MICROSESAME CUBE

FUNCTIONAL DESCRIPTION

Version 2025.1 – March 2025

TIL TECHNOLOGIES

1. Summary

2. MICROSESAME IN A NUTSHELL

MICROSESAME CUBE

MICROSESAME is an embedded system for **Centralised Security Management** (access control, intrusion, video) and for **Building Technical Management**.
It allows the centralised supervision of all electronic information in the site.

Several functions are managed through a common graphical interface, making their operation easier and interventions more efficient.
As interactions between different systems can be fully automated (actions triggered by specific events), quick processing is also guaranteed.

The system consists of a software and a series of IP controllers connected to any type of hardware.

MS ENTRY

MS PRIME

MS HIGH SECURE

This architecture is based on standards that guarantee its durability, but also its ability to evolve at a lower cost.

By integrating SDK or computer protocols (MODBUS...), **MICROSESAME** can monitor information from external systems (such as fire centrals) and behave as a digital video system hypervisor.
It also communicates directly with APIs and other safety or security equipment through gateways (OPC, text...).

In addition to the functional description of MICROSESAME CUBE, you will find at the end of this document the CUBE software/hardware offer according to 3 levels (ENTRY, PRIME, HIGH-SECURE) based on the “control of secrecy”. This CUBE offer is:

- Simpler & richer: All of TIL's software power is included in the basic licence, from the first reader. Only one machine is available, full capacity & options
- More secure: Native cyber security with full system protection, ANSSI conformity
- More scalable: Security control can evolve by simple software update without changing the hardware in place

3. CERTIFIED ARCHITECTURE & ANSSI QUALIFIED

CYBER SECURE HARDWARE AND SOFTWARE ARCHITECTURE

A **MICROSESAME** architecture consists of the following elements:

- A server, which is both a setup and an operating station. It operates under a standard Windows computing environment. Its implementation is easy and user-friendly.

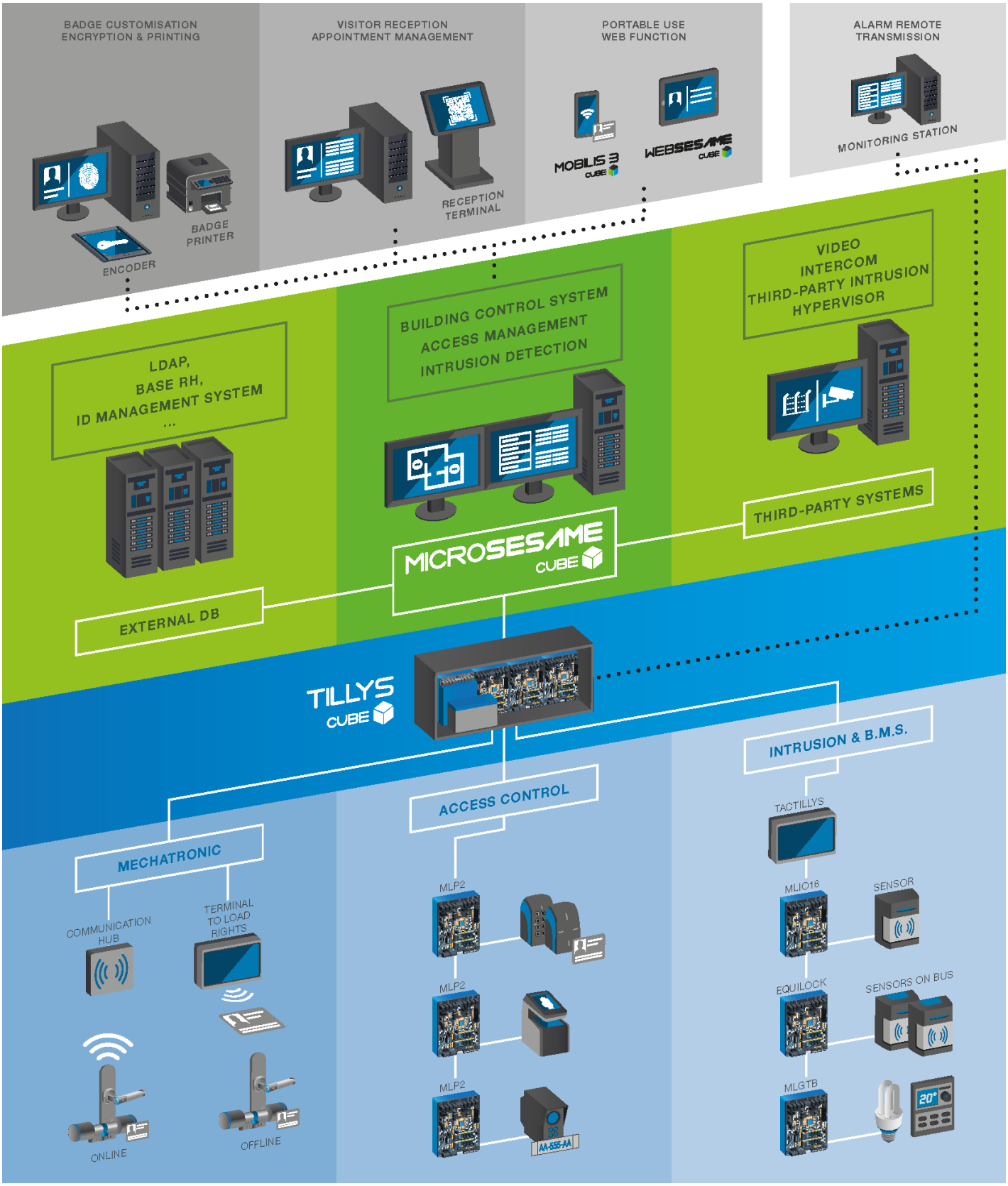
- An Ethernet IP network (wired or Wi-Fi) on which the server is connected to operating stations (**MICROSESAME & VISIOSESAME** heavy clients - light clients via RDP/Citrix - WEB clients via **WEBSESAME** for PC, smartphone or tablets), to TIL centrals (UTL), and mobility tools (MOBILIS terminals).

- The Ethernet network also connects the **MICROSESAME** solution to end-customer systems (Active directory, SNMP supervisor, HR database...) and to third-party applications (VMS server and video recorders, OPC hypervisor, MODBUS controllers...).

- Multifunctional and standalone TIL centrals on IP network for control access, intrusion and BMS.

- Intrusion keyboards, online mechatronic solutions, remote specialised electronic modules (doors modules, entrance/exit modules...), connected to the controller secondary bus for a distributed or centralised architecture.

- Readers, access control keyboard readers, sensors (door contacts, intrusion detectors, etc.), controlled accesses (locks, barriers, tripods, etc.), actuators (sirens, lighting ...) connected to these specialised modules

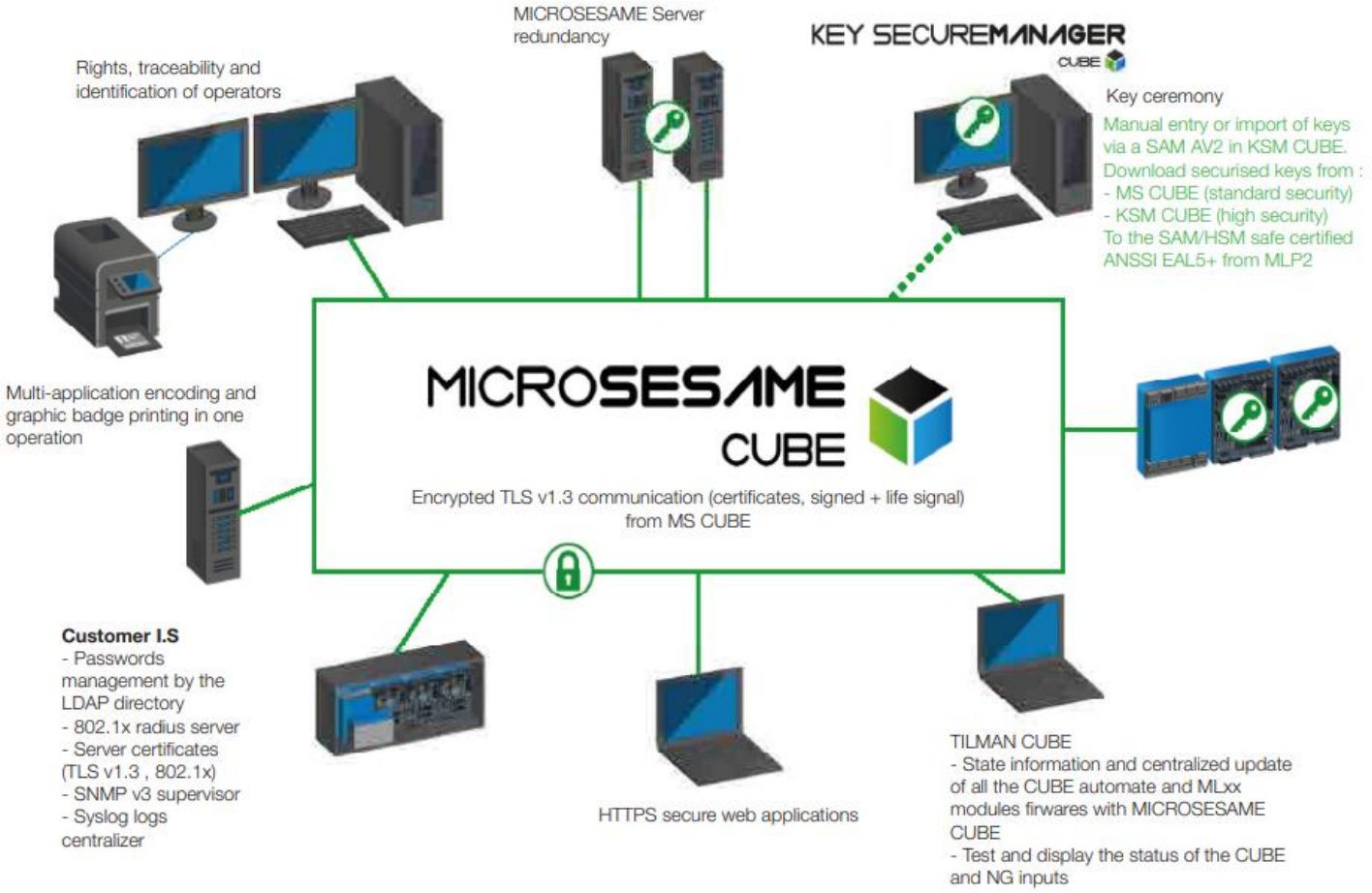

BADGE CUSTOMISATION
ENCRYPTION & PRINTING
VISITOR RECEPTION
APPOINTMENT MANAGEMENT
PORTABLE USE
WEB FUNCTION
ALARM REMOTE
TRANSMISSION
ENCODER
BADGE PRINTER
RECEPTION TERMINAL
MOBILIS 3 CUBE
WEBSESAME CUBE
MONITORING STATION
LDAP,
BASE RH,
ID MANAGEMENT SYSTEM
...
BUILDING CONTROL SYSTEM
ACCESS MANAGEMENT
INTRUSION DETECTION
VIDEO
INTERCOM
THIRD-PARTY INTRUSION
HYPERVISOR
THIRD-PARTY SYSTEMS
EXTERNAL DB
MICROSESAME CUBE
TILLYS CUBE
MECHATRONIC
COMMUNICATION HUB
TERMINAL TO LOAD RIGHTS
ONLINE
OFFLINE
ACCESS CONTROL
MLP2
MLP2
MLP2
AA-555-AA
INTRUSION & B.M.S.
TACTILLYS
MLIO16
SENSOR
EQUILOCK
SENSORS ON BUS
MLGTB
20°

CYBER-SECURE SOLUTION, ARCHITECTURE 1 CSPN CERTIFIED ANSSI

Protecting sites is no longer enough. It is also important to put in place mechanisms to secure the security system itself against external and internal threats.

Across the **MICROSESAME** architecture, from badges to servers, electronic and software protections are implemented to prevent malware or hacking.

To ensure the best security and cyber security, the solution is certified ANSSI, according to the Architecture 1 recommended by ANSSI (transparent reader).



MICROSESAME CUBE, the CUBE hardware range (**TILLYS CUBE**, **ML** remote modules) and "transparent" **EVOLUTION** readers provide you with the following cyber security qualities and capabilities:

- Official ANSSI certification and qualification required for regulated sites, according to the laws in force and advised on all sensitive sites.
- An ANSSI qualification to maintain this level of security in the long term (TIL TECHNOLOGIES committed to maintain the ANSSI standards).
- A secure end-to-end solution, from badge to server.
- All TLS v1.3 secure IP network communications with certificates between the server and the automat on the one hand and customer workstations on the other.

CUBE CASES:

- Default and abuse information can be managed: pull-out, damaged case, communication defaults, power defaults (sector, low battery, charger). Error and sabotage protection through balanced inputs, outputs and RS485 buses. Protection against short circuits, surges and polarity reversals.

TILLYS CUBE CENTRALS:

- An embedded HTTPS web server for local configuration.
- 802.1X (Radius) compatibility. SNMPv3 for monitoring system status and alarms.
- A modular architecture with 3 ANSSI certified and secure AES 128-bit RS485 buses.
  Remote access control and intrusion modules are connected through these buses to allow:
  - Reusing the existing wiring to save costs.
  - Certifying existing wiring.
  - Having a distributed or centralised architecture to choose from
- Firewall Protection for Denial of Service (DoS) Attacks.

MLP DOOR MODULES:

- Secure AES128 bits RS485 communication with transparent readers.
- A natively integrated ANSSI EAL5+ certified HSM containing the "access control" application keys of the badges.
- Applets (setting) to adapt to the customer badge chart and to control LEDs and buzzers of the transparent readers. Access to the MLP/MLD applets settings is protected by operator access rights.

RFID READERS:

- ANSSI-certified keyboard readers under architecture 1 known as "transparent readers" (no badge key stored in the reader) to manage your high security DESFIRE badges.
- EVOLUTION transparent biometric readers managed using the SCCPv1 and SCCPv2 (ANSSI certified) protocols from MLP modules handling new status (Badge OK but fingerprint forbidden, timeout) and duress fingerprints.

KEYS MANAGED BY THE END CUSTOMER:

- For any badge applications (access, restaurant...), which are entered or created (key ceremony) by the customer on a single dedicated interface (KSM NG). These are easily backed up in a secure digital AES256 bits container placed on MICROSESAME version 2018. All these keys are never visible to third parties who design, integrate or maintain the system. 1 key ceremony is required for the integrator and the final customer.

KEYS & APPLETS:

- Secure applet and key, centralised from the server, or **KSM**, to the HSM modules of the MLP/D modules to facilitate the distribution of the keys and be able to change them in all modules from the central system, as required by ANSSI.
- A principle of key diversification, in line with the AN10922 standard, allows the end customer to have different keys depending on the badges and choose its formula by customizable padding.

THE CUBE PRODUCT RANGE:

- **TILMAN CUBE**, offers a centralised view of the entire CUBE fleet (automat, modules) to read and update their firmware versions via global downloads. It therefore makes it easy to manage corrective and scalable maintenance from a central station but also an aid to the commissioning by tests, wiring diagnostics of detector inputs.
- The TILLYS CUBE security solution (which is certified in access control) is also available for intrusion, offering you a cyber-secure central managing intrusion.
- The CUBE firmware is signed to guarantee their integrity.

STRENGTHENED SECURITY

- Strengthening security by removing the reverse DNS code (impact on certificate content).
- Operator passwords are protected in BDD by SHA-512 HASH & 512 random characters SEL.
- **WEBSESAME** portal protected from "CSRF" attacks.
- A web query with library queries about suspicious behaviour (multiple attempts to access no-go zones...). Editable list, automated reports.

HIGH ADAPTABILITY TO YOUR COMPUTING ENVIRONMENT

Hardware and software recommendations depending on your system size are available.
MICROSESAME tracks the evolution of OS and database versions to remain compatible with the latest computing environments.
Before any system installation or migration, you can refer to specific documents, updated regularly and available from your usual TIL contact.

COMPATIBILITE WITH LASTEST OS AND DB:

- Server: Windows 10 or 11 PRO or Enterprise (64 bits) - for small systems. Windows Server 2019 or 2022 Standard or Essential Edition (64 bits).
- Thick-client: Windows 10 or 11 Pro or 64-bit Enterprise.
- Database: SQL Server 2017 to 2019 (64 bits).

ADAPT TO "LIGHT CLIENT" INFRASTRUCTURES:


Windows **RDS**

- Compatibility with RDS (i.e.: TSE)/ Citrix solutions.
- No **MICROSESAME** app to install on stations.
- Connecting from any network station.
- Floating license operation /simultaneous connections.

WEBSESAME WEB PORTAL FOR FUNCTIONS ACCESSIBLE FROM THE CLIENT INTRANET:

- Self-adaptive screens (resolution and orientation) in different format (smartphone, tablet, PC).
- Improved ergonomics for simplified use on tablets and smartphones (self-complete fields, photo display, check buttons).
- Functions available for a large population:
  - WEB-APPOINTMENTS: Managing appointments, visits, visitors
  - WEB-USERS: Managing users
  - WEB-REPORTS: Generate, export reports, predefined queries
  - WEB HISTORY: History access control events, techniques
  - WEB-ALARMS: synthetic view of current alarms
  - WEB-REAL TIME FEED: Real-time monitoring of events access, technique, system. Click to view the user profile of the event. Simplified Event Monitor
  - WEB-AREAS: identify + nb of people present in an area
  - WEB-Activity-tracking: Add and view open operator issues/comments of current acknowledgeable alarms. Simple search or by filters.
  - WEB-My site: Edit synthetic reports & graphs of authorised and refused passages on supervised sites.
  - WEB-Properties: Help to diagnosing its installation: View the list of states / properties (e.g: open port) of a supervision object, perform filter searches, Interact with these states (remote controls), Inhibit a property if maintenance

COMPATIBLE ON A VIRTUAL ENVIRONMENT (VMWARE):

- Server pooling, energy savings.
- Software license compatible with this environment.
- On dedicated physical machine or data centre.

- Redundancy possible by environment (VM HA module).

OPEN TO YOUR NETWORK AND ARCHITECTURE CHOICE:

- Third party architecture (DB, application server, WEB server).
- VPN, VLAN compatible.
- SMTP/email transmissions.
- Automat TILLYS-CUBE 802.1x compatible, SNMPv3, IPv6 ready, Host Name possible.

SYSTEM/HARDWARE REDUNDANCY:

- Compatibility with the SAFEKIT redundancy solution.
- Pre-set interface for **MICROSESAME**.

INSTALLATION PACKAGING. INTEGRATED AND SIMPLIFIED MIGRATION AND RESTAURATION PROCESS:

- Easy installation of **MICROSESAME** server and client stations. All components are included in the installation package.
- Client and server migration tools available.
- Semi-automatic update for light clients through the server.
- All "System" applications in service.
- Backup, automatic DB back up according to a pre-set path, restoration tool.

OPERATOR RIGHTS MANAGED VIA LDAP

See dedicated chapter for further details

SYSLOG SYSTEM EVENT GATEWAY

The system event gateway sends events relating to security, stability and performance to the IT. There are no events related to building security (physical access control, intrusion, etc.). This gateway enables IT to monitor the MICROSESAME application in addition to the traditional OS probes (RAM, CPU, etc.). Each event can be activated/deactivated in the gateway settings. Events are transmitted via the SYSLOG channel. They are also inserted in the system event history.

Event list :

- Operator security events
  - Authentication success / failure
  - Password change
  - Unauthorised action (= elevation of privilege failure)
- Network / machine security event
  - Expiry of communication certificates at different levels of the architecture.
- Stability events
  - Unexpected shutdown of a PLC
- Performance events
  - Access update download time too long

HIGH AVAILABILITY & PERFORMANCES

The architecture has been designed to offer you high-availability and performance through:

- Autonomous operation of each **TILLYS CUBE** unit, with its extension modules and devices, without Ethernet network and/or server, keeping a history log with the last 10,000 events when communication is lost with MICROSESAME, automatically downloaded when restored.
- Direct cross-central IP communication (anti-pass back). No server required.
- The **TILLYS CUBE** centrals simultaneously process badges in less than 500 ms, even with transparent readers and high security badges. The HSM crypto-processor present on all modules manages the readers for parallel decryption.
- Server redundancy is possible with the client virtual environment or the SAFEKIT solution, validated and distributed by TIL.
- Third-party IT architecture possible to multiply machine power
- Temporary license recovery website available 24/7 in the event of a server crash
- Industrially designed CUBE controllers with a 20-year-old MTBF and a 5 mn MTTR
- Parallel download to all UTIL from the server

ASSISTANCE & ADAPTABILITY TO ANSSI BADGE ENCODING CHARTS

The TIL solution allows for high security and project adaptability in key management and badge mapping according to the final customer encoding chart.
TIL TECHNOLOGIES offers support to the end customer to help them develop an encoding chart for multiple application, ANSSI-compliant, high-security, flexible badges.

4. FEATURE-RICH SAFETY AND SMART BUILDING MANAGEMENT

MICROSESAME is an open and scalable system. It supervises its own controllers and devices, sensors and actuators. It handle third-party products or systems (industrial controllers, air conditioning, heating, fire, et.) interfacing with them according to several protocols (MODBUS IP, OPC UA, etc.) as well.

MICROSESAME provides functional richness for safety and smart building management as it covers several safety areas (such as access control, intrusion, supervision...) and several markets (industry, tertiary, sensitive sites, infrastructure, communities,). It allows you to adapt its configuration to the exact needs of the end user and to be scalable if necessary. Here is a non-exhaustive list of key functions:

PEOPLE & OPERATOR MANAGEMENT

USER MANAGEMENT (permanent/temporary users, visitors, operators) and their personal data: identities with pre-existing fields (name, first name,) and customizable fields or pre-set drop-down lists, validity duration, attachments, latest badge passage information, "user status» ("VIP" ...).

ATTRIBUTION OF MULTIPLE ID (badge, car plate, virtual badge, QR code,) per person, up to 4 technologies per server among N, and 99 identifiers per technology (e.g.: 2 badges, 3 cars).

BUILT-IN BADGE BACKGROUND EDITOR: fixed and variable texts, photo, QR code, logos, ...), recto/verso, colour, ... can be used to customise your badges.

MAPPING / ENCODAGE is highly customizable and secure.

GRAPHICAL CUSTOMISATION, MULTIPLE APPLICATION ENCODING: secure (for access, restaurant, time management hourly, ...) and badge enrolment in a single operation on the printer for fast, easy, secure badge productions. Built-in encoding and badge background editing.

AUTOMATIC USER SYNCHRONISATION and generation of multiple application badges, encoded on **MICROSESAME** for Restaurant applications, time schedules, ...

SEE CHAPTER FOR FURTHER DETAILS ON OPERATOR MANAGEMENT, RGPD, ENCODING & BADGE CUSTOMISATION

ACCESS CONTROL

- Management of profile-based individual access rights, with start and end date. Access rights are assigned to the users, regardless of the ID or the online/offline readers.

- Group changes in access rights for people resulting from a multiple criteria search.

- Automatic allocation of access rights for people imported from an HR database, through pre-set rules across all user fields (e.g. profile 1 in department 1).

- Automatic download of the list of authorised persons to the TILLYS NG centrals, as soon as the validation process is finished.

- Elevator management with floor filtering by person, time schedules, crisis level.
  Priority for specific staff (Hospital…).

- Compatibility with different technologies and all types of access control readers:
  - Proximity badge readers in 125 kHz and 13.56 MHz (MIFARE, DESFIRE, ICLASS, ...).
  - MOBILIS Reader 13.56 MHz (MIFARE, DESFIRE).
  - Long-distance readers, active badges or remote controls.
  - License plate readers, biometric readers or QR code displayed and read on smartphone.
  - Cylinders and mechatronic crutches for both online and offline solutions...
  - Online solution TIL + STID for virtual badges on smartphone with:
    - EVOLUTION reader bi-technologic Bluetooth/13.56 MHz +
    - STId cloud platform

- Command of different controlled accesses or actuators (barriers, electric locks, tripods, displays, sirens, lighting, ...).

- Highly flexible modus operandi: 2/3/X door airlocks, single or two-way, reader or keyboard reader (badge + code), mobile terminals, single or double badge swipe for risk areas with mixed populations in different categories, ...

- Advanced features with cumulative impact on access rights:
  - Control of rest times.
  - Clearance (electrical, medical authorizations granting access to specific areas) applied to specific individuals and specific areas, with defined start and end dates.
  - Crisis level among the 7 (vigipirate) possible levels, assigned on a person basis, and for specific floors via an operator command on synoptic or enslavement. Procedures to choose according to crisis levels (badge -> badge, badge + code, double badge).
  - Temporary and geographic anti-passback management, at a local or global level, and depending on APB waiver.
  - Forced access with badge + specific code.
  - Dependency concept: Mandatory badge swipe on reader X before swiping the badge on reader Y.

ACCESS CONTROL SPECIFIC FEATURES

VISITOR MANAGEMENT with a full workflow of visit and visitor creation, from visit validation to on-site visitor hosting.

PARKING MANAGEMENT and sensitive areas with area counting, possible access threshold by category type.

CONTINGENCY PLAN ASSISTANCE (mustering) (simulation or real conditions) with dedicated interface to display the list, the counter, the current location of people in each of the secure/risk areas. Charts and user pictures are available, as well as a printed version, for rescuers to use.

MULTIPLE SITE & LOCATION MANAGEMENT with concepts such as site (hardware, supervision material), entity (individuals), classification (readers), perimeter (keys) as well as operator management.

PCVA: Video access control performed by an operator. After badge detection, the operator may allow access or may just be informed, and access managed according to access rights.

REGISTRATION (electrical authorization, medical authorization, …) per person and per access with start and end dates.

REST TIME MANAGEMENT: to comply with employment regulations.

PATROLLING ROUND MANAGEMENT centralised itineraries, badges swiped on specific badge readers.

QUARANTAINE managed by **TILLYS CUBE** centrals (Quarantine area, itinerary and duration must be defined).

BAGES ACTIVATED ON THE SYSTEM directly by users by entering a personal activation code on the CARDIGO terminal

INTRUSION

MANAGE ALL DETECTION INFORMATION from any contact type (such as radars, sensors) is managed. Contacts may be connected to:

- Controller balanced inputs, TOR of our centrals
- **EQUILOCK** transponders linked by bus to **EQUILOCK** modules,
- Centrals, or third-party systems connected to our system through MODBUS, OPC…,
- Or **SORHEA** solutions (interfaced via **MAXIBUS),** or VMS image analysis data (interfaced via SDK to our system).

INTRUSION RIGHTS ASSIGNED AND CENTRALISED for all **TILLYS** centrals through **MICROSESAME**: simplicity, speed, flexibility. Several intrusion areas can be managed on several authorised intrusion centrals.

ON/OFF SURVEILLANCE ON PARTICULAR AREAS intrusion area surveillance on/off by time schedule, by **TACTILLYS CUBE** keyboard multi-area management with auto/manual/forbidden ejection, counting, authorised access, combination and sequential enslavement defined by project (e.g. triple badge swipe on reader).

FULL & NATIVE INTERACTION with access control features, all managed by the same **TILLYS** central.

AUTOMATED ACTIONS for third-party systems (video, siren, lighting, ...).

TRANSMISSION OF INTRUSION ALARMS (including access control & BMS) to a IP remote monitor with standardized protocol TIL "TIP" - qualified at ESI, Azur soft.

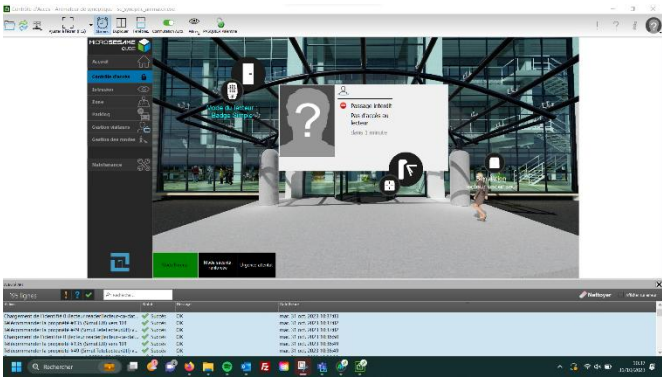
SUPERVISION & HYPERVISION FOR SAFETY AND SMART BUILDING

GENERAL INTERFACE ERGONOMICS
to ensure easy operation.

EVENT MONITOR, real-time alarms with quick search and multi-criteria filtering.

SYNOPTIC GRAPH EDITOR & VIEWER, native and quickly configurable, highly customizable, using the notion of objects, library, zoom, ...

SUPERVISION WITH ANIMATED SYNOPTIC PLANS
Synoptic graphs with animated symbols



REAL TIME MONITORING OF ACCESS CONTROL ALARMS such as intrusion, fire, technical defaults (elevators, air conditioning ...), with alarm acknowledgement, associated instructions and based on the operator profile.

AREA SURVEILLANCE WITH COUNTING
Contingency plan with a dedicated interface displaying the list, counter, location of the presents of each area.

INTERFACING MICROSESAME and VMS in the market (MILESTONE, GEUTEBRUCK,etc). The built-in **VISIOSESAME** feature offers:

- ► Supervising simultaneous video streams of multiple VMS in parallel.
- ► Live images can be viewed by clicking the icons in the synoptic graphs. Piloting domes, image walls …
- ► Automated video recordings to VMS on intrusion alarms, access, ...
- ► Replay of video recordings on VISIOSESAME associated with the alarms in the MICRO-SESAME history log.
- ► Integration of video alarms (image analysis) and VMS cameras defaults (or others).
- ► Dashboard for a supervision of system processes by the I.T. service, DSI (manual start/stop of deamon & services, statistics on polling, ...).

WIDE POSSIBILITY OF INTERFACING & HADWARE OR SOFTWARE GATEWAYS

POSSIBLE CONNECTORS FOR OUR **MICROSESAME** SYSTEM:

- ▶ User base & visitor management: Web service API REST, CSV files.
- ▶ A.D operator management: LDAPs, Authentication with the Windows account (SSO NTLM, WEB:SAMLv2).
- ▶ I.T. Supervisor: SNMPv3 (from automat TILLYS CUBE).
- ▶ Hypervisor: OPC UA, MODBUS IP.
- ▶ Controllers, third-party systems: MODBUS IP.
- ▶ VMS video System: VMS SDK, TEXT/ASCII gateways
- ▶ Specific gateways for projects or hardware (directory, third product, various SDK…)

More information and examples in the dedicated chapters: GATEWAYS AND CONNECTORS, VIDEO SUPERVISION, INTERCOM

ENERGY MONITORING

- ▶ Consumption tracking.
- ▶ Total or partial consumption tracking.
- ▶ Derogation areas by priority level and based on power.
- ▶ Annual programming of controlled areas (up to 3 annual programs)

LIGHTNING AND OTHER ACTUATORS

- ▶ Start/Stop command with time programming.
- ▶ Restart or derogation by timer configurable duration (rooms with irregular occupancy).

HEATING, VMC, AIR CONDITIONING CONTROL

- ▶ On/off control of controllers with time programming option
- ▶ Definition of temperature set points and operating modes: frost protection, reduced, economy, comfort, etc.
- ▶ High and low temperature threshold readings

DOMESTIC HOT WATER CONTROL ECS

- ▶ On/Off control with time programming option
- ▶ Programming of operating modes: Automatic, Manual or programmed restart

5. SYSTEM CAPACITY

Hardware settings	
Simultaneously connected client stations	499
Programmable controllers (TILLYS CUBE, TILLYS NG)	10 000
Controllers on a same IP line	255
Supported drivers (lines)	128
Badge readers	20 000
Video recorders	256

Access Control settings	
Users (users, operators, visitors)	Unlimited
IDs (badge, plate number,)	Unlimited
Sites	2048
Entities	2048
Reader groups	Unlimited
Readers by group	1024
Access areas	128
Clearance	256
Visual access control	256
Patrolling rounds	64

Supervision settings	
Tracks, total properties	40 960
Tracks, properties per line	8 192
Property categories	64
Totalizers	2 048
Properties in a formatting chain	16

Operation settings	
Operators (centralised)	Unlimited
Users of Intrusion TILLYS V2/CUBE/NG (local)	150

Access control (Id/User record)

Reader technologies that can be associated with user records	4
Number of ID per reader technology	99
Length of badge code (to match with TILLYS NG drivers)	32 char.
Length of site code (to match with TILLYS NG drivers)	32 char.
Parameterizable fields (size, breakage, length, free entry, mandatory, assisted)	16
Downloadable fields to TILLYS NG (no more than 20 characters)	Name, first name + first 6

Time schedules and holidays	
Time slots per site / TILLYS NG (single-site, a site may use several centrals)	256
Total time slots on multisite main server	256 x nb of sites
Days per time schedule	9 (week + exceptional days and public holidays)
Daily time schedules	4
Minimum time schedules	1 min
Exceptional days	32

History log	
Events in the history log	Unlimited (depending on DB)
Maximum event number per query	Unlimited
Retention time (parameterizable – For instance, CNIL 3 months requirement)	30 d. by default

Hardware capacities	
Downloadable IDs - TILLYS NG	10,000 (native) up to 600,000 with XL option
Local historic of event - TILLYS NG & CUBE	10,000
Downloadable IDs – TILLYS CUBE	Up to 600,000 (native)
Readers per central – TILLYS NG	8, 16 or 24
Number of intrusion detector groups - TILLYS CUBE	32
Number of detectors per TILLYS - Intrusion CUBE	624

6. CNIL & GDPR COMPLIANCE

FINE MANAGEMENT OF MICROSESAME USER RIGHTS

MICROSESAME complies with the GDPR regulations for the following functions.

It is then appropriate for the end customer to:

- ► Apply and implement **MICROSESAME** features.
- ► Define the data to be recorded in the user record free fields (permanent, temporary, visitors).
- ► Define operators and their data access rights.
- ► Where is installed the SQL database containing the data and who has access to the SQL database.
- ► Follow CNIL procedures (for example, for access control and biometrics in particular).

USER ACCESS CONTROL (INCLUDING OPERATOR RIGHTS FOR VISITOR MANAGEMENT)

- ► Access to personal data from user records, filtered by operator rights according to authorised fields and entities (category or site).
- ► Access to authorised data can be read only or/and read & write.
- ► It is possible to define which fields are required in the visitor records (≠ from permanent records).
- ► Without the "Appoint management profile" assigned, this operator will however be able to:
  - Search for a visitor in an existing visitor database. Self-completion will suggest existing data, to avoid duplicates. Only fields such as name, first name, visitor society will be visible.
  - Create a full visitor record with all the existing fields (birth...), if the visitor does not exist yet on the database.
  - In both cases, the operator will not be able to be edit, change or check the data in the visitor record

  If right is activated is enabled, the operator will then be able to edit, change and view all the information in the visitor record.

TRACEABILITY: TYPE OF TRACES, RECORDED DATA AND CONSERVATION TIMES

- ► All changes, consultations, removal of people data are traced, it is impossible to act on **MICROSESAME** without leaving a trace.
- ► The data conservation duration is adjustable.
- ► Manual removal of data for people no longer being part of the society.
- ► Import users with an automated HR database minimizing human manipulation.

DATA BACKUPS

- ► Periodic, automated backup of DB on disk, without human manipulation.
- ► Possibility to archive history logs.

DATA ENCRYPTION

- ► Securing access flows: Heavy clients in TLSv1.3, light clients in Https.

► Operator passwords in DB protected by HASH SHA-512 + SEL of 512 random character SEL.

► **WEBSESAME** portal protected against "CSRF" attacks.

► **MICROSESAME** allows DB data to be anonymized before being transmitted to a third-party for Bug and migration tests.

SOFTWARE PROTECTION & SECURITY MAINTENANCE

► Updates, security patches provided by the AMCO PREMIUM package (ANSSI certified) from TIL.

DATA PROTECTION IMPACT ASSESSMENT / PRIVACY IMPACT ASSESSMENT

► Not required for implementing badge security devices without biometrics, according to pdf.
The list of types of processing operations for which a data protection impact assessment is not required can be downloaded from the following link:
https://www.cnil.fr/en/guidelines-dpia

CNIL DECLARATION FOR ACCESS CONTROL AND BIOMETRICS

Biometric elements (such as fingerprints...) are not directly managed by TIL TECHNOLOGIES. The **MICROSESAME** solution is therefore not concerned by the AU52 (1:1) - AU53 (1:N) biometrics usage declarations.

The **MICROSESAME** solution integrates biometric readers from the market such as IDEMIA and STID. Our controllers only read the identifier (of the badge or a local database) sent by this reader and in no way the fingerprint. Only these readers manufacturers manage biometrics. They have their own biometric enrolment tools (SECARD BIO, MORPHOMANAGER) and must comply with the technical requirements of the AU52 (1:1) - AU53 (1:N) biometrics declarations.

For the record, here are the following procedures to be established and followed by the end customer:

► CNIL Access Control Statement, excluding biometrics, NS-42 Simplified Standard

- Identification elements: 5 years after the employee departure, manual user removal on **MICROSESAME**
- People travel items (3 months): Historical depth parameterizable on **MICROSESAME**: 3 months or more

► Statement of Use of Biometrics AU52 (1:1) - AU53 (1:N). Fingerprint management must be compliant especially on AU53 (more demanding than AU52)

7. OPERATOR MANAGEMENT

FINE MANAGEMENT OF MICROSESAME RIGHTS

An operator is an individual that is authorised to use the **MICROSESAME** supervision interface. This user, depending on his function, his hierarchical level or his geographical location, may access all or part of the features and data available in **MICROSESAME**.



To assign to each operator only the necessary rights, and to do so quickly by type of operator, **MICROSESAME** integrates the notion of "operator profiles". Such profiles are defined by a system of checkboxes representing the different rights and the possibility to view, create, change or remove:

- ► Access control rights
- ► Operation rights
- ► History rights
- ► User related rights (including personal data)
- ► Visitor related rights
- ► Supervision rights (including property categories such as access, intrusion, fire, ..., alarm, acknowledge level/mask)
- ► Settings related rights (including filtering for multiple site projects based on reader sites, synoptic object's sites, user entities, access classifications at the finest level (fineness higher than the concept of "site")
- ► Security related rights

Given the richness and finesse of these profiles/operator rights, specific documents are made available and updated regularly, to which you can refer for further details, and which are available from your usual TIL point of contact.

For each operator, one or more pre-defined operator profiles may be assigned.

Rights management is secure, easy, planned for a large population. Operation is made easy, as well as maintenance and implementation, because:

- ► Changes in operator profiles will be automatically populated to all concerned operators.
- ► One or more profiles can be associated with the operator to allow the operator to put himself in the same conditions of another operator that he would like to help for example.
- ► An operator is first and foremost a "user" who has physical access rights and who has also been declared as an operator of the **MICROSESAME** software. This avoids duplicating personal data and records.
- ► Hierarchy between operators: In order to change operator rights, the hierarchical level of the operator making the change must be higher than the edited operators (hierarchical level and profile).
- ► Operator passwords are protected in BDD by HASH SHA-512 + 512 random character SEL.
- ► Traceability and history of operator actions (with values/edited fields) which is a regulatory requirement in many sectors of activity (agri-food, pharmaceuticals, transport, nuclear).
- ► Centralised management of operator rights in **MICROSESAME** for all types of client stations (heavy, light, WEB).
- ► A default login and password are provided to each operator. These must be changed by the operator upon first connection, so that these will only be known to him.
- ► Automatic disconnection of **WEBSESAME** operators after a long inactivity period or restart of the WEB apache server.

LDAP/ACTIVE DIRECTORY

Operator management is possible on the **MICROSESAME** system or from a centralised Active Directory (A.D) of the end customer, managed by its I.T. department, and interfaced with **MICROSESAME** by a gateway using the LDAP protocol. This allows:

- ► One single directory is the referent for all users of the company applications. The creation, modification, removal of operators is easier. The update is easier and automatic.
- ► Assigning in this A.D the operator profiles preset in **MICROSESAME**. Considering multiple profile operators with LDAP authentication.
- ► Managing complex passwords by the power of the A. D.
- ► Manage operators in secure mode with LDAPs.

8. MULTIPLE SITE/ CLIENT MANAGEMENT

GEOGRAPHIC OR ORGANIZATIONAL OPERATION

MICROSESAME manages up to 256 different sites from the same system. This function is interesting in many cases:

- The management of geographically dispersed buildings: network of agencies, buildings of a local community, production sites... from a single central server.
- The need, within the same site, of managing different rights adapted to each service.
- The sharing of the same building or tower by several companies or tenants. Differentiation of common area access and company specific access.
- The choice at the server level: 1 national server for all sites or 1 server per site depending on the constraints (network quality) and organization (centralised, decentralised).
- The choice at badge administration level with:
  - Personalization & centralised encoding at headquarters.
  - Centralised generic encoding at headquarters and site-specific customisation.
  - Personalization & encoding on each site.

The use of the multisite function requires a manager/senior administrator to:

- Administering the single centralised database
- Define sites, the smallest site being a TILLYS NG.
  The following elements must be considered:
  - the TILLYS NG is single-site in the architecture
  - the choice and location of the TILLYS NG
  - the associated wiring impacts.
- Define the entity assignment for individuals
- Define operator and operator rights by site, depending on the organization & procedures
- To create managers by site, services, company. The notion of operator hierarchy allows to finely manage each site including:
  - Staff/entity access rights on the site readers and, if any, on the common readers (reception hall, car parks, elevators...).
  - History and staff moves can be checked.

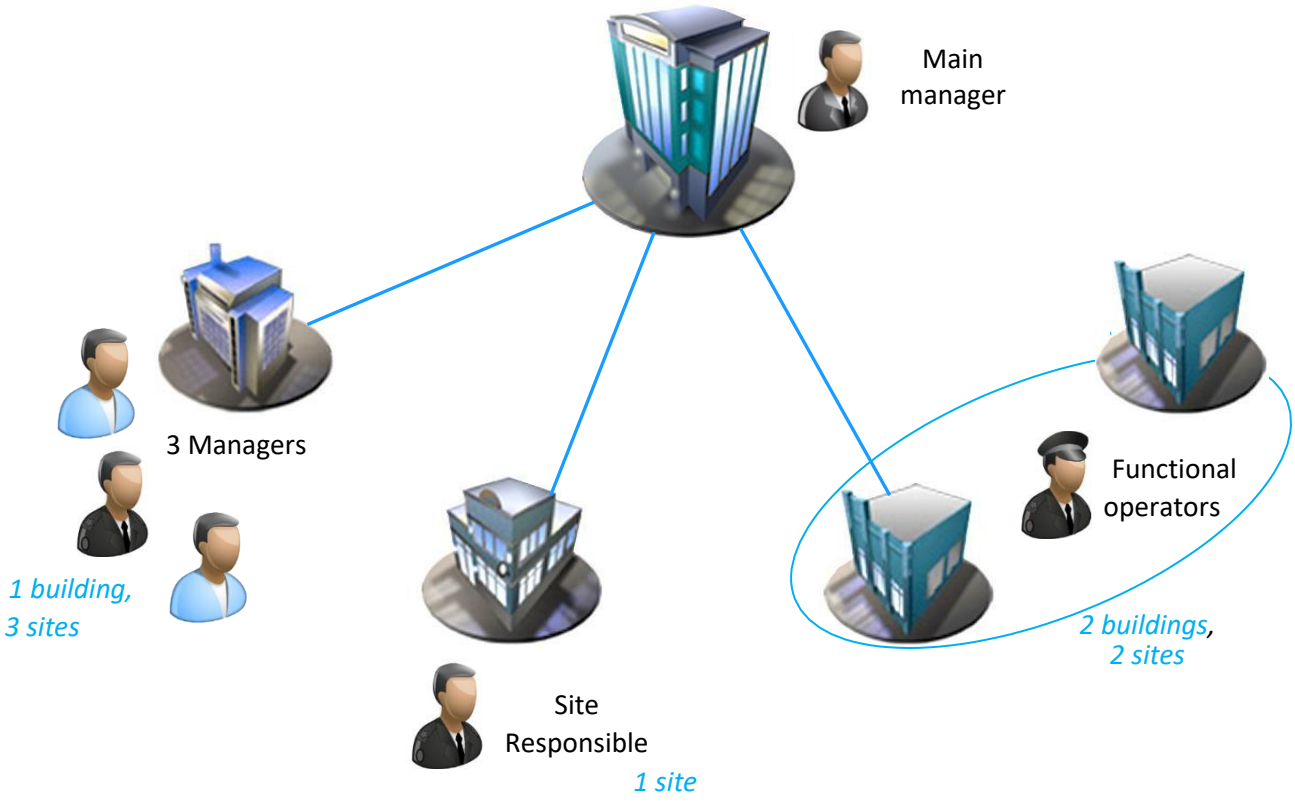
  They will not see the readers neither the access rights for other sites, nor the people and their entity history.

Each site has 256 independent time schedules, used either as part of the access control, the intrusion, or as part of the technical management of buildings (alarm system, automatic watering...).

For all sites, the system can create up to 256 sites and 256 x 256 time-schedules in total.

For badge key security, KSM, the encoding tools and TILLYS centrals allow the central security officer to manage, if necessary, different badge keys per site. The perimeter concept is used as required by the ANSSI guidelines.

Specific documents on multisite architectures can be provided by your usual TIL point of contact.



9. ACCESS MANAGEMENT

PROFILES, SCHEDULES, CLEARANCE, READERS, AREAS...

The user/ID record aggregates and defines:

USER DATA: validity dates, company, department, contact information, as well as 16 additional customizable fields. Attachments may also be associated (work contract, photo...)

USER IDs: up to 4 different ID technologies are possible (13.56 MHz badge, 125kHz badge, keyboard code, license plate, QR Code...). Up to 99 IDs per user and technology can be used. IDs may have several statuses: broken, lost, stolen, not rendered... explaining why access was denied. One user can have several IDs assigned.

SPECIFIC ATTRIBUTES: anti-pass back, blacklist (for specific monitoring), accreditations (levels in crisis mode), possibility to receive visits, escorts, ...

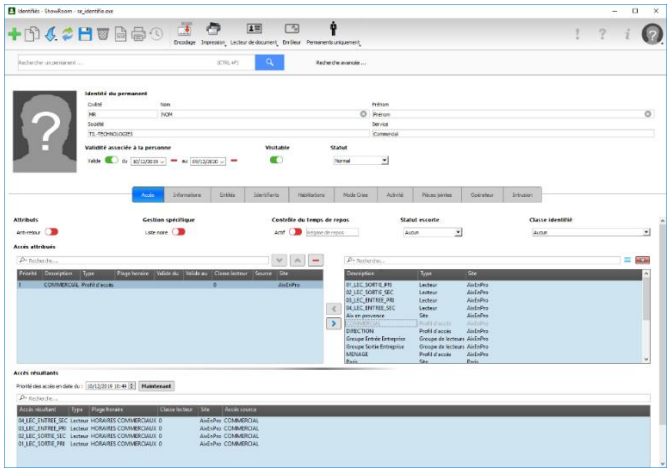
A VALIDITY PERIOD: which is associated with each user and allows to quickly and temporarily invalidate an ID, without destroying the list of its permissions

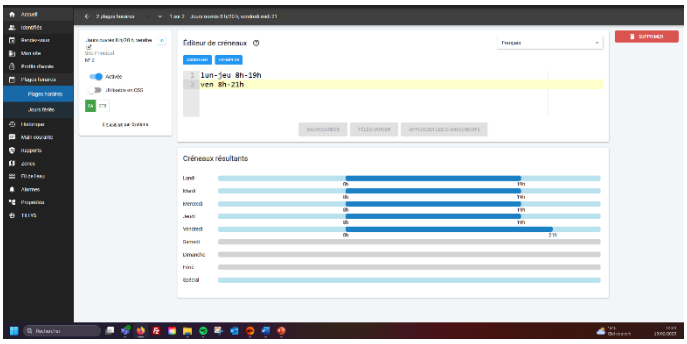
ACCESS RIGHTS MANAGEMENT, OFFERING FLEXIBLE VIEWING AND RAPID ALLOCATION OF ACCESS RIGHTS: common view, text filter, selection of multiple rights in a list of profiles, online/offline readers, reader groups, elevator floors, keys and group ofkeys for connected cabinets. Access rights are assigned to the user, not to the IDs (badge). So even if you lose and reassign another badge, it doesn't change the access rights.

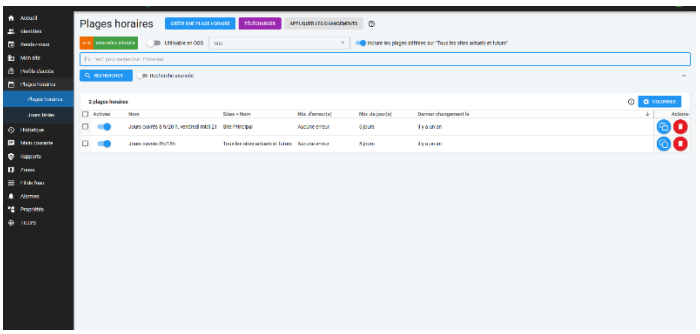
INDIVIDUAL ACCESS RIGHTS

Granting access rights allow the user to access the area concerned by a reader or reader group, according to a defined schedule (Up to 128 different time schedules possible).

The **TILLYS CUBE UTL** times are periodically updated by **MICROSESAME**, the time master, to ensure that there is no drift between the UTLs and the server and that the time slots are respected.





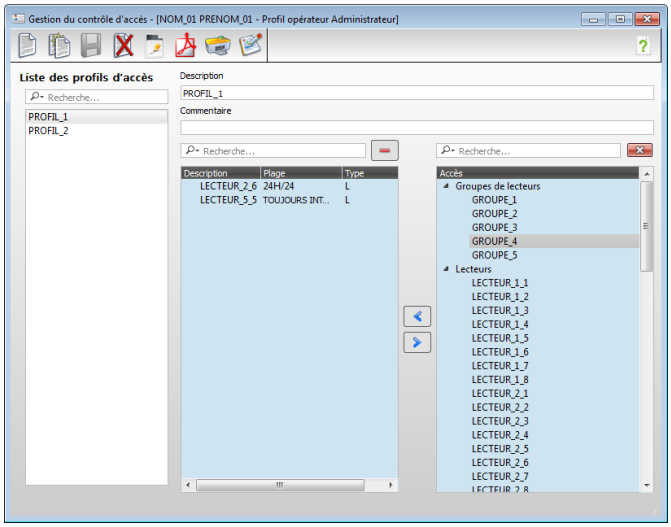


PROFILE-BASED ACCESS MANAGEMENT

The access profile allows you to pre-set access rights for a category of users, on one or more sites.
The profile consists of a list of

- Online/offline readers and/or
- groups of readers and/or
- Keys of connected cabinets
- Groups of keys and/or
- Lift level

Each reader or group can be associated with a different time slot.
Each user can have one or more access profiles associated.
Exceptions can be created for a particular person using individual access management by reader and/or reader group.



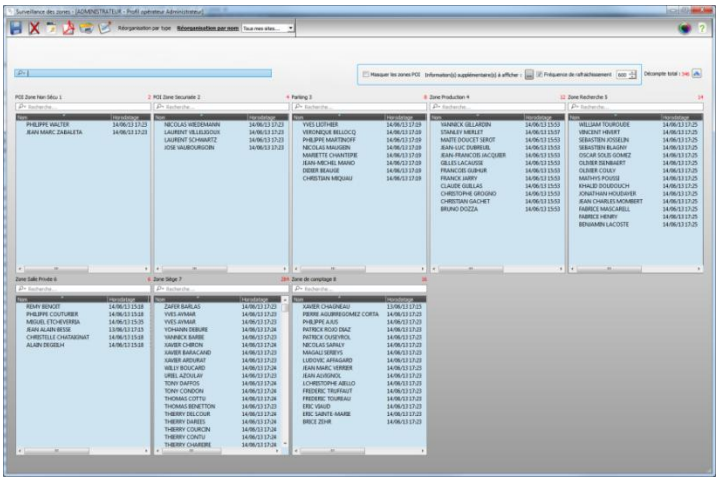
For example, a "general" profile can be used for common access, a "service" profile can be used for accessing certain areas and user-specific requests, concerning their function or hierarchical level.

MICROSESAME includes an "all-reader" access profile for each site that encompasses all existing and future readers of the site. This profile is handy when you want to provide a user with access to all the readers of a site. No need to edit profiles every time a new reader is added for a given site.

The management of user access rights is very flexible. Easy viewing and quick access rights attribution: full access view, text filter, multiple access selection in a list of profiles, readers, reader groups and lift floors.

The user management feature continuously displays "resulting access" obtained from access right attribution.

AREA MANAGEMENT



MICROSESAME includes the area management feature. One area is defined by two groups of readers: a group to enter the area and a group to leave the area. A group of readers may contain any number of readers.

It is possible to know exactly how many people are present in each area and to list them, in alphabetical order, in chronological order of arrival or any other sorting criteria.

Highly used by SEVESO-classified institutions, this zone management is essential to the implementation of the specific application developed by TIL for assistance to the Internal Operating Plan. See following pages for further details.

It is possible to send a list of presents in an area by email if the Contingency Plan is triggered.

Area management also allows for precise traffic control with the concept of dependencies:
The ability to nest one area into another and the activation of readers depending on exits in another area ("mandatory passage").

CLEARANCE MANAGEMENT

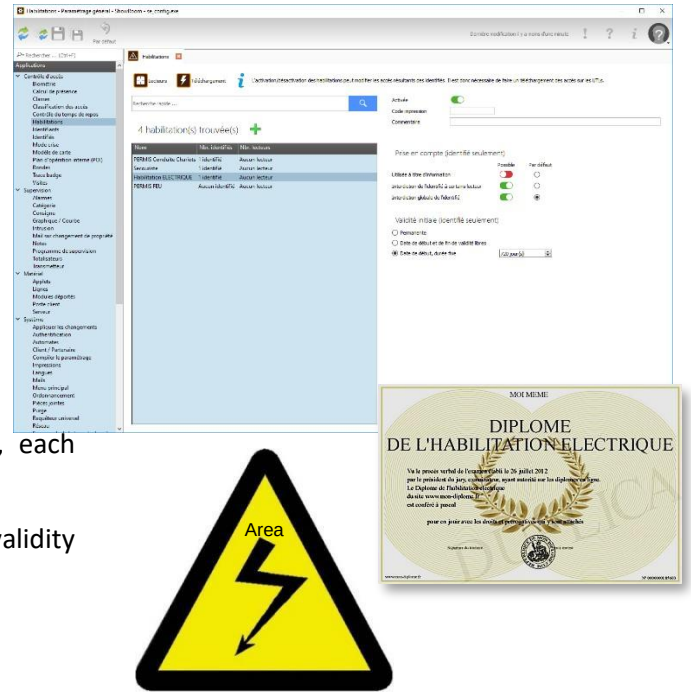
The user access authorizations, for certain areas or readers, can be conditioned by the possession of an authorization, external to the access control, that must be valid: electrical clearance, ATEX, driving clearance, first aid, temporary contract, medical, ...

This validity condition can be managed by different people, such as the HR department or any relevant functional manager.

This feature allows up to 256 clearance items.

Each user can accumulate several authorizations, each having its own validity period.

Access to a particular reader may be subject to the validity of one or more clearance authorizations.

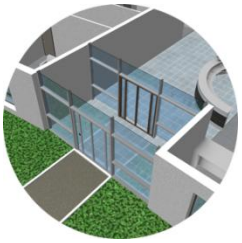


Electric authorization - Clearance

ENHANCED SECURITY FUNCTIONS

ANTI-PASSBACK: Areas having entrance and exit readers can use the area management feature to implement an "anti-passback" mechanism to prevent a user from entering an area several times in a row, without having left first.

MANAGEMENT OF ENTRACE HALLS & AIRLOCKS: The system programming strength also allows for the customisation of door enslavement. Several technologies can be combined: contact mats, uniqueness mats, video cameras, biometric readers...



TIGHTENED CONTROL ACCESS: **MICROSESAME** offers the possibility to declare certain readers using double control, by passing an authorised badge and entering a secret code on a keyboard. This enhanced control allows for strong authentication of the badge holder for sensitive access.

The secret code can be the same for all users or customised for each user.

DURESS CODE: **MICROSESAME** manages duress keyboard codes. A silent alarm is then generated immediately on the operator station and access normally opens without an audible alarm.

"BLACK LIST" MONITORING: This function allows you to set off an alarm as soon as a "black list" badge is displayed on one of the site readers. For example, on-site intervention in case of attempted fraudulent use of a lost or stolen badge.

CRISIS MODE: **MICROSESAME** helps manage crisis thresholds. Based on site-specific criteria, 7 levels can be assigned, both to people (according to hierarchy, clearances...) and to readers (depending on the areas, types of alarms...).

When a crisis mode is triggered, each system TILLYS NG receives the threshold change order and automatically manages matches between people accreditation levels and reader security levels. A person having a lower level (than the reader) will no longer be able to enter and/or access a floor via the elevator. Indeed, the crisis mode acts on all access rights for online readers including cabin management readers (elevators).

It is possible to generate several crisis scenarios by:

- Automatic enslavements according to combinations of inputs
- Operator actions allowed with a simple click on synoptic buttons previously configured by the integrator: X scenario will set the concerned readers at the desired crisis level.

QUARANTINE

MICROSESAME features highly configurable quarantine time management (from TILLYS NGv2.3 firmware).

It is recommended to use one TILLYS NG per quarantine area.
For each reader access given by a person X (quarantine reader), it is possible to set durations for the readers that are dependent on quarantine for person X (2 Hours on reader 1; 5 days on reader 2; etc...).

An alarm on the event monitor appears when person X, after passing on the drive triggering quarantine, attempts to enter a dependent access, without respecting quarantine times.
In case of a ban on access for non-compliance with the quarantine by person X, the message indicates that the person will be able to enter using the dependent readers, from a period expressed in days/hours.

TILLYS NG are fully autonomous, as they communicate directly with each other.
On network outage, each TILLYS NG memorizes the messages and badge times. These are automatically sent to other TILLYS NG upon network recovery.

ELEVATOR MANAGEMENT

The installation of badge readers in the building elevators limit access to certain floors, according to individual rights, staff profiles or companies in the case of a multi-site buildings.

MICROSESAME natively manages this feature, directly from the user right settings. Floors or floor groups are considered as readers in the building and can therefore be integrated into regular reader groups or access profiles.

Multiple site management in a multiple tenant building allows you to filter which floor is managed by which operator by recalling that a TILLYS NG is single-site. For example, the floors can be organized as follows:

- The developer, senior manager can manage access rights on all floors
- Each tenant manages the access rights only to these rented floors and common floors (DRC/home, car parks, canteen...) and only for his personal thanks to the entities

A tenant will be able to grant access to his floors and the common area. But the building main manager will keep hold of the common time schedules.

A TILLYS NG dedicated to elevator management is required to take advantage of this feature.

VEHICLE ACCESS AND CAR PARK MANAGEMENT

MICROSESAME can supervise readers dedicated to vehicle access, such as long-distance readers (remote control or active badges) or license plate or QR Code readers.

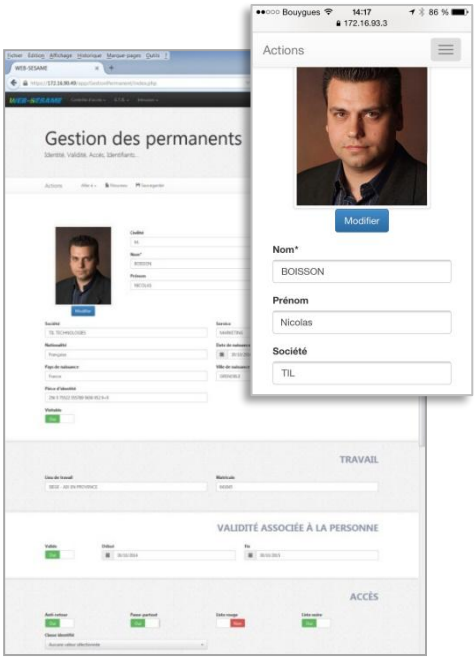
Such equipment facilitates the management of vehicle flows, especially at peak times, and provide greater comfort for users.

Integration in **MICROSESAME** is seamless: remote controls or long-range badges bring up a number, as a regular badge. License plates are directly managed in the user/ID record (up to 99 car plates per user).

This integrated ID management not only controls access but also allows, for example, to know:

- The total number of vehicles
- Occupancy rates by type of staff, service or company – in case of a common parking
- Volumes and occupancy times for imputations or rebills...

WEB-BASED USER MANAGEMENT



For simplified access control, in addition to server and client interfaces (See user record details on page 11), "light" web interfaces are available for user and visitor management.

From any PC or mobile device equipped with an Internet browser and connection, the new **WEBSESAME** interface allows:

- Searching and displaying users, depending on several criteria.
- The creation or modification of records, including the association of a photo (taken quickly by smartphone or tablet).
- The allocation of access profiles and existing users.
- Import/export of identifiers/identifiers.

These same functions are available for user record management (external to the site).

Other access control interfaces are also available in web mode, such as managing appointments (external visitors) or checking the access control history.

The ergonomics in **WEBSESAME** are optimized for use on tablets and smartphones (responsive):

- Self-adaptive screens (resolution and orientation).
- Auto-completion suggestions and photo display.
- Check buttons.

10. VISITOR MANAGEMENT

VISITOR HOSTING AND APPOINTMENT MANAGEMENT

On a site equipped with access control, external people must be able to be registered, accompanied or even provided with an ID, in order to be able to move in the authorised areas. This objective is requested in the final customer security policy or imposed by legislation (ANSSI guide for IVOs, OSE...).

The **MICROSESAME** visitor management allows planning, visitor flow management to optimize hospitality procedures and combines flexibility and security. To best adapt to the needs, procedures and organization of the end customer, the solution offers general parameters to predefine (e.g., limit the duration of a default appointment) and functional limits according to the operator profile of each applicant, validator, receptionist.

This **MICROSESAME** software option is made across three dedicated interfaces:

- The **WEBSESAME** web interface
- Reception stations (heavy client)
- Reception terminals (heavy client)

The ergonomics of these interfaces have been designed to provide with quick processing and with a clean interface to:

- Access functional tabs, filtered according operator rights, and data (default or specific)
- Self-adaptive web screens for resolution and navigation (portrait/landscape, field layout adapted to width...)
- Entering and searching for visitors using the self-completion feature,
- Adding photos by instant take (via webcam, tablet or smartphone).

The **WEBSESAME** interface is accessible to all authorised users with their PCs with a web browser from the company intranet. It allows visitors to be created, to plan and/or validate appointments and to complete the necessary information (time schedule, access profile, host, visitor card...).

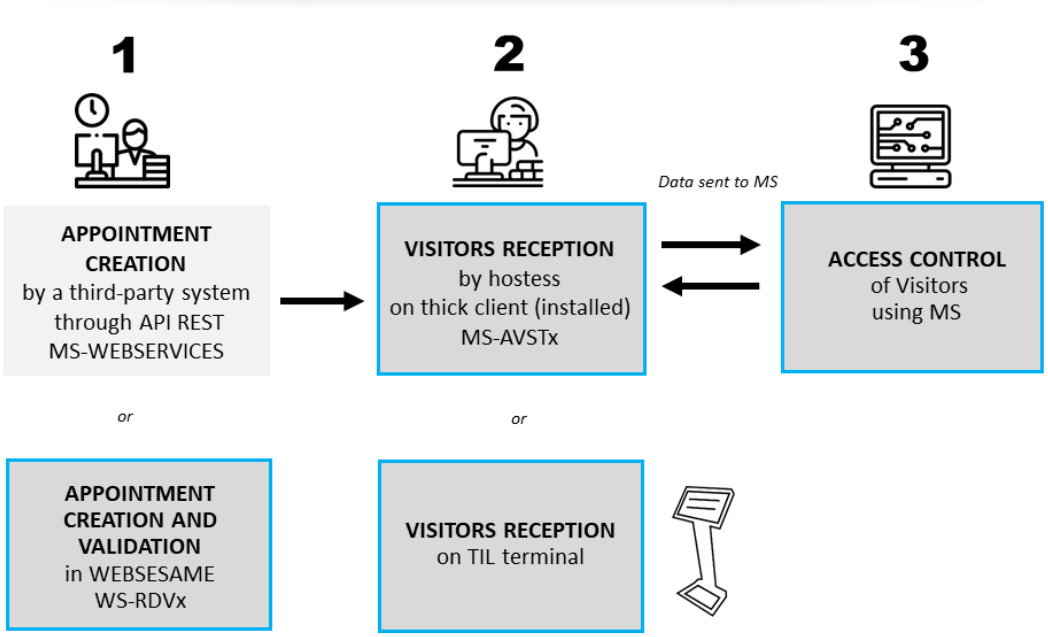
The Visitor hosting application, installed in heavy clients at the physical entrance of the building, allows a great fluidity and the most complete operations, from the allocation to the return of badges to visitors, the creation of unexpected visits, the scan of identity papers or the printing of personalized badges/cards. "Heavy" stations must be connected by network to the **MICROSESAME** application server.

The touch- terminal, with built-in QR code scanner, offers 2 choices on its screen:

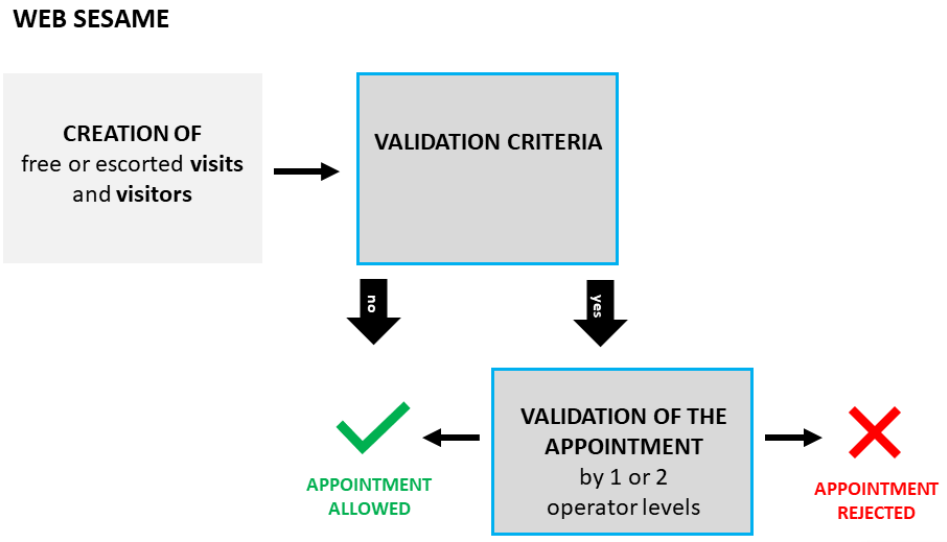
- For the expected visitor who scans his QR code received by email
- For the unannounced visitor who creates his card and his request for a visit

There is a specific document on visitor management that is available from your usual TIL contact.

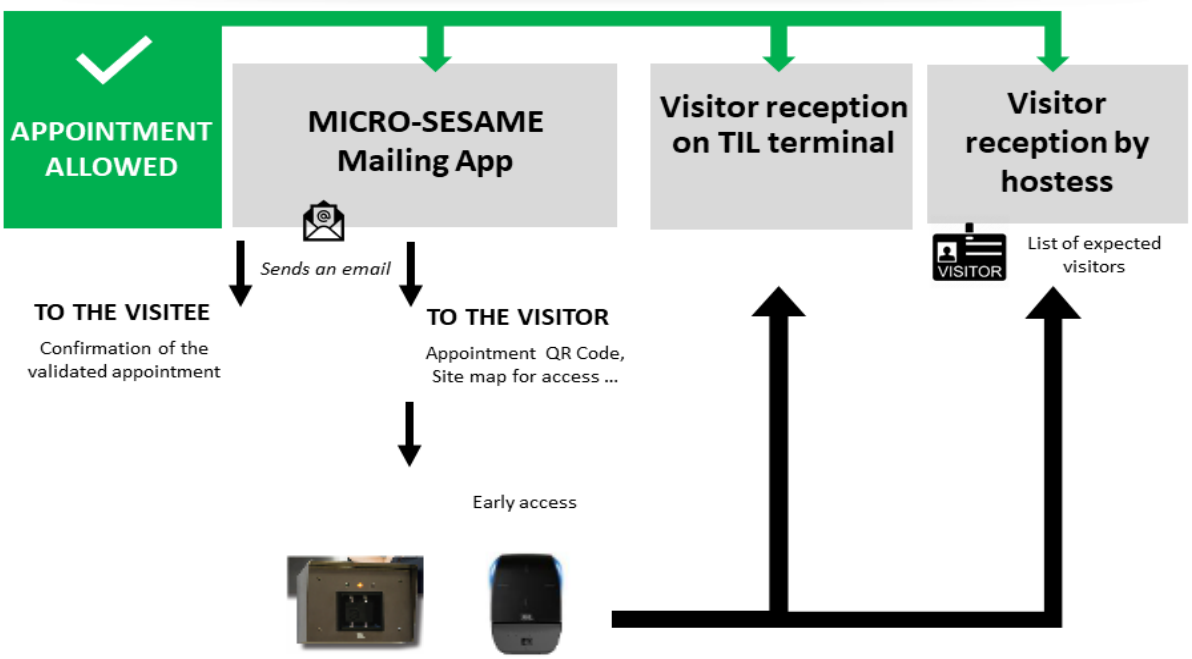
SIMPLIFIED VISITOR MANAGEMENT WORKFLOW



VISITOR MANAGEMENT WORKFLOW



If an appointment is accepted:



This solution offers many advantages:

- Managing visitors via a complete workflow with a built-in access management
- Optimizing, streamlining, securing visitor reception and access to sites
- Offering free or escorted visits, registering unexpected appointments
- Validating appointments according to client specific customizable criteria:
    - Automatic email notifications with attached ICS file to guests, visitors and accompanying persons to record appointments in Outlook with 1 click
- Allowing early access for visitors (Parking lot access...)
- Creating visits by authorised employee from their office computers

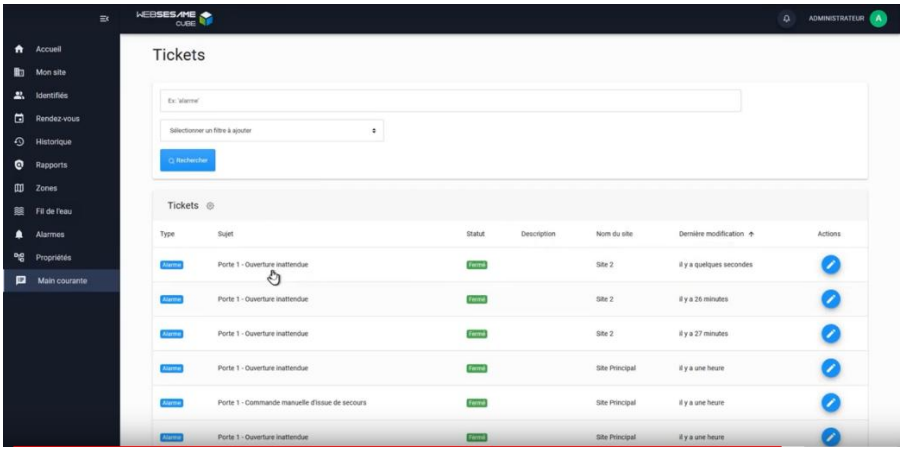
- Comply with ANSSI requirements
- Offering 2 types of visitor reception (Receptionist and/or terminal based hosting), dealing with 2 different types of issues: Security & Cost.
- Edition of custom visitor badges (customer graphic chart, name, colour codes, ...)
- Enable unannounced appointments to be created

WEBSESAME displays two icons for visitor management: "Visitors" and "Appointments"

VISITOR MANAGEMENT will allow you to enter any necessary information in order to register visitors that have site access granted (alone or escorted visitors). The designation of the mandatory fields to be entered by users can be set by **MICROSESAME** operators. Access management features are voluntarily limited, compared to a **MICROSESAME** heavy client. The proposed features are exclusive of the visitor management functions and the staff that will be using this interface (staff other than reception and security):

- Access profiles among those allowed for visitors
- Assigning a free ID (badge) among those created for visitors
- Validity, Anti-pass back, master-key access, blacklist...
- The visitor "status" can be made visible only to specific operators.

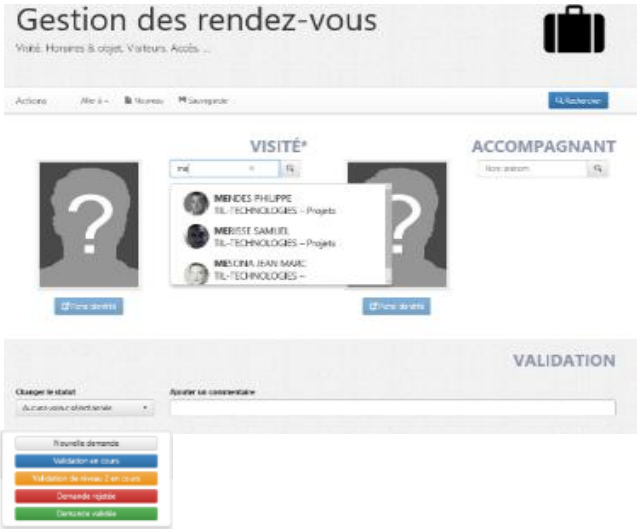
This allows to create limited access rights for a given period



THE APPOINTMENT MANAGEMENT feature allows you to search and create appointments with:

- The employee, to be chosen among those authorised having a "visit able" status
- Dates, times, and additional information (reasons for appointments...)
- Visitor(s) selected following searches, to avoid duplicates, or failing that, by creating new visitors directly in a simplified pop-up.
- Assigning access profiles, among visitor-authorised profiles and profiles assigned to the operator (multiple site management, classification management)
- A visit location can be chosen from a dropdown list and entered for multiple site projects. Email notifications can be sent to the visit validators in the sites concerned.

- Assigning early access will allow your visitors to join the reception from the site car park using QR code readers. A QR code (or PIN) is sent by email to the appointment visitor
- The possible escort can be chosen among the possible escort users. In this case, the access will require a double swipe: a first badge swipe by the visitor, a second badge swipe by anyone having the escort status. Both badge swipes must happen during a given period. Both visitor and escort must have the necessary access profiles and be granted access.
- Annotation of specific instructions



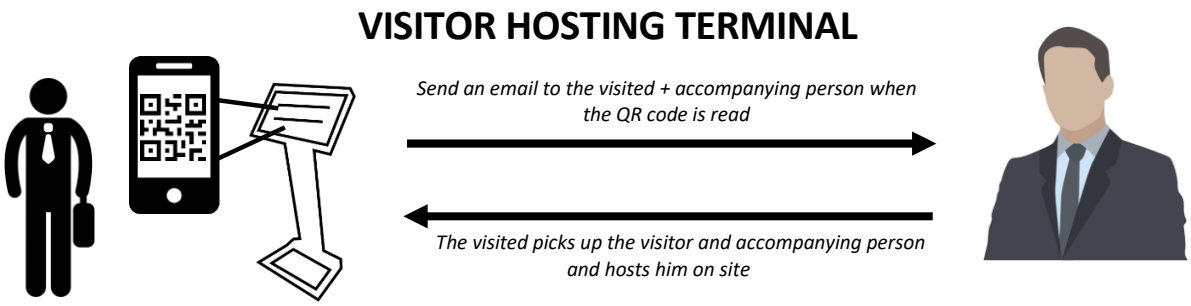
THE APPOINTMENT VALIDATION FEATURE is also available in this interface if the company internal processes require approval by one or two third parties (security officer, service manager, etc.):

- It is possible to manage up to 2 levels of validation (1 & 2 level operators)
- The criteria for validating each appointment, which will validate it automatically or by one or two operators, are configurable for each final customer by requests based on data related to the applicant (service, status...), to the visit (date, location...) or visitors (nationality, society...)
- Customizable email notifications can be sent automatically to the people concerned (visitor, visit, validator) to inform them of the validation process and the status of the visit (pending validation, to be validated, accepted, refused...).

Once the appointment has been validated (automatically or by operator), the visit is no longer editable. However, it is possible to duplicate a validated appointment.

VISITOR RECEPTION

VISITOR HOSTING WORKFLOW FOR TERMINALS:



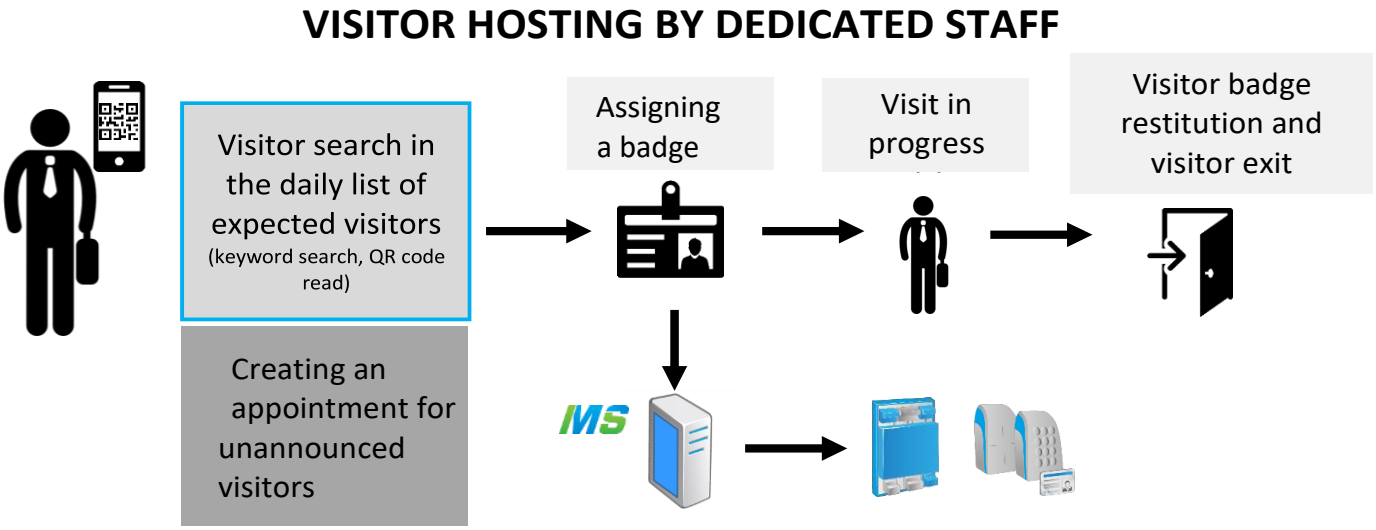
Touch terminal with built-in QR code scanner with 2 choices on home screen:

1. An option for the expected visitor who scans his QR code
2. An option for the unannounced visitor who creates his card and his request for a visit

This terminal based visitor reception solution offers specific advantages:

- Easy management of visitor hosting with a lighter workflow
- Costs-savvy solution (reception staff, visitor badges, etc.)
- Visitee escort the visitors. visitee are the only ones to have a badge and an access right
- Keep track of visits and site entries with the MICROSESAME history log

VISITOR HOSTING WORKFLOW FOR RECEPTIONISTS:



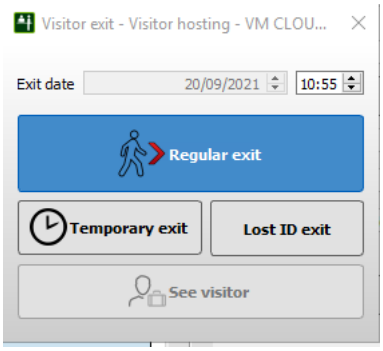
SOLUTION ADVANTAGES:

- Providing visitors with a badge and downloading access rights in less than 10 seconds.
- Listing and locating on-site visitors and check their status (pending, current, exit, ...).
- Keeping track of all visits and visitor movements with the **MICROSESAME** history log.
- Several exit types possible.

STAFF ADVANTAGES:

- Quick visitor search and processing.
  - Search by visitor name or visited name
  - Reading the visitor QR code, received by email using a reader
  - Possibility to create an appointment for an unannounced visit, if staff is authorised to
    - Specific visitor access profiles (visitor parking slots...).
    - Validity duration (going through several days and including temporary site exit)
    - With or without an escort by an authorised escort (double badge)
    - The ability to connect the OCR reader, to automatically reassemble information Identity cards and passports in the interface fields.
- Assigning a visitor badge available by swiping a badge on a table reader.
- Update the visitor status: Bring the visitor in or place the visitor on hold (The visitor is registered but waiting in the site reception).

- Several customizable documents can be created and printed for incoming visitors (business card, visit slip, site map, vehicle authorization coupon, with visitation pattern, name visited).
- Possible gateways with third-party applications (meetings, training, etc.) on visitors.
- Get a visitor out and finish a visit. After the visit, it is necessary to declare the exit of the visitor. Several types of outings are possible:
  - Regular exit: Closing the current visit. The visitor disappears from the list of registered visitors. The visitor badge is again available and reusable
  - Temporary exit: Once the visitor has temporarily left the site, access is disabled. The visitor must be re-registered upon his return on site.
  - Lost badge and exit: The visitor completes the visit on site, but his badge is not returned (or broken). The current visit is closed. The visitor disappears from the list of registered visitors. The unreturned badge can no longer be reassigned.



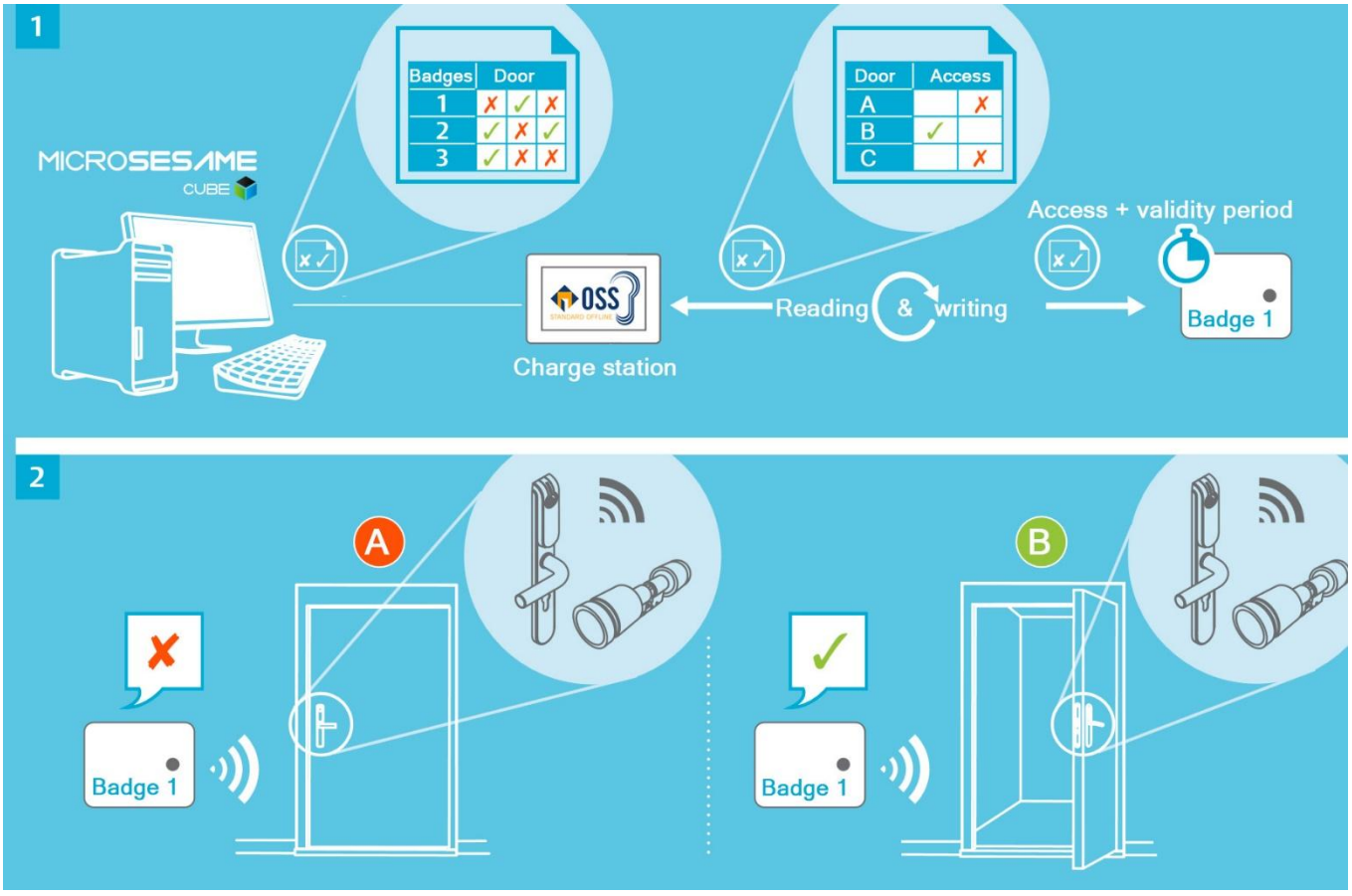
- ► Possibility to use readers managing automatic exit (Badge Swallowing Readers). No need to go through the site reception to exit the site.
- ► View a list of visitors and their different statuses.
  - Expected visitors: the visitor is pre-registered and has not yet shown up at the visitor reception
  - Visitors on standby
  - Visitors entered: the visitor is registered and entered on site and not yet released
  - Visitors having left the site
  - Outdated visit: When the scheduled end of the visit is exceeded, and if the visitor has not left the site, an alarm appears, and an icon signals it.
- ► Edition of visit history or visitor lists (expected, waiting, temporary outings...)
  printers or file exports in EXCEL-compatible files.
- ► Synchronization possible with Outlook calendars thanks to the I Calendar file (ICS) attached to the email sent to the visitors.
- ► Purge visitors that did not show up for scheduled appointments.

11. "OFFLINE" ACCESS CONTROL

MANAGEMENT OF AUTONOMOUS MECATRONIC CYLINDERS AND STRUTS TO THE OFFLINE OSS STANDARD

MICROSESAME natively manages "offline" access rights, i.e. on autonomous mechatronic equipment (cylinders, levers, handles,…), not connected to the system in real time.
MICROSESAME handle access rights who are encoded directly in the user badges, for a defined validity period (preferably short).

Mechatronic locks incorporate intelligence and data (access group, clock, etc.) and unlock when the badge's access rights are recognised and validated by the lock.



Periodic reloading of rights in user badges can be carried out:

- ► Via badge encoders connected to MICROSESAME (PRIME/HIGH SECURE): initial encoding and reloading.

- On rights loading terminals (all ranges): initial encoding and reloading.
- Via the site's wired readers (all ranges), if they are compatible and connected to dedicated MLP2-OSS modules: reloading of rights only.

For the operator, the allocation of rights to these unconnected accesses is completely transparent, through the same "User/ID" interface that also manages connected readers.
The system flexibility avoids having two interfaces or having two databases interacting. It also allows these stand-alone accesses, like any reader on the site, to benefit from **MICROSESAME** features related to multi-site management and the allocation of access profiles.

The centralised management of autonomous mechatronic elements is also beneficial for information sharing. Indeed, with each ID passage of a user on a charging station, the following elements will be sent to **MICROSESAME**:

- Passage history log.
- Low battery alarms.

The OSS (Open Security Standards Association) offline standard and its advantages:

- Created by an association of mechatronics manufacturers:
  - ASSA ABLOY, DEISTER, UZ, DORMA KABA, Zugang GmbH...
- The data written to the badges (access rights, etc.) is common to all manufacturers who comply with the OSS offline standard.
- OSS-compatible locks from different brands can read data and access rights from badges in the same way. The end customer is free to choose the lock manufacturer.

A more comprehensive PPT is available from your sales representative, along with product sheets for the OSS Offline terminal and the MLP2-OSS updater module.

12. “CLIQ” OFFLINE ACCESS CONTROL

CYLINDERS AND ELECTRONIC KEYS MANAGEMENT

MICROSESAME has a built-in connector for interfacing with ASSA ABLOY's CLIQ electronic key management technology.

With this "Offline" access control system, user rights are stored in an "active" key. Unlike Offline OSS solutions, the locking cylinders into which CLIQ keys are inserted require no power supply or battery. It is the key that contains the energy needed to check that the embedded rights correspond to the door being used or the lock to be opened.

As with any offline system, updating the rights of identifiers in their key requires occasional updating operations:

- Either by walking past a CLIQ recharging point.
- Or via their smartphone, using the CLIQ CONNECT mobile application.

MICROSESAME is easy to integrate and can be set up in just 5 minutes by importing keys, cylinders and terminals from the CLIQ WEB MANAGER software:

- CLIQ keys are imported as identifiers into **MICROSESAME**.
- Cylinders and cylinder groups are imported as items assignable as accesses.
- Access rights are assigned to these cylinders and groups of cylinders in the same way as for conventional readers: in the "Identified" and "Access profiles" interfaces of **MICROSESAME** and **WEBSAME**.
- The charging point is a supervisable element. A "supervision object" is available with connection and fault properties.

13. BADGE ENCODING

ELECTRICAL CUSTOMISATION

Electrical badge customisation (MS-ENCODBADGE) is a **MICROSESAME** software option allowing data to be written in the Mifare family of badges.

The software manages the encoding of most formats: Mifare Classic, Mifare Desfire EV1, defining the location (e.g. Mifare Classic sector, Mifare Desfire applications and files) and the format of users (decimal, hexadecimal, alphanumeric...).

Several applications with multiple IDs can be encoded at once.

The identifier can be generated by **MICROSESAME** or provided by a third-party application.

Physical encoding can be done individually or by set of badges, on a table encoder or directly in a badge printer with a built-in encoding device. In this case, it is possible to perform simultaneously, automatically for a population of people:

- Graphic customisation
- Multi-application encoding
- Enlisting each badge to the associated person.

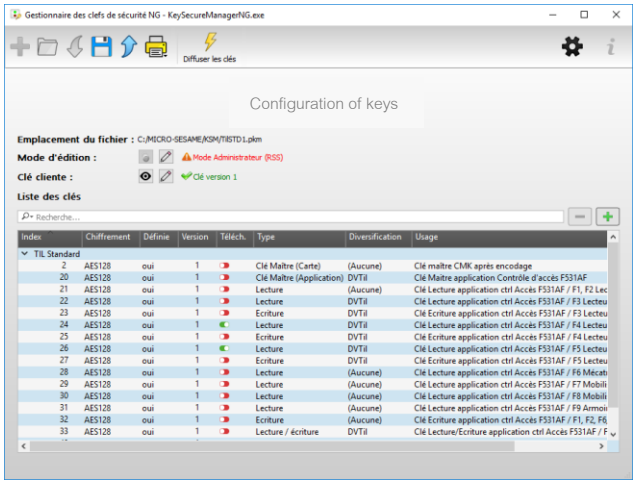
This solution offers: speed, simplicity, security

BADGE KEY MANAGEMENT WITH KSM

The KEY SECURE MANAGER software manages the badge security keys. It allows secure encoding and fully tailor-made encoding for the end customer:

- Configuration of keys (depending on the size and types of keys used) of the badges.
- Generating keys and backup files
- Generating the file associated with MS-ENCODBADGE for encoding or enrolment of the badge on the transparent reader of a **MICROSESAME** client station

There is more detailed dedicated KSM NG documentation.



14. BADGE CUSTOMISATION

Badge customisation is a basic built-in function in **MICROSESAME** that allows graphic creation (custom text based on data from the user cards, fixed text, logo, photo, pictograms, QR code, etc.) and thermal printing.

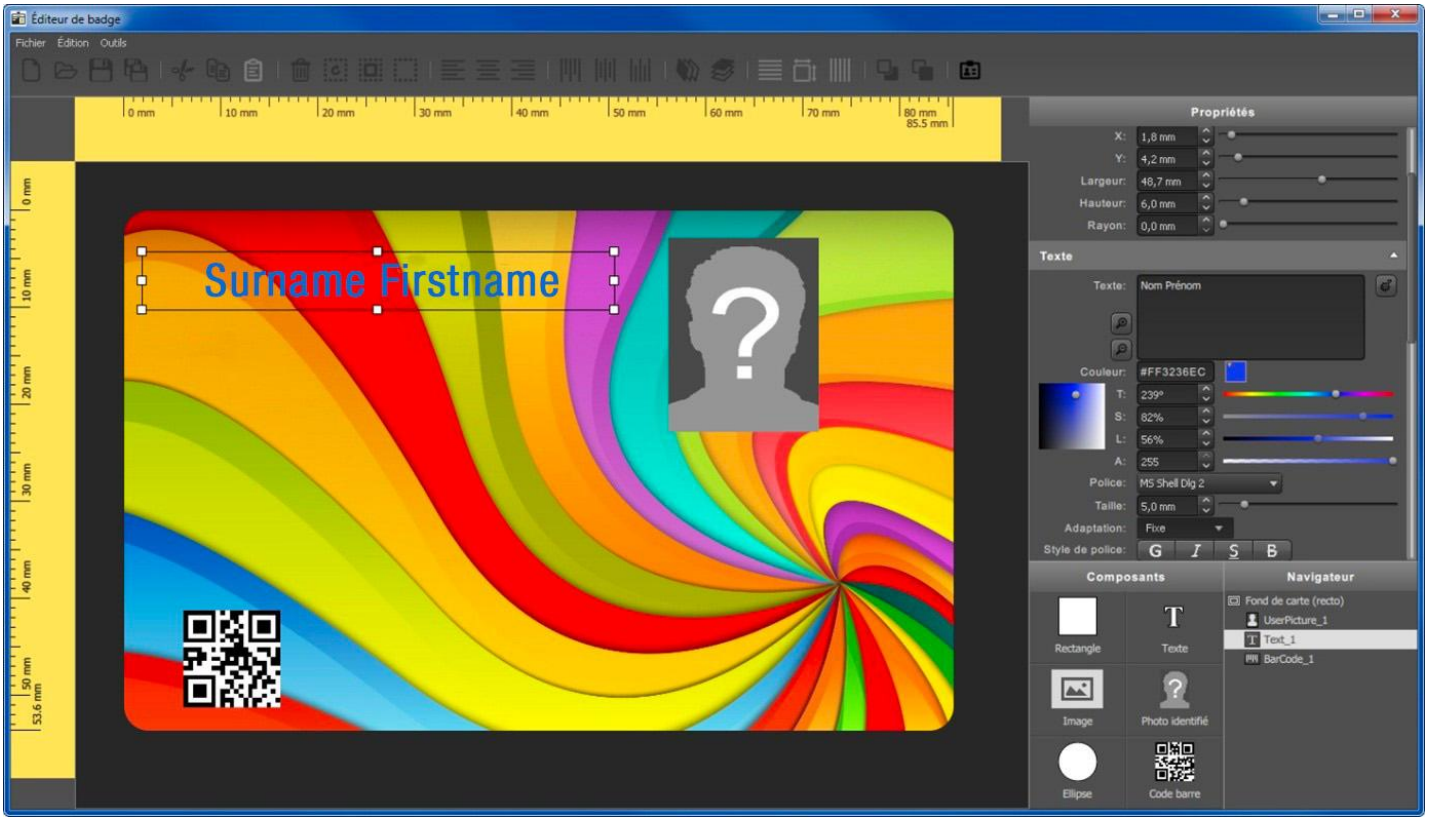
It is possible to store for each person a photo from an existing file, a scanner, a video source or any Webcam.

The graphic editor in **MICROSESAME** allows to create the card funds on a single or double-sided, and to set up different labels to print (name, service, empowerment...). This printed data can be written with all international alphabets including Arabic alphabets.

For example, pictograms symbolizing the different authorizations the user has can be added to the print Such symbols are specific to the card holder (electric clearance, dangerous atmosphere permit...)

The badge background editor allows you to export badge backgrounds that have already been created to import and reuse them on other sites of the same client, for example.

The solution allows you to create different badge backgrounds (permanent, temporary, visitor...) and assign the right format to the right person before serial printing.

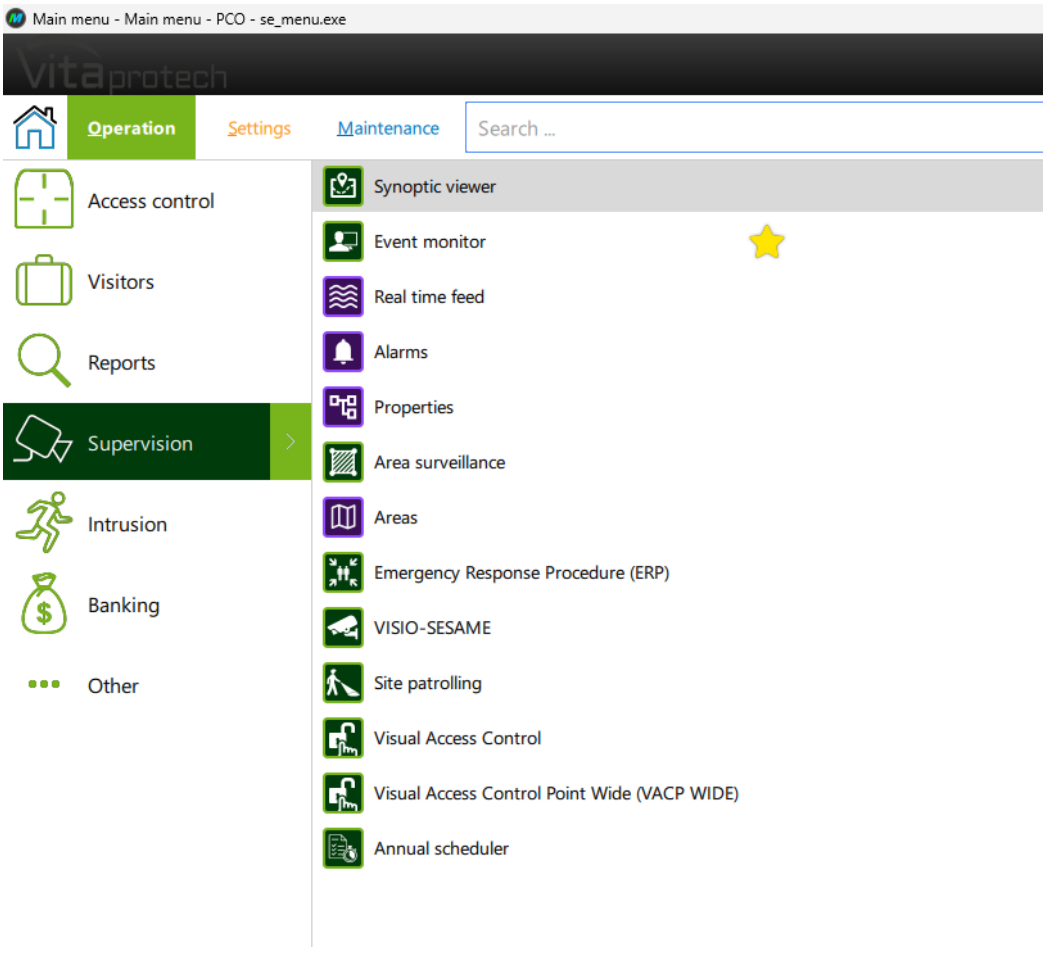


15. MONITORING & SUPERVISION

REAL-TIME EVENT MONITOR, SYNOPTIC GRAPHS, AREA MONITORING

MICROSESAME allows monitoring of events, alarms, access control defaults, intrusion, system, technical management and launch related actions (payment, various orders, viewing video streams, ...) through these functions:

- Synoptic graph viewing tool.
- Event and alarm monitor.
- Area monitoring.
- Contingency plan, mustering areas (see dedicated chapter).



GENERAL ERGONOMICS

- Interface ergonomics offer easy, fast operation with:
  - A single unified interface managing all the safety features.
  - The operator does not see the functions or the data that is forbidden to him.
  - Multilanguage management.
  - Each interface is dedicated to certain functions (users, mustering, monitor, synoptic graphs, ...).
  - Functions used by a large population are accessible on WEB (Appointments ...).
  - Separate navigation and colour from apps: Operation – Settings – Maintenance.
  - A Menu search field makes it easy to find available features.

  View of the connected operator on the top bar.
- Favourites, shortcuts and list of the latest apps opened in the main menu for quick access to current features.

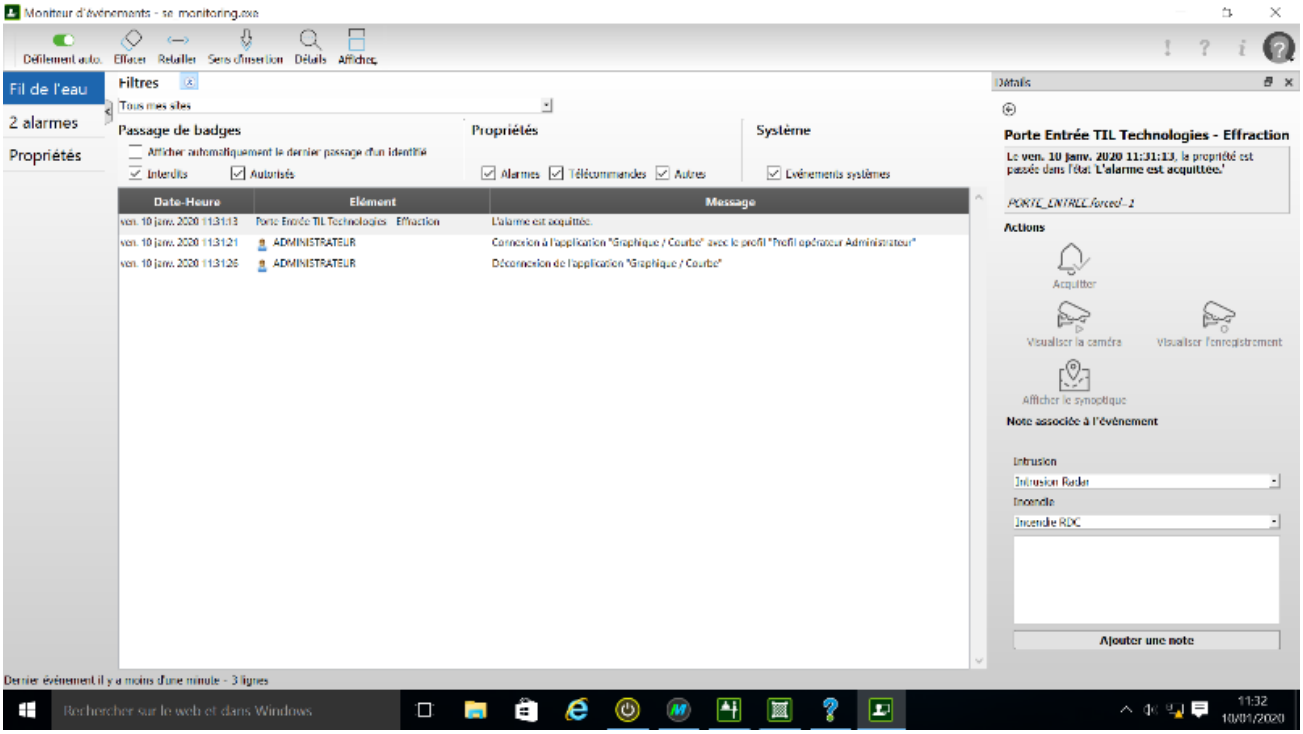
- Self-completion suggestions allowing the user to limit the amount of information he enters with his keyboard, by being offered a suggestion that might suit the string of characters he has started typing.
- Checking the consistency of the data being written by the input field.
- Operator error notifications.
- Most of the form results can be customised:
  - Selecting the fields and the data you want on display
  - Backing up their position
  - Possible change by the operator at any time

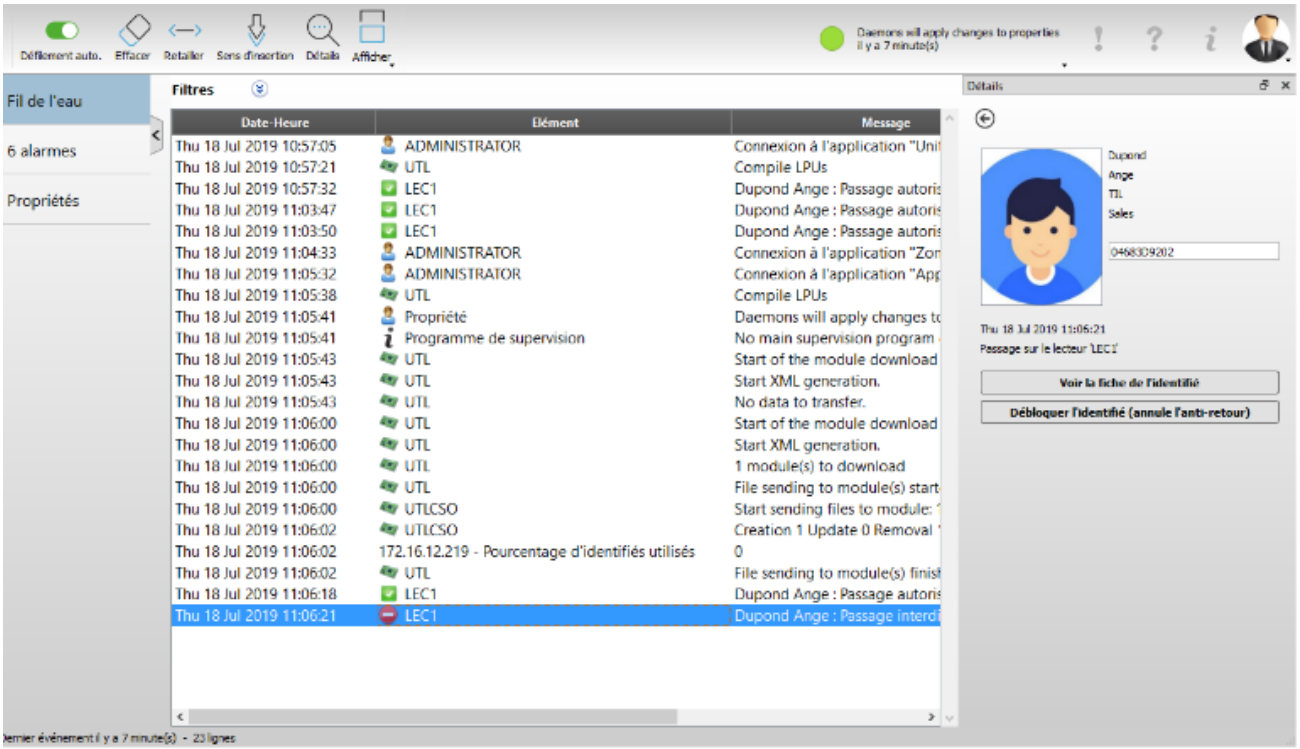
INTERACTIVE EVENT MONITOR, ALARMS

The Interactive Event Monitor centralizes the monitoring of all events, alarms and defaults received by **MICROSESAME**, displays them in real time, and allows to acknowledge the alarms, launch actions and remote controls, force the status of the properties...

Each operator only sees its authorised sites, event categories, ... In any case, all appearances, acknowledgment and alarm removals are time-stamped and archived in the database (see History log and Operators for further details).

REAL TIME EVENTS TAB:





REAL TIME EVENTS:

The "Real time events" tab displays all events in chronological order.

It is possible to disable the automatic scrolling of events to give the user the time to view all the events that occurred before and after the concerned item.

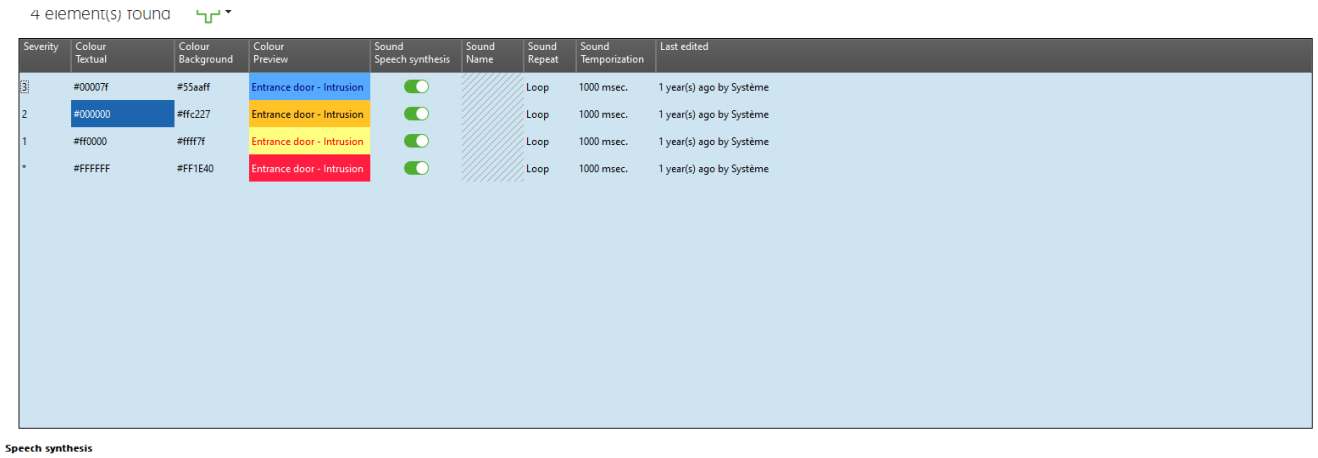
Whether the event list is important or not, it is always possible to use a dynamic filter according to:

- The site (for multiple site management).
- The type of events (passage is granted or forbidden, alarms, remote controls, system, the last user passage).
- A keyword in quick search (name....).

"DETAILS":

When selecting an event displayed in the water wire, the "Details" area allows you to view additional information about the event and see the associated available actions:

- Acknowledge an alarm: Il will make it possible to ensure that the operator has taken the alarm into account. The obligation to acknowledge an alarm can be set for each type of event in alarm.
  - Single/multiple alarm acknowledgement by 1 or X operators according to alarm categories (AC, IA, ...) and their acknowledgement mask level. An alarm may need to be acknowledged by several operators.
  - Alarms to be acknowledged can be set to blink.
- Read a statement.
- View the live camera.
- View recording of a video sequence of the alarm or badge swipe.
- View the synoptic graph associated to an alarm.
- Upon passing a badge, quickly access the information of the user by opening his card and unlock the exit temporarily in case of anti-pass back/anti-return alarm.
- On value change: know the status, force the status, launch a remote control ...
- Viewing the photo associated with the latest passage.
- Open the notes interface (free or related to an event).



Alarms can have a severity level from 0 (least important) to 512 (highest).

The alarm colour codes are:

- Red background colour and white text: ongoing unacknowledged alarm (Default colour, and customizable). These alarms can be distinguished based on their severity level of 0 which is customizable by:
  - Text colours and background of text to choose from and/or
  - Audio, sounds of your choice (Windows voice synthesis, audio file)
- White background colour and black text: An unacknowledgeable alarm in progress.
- White background colour and red text: Acknowledged alarm that is still in progress.

THE ALARMS TAB:

Provides an exhaustive view of ongoing or undischarged alarms. The alarms that have been paid and which are no longer in progress are disappearing.

The alarms are first sorted in order of gravity. Most of the actions available are also available in this view with:

- View an alarm history graph (see Charts).
- Quick access to the alarm property settings.

THE PROPERTIES TAB:

Allows you to monitor, search for different types of properties, monitor their status notifications (when an open door is detected, for example), edit them and interact with them.

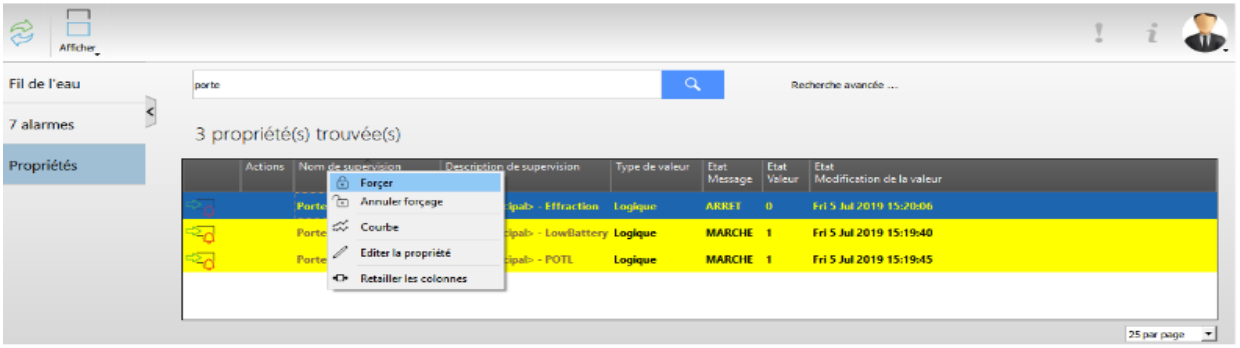
An object represents an item installed on site that generates information (e.g. a door).

Supervision properties have different status, remote controls that apply to the same object and that allow the object to be controlled via MICROSESAME.

This view is useful to the operator but also to the integrator when setting a site because it can diagnose its installation (executing remote controls, checking status, executing another remote control, open a synoptic graph...).

Possible property actions according to their types:

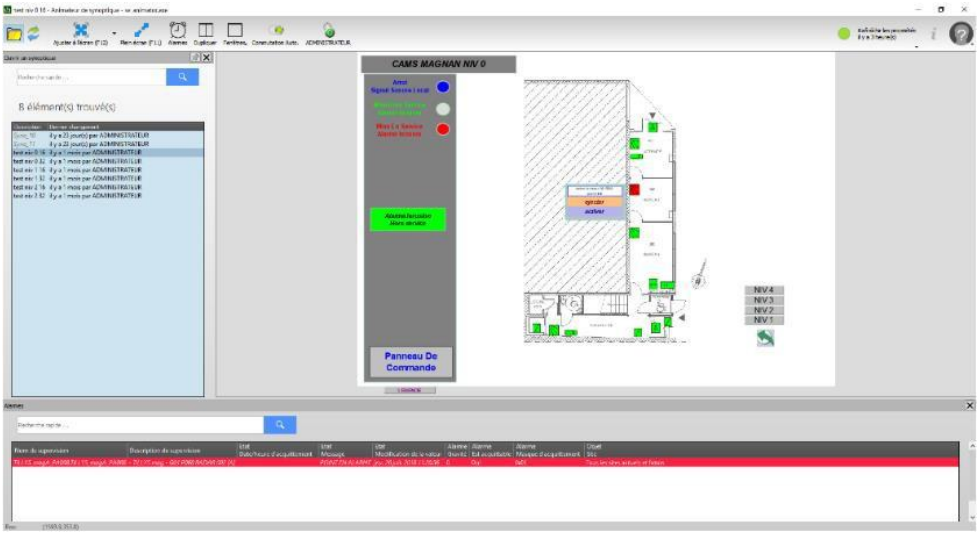
- Force: inhibits properties, for example temporarily in case of maintenance, detector default...
- Send an order or pulse
- View the associated curve
- See the associated synoptic
- Edit the property



Properties can be displayed in different colours: Yellow background brown text if the property was forced.

SYNOPTIC GRAPH VIEWER

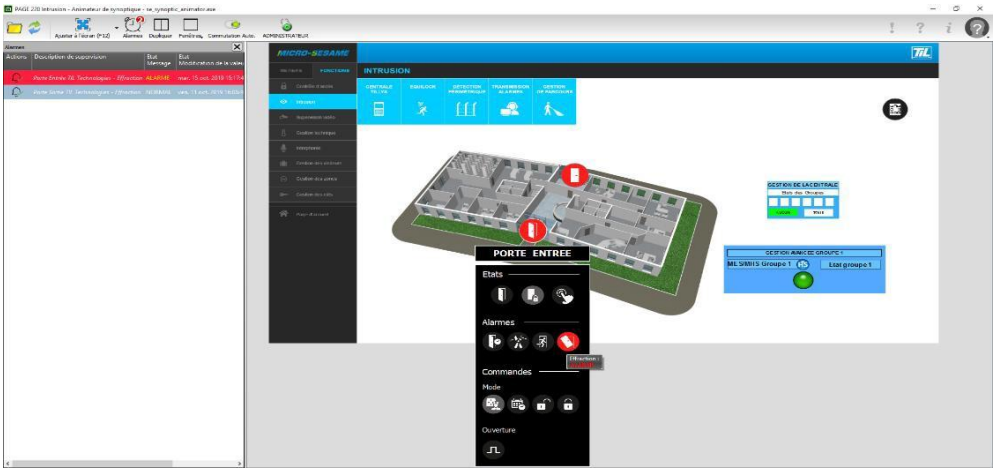
The **MICROSESAME** synoptic graph viewer allows you to customise the interface according to the sites for monitoring (viewing alarms, logical status and numerical values) and quick operator action (processing alarms in accordance with instructions, launching remote controls, actions). A synoptic graph is a representation of the installation to be monitored and consists of a set of graphic objects on backgrounds.



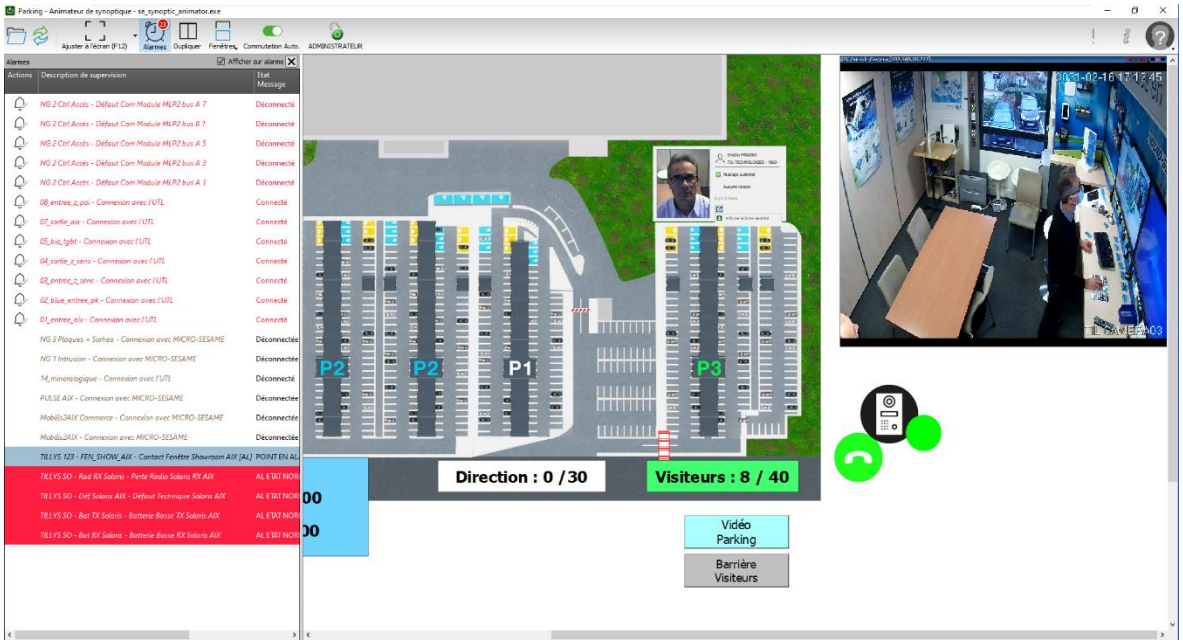
Features associated with synoptic graphs include:

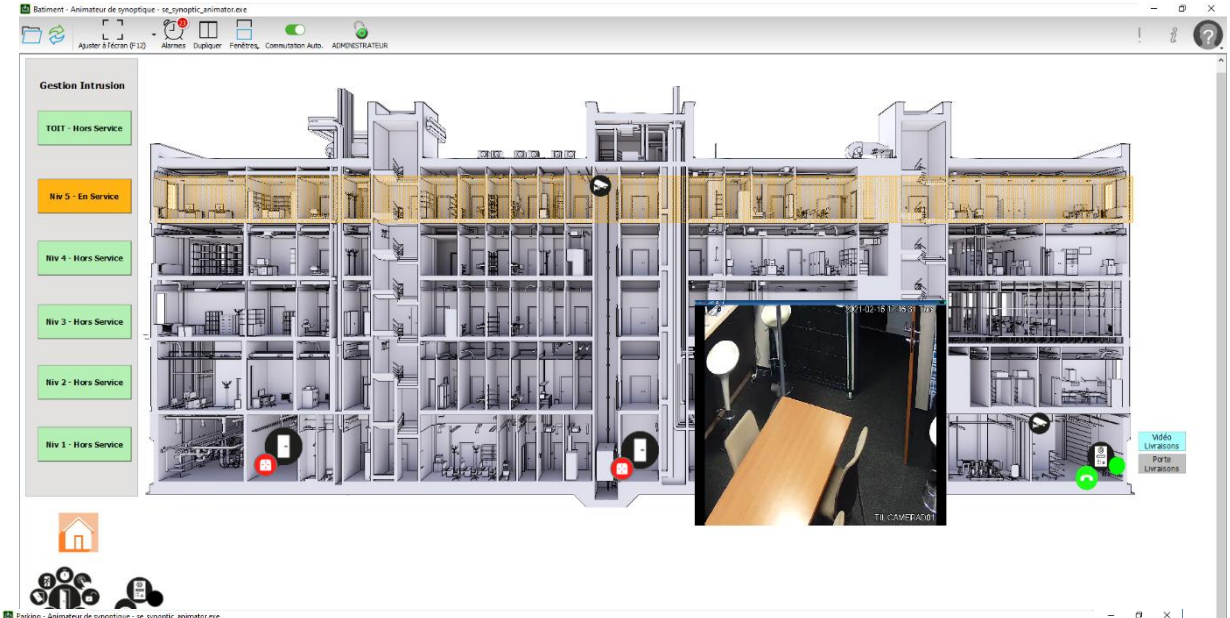
NATIVE EDITOR & ANIMATOR OF SYNOPTIC GRAPHS, WITH FAST SETUP AND HIGHLY CUSTOMISABLE:

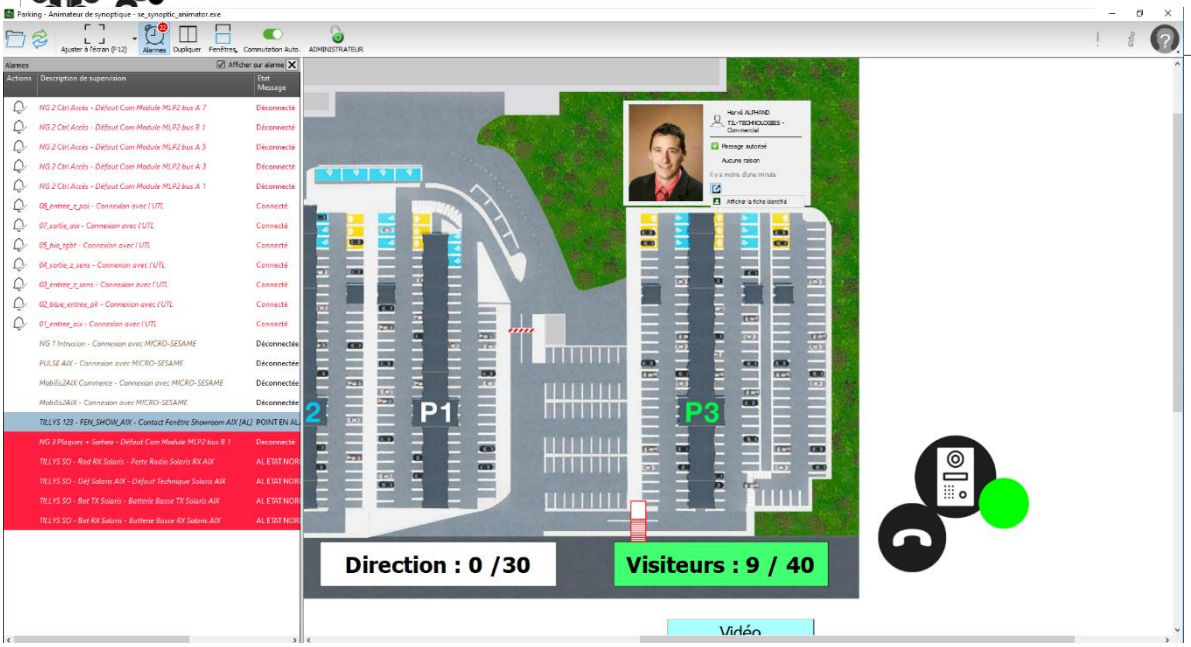
- ► The concept of objects having their own properties (information, status, commands)
- ► A library of pre-defined object models, delivered with MICROSESAME (LPU, doors, MAXIRIS, ...) that integrate the business and supervision configurations:
  - Easy to setup, by drag and dropping an object from an existing model
  - Automatically assigns automatisms, inputs, outputs to be wired according to a typical scheme with possible choices to be selected with just one click
  - The ability to change the image of the object by keeping the entire configuration
  - Ex with the "standard door" object: choice to activate as input: contact door, command, BBG contact, locked door contact
- ► The ability to create, import, copy custom objects/properties on a project
- ► The support of .SVG that facilitates the import and export of construction plans,
- ► Simulation is possible directly from the editor to get a preview,



- ► Animate objects according to the status of the equipment (colour, flashing, audio message...)
- ► Execute remote controls, operators run various actions from the objects, the buttons
- ► Browse from one graph to another
- ► Zoom in and out on a synoptic graph
- ► Quickly adjust the synoptic on the screen or switch to full-screen mode using any of the 2 shortcuts available
- ► Manage and supervise alarms directly from the synoptics graph through:
  - The ability to acknowledge the alarms
  - Opening the properties of an object
  - Viewing the corresponding graphs
  - A specific detachable window containing alarms with widget / counter and list of alarms (as from the event monitor) with different display colours depending on their condition and their acknowledge
  - Below are some examples of Widgets, objects (door, intercom, camera…) with photo and real time information of the badging people.


Parking - Animateur de synoptique - se_synoptic_animator.exe
Ajuster à l'écran (F12)
Alarmes
Dupliquer
Fenêtres
Commutation Auto.
ADMINISTRATEUR
Alarmes
Afficher sur alarme
Actions
Description de supervision
Etat Message
P2
P2
P1
P3
Direction : 0 /30
Visiteurs : 8 / 40
Vidéo Parking
Barrière Visiteurs


Batiment - Animateur de synoptique - se_synoptic_animator.exe
Ajuster à l'écran (F12)
Alarmes
Dupliquer
Fenêtres
Commutation Auto.
ADMINISTRATEUR
Gestion Intrusion
TOIT - Hors Service
Niv 5 - En Service
Niv 4 - Hors Service
Niv 3 - Hors Service
Niv 2 - Hors Service
Niv 1 - Hors Service
Vidéo Livraisons
Porte Livraisons


Parking - Animateur de synoptique - se_synoptic_animator.exe
Ajuster à l'écran (F12)
Alarmes
Dupliquer
Fenêtres
Commutation Auto.
ADMINISTRATEUR
Alarmes
Afficher sur alarme
Actions
Description de supervision
Etat Message
P1
P3
Direction : 0 /30
Visiteurs : 9 / 40
Vidéo

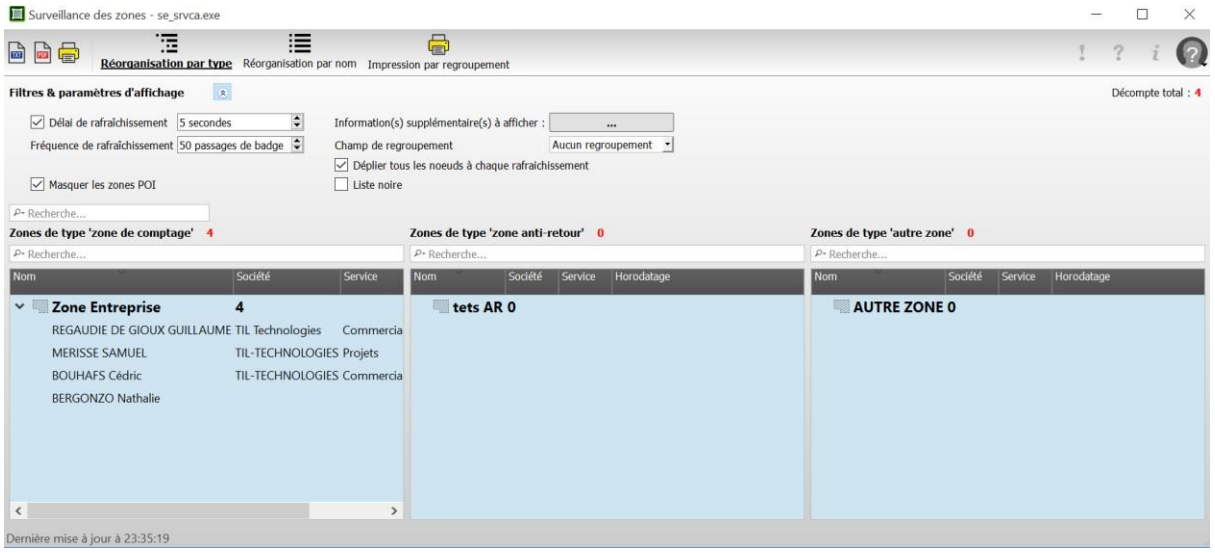
MONITORING AREAS

AN AREA IS A CLOSED ZONE (SUCH AS FLOORS, BUILDINGS...) AND MUST FOLLOW SPECIFIC RULES:

- It must have a group of entrance readers
- It must have a group of exit readers
- Physical tightness (wall) ensures that it functions properly, being impossible to enter or leave the area without being checked.
- A unique access pass mechanism is needed for effective counting

THERE ARE SEVERAL ZONES REQUIRING SPECIFIC MANAGEMENT:

- Counting (depending on the entrances and the exits) of the present users
- Anti-pass back (geographic or timed)
- Internal operating plan (see POI chapter)
- Other types of zones (e.g. to manage specific identifies such as those on the black list)



AREA SUPERVISION WITH A DEDICATED WINDOW:

- To list and count people in real time by area and type of area
- Print and export to TXT and pdf
- Offering different display settings

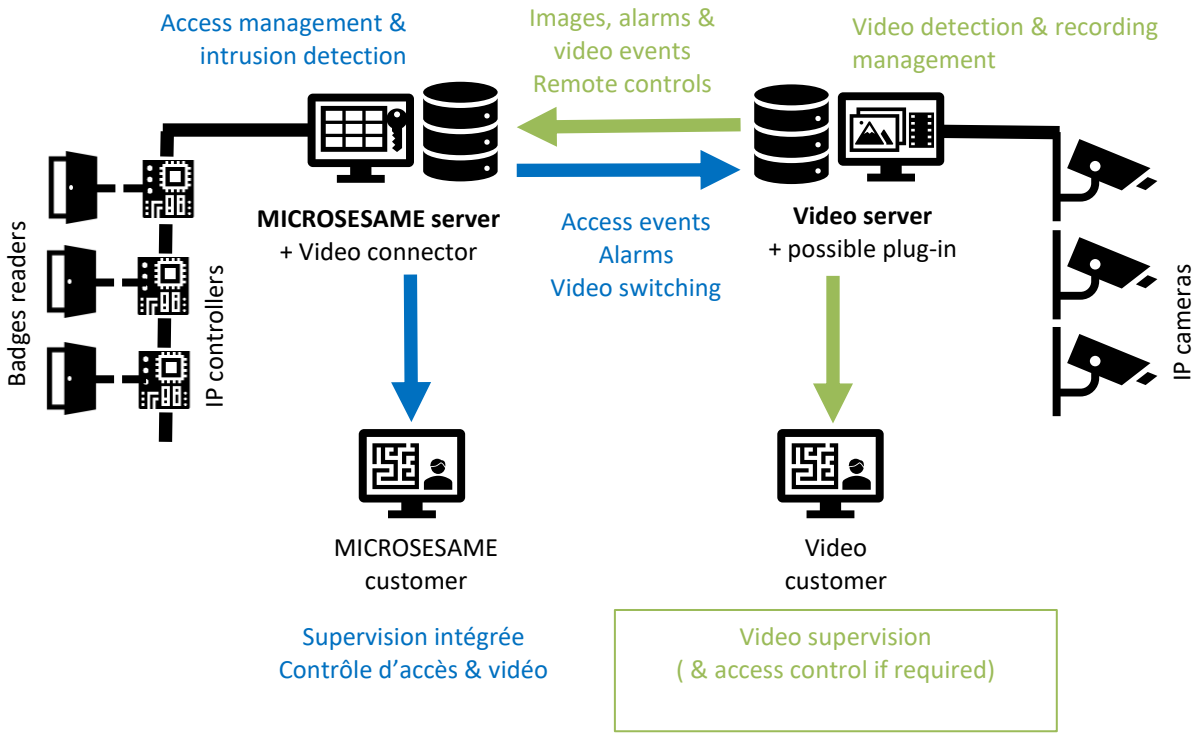
16. VIDEO SUPERVISION

VISIOSESAME

The software function of VISIOSESAME de MICROSESAME CUBE allows to:

- Communicate, in both directions, with many VMS, and digital video recorders of the market such as MILESTONE, GEUTEBRUCK, GENETEC, HIK, DAHUA, DIGIFORT, VIDEOWAVE with integrated connectors and optional in MICROSESAME CUBE.
- Pilot all security functions from a unique supervisor, common with all the building's systems (access control, intrusion, fire, technical management).
- Realise most of the usual operations of video surveillance from any **MICROSESAME** CUBE client station with one or many VMS at once:
  - Live visualisation
  - Recording
  - Events and alarms receipt
  - Recorded picture consulting
  - Dome control

With video integration in **MICROSESAME** CUBE, the operation becomes much simpler for the user. Interactions between video and other systems can be fully automated (actions on alarms or events), the speed and effectiveness of treatments are guaranteed. In order to keep it running smoothly, the customer position using **VISIOSESAME** must have two displays



TYPICAL DATA FLUX BETWEEN VMS AND MICROSESAME IS:

- CCTV camera detects images to be recorded.
- The digital recorder records the detected images.
- The **VISIOSESAME** client station directly checks real-time images or images recorded from the recorder, without going through the **MICROSESAME** server, depending on the setting in the **MICROSESAME** server accessed by the client station.
- Video images are not stored on the **MICROSESAME** stations but only on VMS recorders.

VISIOSESAME FEATURES ARE:

EVENTS, ALARMS WITH SEVERAL SIMULTANEOUS VMS:

- **MICROSESAME** -> VMS: trigger/stop recording, dome steering with preposition choice and zoom, ...
- VMS -> **MICROSESAME**: alarm detection, camera default, recording default, connected recorder, connected camera…

QUICK SETUP

for the video feature:

- **MICROSESAME'S** Integrated and optional connectors are using the SDK of the VMS and objects/properties of native TIL configuration for an easy and fast setup
- The notion of a "Camera" object in the synoptic editor
- The import of VMS camera labels

SUPERVISION OF OPERATIONAL ALARMS

(video activity detection) and operating alarms (loss of video signals or other outages) from recorders with event monitor, alarm blindfold, real-time

A dedicated HARWARE ARCHITECTURE interface that can be displayed on request

DOME CONTROL (zoom, preposition selection) through a dedicated window.

FULLY CUSTOMIZABLE CAMERA VISUALIZATION AREA according to pre-set scenarios that position one or more monitors in different positions and sizes (3 x 3, 2x 2...). It is possible to add as many monitors as sources. The colours of the monitor title bar provide information about its content and condition.

LIVE VIDEO STREAM VISUALIZATION (Live)

multiple VMS sets in parallel on selection of icons on operating synoptics, on alarms

TRIGGERING RECORDINGS

AUTOMATICALLY by event (badge passage on a given reader), an alarm, complex enslavement, a manual operator control from the synoptic by clicking a button or graphic object, a command from the Event Monitor.

IMAGE WALL (matrix) that manages a wall of images made up of multiple screens and displays a camera in an area (tile)

The SYNOPTIC GRAPHIC VIEWER allows, from a simple click on an object of a synoptic, to:

- Launch a view of one or more live cameras
- Watch a recorded sequence for a given source
- Automatically combine preset settings for display (selecting a group of monitors, selected preposition, video source...)

VIDEO ACTIONS
for an event or remote control by an operator. For example, automatic pre-positioning of a dome on forbidden badge detection.

VISUALISATION OF RECORDED VIDEO SEQUENCES
associated with an alarm directly from the "history" function in MICROSESAME which ensures the synchronization of information (single history file for access control, intrusion and video) and thus greatly facilitates the search for a video sequence. No need to know the source, the name of the camera, the time, a click on this video symbol associated with the alarm is enough and indicates that there is an associated video recording

A QUICK ACTION AREA, at the bottom of the screen, offers direct controls for actions such as: Captures of the current image, enable recording, Change the playback mode, direct/record, release a monitor, ...

VMS **MICROSESAME** INTERFACES VIA CONNECTORS

The list of solutions, compatible versions and accessible features is constantly evolving with integrated connectors and their products/properties; and the gateways interfaced in with **MICROSESAME**. There is a specific guide on **VISIOSESAME** available from your TIL contact that details the list of VMS and their functions compatible with **MICROSESAME**. According to VMS, not all versions of SDK are supported and not all features are available. Compatibility must be checked with TIL TECHNOLOGIES before any installation.

It is strongly advised to consult the requirements for video operating stations (screen surface, OS, graphics card, network card...) and for the network (debit, latency, ...) indicated by the manufacturer of the video recorder to which **VISIOSESAME** client workstations will have access.

As an indication, here is a list of VMS currently integrated or interfaced with **MICROSESAME**:

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

NB: A generic gateway ASCII with VMS exists in MICROSESAME CUBE (**LIC GENERIC** TEXT) option without **VISIOSESAME**, that means without a visual feed on MICROSESAME. It has been used with VIVOTECK, AVIGNONG ,ARGOS.

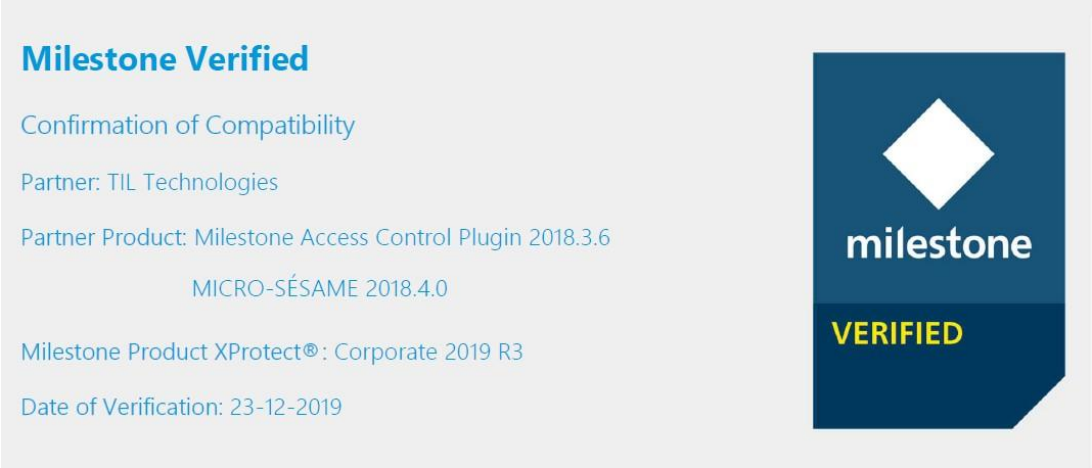
MILESTONE PLUG-IN

For customers mainly using video and want unified oversight, the **MICROSESAME CUBE** option **LIC-MILESTONE-PAC** integrates MILESTONE ACCESS CONTROL PLUG-IN to oversee TIL access control from the MILESTONE X-PROTECT supervision solution.

This interface, certified by MILESTONE, allows the VMS XPROTECT supervisor to:

- Manage TIL alarms (**MICROSESAME** -> X-PROTECT)
- Manage badge passages with Photos (**MICROSESAME** -> X-PROTECT)
- Launch remote controls to open managed access on **MICROSESAME**

  (**MICROSESAME**<- X-PROTECT)>



ACCES VISUAL CONTROL POINTS (PCVA)

On an access equipped with a badge reader and a video camera, the **MS-CVA** option enables the photo of the badge holder and the video image of the access to be displayed simultaneously when a person badges in. When the photo is superimposed, an icon indicates the status of the badge (authorised, forbidden, unknown).

An icon superimposed on the photo indicates the status of the badge (authorised, prohibited, unknown).

Opening the door can be manual or automatic or optional depending on the level of security. Other actions can be set up, such as turning on/off the lights, displaying a message, disabling the intrusion detection on the area...

17. INTRUSION MANAGEMENT

There are specific documents on intrusion management available from your usual TIL contact (Intrusion Setting Guide, Intrusion Detection Wiring Principle, Transmission Setting Guide, etc.)

THE NEW 2024 INTRSION CUBE

The new Intrusion Cube 2024 benefits from a major upgrade to adapt to new threats and heightened security requirements. This new version is based on four areas of improvement: cyber security, integration, ergonomics and functional power.

ENHANCED CYBER SECURITY

To guarantee optimum protection against cyber-attacks, Intrusion Cube adopts the same ANSSI-certified technical architecture as TIL access control. All communications are encrypted, and hardware and firmware are protected against sabotage. In addition, rigorous monitoring of CVE vulnerability patches is in place to ensure that security is always up to date.

MORE INTEGRATED SUPERVISION

Intrusion Cube facilitates system management by unifying intrusion operator profiles with access control rights. Equipment integration (detectors, groups of detectors, sirens) is simplified, and the system can be opened up to third-party applications via web services, reinforcing its interoperability with other security solutions.

OPTIMIZED ERGONOMICS

The user experience has been enhanced with the introduction of the new TACTILLYS-IP touchscreen, designed for simplified arming and operation. Monitoring is now more intuitive with animated widgets providing interactive visual control of ongoing events. Additionally, the event history is now better consolidated in **MICROSESAME**, ensuring improved traceability and more effective incident analysis.

ENHANCED FUNCTIONAL POWER

To meet the needs of large-scale infrastructures, the Intrusion Cube now supports multi-panel operation and handles both physical and virtual detectors. Alert transmission has been improved with the SIA DC-09 protocol, ensuring efficient communication with monitoring centers. Finally, new integrated testing and diagnostic tools simplify system maintenance and optimization.

With these advancements, the new Intrusion Cube 2024 stands out as a more efficient, intuitive, and secure intrusion detection solution, perfectly suited to today's security challenges.

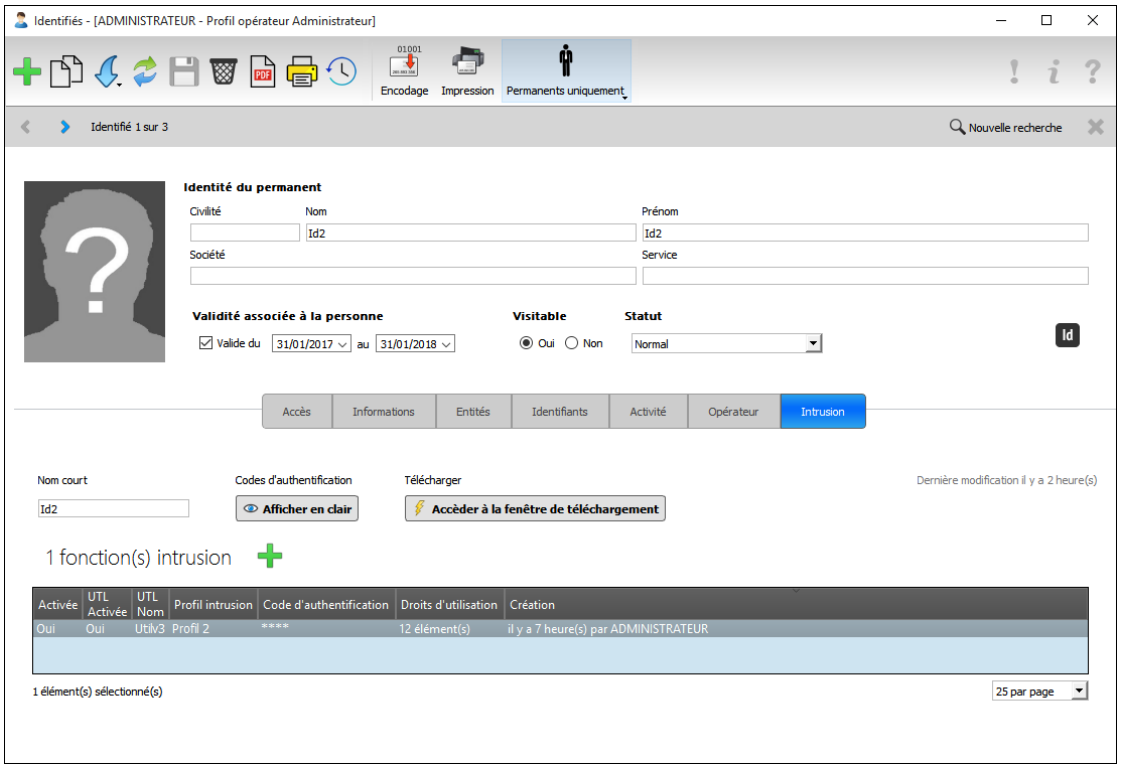
MICROSESAME NATIVE INTRUSION

THE MICROSESAME SERVER MANAGES THE USERS. INTRUSION RIGHTS ARE MANAGED IN A MULTIPLE CENTRAL WAY.

A user and his ID code are created only once for X centrals:

A "TILLYS USER" is a person authorised to identify himself on the intrusion keyboard of the **TILLYS** central. Each user is associated with an intrusion profile, usage rights and an intrusion ID code that is automatically generated. Intrusion profiles can be duplicated

USAGE RIGHTS: Usage rights are actions that a user can perform from the intrusion keyboard (access to the menu, decommissioning of a group, making a waiver... etc.). Each user can receive different rights



TILLYS Cube CENTRALS operate in standalone mode with their operating procedures having been previously configured and downloaded from **MICROSESAME**. Each **TILLYS UBE** has a capacity to:

- 32 Point/detector groups
- 624 detectors/points
- 150 local users
- 8 keyboard functions per bus, 16 siren functions
- An integrated IP transmitter "TIP" function

TACTILLYS CUBE INTRUSION KEYPADS

connected to the **TILLYS** RS485 bus, for autonomous local operation of an intruder control unit in just a few clicks. Each keyboard can be associated with a group list limiting the operating possibilities to a small part of the installation

- New modern and ergonomic keyboard with its 7-inch touchscreen, installation in Portrait or Landscape mode, its optional badge reader whose key security is ensured by an HSM EAL5+

ENTRANCE REMOTE MODULES connected to the buses of the TILLYS centrals, on which sensors, detectors and actuators (sirens, lighting control ...) are connected.

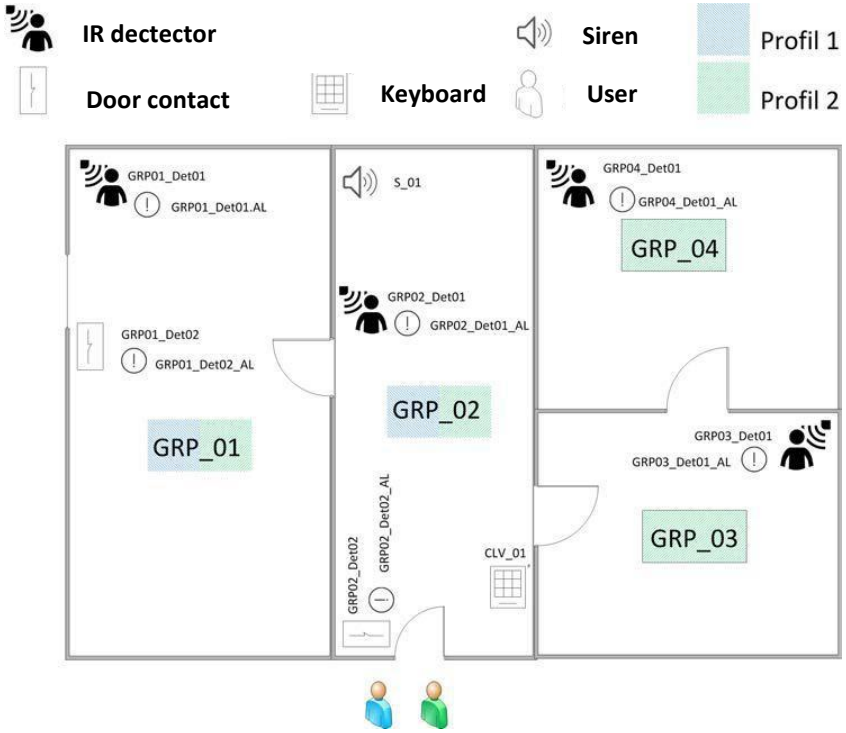
SPECIAL INTRUSION MODULES

High security **EQUILOCK** modules have 2 secure buses of 32 small transponders that can be addressed and integrated into the detectors.

THE SOLUTION OFFERS A GREAT FUNCTIONAL ADAPTABILITY, ESPECIALLY THANKS TO THE FOLLOWING FUNCTIONS:

- Each point/detector must be associated with a type of point that conditions the triggering of an alarm. Possible types are: intrusion alarms, 24/24 alarms, Silent Intrusion Alarm, Technical Alarm, Silent System Default, Emergency Call, Fire alarms
- Group of detectors defines a set of detectors, points related to each other (building, floor, service, perimetry, area, ...) and benefiting from a common management mode such as:
  - On/off-surveillance
  - Sending alarm codes to a remote monitor
  - Managing one or more sirens
  - Implementation of pre-alarm or derogation mechanisms

TACTILLYS CUBE keypad reader (2020)



E.g.:

Profile 1 can put the GRP_01 and GRP_02 in/out of service.

Profile 2 can put all groups in/out of service.

DISTURBANCE POINTS: A disturbance point is a point that would disturb the user in certain specific cases (e.g. during work, etc.).

EJECTION: A function to exclude a point from surveillance definitively or momentarily in order to allow the monitoring of a group to which it belongs and to avoid the systematic triggering of alarms or the action of the telemonitors especially if the point is, for example, in disturb or not significant. There are several modes of ejection (prohibited ejection, manual ejection, automatic ejection, automatic reinjection ejection, permanent ejection). A Re-injection action can stop the ejection of a point.

PRE-ALARM: corresponds to a timer that allows, via a siren action, to warn the occupants of the impending surveillance of the building while leaving them the possibility to restart a derogation.

DEROGATION: The function of pushing back an adjustable and explicit on-demand period of automatic commissioning on a trigger schedule. The request is possible from the keyboard intrusion by a TILLYS user or by Microcode or remote control from the supervisor **MICROSESAME**

COMMISSIONING WITH TRIGGER: Allows for automated launch of the monitoring of a group in the central (ex: time slots). Automated off-monitoring is possible but not recommended for obvious security reasons.

DELAY: A group of points can be timed for a time that can be set in or out to allow the keyboard to be reached when it is in a monitored area. The values of the timeout apply to the group and the fact of being timed in entry or/and exit is defined for the points concerned of the group.

SURVEILLANCE ON/OFF: The surveillance of one or more groups is the action of making operational the monitoring of intrusion alarm points associated with such group(s). The request for monitoring can be made in several ways:

- By user operation on a TACTILLYS CUBE intrusion keyboard
- Using time schedules
- By any other action, enslavements configured according to entrances, events, occupation (access control, intrusion, technique, fire centrals, ...)

ACKNOWLEDGMENT of an alarm point from the supervisor (see supervision).

INHIBITION of a point or group of points made temporarily inoperative from the supervisor (see supervision).

THE **TILLYS CUBE** CONTROL UNIT'S INTEGRATED IP "**TIP**" TRANSMITTER FUNCTION :

The **TILLYS CUBE** central incorporates an IP transmitter function ("**TIP**"). It allows the transmission of intrusion alarms, access control alarms and technical alarms to an IP remote monitor using the TIL "**TIP**" protocol, based on ID-Contact or CESA 200 standards, and qualified at ESI and Azur soft.

The main functions related to transmission offer great richness, functional adaptability:

THE CAPACITIES OF EACH LPU ARE:

- 4 recipients & potential users for receiving alarms (monitoring) and who will be able to setup the central.
- 8 call profiles for alarm transmission to define which recipient (s) to contact and in what order.
- 32 remote controls: actions that can be triggered by users

POLLING: Allows the recipient to periodically ask the central in order to detect if it is still present on the network.

CYCLIC TESTING: Transmission to a recipient is periodically performed in order to check the operation of the communication lines. Frequency is adjustable (precise time, related to the commissioning of one or more groups, different on the recipient)

CODING TABLE: A coding table is a table where we will set an event code for each type of alarm (intrusion, access, fire...) which will be sent to the remote monitor. These codes are therefore to be defined with the chosen remote monitor

SUPERVISING INTRUSION OF THIRD PRODUCTS:

Thanks to the gateways with intrusion automats (GALAXY NFA2P plant, SORHEA perimeter detection products with MAXIBUS protocol…), MICROSESAME allows alarms supervision. More information and examples in the dedicated chapter: GATEWAYS AND CONNECTORS, MONITORING AND SUPERVISION, VIDEO SUPERVISION

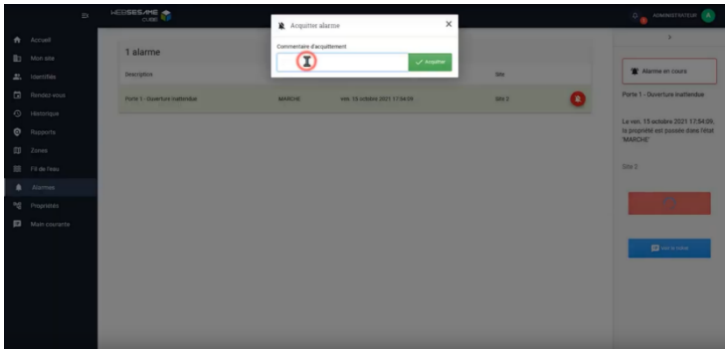
18. HANDRAIL

The activity-tracking function allows you to add comments at any stage in the processing of an alarm, whatever its nature (intrusion detection, unexpected door opening, etc.). It can be used in three ways:

- Directly when an alarm is acknowledged, either in the thick client interface or in the **WEBSESAME** interface.
- In the Event Monitor and Search History (fat client), by clicking on the alarms concerned.
- In a specific **WEBSESAME** tab, for tracking all the activity-tracking "tickets".

ALARM ACKNOWLEDGEMENTS

When an alarm is acknowledged, the operator can fill in an "acknowledgement comment" field next to the acknowledge button. This is the same principle in the thick client and in **WEBSESAME**.

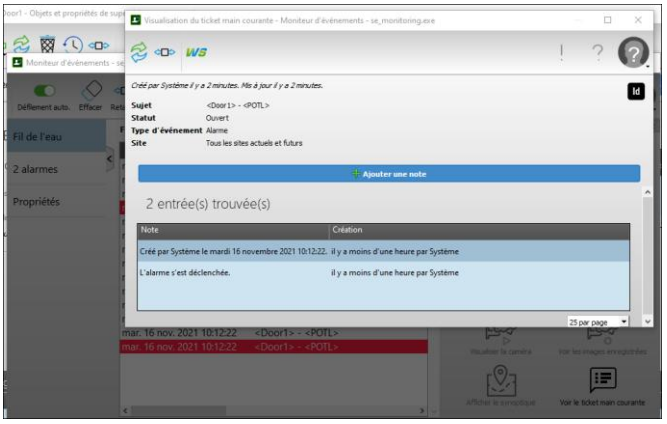


(Example of alarm processing in the WEBSESAME interface)

ACTIVITY-TRACKING TICKETS

In the Event Monitor or in the search history, by clicking on a selected alarm, all the comments can be viewed via a " activity-tracking ticket ".

This activity-tracking ticket chronologically presents all the events linked to the alarm (triggering, acknowledgement, shutdown) as well as all the comments entered by the operators.

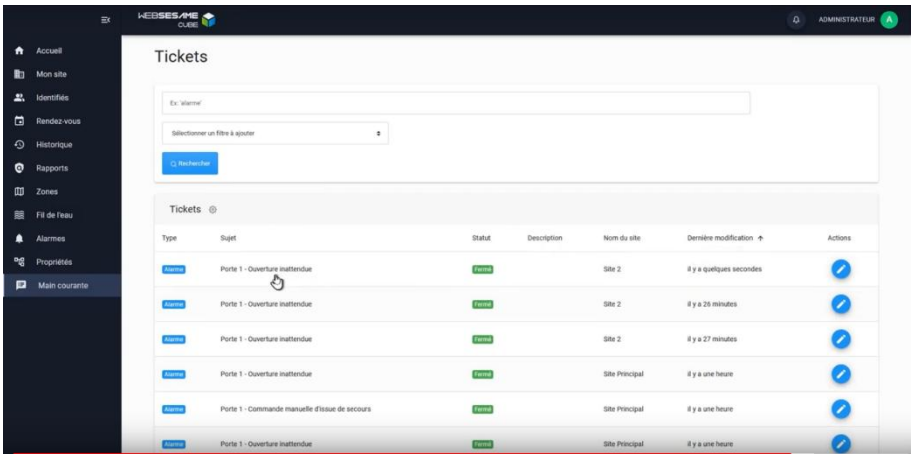


(Viewing a ticket from the event monitor)

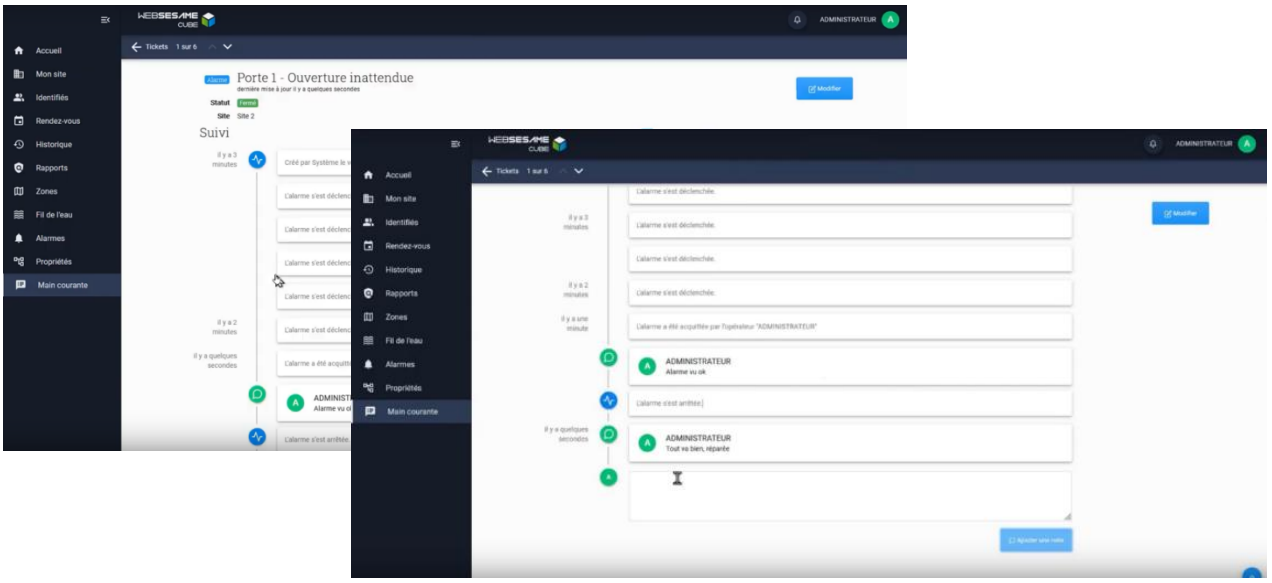
Each operator can enter as many new comments as necessary, if they wish to provide additional information or if the resolution of the event involved several stages (field inspection, informing the hierarchy, measures taken, etc.).

DEDICATED TAB IN WEBSESAME

In the **WEBSESAME** tab specific to the activity-tracking, all tickets linked to alarms are displayed in the form of a list. This list can be presented chronologically (last modification date) or sorted using other search filters (site name, alarm name, status, etc.). It can also be exported in CSV format.



As with a heavy client, each ticket can then be expanded to show the chronological tracking of actions and comments, and each operator can enter as many new comments as necessary.



Finally, and only in this web interface, it is possible to print out this chronological tracker on paper or in pdf format, to pass it on to a third party for example.

19. INTERPHONY

USIGN INTERCOMS WITH MICROSESAME

With the integration of intercom into **MICROSESAME**, communication functions are controlled from the same graphical interface as other building security systems (access control, video, Intrusion, BMS...).

Event actions can therefore be fully automated. Exploitation becomes a lot easier for the user and the speed of processing is guaranteed.

The examples are many:

- Intercom call can command video, for a more effective visual check and lighting as well or any other automatism.
- After the call, the door opening can turn off the intrusion surveillance.
- In the other way, the scan of an unauthorised badge on a reader can activate a pre-registered message on the intercom.

Finally, another advantage of this integration is that the intercom benefit from all the information function of **MICROSESAME**: mutualised history, advanced research, report editing for using analyse and statistic.

INTER-OPERATING WITH COMMEND SYSTEM

MICROSESAME allows communication with **COMMEND IP** (GE800, GE300, IS300, VIRTUOSIS). Intercom centrals are allowed from any **MICROSESAME** operating station:

- Total virtualization of the master station (with microphone and speakers plugged directly into the operating station)
- Display, status of intercom calls from subscribers to master station and status of subscribers (in communication, ...)
- 2-level differential processing: regular or emergency communication.
- Call processing, interruption or cancellation.
- Activation and deactivation of an intercom
- Visualisation of the connection status and the reason to the intercom server: energy issue, sabotage, short circuit…
- Establish and/or close a communication between 2 stations (direct button or keyboard of the virtual master station).
- Night transfer of calls from the master station to another station (e.g. day/night).
- Remote listening.
- Pre-registered audio message diffusion on the intercom COMMEND
- COMMEND relay control, on intercom or virtual (lighting…)
- Pressing a button on an COMMEND intercom, opens a door which is wired on an TIL automat

EASY INTEGRATION AND CONFIGURATION

NATIVE INTEGRATION WITH THE SPECIFIC “OBJECTS AND PROPERTIES”

The integration of COMMEND Intercom Servers has been designed to save time when setting up parameters thanks to the concept of “Server” and “Subscriber” objects.

All that is required Is to declare the intercom server and then import the list of subscribers already created by the COMMEND tools. The supervision elements are then automatically created in **MICROSESAME** for the server and the subscribers. **MICROSESAME** can connect to several COMMEND servers simultaneously.

Some specific functions are not natively integrated but are quite possible with additional configuration either on the **MICROSESAME** side or on the COMMEND server side. For example, the command to broadcast an evacuation message to all intercoms (instead of one by one).

GRAPHICAL SUPERVISION

For the graphical supervision, the objects include preconfigured symbols (images) for direct integration into **MICROSESAME** synoptic screens.

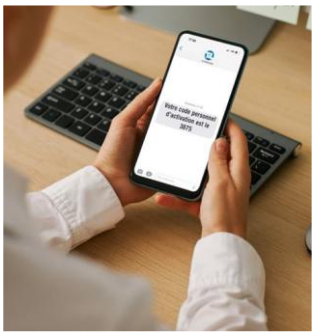
These symbols do not include all the properties of the objects, but they can be completed with the **MICROSESAME** versions. Of course, you can also customise your own intercom symbols and integrate the properties you want into the synoptic screens.

20. CARDIGO CUBE ON-BOARDING

CARDIGO enables the early distribution and circulation of new access control badges without any risk until their first actual use.

For users, company access is made easier, as their badge is issued in advance (for example, delivered to their home by mail).
For the Security department, since badges remain inactive until authenticated on a CARDIGO terminal, there is no longer a risk of misuse due to loss or third-party intermediaries.
To activate a badge in the system, each user authenticates independently using a personal code received separately from the badge.
Without geographic or time constraints, this solution is more convenient for the entire organization—no need to report to a specific security post or adhere to a set schedule.

ACTIVATION CODE PROCESS



- Generation of personal codes in an external CSV file for import into MICROSESAME
- Sending of personal codes separately from badge distribution
- Distribution method managed by the client (mail, email, or SMS)

BADGE/CODE MATCHING ON CARDIGO

- Badge scanning followed by entry of the personalized code
- Match found: The system activates the badge, and access rights are downloaded to the controllers
- No match: No owner information is displayed, and the badge remains inactive with no access

Discover all the badge functionalities available to users in the following video:
https://www.youtube.com/watch?v=8QPhHKuR38E

21. MOBILIS CUBE 2024 PORTABLE READER

NEW DATABASE SYNCHRONIZATION METHOD

- Up to 50,000 identities downloaded in under 10 minutes

SIMPLIFIED CONFIGURATION & DEPLOYMENT

- Checkpoint configuration profiles managed directly in MICROSESAME
- Operator-accessible functions and information on the terminal can now be assigned with greater precision

ENHANCED ERGONOMICS

- New simplified theme available for automatic access control: displays photo, ID, and a green or red background depending on the decision (in addition to the standard theme)
- Badge reading or, with a single click, QR code scanning

CYBERSECURITY & MILITARY-GRADE HARDENING

- Passwords stored with signed hashing & salting
- Automatic deletion of offline data from MOBILIS after a configurable number of hours of server disconnection or after multiple failed authentication attempts
- Encrypted SQLite database
- No badge key storage—only CSN reading
- Internal anti-time-back management within MOBILIS

Discover five real-world use cases in this video: https://youtu.be/VVrwGaqQwDg

This explanatory video presents the five main use cases for the advanced features of the MOBILIS CUBE:

1. Mobile access control
2. Emergency evacuation area headcount
3. Restricted area entry control
4. On-the-fly presence control by a security patrol
5. Replacing a wired reader for a temporarily open access point

22. KEY CABINET

MICROSESAME integrates connectors with ASSA ABLOY's TRAKA and DEISTER's PROXSAFE key cabinets. These connectors, subject to licence, enable the following operations to be carried out directly from a **MICROSESAME** client or server workstation:

- Assign access rights to keys/keytags and groups of keys/keytags
- Supervise events relating to cabinets and keys (Supervision objects).
- Pass remote controls to cabinets (Supervision objects).

SET UP AND ASSIGN KEYS TO USERS

Integration into **MICROSESAME** is simple, and set-up takes just a few minutes. All the information on keys, groups of keys and cabinets can be imported from the TRAKA or PROXSAFE software in a single operation.

The assignment of access rights to these keys or groups of keys are then attributed transparently: directly in the “User” and “Access Profiles” interfaces of **MICROSESAME** and **WEBSESAME**.

Thus, this key management benefits from all the precision of traditional access rights (membership of profiles, time schedules...) and all the advanced features such as operator filtering, bulk edits, searches, user gateways...

SUPERVISE TRAKA & DEISTER CABINETS

Importing the key cabinet configuration allows the automatic creation of supervision objects associated with TRAKA and PROXSAFE equipment:

- For cabinets: connection properties, battery status, defects, door opening...
- For keys/keytags or groups of keys/keytags: take/return properties, user concerned, return time, out of time, position in the cabinet...

The properties of these supervision objects are animated according to the events reported by the TRAKA or PROXSAFE servers.
The commands associated with the cabinets can be used to transmit a state change directly to the servers.
The key access history is available via the technical history (supervision objects).
Finally, these properties can be used in a supervision synoptic and their state can be observed in the event monitor.
For TRAKA cabinets, a graph symbol is directly available for integration into the synoptics.

The following is a list of available properties for each supervision object:

proxSafe®

PROXSAFE Cabinet object:

- Power outage
- Low battery
- Connection to the server COMMAND
- Date/time of last event
- Opening the cabinet
- Door opened too long
- Department open
- Tamper alarm
- Tear alarm on department compartment
- Three incorrect codes
- Unexpected opening
- Unknown keyTag rendered
- Unknown keyTag removed
- No exchange of keyTags *(Port opened and closed without KeyTag movement)*

PROXSAFE Keytag object:

- Date/time of last event
- Keytag removed by the user
- Unexpected withdrawal
- Withdrawn too long ago
- Keytag returned by the user
- Return incorrect
- Secure return bypassed *(Non-compliance with restitution protocol)*
- Return time exceeded
- Unlock for restitution for the user

PROXSAFE Keytag Group object:

- Date/time of last event
- Group withdrawn incomplete
- Group returned incomplet

traka

ASSA ABLOY

Subject Cabinet **TRAKA**:

- Power
- Connected battery
- Battery level (3 levels)
- Connection to the TRAKA server
- Logged in user
- Connection time
- Opening the cabinet
- Duration of operation
- Door opened too long
- Department open
- Tamper alarm
- Unexpected opening

Key Object **TRAKA**:

- Position
- Key plugged/available
- Key taken by the user...
- Date/time of intake
- Key returned by the user...
- Date/time of return
- Return time exceeded
- Return incorrect (wrong slot)
- Unexpected withdrawal

23. EMERGENCY RESPONSE PROCEDURE (POI)

ASSISTANCE TO EVACUATION AND EMERGENCIES

The emergency response procedure defines the organizational measures, the emergency methods and resources that the operator must implement to protect its staff, the general public and the environment. The main demands for facilities with the greatest risks, including facilities under a specific response plan (SRP).

MICROSESAME INTEGRATION

The POI support application built into MICROSESAME is involved in the process of protecting staff through IHMs, simple dedicated windows and through the following functions:

- Setting POI zones into two categories: secure and unsecure
  - Safe areas are those where staff are gathered free from hazards
  - Unsecured areas correspond to the rest of the site
- Providing the list and number of people present on site in real time by area, with display of their clearances (if used), according to their badges on badge readers
- Real-time monitoring of staff migration from work areas to secure areas after triggering the POI, during exercises or incidents
- Search for a person to know their location (safe area or not)
- Edition of people names with charts for selected areas
- Possible export to pdf file of the list of people
- The operation and display of POI areas starts from a synoptic plan or the general menu

To facilitate the census at gathering points (secure areas), it is convenient to use the **MOBILIS** portable terminal, which is intended for outdoor use. No need to wire readers, the badges are read by the evacuation officers.

24. CONTROL OF REST TIME

RESPECT FOR LABOUR LEGISLATION

Article L3131-1-2 of the French Labour Code stipulates that every employee enjoys a daily rest of at least eleven consecutive hours and a weekly rest of a minimum of 35 consecutive hours.

MICROSESAME, through the "**Rest Time Control**" function, allows you to easily comply, using the building access control system.

The automatic analysis of employee badge passages allows to calculate whether these legal rest times, or other resting times stipulated by the company, have been respected. Several options are available to choose from:

AUTOMATICALLY BLOCK ACCES to employees who have not followed the appropriate deadlines between exit and entrance to the site, on a temporary basis until the times are respected.

SIGNAL THE FORBIDDEN ACCESS temporarily with a date and time for the next access authorization displayed in the user record. Access blocked optional.

TEMPORARY BLOCKAGE can be manually removed by authorised operators.

REPORT GENERATION to check anomalies on rest time.

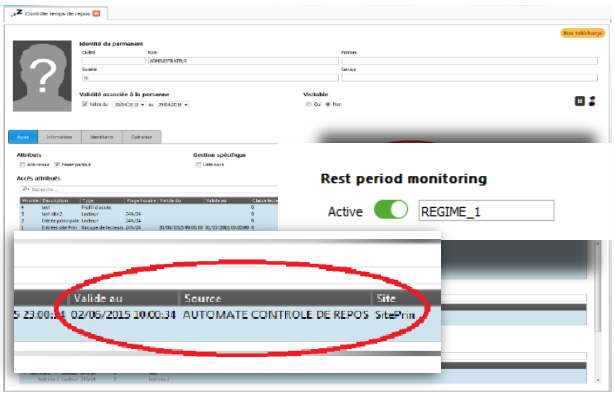
EXCEPTIONAL EVENTS: it is also possible to "disengage" the monitoring of the rest time for all employees.

To quickly deal with large populations, the resting time control function is based on the concept of "resting regimes". Each "rest regime" requires declaring entrance/exit readers, establishing the durations and days of rest, and the start times of weekly and daily calculations. It is possible to record several "rest regimes" so that each user is controlled according to the rules and readers that concern him. This attribution can be carried out directly in **MICROSESAME** or via a gateway with the company HR database.

When the option is enabled for an employee, rejected reader passages appear as "off time schedule" in the event monitor and the history log in **MICROSESAME**.

By opening the ID record, it is possible to view the temporary access ban and to know the date and time of the next access authorization.

If necessary, this temporary blockage can be manually removed by an authorised operator.



Finally, to carry out a more comprehensive follow-up of employees through the HR and Security services, the **MICROSESAME** Universal Requester allows to launch weekly analyses to generate a file containing all the “off time schedule” forbidden access (see History and Reports).

25. PATROLLING ROUNDS

PATROLLING ASSISTANCE

Patrolling management (**MS-PCR**), a former software option now included in **MICROSESAME,** software option that allows you to create rounds and agents that are required to perform patrolling rounds on a site in real time.

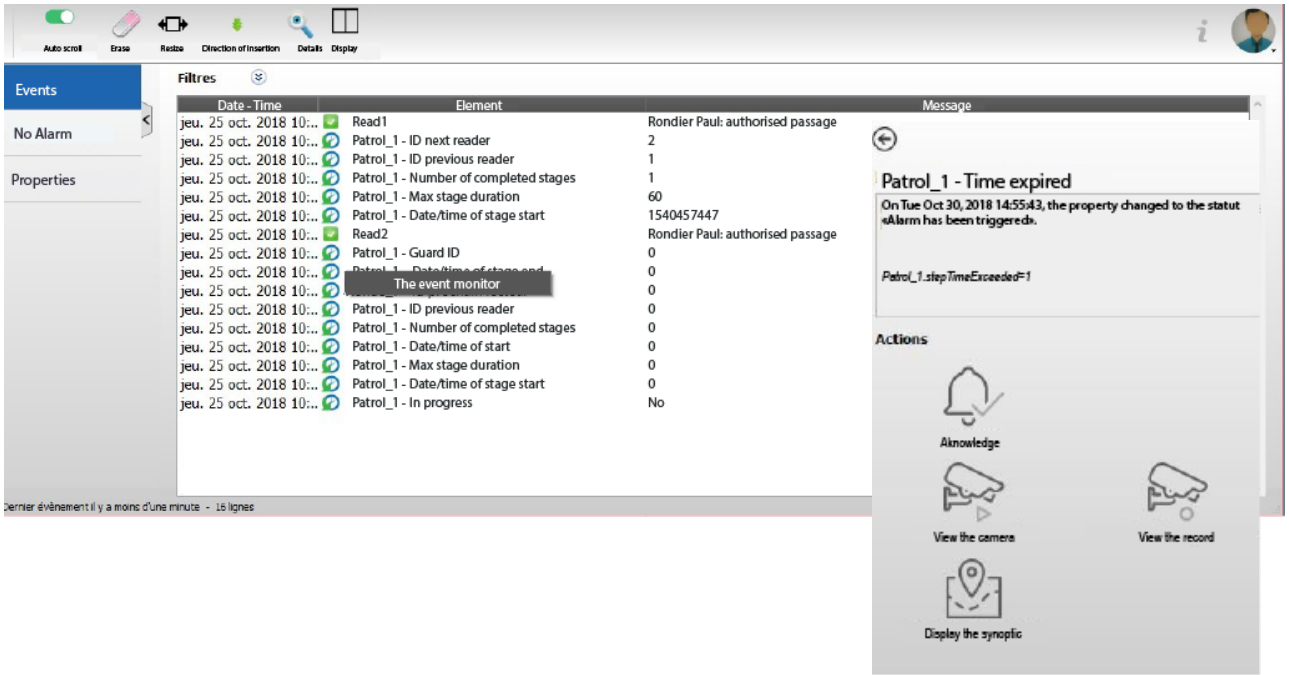
A surveillance round is a predefined route of readers, on which the patrolmen in charge of the round must present their ID in succession. This option allows you to control the progress of several operators over 64 different routes. (one operator/round).

MANAGEMENT OF PATROLLING ROUNDS can use existing readers on your site without dedicated readers or specific material for carrying out rounds.

THE PATROLLING ROUND can be carried out without the right of access to the relevant readers but in this case without authorised access. The patrolling operator can use its access control ID (badge) to complete the round.

SPECIFIC OPERATOR RIGHTS exist for patrolling rounds management (access to the application and round management, without the necessary access rights) to operators with restricted profiles.

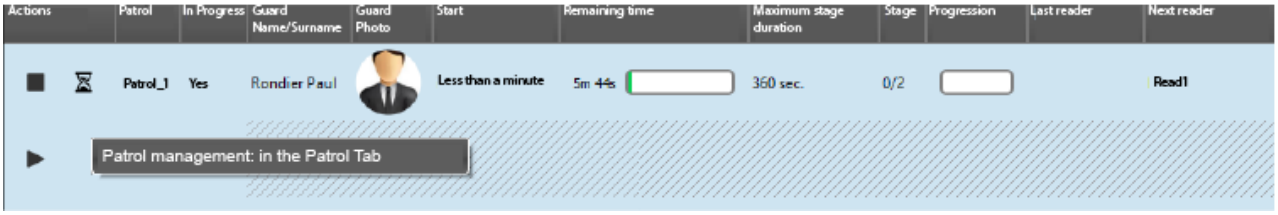
To start a patrolling round, select a round from the list and choose the operator in charge of the round. The time set between each reader must be respected. In case of time overrun between 2 readers, an event or alarm is automatically triggered on the event monitor, specifying the operator and the concerned patrolling round. On alarm, the possible actions are: Acknowledge, View the synoptic graph, View the associated camera in **VISIOSESAME**.



A dedicated table shows in real time the different information and round status:

- In progress, the operator that makes the round,
- The delay since the start of the round,
- The time allocated to the operator for swiping his badge on the next reader with a progression bar (with colours green, yellow, orange, red), depending on the remaining time,
- The total time for each step,
- The total number of steps,
- The current status,
- The last reader where the operator ID was detected,
- The operator ID or point must be presented.

The operator can also allow extra time for the operator to swipe his badge on the reader (passages are still possible at any time), or to cancel the round.



26. HISTORY, APPLICANT, REPORTS & JOURNALS

These functions are natively integrated into the **MICROSESAME** solution.

HISTORY

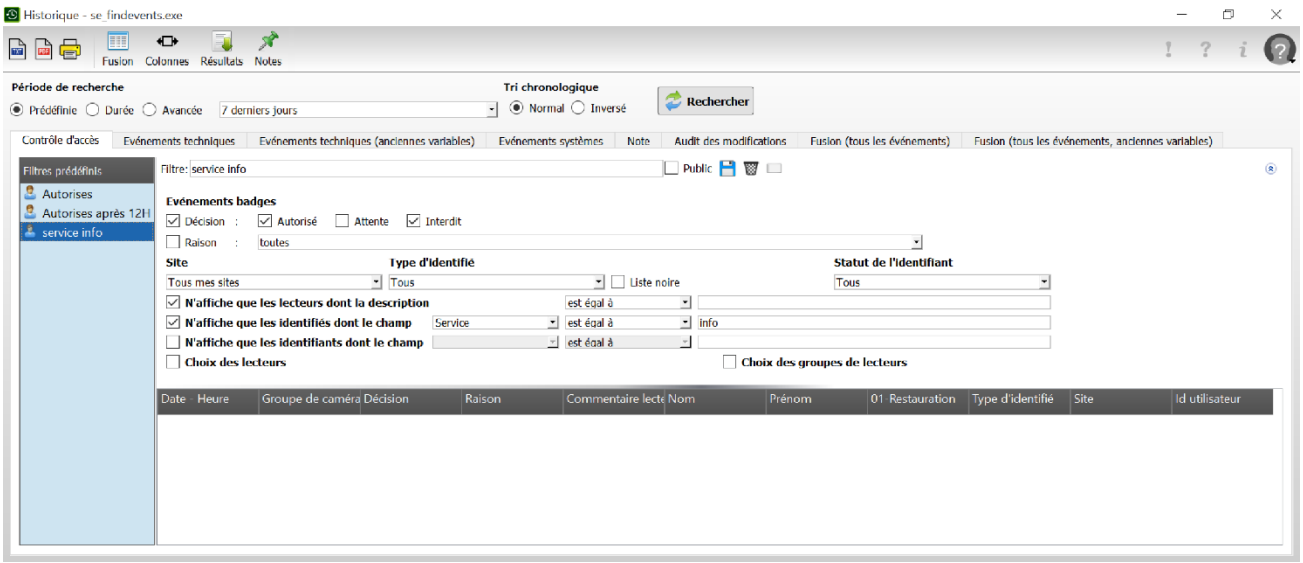
The "**History**" feature, from a heavy client, allows you to view all the events in the database. It keeps track of the building (badges, technical alarms...), the system and the actions taken by the operators.

Storage capacity is not limited. By default, the event retention period is set at 30 days, but this value is adjustable (3 months is the value used by the CNIL).

The criteria for searching and displaying events, alarms, movements are presented by a global view with common criteria and by the following tabs corresponding to types of events:

- Access control.
- Technical events.
- System events.
- Audit of changes (operator actions).
- Merge of all events.

These fields are different for each tab. By default, the search period uses the current time and the last 7 days.



The History feature offers finesse, customisation and speed to the customer through:

FILTER ON CERTAIN DATA (fields): they allow to edit very precisely the events sought. To get quick and relevant filter choices, they can be in preset drop-down lists depending on the system setting. For example, the site choice (in multi-site management), the user type (visitor or permanent), the ID status (lost, stolen, active...), ...

BACKUP AND NAMING: To simplify recurring needs, it is possible for each operator to back up and name typical searches with their settings and pre-filled settings. These different typical searches are recorded in the "pre-set filters" window with the choice between private backup (visible for the operator who created it) or public (visible for other operators as well). This avoids entering the same search criteria over and over and represents a significant time saving

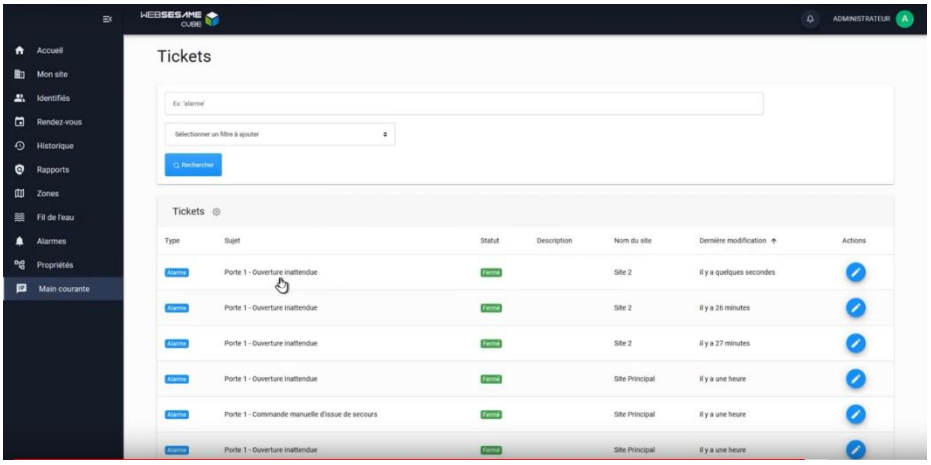
FILTERING of the property visualization according to the operator "category".

INFORMATION FOR FORBIDDEN PASSAGES: site, unknown identifier, tightened control, controlled passage, no access.

WEBSESAME

The **WEBSESAME** port offers among others these applications concerning this history theme, report,...

- WEB-REPORTS: Generate, export reports, predefined queries
- WEB HISTORY: History access control events, techniques
- WEB-ALARMS: synthetic view of current alarms
- WEB-REAL TIME FEED: Real-time monitoring of events access, technique, system. Click to view the user profile of the event. Simplified Event Monitor
- WEB-Activity-tracking: Add and view open operator issues/comments of current acknowledgeable alarms. Simple search or by filters.
- WEB-My site: Edit synthetic reports & graphs of authorised and refused passages on supervised sites.
- WEB-Properties: Help to diagnosing its installation: View the list of states / properties (e.g: open port) of a supervision object, perform filter searches, Interact with these states (remote controls), Inhibit a property if maintenance



WEBSESAME ACCESS CONTROL HISTORY

MICROSESAME web interface includes a tab that allows you to easily view access control history to search for badge passages.

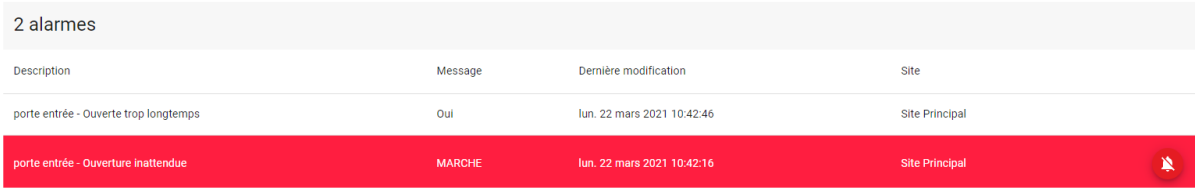
Different parameters and filters, date, events (badges allowed, prohibited...), can be applied to facilitate the viewing of data. The fields displayed as results are adjustable (title, name, id...).

HISTORY OF TECHNICAL EVENTS WEBSESAME

Technical events related to the access control system can be searched via the History log.

ALARMS WEBSESAME

The operator can view the current alarms at the site(s) under his supervision. The information raised in the table is updated in real time. Color coding makes it easy to distinguish between acknowledgeable alarm.



WEBSESAME REPORT, UNIVERSAL APPLICANT

Also accessible from the **WEBSESAME** portal, the universal applicant allows the extraction of all types of information contained in the **MICROSESAME** database through the execution of an SQL query and the generation of a report/result.

The following options are possible:

QUERIES : They natively exist in the product (see list below) allowing you to have the most common searches. Library of queries available in: Serveur\ScriptsSql\SqlServer\Requestor\FR

RESULTS, REPORT : It appears directly in the HMI after the desired query has been executed. It is possible to export this result to a file in CSV and PDF format. You can then use the CSV file from an Excel spreadsheet or text editor to edit graphs, make statistics, ...

REPORT EXECUTION : on change of ownership and automatic e-mailing

CREATION OF CUSTOM QUERIES:

- Through the integrator, the end customer having a good knowledge of the SQL script language, may use custom simple queries based on examples of existing ones
- By TIL TECHNOLOGIES, on a project basis, to carry out more complex queries according to customer requirements, the database schema & table content (MCD) not being documented.

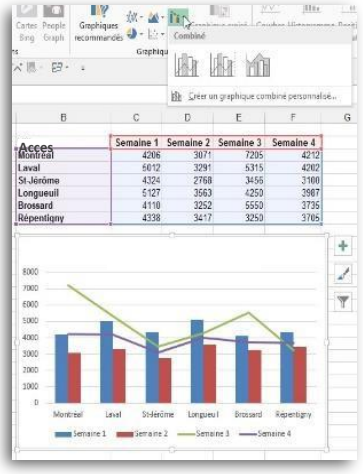
IMPORT, EXPORT QUERIES in format "file.json". It is possible to import a query that has been previously exported from another **MICROSESAME** system.

FILTERS: The query may include settings to filter the expected result based on a date, time, choice in a drop-down list (company, service, reader, ...), person, etc. If a filter field is not filled, it concerns "all" of the relevant field

EXTRACTOR TOOL: available in the solution, allows you to make automatic - periodic reports of desired queries in defined directories to simplify your recurring tasks.

LIST OF EXISTING REQUETES IN THE LIBRARY

- 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



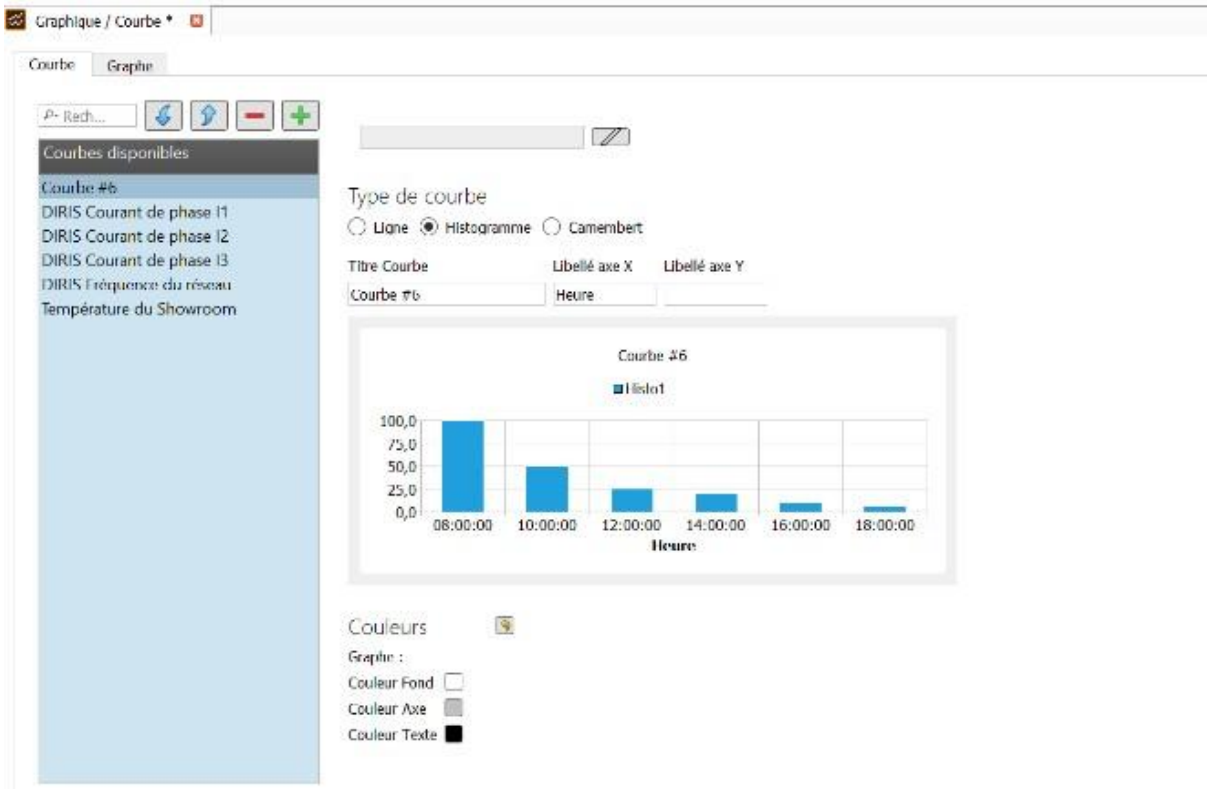
DESCRIPTION OF SAMPLE QUERIES:

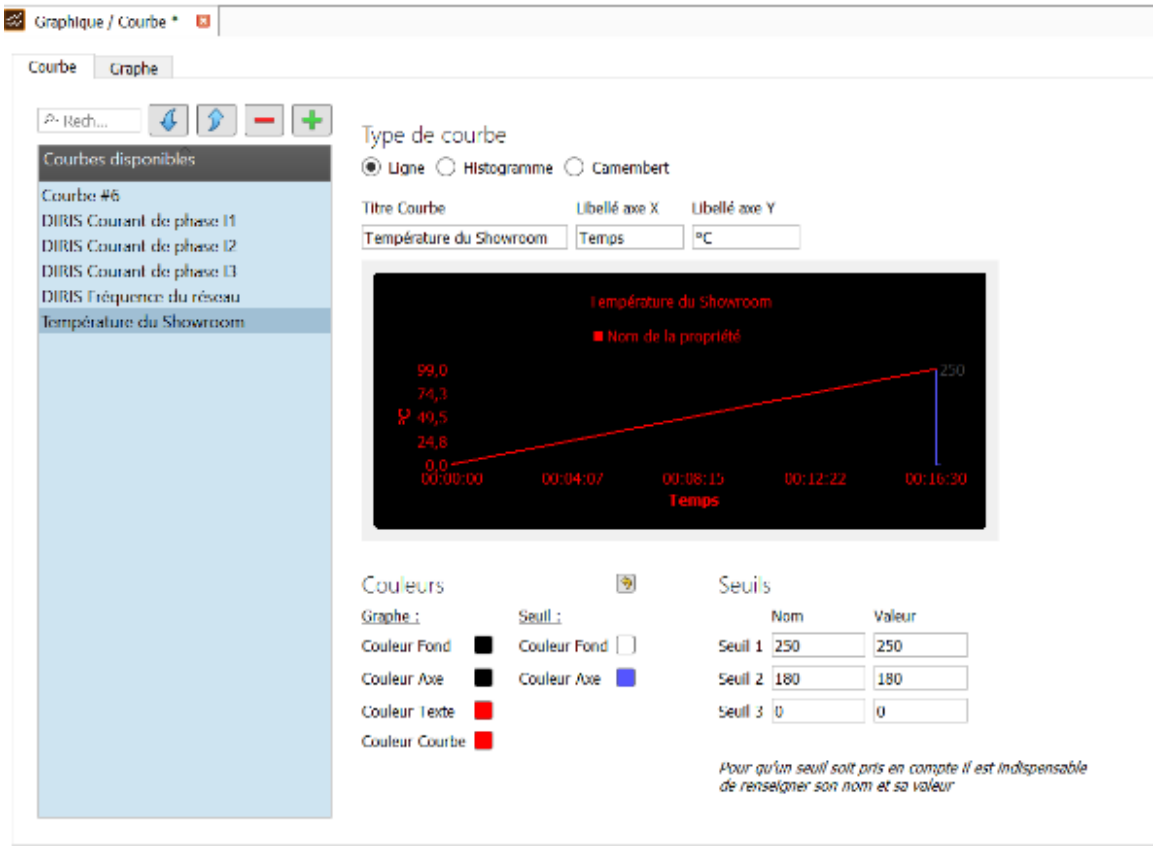
- "Rest request": List of users who did not respect their assigned rest times.
- "Users that will be no longer be valid on next month": List of people who will be disabled on a given date. The interface for this query below displays the following filters: start-end date, registration number, name, first name.

GRAPHICS AND CURVES IN MICROSESAME

MICROSESAME integrates a graph/curve application that allows you to visualize the evolution of digital or logic variables over a defined period of time and in the form of curves. This application offers the following possibilities:

- A specific search period to filter obtained data.
- The curves - data obtained are exportable in PDF format or a file.JSON at a chosen location. JSON files can also be used to import external settings.
- Graphs allow you to group several curves under one graph.
- The following curve display characteristics can be configured:
  - Colours on the curve, background, axes, texts, thresholds, title of X and Y, curve types to be chosen among the 3 different types:
    - Line: used by MICROSESAME "properties" (Notion of 3 possible thresholds with name and the value of each threshold)
  - Histogram: generated from an SQL query
  - Camembert: generated from an SQL query


Graphique / Courbe *
Courbe
Graphe
Rech...
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
Rech...
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
°C
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

27. GATEWAYS AND CONNECTORS

MICROSESAME CUBE is a safety hypervisor that integrates and interfaces with a large number of software, hardware, systems, directories, etc. to offer a centralised global solution, the widest possible openness and ease of adaptation to future needs.

MICROSESAME CUBE therefore makes it possible to manage a large ecosystem of functions and professions and to supervise alarms, defects of these systems with the capabilities of the solution described in the dedicated chapters: MONITORING & SUPERVISION, SUPERVISION VIDEO, INTRUSION

POSSIBLE CONNECORS FOR OUR **MICROSESAME** SYSTEM:

- BDD users & visitors: Web Department REST API, TXT/CSV files
- Operator management LDAP, Windows Authentication (SSO => Heavy: NTLM, WEB: SAMLv2)
- Supervisors I.T: SNMPv3 (from LPU TILLYS CUBE)
- Hypervisors / BMS: OPC UA, MODBUS IP, Bacnet
- Daemon, third party system (fire, ...), UGIS: MODBUS IP
- VMS video system: SDK VMS, gateway TEXT/ASCII
- Specific gateways projects and/or products (Web Department REST API, various SDKs, ...)
- Alarms to remote monitors under the TIL "**TIP**" protocol, based on ID-Contact or CESA 200 standards, and qualified at ESI and Azur soft

EXAMPLES OF INTERFACES REALISED ON OUR **MICROSESAME** SYSTEM:

- Building hypervisor, BMS: PRYSM, PC VUE, PANORAMA…
- Room and resource reservation: ASW, Planitec…
- Truck flow management: EASYPROG, STACKR
- Video: MILESTONE, GEUTEBRUCK, VIDEOWAVE, GENETEC (see chapter VIDEO SUPERVISION)
- Integration of the MILESTONE ACCESS CONTROL plug-in, for supervision of TIL access control in the MILESTONE X-PROJECT supervision interface (see the dedicated chapter VIDEO SUPERVISION)
- Intercom: COMMEND in IP/Import of subscribers, Calls, call notification (with distinction between normal and urgent), Night call transfer, possibility to connect to the intercom server (see dedicated chapter INTERPHONY)
- DEISTER key cabinet: Synchronisation of identifications with COMMANDER 4 software
- **SORHEA** perimeter detection via the MAXIBUS protocol of SORHEA
- Fire panels via MODBUS protocol
- AVIGILON video matrixes and multiplexers, STENTOFON intercoms ... via ASCII, TXT protocol
- IDEMIA MORPHO biometrics (see BIOMETRY chapter)
- Elevators SCHINDLER, KONE…
- MEMOGUARD on-call management
- AASTRA Autocom
- PTI systems (Protection of Isolated Worker)
- HR directories: SNCF'S CANIF, Société Générale's BDRS, DGAC's STITCH, etc.
- SMTP messaging for emails

GALAXY INTRUSION CONTROL UNIT

Honeywell
GALAXY

MICROSESAME CUBE interfaces with the Honeywell NFA2P GALAXY Intrusion Control Unit using the TCP/IP protocol (SIA) (the use of RS232/RS485 ports and the use of a converter is no longer necessary). The use of Honeywell Galaxy E080-10 – Ethernet IP Transmitter module is also required.
Interfacing with Galaxy control units is quick and easy.
A maximum of 512 zones, 256 outputs and 32 groups can be managed with this gateway.
See PDF MS_Cube_ Galaxy_Gateway for more details

Simply define the communication parameters and the desired "zone", "group" and "output" supervision objects from the templates provided by TIL in the library:

- Point status feedback (rest/Default/Alarm/Short circuit/ Masked/Excluded)
- Group status feedback (MES/MHS/MESP)
- Alarm feedback by individual point
- Alarm acknowledgement by individual point
- Ejection of points from the **MICROSESAME** supervision

- Interface default feedback (RIO) (1)
- Feedback of the control unit status
- Sending of remote controls from MICROSESAME -> GALAXY
    - Activation and deactivation of alarm groups
    - Activation of an output on the GALAXY from the MS supervision
    - Siren stops per group

(1) The Galaxy control unit provides some information about its status.
With specific configuration using Frontshell software, it is possible to retrieve certain information using the outputs of the Galaxy control unit. The information available is detailed in the Galaxy documentation. If the desired information is not configurable on the control unit, it will not be available in **MICROSESAME**.

BIOMETRY

MICROSESAME is able to manage the biometric readers of several brands & ranges: EVOLUTION CUBE, IDEMIA, STID, HANDKEY.

For the EVOLUTION CUBE TIL and STID:

- EVOLUTION CUBE TIL and ARCHITECT readers
- TIL has integrated biometric readers in transparent mode with ANSSI compliant (SCCPv1) and ANSSI certified protocol (SCCPv2)
- Biometric solution with badge + bio (1:1) compliant with CNIL recommendation AU52: the fingerprints are in each person's badge and not in a centralised database. In this case, the fingerprints are enrolled in the STID SECARD BIO software, which writes them to the badge.

For the IDEMIA brand (e.g: MORPHO):

- SIGMA (fingerprint) series readers, MORPHOWAVE COMPACT (contactless on-the-fly reading of fingerprints...
- The biometric registration is done through the MORPHOMANAGER log of IDEA which can be opened by a simple click on a favorite in the user form of **MICROSESAME**
- TIL has integrated the MORPHO-BRIDGE gateway from the MORPHOMANAGER software to be able to send user records and credentials, created in **MICROSESAME**, to the MORPHOMANAGER software, in order to avoid duplicates.
- Biometric solution with:
    - badge + bio (1:1) CNIL AU52 compliant: fingerprints placed in each badge and not in a centralized database. In this case the fingerprints are enrolled in the MORPHOMANAGER log which writes them in the badge.
    - bio only (1:N) subject to more constraints by CNIL AU53 because fingerprints are centralized in a database that needs to be protected (see RGPD). In this case the fingerprints are enrolled in the MORPHOMANAGER log which sends them directly to the BIO readers.

STANDARD INFORMATIC PROTOCOLS

It is possible to interface industrial daemons or BMS systems using the **MODBUS IP** protocol.

MICROSESAME also has **secure UA OPC** protocols (server only). These protocols are widely used in the market, allowing the link between systems.

This allows you to interface:

OF SUPERVISORS

- Prysm Appvision
- Codra Panorama
- Wonderware
- PCVUE

DAEMONS, FIRE POWER PLANTS COMPATIBLE WITH MODBUS IP OR OPC

- Schneider
- DIRIS...

API REST & WEBSERVICES

TIL provides its customers and technology partners with an API, acronym for “Application Programming Interface”.

This API makes it easy to develop gateways between **MICROSESAME** and other applications by exchanging data in the TIL supervisor database:

The API precisely defines the methods by which computer developers can write programs, in their own applications, that can interact with microphone (function or data call).

The dialogue between **MICROSESAME** and third-party applications takes place over the network via Web Department. That is, the API uses the https protocol, the most commonly used communication protocol.

Caution: Access to the MICROSESAME API is subject to the signing of a Non-Disclosure Agreement (NDA).

EXAMPLES OF REST API EXCHANGES WITH OTHER LOGS:

The interfaces already realized concern both existing and commercialized logs and applications developed specifically by our customers:

- Specific Visitor Management Log (QR-code...) or personalized intranets with appointment interface (users and credentials)
- ASW Meeting Room Booking Log (Users)
- Personalized room booking application (users and credentials)
- Attendance time calculation application (users and history of badges)
- Conference hosting application (users and history on mobile reader)
- Canteen billing log (users and history badges)

- eGestrack operations tracking log (from STACKr) for logistics platforms (users, credentials and history badges)
- Rail/Road Transfer Platform Management Application (users and history of license plate readings)
- Interface between **MICROSESAME** and KONE elevator (user and credential)
- interface between **MICROSESAME** and TEB video log

GATEWAYS WITH MANAGEMENT APPLICATIONS, HUMAN RESOURCES, DIRECTORIES, ETC.

In many cases, it may be interesting to exchange data between **MICROSESAME** and databases that manage the company's employees or users (HR bases, directories, etc.).

Automating the synchronisation of these databases with the access control system is useful as the number of badges in circulation is important, and it allows:

- Preventing duplicates (significant time saving and accuracy)
- Automatically assigning access to people based on rules (aliases) to be defined by project (according to their service, function, etc.)
- Immediate and automatic consideration of staff arrivals or departures, ensuring optimal security.

With the gateways proposed by TIL, WEB SERVICES API REST or MS-SYNCH (CSV), the automatic data update can be set up to occur at a fixed time or whenever the source file changes. Of course, manual synchronisation is still possible.

MICROSESAME supports synchronisation with several different sources, each source may have a specific synchronisation configuration.

MICROSESAME can also be transformed into a data provider, to deliver to third-party systems (Restoration, Printing Service, Key Cabinet Management, etc.) personal data created by access control and multi-application badge encoding, with WEB SERVICES or MS_RSYNC (CSV) gateways. **MICROSESAME** can power different systems with custom data for each third-party application.

This automatically updates the basics of third-party systems, and prevents users from registering and enrol their badges on each system.

MESSAGING

MICROSESAME incorporates an email-on-alarm function via SMTP. An alarm (intrusion, access control, technical alarms) can be sent by email.

It is also possible, following the execution of a report with the universal applicant, to automatically trigger its sending by email to defined recipients.

Sending by SMS is not directly integrated with **MICROSESAME** and requires taking a third-party solution.

MICROSESAME INTER-SYSTEM

The ISMS gateway allows the exchange of data via IP network between several independent **MICROSESAME** systems (UDP protocol). Data exchanges are based on property names.

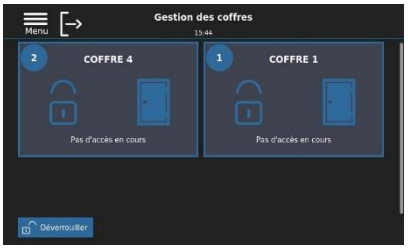
Example of use: A customer has several sites with a server and a security PC operating by site. The customer has an inter-site IP network. A site could act as a centraliser of synthetic alarms at weekends and host a client capable of connecting to all the sites/servers (one at a time). Thus, if a major synthetic alarm is sent from the X server to that central server, the central operator will receive that alarm on its site operating station. It will be instructed to log on the client station pointing to the X server and manage the alarm.

28. BANKING MANAGEMENT

Securing a banking agency must respond to specific processes and use particular access control functions. Faced with the risks of robbery, duress access or internal maliciousness, entry into secure areas and opening of safes must be ensured by strong authentication solutions (double identification...) and according to defined scenarios (timeouts, sequences of actions...). The solutions implemented must therefore allow complex automations to be configured in a simple and scalable way.

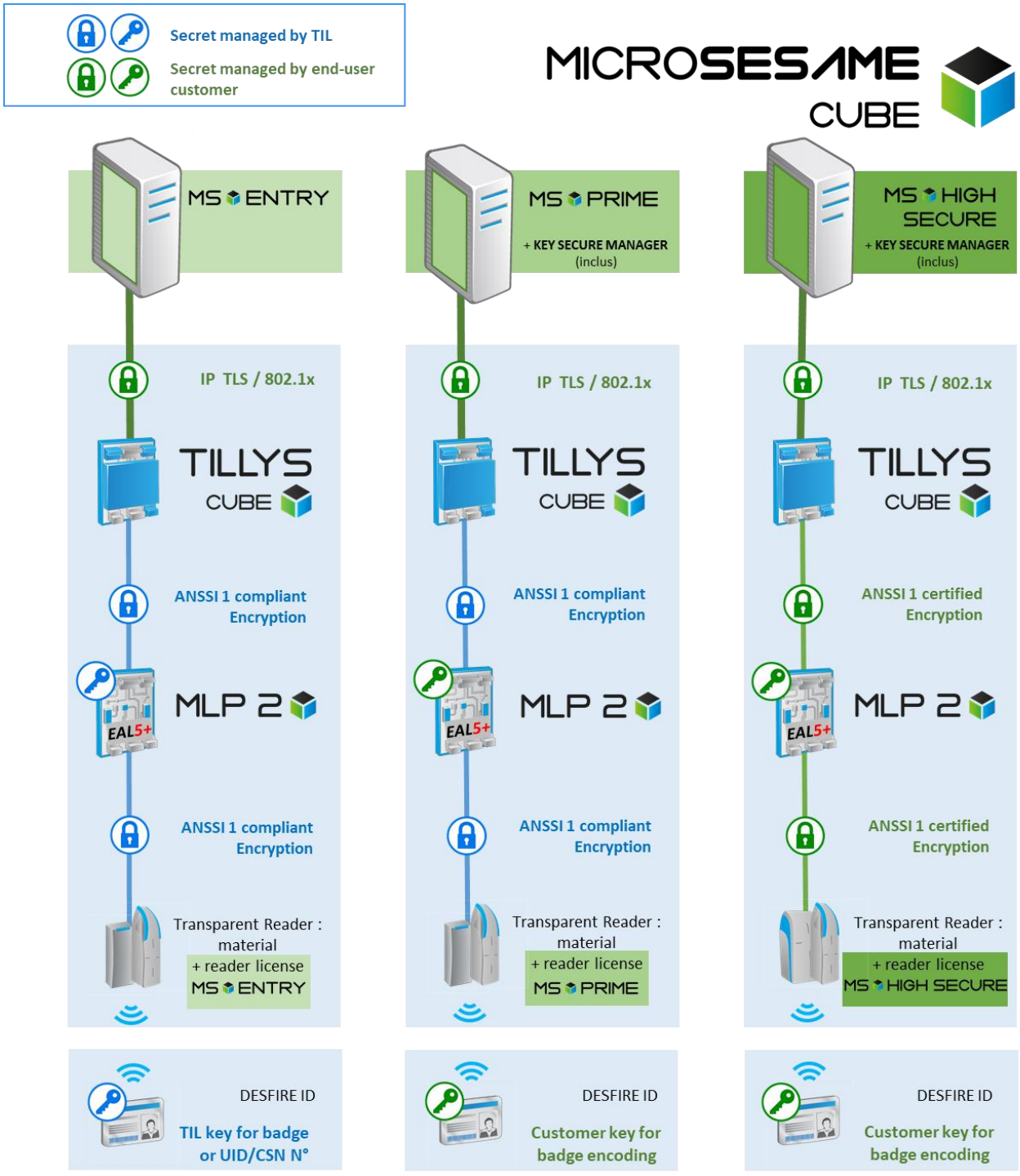
TILLYS daemons, VAULTYS operation keyboards and **MICROSESAME** logs can meet all banking agency needs.

- Complete local setting of a serverless banking agency with export of the setting to import into the central server and duplicatable on all X agencies
- Agency equipment with HMI dedicated & simplified: LED colors of readers customizable according to states, badge reader display with timeout countdown and color according to state EN/Off monitoring STE,
- SAS and unique access to STE (Secure Technical Enclosure)
  - One open port between each safe and STE access
  - STE entry prohibited if an open safe and/or a person already on area
  - Multiple authorized persons but only one type of worker at a time (unique population)
- Chests management and timeout on the VAULTYS 7" colour touch screen:
  - Identification by code, badge or badge + code
  - Permitted opening of only one chest at a time
  - Visualization of the current timeout
  - Filtering accessible safes and customizing timeouts according to the speaker, time schedules or other conditions...
- Customizable conditional or sequential controls
  - Combinations of actions between badge access, in/out intrusion, “Everything is fine” button, ...
  - Different depending on the type of worker: conveyor, employee, line manager...



29. UNDERSTANDING THE SOFTWARE OFFER & MATERIAL CUBE

CUBE OFFER: SCALABLE ACCESS CONTROL SOLUTIONS



THE MICROSESAME CUBE LICENCING OFFER

SERVER LICENSES

By level of cybersecurity management, number of readers and users

MICROSESAME CUBE

Basic License - All Access Control / Intrusion / BMS functions available

MS ENTRY	MS PRIME	MS HIGH SECURE
Number of readers MS ENTRY	Number of readers MS PRIME	Number of readers MS HIGH SECURE

Number of Mechatronic readers
(Same license for ENTRY, PRIME or HIGH SECURE)

Number of Manager Operators

Number of Web Operators

OPTIONAL FUNCTIONS

Fixed cost at option activation

- Multisite Management
- Telesurveillance
- Visitors Management
- Server Redundancy

GATEWAYS

Fixed cost at gateway activation

- Passerelle Import
- Passerelle Export
- Texte
- LDAP
- MODBUS
- OPC UA
- OPC DA
- Plugin CA MILESTONE
- Biométrie MORPHO

INTEGRATED CONNECTORS

Variable cost by number of supervised objects

Supervised Objects with Advanced Integration:
Cameras, SORHEA sensors, GALAXY sensors, COMMEND interphones

- 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

Find out more about our products and news on :

www

til-technologies.fr/en

in

TIL TECHNOLOGIES

TIL TECHNOLOGIES
Parc du Golf - Bât 43
350, rue de la Lauzière - CS 60481
13592 Aix-en-Provence Cedex 3

Tél : 04 42 37 11 77
Mail : info@til-technologies.fr

TIL TECHNOLOGIES