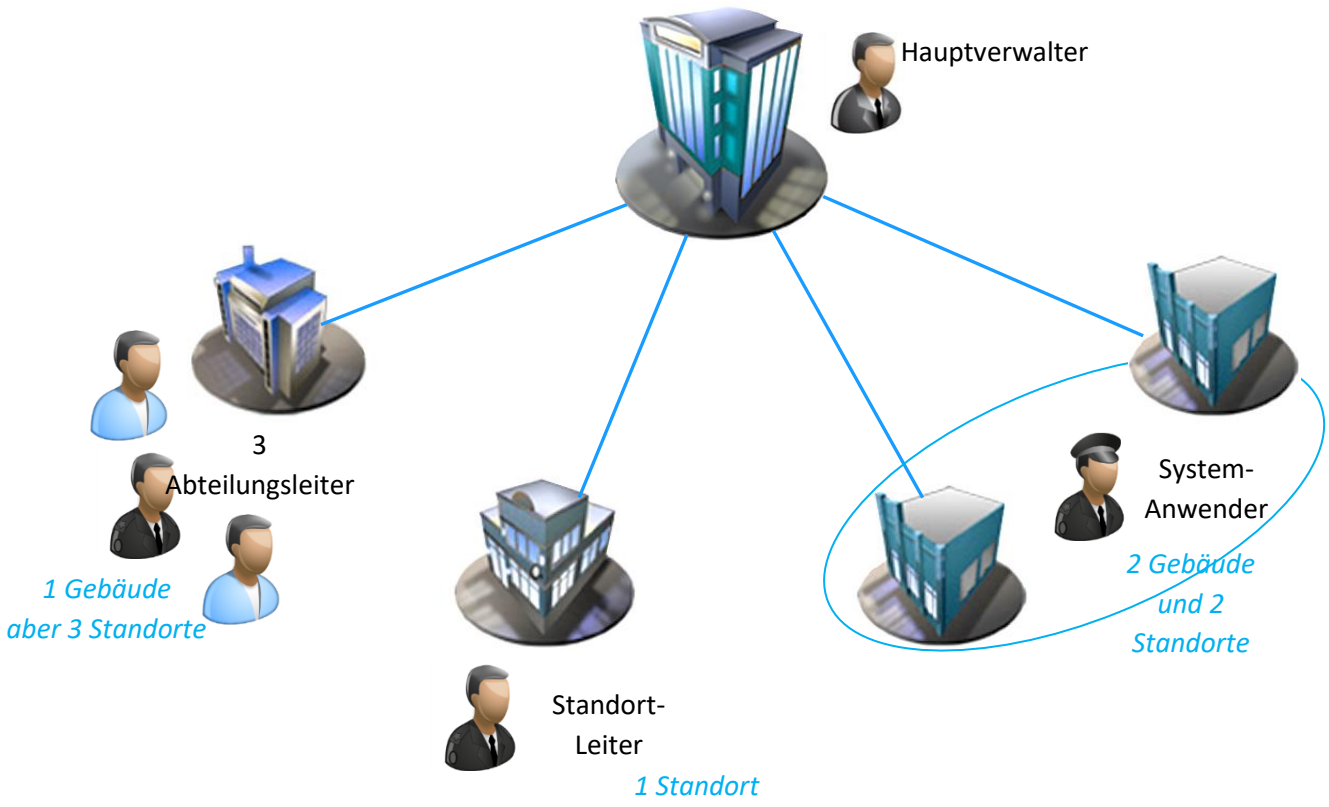
Es werden weder die Leseeinheiten und Zutrittsberechtigungen anderer Standorte, noch die Personen und deren Verlauf anderer Entitäten sichtbar

Jeder Standort verfügt über 128 unabhängige Zeitfenster, die entweder für Zutrittskontrolle, Einbruch oder das technische Gebäudemanagement (Alarmanlage, automatische Bewässerung...) verwendet werden.

Das Zentralsystem kann bis zu 256 Standorte und insgesamt 256 Zeitpläne für alle Standorte erstellen

Zum Schutz des Ausweis-Entschlüsselungscodes ermöglicht das KSM-Dienstprogramm (Key Secure Manager), Codierungstools und die CUBE-Zentrale dem Haupt-Sicherheitsbeauftragten, bei Bedarf verschiedene Ausweiscodes je Standort in einem bestimmten Perimeter zu verwalten, gemäß ANSSI-Leitfaden.

Ein Merkblatt zu möglichen Multistandort-Architekturen ist bei Ihrem bekannten TIL-Ansprechpartner erhältlich.



ZUTRITTSKONTROLLE

PROFILE, ZEITPLÄNE, BEFÄHIGUNGEN, LESEEINHEITEN, ZONEN...

Die User-Kartei umfasst und definiert:

INFORMATIONEN ZUM USER: Gültigkeitsdaten, Firma, Abteilung, Kontaktdaten sowie 16 zusätzliche individualisierbare Felder. Anhänge können ebenfalls zugeordnet werden (Arbeitsvertrag, Bild, Zertifikate, Befähigungszeugnisse...)

DIE ID-MITTEL DES BENUTZERS: Es sind bis zu 4 verschiedene Identifizierungstechnologien möglich (Bsp. 13,56 MHz-Ausweis, 125-kHz-Ausweis, PIN-Code, Kfz-Kennzeichen, QR-Code...). Für jeden Benutzer können bis zu 99 ID-Mittel pro Technologieart gespeichert werden. Die ID-Mittel können mehrere Status aufweisen: kaputt, verloren, gestohlen, nicht zurückgegeben, um einen Verbotsgrund darzustellen. Somit wird auch bei mehreren ID-Mitteln die Erstellung nur eines Users benötigt.

SPEZIFISCHE ATTRIBUTE: Rückkehrsperre, schwarze Liste (zur spezifischen Überwachung), Akkreditierungsstufe (Krisenmodus), Besuchsempfang, Besuchsführung…

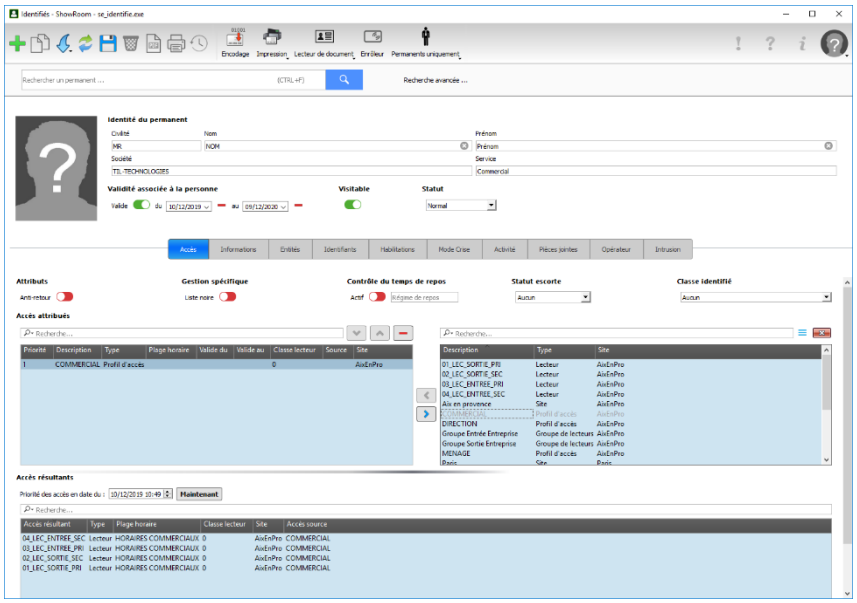
DIE GÜLTIGKEITSDAUER: die jedem User zugeordnet ist und die Gültigkeit eines ID-Mittels schnell und vorübergehend ohne Löschung der Berechtigungen aufhebt (oder erneut verlängert)

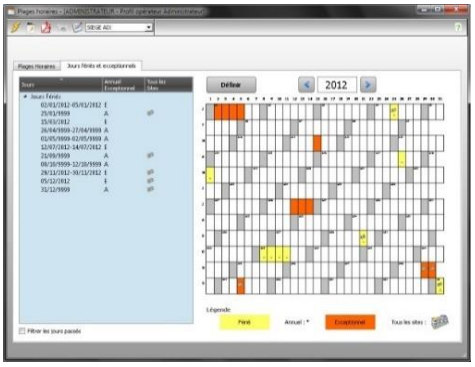
DIE VERWALTUNG UND SCHNELLE ZUWEISUNG VON ZUTRITTSBERECHTIGUNGEN IM FLEXIBLEN ANSICHTSMODUS: gemeinsame Ansicht, Textfilter, Auswahl mehrerer Berechtigungen in einer Liste mit Profilen, Leseeinheiten, Gruppen von Leseeinheiten und Aufzugsetagen. Zutrittsberechtigungen werden der Person und nicht den ID-Mitteln (Ausweisen) zugewiesen. Auch wenn ein Ausweis verloren geht und ein anderer neu zugewiesen wird, ändert dies an den Zutrittsberechtigungen also nichts.

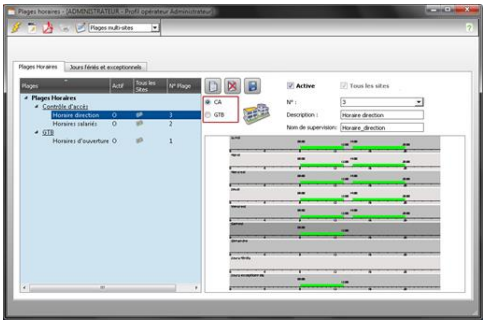
VERWALTUNG EINZELNER ZUTRITTE

Die Vergabe eines Zutrittsrechts ermöglicht es dem User, eine Leseeinheit oder eine Gruppe von Leseeinheiten entsprechend eines definierten Zeitprogramms über die Benutzeroberfläche (128 Zeitpläne) zu passieren.

Die **TILLYS CUBE**-Zentralen werden von **MICROSESAME** als Zeitmaster regelmäßig aktualisiert. Damit wird sichergestellt, dass Abweichungen zwischen den Zentralen und dem Server vermieden werden und die pünktliche Einhaltung von Zeitplänen garantiert ist.

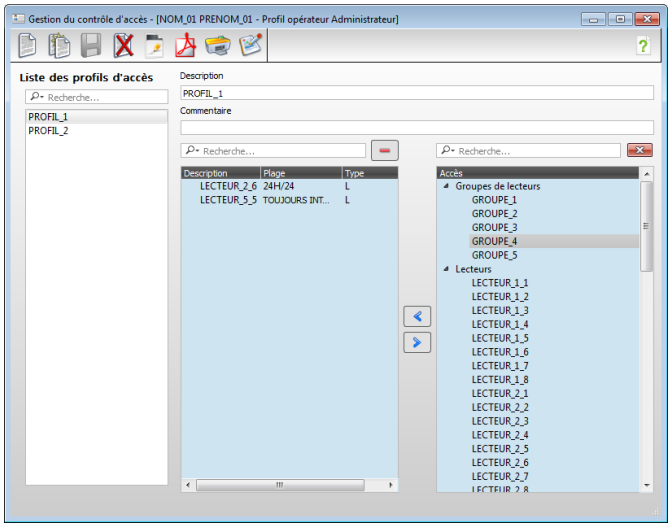






PROFILABHÄNGIGE ZUTRITTSVERWALTUNG

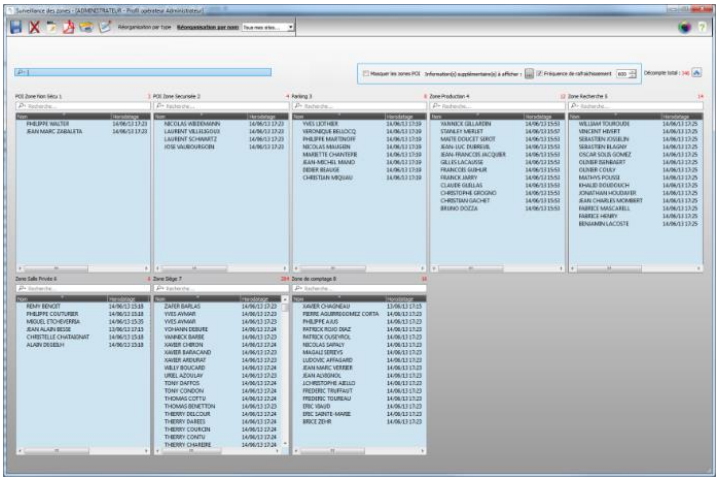
Ein Zutrittsprofil wird verwendet, um Zutrittsberechtigungen für eine Kategorie von Usern an einem oder mehreren Standorten vorzudefinieren. Das Profil besteht aus einer Liste von Leseeinheiten und/oder Gruppen von Leseeinheiten und/oder Aufzügen, wobei jedem Leseeinheit oder jeder Gruppe einen anderen Zeitplan zugeordnet werden kann. Jedem Benutzer können ein oder mehrere Zutrittsprofile zugewiesen werden.
Über die benutzerdefinierte Verwaltung von Zutritten nach Leseeinheiten und/oder Leseeinheitengruppen können für eine bestimmte Person Ausnahmen festgelegt werden.



So können beispielsweise für gemeinsame Zugänge ein „allgemeines“ Profil, für den Zutritt zu bestimmten Zonen ein „Dienst“-Profil und je nach Funktion oder hierarchischer Stufe der Person entsprechende Besonderheiten zugewiesen werden.

MICROSESAME besitzt für jeden Standort ein Zutrittsprofil „alle Leseeinheiten“, dass alle bestehenden und zukünftigen Leseeinheiten des Standorts umfasst. Dieses Profil ist nützlich, wenn einem Benutzer alle Leseeinheiten eines Standorts zugeteilt werden soll, ohne dass bei jedem Hinzufügen neuer Leseeinheiten für einen bestimmten Standort jeweils das Profil geändert werden muss. Das Verwalten von Zutrittsberechtigungen für User ist hochflexibel. Sie ermöglicht eine schnelle Visualisierung und Vergabe von Zutrittsberechtigungen: Gesamtansicht der Zugänge, Textfilter, Auswahl mehrerer Zugänge aus einer Liste mit Profilen, Leseeinheiten, Leseeinheitengruppen und Aufzugsetagen. Eine Funktion in der User-Verwaltung zeigt die „resultierenden Zugänge“ permanent an, die sich aus der Zuordnung aller dem User zugewiesenen Zutrittsberechtigungen ergeben.

ZONENEMANAGEMENT



MICROSESAME Unterstützt das Zonenmanagement. Eine Zone besteht aus mindestens zwei Gruppen von Leseeinheiten: eine Gruppe zum Betreten und eine Gruppe zum Verlassen der Zone. Eine Gruppe von Leseeinheiten kann in einer Anlage eine beliebige Anzahl von Leseeinheiten zählen.

Es ist möglich, die Anzahl der in jeder Zone befindlichen Personen genau zu erfahren und diese Liste in alphabetischer oder in chronologischer Reihenfolge der Ankunft oder nach anderem Sortierkriterien wie Firma oder anderen zu erstellen.

Dieses Zonenmanagement wird häufig von SEVESO-klassifizierten Einrichtungen verwendet und ist für die Implementierung der von TIL entwickelten spezifischen Anwendung zur Unterstützung des NOMAN (Notfallmanagement) unerlässlich.

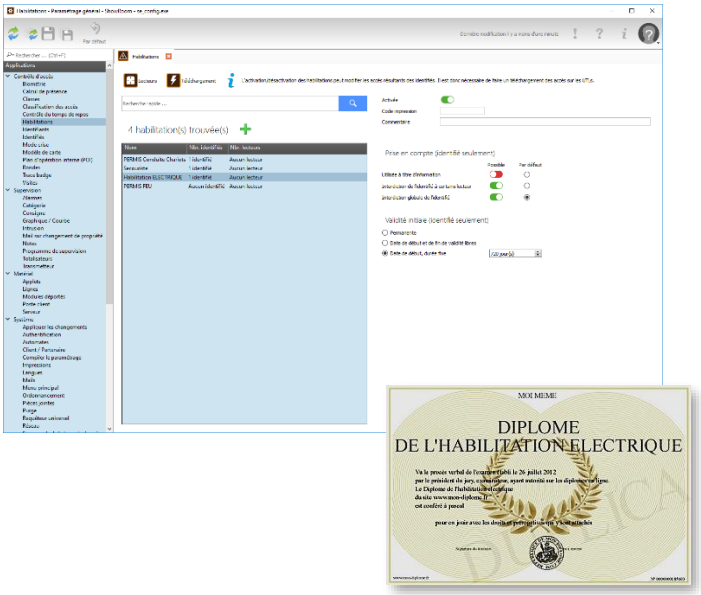
Die Liste der in einem Bereich anwesenden Personen kann bei Auslösung eines NOMANs per E-Mail gesendet werden.

Das Zonenmanagement ermöglicht auch die Implementierung einer präzisen Verkehrsüberwachung.
Es ist möglich, eine Zone in eine andere zu verschachteln und die Leseeinheiten entsprechend dem Verlassen einer anderen Zone zu aktivieren, wodurch tatsächlich ein „obligatorischer Durchgang“ entsteht.

BEFÄHIGUNGSMANAGEMENT

Die Zutrittsfreigabe eines Benutzers für bestimmte Zonen oder bestimmte Leseeinheiten kann vom Besitz einer gültigen Befähigung über die Zutrittskontrolle hinaus abhängig sein: Elektro-Zulassung, Befähigung zum Führen von Maschinen, Erste Hilfe, befristeter Vertrag, medizinische Versorgung...

Diese Gültigkeitskonditionierung kann von verschiedenen Personen verwaltet werden, beispielsweise von der Personalabteilung oder einem zuständigen Funktionsverantwortlichen.



Diese Funktion unterstützt bis zu 256 Befähigungen.

Jeder Identifizierte kann mehrere Befähigungen mit jeweils eigener Gültigkeitsdauer besitzen.

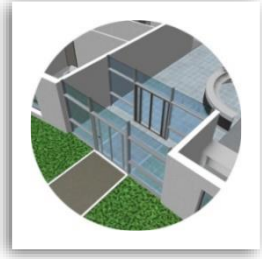
Der Zutritt an einer bestimmten Leseeinheit kann von der Gültigkeit einer oder mehrerer Befähigungen abhängen.

Elektro-Zulassung

ERHÖHTE SICHERHEITSFUNKTIONEN

RÜCKKEHRSPERRE: Bei Zugängen mit Ein- und Ausgangsleseeinheiten ermöglicht das Zonenmanagement die Einrichtung eines „Anti-Rückkehr"-Mechanismus, um zu verhindern, dass ein Benutzer einen Bereich mehrmals hintereinander betritt, ohne diesen zuvor verlassen zu haben.

SCHLEUSENMANAGEMENT: Die Leistungsfähigkeit der Systemprogrammierung ermöglicht, die Steuerung mehrerer Türen untereinander nach Projektanforderungen. Bei einer solcher Programmierung können mehrere Technologien miteinander kombiniert werden: Kontaktmatte, Eindeutigkeitsmatte, Videokamera, biometrische Leseeinheit usw.



MEHRFACHAUTHENTIFIZIERUNG: **MICROSESAME** bietet die Möglichkeit zur Anmeldung bestimmter Leseeinheiten mit doppelter Kontrolle: Vorhalten eines berechtigten Ausweises und zusätzliche Eingabe eines PIN-Codes über Tastatur. Diese verstärkte Kontrolle ermöglicht eine robuste Verifikation des Ausweisinhabers für sensible Zutrittspunkte.
Der PIN-Code kann für alle ID-Mittel identisch und für jeden Benutzer individuell sein.

EINSCHRÄNKUNGSCODE: **MICROSESAME** unterstützt eine Tastaturcode-Eingabe mit Einschränkung. An der Benutzerstation wird dann sofort ein stiller Alarm generiert und der Zutritt öffnet sich normal ohne akustischen Alarm.

ÜBERWACHUNG DER „SCHWARZEN LISTE": Diese Funktion wird verwendet, um einen Alarm auszulösen, sobald ein in der „schwarzen Liste" eingetragener Ausweis an einem der Leseeinheiten des Standorts vorgezeigt wird. Zum Beispiel, um vor Ort einzugreifen, wenn versucht wird, einen verlorenen oder gestohlenen Ausweis in betrügerischer Absicht zu verwenden.

KRISENMODUS: **MICROSESAME** ermöglicht die Verwaltung von Krisenschwellen. Basierend auf standortspezifischen Kriterien können 7 Stufen sowohl Personen (nach Hierarchie, Befähigungen...) als auch Leseeinheiten (nach Zonen, Alarmarten usw.) zugeordnet werden.

Wenn ein Krisenmodus ausgelöst wird, erhält jede Zentrale im System den Schwellenwertänderungsauftrag und verwaltet automatisch die Korrespondenzen zwischen den Akkreditierungsebenen der Personen und den Sicherheitsebenen der Leseeinheiten. Eine Person mit einer niedrigeren Ebene als die der Leseeinheiten kann eine Etage nicht mehr über den Aufzug betreten und/oder erreichen. Tatsächlich wirkt der Krisenmodus auf alle Zutrittsberechtigungen von Online-Leseeinheiten, einschließlich des Etagenmanagements.

Generiert werden mehrere Krisenszenarien durch:

- Automatische Steuerungen nach Zutrittskombinationen
- Benutzeraktionen, die durch einen einfachen Klick auf Schaltflächen auf zuvor vom Errichter konfigurierten Anlagen autorisiert werden: ein X-Szenario bringt die definierten Leseeinheiten auf die gewünschte Krisenstufe

VIGIPIRATE
SECURITE RENFORCEE
RISQUE ATTENTAT

QUARANTÄNE

MICROSESAME verfügt über eine hochgradig konfigurierbare Verwaltung von Quarantänenfristen.

Es wird empfohlen, eine Zentrale für jeden Quarantänezone zu verwenden.
Für jeden Zutritt an einem Leseeinheit durch eine Person X (Quarantänen-Leseeinheit) können konfigurierbare Fristen für Leseeinheiten abhängig von der Quarantäne für Person X definiert werden (2 Stunden für Leseeinheit 1; 5 Tage für Leseeinheit 2; usw.).

Ein Alarm auf dem Ereignismonitor erscheint, wenn Person X, nachdem sie die Quarantäne auslösende Leseeinheit passiert hat, versucht, einen abhängigen Zutritt zu betreten, ohne die Quarantänefrist einzuhalten.
In diesem Fall des Zutrittsverbots wegen Nichteinhaltung der Quarantäne durch Person X zeigt eine Nachricht an, dass sie die betroffenen abhängigen Leseeinheiten erst ab einem in Tagen/Stunden ausgedrückten Zeitraum betreten darf.

Die Autonomie von Zentralen ist vollständig, da sie direkt untereinander kommunizieren können.
Bei Netzwerkunterbrechung speichert jede Zentrale die Nachrichten und die Ausweisprüfungszeit und sendet sie automatisch an die anderen Zentralen, sobald das Netzwerk wiederhergestellt ist.

AUFZUGSMANAGEMENT

Die Installation von Ausweis-Leseeinheiten in den Aufzugskabinen eines Gebäudes ermöglicht es, bei einem mehrstöckigen Gebäude den Zutritt zu bestimmten Stockwerken nach individuellen Rechten, Personalprofilen oder Firmenzugehörigkeit zu regeln.

MICROSESAME verwaltet diese Funktion nativ, direkt aus den Benutzerrechten. Die Etagen oder Etagengruppen werden als Ausweis-Leseeinheiten des Gebäudes angesehen und können daher in Gruppen von Leseeinheiten oder in Zutrittsprofile aufgenommen werden.

Das Multistandort-Management bei einem Gebäude mit mehreren Mietern ermöglicht es, zu filtern, welche Etage von welchem Benutzer verwaltet wird, wobei zu berücksichtigen ist, dass es sich bei einer Zentrale um einen Einzelstandort handelt. Etagen können beispielsweise wie folgt organisiert werden:

- Der Urheber, Systemverwalter darf die Zutrittsberechtigungen aller Stockwerke verwalten
- Jeder Mieter verwaltet Zutrittsberechtigungen nur zu den angemieteten und den Gemeinschaftsetagen (Erdgeschoss/Empfang, Parkplätze, Kantine...) und nur für sein Personal durch Entitäten

Ein Mieter kann somit Zutritt zu seinen eigenen Etagen und zum Gemeinschaftsteil gewähren. Doch der Systemverwalter des Büroturms beispielweise behält die Kontrolle über die Zeitpläne der gemeinsamen Etagen. Um diese Funktion zu nutzen, ist eine speziell für das Aufzugsmanagement vorgesehene Zentrale einzusetzen.

FAHRZEUGZUFAHRT UND PARKPLATZMANAGEMENT

MICROSESAME kann für die Fahrzeugzufahrt vorgesehene Leseeinheiten, wie Fernleseeinheiten (mit Fernbedienung oder aktiven Ausweisen) oder Kfz-Kennzeichenleser oder QR-Codes überwachen.

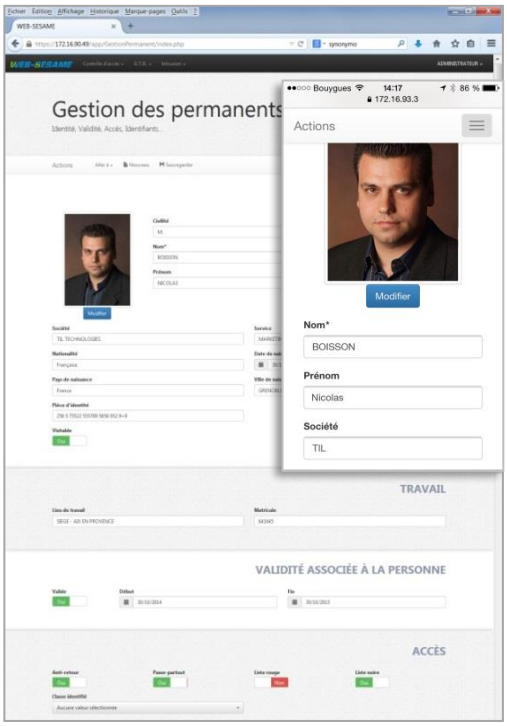
Diese Funktion erleichtert das Management von Fahrzeugströmen, insbesondere zu Stoßzeiten, und erhöht den Benutzerkomfort.

Die Integration in **MICROSESAME** ist transparent: Fernsteuerungen oder -Ausweise senden, wie bei jedem anderen Ausweis auch eine Nummer. Kfz-Kennzeichen werden direkt in der User-Kartei (bis zu 99 Kfz-Kennzeichen pro Benutzer) verwaltet.

Die integrierte Verwaltung von ID-Mitteln dient nicht nur der Zufahrtkontrolle, sie liefert auch beispielsweise folgende Informationen:

- Gesamtanzahl der Fahrzeuge
- Auslastung nach Mitarbeitertyp, Abteilung oder bei Gemeinschaftsparkplätzen Firma
- Die Volumina und Belegungszeiten für Gebühren oder Neuabrechnungen...

WEB-MANAGEMENT VON BENUTZERN



Zur vereinfachten Nutzung der Zutrittskontrolle stehen neben Server- und Heavy-Client-Schnittstellen (User-Karte siehe Seite 11) auch „Thin“-Webschnittstellen zur User- und Besucherverwaltung zur Verfügung.

Von jedem mit Internetbrowser und -verbindung ausgestatteten PC oder Mobilgerät aus unterstützt die neue **WEBSESAME**-Schnittstelle:

- Die Suche und Anzeige von User-Karteien nach mehreren Kriterien
- Das Anlegen oder Ändern von Karteien, insbesondere das Zuordnen eines Bilds (Schnellaufnahme per Smartphone oder Tablet).
- Die Vergabe von Zutrittsprofilen und bereits vorhandenen ID-Mitteln.
- Import/Export von Usern/ID-Mitteln

Dieselben Funktionen stehen für die Verwaltung von Besucher-Karteien (außerhalb des Standorts) zur Verfügung.

Auch andere Zutrittskontrollschnittstellen wie zum Beispiel die Terminverwaltung (externe Besucher) oder die Abfrage des Zutrittskontrollverlaufs stehen im Web-Modus zur Verfügung.

Die Ergonomie von **WEBSESAME** ist für eine Nutzung auf Tablets oder Smartphones (responsive) optimiert:

- Selbstanpassende Bildschirme (Auflösung und Ausrichtung)
- Automatisches Ausfüllen von Feldern und Bildansicht
- Ankreuzfelder

BESUCHERVERWALTUNG

TERMINPLANUNG UND BESUCHEREMPFANG

An einem mit Zutrittskontrolle ausgestatteten Standort müssen unternehmensfremde Personen registriert, begleitet und sogar mit einer Identifikation versehen werden, damit sie sich in die für sie zugelassenen Bereiche begeben dürfen. Dieses Ziel ist in der Sicherheitspolitik des Endkunden eigens oder gesetzlich geregelt (ANSSI-Leitfaden für wichtige, essenzielle Bereiche).

Die Besucherverwaltung von **MICROSESAME** unterstützt die Planung und die Verwaltung von Besucherströmen und die Optimierung des Registrierungsvorgang. Sie vereint Flexibilität und Sicherheit. Zur optimalen Anpassung an die Bedürfnisse, Abläufe und Organisation des Endkunden bietet die Lösung voreinstellbare Standardparameter (Bsp. standardmäßige Termindauer) und Funktionsgrenzen entsprechend dem Benutzerprofil des Antragstellers, Genehmigers, Empfangsmitarbeiters.

Diese Funktion von **MICROSESAME** wird über drei spezifische Schnittstellen gewährleistet:

- Die **WEBSESAME**-Benutzeroberfläche
- Empfangsarbeitsplatz (Heavy Clients)
- Empfangsterminals (Heavy Clients)

Die Ergonomie dieser Schnittstellen wurde gezielt entworfen, um sowohl eine verfeinerte Benutzeroberfläche zu bieten, als auch eine rasche Verarbeitung zu gewährleisten und zwar durch:

- Zugriff auf funktionale Registerkarten gemäß User-Rechten und vorgeschlagenen oder auferlegten Standarddaten
- Selbstanpassende Web-Bildschirme für Auflösung und Navigation (Hoch-/Querformat, Anordnung der Felder nach Breite...)
- Erfassung von und Suche nach Besuchern mit automatischer Vervollständigung der Eingabefelder,
- Hinzufügung von Bildern durch Sofortaufnahme (Webcam, Tablet oder Smartphone)

Die **WEBSESAME**-Benutzeroberfläche ist für alle zugelassenen Benutzer von Büro-PCs mit Webbrowser im Intranet des Unternehmens erreichbar. Es können Besucher angelegt, Termine geplant und/oder genehmigt und die notwendigen Informationen (Zeitfenster, Zutrittsprofil, Begleitperson, Besucherkartei...) vervollständigt werden.

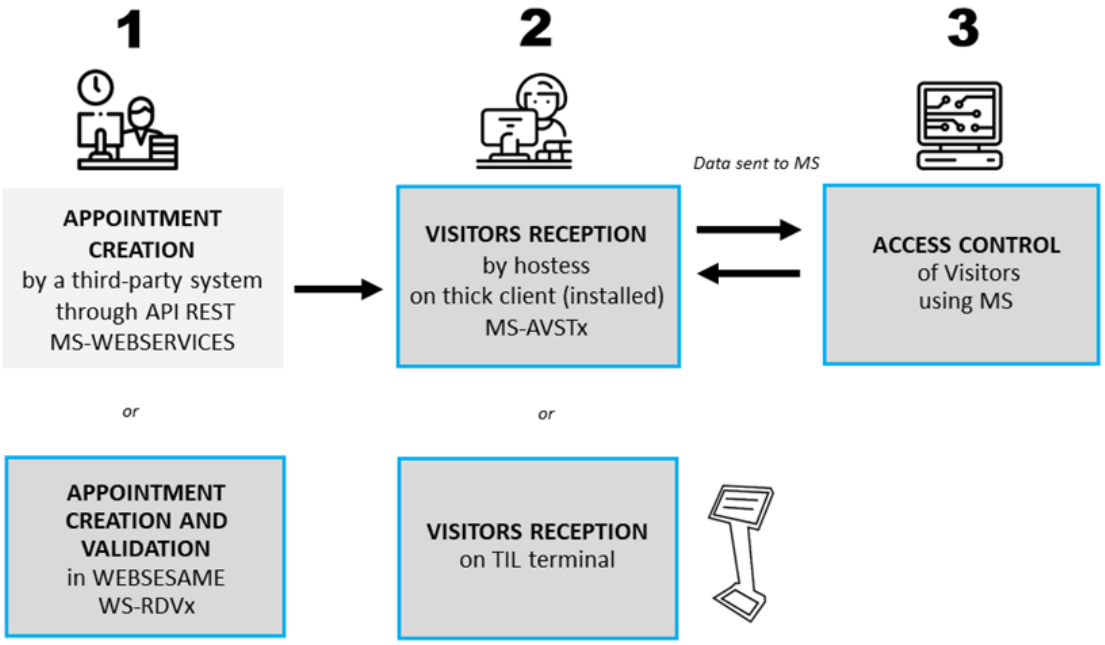
Der in der Heavy-Client-Arbeitsplatz am physischen Gebäudeeingang installierte Besucherempfang ermöglicht eine reibungslose und vollständige Nutzung: Zuweisung und Rückgabe von wiederverwertbaren Besucherausweisen, Registrierung angekündigter Besuche, Scannen von Ausweispapieren oder Druck von personalisierten Zutrittsausweisen. Die „Heavy“-Clients müssen über das Netzwerk mit dem **MICROSESAME**-Server in Verbindung stehen.

Das Touchscreen-Empfangsterminal mit integriertem QR-Code-Scanner bietet auf seinem Bildschirm zwei Auswahlmöglichkeiten:

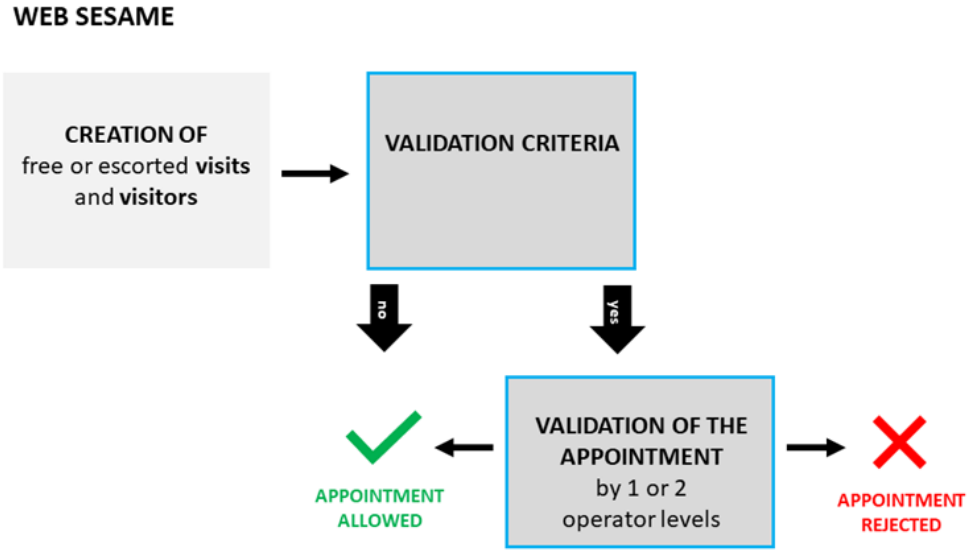
- Für den angekündigten Besucher, der seinen per E-Mail zugesandten QR-Code einscannt
- Für den unangekündigten Besucher, der seine Kartei und seine Besuchsanfrage selbst erstellt

Ein spezielles Dokument zur Besucherverwaltung ist bei Ihrem bekannten TIL-Ansprechpartner erhältlich.

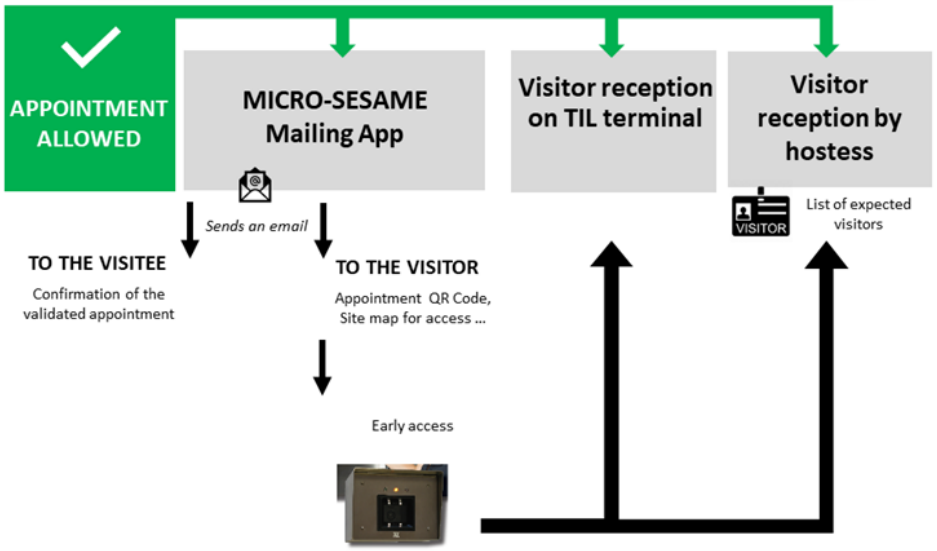
VEREINFACHTER WORKFLOW DER BESUCHERVERWALTUNG



DETAILLIERTER WORKFLOW DER BESUCHERVERWALTUNG



Bei Freigabe eines genehmigungspflichtigen Termins:



Diese Lösung bietet folgende Vorteile:

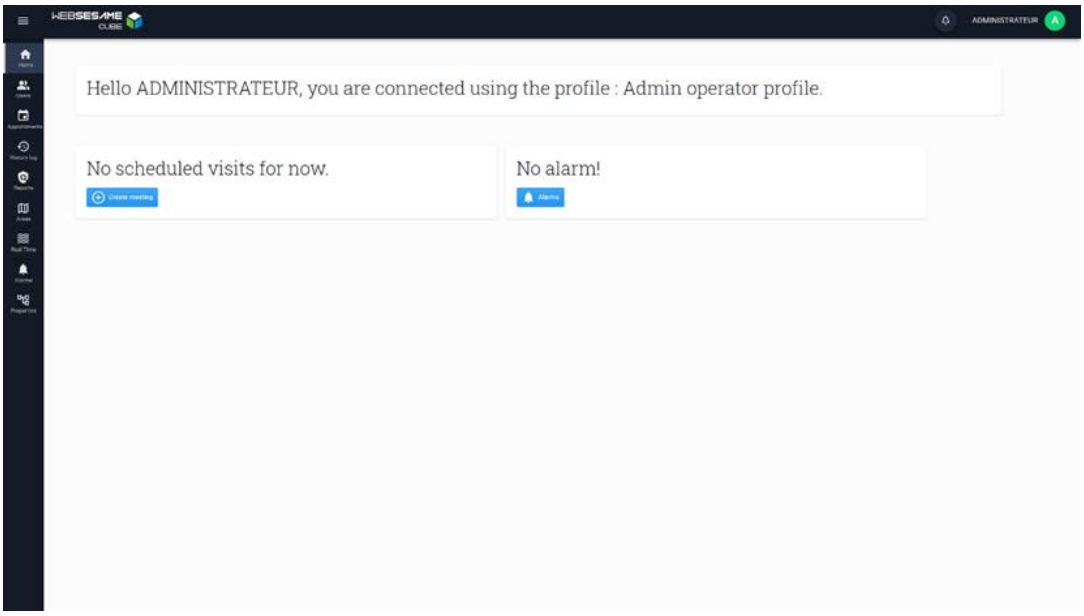
- Besucherverwaltung mittels vollständig in Zutrittsmanagement integrierten Workflows
- Optimierter, reibungsloser und sicherer Besucherempfang und -Zutritt zu den Besuchsbereichen
- Wahlmöglichkeit zwischen freien und geführten Besuchen, Erfassung spontaner Termine
- Terminbestätigung nach Kriterien, die vom Kunden individualisiert werden können
- Genehmigung vorzeitiger Besucherzugänge (Parkplätze usw.)
- Erfassung von Besuchen zulässiger Besucher vom PC-Arbeitsplatz aus
- Einhaltung der ANSSI-Anforderungen
- Angebot von zwei Arten von Besucherempfängen (mit Empfangspersonal und/oder über Besucher-Empfangsterminal mit Touch Screen) für zwei Problemstellungen (Sicherheit, Kosten)
- Ausgabe kundenindividueller Besucherausweise (Design, Name, Farbige Codes ...)

In **WEBSESAME** sind für die Besucherverwaltung zwei Icons sichtbar: „Besucher/User“ und „Termine“

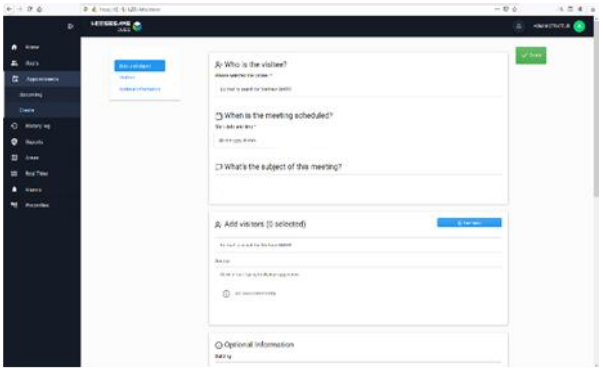
DIE BESUCHERVERWALTUNG ermöglicht die Eingabe aller erforderlichen Informationen zur Erfassung eines Besuchers einschließlich der Berechtigung, sich allein oder mit einer Begleitung am Standort zu bewegen. Systembenutzer können die Bezeichnung der Eingabepflichtfelder ändern. Die nutzbaren Funktionen für das Zutrittsmanagement sind im Vergleich zum **MICROSESAME**-PC-Arbeitsplatz (Heavy Client) auf das Wesentliche reduziert, damit Tätigkeiten vom Empfangspersonal oder einem beauftragten Sicherheitsdienst erleichtert und beschleunigt werden:

- Zutrittsprofile für zugelassene Besucher
- Vergabe einer verfügbaren Besucher-ID (Ausweis)
- Einstellung der Ausweisgültigkeit, Anti-Rückkehr-Funktion, Schwarze Liste-Aktivierung...
- Besucher-„Status“, der nur für bestimmte Benutzer sichtbar ist

Das ganze Prozess dient der Erstellung begrenzter Zutrittsberechtigungen für einen begrenzten Zeitraum



DIE TERMINVERWALTUNG ermöglicht das Suchen oder Erstellen von Terminen mit:



- Der besuchten und durch den Status „besuchbar“ autorisierten Person mit Angabe von
  - Datum, Uhrzeit und Zusatzinformationen (Termingrund...)
- Einem bereits bekannten Besucher oder direkt in einem vereinfachten Popup-Fenster schnell neue erstellten Besucher (Vermeidung von doppelter Erfassung)
- Zuweisung von Zutrittsprofilen, unter den für Besucher und Benutzer autorisierten Varianten (Multistandort-Management, Benutzerklasse)
- Besuchsortbezeichnung in einem Eingabefeld mit vordefinierter Drop-Down-Liste für Multistandort-Projekte. Eine E-Mail-Benachrichtigung an Genehmiger der betroffenen Standorte ist möglich.
- Frühzeitiger Zutrittsfreigabe, um von einem Parkplatz mit QR-Code-Leseeinheiten vor eigentlichem Termin zum Empfang gelangen zu können. Ein QR-Code (oder PIN-Code) wird dann per E-Mail an den vorgesehenen Besucher gesendet.
- Der vorgesehenen Begleitung, unter den zur Auswahl stehenden Begleitpersonen. In diesem Fall erfordert die Zutrittsöffnung eine doppelte Authentifizierung, zunächst die des Besuchers und danach die von jeder Person mit dem Status Begleitperson binnen eines vordefinierten Zeitfensters. Sowohl für den Besucher als auch für den Begleiter müssen die autorisierte Zutrittsprofile vorliegen.
- Gegebenenfalls Hinzufügung spezifischer Anweisungen.

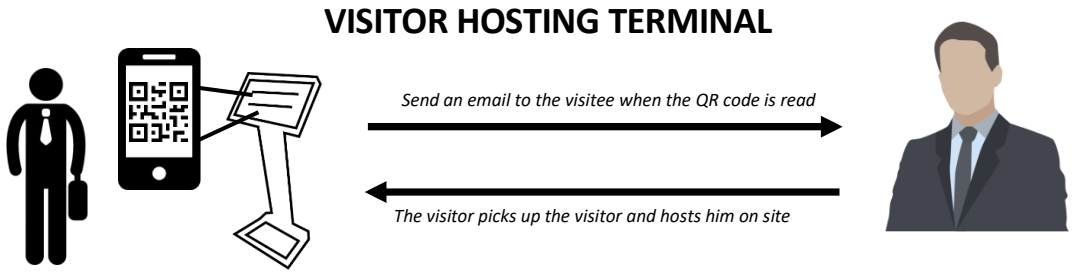
EINE FUNKTION „TERMINBESTÄTIGUNG“ ist auf dieser Schnittstelle ebenfalls verfügbar, falls unternehmensinterne Prozessregeln die Termingenehmigung durch einen oder zwei Instanzen (Sicherheitsbeauftragten, Abteilungsleiter...) vorsehen:

- Bis zu zwei Genehmigungsstufen können eingestellt werden (Benutzerstufe 1 und 2)
- Die Bestätigungskriterien für diesen automatisch oder durch einen oder zwei Benutzer genehmigten Termin können für jeden Endkunden durch Anfragen gemäß Eingabedaten konfiguriert werden, die mit dem Anfragesteller (Abteilung, Status…), dem Besuch (Datum, Ort...) oder dem Besucher (Nationalität, Firma...) in Relation stehen.
- Individualisierte E-Mail-Benachrichtigungen können automatisch an die betreffenden Personen (Besucher, Besuchter, Genehmiger) gesendet werden, um sie über den Bestätigungsprozess und den Besuchsstatus (ausstehende Bestätigung, zu bestätigen, genehmigt, abgelehnt...) zu informieren.

Sobald der Termin genehmigt wurde (automatisch oder vom Benutzer), kann er nicht mehr geändert werden. Er kann jedoch dupliziert werden.

BESUCHEREMPFANG

DETAILLIERTER WORKFLOW ZUM BESUCHEREMPFANG AM EMPFANGSTERMINAL:



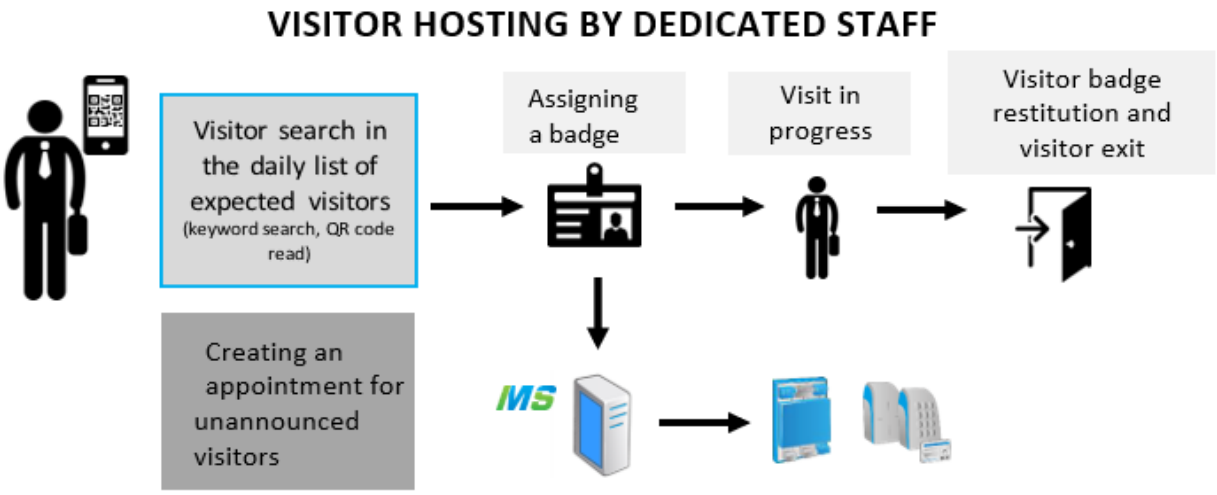
Touch-Terminal mit integriertem QR-Code-Scanner mit 2 Auswahlmöglichkeiten auf dem Startbildschirm:

1. Für den angekündigten Besucher: QR-Code scannen
2. Für den unangekündigten Besucher: eigene ID-Kartei und Besuchsanfrage selbst erstellen

Vorteile dieser Besucherempfangsmethode am Empfangsterminal:

- Vereinfachte Besucherregistrierung durch schlanken Workflow
- Kostensenkung (Empfangspersonal, Besucherausweise...)
- Begleitung von Besuchern durch Besuchte, die als einzige über Ausweis und Zutrittsrecht verfügen
- Nachverfolgung von Besuchen und Besucherzutritten am Standort im **MICROSESAME**-Verlauf

DETAILLIERTER WORKFLOW ZUM BESUCHEREMPFANG DURCH EMPFANGSPERSONAL::



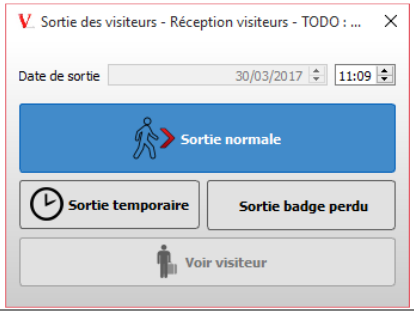
BESONDERE VORTEILE DER BESUCHEREMPFANGSMETHODE DURCH EMPFANGSPERSONAL:

- Zuweisung von Besucherausweis und Zutrittsberechtigungen in 10 Sekunden
- Auflisten, Orten der vor Ort befindlichen Besucher mit ihrer aktuellen Status (erwartet, in der Warteschleife, vor Ort, vorübergehender Austritt...) über das Besucher-Hosting-Menü
- Nachverfolgung von Besuchen und allen Besucherbewegungen mit dem **MICROSESAME**-Verlauf
- Mehrere Austrittarten möglich

HAUPTFUNKTIONEN FÜR EMPFANGSPERSONAL MIT IM BESUCHEREMPFANGSMENÜ:

- Besucherempfang und -schnellsuche
  - Suche nach Besuchstitel- oder Besuchernamen
  - Lesen des per E-Mail erhaltenen Besucher-QR-Codes über Handscanner
  - Sofern erlaubt, Erfassung eines unangekündigten Besuchs ohne vorherige Terminvereinbarung möglich
    - mit Zuordnung vorgesehener Besucherzutrittsprofile (Besucherparkplätze...).
    - mit Gültigkeitsdauer (mehrtätige Genehmigung und vorübergehende Ausgänge)
    - mit oder ohne Begleitung durch befugte Begleitperson (doppelte Authentifizierung)
    - mit möglichem Anschluss eines OCR-Scanner zum automatischen Hochladen der Personalausweis- und Reisepassinformationen in die passenden Eingabefelder
- Vergabe eines Besucherausweises durch einfache Ausweisprüfung an einem RFID-Tischlesegerät
- Aktualisierung des Besucherstatus: Den Besucher hereinlassen oder in die Warteschleife stellen (der Besucher ist registriert, wartet aber im Besucherempfangsbereich des Standortes).

- Für ankommende Besucher können mehrere individualisierte Dokumente erstellt und gedruckt werden (Besucherkarte, Besuchsschein, Lageplan, Fahrzeugberechtigungsschein, Besuchsgrund, Besuchstitel)
- Mögliche Schnittstellen zu externen Drittanwendungen für Besucher (Raumbuchungen, Schulungen...)
- Besucher herauslassen und Besuch beenden: Nach dem Besuch muss der Besucheraustritt gemeldet werden. Es sind mehrere Arten von Austritten möglich:
  - Normaler Ausgang: Beendigung des aktuellen Besuchs. Der Besucher verschwindet aus der Liste registrierter Besucher. Der Besucherausweis ist erneut verfügbar und wiederverwendbar
  - Temporärer Ausgang: Nachdem der Besucher den Standort vorübergehend verlassen hat, wird die Zutrittsberechtigung deaktiviert. Bei seiner Rückkehr muss er erneut registriert werden.
  - Ausgang und Ausweis verloren: Der Besucher beendet seinen Standortbesuch. Sein Ausweis wird jedoch nicht zurückgegeben (oder vernichtet). Der laufende Besuch wird beendet. Der Besucher verschwindet aus der Liste der registrierten Besucher. Der nicht zurückgegebene Ausweis steht für eine neue Zuordnung nicht mehr zur Verfügung.

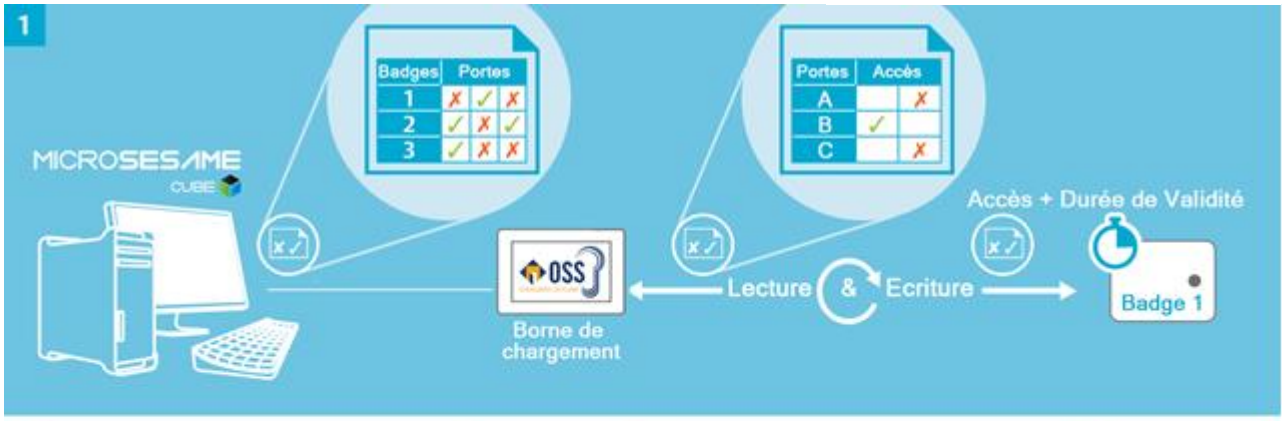


- ► Leseeinheit mit automatischem Austrittsstatus ohne erneutes Erscheinen am Empfang (Leseeinheit mit Karteneinzugsvorrichtung)
- ► Anzeige einer Besucherliste mit den unterschiedlichen Besucherstatus
  - Angekündigter Besucher: Besucher ist vorregistriert aber noch nicht am Besucherempfang erschienen
  - Ausstehende Besucher
  - Eingetretene Besucher: Der Besucher hat sich registriert, den Standort betreten und noch nicht verlassen
  - Ausgetretene Besucher
  - Überschrittene Besuchszeit: Wenn das geplante Besuchszeitende überschritten ist und der Besucher den Standort noch nicht verlassen hat, wird ein Alarm angezeigt und ein Symbol weist auf die Zeitüberschreitung hin
- ► Erstellung von Besuchsverläufen oder Besucherlisten über Drucker oder EXCEL-Dateienexporte (angekündigte, ausstehende, vorübergehende Ausgänge...)
- ► Synchronisation mit Outlook-Kalendern über ICalendar-Datei (ICS) im Anhang der E-Mail an die Beteiligten möglich
- ► Bereinigung von Besuchern, die zu einem Termin nicht erscheinen

„OSS“-OFFLINE-ZUTRITTSKONTROLLE

MANAGEMENT AUTONOMER MECHATRONISCHER SYSTEME

MICROSESAME unterstützt nativ die Verteilungslogik von Offline-Zutrittsberechtigungen für mechatronische Schließsysteme. Dabei kodiert das System die Zutrittsberechtigungen direkt in die Benutzerausweise mit einer definierbaren Gültigkeitsdauer ein. Mechatronische Zylinder integrieren Intelligenz und Daten (Zutrittsgruppe, Uhr usw.) und entriegeln, wenn die Zutrittsrechte des Ausweises vom Schloss erkannt und validiert werden.



Die regelmäßige Aufladung dieser Rechte in Benutzerausweise kann erfolgen:

- ► Über an MICROSESAME angeschlossene Badge-Encoder (ab PRIME/HIGH SECURE): als Erstcodierungs- und Nachladen.
- ► An Rechteladeterminals (alle Bereiche): Erstverschlüsselung und Nachladen

- Über die Kabelgebundenen Leseeinheitendes Standorts (alle Sortimente), wenn sie kompatibel und an dedizierte MLP2-OSS-Module angeschlossenen sind: nur Nachladen von Rechten.

Die Rechtevergabe an unverbundene Zutrittspunkten erfolgt durch Benutzer wie üblich über dieselbe Schnittstelle "Benutzer/ID-Mittel", die er auch zur Verwaltung von angeschlossenen Leseeinheiten nutzt. Dadurch wird vermieden, dass zwei Schnittstellen oder Datenbanken miteinander kommunizieren müssen.

Diese Systemflexibilität ermöglicht es autonomen Zutrittspunkten sowie jedem Lesegerät am Standort, von den MICROSESAME-Funktionalitäten mit Multistandort-Management und der Vergabe von Zutrittsprofilen gleichmäßig zu profitieren.

Die zentralisierte Verwaltung autonomer mechatronischer Elemente bietet auch Vorteile für die Informationsübermittlung. Bei jedem Passieren eines Aufladeterminals (Updater) werden folgende Informationen in MICROSESAME hochgeladen:

- Verlauf von Ausweisdurchgängen.
- Alarme bei niedrigem Batteriestand.

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

- Verband verschiedener Hersteller von mechatronischen Schließsystemen:
  - ASSA ABLOY, DEISTER, UZ, DORMA KABA...
- Die in die Ausweise geschriebenen Daten (Zugriffsrechte etc.) sind allen Herstellern gemeinsam, die den Offline-OSS-Standard einhalten
- OSS-kompatible Schlösser unterschiedlicher Marken können Kartendaten & Zutrittsrechte auf die gleiche Weise auslesen. Der Endkunde kann den Schlosshersteller frei wählen

“CLIQ“-OFFLINE ZUTRITTKONTROLLE

VERWALTUNG VON ZYLINDERN UND ELEKTRONISCHEN SCHLÜSSELN

MICROSESAME verfügt nativ über einen Konnektor zur Integration der elektronischen Schlüssel-Verwaltungstechnologie CLIQ von ASSA ABLOY.

Bei diesem Offline-Zutrittskontrollsystem werden die Benutzerrechte in einem "aktiven" Schlüssel gespeichert. Im Gegensatz zu anderen Offline-OSS-Lösungen benötigen die Schließzylinder, in die die CLIQ-Schlüssel gesteckt werden, keine Stromversorgung oder Batterie. Der Schlüssel enthält die notwendige Energie, um die Übereinstimmung zwischen den Zutrittsberechtigungen und des zu entriegelnden Zylinders zu überprüfen.

Wie bei jedem Offline-System erfordert die Aktualisierung der Zutrittsberechtigungen identifizierter Benutzer gelegentliche Aktualisierungsvorgänge:

► Entweder an einer CLIQ-Ladestation.

► Oder über ein Smartphone mit der mobile CLIQ CONNECT-App.

Die Integration in **MICROSESAME** ist einfach und die Konfiguration erfolgt in 5 Minuten dank des Imports von Schlüsseln, Zylindern und Terminals aus dem mit **MICROSESAME** verlinkten CLIQ WEB MANAGER: :

► CLIQ-Schlüssel werden als ID in **MICROSESAME** importiert.

► Zylinder und Zylindergruppen werden als belegbare Elemente als Zutrittspunkte importiert.

► Die Zuweisung von Zutrittsberechtigungen an Zylindern und Zylindergruppen erfolgt wie bei herkömmlichen RFID-Einheiten im System: in den Menüs „User“ und „Zutrittsprofile“ von **MICROSESAME** oder **WEBSAME**.

► Das Ladeterminal ist ein überwachbares Element. Ein sogenanntes „Überwachungsobjekt“ mit Verbindungs- und Fehlereigenschaften ist verfügbar.

AUSWEISKODIERUNG

ELEKTRISCHE PERSONALISIERUNG

Die elektrische Ausweispersonalisierung (MS-ENCODBADGE) ist eine **MICROSESAME**-Softwareoption, die das Schreiben von Daten auf Ausweisen der Mifare-Familie ermöglicht.

Die Software verwaltet die Kodierung der marktüblichen Formate: Mifare Classic, Mifare Desfire EV1, insbesondere durch Festlegung der Stelle (Bsp.:Mifare Classicr, Mifare Desfire-Anwendungen und -Dateien) und des ID-Formats (dezimal, hexadezimal, alphanumerisch...)

Mehrere Anwendungen mit mehreren IDs können gleichzeitig kodiert werden.

Die ID kann von **MICROSESAME** generiert oder von einer dritten Anwendung geliefert werden.

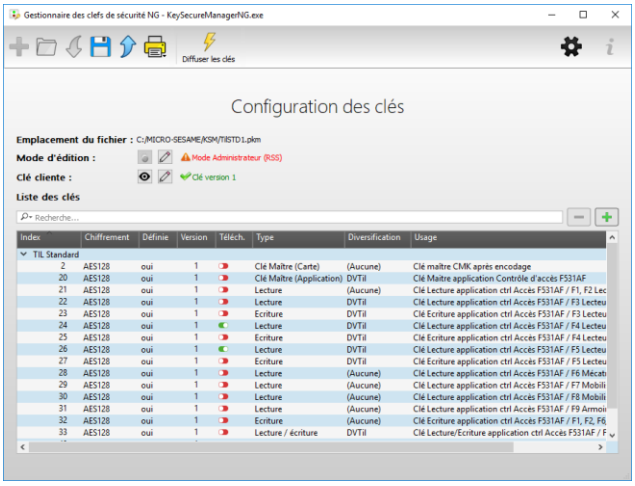
Die physikalische Ausweiskodierung erfolgt entweder einzeln oder serienweise an einem Tischkodierer oder direkt an einem Ausweisdrucker mit integriertem Kodierer. In diesem Fall ist es möglich, gleichzeitig für eine Population von Personen Folgendes automatisch durchzuführen:

- ► Individueller grafischer Kartendruck
- ► Kodierung für multiple Anwendungen
- ► Registrierung jedes Ausweises bei der zugehörigen Person

Mit dieser Lösung sind Geschwindigkeit, leichte Handhabung und Sicherheit gewährleistet

AUSWEISSCHLÜSSELVERWALTUNG MIT KSM

Die Software KEY SECURE MANAGER dient als Sicherheitscode-Verwalter für Ausweise. Sie ermöglicht dem Endkunden eine sichere und vollkommen individuelle Verschlüsselung:



- ► Ausweis-Schlüsselkonfiguration (gemäß verwendeten Schlüsselformaten und -typen).
- ► Generierung von Schlüsseln und Backup-Dateien
- ► Generierung der mit MS-ENCODBADGE verknüpften Datei für die Kodierung oder physische Registrierung des Ausweises an einer transparenten Leseeinheit eines **MICROSESAME**-Client-Arbeitsplatzes

Eine ausführlichere spezifische KSM-Dokumentation ist erhältlich.

AUSWEISPERSONALISIERUNG

Die Ausweispersonalisierung ist eine grundlegende **MICROSESAME**-Funktion, die die grafische Erstellung (Individueller Text nach Benutzerkarteien, fester Text, Logo, Bild, Piktogramm, QR-Code...) und den Thermoaufdruck umfasst.

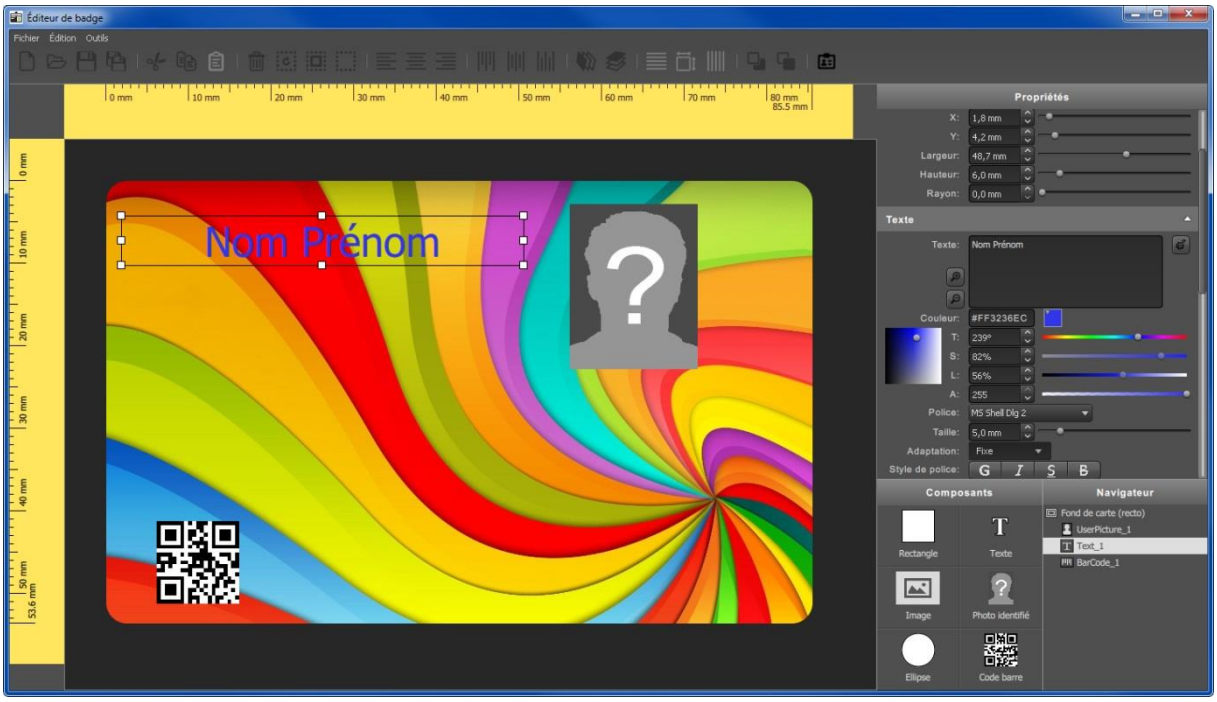
Für jede Person kann ein Bild aus einer bestehenden Datei, einem Scanner, einer Videoquelle oder von einer beliebigen Webcam gespeichert werden.

Der **MICROSESAME**-Grafikeditor ermöglicht das Erstellen einseitiger oder beidseitiger Kartenvorlagen sowie die Konfiguration verschiedener zu druckender Bezeichnungen (Name, Abteilung, Befähigung...). Diese gedruckten Daten können mit allen internationalen Schriftzeichen einschließlich der arabischen geschrieben werden.

So können dem Aufdruck Piktogramme beispielsweise hinzugefügt werden, die bestimmte Befähigungen des Karteninhabers (Elektro-Zulassung, explosionsgefährdete Atmosphäre, Lizenz...) symbolisieren sollen.

Mit dem Ausweisvorlagen-Editor können bereits erstellte Ausweisvorlagen exportiert werden, um sie nach dem Importieren an anderen Standorten desselben Kunden beispielsweise wiederzuverwenden.

Mit der Lösung können mehrere Ausweishintergründe nach Wahl (permanent, temporär, Besucher...) mit unterschiedlichen Eigenschaften erstellt und das richtige Format vor Seriendruck jeder Person zugewiesen werden.

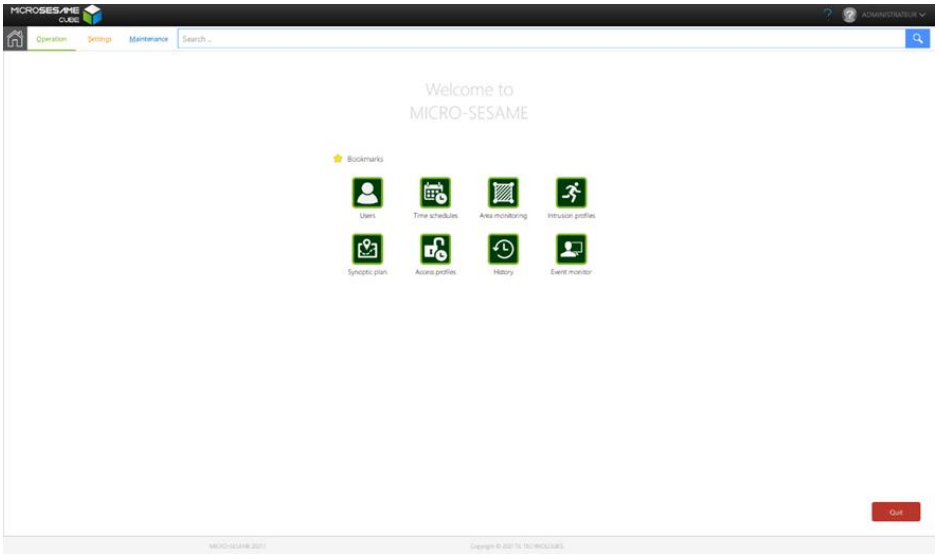


MONITORING UND ÜBERWACHUNG

Echtzeit-Ereignismonitor, Grafikübersichten, Zonenüberwachung

In **MICROSESAME** wird die Überwachung von Ereignissen, Alarmen, Zutrittskontrollfehlern, Einbruch, System, technischem Management und das Starten darauffolgender Aktionen (Qualifizierung, verschiedene Befehle, Anzeige von Videostreams...) mittels folgender Funktionen unterstützt:

- Übersichtsanimation
- Ereignis- und Alarmmonitor
- Bereichsüberwachung
- Verwaltung von NOMAN-Zonen (siehe entsprechendes Kapitel)



ALLGEMEINE ERGONOMIE

- Auf eine einfache und schnelle Bedienung ausgelegt ist die Benutzeroberfläche durch:
  - Eine einzige vereinheitlichte Benutzeroberfläche für das gesamte Sicherheitsmanagement
  - Die Unsichtbarkeit der dem Benutzer verbogenen Funktionen oder Daten
  - Die mehrsprachige Verwaltung der Benutzeroberfläche
  - Für bestimmte Funktionen spezifische Benutzeroberfläche (Benutzer, NOMAN, Monitor, Übersicht...)
  - Von einer großen Population nutzbare und über WEB zugängliche Funktionen (Termine...)
  - Die Navigation und getrennte App-Farbgebung: Betrieb – Einstellungen – Wartung

  Ein Menü-Suchfeld, welches das Finden sämtlicher Funktionen wesentlich erleichtert und das Anzeigen des eingeloggten Benutzers in der oberen Leiste

- Favoritenübersicht, Verknüpfungen und Liste der zuletzt geöffneten Anwendungen im Hauptmenü für einen schnellen Zugriff auf häufige Funktionenanforderungen

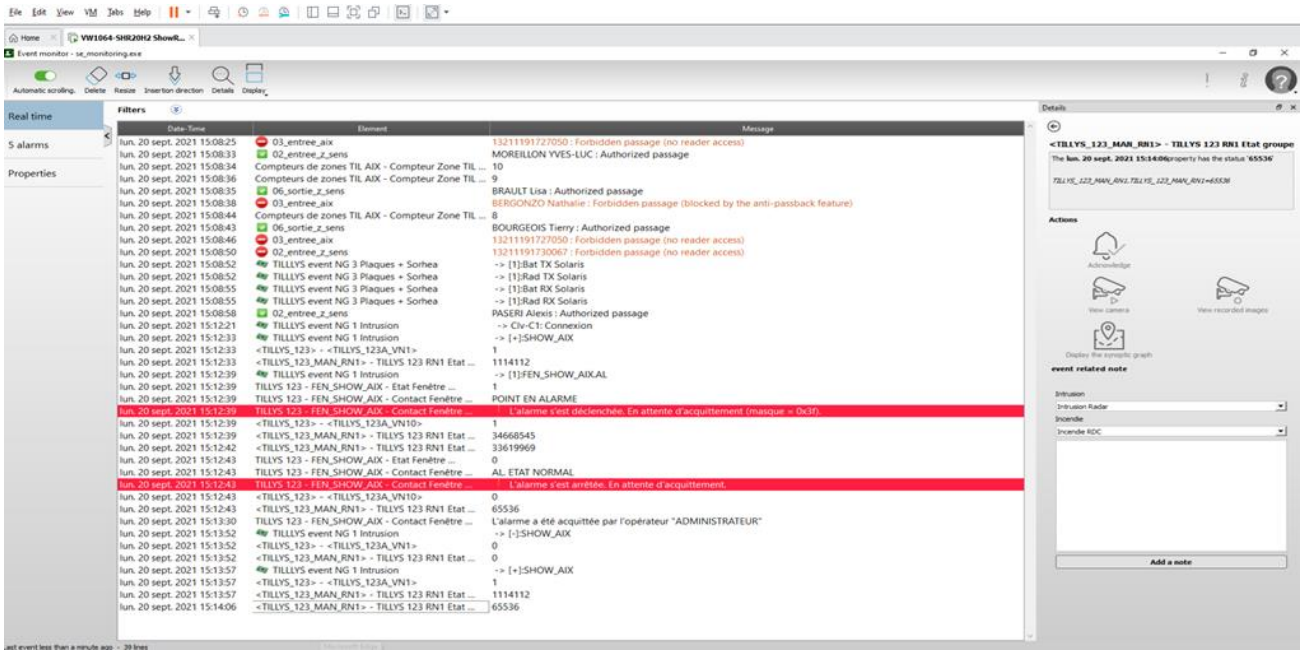
- Auto-Ausfüllen, damit die Menge der über Tastatur vom Benutzer einzugebenden Informationen durch einen passenden Ergänzungsvorschlag minimal bleibt
- Kohärenzprüfung im Eingabefeld während der Dateneingabe
- Benachrichtigung an Benutzer über Fehler oder Auslassungen je nach Eingabe
- Benutzerdefinierte Spaltendarstellung für Ergebnisansichten:
  - Auswahl gewünschter Felder und Daten in der Anzeige
  - Speicherung derer Position
  - Änderung durch Benutzer jederzeit möglich

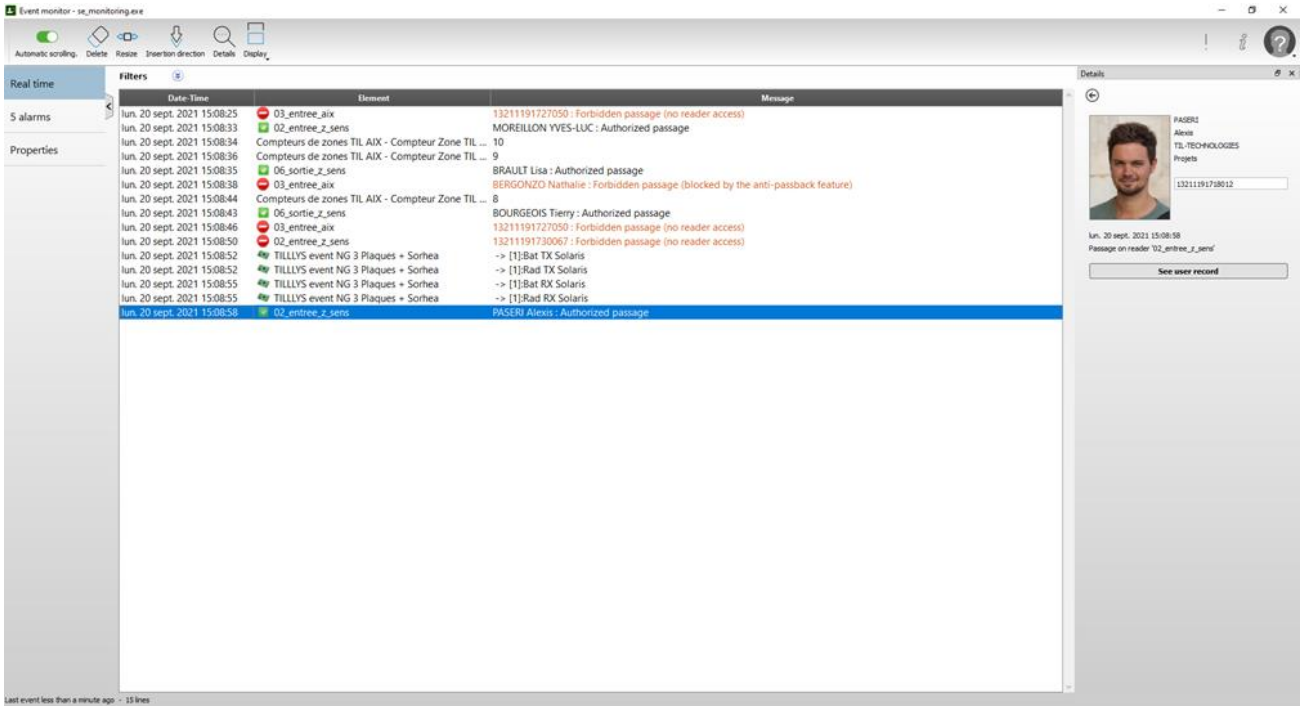
Interaktiver Monitor für Ereignisse, Alarme

Der Interactive Event Monitor bietet eine Zentralüberwachung aller Ereignisse, Alarme, Fehler, die von **MICROSESAME** empfangen wurden. Er zeigt sie in der Ereignisliste in Echtzeit an und ermöglicht die Qualifizierung von Alarmen, das Starten von Folge-Aktionen und Fernsteuerungen, die Erzwingung von Statuseigenschaften...

Jeder Benutzer sieht nur die für ihn autorisierten Standorte, Ereigniskategorien... In allen Fällen werden Alarmmeldungen, -Qualifizierungen und -löschungen mit einem Zeitstempel versehen und in der Datenbank zur späteren Abfrage archiviert (siehe Kapitel Verlauf und Benutzer).

REGISTERKARTE MIT EREIGNISLISTE





„EREIGNISMONITOR“

Die Registerkarte „Ereignismonitor“ zeigt in Echtzeit alle Ereignisse chronologisch gemäß dynamischer Filtereinstellung an.

Das automatische Scrollen von Ereignissen kann deaktiviert werden, damit dem Benutzer genügend Zeit zum Lesen der vor und nach dem untersuchten Vorfall aufgetretenen Ereignisse.

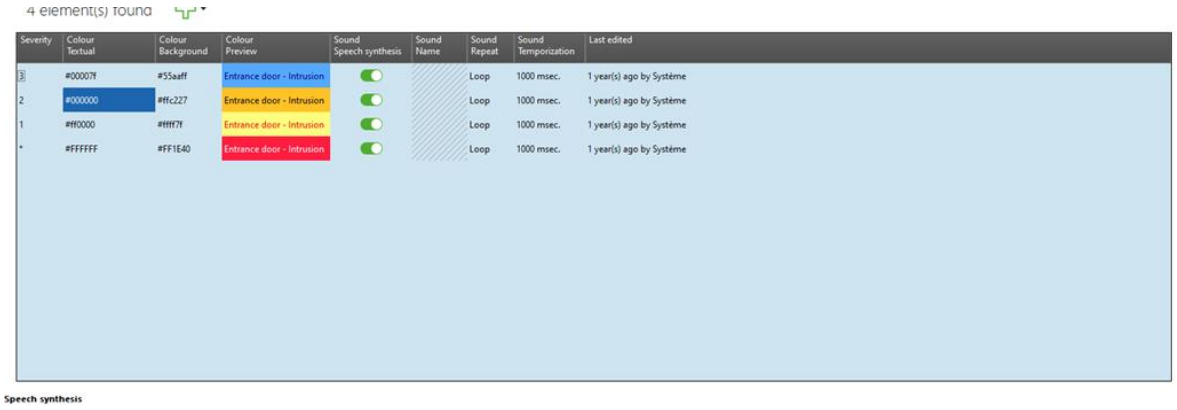
Ob lang oder kurz kann die Ereignisliste stets nach folgenden Werten dynamisch gefiltert werden:

- ► Standort (beim Multistandort-Management)
- ► Ereignisart (erlaubter oder verbotener Durchgang, Alarm, Fernbedienung, System, letzter Durchgang eines ID-Besitzers)
- ► Suchbegriff in der Schnellsuche (Name...)

„DETAILS“

Wird ein in der Liste angezeigtes Ereignis ausgewählt, können im Bereich „Details“ zusätzliche Ereignisinformationen und die zugehörigen verfügbaren Aktionen angezeigt werden:

- ► Alarm qualifizieren: Das Qualifizieren eines Alarms belegt, dass der Benutzer ihn gesehen hat. Für jedes als Alarm geltendes Ereignis kann konfiguriert werden, ob das Qualifizieren notwendig ist, oder nicht
  - Einzel-/Mehrfachqualifizierung bei Alarmen durch 1 oder X berechtigte Benutzer entsprechend den Alarmkategorien (CA, AI...) und deren Qualifizierungsstufen (Maske). Ein Alarm kann ggf. von mehreren Parteien qualifiziert werden müssen
  - Bei zu qualifizierenden Alarmen wahlweise blinken oder nicht
- ► Anweisung lesen
- ► Kamera Live anschauen
- ► Aufzeichnung einer relevanten Videosequenz des Alarm- oder Ausweisdurchgangs anschauen
- ► Zum Alarm passende Übersicht anzeigen
- ► Beim Durchgang eines Ausweises schnell auf die Informationen des Benutzers zugreifen, indem seine Kartei geöffnet und im Falle eines Antipassback-/Anti-Rückkehr-Alarms der Austritt vorübergehend entsperrt wird
- ► Beim Ändern eines Wertes den Status ermitteln, erzwingen, eine Fernsteuerung bewirken...
- ► Mit dem letzten Durchgang verbundenes Bild anzeigen
- ► Notizenschnittstelle öffnen (freie oder mit variablem Ereignis verknüpfte Notizen)



Alarme können nach einem Schweregrad von 0 (am wenigsten wichtig) bis 512 (am wichtigsten) unterschieden werden.

Die Farbcodes der Alarme sind:

- ► Rote Hintergrundfarbe und weißer Text: unbestätigter aktueller Alarm (Standard- und benutzerdefinierte Farbe). Diese zu bestätigenden Alarme können nach ihrem benutzerdefiniert konfigurierbaren Schweregrad 0 unterschieden werden, mit:
  - Text- und Hintergrundfarben nach Wahl und/oder
  - Audios, Sounds nach Wahl (Windows Sprachsynthese, Audiodatei)
- ► Weiße Hintergrundfarbe und schwarzer Text: laufender nicht qualifizierbarer Alarm
- ► Weiße Hintergrundfarbe und roter Text: qualifizierter aber noch laufender Alarm

REGISTERKARTE ALARME

Bietet einen umfassenden Überblick über laufende oder noch nicht qualifizierte Alarme. Qualifizierte und nicht mehr aktuelle Alarme verschwinden.

Die Alarme werden zunächst nach Schweregrad sortiert. Die meisten der in der Ereignisliste verfügbaren Aktionen zu Alarmen sind auch in dieser Ansicht verfügbar sowie darüber hinaus:

- ► Die Anzeige des Verlaufskurvenfensters eines Alarms (siehe Kapitel Grafik / Kurve)
- ► Der schnelle Zugriff auf die Parametrierung einer mit dem Alarm verknüpften Eigenschaft

REGISTERKARTE EIGENSCHAFTEN:

Ermöglicht die Überwachung und Suche der verschiedenen Arten von Eigenschaften, die Überwachung ihres Zustandes (Bsp. Benachrichtigung bei Erkennung einer offenen Tür) zu deren Bearbeitung und Interaktion mit ihnen.

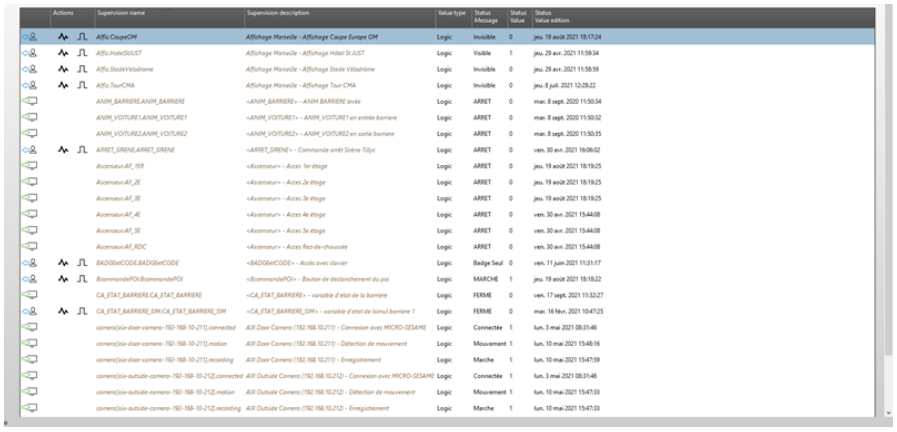
Ein Objekt ist ein vor Ort installiertes Element, das Informationen generiert (Bsp.: eine Tür).

Überwachungseigenschaften sind die verschiedenen für ein Objekt geltenden Zustände und Fernsteuerungen, die über **MICROSESAME** angesteuert werden können (Bsp. für ein Objekt Tür: Feststellanlage, Türkontakt, Einbruch, Öffnung).

Diese Ansicht ist für den Benutzer und den Integrator beim Einrichten eines Standorts nützlich, da sie eine Installationsdiagnose ermöglicht (Bsp.: Fernbedienung übergeben, Status ansehen, andere Fernbedienung übergeben, Übersicht öffnen).

Die möglichen Aktionen für diese typenabhängigen Eigenschaften sind:

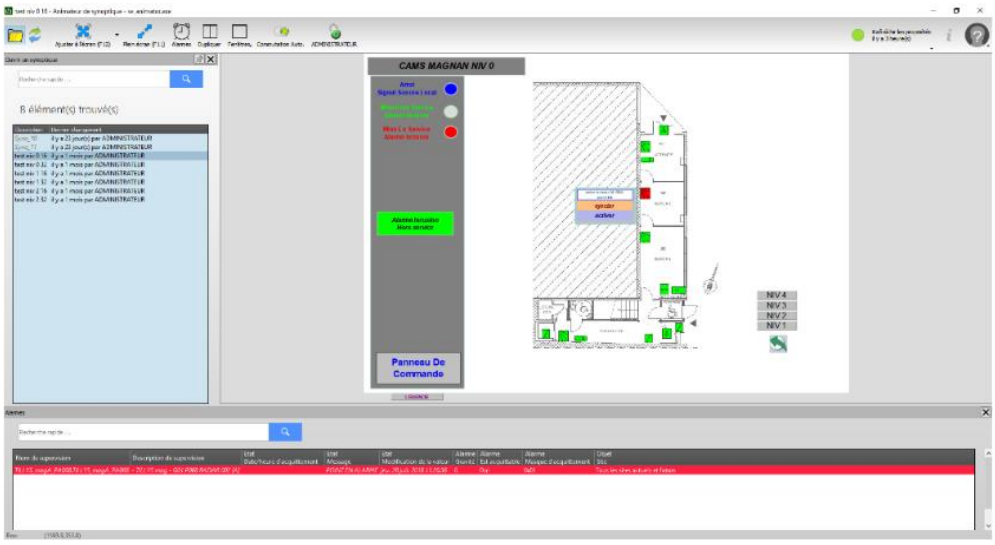
- ► Erzwingen: zur Sperrung von Eigenschaften, Bsp. vorübergehend bei Wartung, defektem Melder…
- ► Einen Befehl oder Impuls senden,
- ► Zugehörige Kurve anzeigen,
- ► Zugehörige Übersicht ansehen,
- ► Eigenschaft bearbeiten



Eigenschaften können mit verschiedenen Farben angezeigt werden. Beispiel Gelber Hintergrund mit braunem Text = erzwungener Zustand einer Eigenschaft.

Grafische Übersichtsanimation

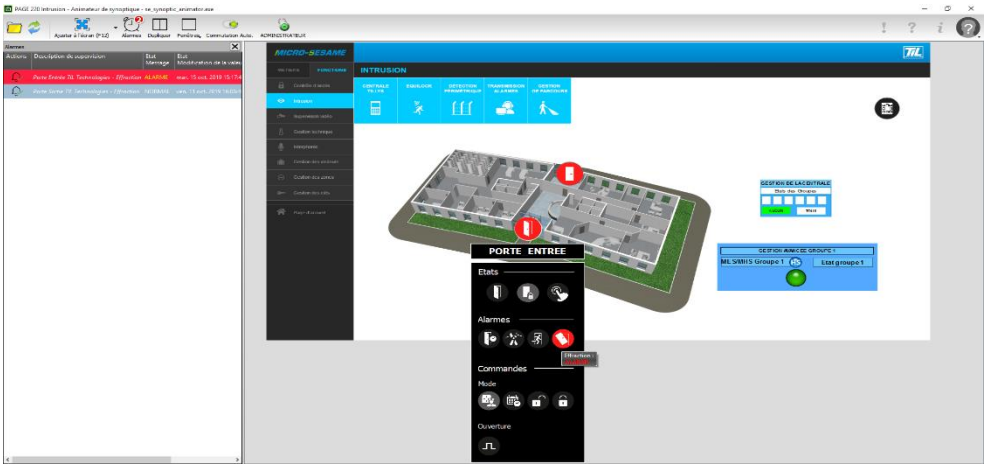
Die **MICROSESAME**-Übersichtsanimation ermöglicht die standortabhängige Personalisierung der Benutzeroberfläche für eine Überwachungsfunktionalität (Visualisierung der Alarme, der logischen Status und der digitalen Werte) und eine schnelle Reaktivität des Systemanwenders (Alarmbearbeitung nach Anweisungen, Starten von Fernsteuerungen, Aktionen). Unter Übersicht versteht man eine grafische Darstellung der zu überwachenden Installation. Sie besteht aus einer Reihe grafischer Objekte auf Hintergrundplänen.



Die übersichtsverbundenen Funktionalitäten sind insbesondere:

DER SCHNELL KONFIGURIERBARE HOCHGRADIG ANPASSBARE UND NATIV INTEGRIERTE ÜBERSICHTSANIMATOR UND -EDITOR, DANK:

- ► Den Objekteigenschaften (Informationen, Zustände, Befehle)
- ► Einer mit **MICROSESAME** gelieferten Bibliothek vordefinierter Objektmodelle (Zentrale, Port, MAXIRIS...), die Tätigkeits- und Überwachungskonfiguration umfassen:
  - Einfache schnelle Parametrierung durch Ziehen und Ablegen eines Objekts aus der Modellvorlage
  - Automatische Zuweisung der zu verkabelnden Automatisierungen, Eingänge und Ausgänge nach einem Standarddiagramm mit Auswahl per Mauschklick
  - Änderbarem Objektbild bei Aufrechterhaltung der gesamten Konfiguration
  - Beispiel mit dem Objekt „Standardtür“: Auswahl zur Aktivierung als Eingang: Türpositionskontakt, Steuerung, Notfallglasbruchschalter oder Türverriegelungskontakt
- ► Möglichem Erstellen, Importieren und Kopieren personalisierter Objekte/Eigenschaften in Projekt
- ► .svg-Unterstützung zum erleichterten Im- und Export von Gebäudeplänen
- ► Simulation aus dem Editor, um sich einen Überblick zu verschaffen,



- ► Objektanimation gemäß Gerätstatus (Farbe, Blinken, Audionachricht...)
- ► Umsetzung von Fernsteuerungen, diversen Benutzeraktionen über Objekte oder Tasten
- ► Verwendung des Übersichtsfensters, um von einer Anlagenübersicht zu einer anderen innerhalb einer Baumstruktur zu navigieren (Bsp.: erst Gelände-Gesamtansicht, dann Klick auf jedes Gebäude zum Vergrößern und Ansicht nach Gebäudestockwerk...)
- ► Verwendbaren Funktionen zur Übersichtsvergrößerung und -verkleinerung
- ► Schnellem Anpassen der Übersicht an den Bildschirm oder Wechseln in Vollbildmodus über 2 Shortcuts
- ► Verwalten und Überwachen von Alarmen direkt aus der Übersicht durch:
  - Spezielles abnehmbares Alarmfenster mit Widget/Zähler und Liste der Alarme (wie vom Ereignismonitor) mit den verschiedenen Anzeigefarben entsprechend ihrem Status und ihrer Qualifizierung
  - Die Möglichkeit, Alarme zu qualifizieren
  - Öffnen der Eigenschaften eines Objekts
  - Visualisierung der entsprechenden Kurven

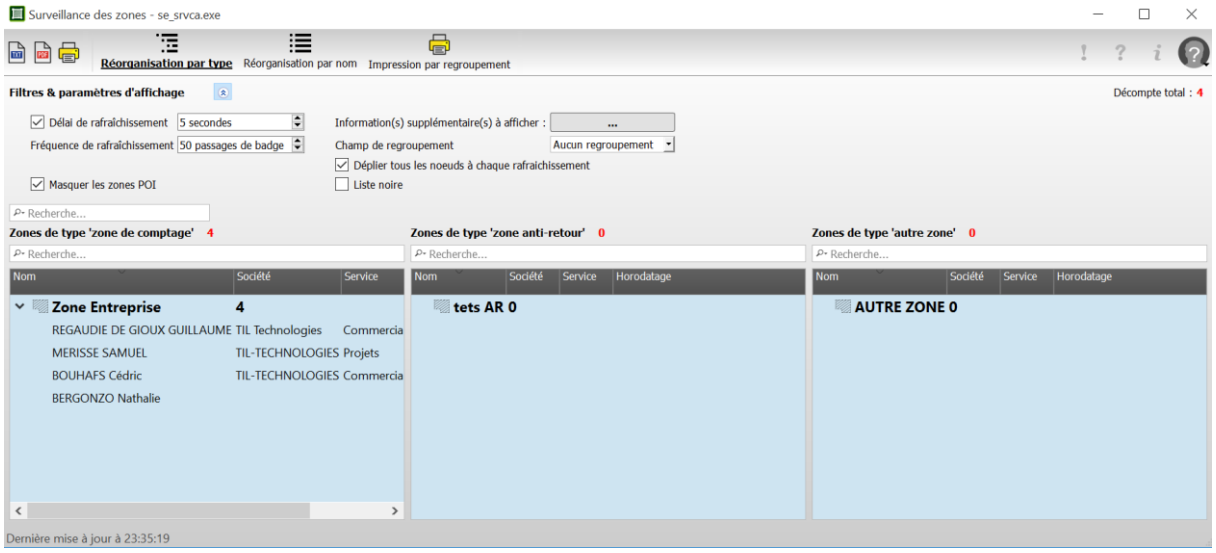
Zonenüberwachung

EINE ZONE IST EIN BESTIMMTEN REGELN UNTERLIEGENDER UND GESCHLOSSENER BEREICH (BÜRO, ETAGE, GEBÄUDE...) MIT

- Zwangsweise einer Leseeinheitengruppe am Austrittspunkt
- Zwangsweise einer Leseeinheitengruppe am Zutrittspunkt
- Einer physischen Undurchlässigkeit (Wand), die seine ordnungsgemäße Nutzung garantiert und das unkontrollierte Betreten oder Verlassen des Bereichs verhindert
- Einem notwendigerweise eindeutigen Zutrittsmechanismus zur effizienten Zählung

MEHRERE ARTEN VON ZONEN MIT EIGENVERWALTUNG SIND WÄHLBAR:

- Je nach Ein- und Ausgängen, Vor- oder Rückwärtszählen der anwesenden Personen
- Standort- oder Zeitabhängig gesteuerte Rückkehrsperre
- Notfallmanagement (siehe Kapitel NOMAN)
- Andere Bereichsarten (Bsp.: zur Verwaltung von Benutzern die auf der Black List stehen)



MIT DER ZONENÜBERWACHUNG IM SPEZIFISCHEM EINGABEFENSTER KÖNNEN:

- Die Liste und Anzahl der Personen in Echtzeit nach Zone und Zonenart dargestellt,
- Diese Listen gedruckt und im TXT- und PDF-Format exportiert,
- Verschiedene Anzeigeeinstellungen genutzt werden.

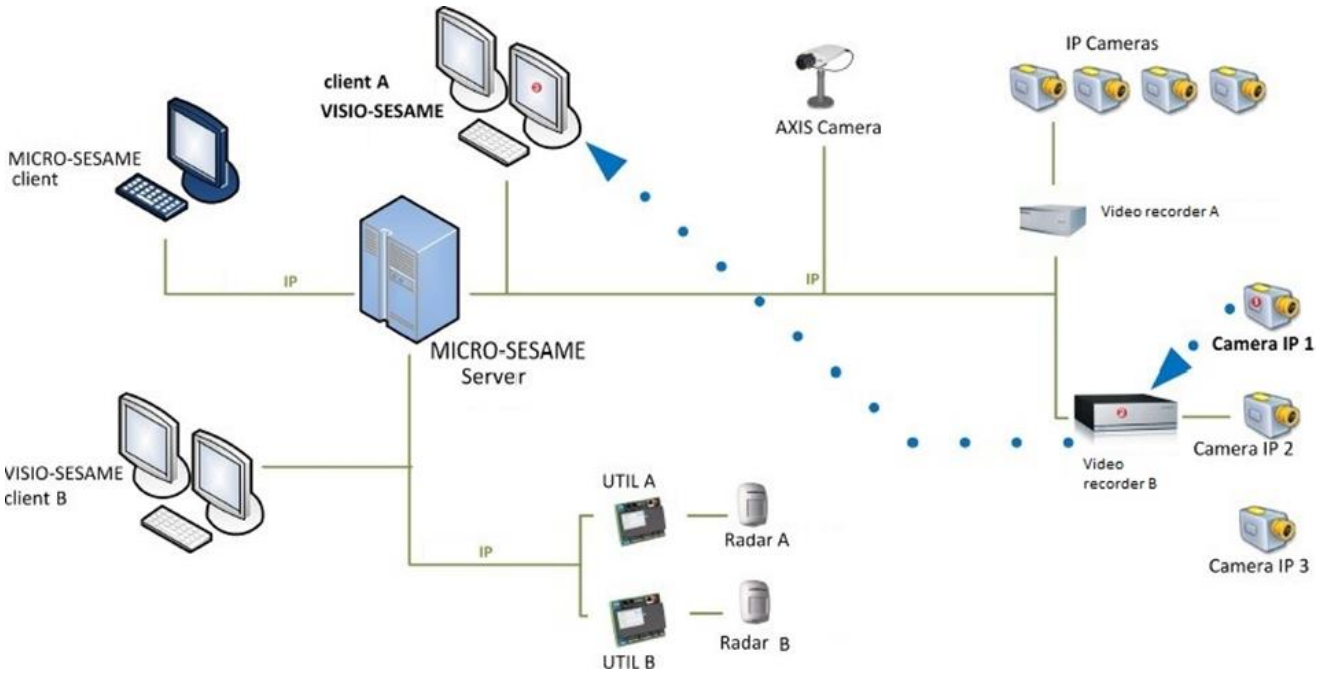
VIDEOÜBERWACHUNG

VISIOSESAME

Die Funktion VISIOSESAME von MICROSESAME CUBE ermöglicht:

- Über in MICROSESAME CUBE integrierte und optionale Anschlüsse den beidseitigen Dialog mit Zahlreichen Video Management-Systemen (VMS) und Videorekordern wie MILESTONE, GEUTEBRUCK, GENETEC, HIK, DAHUA, DIGIFORT, BOSCH…
- Die Steuerung aller Sicherheitsfunktionen über einen einzigen Supervisor für sämtliche Gebäudesysteme (Zutrittskontrolle, Einbruch, Brand, Gebäudetechnik).
- Die Durchführung der gängigsten Videoüberwachungsvorgänge von jeder MICROSESAME CUBE-Client-Arbeitsplatz aus mit einem oder mehreren VMS gleichzeitig:
  - Live-Ansicht
  - Aufnahmeauslösung
  - Empfang, Übermittlung von Ereignissen und Alarmen
  - Ansicht aufgenommener Bilder
  - Steuerung von Kuppelkameras

Durch die Videointegration in MICROSESAME CUBE wird die Bedienung für den Anwender vereinfacht. Interaktionen zwischen Video und anderen Systemen können vollständig automatisiert werden (Aktionen bei Alarmen oder Ereignissen), sodass eine hohe Verarbeitungsgeschwindigkeit und eine gesteigerte Effizienz gewährleistet werden können. Zur Nutzung unter bestmöglichen Voraussetzungen muss der **VISIOSESAME**-Client-Arbeitsplatz über mindestens zwei Anzeigemonitore verfügen.



DER TYPISCHE DATENFLUSS ZWISCHEN DEM VMS UND MICROSESAME IST, WIE FOLGT:

- Die Videokamera erkennt aufzunehmende Bilder
- Der Digitalrekorder zeichnet die erkannten Bilder auf
- Je nach Parametrierung des **MICROSESAME**-Servers, auf den der **VISIOSESAME** Client-Arbeitsplatz zugreift, fragt letztere die gespeicherten Bilder ohne Umweg über **MICROSESAME**-Server in Echtzeit aus dem Rekorder ab.
- Videobilder werden nicht auf dem **MICROSESAME**-Server oder -Arbeitsplatz, sondern sie bleiben ausschließlich auf VMS-Rekordern lokal gespeichert

VISIOSESAME BIETET FOLGENDE FUNKTIONEN:

EMPFANG UND VERSAND VON EREIGNISSEN, ALARMEN ÜBER MEHREREN VMS GLEICHZEITIG:

- **MICROSESAME** → VMS: Aufnahme starten/stoppen, Kuppelsteuerung mit Wahl von Voreinstellung und Zoom...
- VMS → **MICROSESAME**: Erkennungsalarm, Kamerafehler, Aufnahmefehler, angeschlossener Rekorder, angeschlossene Kamera...

NIEDRIGERE KONFIGURATIONSZEIT für die Videofunktion:

- Integrierte und optionale Konnektoren in MICROSESAME CUBE zur Verwendung von VMS-SDKs und nativen TIL-Objekten/-Eigenschaften für eine schnelle und einfache Parametrierung
- „Kamera“-Objekte im Übersichtseditor
- Import von VMS-Kamerabezeichnungen

ÜBERWACHUNG VON BETRIEBSALARMEN (Aktivitätserkennung per Video) und Betriebsalarmen (Verlust von Videosignalen oder andere Störungen) von den Rekordern über Ereignismonitor, Alarmbanner, Echtzeit wie alle anderen

DEDIZIERTES HARDWARE-ARCHITEKTURFENSTER

Kann auf Anfrage optional angezeigt werden

STEUERUNG DER KUPPELKAMERAS (Zoom, Wahl einer vordefinierten Vorposition) über ein entsprechendes Fenster

VOLLINDIVIDUALISIERBARER KAMERA-ANSICHTSBEREICH gemäß vordefinierten Szenarien, die einen oder mehrere Monitore in unterschiedlicher Zusammenstellung positionieren (3x3, 2x2...). Es können so viele Monitore hinzugefügt werden, wie Quellen vorhanden sind. Die Farben der Monitortitelleiste geben Auskunft über Inhalt und Status.

GLEICHZEITIGE ANSICHT DER VIDEO-LIVESTREAMS mehrerer VMS parallel durch Icon-Auswahl in Betriebsübersichten bei Alarm

AUTOMATISCHE AUSLÖSUNG VON AUFZEICHNUNGEN, die durch ein Ereignis (abgelehnter Ausweis an einer bestimmten Leseeinheit), einen Alarm, eine komplexe Steuerung, einen manuellen Benutzerbefehl aus der Übersicht beim Klicken auf eine Schaltfläche oder ein Objekt bzw. einen Befehl am Ereignismonitor ausgeführt werden kann

VIDEOWAND-MANAGEMENT (Matrixfunktion) zum Verwalten einer aus mehreren Bildschirmen bestehenden Videowand und zur Wiedergabe einer Kamera in einem bestimmten Bereich (Kachel)

DIE ÜBERSICHTSANIMATION bewirkt mit einem einfachen Klick auf ein Übersichtsobjekt:

- Das Starten der Live-Ansicht einer oder mehrerer Kameras
- Das Anschauen einer von einer bestimmten Quelle aufgenommenen Sequenz
- Das automatische Verknüpfen vordefinierter Parameter für die Wiedergabe (Auswahl einer Monitorgruppe, der gewählten Voreinstellung, der Videoquelle...)

STEUERUNG EINER VIDEOAKTION nach Ereignis oder Fernsteuerung durch Benutzer. Zum Beispiel automatische Voreinstellung einer Kuppelkamera bei Erkennung eines abgelehnten Ausweises.

ANSICHT DER AUFGEZEICHNETEN VIDEOSEQUENZEN in Verbindung mit einem Alarm direkt aus der Funktion „Verlauf“ von **MICROSESAME** zur Sicherung der Synchronisation von Informationen (eindeutige Verlaufsdatei für Zutrittskontrolle, Einbruch und Video), die so die Suche nach einer Videosequenz unterstützt ohne Kenntnis der Quelle, des Kameranamens, der Uhrzeit. Ein Klick auf dieses dem Alarm zugeordnete Videosymbol genügt und zeigt an, dass eine verknüpfte Videoaufzeichnung vorliegt

EINE SCHNELLAKTIONSLEISTE am unteren Bildschirmrand liefert zusätzlich zu den VCR-Tasten für das Aufnahmeverwaltung Direktbefehle, die je nach Rekorder aktiv sind: aktuellen Screenshot machen, Aufnahme aktivieren, Wiedergabemodus ändern (Live/Aufzeichnung), Monitor freigeben usw.

VMS- **MICROSESAME-**SCHNITTSTELLEN ÜBER KONNEKTOREN UND GATEWAYS

Die Liste der Lösungen, kompatiblen Versionen und zugänglichen Funktionalitäten wird mit nativ integrierten Konnektoren für TIL-Objekte/Eigenschaften und optionale Gateways für **MICROSESAME** ständig erweitert. Ein spezieller Leitfaden zu **VISIOSESAME** mit der Liste der VMS und ihrer mit **MICROSESAME** kompatiblen Funktionen ist bei Ihrem TIL-Partner verfügbar. Je nach VMS kann es vorkommen, dass einzelne SDK-Versionen und Funktionen nicht unterstützt werden. Die Kompatibilität sollte vor jeder Installation bei TIL TECHNOLOGIES daher gezielt erfragt werden.

Es wird dringend empfohlen, für die IT-Voraussetzungen gemäß Herstellerangaben des für die **VISIOSESAMe**-Clients zugänglichen Videorekorders bei den Video-Arbeitsplätzen (Bildschirmoberfläche, Betriebssystem, Grafikkarte, Netzwerkkarte...) und dem Netzwerk (Geschwindigkeit, Latenz...) zu sorgen.

Als Anhaltspunkt folgt hier eine Liste integrierter oder über Gateways mit **MICROSESAME** verbundener VMS:

- MILESTONE X-PROTECT (CORPORATE /EXPERT /PROFESSIONAL)
- GEUTEBRUCK Geviscope und G-Scope
- GENETEC Security Center
- VIDEOWAVE OneTrack
- HIKVISION iVMS-4200 (SDK v6.1.4.17)
- DAHUA DSS Express (DPSDK v1.0.001)
- DIGIFORT DGF Enterprise (SDK HTTP API 1.9.0)

Hinweis: Eine ASCII-Text-Gateway ist mit VMS in MICROSESAME CUBE ohne vorausgesetzte Nutzung von VISIOSESAME, sprich ohne Videostream in MICROSESAME, standardmäßig vorhanden (Option **LIC-GENERIC-TEXT**). Sie wurde mit VIVOTEK, AVIGILON, ARGOS implementiert.

PLUG-IN VON MILESTONE

Für diejenigen Kunden, die in erster Linie VIDEO nutzen und eine einheitliche Überwachung bevorzugen, stellt **MICROSESAME CUBE** die **LIC-MILESTONE-PAC**-Option mit dem integrierten MILESTONE ACCESS CONTROL-PLUG-IN bereit. Mit ihr kann wiederum die TIL-Zutrittskontrolle über die Überwachungsschnittstelle X-PROTECT von MILESTONE verwaltet werden.

Diese von MILESTONE zertifizierte Schnittstelle ermöglicht dem XPROTECT VMS-Supervisor:

- Die TIL-Alarme zu verwalten (**MICROSESAME** -> X-PROTECT)
- Den Durchgang dank Ausweise mit Bild zu verwalten (**MICROSESAME** -> X-PROTECT)
- Das Starten von Fernsteuerungen zum Öffnen des in **MICROSESAME** verwalteten Zutritts (**MICROSESAME** <- X-PROTECT)

Milestone Verified

Confirmation of Compatibility

Partner: TIL Technologies

Partner Product: Milestone Access Control Plugin 2018.3.6

MICRO-SÉSAME 2018.4.0

Milestone Product XProtect®: Corporate 2019 R3

Date of Verification: 23-12-2019

milestone VERIFIED

VISUELLE ZUTRITTSKONTROLLPUNKTE (VZKP)

Ist ein Zutritt mit Ausweis-Leseeinheit und Videokamera ausgerüstet, werden bei der **MS-CVA**-Option für Personen mit Ausweis das Bild des Ausweisinhabers und sein Videobild gleichzeitig abgebildet.

Ein dem Bild überlagertes Symbol zeigt den Ausweisstatus an (autorisiert, verboten, unbekannt).

Das Türöffnen kann je nach Sicherheitsstufe manuell, automatisch oder optional erfolgen. Weitere Aktionen sind konfigurierbar, Bsp. Beleuchtung einschalten, Meldung anzeigen, Einbruchserkennung im Bereich deaktivieren usw.

EINBRUCHMELDETECHNIK

Eine spezifische Dokumentation zum EMT-Management ist bei Ihrem TIL-Ansprechpartner erhältlich (Leitfaden zur Parametrierung für Einbruchschutz, Verkabelungsprinzip zur Einbruchserkennung, Leitfaden zur Parametrierung von Alarmübertragungen...).

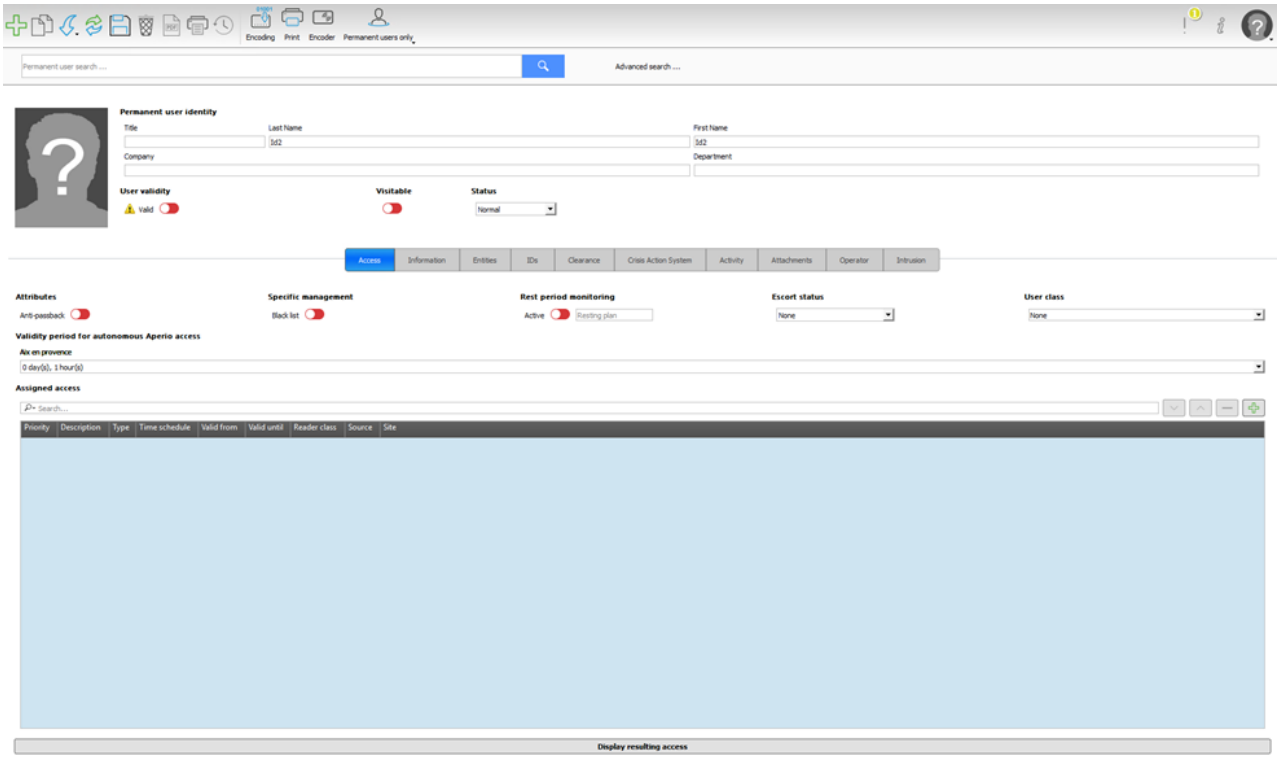
Die Verwaltung der Einbruchmeldetechnik ist in der TIL TECHNOLOGIES-Lösung nativ enthalten.

DER MICROSESAME-SERVER VERWALTET BENUTZER UND DEREN ZENTRALISIERTE EMT-BERECHTIGUNGEN FÜR MULTIPLE ZENTRALEN.

Der Benutzer und sein PIN-Code werden für beliebig viele Zentralen nur einmalig erstellt:

Ein „TILLYS-BENUTZER“ ist eine Person mit der Berechtigung zur Identifikation an der Steuerungstastatur der **TILLYS**-Zentrale. Jedem Benutzer sind ein Einbruchprofil, Benutzerrechte und ein automatisch generierter EMT-PIN zugeordnet. Ein Einbrucsprofil kann dupliziert werden.

NUTZUNGSRECHTE: Die Nutzungsrechte sind Aktionen, die ein Benutzer über die Steuerungstastatur ausführen darf (Menüzugriff, Scharf-/Unscharfschaltung einer Gruppe, Erteilung einer Ausnahmeregelung...). Jedem Benutzer können unterschiedliche Rechte zugewiesen werden



TILLYS CUBE-ZENTRALEN funktionieren autonom. Ihre Betriebsart wird zuvor in **MICROSESAME** konfiguriert und von dort heruntergeladen. Pro **TILLYS CUBE** Zentrale gelten folgende Leistungsgrenzen:

- 32 Punkt-/Meldergruppen
- 624 Melder/Punkte
- 150 lokale Benutzer
- Je Bus 8 Tasten-, 16 Sirenenfunktionen
- Eine integrierte „TIP“-IP-Fernmelde-Alarmfernübertragungsfunktion

TACTILLYS CUBE-TOUCHSCREEN-STEUERUNG zur autonomen lokalen Nutzung einer Eingabetastatur, die an einem **TILLYS**-RS485-Bussen angeschlossen ist, per Fingerdruck. Jeder Tastatur kann eine Liste von Meldergruppen zugeordnet werden, damit die Steuerung nur einen bestimmten Teil der Anlage kontrolliert.

- Neue moderne und ergonomische Tastatur mit 7-Zoll-Touchscreen, im Hoch- oder Querformat und optionalem Ausweis-Leseeinheit, dessen Entschlüsselungscode in einem HSM EAL5+-Modul geschützt aufbewahrt wird.

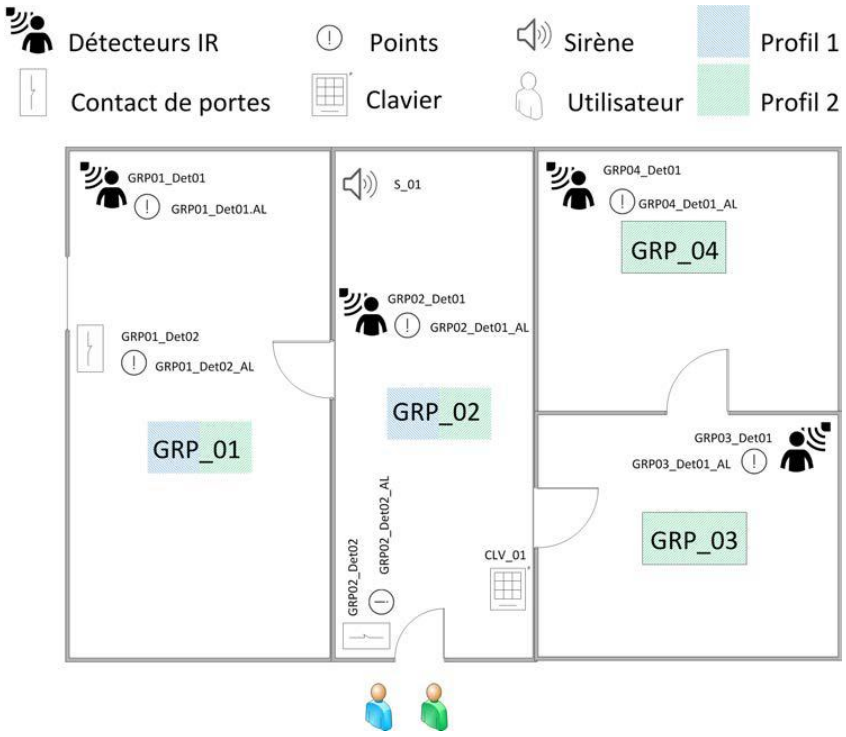
I/O-MODULE ZUR FERNSTEUERUNG, die mit den TILLYS-RS485-Bussen verbunden sind, an welchen Sensoren, Melder und Schaltungen angeschlossen sind (Sirenen, Lichtsteuerung...)

SPEZIFISCHE EINBRUCHMELDER, die mit **EQUILOCK**-Hochsicherheit über 2 Busse mit 32 kompakten in den Meldern ansprechbaren und integrierten Transpondern geschützt sind…

GROSSE REICHWEITE UND FUNKTIONALE ANPASSUNGSFÄHIGKEIT DURCH FOLGENDE MERKMALE:

- Jedem Punkt/Melder muss ein Punkttyp zugeordnet werden, der die Auslösung eines Alarms bedingt. Die möglichen Typen sind: Einbruchalarm, 24/24-Alarm, stiller Einbruchalarm, technischer Alarm, stille Systemstörung, Notruf, Brand
- Eine Meldergruppe steht für Melder-/Punkteeinheit in Verbindung miteinander (Gebäude, Etage, Abteilung, Umkreis, Bereich...), die von einem gemeinsamen Verwaltungsmodus profitieren, wie:
  - Scharf-/Unscharfschlatung
  - Senden von Alarmcodes an eine externe Service- und Notrufstelle (SOC)
  - Verwaltung einer oder mehrerer Sirenen
  - Implementierung eines Voralarm- oder Ausnahmemechanismus

Neue TACTILLYS CUBE-ALARMSTEUERUNG (2020)



Bsp.:

Profil 1 kann GRP_01 und GRP_02 aktivieren/deaktivieren.

Profil 2 kann alle Gruppen aktivieren/deaktivieren

PUNKTE IN STÖRUNG: Ein Punkt in Störung ist ein Punkt, der in bestimmten Fällen den Benutzer behindert (Bsp. bei Arbeiten...)

AUSSCHLUSS: Mit dieser Funktion kann die Überwachung eines Punktes vorübergehend oder endgültig ausgeschlossen werden, damit die Überwachung der Gruppe, zu der er gehört, ermöglicht und die systematische Auslösung von Alarmen oder eine Aktion der externen SOC vermieden wird, Insbesondere wenn beispielsweise dieser Punkt in Störung oder nicht so wichtig ist. Mehrere Ausschlussmodi sind möglich (gesperrter Ausschluss, manueller Ausschluss, automatischer Ausschluss, Ausschluss mit automatischer Wiederaufnahme, dauerhafter Ausschluss). Mit einer Wiederaufnahmeaktion kann der Ausschluss eines Punktes beendet werden.

Der VORALARM: entspricht einer konfigurierbaren Zeitverzögerung, mit der durch eine kurze Aktion von Sirenen die Anwesenden vor der bevorstehenden Scharfschaltung der EMA gewarnt und ihnen die Möglichkeit zu einer Ausnahmeregelung gegeben wird.

AUSNAHME: Funktion zum Verschieben einer automatischen Scharfschaltung für eine konfigurierbare Zeitdauer und auf ausdrücklichen Wunsch in einem Zeitprogramm (Trigger). Die Anforderung ist über die Einbruchtastatur durch einen TILLYS-Benutzer oder durch eine „Microcode“-Sonderprogrammierung oder einen Fernsteuerungsbefehl am MICROSESAME-Leitstand möglich.

INBETRIEBNAHME MIT TRIGGER: Ermöglicht die Scharfschaltung einer Gruppe der Zentrale (z.B. Gemäß Zeitplan). Automatisierte Unscharfschaltungen sind möglich, werden aber aus nachvollziehbaren Sicherheitsgründen nicht empfohlen.

ZEITÜBERSCHREITUNG: Eine Gruppe von Punkten kann für einen konfigurierbaren Zeitraum am Eingang oder/und Ausgang für den Zugriff auf die Scharf-/Unscharf-Steuerungstastatur verzögert werden, wenn sich diese in der überwachten Zone befindet. Die Zeitverzögerungswerte gelten für die Gruppe und die Verzögerung beim Eingang und/oder Ausgang sind für die betroffenen Punkte der Gruppe definierbar.

SCHARF-/UNSCHARFSCHALTUNG: Die Scharfschaltung einer oder mehrerer Meldergruppen ist der Vorgang, mit dem die Überwachung der mit dieser/diesen Gruppe(n) verbundenen Einbruchmeldepunkte aktiviert wird. Die Anfrage zum Start der Überwachung kann auf unterschiedliche Weise gestellt werden:

- Durch einen Benutzereingriff an der TACTILLYS CUBE-Tastatur
- Durch einen zugewiesenen Zeitplan
- Durch jede andere Aktion, Steuerungen nach Zutritt, sämtliche Ereignisse (Zutrittskontrolle, Einbruch, Technik, Brand...)

QUALIFIZIERUNG eines Alarmpunktes von der Aufsicht (siehe Überwachung)

FUNKTIONSUNTERDRÜCKUNG für einen durch die Aufsicht vorübergehend ausgeworfenen Punkt oder eine Punktegruppe (siehe Überwachung)

INTEGRIERTE „**TIP**“-IP-SENDERFUNKTION DER **TILLYS CUBE**-ZENTRALE:

Die **TILLYS CUBE**-Zentrale besitzt eine „**TIP**“-IP-Senderfunktion. Sie ermöglicht die Übertragung von Einbruchalarmen (auch für Zutrittskontrolle und Gebäudetechnik) über IP an eine Service- und Notrufstelle (SOC) über ID-Contact- oder CESA 200-Standards basierenden und bei ESI und Azur Soft qualifizierten „**TIP**“-Protokoll von TIL.

Die Übertragungshauptfunktionen bieten eine große Reichweite und funktionale Anpassungsfähigkeit:

JEDE ZENTRALE BEINHALTET:

- 4 Empfänger und potenzielle Benutzer für den Empfang von Alarmen (zentrale Überwachungsstation), die Bedienungen an der Steuereinheit durchführen dürfen
- 8 Anrufprofile für die Alarmübertragung zur Festlegung der Empfänger und der Kontaktreihenfolge
- 32 Fernsteuerungsbefehle für Benutzerinterventionen

POLLING: Mit dieser Funktion kann der Empfänger die Zentrale regelmäßig abfragen und feststellen, ob diese im Netzwerk noch auffindbar ist

ZYKLISCHER TEST: die Zentrale führt zur Funktionsprüfung der Kommunikationsleitung eine periodische Übertragung an einen Empfänger durch. Die Häufigkeit ist konfigurierbar (genaue Zeit, in Verbindung mit dem Einschalten einer oder mehrerer Gruppen, pro Empfänger unterschiedlich)

KODIERUNGSTABELLE: Eine Kodierungstabelle ist eine Tabelle, in der ein Ereigniscode für jeden Alarmtyp definiert wird (Einbruch, Zutritt, Brand...), der an die Fernüberwachungsstation gesendet wird. Diese Codes müssen daher mithilfe der ausgewählten Fernüberwachungsstation festgelegt werden

EINBRUCHÜBERWACHUNG VON DRITTPRODUKTEN:

Dank Gateways mit Einbruch-Überwachungsprodukten von Drittanbietern (GALAXY NFA2P IP-Steuereinheit, SORHEA Perimeterschutz mit MAXIBUS-Protokoll...) ermöglicht MICROSESAME auch die Überwachung von Einbruchalarmen mit solchen Drittsystemen. Weitere Informationen und Beispiele in den entsprechenden Kapiteln: GATEWAYS UND KONNEKTOREN, MONITORING UND ÜBERWACHUNG, VIDEOÜBERWACHUNG

GEGENSPRECHANLAGEN

BETRIEB VON GEGENSPRECHANLAGEN MIT MICROSESAME

Durch die Integration einer Gegensprechanlage in die **MICROSESAME**-Sicherheitsarchitektur werden Kommunikations- und andere Gebäudesicherheitsfunktionen (Zutrittskontrolle, Video, Einbruch, Gebäudemanagement...) über eine und dieselbe Grafikschnittstelle verwaltet.

Ereignisaktionen können somit vollständig automatisiert werden. Für den Benutzer wird die Bedienung deutlich vereinfacht und eine hohe Verarbeitungsgeschwindigkeit erreicht.

Zahlreiche Beispiele:

- Der Intercom-Anruf kann Video-Befehle zur effektiveren visuellen Kontrolle beziehungsweise die Beleuchtung oder andere Automatisierungen gleichzeitig ansteuern.
- Nach dem Anruf kann durch eine Türöffnung ebenfalls die Einbruchüberwachung deaktiviert werden.
- Umgekehrt kann das Vorhalten eines verbotenen Ausweises an einer Leseeinheit die Übertragung einer vorab aufgezeichneten Nachricht über die Gegensprechanlage veranlassen.

Schließlich liegt ein weiterer Vorteil dieser Integration darin, dass der Betrieb der Gegensprechanlage von allen **MICROSSEAME-**"Info-Funktionen" profitiert: gemeinsamer Verlauf, erweiterte Suche, Ausgabe von Berichten zur Analyse und Nutzungsstatistiken...

INTERAKTIONEN MIT COMMEND-LÖSUNGEN

MICROSESAME kommuniziert mit den **COMMEND-IP**-Gegensprechanlagezentralen (GE800, GE300, IS300, VIRTUOSIS), die in Deutschland bei Schneider Intercom erhältlich sind.
Die gängigsten Kommunikationsvorgänge können von jeder **MICROSESAME**-Bedienstation aus ausgeführt werden:

- Vollständige Virtualisierung des Master-Arbeitsplatzes (mit direkt an die Bedienstation angeschlossenen Mikrofon und Lautsprechern).
- Anzeige der Anrufe der Gegensprechanlage zum Master-Arbeitsplatz.
- In 2 Stufen differenzierte Behandlung: Normal oder Notruf.
- Anrufannahme, -unterbrechung oder -stornierung
- Aktivieren und Deaktivieren einer Gegensprechanlage
- Visualisierung des Verbindungsstatus zum Intercom-Server mit Grund: Stromversorgungsproblem, Sabotage, Kurzschluss...
- Kommunikationsverbindung zweier Arbeitsplätze (Direkttaste in grafischer Überwachung oder Tastatur des virtuellen Master-Arbeitsplatzes).
- Anrufweiterleitung vom Master-Arbeitsplatz zu einem anderen im Tag-/Nachtbetrieb.
- Fernlauschen.
- Übertragung voraufgezeichneter Audionachrichten über COMMEND-Gegensprechanlagen.
- Steuerung der COMMEND-Gegensprechanlagen- oder virtuellen Relais (Beleuchtung...)
- Öffnen einer an einem mit TIL-Erweiterungsmodul verkabelten Tür durch Drücken einer Taste an einer COMMEND-Gegensprechanlage

VEREINFACHTE INTEGRATION UND KONFIGURATION

Native Integration mit spezifischen „Objekten und Eigenschaften“

Die Integration von COMMEND-Intercom-Servern wurde zur Reduzierung der Konfigurationsdauer mit den Objektbegriffen „Server“- und „Abonnent“ konzipiert.

Es müssen lediglich der Intercom-Server angegeben und dann die bereits von den COMMEND-Tools erstellte Teilnehmerliste importiert werden. Die Überwachungselemente werden dann für Server und Abonnenten automatisch in **MICROSESAME** erstellt. **MICROSESAME** kann sich mit mehreren COMMEND-Servern zeitgleich verbinden.

Einige spezifische Funktionen sind nativ nicht integriert, jedoch mit einer zusätzlichen Konfiguration entweder seitens **MICROSESAME** oder seitens COMMEND-Server durchaus möglich, zum Beispiel der Befehl, eine Broadcast-Evakuierungsnachricht an alle Gegensprechanlagen (anstatt einzelne) zu senden.

Grafische Überwachung

Zur grafischen Überwachung enthalten die Objekte vorkonfigurierte Icons (Bilder) zur direkten Integration in die **MICROSESAME**-Übersichtsbildschirme.

Diese Icons beinhalten nicht alle Objekteigenschaften, können aber je nach **MICROSESAME**-Version ergänzt werden. Selbstverständlich können auch eigene Intercom-Icons angepasst und die gewünschten Eigenschaften in die Übersichtsbildschirme integriert werden.

NOTFALLMANAGEMENT

UNTERSTÜTZUNG BEI EVAKUIERUNGEN UND NOTEINSÄTZE

Als NOMAN werden die organisatorischen Maßnahmen die Einsatzmethoden und die notwendigen Mittel definiert, die der Benutzer zum Schutze seines Personals, der Populationen und der Umwelt ergreifen muss. Er ist hauptsächlich für Anlagen mit den größten Risiken erforderlich, insbesondere für Anlagen, für die ein besonderer Interventionsplan gilt.

INTEGRATION IN MICROSESAME

Die in MICROSESAME integrierte NOMAN-Assistenzanwendung greift über Benutzeroberfläche, dedizierte Fenster mit folgenden Funktionen in den Personenschutzprozess ein:

- ► Unterteilung von NOMAN-Zonen in zwei Kategorien: gesichert und ungesichert
  - Gesicherte Zonen sind Bereiche, in denen sich Personen von Gefahren fernhalten können
  - Die ungesicherten Zonen sind der Rest des Geländes.
- ► Bereitstellung der Liste und der Anzahl der vor Ort anwesenden Personen in Echtzeit in jeder zone mit Anzeige ihrer Befähigungen gemäß ihren Ausweisprüfungen an Ausweis-Leseeinheiten (sofern verwendet)
- ► Nach Auslösen des NOMAN, bei Übungen oder realen Vorfällen: Echtzeitüberwachung von Personalbewegungen aus den Arbeits- in die gesicherten Zonen
- ► Suche nach einer Person, um ihren Aufenthaltsort zu lokalisieren (gesicherte Zone oder nicht)
- ► Personennamen bearbeiten über eine Mitarbeiterwand für ausgewählte Zonen
- ► PDF-Export der Personenliste in ein bestimmtes Verzeichnis
- ► Bedienung und Anzeige der NOMAN-Zonen mit Übersicht oder über allgemeinem Menü

Zur erleichterten Zählung an Sammelplätzen (gesicherte Zonen) kann das für den Außenbetrieb geeignete tragbare **MOBILIS**-Ausweis-Lesegerät verwendet werden. Diese Lesegeräte sind nicht verkabelt. Die Ausweise können von den Evakuierungsverantwortlichen mit Hillfe dieser Geräte mobil geprüft werden.

RUHEZEITENKONTROLLE

EINHALTUNG DES ARBEITSZEITGESETZES

§3 des deutschen Arbeitszeitgesetzes (ArbZG) sieht vor, dass die werktägliche Arbeitszeit von Arbeitnehmern von 8 auf bis zu 10 Stunden nur dann überschreiten darf, wenn innerhalb von 6 Kalendermonaten oder 24 Wochen im Durchschnitt 8 Stunden nicht überschritten wurden. Ruhepausen von 30 Minuten ab 6 und von 45 Minuten ab 9 Stunden Arbeitszeit sind einzuhalten.

Mit der **MICROSESAME**-Funktion „**Ruhezeitenkontrolle**“ kann in einfacher Weise die Einhaltung des ArbZG unter Anwendung der Gebäudezutrittskontrolle gewährleistet werden.

Durch die automatische Analyse der Durchgänge von Mitarbeiterausweisen wird geprüft, ob diese oder andere gesetzlich vorgeschriebene Ruhezeiten eingehalten wurden. Es bieten sich folgende Optionen an:

AUTOMATISCHE ZUTRITTSSPERRUNG vorübergehend und für Mitarbeiter mit nicht eingehaltenen Zeitlimits zwischen Verlassen und Betreten des Standorts, bis der Zeitplan eingehalten wird.

ZUTRITTSVERBOTSMELDUNG temporärer Art mit Datum und Uhrzeit der nächsten Zutrittsberechtigung an Systembenutzer in der Benutzerkartei mit oder ohne verbundene Sperrung nach Wahl.

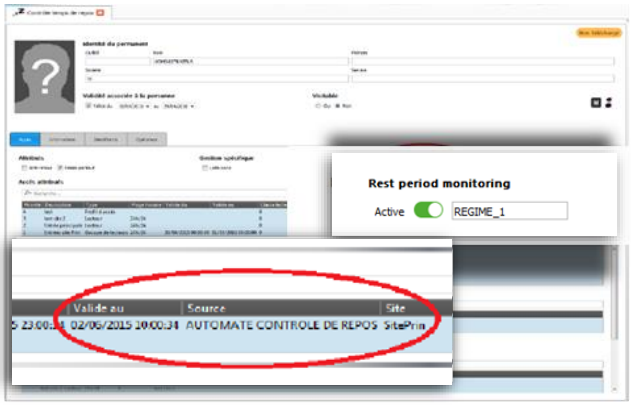
TEMPORÄRE SPERRUNG, die von einem autorisierten Benutzer manuell aufgehoben werden kann.

BERICHTSERSTELLUNG zum Anzeigen der Ruhezeitenabweichungen.

AUSSERGEWÖHNLICHE EREIGNISSE: Hierbei kann auch die Ruhezeitenkontrolle für alle Mitarbeiter „ausgeschaltet“ werden.

Zur schnellen Abfertigung großer Populationsgruppen basiert die Ruhezeitenkontrollfunktion auf der Idee der „Ruhezeitregelung“. Jede „Ruhezeitregelung“ erfordert die Meldung von Ein-/Ausgangs-Leseeinheiten, die Festlegung von Ruhezeiten und -tagen sowie die Festlegung von Anfangszeiten der wöchentlichen und täglichen Berechnungen. Es können mehrere „Ruhezeitregelungen“ erfasst werden, sodass die Ruhezeit jedes Benutzers gemäß individueller Regelung und Leseeinheiten kontrolliert wird. Diese Zuweisung kann direkt in **MICROSESAME** oder über ein Gateway mit dem HR-Datensatz des Unternehmens erreicht werden.

Ist diese Option für einen Mitarbeiter aktiviert, werden abgelehnte Lesedurchgänge im Ereignismonitor und im Verlauf von **MICROSESAME** als „außerhalb des Zeitfensters“ eingeordnet.



Durch das Öffnen der Benutzerkartei können die temporäre Zutrittssperre eingesehen und Datum und Uhrzeit der nächsten Zutrittsberechtigung in Erfahrung gebracht werden. Bei Bedarf kann diese temporäre Sperrung von einem autorisierten Benutzer manuell aufgehoben werden.

Um schließlich eine umfassendere Nachverfolgung der Mitarbeiter durch die Personal- und Sicherheitsabteilungen durchzuführen, kann mit dem universellen Requester von **MICROSESAME** das Starten wöchentlicher Analysen zum Generieren einer Datei, die alle als „außerhalb des Zeitfensters“ abgelehnten Zugänge enthält (siehe Abschnitt Verläufe, Berichte und Requester) gesteuert werden.

STRECKENMANAGEMENT

UNTERSTÜTZUNG BEI KONTROLLGÄNGEN

Mit der Softwareoption (**MS-PCR**) von **MICROSESAME** werden Kontrollgänge erstellt und die Nachverfolgung von Kontrollgängern (Bevollmächtigten), die ihre Rundgänge in Echtzeit vor Ort durchführen sollen, ermöglicht.

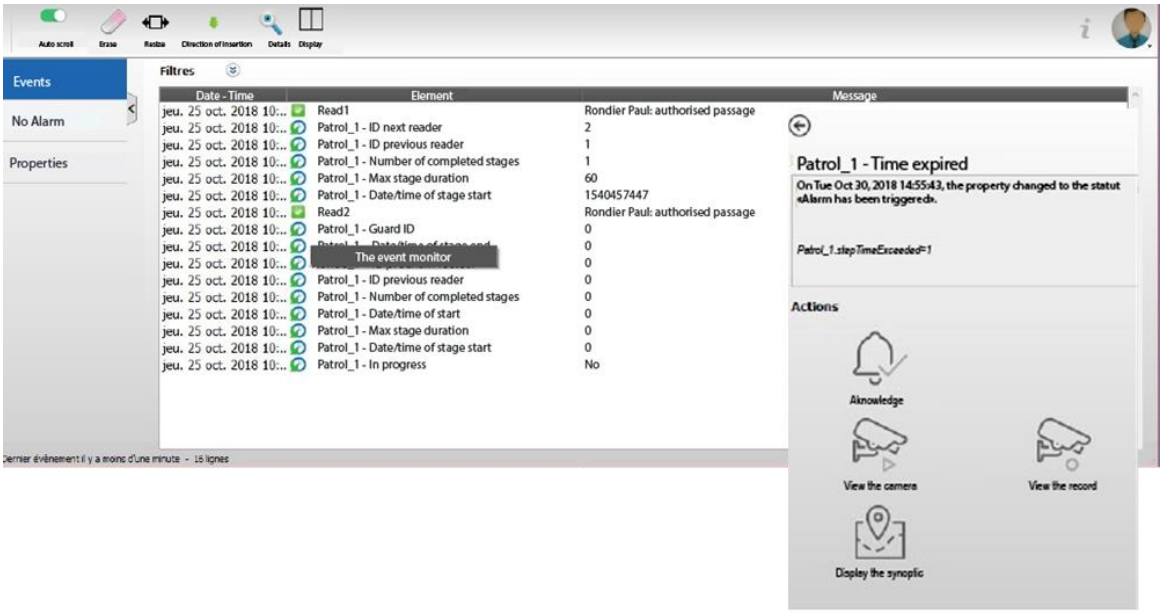
Ein Kontrollgang ist eine vordefinierte Strecke an Leseeinheiten vorbei, bei der die durchführenden Kontrollgänger nacheinander ihre Ausweise vorhalten müssen. Mit dieser Option wird das Fortschreiten mehrerer Kontrollgänger auf bis zu 64 verschiedenen Strecken überwacht. (ein Sicherheitsagent/Kontrollgänger pro Kontrollgang).

FÜR DAS STRECKENMANAGEMENT können die am Standort bereits vorhandenen Leseeinheiten genutzt werden, ohne dass Leseeinheiten oder Ausrüstung speziell zur Durchführung von Kontrollgängen zusätzlich benötigt werden.

DER KONTROLLGANG kann ohne Zutrittsberechtigungen auf die betroffenen Leseeinheiten ausgeführt werden. Der Kontrollgänger kann sein ID-Mittel (Ausweis) verwenden, um den Kontrollgang durchzuführen.

SPEZIFISCHE BENUTZERRECHTE für die Verwaltung der Kontrollgänge (Zugriff auf die Anwendung und Verwaltung der Kontrollgänge, ohne erforderliche Zutrittsberechtigungen) bestehen zum Beispiel für Benutzer mit eingeschränktem Profil

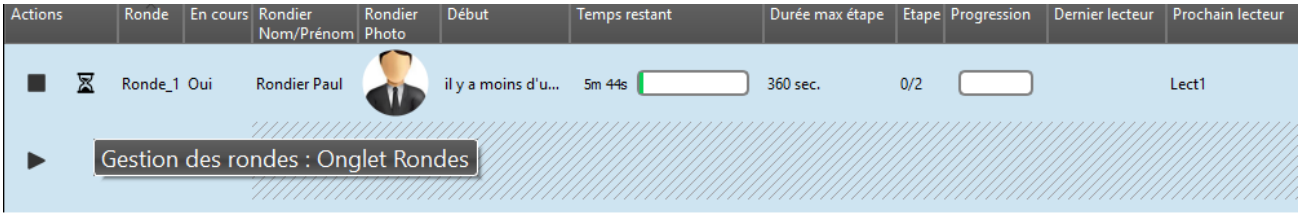
Zum Starten eines Kontrollganges werden jeweils ein Kontrollgang aus der Liste und der Kontrollgänger ausgewählt, der den Kontrollgang auf dem Gelände durchführt. Die definierte Zeit zwischen den einzelnen Leseeinheiten ist einzuhalten. Bei Überschreitung des Zeitlimits zwischen 2 Leseeinheiten wird automatisch ein Ereignis oder ein Alarm auf dem Ereignismonitor unter Angabe des Kontrollgängers und der betroffenen Strecken ausgelöst. Im Alarmfall werden die möglichen Handlungsoptionen: Qualifizieren, Übersicht anzeigen, verknüpfte Kamera in **VISIOSESAME** anzeigen.



Eine spezielle Tabelle zeigt die verschiedenen Informationen und den Status der Kontrollgänge in Echtzeit an:

- In Gange, den Kontrollgang durchführenden Kontrollgänger,
- Die seit Beginn des Kontrollgangs verstrichene Zeit,
- Die verbliebene Zeit für den Kontrollgänger zum Vorhalten seines Ausweises an der nächsten Leseeinheit mit Fortschrittsfärbung (grün, gelb, orange, rot)
- Die Gesamtzeit pro Etappe
- Die Gesamtzahl aller Etappen
- Die aktuelle Etappe
- Die letzte Leseeinheit, bei dem der Ausweis des Kontrollgängers erkannt wurde
- Der Kontrollpunkt, an dem der Ausweis des Kontrollgängers vorgehalten werden muss

Der Systemanwender kann der Leseeinheit auch eine zusätzliche Zeit für den Durchgang gewähren oder den Kontrollgang abbrechen (jederzeit möglich).



VERLÄUFE, SUCHEN, BERICHTE UND PROTOKOLLIERUNGEN

Diese Funktionen sind in der **MICROSESAME**-Lösung nativ integriert

VERLAUF

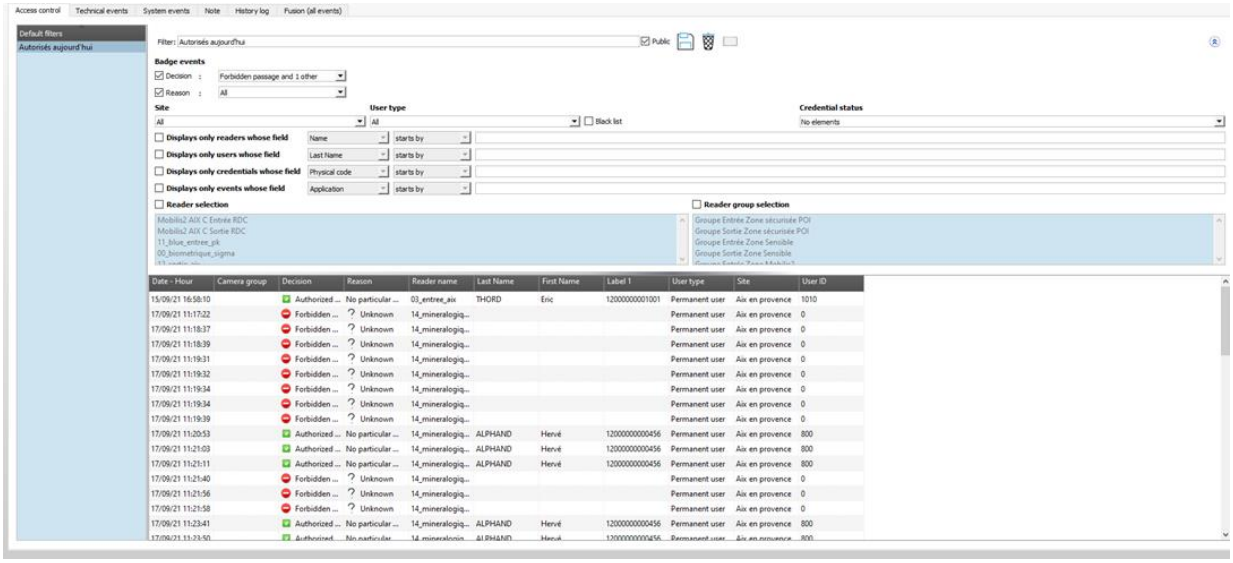
Die Funktionalität „**Verlauf**“, von einer Heavy-Client-Arbeitsplatz aus ermöglicht die Abfrage aller in der Datenbank eingetragenen Ereignisse. Sie verfolgt sowohl das Gebäudemanagement (Ausweisdurchgänge, technische Alarme...) als auch den Systembetrieb und die Benutzereingriffe.

Die Speicherkapazität ist unbegrenzt. Standardmäßig ist die Aufbewahrungsfrist für Ereignisse auf 30 Tage voreingestellt, dieser Wert kann jedoch konfiguriert werden, z. Bsp. auf 90 Tage.

Die Suchkriterien und die Anzeige von Ereignissen, Alarmen, Bewegungen werden durch eine Gesamtansicht mit gemeinsamen Kriterien durch folgende Registerkarten der Ereignisarten entsprechend dargestellt:

- Zutrittskontrolle
- Technische Ereignisse
- Systemereignisse
- Prüfung von Änderungen (Benutzeraktionen)
- Zusammenführung aller Ereignisse

Diese Felder sind für jede Registerkarte unterschiedlich. Standardmäßig wird der Suchzeitraum auf die aktuelle Uhrzeit und auf die letzten 7 Tage gesetzt.



Die Verlaufsfunktion bietet dem Kunden Feineinstellungen, Personalisierung und rasche Handhabung durch:

DATENABHÄNGIGE FILTERFUNKTION (Felder): Sie ermöglicht eine sehr genaue Suche nach Ereignissen. Für eine schnelle und relevante Auswahl an Filtern, können diese je nach Systemkonfiguration in vordefinierten Dropdown-Listen angezeigt werden. Zum Beispiel die Art des Standorts (beim Management mehrerer Standorte), des Benutzers (Dauer-User oder Besucher), des ID-Mittel-Status (verloren, gestohlen, aktiv...)

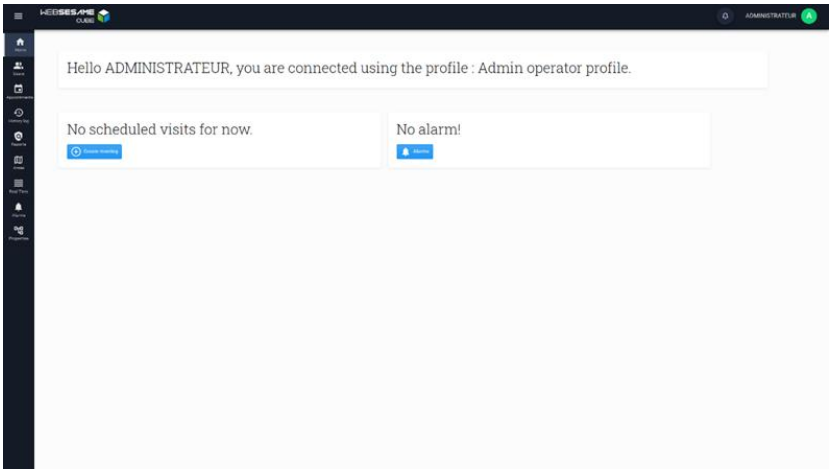
SPEICHERN UND BENENNUNG: Um wiederkehrende Anforderungen zu vereinfachen, kann jeder Benutzer Standardsuchen mit voreingestellten Parametern und Filtern speichern und benennen. Diese verschiedenen Standardsuchen werden im Fenster „vordefinierte Filter“ mit der Wahl zwischen privatem Backup (nur für den Benutzer sichtbar, der es erstellt hat) oder öffentlich (für andere Benutzer verfügbar) gespeichert. Dies vermeidet die erneute Eingabe gleicher Suchkriterien und führt zu einer erheblichen Zeitersparnis.

FILTERN der Visualisierung von Eigenschaften gemäß der „Kategorie“-Berechtigung des Benutzers

HINZUFÜGEN VON DETAILS ZU VERBOTENEN DURCHGÄNGEN: Standort, unbekannte ID-Mittel, verstärkte Kontrolle, kontrollierter Durchgang, kein Zutritt

WEBSESAME

Das **WEBSESAME**-Portal schlägt unter anderem diese 3 Anwendungen vor: Zutrittskontrollverlauf, Verlauf von Variablen (Eigenschaften), Universal Requester



VERLAUF DER WEBSESAME-ZUTRITTSKONTROLLE

Die **MICROSESAME**-Webschnittstelle beinhaltet eine Registerkarte zur einfachen Anzeige des Zutrittskontrollverlaufs und zur Suche nach Ausweisdurchgängen

Zur Erleichterung der Datenabfrage können verschiedene Parameter und Filter, Datum, Art des Ereignisses (erlaubte, verbotene Ausweise...) angewendet werden. Die Felder der anzuzeigenden Ergebnisse sind vollkonfigurierbar (Anrede, Name, ID-Mittel...)

VERLAUF DER WEBSESAME-VARIABLEN/-EIGENSCHAFTEN

Mit der Anwendung Variablenverlauf (Eigenschaften) wird nach technischen Ereignissen im Zusammenhang mit dem Zutrittskontrollsystem gesucht.

UNIVERSELLER WEBSESAME-REQUESTER, BERICHTE

Der über das **WEBSESAME**-Portal zugängliche universelle Requester zur Extraktion aller in den **MICROSESAME**-Datenbanken enthaltenen Informationsarten durch Ausführung eines SQL-Requesters und die Generierung eines Berichts/Ergebnisses ist ebenfalls von großem Nutzen.

Der universelle Web-Requester bietet folgende Möglichkeiten:

ANFRAGEN: Sie sind nativ im Produkt vorhanden (siehe Liste unten), sodass die gängigsten Suchen durchgeführt werden können. Abfragebibliothek in Server\ScriptsSql\SqlServer\Requester\DE verfügbar.

ERGEBNIS, BERICHT: wird direkt in der Benutzeroberfläche angezeigt, nachdem die gewünschte Abfrage ausgeführt wurde. Dieses Ergebnis kann als CSV- oder PDF-Datei exportiert werden. Die CSV-Datei kann dann aus einer Excel-Tabelle oder einem Texteditor genutzt werden, um Grafiken oder Statistiken zu erstellen usw.

AUSFÜHREN EINES BERICHTS: bei Eigenschaftsänderung und per automatischem E-Mail-Versand

BENUTZERDEFINIERTE ANFRAGE-ERSTELLUNG:

- Durch den Errichter oder den Endkunden mit guten Kenntnissen der SQL-Skriptsprache zum einfachen Abfragen anhand bestehender Abfragenbeispiele,
- Von TIL TECHNOLOGIES nach Projekt für komplexere Abfragen nach Kundenwunsch, wobei Datenbankschema und Tabelleninhalt (MCD) nicht dokumentiert werden.

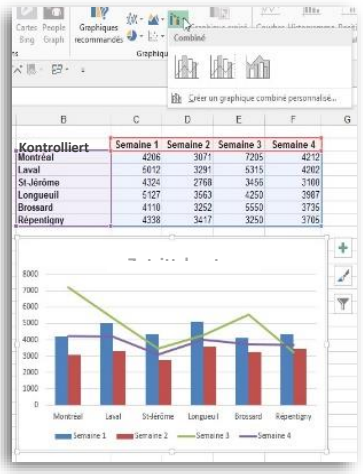
IMPORT, EXPORTABFRAGE im Format „file.json“. Es kann eine Abfrage importiert werden, die zuvor aus einem anderen **MICROSESAME**-System exportiert wurde.

FILTER: Die Abfrage kann Parameter enthalten, mit den das erwartete Ergebnis nach Datum, Uhrzeit, Auswahl in einer Dropdown-Liste (Firma, Abteilung, Leseeinheit, Person...) gefiltert wird. Ist ein Filterfeld nicht ausgefüllt, werden „alle“ gewählt.

„EXTRAKTOR“-Werkzeug: In der Lösung verfügbar. Mit ihm werden automatische und regelmäßige Berichte über gewünschte Anfragen in definierten Verzeichnissen zur Vereinfachung von Aufgaben bei wiederkehrenden Anforderungen durchgeführt.

LISTE DER IN DER BIBLIOTHEK VORHANDENEN ABFRAGEN

- appartenance_lecteur.json
- appartenance_lecteur_site.json
- contenu_groupe_lecteur_appartenance_profil.json
- Echeance_Habilitation_Inferieure_A_Un_Mois.json
- evolution_nombre_visite_par_heure.json
- evolution_nombre_visite_par_jour.json
- Identifies_Devalides_Mois_Prochain.json
- liste_identifies_valides_en_liste_noire.json
- liste_passages_historises_sur_lecteurs_par_date.json
- requete_acces_resultants.json
- requete_identifie_identifiants.json
- requete_repos.json
- variables_sollicitees_sql.json
- Visualiser_les_comportements_suspects.json
- Visualiser_les_deconnexions_modules.json



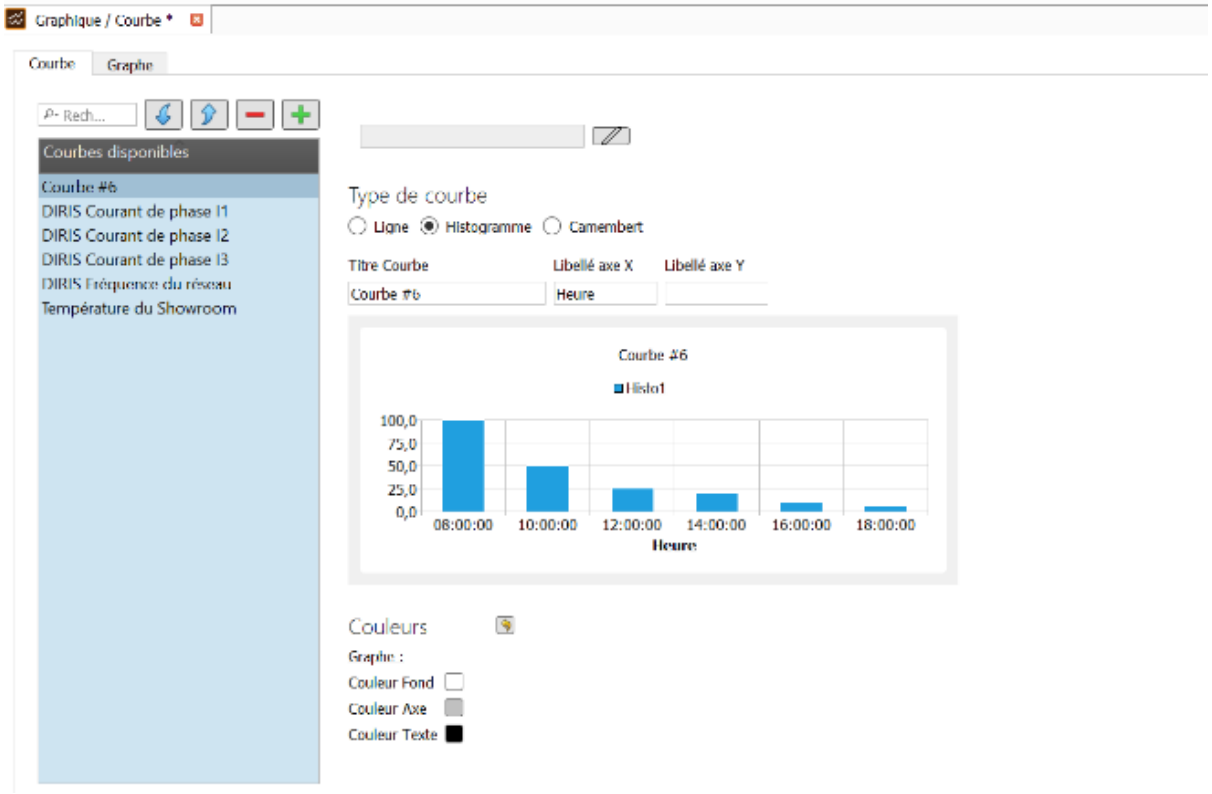
BESCHREIBUNG EINIGER BEISPIELABFRAGEN:

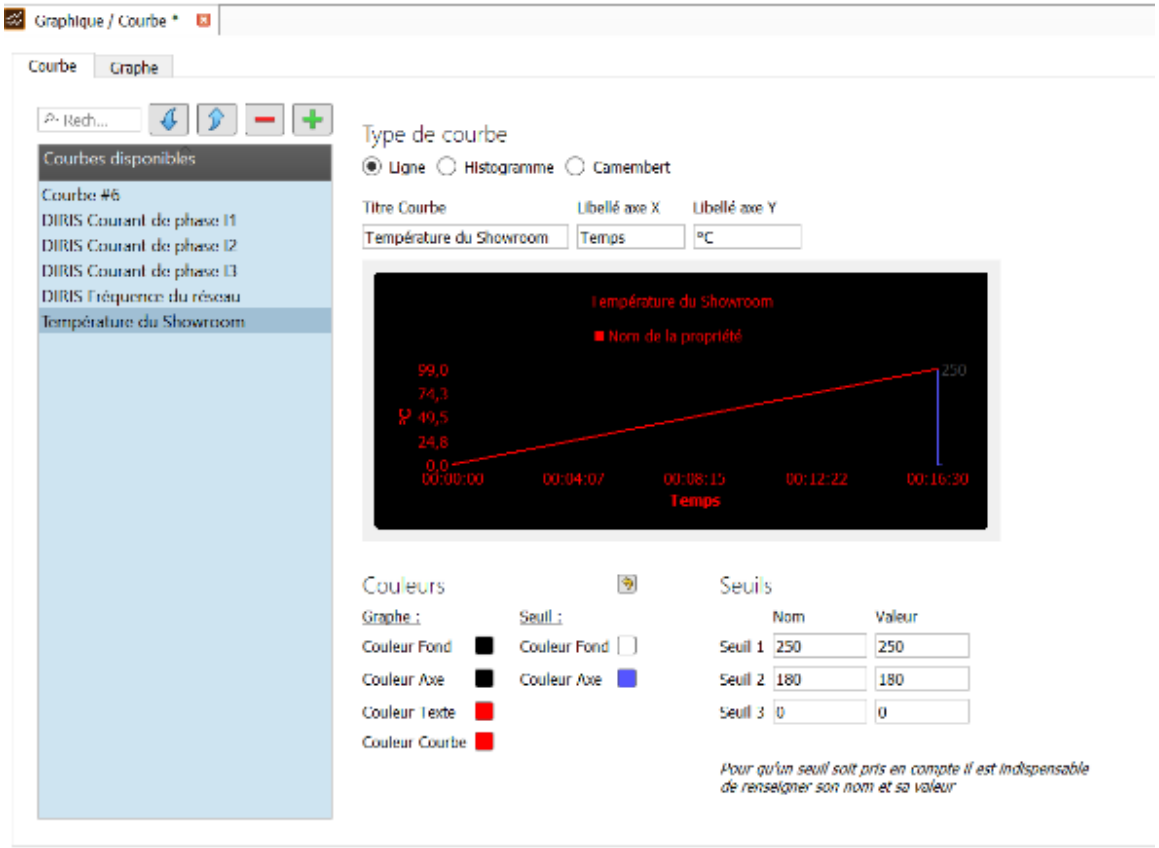
- „Ruhezeitanforderung“: Liste der Benutzer, die ihre Ruhezeiten nicht eingehalten haben
- Abfrage „Benutzer nächsten Monat ungültig machen“: Liste der Personen, die an einem bestimmten Datum für ungültig erklärt werden. In der Benutzeroberfläche dieser Abfrage sind folgende Filter auffindbar: Start-Ende-Datum, Kennziffer, Name, Vorname

GRAFIKEN UND KURVEN IN MICROSESAME

MICROSESAME beinhaltet eine Grafik-/Kurvenanwendung, welche die grafische Darstellung der Entwicklung digitaler Variablen oder Logiken über einen festgelegten Zeitraum hinweg und in Form von Kurven ermöglicht. Diese Anwendung bietet folgende Möglichkeiten:

- Einen bestimmten Suchzeitraum zum Filtern der erhaltenen Daten
- Die erhaltenen Kurven – Daten, die als PDF- oder JSON-Datei an einen ausgewählten Ort exportiert werden können. JSON-Dateien können auch zum Importieren externer Parameter verwendet werden
- Die Grafiken erlauben die Gruppierung mehrerer Kurven unter demselben Graphen.
- Die folgenden Kurvendarstellungseigenschaften können konfiguriert werden:
  - Farben auf Kurve, Hintergrund, Achsen, Texten, Schwellenwerten | Diagrammtitel | Bezeichnung von X und Y | Kurventyp aus den 3 für die Konfiguration verfügbaren Kurventypen:
    - Linie: von den **MICROSESAME** -„Eigenschaften“ verwendet (Begriff von 3 möglichen Schwellenwerten mit Name und Wert jedes Schwellenwertes)
  - Histogramm: aus einer SQL-Abfrage generiert
  - Kuchendiagramm: aus einer SQL-Abfrage generiert


Graphique / Courbe *
Courbe
Graphe
Courbes disponibles
Courbe #6
DIRIS Courant de phase I1
DIRIS Courant de phase I2
DIRIS Courant de phase I3
DIRIS Fréquence du réseau
Température du Showroom
Type de courbe
Ligne
Histogramme
Camembert
Titre Courbe
Libellé axe X
Libellé axe Y
Courbe #6
Heure
Courbe #6
Histo1
100,0
75,0
50,0
25,0
0,0
08:00:00
10:00:00
12:00:00
14:00:00
16:00:00
18:00:00
Heure
Couleurs
Graphe :
Couleur Fond
Couleur Axe
Couleur Texte


Graphique / Courbe *
Courbe
Graphe
Courbes disponibles
Courbe #6
DIRIS Courant de phase I1
DIRIS Courant de phase I2
DIRIS Courant de phase I3
DIRIS Fréquence du réseau
Température du Showroom
Type de courbe
Ligne
Histogramme
Camembert
Titre Courbe
Libellé axe X
Libellé axe Y
Température du Showroom
Temps
°C
Température du Showroom
Nom de la propriété
99,0
74,3
49,5
24,8
0,0
250
00:00:00
00:04:07
00:08:15
00:12:22
00:16:30
Temps
Couleurs
Graphe :
Couleur Fond
Couleur Axe
Couleur Texte
Couleur Courbe
Seuil :
Couleur Fond
Couleur Axe
Seuils
Nom
Valeur
Seuil 1
250
250
Seuil 2
180
180
Seuil 3
0
0
Pour qu'un seuil soit pris en compte il est indispensable de renseigner son nom et sa valeur

GATEWAYS UND KONNEKTOREN

MICROSESAME-CUBE ist ein Sicherheits-Hypervisor, der eine beeindruckende Anzahl an Softwares, Hardwares, Systemen, Verzeichnissen usw. vereinheitlicht und damit Schnittstellen bildet. Er bietet eine globale zentralisierte Lösung mit der größtmöglichen Öffnung und einer hohen Anpassungsfähigkeit an zukünftige Bedürfnisse.

MICROSESAME-CUBE ermöglicht also die Verwaltung eines skalierbaren Ökosystems aus Funktionen und Tätigkeiten sowie die Überwachung von Alarmen oder Fehlern dieser Systeme mit der Funktionalität der in entsprechenden Kapiteln beschriebenen Lösung: MONITORING UND ÜBERWACHUNG, VIDEOÜBERWACHUNG, EINBRUCH

MÖGLICHE KONNEKTOREN DES **MICROSESAME**-SYSTEMS:

- Benutzer- und Besucherdatenbank: Webdienste REST-API, TXT/CSV-Dateien
- A.D.-Benutzerverwaltung: LDAP, Windows-Authentifizierung (SSO NTLM)
- IT-Supervisor: SNMPv3 (von Zentrale TILLYS CUBE)
- Hypervisor / Technisches Gebäudemanagement: OPC UA, MODBUS-IP, Bacnet
- Zentrale, Drittsystem (Brandschutz...) : MODBUS IP
- VMS-Videosystem: VMS SDK, TEXT/ASCII-Gateway
- Spezifische Projekt- und/oder Produkt-Gateways (Webdienste, REST-API, diverse SDKs usw.)

EINIGE BEISPIELE REALISIERTER SCHNITTSTELLEN FÜR **MICROSESAME**:

- Hypervisor-Aufbau, Technisches Gebäudemanagement: PRYSM, PC VUE, PANORAMA….
- Zimmer- und Ressourcenreservierung: ASW, Planitec usw.
- LKW-Flussmanagement: EASYPROG, STACKR
- Video: MILESTONE, GEUTEBRUCK, VIDEOWAVE, GENETEC (siehe Kapitel VIDEOÜBERWACHUNG)
- Integration des MILESTONE ACCESS CONTROL-Plug-ins zur Überwachung der TIL-Zutrittskontrolle in die X-PROTECT-Überwachungsschnittstelle von MILESTONE (siehe entsprechendes Kapitel VIDEOÜBERWACHUNG)
- Gegensprechanlage: COMMEND über Teilnehmer-IP/Import, Anrufe, Anrufbenachrichtigung (mit Unterscheidung zwischen normal und dringend), Nachtrufweiterleitung, Verbindungsoption zum Intercom-Server (siehe entsprechendes Kapitel GEGENSPRECHANLAGE)
- DEISTER-Schlüsselschrank: Synchronisation der Identifikation mit COMMANDER 4-Software
- SORHEA-Perimeterschutz über das MAXIBUS-Protokoll von **SORHEA**
- Brandzentralen über das MODBUS-Protokoll
- AVIGILON-Videomatrizen und -Multiplexer über ASCII-, TXT-Protokoll
- IDEMIA MORPHO-Biometrie (siehe Kapitel BIOMETRIE)
- SCHINDLER-, KONE-Aufzüge...
- MEMOGUARD-Rufbereitschaftsmanagement
- AASTRA-Autocoms
- LWP-Systeme (Alleinarbeiterschutz)
- CANIF von SNCF, BDRS von Société Générale, STITCH von DGAC...
- SMTP-Nachrichtendienst für E-Mails…

GALAXY-Einbruchzentrale

Honeywell
GALAXY

MICROSESAME CUBE verbindet sich über das native IP-Galaxy-Protokoll mit der Einbruchzentrale NFA2P GALAXY. Die Anbindung an Galaxy-Zentralen wird schnell und einfach durchgeführt. Es müssen lediglich die Kommunikationsparameter und die gewünschten Überwachungsobjekte „Bereich“, „Gruppe“ und „Ausgang“ aus den von TIL in der Bibliothek bereitgestellten Modellen definiert werden:

- Statusrückmeldung der Punkte (Ruhe/Störung/Alarm/Kurzschluss/Maskiert/Ausgeschlossen)
- Gruppenstatusmeldungen (MES/MHS/MESP)
- Alarmmeldungen nach einzelnen Punkten
- Qualifizierung von Alarmen nach Einzelpunkt
- Ausschluss von Punkten aus der MICROSEAME-Überwachung

- Schnittstellen-Fehlerrückmeldungen (RIO) (1)
- Zustandsrückmeldung der Zentrale (1)
- Fernsteuerbefehle **MICROSESAME** → GALAXY
    - Aktivierung und Deaktivierung von Alarmgruppen
    - Aktivierung eines Ausgangs von der MS-Überwachung an Galaxy
    - Sirenenabbruch pro Gruppe

(1) Die Galaxy-Zentrale liefert bestimmte Informationen zu ihrem Status. Bei einer spezifischen Konfiguration mit Hilfe der Frontshell-Software können bestimmte Informationen über die Ausgänge des Galaxy-Steuergeräts gemeldet werden. Die verfügbaren Informationen sind in der Galaxy-Dokumentation ausführlich beschrieben. Ist eine gewünschte Information in der Zentrale nicht konfigurierbar, steht diese in **MICROSESAME** auch nicht zur Verfügung.

BIOMETRIE

MICROSESAME kann biometrische Leseeinheiten verschiedener Marken und Modelle verwalten: EVOLUTION CUBE, IDEMIA, STID, HANDKEY.

Für die Marke EVOLUTION CUBE TIL und STID:

- Leseeinheiten der Baureihe EVOLUTION CUBE TIL und ARCHITECT
- TIL hat biometrische Leseeinheiten im transparenten Modus mit dem ANSSI-konformen Protokoll (SCCPv1) und dem ANSSI-zertifizierten Protokoll (SCCPv2) integriert.
- Biometrische Lösung mit Ausweis + Bio (1:1) gemäß CNIL AU52-Empfehlung: Die Fingerabdrücke befinden sich auf dem Ausweis jeder Person und nicht in einer zentralen Datenbank. In diesem Fall werden die Fingerabdrücke in die STiD SECARD BIO-Software aufgenommen, die sie auf den Ausweis schreibt

Für die Marke IDEMIA (ex MORPHO):

- Leseeinheiten der Baureihen SIGMA (Fingerabdruck), MORPHOWAVE COMPACT (kontaktloses Lesen der Fingerabdrücke...)
- Die biometrische Registrierung erfolgt über die MORPHOMANAGER-Software von IDEMIA.
- TIL hat die MORPHO-BRIDGE-Gateway von MORPHOMANAGER integriert, um die in **MICROSESAME** erstellten Personenkarteien und ID-Mittel an MORPHOMANAGER zu übermitteln und eine doppelte Eingabe zu vermeiden
- Biometrische Lösung mit:
    - Ausweis + Bio (1:1): Die Fingerabdrücke befinden sich auf dem Ausweis jeder Person und nicht in einer zentralen Datenbank. In diesem Fall werden die Fingerabdrücke in die MORPHOMANAGER-Software aufgenommen, die sie auf den Ausweis schreibt

- Nur Bio (1:N) unter Einhaltung weiterer Einschränkungen, da die Fingerabdrücke in einer zu schützenden Datenbank zentralisiert werden (siehe DSGVO). In diesem Fall werden die Fingerabdrücke in die MORPHOMANAGER-Software aufgenommen, die sie direkt an die BIO-Leseeinheitensendet.

STANDARD-IT-PROTOKOLLE

Industrielle SPS oder BMS können im **MODBUS IP**-Protokoll (Master oder Slave) über Schnittstelle verankert werden.

MICROSESAME verfügt zudem über **sichere OPC UA**- (nur Server) sowie **OPC DA2**-Protokolle (Client oder Server). Diese Protokolle sind in der Welt der Automatisierung weit verbreitet und ermöglichen die Verbindung mit BMS.

Somit ist eine Schnittstelle verfügbar für:

PSIMs VON

- Codra-Panorama
- Wonderware
- Prysm-Appvision
- PCVUE

MIT MODBUS IP ODER OPC KOMPATIBLEN ZENTRALEN, BSZ VON

- Schneider
- DIRIS usw.

REST-API UND WEBDIENSTE

TIL stellt seinen Kunden und Technologiepartnern eine API, die Abkürzung für „Application Programming Interface“, zur Verfügung.

Mit dieser API können auf einfacher Weise Gateways zwischen **MICROSESAME** und anderen Anwendungen durch den Austausch von Daten in der TIL-Supervisor-Datenbank entwickelt werden:

Die API definiert genau die Methoden, mit denen Software-Entwickler für eigene Anwendungen Programme schreiben, die mit MICROSESAME (Aufruf von Funktionen oder Daten) interagieren können.

Der Dialog zwischen MICROSESAME und Drittanwendungen erfolgt über Webdiensten im Netzwerk. Das heißt, die API verwendet https, das am häufigsten verwendete Kommunikationsprotokoll.

Achtung: Der Zugriff auf die MICROSESAME-API unterliegt der Unterzeichnung einer Geheimhaltungsvereinbarung (NDA).

BEISPIELE FÜR AUSTAUSCH DER REST-API MIT ANDEREN BRANCHENSOFTWARE

Die bereits realisierten Schnittstellen betreffen sowohl bestehende und am Markt erhältliche Software als auch kundenspezifisch entwickelte Anwendungen:

- Spezifische Besucherverwaltungssoftware (QR-Code usw.) oder an Terminschnittstelle (Benutzer und ID-Mittel) angepasste Intranets
- ASW-Raumbuchungssoftware für Besprechungsräume (Benutzer)
- Zimmerreservierungsanwendung (Benutzer und ID-Mittel)
- Anwendung zur Berechnung der Anwesenheitszeit (Benutzer und Verlauf von Ausweisdurchgängen)
- Konferenzempfangsanwendung (Benutzer und Verlauf von Durchgängen am mobilen Leseeinheit)
- Kantinenabrechnungssoftware (Benutzer und Verlauf der Ausweisdurchgänge)
- eGestrack-Vorgangstrackingsoftware (von STACKr) für Logistikplattformen (Benutzer, ID-Mittel und Verlauf von Ausweisdurchgängen)
- Managementanwendung für Schienen-/Straßen-Umladeplattform (Benutzer und Verlauf der Durchgänge von Kfz-Kennzeichen)
- Schnittstelle zwischen MICROSESAME und KONE-Aufzügen (Benutzer und ID-Mittel)
- Schnittstelle zwischen MICROSESAME und TEB-Videosoftware

GATEWAYS MIT VERWALTUNGS-, HR-ANWENDUNGEN, VERZEICHNISSEN…

In vielen Fällen kann einen Datenaustausch zwischen **MICROSESAME** und Datenbanken zur Verwaltung von Unternehmensmitarbeitern oder -benutzern sinnvoll sein (HR-Datenbanken, Verzeichnisse...)

Die Automatisierung der Synchronisation dieser Datenbanken mit dem Zutrittskontrollsystem ist umso nützlicher, je höher die Anzahl der im Umlauf befindlichen Ausweise ist, denn sie ermöglicht es:

- Doppelte Eingaben zu vermeiden (hohe Zeitersparnis und Präzision)
- Personen Zutrittspunkte nach projektspezifischen Regeln (Aliasen) automatisch zuzuweisen (entsprechend ihrer Abteilung, ihrer Funktion...)
- Die sofortige und automatische Berücksichtigung von Personalzugängen oder -abgängen festzustellen, was für eine optimale Sicherheit sorgt.

Die automatische Datenaktualisierung kann mit den von TIL angebotenen Gateways, WEBDIENSTE REST-API oder MS-SYNCH (CSV) so konfiguriert werden, dass sie zu einem festen Zeitpunkt oder bei jeder Änderung der Quelldatei greift. Selbstverständlich ist bei Bedarf eine manuelle Synchronisation weiterhin möglich.

MICROSESAME unterstützt die Synchronisation mit mehreren Quellen, jede Quelle kann über eine eigene Konfiguration der Synchronisation verfügen.

MICROSESAME kann auch mit WEBDIENST- oder MS_RSYNC(CSV)-Gateways als Datenlieferant dienen, um Personaldaten an Drittsysteme (Wiederherstellung, Druckdienst, Schlüsselschrankmanagement...) zu liefern, die durch die Zutrittskontrolle und Kodierung des Multi-Anwendungs-Ausweises entstehen. **MICROSESAME** kann für jede der Drittanwendungen unterschiedliche Systeme mit personalisierten Daten liefern.

Dadurch können die Datenbanken von Drittsystemen automatisch aktualisiert werden. So wird verhindert, dass sich Benutzer auf jedem System registrieren und Ausweise registrieren müssen (keine Doppeleinträge mehr).

BENACHRICHTIGUNGEN

MICROSESAME enthält eine Funktion zum Versenden von E-Mails per SMTP-Nachrichtendienst im Alarmmodus. Ein im System aufgezeichneter Alarm (Einbruch, Zutrittskontrolle, technischer Alarm) kann per E-Mail versendet werden.

Nach der Ausführung eines Berichts mit dem Universal Requester kann auch automatisch dessen Versand per E-Mail an definierte Empfänger ausgelöst werden.

Der SMS-Versand ist in **MICROSESAME** nicht direkt enthalten und erfordert das Mitwirken eines Drittsystems.

MICROSESAME-ZWISCHENSYSTEME

Eine Gateway (ISMS) für den Datenaustausch zwischen mehreren unabhängigen **MICROSESAME**-Systemen (im UDP-Protokoll) per IP-Netzwerk ist erhältlich. Der Datenaustausch basiert auf der Bezeichnung der Eigenschaften.

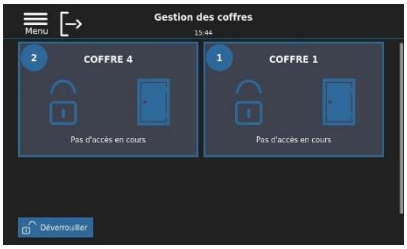
Anwendungsbeispiel: Ein Kunde hat mehrere Standorte mit einem Server und einem gesicherten Arbeits-PC (PCS) pro Standort. Der Kunde verfügt über ein standortübergreifendes IP-Netzwerk. Ein Standort könnte die Rolle der Zentralisierung von Sammelalarmen an Wochenenden übernehmen und einen Client-Arbeitsplatz hosten, der eine Verbindung zu allen Standorten/Servern (jeweils einzeln) herstellen kann. Wenn also ein dringender Sammelalarm von einem Server X an diesen zentralen Server gesendet wird, empfängt der zentrale Benutzer diesen Alarm an seinem Arbeitsplatz vor Ort. Er wird angewiesen, sich mit dem nicht markierten Client-Arbeitsplatz, der auf den Server X zeigt, zu verbinden und den Alarm mit allen verfügbaren Details zu behandeln.

BANKING

Die Absicherung einer Bankfiliale muss auf Prozesse reagieren und ganz spezifische Zutrittskontrollfunktionen nutzen. Angesichts der Risiken von Raubüberfällen, gewaltsamen Zugriffen oder internen böswilligen Handlungen muss der Zugang zu Sicherheitszonen und das Öffnen von Tresoren durch sichere Authentifizierungsmethoden (Zweifach-, Mehrfach-) und gemäß definierten Szenarien (Zeitüberschreitungen, Aktionssequenzen ...) sichergestellt werden.). Die eingesetzten Methoden müssen daher eine einfache und skalierbare Konfiguration komplexer Automatisierungen ermöglichen.

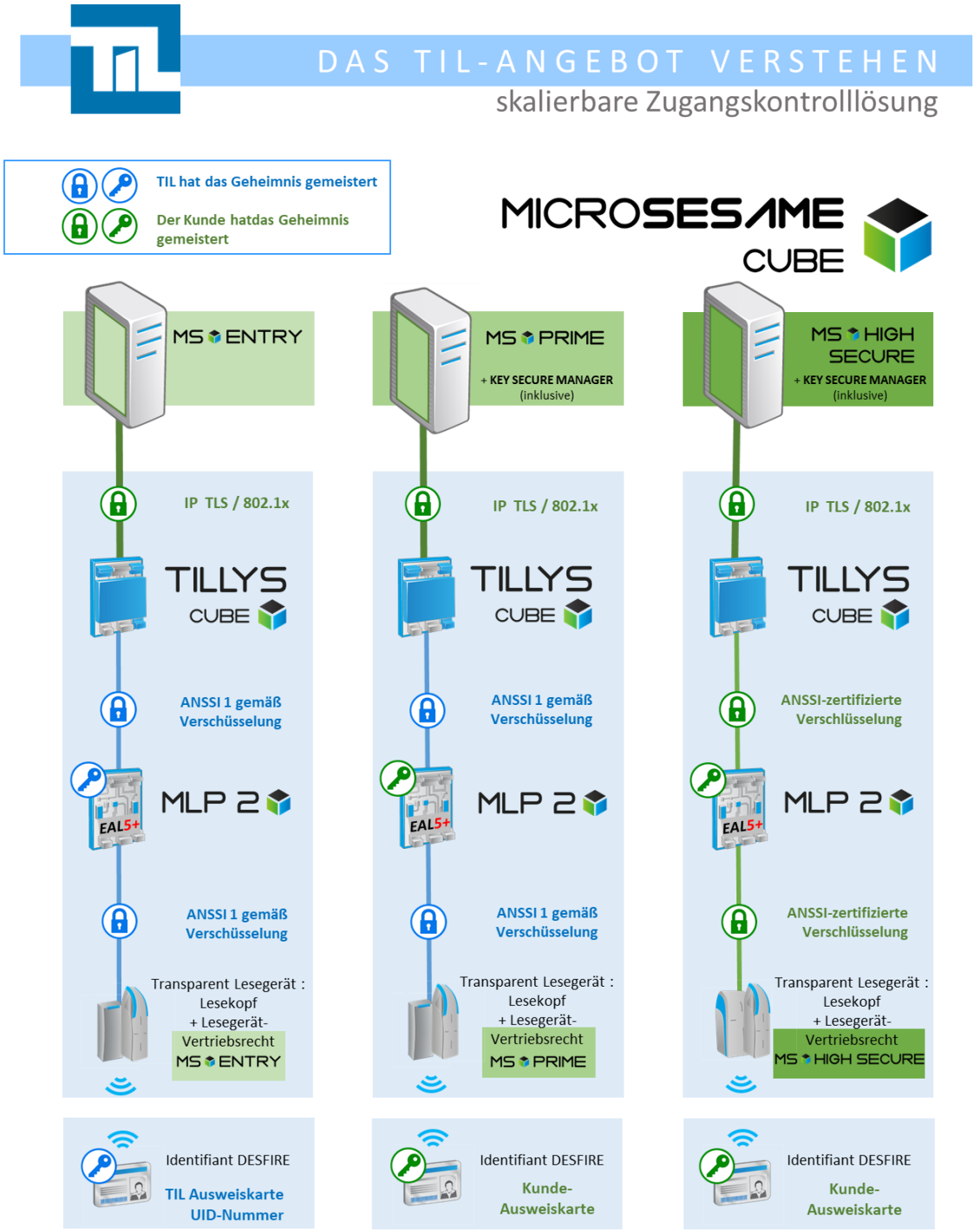
TILLYS-Zentralen, VAULTYS-Steuerungen und die MICROSESAME-Software können alle Anforderungen von Bankfilialen erfüllen.

- Vollständige lokale Konfiguration einer serverlosen Bankfiliale mit Export der Konfiguration, um sie auf den zentralen Server zu importieren und auf X-Filialen zu duplizieren
- Filialausrüstung mit dedizierten und vereinfachten HMIs: LED-Farben der Leseeinheit, je nach Status anpassbar, Ausweisleser mit Timer-Countdown und Farbe je nach Status EIN/AUS ETS-Überwachung,
- Schleuse und eindeutiger Zugriff auf die ETS (Secure Technical Enclosure)
  - Eine einzige offene Tür zwischen jedem Safe und dem ETS-Zugang
  - ETS-Eintritt verboten, wenn sich ein offener Tresor und/oder eine Person bereits im Bereich befinden
  - Mehrere autorisierte Personen, aber jeweils nur ein Sprechertyp (eindeutige Population)
- Sichere Verwaltung und Timings auf dem 7’’ Farb-Touchscreen von VAULTYS:
  - Identifizierung durch Code, Badge oder Badge + Code
  - Es kann immer nur ein Tresor geöffnet werden
  - Anzeige der laufenden Zeitverzögerung
  - Filtern zugänglicher Safes und Anpassen von Timeouts nach Redner, Zeitfenstern oder anderen Bedingungen...
- Anpassbare bedingte oder sequentielle Steuerungen
  - Kombinationen von Aktionen zwischen Zutrittssausweisen, Einbruch aktivieren/deaktivieren, Schaltfläche „Alles in Ordnung“ usw.
  - Unterschiedlich je nach Art des Stakeholders: Förderer, Mitarbeiter, Vorgesetzter usw.



CUBE SOFT- UND HARDWARE-SORTIMENT

CUBE-ANGEBOT: JEDERZEIT SKALIERBARE ZUTRITTSKONTROLLE



MICROSESAME-CUBE-LIZENZMODELL

DAS TIL- ANGEBOT VERSTEHEN

MICROSESAME SOFTWARE

SERVER LIZENZ

Nach Cyber-Sicherheit Stufe, Lesegerät- und Benutzerzahl

MICROSESAME CUBE

Basis Lizenz – Alle Zugangskontrollefunktionen / Einbruch / GLT-System.

MS ENTRY	MS PRIME	MS HIGH SECURE
Anzahl der Lesegerät MS ENTRY	Anzahl der Lesegerät MS PRIME	Anzahl der Lesegerät MS HIGH SECURE

Anzahl der Mechatronik Lesegerät
(Identisches Lizenz für ENTRY, PRIME und HIGH SECURE)

Bedienerhandlungen Anzahl

Web-Benutzer Anzahl

WAHLFREI FUNCTIONNEN

Feste Kosten für die Anlage

- Multi-Standort Verwaltung
- Fernübertragung
- Besuchersverwaltung
- Server-Redundanz

GATEWAYS

Feste Kosten für die Aktivierung

- Import Gateways
- Export Gateways
- Text
- LDAP
- MODBUS
- OPC UA
- OPC DA
- Plugin CA MILESTONE
- MORPHO Biometrie

INTEGRIERTE ANSCHLÜSSE

Variable Kosten nach der Anzahl der Überwachten objekte

Überwachte Objekte mit fortgeschrittener Integration :
Cameras, SORHEA Barrieren, COMMEND Gegensprechanlage, GALAXY Detektors

- MILESTONE XProtect
- GEUTEBRUCK G-scope
- GEUTEBRUCK Geviscope
- BOSCH BVMS
- CASD Visimax
- HIK VISION
- DAHUA
- DIGIFORT
- GENETEC Security Center
- VIDEOWAVE OneTrack
- SORHEA Maxibus
- HONEYWELL Galaxy
- COMMEND

Folgen Sie uns auf

hirschsecure.de

TIL TECHNOLOGIES GmBH

TIL TECHNOLOGIES GmbH
Eisenstraße 2-4
65428 Rüsselsheim

Tél : 06142-481 00 66
Mail : info@hirschsecure.de

TIL TECHNOLOGIES
by HIRSCH