



JANVIER 2020

DESCRIPTIF FONCTIONNEL

MICRO-SESAME

Version 2018.5

TIL TECHNOLOGIES

SOMMAIRE

MICRO-SESAME EN QUELQUES MOTS	3
ARCHITECTURE CERTIFIEE & QUALIFIEE ANSSI	4
RICHESSSE FONCTIONNELLE EN SURETE ET SMART BUILDING	12
CAPACITES DU SYSTEME	18
CONFORMITE RGPD & CNIL	20
GESTION DES OPERATEURS	22
GESTION MULTI-SITES / MULTI-CLIENTS	24
GESTION DES ACCES	26
GESTION DES VISITEURS	32
CONTROLE D'ACCES "OFFLINE"	40
ENODAGE DES BADGES	41
PERSONNALISATION DES BADGES	42
MONITORING & SUPERVISION	43
SUPERVISION VIDEO	51
GESTION INTRUSION	55
INTERPHONIE	59
PLAN D'OPERATION INTERNE (POI)	60
CONTRÔLE DU TEMPS DE REPOS	61
GESTION DES PARCOURS	62
HISTORIQUES, REQUETEUR & JOURNAUX	64
PASSERELLES ET INTERFACES	69

MICRO-SESAME EN QUELQUES MOTS

MICRO-SESAME

MICRO-SESAME est un système intégré pour la **Gestion Centralisée de la Sûreté** (contrôle d'accès, intrusion, vidéo) et la **Gestion Technique du Bâtiment**.

Il permet la supervision unifiée de toutes les informations électroniques du bâtiment.

Le pilotage des différentes fonctions à travers une interface graphique commune rend leur exploitation beaucoup plus simple et les interventions plus efficaces.

Les interactions entre les différents systèmes pouvant être complètement automatisées (actions sur évènements), la rapidité des traitements est également garantie.

Le système se compose d'une partie logicielle et d'automates IP sur lesquels sont raccordés tous types de matériels.

Cette architecture s'appuie sur des standards qui garantissent sa pérennité, mais aussi sa capacité à évoluer à moindre coût.

Par l'intégration de SDK ou de protocoles informatiques (MODBUS...), **MICRO-SESAME** peut superviser des informations en provenance de systèmes externes (comme les systèmes de sécurité incendie) et de se comporter en hyperviseur de systèmes vidéo numériques.

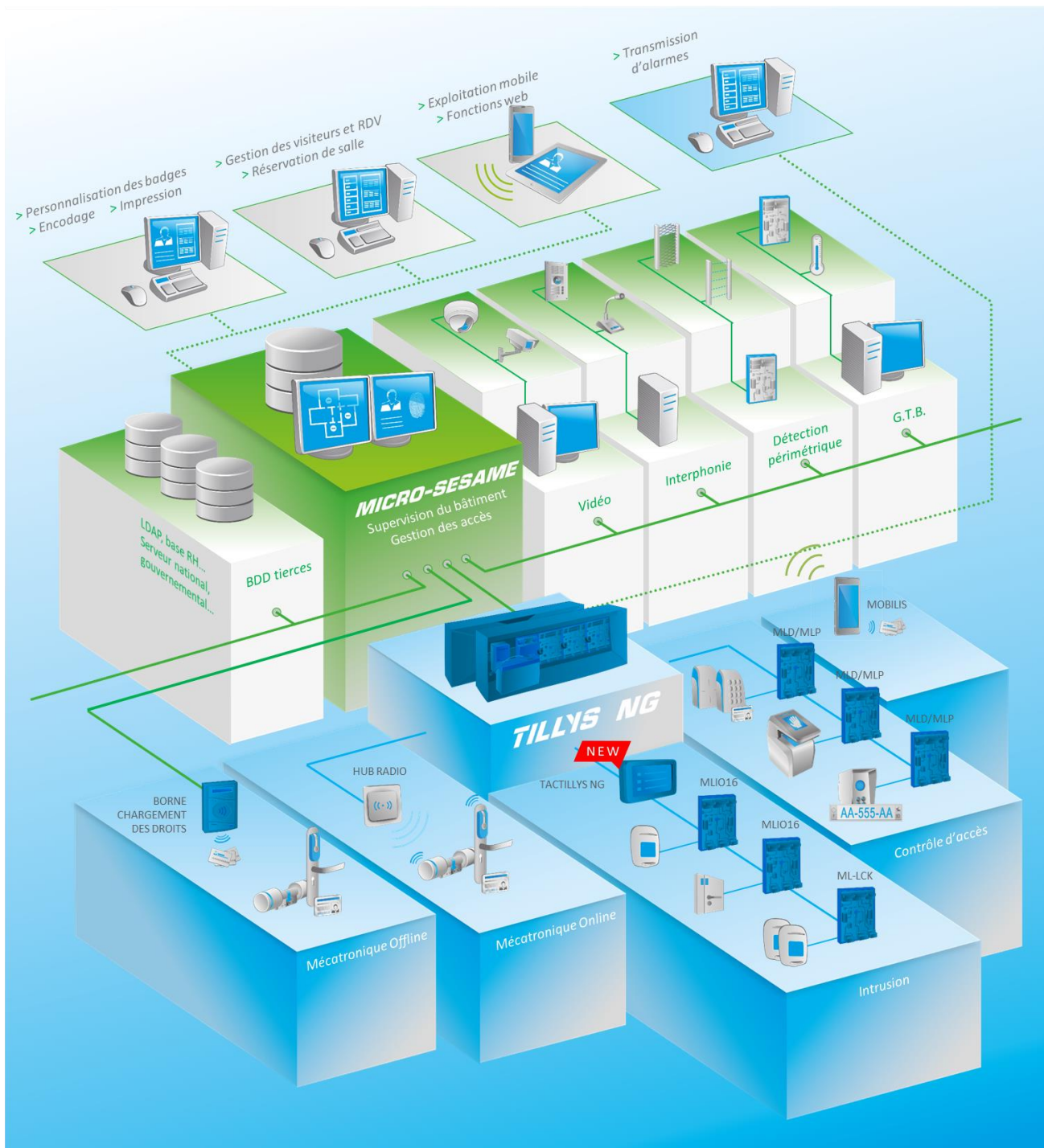
Il communique aussi directement avec des automates programmables industriels (API) et d'autres équipements de sécurité ou de sûreté au moyen de passerelles (OPC, texte...).

ARCHITECTURE CERTIFIEE & QUALIFIEE ANSSI

ARCHITECTURE MATERIELLE ET LOGICIELLE CYBER SECURISEE

Une architecture **MICRO-SESAME** se compose des éléments suivants :

- ▶ Un serveur, qui est à la fois un poste de paramétrage et d'exploitation fonctionnant sous un environnement informatique standard Windows. Sa mise en œuvre est facile et conviviale
- ▶ Un réseau Ethernet IP (filaire, wifi) sur lequel le serveur est connecté à des postes d'exploitation (clients lourds **MICRO-SESAME** & **VISIO-SESAME**, clients légers via RDP/Citrix, clients WEB **WEB-SESAME** sur PC, smartphone, ou tablettes), à des automates TIL (UTL), et à des outils de mobilités (lecteur MOBILIS en wifi)
- ▶ Le réseau Ethernet permet également de relier la solution **MICRO-SESAME** à des systèmes du client final (Active directory, superviseur I.T SNMP, base RH,...) et à des applications tierces (serveur VMS et enregistreurs vidéo, hyperviseur OPC, automates via MODBUS,...)
- ▶ Des automates TIL (UTL) autonomes & multifonctions sur réseau IP, pour le pilotage du contrôle d'accès, de l'intrusion et de la G.T.B.
- ▶ Des claviers intrusion, Des solutions mécatroniques online, Des modules électroniques spécialisés déportés (modules portes, modules entrées/sorties, ...), raccordés sur les bus secondaires des automates pour une architecture distribuée ou centralisée au choix
- ▶ Des lecteurs, lecteurs clavier de contrôle d'accès, des capteurs (contacts, détecteurs intrusion, ...), des accès contrôlés (serrures, barrières, tripodes, ...), des actionneurs (sirènes, éclairages,...),... connectés à ces modules spécialisés

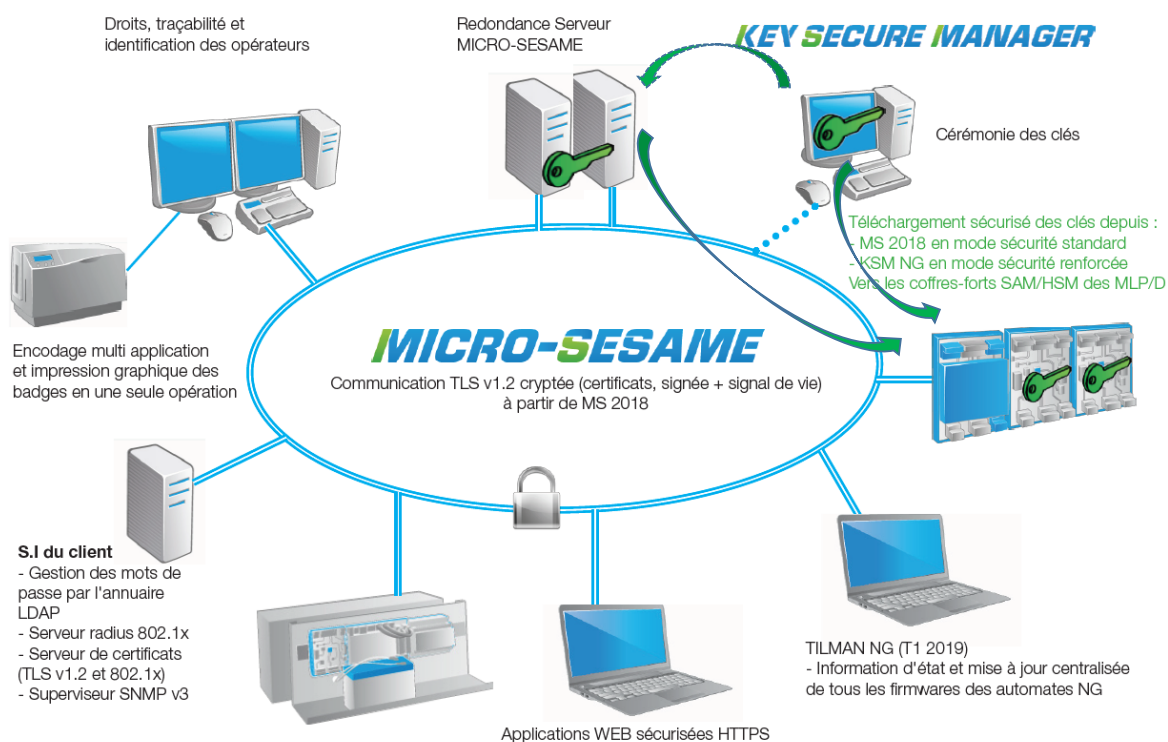


SOLUTION CYBER SECURISEE, CERTIFIEE CSPN ARCHITECTURE 1 ET QUALIFIEE ANSSI

Protéger les sites ne suffit plus. Il est également important de mettre en place des mécanismes pour sécuriser le système de sûreté lui-même contre les menaces extérieures et intérieures.

Sur toute l'architecture **MICRO-SESAME**, du badge jusqu'au serveur, des protections électroniques et informatiques, sont mises en œuvre pour prévenir les malveillances ou le piratage.

Pour vous garantir la meilleure sécurité et cyber sécurité, la solution est certifiée et qualifiée ANSSI selon l'architecture 1 recommandée par l'ANSSI (lecteur transparent).





MICRO-SESAME v2018, la gamme matérielle NG (TILLYS NG, module déporté ML) et les lecteurs EVOLUTION « transparents » vous apportent notamment les qualités et capacités de cyber sécurité suivantes :

- ▶ Une certification & qualification ANSSI officielle nécessaires pour les sites réglementés (OIV, OSE, ...) selon les lois LPM et NIS en vigueur et conseillée sur tous les sites sensibles
- ▶ Une qualification ANSSI pour maintenir ce niveau de sécurité dans la durée (engagement de TIL TECHNOLOGIES auprès de l'ANSSI)
- ▶ Une solution sécurisée de bout en bout, du badge jusqu'au serveur
- ▶ Toutes les communications sur réseau IP sécurisées TLS v1.2 avec certificats entre le serveur et les UTL d'une part et les postes clients d'autre part

DES AUTOMATES NG :

- ▶ Gérant des informations de panne ou de malveillance : arrachement, ouverture de coffret, défaut de communication et d'alimentation (secteur, batterie basse, chargeur), et protégés contre les erreurs et le sabotage grâce aux entrées équilibrées, sorties et bus RS485, protégés contre les courts-circuits, surtensions et inversions de polarités

DES UTL TILLYS NG AVEC :

- ▶ Un Web serveur embarqué HTTPS pour la configuration locale
- ▶ Une compatibilité 802.1X (Radius), et SNMPv3 pour une surveillance des états systèmes & alarmes métiers par la DSI, I.T du client final
- ▶ Une architecture modulaire 3 bus de terrain RS485 certifiés ANSSI et sécurisés AES 128 bits, sur lesquels sont connectés les modules déportés contrôle d'accès et intrusion permettant de
 - Réduire les coûts en récupérant au mieux le câblage existant
 - Certifier vos câbles existants
 - Avoir au choix une architecture distribuée ou centralisée
- ▶ Une protection des attaques par déni de service (DoS) par le Firewall

DES MODULES DE PORTE MLP AVEC :

- ▶ Une communication RS485 sécurisée AES128 bits avec les lecteurs transparents
- ▶ Un composant HSM certifié ANSSI EAL5+ nativement intégré qui est le crypto-processeur et coffre-fort contenant les clés de l'application « contrôle d'accès » des badges
- ▶ Des applets (paramétrage) pour s'adapter à la charte des badges du client et piloter les LED et buzzers des lecteurs transparents. Des droits opérateurs sécurisent l'accès au paramétrage des applets MLP / MLD

DES LECTEURS :

- ▶ Lecteurs clavier certifiés ANSSI selon architecture 1 dits « lecteur transparent » (aucune clé badge stockée dans le lecteur) pour gérer vos badges DESFIRE hautes sécurités
- ▶ Des lecteurs biométriques transparents EVOLUTION gérés en protocoles SCCPv1, SCCPv2 certifié ANSSI depuis les modules MLP qui gèrent de nouveaux états (badge OK mais pas empreinte, timeout) et le doigt sous contrainte

LE CLIENT FINAL MAITRISE SEUL SES CLES :

- ▶ Pour toutes les applications du badge (accès, restaurant,...), qui sont saisies ou créées (cérémonie des clés) par lui-même sur une seule IHM dédiée pour cet objectif, **KSM NG**, et sont sauvegardées facilement dans un conteneur numérique sécurisé AES256 bits placées sur **MICRO-SESAME v2018**. Toutes ces clés ne sont jamais visibles des tiers qui conçoivent, intègrent ou maintiennent le système. 1 seule cérémonie des clés est nécessaire pour l'intégrateur et le client final

CLES & APPLETS :

- ▶ Téléchargement des clés & applets sécurisé, centralisé depuis le serveur, ou **KSM NG**, jusqu'aux modules HSM des MLP/D pour faciliter la diffusion des clés et pouvoir éventuellement les changer dans tous les modules depuis le système central, comme demandé par l'ANSSI
- ▶ Un principe de diversification des clés, conforme au standard AN10922, permet au client final d'avoir des clés différentes par badges et de choisir sa formule par un padding personnalisable

LA GAMME NG :

- ▶ **TILMAN NG**, utilitaire dédié de **MICRO-SESAME**, offre une vue centralisée de tout le parc des automates de la gamme NG (UTL, module) pour lire et mettre à jours leurs versions de firmware via des téléchargements globaux. Il permet donc de gérer facilement la maintenance corrective et évolutive depuis un poste central mais également une aide à la mise en service par des tests, diagnostics de câblage des entrées détecteurs
- ▶ La sécurité de la **TILLYS NG** certifiée en contrôle d'accès est également active en intrusion vous offrant une centrale intrusion cyber sécurisée
- ▶ Les firmwares des automates de la gamme NG sont signés pour garantir leurs intégrités.

RENFORCEMENT DE LA SECURITE

- ▶ Renforcement de la sécurité en supprimant le code de Reverse DNS (impact sur le contenu des certificats)
- ▶ Mots de passe opérateur protégés en BDD HASH SHA-512 + SEL de 512 caractères aléatoires
- ▶ Portail **WEB-SESAME** protégé contre les attaques "CSRF"
- ▶ Un requêteur web avec des requêtes en bibliothèque sur des comportements suspects (tentatives multiples d'accéder à des zones interdites,...). Liste éditable et rapport automatique

HAUTE ADAPTABILITE A VOTRE ENVIRONNEMENT INFORMATIQUE, S.I

Selon la taille de votre système, des préconisations machines et logicielles vous sont conseillées.

MICRO-SESAME suit les évolutions des versions d'OS et de Base De Données pour rester compatible avec les derniers environnements S.I.

Avant toute installation système ou migration, vous pouvez vous référer à des documents spécifiques, mis à jour régulièrement et disponibles auprès de votre interlocuteur TIL habituel.

COMPATIBILITE AVEC LES DERNIERS OS ET BDD :

- ▶ Serveur : de Windows 10 PRO ou Entreprise (64 bits) pour les petits systèmes à Windows Server 2019 Standard ou Essential Edition (64 bits)
- ▶ Client lourd : Windows 10 Pro ou Entreprise 64 bits
- ▶ Base de données : SQL Serveur 2014 à 2017 (64 bits)

ADAPTE AUX INFRASTRUCTURES « CLIENT LEGER » :

- ▶ Compatibilité avec les solutions RDS (ex TSE)/ Citrix
- ▶ Pas d'application **MICRO-SESAME** à installer sur les postes
- ▶ Connexion depuis n'importe quel poste du réseau
- ▶ Fonctionnement en licence flottante / connexions simultanées



PORTAIL WEB WEB-SESAME POUR LES FONCTIONS ACCESSIBLES SUR L'INTRANET DU CLIENT :

- ▶ Ecrans auto-adaptatifs (résolution et orientation) au format (smartphone, tablette, PC)
- ▶ Ergonomie optimisée pour une utilisation simplifiée sur tablettes et smartphones (Auto-complétion des champs, affichage photo, boutons à cocher)
- ▶ Fonctions disponibles pour une grande population :
 - Gestion des rendez-vous, visites, visiteurs
 - Gestion des identifiés
 - Requêteur, Historique états/alarmes

WEB-SESAME

COMPATIBLE SUR UN ENVIRONNEMENT VIRTUEL TYPE VMWARE :

- ▶ Mutualisation des serveurs, économies d'énergie
- ▶ Licence logicielle compatible avec cet environnement
- ▶ Sur machine physique dédiée ou datacenter
- ▶ Redondance possible par l'environnement VM module HA



OUVERT A VOS CHOIX D'ARCHITECTURE & RESEAU :

- ▶ Architecture n tiers (BDD, serveur d'applications, serveur WEB)
- ▶ Compatible VPN, VLAN
- ▶ Transmissions email/SMTP,
- ▶ UTL TILLYS-NG compatible 802.1x, SNMPv3, IPv6 ready, Host Name possible

REDONDANCE MATERIELLE / SYSTEME :

- ▶ Compatibilité avec la solution de redondance à chaud SAFEKIT
- ▶ Interface pré-paramétrée pour **MICRO-SESAME**



PACKAGING D'INSTALLATION, MIGRATION, RESTAURATION, INTEGRE ET SIMPLIFIE :

- ▶ Installation serveur et postes clients **MICRO-SESAME** facile avec tous les composants inclus dans le package d'installation
- ▶ Outils de migration du serveur et poste client disponible
- ▶ Mise à jour semi-automatique des postes clients lourds après le serveur
- ▶ Toutes les applications « Système » en Service
- ▶ Sauvegarde, back up automatique de la BDD selon chemin prédéfinie. Outil de restauration

GESTION DES DROITS OPERATEURS DEPUIS L'A.D DU CLIENT VIA LDAP (VOIR CHAPITRE DEDIE)

HAUTE DISPONIBILITE & PERFORMANCES

L'architecture a été pensée pour vous offrir une haute disponibilité & performance grâce à :

- ▶ Un fonctionnement autonome de chaque **TILLYS NG**, avec ses modules d'extension et périphériques, sans réseau Ethernet et/ou serveur, et qui garde un historique des 10 000 derniers événements quand la communication est perdue avec **MICRO-SESAME**, automatiquement téléchargé quand rétablie
- ▶ Une communication directe inter UTL **TILLYS NG** sur IP (antipassback) sans besoin du serveur
- ▶ La **TILLYS NG** traite simultanément de nombreux badgeages chacun en moins de 500 ms, même avec les lecteurs transparents et badges hautes sécurités, grâce au crypto-processeur HSM présent sur tous les modules gérant ses lecteurs pour un déchiffrement en parallèle
- ▶ La redondance du serveur possible avec l'environnement virtuel du client ou la solution SAFEKIT validée et distribuée par TIL
- ▶ Une architecture informatique tiers possible pour démultiplier les puissances machines
- ▶ Site web 24/7 de récupération de licences provisoires en cas de crash du serveur
- ▶ Des automates NG de conception industrielle avec un MTBF de 20 ans et un MTTR de 5 mn
- ▶ Téléchargement parallélisé vers tous les UTIL depuis le serveur

ASSISTANCE & ADAPTABILITE AUX CHARTES D'ENCODAGE DES BADGES NIVEAU ANSSI

La solution TIL permet une haute sécurité et une grande adaptabilité projet dans la gestion des clés et du mapping du badge selon la charte d'encodage du client final.

La société TIL TECHNOLOGIES offre un service d'assistance au client final pour l'aider à élaborer une charte d'encodage des badges multi-applications, conforme ANSSI, haute sécurité, et flexible pour permettre au mieux l'utilisation des applications prévues ou futures avec son badge.

RICHESSE FONCTIONNELLE EN SURETE ET SMART BUILDING

MICRO-SESAME est un système ouvert et évolutif. Il supervise ses propres automates et les périphériques, capteurs et actionneurs qui y sont raccordés mais également des systèmes ou produits tiers (Automates industriels, climatisation, chauffage, incendie, etc.) qui y sont interfacée selon plusieurs protocoles disponibles (MODBUS, OPC UA, etc).

MICRO-SESAME intègre une grande richesse fonctionnelle en sûreté et GTB car couvre plusieurs métiers (contrôle d'accès, intrusion, supervision,...) et plusieurs marchés (industrie, tertiaire, sites sensibles, infrastructure, collectivités,...). Il permet d'adapter sa configuration aux besoins exacts de l'utilisateur final et d'être évolutif si besoin. Voici une liste non exhaustive des principales fonctions :

GESTION DES PERSONNES & OPERATEURS

GESTION DES IDENTIFIES (personnes, visiteurs, opérateurs) et de leurs données personnelles : identités avec des champs préexistants (nom, prénom,...) et personnalisables ou à listes déroulantes prédéfinies, durée validité, attribution de fichiers joints possible, information sur du dernier badgeage, notion de « statut d'identifié » ("VIP", ...)

ATTRIBUTION DE MULTIPLES IDENTIFIANTS (badge, n° plaque voiture, badge virtuel, QR code,...) par personne, jusqu'à 4 technologies par serveur parmi N, et 99 identifiants par technologie (ex : 2 badges, 3 voitures)



EDITEUR DE CREATION DE FONDS GRAPHIQUES DE BADGE INTEGRE : textes fixes et variables, photo, QR code, image fixe comme logo, ...), recto / verso, couleur, ... pour personnaliser les badges

GESTION DE PLUSIEURS MAPPING / ENCODAGE de badge hautement personnalisable et sécurisé

PERSONNALISATION GRAPHIQUE, ENCODAGE MULTI-APPLICATIONS sécurisé (accès, restaurant, gestion horaire, ...) et enrôlement des badges en une seule opération sur l'imprimante pour des productions de badges rapides, faciles, sécurisés. Editeur fond de badge et d'encodage intégré

SYNCHRONISATION AUTOMATIQUE possible des personnes créées & badges multi-applications encodés sur **MICRO-SESAME** vers les applications Restaurant, Gestion horaires, ...

VOIR LES CHAPITRES GESTION DES OPERATEURS, RGPD, ENCODAGE & PERSONNALISATION DES BADGES

CONTROLE D'ACCES ONLINE ET OFFLINE

- ▶ Gestion des droits d'accès individuels, par profil, avec date de début et fin. Les droits d'accès sont attribués aux identifiés, indépendamment des identifiants ou des lecteurs online / offline
- ▶ Modification groupée des droits d'accès sur les personnes issues d'une recherche multicritères
- ▶ Attribution automatique des droits d'accès, sur les personnes importées d'une base RH, grâce à des règles prédéfinies selon tous les champs des identifiés (Ex : le profil 1 au service 1)
- ▶ Téléchargement automatique vers les UTL de la liste des personnes autorisées dès validation
- ▶ Gestion ascenseur avec filtrage des étages autorisés par personne, plage horaire, niveau crise. Appel ascenseur prioritaire pour le personnel concerné (CHU,...)
- ▶ Compatibilité avec différentes technologies et tous types de lecteurs de contrôle d'accès :
 - Lecteurs de badges de proximité 125 kHz et 13.56 MHz (MIFARE, DESFIRE, ICLASS, ...)
 - Lecteur mobile MOBILIS 13.56 MHz (MIFARE, DESFIRE)
 - Lecteurs longue distance, Bluetooth, badges actifs ou télécommande
 - Lecteurs de plaques minéralogiques, biométriques ou QR code affiché sur smartphone
 - Cylindres et béquilles mécatroniques (online et offline),...
- ▶ Commandes de différents accès contrôlés ou actionneurs (barrière, serrure électrique, tripodes, afficheurs, sirènes, éclairages, ...)
- ▶ Grande adaptabilité du mode opératoire des accès : SAS à 2/3/X portes, simple ou double sens, lecteur ou lecteur clavier (badge + code), lecteurs mobiles, simple ou double badgeage pour zones à risques avec des personnes de catégories différentes possibles, ...
- ▶ Fonctions avancées qui ont toutes un impact cumulatif sur les droits d'accès :
 - Contrôle des temps de repos
 - Habilitation (électrique, médicale, ...) par personne et accès, avec dates de début et fin
 - Niveau de crise parmi les 7 possibles (vigipirate) attribué par personne, et à chaque accès et étages sur commande opérateur sur synoptique ou asservissement. Modes opératoires au choix selon crise : badge -> badge, badge + code, double badgeage
 - Gestion anti-retour géographique & temporel, local ou global, selon dérogation APB
 - Accès sous contrainte avec badge + code spécifique
 - Notion de dépendance : badgeage sur lecteur X obligatoire avant celui du lecteur Y

FONCTIONS SPECIALISEES ASSOCIEES AU CONTROLE D'ACCES

GESTION DES VISITEURS avec un workflow complet de la création des visites & visiteurs, la validation des visites jusqu'à l'accueil sur site

GESTION DES PARKINGS et zones sensibles avec comptage par zone, seuil possible d'accès par catégorie de personne

ASSISTANCE PLAN EVACUATION POI (exercice ou réel) avec IHM dédié affichant la liste, compteur, localisation des présents de chaque zone sécurisée / à risque avec photo, trombinoscopes, et impression pour secouristes

GESTION MULTISITES & MULTILOCATAIRES avec les notions de site (matériel), entité (personnes), classification (lecteur), périmètre (clés), et de gestion des opérateurs

PCVA : Contrôle vidéo des accès par un opérateur qui, après badgeage, autorise l'accès ou est juste informé et accès selon droits d'accès

HABILITATION : (électrique, médicale, ...) par personne et accès, avec dates de début et fin

CONTROLE DES TEMPS DE REPOS

GESTION DE RONDES : parcours centralisés avec des badges et lecteurs de badges

GESTION DE LA QUARANTAINE avec **TILLYS NG** (chemin et durée entre zones configurables)

INTRUSION

GESTION DE TOUTES INFORMATIONS DE DETECTION de type contact (radars, détecteurs,) raccordées sur :

- Les entrées équilibrées, TOR de nos automates
- Les transpondeurs **EQUILOCK** en bus avec notre module **EQUILOCK**
- Des automates, systèmes tiers interfacés à notre système par MODBUS, OPC,...

ou provenant des solutions **SORHEA** via leur interface **MAXIBUS** avec notre système ou provenant d'analyse d'image de VMS via leur interface SDK avec notre système

GESTION ET ATTRIBUTION CENTRALISEE DES DROITS intrusions de toutes les centrales **TILLYS** sur **MICRO-SESAME** : simplicité, rapidité, flexibilité. Ainsi les usagers peuvent gérer plusieurs zones intrusions sur plusieurs centrales intrusion mais que celles autorisées

MISE EN/HORS SURVEILLANCE DES ZONES intrusion sur plage horaire, par clavier **TACTILLYS NG** multi-zones avec éjection auto/manu/interdite, comptage, accès autorisé, asservissements (combinatoire et séquentiel) définis par projet (ex : triple badgeage sur lecteur mettra en surveillance)

INTERACTION NATIVE & COMPLETE avec le contrôle d'accès car géré par le même UTL **TILLYS** Automatismes, actions avec les autres systèmes (vidéo, sirène, éclairage, ...)

AUTOMATISMES, actions avec les autres systèmes (vidéo, sirène, éclairage, ...)

TRANSMISSION DES ALARMES INTRUSION (y compris contrôle d'accès & GTB) vers un télésurveilleur par IP avec protocole standardisé « TIP » de TIL qualifié chez ESI, Azur soft

SUPERVISION & HYPERVISION SURETE ET SMART BUILDING

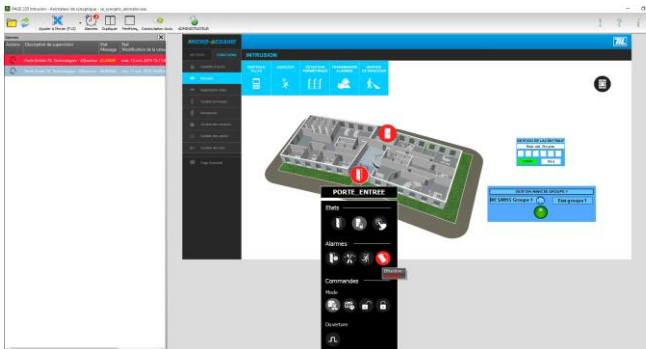
ERGONOMIE GENERALE DES INTERFACES IHM

étudiée pour offrir une exploitation facile

MONITEUR D'ÉVÉNEMENTS, alarmes temps réel avec recherche rapide & filtres multicritères

ÉDITEUR & ANIMATEUR DE SYNOPTIQUES intégré nativement rapidement configurable et hautement personnalisable avec la notion d'objets, bibliothèques d'objets, zoom des synoptiques, ...

SUPERVISION AVEC ANIMATION GRAPHIQUE DE PLANS & synoptiques avec symboles animés



SUPERVISION EN TEMPS REEL D'ALARMES DE CONTROLE D'ACCES, intrusion, incendie, techniques (défauts ascenseurs, défauts climatisation, défaut disjoncteurs, ...) ... avec acquittement, consignes associées configurables par alarmes et selon le profil opérateur

SURVEILLANCES DES ZONES AVEC COMPTAGE, POI avec IHM dédié affichant la liste, compteur, localisation des présents de chaque zone

INTERFACES ENTRE MICRO-SESAME et des VMS du marché (MILESTONE, GEUTEBRUCK, **VIDEOWAVE**, ...), la fonction intégrée **VISIOSESAME** permet d'offrir :

- ▶ Une supervision de flux vidéo simultanés de plusieurs VMS en parallèle
- ▶ Une visualisation d'images live sur sélection d'icônes sur synoptiques d'exploitation, sur alarmes, un pilotage des dômes et des murs d'images
- ▶ Des enregistrements vidéos automatiques aux VMS sur alarmes intrusion, accès, ...
- ▶ Une relecture des enregistrements vidéo sur VISIOSESAME associés aux alarmes recherchées dans l'historique de MICRO-SESAME
- ▶ Une intégration des alarmes vidéo (analyse d'image) et des défauts (défauts caméras,...) de VMS

LARGE POSSIBILITE D'INTERFAÇAGES & PASSERELLES MATERIELS OU LOGICIELS

LES CONNECTEURS POSSIBLES DE NOTRE SYSTEME MICRO-SESAME :

- ▶ Base usagers & gestion visiteur : Web service API REST, CSV
- ▶ Gestion opérateur A.D : LDAP
- ▶ Superviseur I.T : SNMPv3 (depuis UTL TILLYS NG)
- ▶ Hyperviseur : OPC UA
- ▶ Automates, système tiers : MODBUS IP, passerelle TEXT/ASCII,
- ▶ SDK VMS, SDK divers, Passerelles spécifiques sur projets, ...

EXEMPLE DES PASSERELLES REALISEES SUR NOTRE SYSTEME MICRO-SESAME :

- ▶ Hyperviseur bâtiment : PRYSM, PC VUE, PANORAMA....
- ▶ GTB : PRYSM, PC VUE, PANORAMA....
- ▶ Réservation de salle et ressources : ASW, Planitec ...
- ▶ Gestion de flux camion : EASYPROG, STACKR
- ▶ Vidéo : MILESTONE, GEUTEBRUCK, VIDEOWAVE, GENETEC
- ▶ Intégration du Plug-in MILESTONE ACCESS CONTROL, pour supervision du contrôle d'accès TIL dans l'interface de supervision X-PROTECT de MILESTONE
- ▶ Interphonie : COMMEND en IP / Import des abonnés, Appels, Notification d'appels (avec distinction entre normal et urgent), Transfert d'appel de nuit, possibilité de connexion au serveur d'interphonie
- ▶ Armoire à clés DEISTER : Synchronisation des identifiés avec le logiciel COMMANDER 4
- ▶ Centrale intrusion NFA2P GALAXY via le protocole natif IP Galaxy
- ▶ Détection périmétrique SORHEA via le protocole MAXIBUS de **SORHEA**
- ▶ Centrales incendie
- ▶ Matrices et multiplexeurs vidéo AVIGILON
- ▶ Annuaires RH : CANIF de SNCF, BDRS de Société générale, STITCH de la DGAC, ...
- ▶ Messagerie SMTP pour les emails
- ▶ Biométrie : MORPHO-BRIDGE avec MORPHOMANAGER d'IDEMIA

SUPERVISION DE L'ENERGIE

- ▶ Suivi des consommations
- ▶ Visualisation des puissances totales ou partielles consommées
- ▶ Dérogation de zones par niveau de priorité en fonction de la puissance souscrite
- ▶ Programmation annuelle des rythmes de fonctionnement des zones pilotées (jusqu'à 3 programmes annuels)

ASSERVISSEMENT DE L'ECLAIRAGE ET AUTRES ACTIONNEURS

- ▶ Commande Marche/Arrêt avec possibilité de programmation horaire
- ▶ Relance ou dérogation par minuterie de durée paramétrable (salles à occupations irrégulières)

ASSERVISSEMENT DU CHAUFFAGE, VMC, CLIMATISATION

- ▶ Commande Marche/Arrêt des régulateurs avec possibilité de programmation horaire
- ▶ Définition des consignes de température et des régimes de fonctionnement : hors-gel, réduit, économique, confort...
- ▶ Relevés de seuils haut, bas de températures

ASSERVISSEMENT DE L'EAU CHAUDE SANITAIRE ECS

- ▶ Commande Marche/Arrêt avec possibilité de programmation horaire
- ▶ Programmation des modes de fonctionnement : Automatique, Relance manuelle ou programmée

CAPACITES DU SYSTEME

Paramétrage Matériel

Postes clients connectés en simultané	499
Automates programmables (TILLYS NG, TILLYS V2, UTIL V2, PULSE)	10 000
Automates sur une même ligne IP	255
Drivers (lignes) supportés	128
Lecteurs de badges	20 000
Enregistreurs vidéo	256

Paramétrage Contrôle d'accès

Identifiés (usagers, opérateurs, visiteurs)	Illimité
Identifiants (badge, n° de plaque,...)	Illimité
Sites	256
Entités	256
Groupes de lecteurs	Illimité
Lecteurs par groupe	1 024
Zones d'accès	128
Habilitations	256
Points de contrôle visuel des accès	256
Parcours	64

Paramétrage Supervision

Voies, propriétés totales	40 960
Voies, propriétés par ligne	8 192
Catégories de propriétés	64
Totalisateurs	2 048
Propriétés dans une chaîne de formatage	16

Paramétrage Exploitation

Opérateurs (centralisé)	Illimité
Utilisateurs Intrusion TILLYS V2 ou TILLYS NG (local)	150

Contrôle d'Accès (fiche identifiés/identifiants)	
Technologies lecteurs associables à une fiche Identifié	4
Nombre d'identifiants par technologie lecteur	99
Longueur code badge (harmoniser avec les pilotes de l'UTL)	32 car.
Longueur code site (harmoniser avec les pilotes de l'UTL)	32 car.
Champs définissables (taille, casse, longueur, saisie libre, obligatoire, assistée,...)	16
Champs téléchargeables dans un UTL (sans dépasser 20 caractères)	Nom, prénom + 6 premiers

Plages horaires et jours fériés	
Plages horaires par site / UTL (UTL est mono-site mais un site peut avoir X UTL)	128
Plages horaires totales sur serveur central multisites	256
Jours par plage	9 (semaine + J fériés + J exceptionnels)
Créneaux par jour	4
Créneau mini	1 min
Jours exceptionnels	32

Historiques	
Evènements dans l'historique	Illimité (selon BDD)
Nombre maxi d'évènements par requête historique	Illimité
Durée de rétention (paramétrable, par exemple pour respect les 3 mois CNIL)	30 j. par défaut

Capacités matérielles des automates	
Identifiants téléchargeables – UTIL, PULSE, TILLYS V2	10 000, 19 000, 30 000, 40 000 selon firmware
Identifiants téléchargeables – TILLYS NG	10 000 natif, jusqu'à 600 000 sur option XL
Lecteurs par automate – UTIL, PULSE, TILLYS V2	2, 8 ou 16
Lecteurs par automate – TILLYS NG	8, 16 ou 24

CONFORMITE RGPD & CNIL

GESTION FINE DES DROITS D'UTILISATION DE MICRO-SESAME

MICRO-SESAME est conforme aux réglementations RGPD & CNIL par les fonctions ci-dessous disponibles dans chacun des grands thèmes de la RGPD.

Il convient ensuite au client final de :

- ▶ Appliquer, et mettre en œuvre les fonctions ci-dessous disponibles dans MICRO-SESAME
- ▶ Définir quelles données sont à enregistrer dans les champs libres des fiches identifiés (permanents, temporaires, visiteurs)
- ▶ Définir les opérateurs et leurs droits d'accès aux données
- ▶ Où est installée la base de données SQL où sont enregistrées ces données identifiées et qui a accès à la base de données SQL
- ▶ Respecter les procédures CNIL (par exemple pour la déclaration d'un contrôle d'accès sur le site et la biométrie en particuliers)

CONTROLE D'ACCES DES UTILISATEURS (DONT DROIT OPERATEUR FIN POUR LA GESTION DES FICHES VISITEURS)

- ▶ L'accès aux données personnelles, dans les fiches identifiées, filtrés par des droits opérateurs selon les champs et entités (catégorie ou site de personnes) autorisées
- ▶ L'accès aux données autorisées peut être en lecture seule ou/et écriture
- ▶ On peut définir quelles sont les champs obligatoires dans les fiches visiteurs à la création (≠ des fiches permanents)
- ▶ Sans le droit opérateur des visiteurs « profil GESTION-RDV », cet opérateur pourra :
 - Rechercher un visiteur dans la base des visiteurs existant par autocomplétions, pour éviter les doublons, et ne voir que les champs nom, prénom, société des visiteurs
 - Créer un visiteur complet avec tous les champs (naissance...) s'il n'existe pas
 - Dans ces 2 cas, ensuite, il ne pourra pas éditer, modifier, consulter les autres informations de la fiche visiteur

Si droit activé, il pourra éditer, modifier, consulter toutes les informations de la fiche visiteur

TRAÇABILITE : NATURE DES TRACES, LES DONNEES ENREGISTREES ET LEUR DUREE DE CONSERVATION

- ▶ Toutes les modifications, consultations, suppressions des données des personnes sont tracées, impossible d'agir sur Micro Sésame sans avoir la trace
- ▶ La durée de conservation des données est paramétrable
- ▶ Effacement manuel des données des personnes ne faisant plus parties de la société
- ▶ Import usagers avec base RH automatique minimisant les manipulations humaines

SAUVEGARDE DES DONNEES

- ▶ Sauvegarde automatique périodique de la BDD sur disque sans manipulation humaine
- ▶ Archivage périodique des historiques possible

CHIFFREMENT DES DONNEES

- ▶ Sécurisation des flux d'accès : Postes clients lourds en TLSv1.2, légers en Https
- ▶ Mots de passe opérateur protégés dans BDD HASH SHA-512 + SEL de 512 caractères aléatoires
- ▶ Portail WEB-SESAME protégé contre les attaques "CSRF"
- ▶ MICRO-SESAME permet d'anonymiser les données de la BDD avant de la transmettre à un tiers pour debug, test migration

MESURES DE PROTECTION DES LOGICIELS & MAINTIEN EN CONDITION DE SECURITE

- ▶ Mises à jour, correctifs de sécurité fournis par forfait AMCO PREMIUM de TIL qualifié ANSSI

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

- ▶ Non requise pour la mise en place d'un dispositif de sécurité par badge sans biométrie, selon pdf Liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données n'est pas requise à télécharger au lien suivant
- ▶ <https://www.cnil.fr/fr/ce-quel-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-aipd>

DÉCLARATION CNIL POUR LE CONTRÔLE D'ACCÈS ET EN PARTICULIER POUR LA BIOMÉTRIE

TIL TECHNOLOGIES et sa solution **MICRO-SESAME** ne gèrent aucun élément biométrique (empreinte, minutie,...) directement et ne sont donc pas concernés par les déclarations d'utilisation de la biométrie AU52 (1:1) & AU53 (1:N).

La solution **MICRO-SESAME** intègre des lecteurs biométriques du marché comme ceux d'IDEMIA et de STID. Nos automates ne lisent que l'identifiant (du badge ou d'une base locale) envoyé par ce lecteur et en aucun cas l'empreinte. Seuls ces constructeurs de lecteurs gèrent les éléments biométriques. Ils ont leurs propres outils d'enrôlement biométrique (SECARD BIO, MORPHOMANAGER) et doivent respecter les exigences techniques des déclaration d'utilisation de la biométrie AU52 (1:1) & AU53 (1:N).

Pour mémoire, voici les procédures suivantes à établir et respecter par le client final :

- ▶ Déclaration CNIL contrôle d'accès, hors biométrie, norme simplifiée NS-42
 - Eléments d'identification : 5 ans après le départ du salarié : Suppression manuelle des usagers sur **MICRO-SESAME**
 - Eléments relatifs aux déplacements des personnes (3 moi)s : Profondeur historique paramétrable sur **MICRO-SESAME**: 3 mois ou autre
- ▶ Déclaration d'utilisation de la biométrie AU52 (1:1) & AU53 (1:N). La gestion des empreintes devra être conformes en particulier sur AU53 plus exigeante que AU52 simple et facile

GESTION DES OPERATEURS

GESTION FINE, SECURISEE DES DROITS D'UTILISATION DE MICRO-SESAME

Un opérateur est une personne physique, autorisée à utiliser l'interface de supervision **MICRO-SESAME**. Cet utilisateur, selon sa fonction, son niveau hiérarchique ou sa situation géographique, peut accéder à la totalité ou à une partie des différentes fonctions, données disponibles dans **MICRO-SESAME**.



Pour affecter à chaque opérateur uniquement les droits qui lui sont nécessaires, et le faire rapidement par type d'opérateurs, **MICRO-SESAME** intègre une notion de "profils opérateurs". Ces profils sont définis par un système de cases à cocher représentant les droits accessibles avec finesse dans chacune des grandes fonctions suivantes et en visualisation, création, modification, suppression :

- ▶ Droits liés au contrôle d'accès
- ▶ Droits liés à l'exploitation
- ▶ Droits liés à l'historique
- ▶ Droits liés aux identifiés (dont quelles données personnelles)
- ▶ Droits liés aux visites
- ▶ Droits liés à la supervision (dont catégories des propriétés par ex : accès, intrusion, incendie, ..., masque / niveau d'acquittement des alarmes)
- ▶ Droits liés au paramétrage (dont filtrage pour les projets multi-sites selon sites lecteurs, entités identifiés, classification de chaque accès dont la finesse est supérieure à la notion de site)
- ▶ Droits liés à la sécurité

Vue la richesse et finesse de ces profils / droits opérateurs, il existe des documents spécifiques mis à jour régulièrement, auquel vous pouvez vous référer et qui sont disponibles auprès de votre interlocuteur TIL habituel.

Pour chaque opérateur créé, il suffit ensuite de lui attribuer un ou plusieurs profils opérateurs pré définis.

La gestion des droits est sécurisée, facile, prévue pour une grande population, et simplifie l'exploitation la maintenance et la mise en œuvre car :

- ▶ Une modification des profils opérateurs modifie automatiquement tous les opérateurs qui y sont associés
- ▶ On peut associer un ou plusieurs profils à l'opérateur pour permettre à ce dernier de se mettre dans les mêmes conditions d'un autre opérateur qu'il souhaiterait aider par exemple
- ▶ Un opérateur est d'abord un "Identifiés" qui a des droits d'accès physique et que l'on a déclaré en plus comme opérateur du logiciel MICRO-SESAME. Cela évite une double saisie des données personnelles et des fiches
- ▶ Hiérarchie entre opérateurs : Afin de modifier les droits des opérateurs, le niveau hiérarchique de l'opérateur réalisant la modification doit être supérieur aux opérateurs modifiés (niveau hiérarchique et profil)
- ▶ Les mots de passe opérateur sont protégés en BDD par un HASH SHA-512 + SEL de 512 caractères aléatoires
- ▶ Traçabilité et historique des actions opérateurs (avec valeurs/champs modifiés) qui est une exigence réglementaire dans de nombreux secteurs d'activité (Agro-alimentaire, pharmaceutique, transport, nucléaire,)
- ▶ Gestion centralisée des droits opérateurs dans MICRO-SESAME pour tous les types de postes clients (lourds, léger, WEB)
- ▶ Un login et mot de passe par défaut est donné à chaque opérateur qui devra les modifier à sa première connexion et qui seront connus que de lui
- ▶ Déconnexion automatique des opérateurs WEB-SESAME après un temps d'inutilisation trop long ou au redémarrage du serveur WEB apache.

Annuaire LDAP/Active Directory

La gestion des opérateurs est possible sur le système MICRO-SESAME ou depuis un annuaire centralisé Active Directory (A.D) du client final géré par son service I.T et interfacé à MICRO-SESAME par une passerelle au protocole LDAP. Cela permet :

- ▶ D'avoir un seul annuaire référent pour tous les utilisateurs des applications d'une société qui simplifie la création, modification, suppression des opérateurs. La mise à jour est facilitée et automatique.
- ▶ D'attribuer dans cet A.D le ou les profils opérateur prédéfinis dans MICRO-SESAME qui portent le métier. Prise en compte du multi-profil opérateur avec l'authentification LDAP
- ▶ De gérer des mots de passe complexes par la puissance de l'A.D
- ▶ De gérer les opérateurs en mode sécurisé avec LDAPs

GESTION MULTI-SITES / MULTI CLIENTS

EXPLOITATION GEOGRAPHIQUE OU ORGANISATIONNELLE

MICRO-SESAME permet de gérer jusqu'à 256 sites différents à partir du même système. Cette fonction est intéressante dans plusieurs cas :

- ▶ La gestion de bâtiments disséminés géographiquement : réseau d'agences, bâtiments d'une collectivité locale, sites de production... depuis un seul serveur central.
- ▶ La nécessité, au sein d'un même site, d'une maîtrise de droits différents au niveau de chaque service.
- ▶ Le partage d'un même bâtiment ou tour par plusieurs sociétés, locataires et différencier les accès communs et ses accès propres.
- ▶ Le choix au niveau des serveurs : 1 serveur national pour tous les sites ou 1 serveur par site selon les contraintes (qualité du réseau) et organisation prévues (centralisée, décentralisée,)
- ▶ Le choix au niveau de l'administration des badges avec :
 - Personnalisation & encodage centralisé au siège
 - Encodage générique centralisé au siège et personnalisation sur chaque site
 - Personnalisation & encodage sur chaque site

L'utilisation de la fonction multisites exige un gestionnaire / administrateur principal afin :

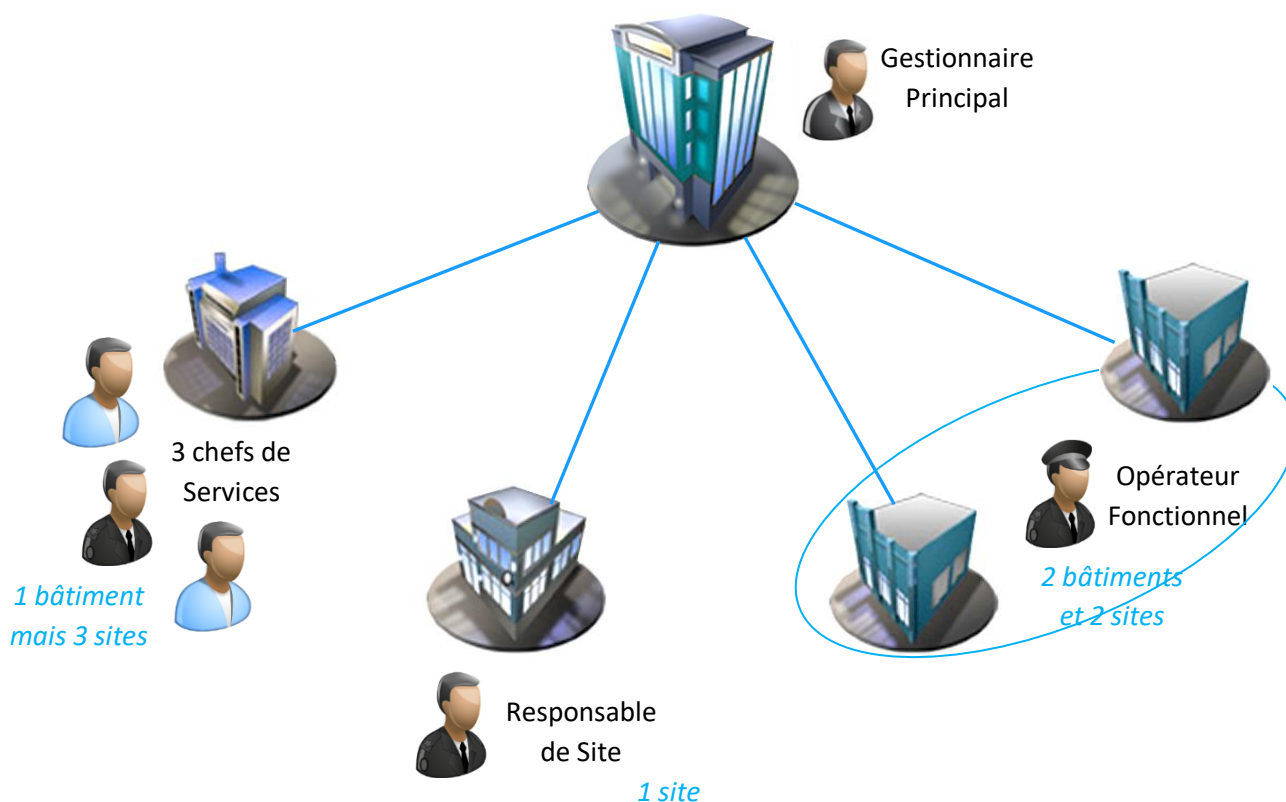
- ▶ D'administrer la base de données unique centralisée
- ▶ De créer des gestionnaires par site, services, société, ... qui peuvent recevoir sa délégation, grâce à la notion de hiérarchie d'opérateur, pour gérer finement chaque site dont :
 - Les droits accès de leur personnel / entité sur les lecteurs de leur site et, s'il y en a, sur les lecteurs communs (accueil, parkings, ascenseurs...)
 - La consultation des historiques et mouvements de leur personnel
- ▶ Définir les sites, le site le plus petit étant un UTL :
Il faut bien prendre en compte que l'UTL est mono-site dans l'architecture, le choix et localisation des UTL et l'impact câblage associé
- ▶ Définir les entités d'affectation des personnes
- ▶ Définir les droits opérateurs et les opérateurs par site selon l'organisation & procédures
- ▶ Ils ne verront ni les lecteurs & droits d'accès des autres sites, ni les personnes et leur historique des autres entités

Chaque site possède 128 plages horaires indépendantes, utilisées soit dans le cadre du contrôle d'accès, soit de l'intrusion, soit dans le cadre de la gestion technique des bâtiments (système d'alarme, arrosage automatique...).

Le système central peut créer jusqu'à 256 sites et 256 plages horaires au total pour tous les sites

Pour la sécurité des clés des badges, l'utilitaire KSM NG, les outils d'encodage et les UTL NG permettent à l'officier central de sécurité de gérer, si besoin, des clés badges différentes par site avec la notion de périmètre, comme demandé dans le guide ANSSI.

Il existe un document spécifique sur les architectures multisites possibles qui est disponible auprès de votre interlocuteur TIL habituel.



GESTION DES ACCES

PROFILS, HORAIRES, HABILITATIONS, LECTEURS, ZONES...

La fiche Identifié/Identifiants regroupe et définit :

LES INFORMATIONS DE L'IDENTIFIE : dates de validité, société, service, coordonnées, ainsi que 16 libellés personnalisables supplémentaires. Des pièces jointes peuvent également être associées (contrat de travail, photo,)

LES IDENTIFIANTS DE L'IDENTIFIE : jusqu'à 4 technologies différentes d'identifiants sont possibles (ex : badge 13,56 MHz, badge 125kHz, code clavier, plaque minéralogique, QRCode...), pour chaque Identifié on peut stocker jusqu'à 99 identifiants par technologie. Les identifiants peuvent avoir plusieurs statuts : cassé, perdu, volé, non rendu pour expliquer le motif d'interdiction. Ainsi, on ne crée qu'une seule personne même avec pour plusieurs identifiants

DES ATTRIBUTS SPECIFIQUES : anti-retour, liste noire (pour surveillance spécifique), niveau d'accréditation (mode crise), possibilité de recevoir des visites, d'être accompagnant, ...

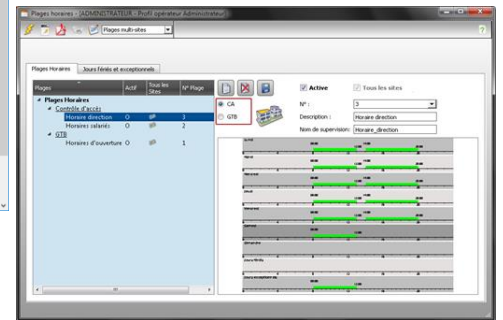
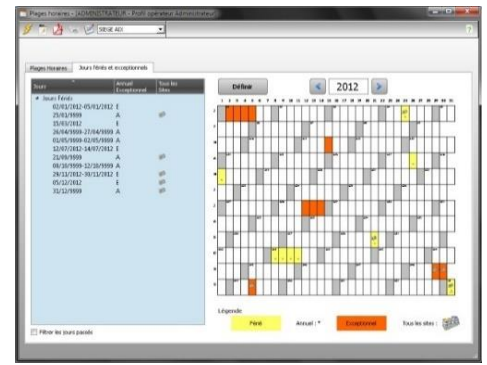
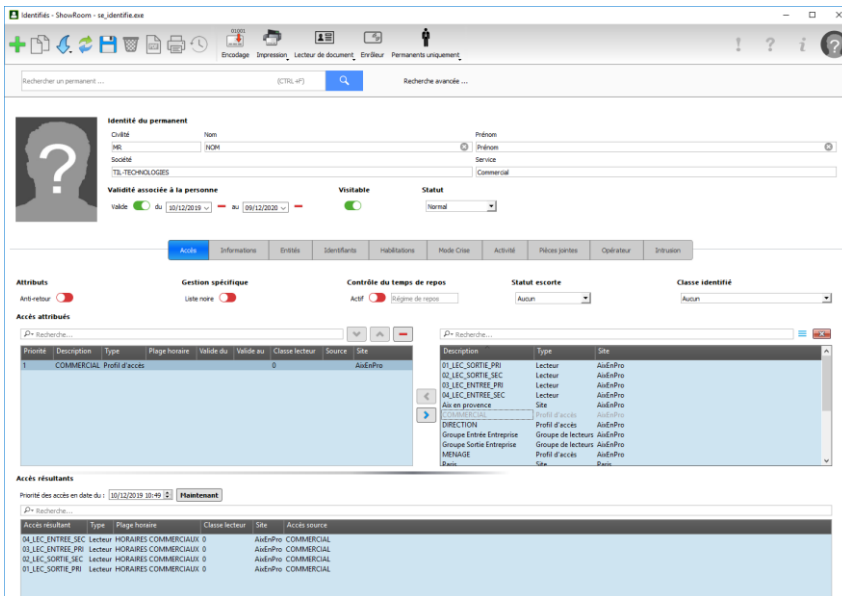
UNE PERIODE DE VALIDITE : qui est associée à chaque identifié et permet d'invalider (ou revalider) rapidement et temporairement un identifiant, sans détruire la liste de ses autorisations

LA GESTION DES DROITS D'ACCES QUI OFFRE UNE SOUPLESSE DE VISUALISATION ET RAPIDITE D'ATTRIBUTION DES DROITS D'ACCES : vue commune, filtre textuel, sélection de droits multiples dans une liste regroupant les profils, les lecteurs, les groupes de lecteurs et les étages d'ascenseurs. Les droits d'accès sont attribués à la personne, pas aux identifiants (badge). Ainsi, même si on perd et réattribue un autre badge, cela ne change pas les droits d'accès

GESTION DES ACCES INDIVIDUELS

L'attribution d'un droit d'accès permet d'autoriser le passage d'un identifié sur un lecteur ou un groupe de lecteurs, en fonction d'un programme horaire défini (128 programmes horaires).

Les UTL **TILLYS NG** sont périodiquement mises à l'heure par **MICRO-SESAME**, maître du temps, pour s'assurer qu'il n'y a pas de dérive entre les UTL et le serveur et bien respecter les plages horaires.



GESTION DES ACCES PAR PROFILS

Le profil d'accès permet de prédéfinir les droits d'accès pour une catégorie d'identifiés, sur un ou plusieurs sites. Le profil est composé d'une liste de lecteurs et/ou de groupes de lecteurs et/ou d'ascenseur, chaque lecteur ou groupe pouvant être associé à une plage horaire différente.

A chaque identifié, il est possible d'associer un ou plusieurs profils d'accès.

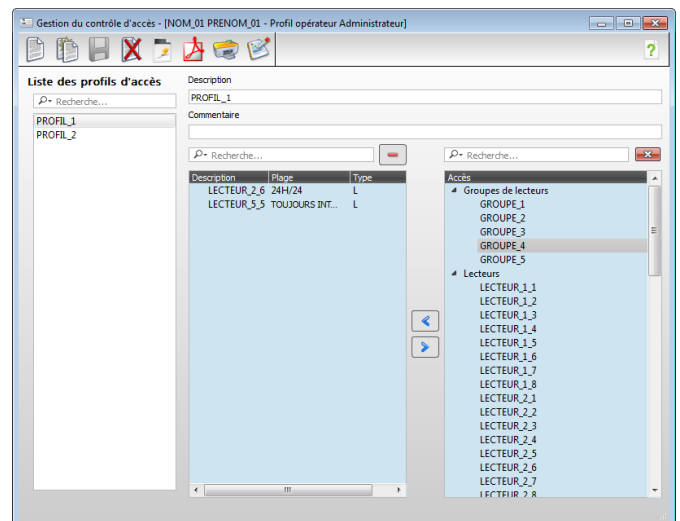
Il est possible de créer des exceptions pour une personne particulière en utilisant la gestion individuelle des accès par lecteurs et/ou groupes de lecteurs.

On pourra par exemple associer un profil « général » pour les accès communs, un profil « service » pour l'accès à certaines zones et des particularités propres à la personne, liée à sa fonction ou à son niveau hiérarchique.

MICRO-SESAME intègre une notion de profils d'accès « tous lecteurs » pour chaque site qui englobe tous les lecteurs existants et futurs du site. Ce profil est pratique quand on veut donner à un identifié tous les lecteurs d'un site sans avoir à modifier le profil à chaque ajout de nouveaux lecteurs pour un site donné.

La gestion des droits d'accès des Identifiés est d'une très grande souplesse. Elle permet une visualisation et une attribution rapides des droits d'accès : vue complète des accès, filtre textuel, sélection d'accès multiples dans une liste regroupant les profils, les lecteurs, les groupes de lecteurs et les étages d'ascenseurs

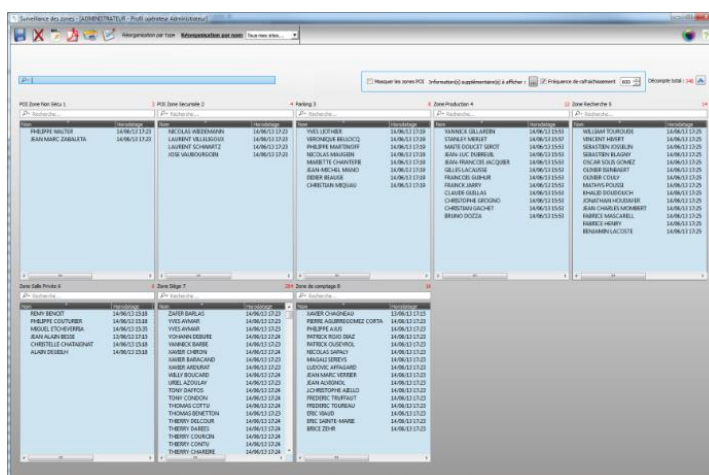
Une fonctionnalité de la gestion des Identifiés affiche en permanence les « accès résultants » issus de l'attribution de tous les droits d'accès affectés à l'Identifié.



GESTION DE ZONES

MICRO-SESAME intègre une gestion de zones. Une zone est délimitée par deux groupes de lecteurs : un groupe permettant d'entrer dans la zone et un groupe permettant de sortir de la zone. Un groupe de lecteurs peut contenir un nombre quelconque de lecteurs d'une installation.

Il est possible de connaître exactement le nombre de personnes présentes dans chaque zone et d'en établir la liste, par ordre alphabétique, par ordre chronologique d'arrivée ou d'autres critères de tri comme la société etc.



Très utilisée par les établissements classés SEVESO, cette gestion des zones est indispensable à la mise en place de l'application spécifique développée par TIL pour l'assistance au POI (Plan d'Opération Interne, voir pages suivantes).

Il est possible d'envoyer par mail la liste des présents dans une zone en cas de déclenchement d'un POI.

La gestion des zones permet également la mise en place d'un contrôle précis des circulations. La possibilité d'imbriquer une zone dans une autre et l'activation de lecteurs en fonction de la sortie d'une autre zone créant, de fait, un « passage obligé », appelé notion de dépendance dans **MICRO-SESAME**

GESTION DES HABILITATIONS

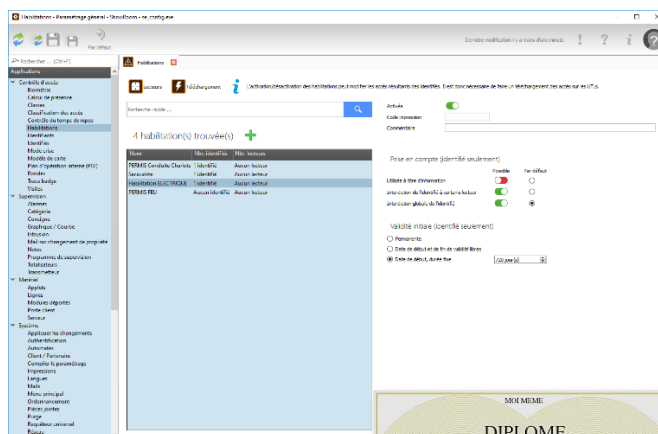
Les autorisations d'accès d'un identifié, sur certaines zones ou certains lecteurs, peuvent être conditionnées par la possession d'une habilitation, externe au contrôle d'accès, en cours de validité : habilitation électrique, ATEX, Habilitation à la conduite d'engins, secourisme, contrat temporaire, médicale,...

Cette condition de validité peut être gérée par des personnes différentes, par exemple le service RH ou n'importe quel responsable fonctionnel concerné.

Cette fonctionnalité permet jusqu'à 256 habilitations.

Chaque identifié peut cumuler plusieurs habilitations, possédant chacune sa propre période de validité.

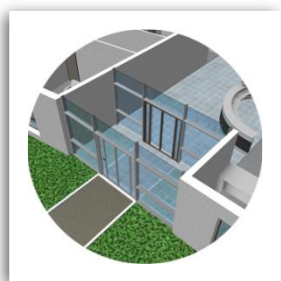
L'accès à un lecteur donné peut être soumis à la validité d'une ou plusieurs habilitations.



FONCTIONS DE SECURITE RENFORCEE

ANTI-RETOUR : Sur des accès avec lecteurs en entrée et sortie, la gestion des zones permet de mettre en place un mécanisme "anti-retour" afin d'empêcher un identifié d'entrer plusieurs fois de suite dans une zone, sans en être préalablement sorti.

GESTION DE SAS : La force de la programmation du système permet également de personnaliser l'asservissement de plusieurs portes entre elles selon les besoins projets. Cette programmation permet de combiner plusieurs technologies : tapis contact, tapis d'unicité, caméra vidéo, lecteur biométrique...



CONTROLE RENFORCE : **MICRO-SESAME** offre la possibilité de déclarer certains lecteurs avec double contrôle : passage d'un badge autorisé et saisie d'un code secret sur un clavier. Ce contrôle renforcé permet une authentification forte du porteur du badge pour les accès sensibles.

Le code secret peut être identique pour tous les identifiants et personnalisé pour chaque identifié.

CODE CONTRAINTE : **MICRO-SESAME** prend en compte un code clavier saisi sous contrainte. Une alarme silencieuse est alors générée immédiatement sur le poste opérateur et l'accès s'ouvre normalement sans alarme sonore.

SURVEILLANCE DE LA "LISTE NOIRE" : Cette fonction permet de déclencher une alarme dès qu'un badge inscrit en "liste noire" est présenté sur l'un des lecteurs du site. Par exemple pour intervenir sur le terrain en cas de tentative d'utilisation frauduleuse d'un badge perdu ou volé.

MODE CRISE : **MICRO-SESAME** permet de gérer des seuils de crise. Basés sur des critères propres à chaque site, 7 niveaux sont attribuables, aussi bien aux personnes (selon la hiérarchie, les habilitations...) qu'aux lecteurs (selon les zones, les types d'alarmes...).

Lorsqu'un mode crise est déclenché, chaque UTL du système reçoit l'ordre de changement de seuil et gère automatiquement les correspondances entre les niveaux d'accréditation des personnes et les niveaux de sécurité des lecteurs. Une personne d'un niveau inférieur à celui du lecteur ne pourra plus entrer et/ou accéder à un étage via l'ascenseur. En effet le mode crise agit sur tous les droits d'accès des lecteurs onlines y compris lecteur cabine de gestion des étages.

Il est possible de générer plusieurs scénarios de crises par :

- ▶ Des asservissements automatiques selon des combinaisons d'entrées
- ▶ Des actions opérateurs autorisés par un simple clic sur des boutons sur synoptiques préalablement configurés par l'intégrateur : un scénario X va mettre les lecteurs définis dans un niveau de crise souhaité



QUARANTAINE

MICRO-SESAME dispose d'une gestion des durées de mise en quarantaine hautement configurable (à partir de MS2018.4 et firmware TILLYS NGv2.3)

Il est recommandé d'utiliser une UTL par zone de quarantaine.

Pour chaque accès sur un lecteur donné par une personne X (lecteur de mise en quarantaine), on peut définir des durées paramétrables vers des lecteurs dépendants de la quarantaine pour la personne X (2 Heures sur lecteur 1; 5 jours sur lecteur 2; etc...).



Une alarme sur le moniteur d'événements apparaît quand la personne X, après avoir passé sur le lecteur déclenchant la mise en quarantaine, tente d'entrer sur un accès dépendant, sans respecter les durées de mise en quarantaine.

Dans ce cas d'interdiction d'accès pour non-respect de la quarantaine par la personne X, le message indique qu'elle pourra rentrer sur les lecteurs dépendants concernés, à partir d'une durée exprimée en jours/heures.

L'autonomie des UTL est complète car elles communiquent directement entre elles.

Sur coupure réseau, chaque UTL mémorise les messages et l'heure de badgeage et les envoie automatiquement aux autres UTL au rétablissement du réseau

GESTION D'ASCENSEUR

La mise en place de lecteurs de badges dans les ascenseurs d'un bâtiment permet de limiter l'accès à certains étages en fonction de droits individuels, de profils de personnel ou des sociétés d'appartenance, dans le cas d'un immeuble multi-sites.



MICRO-SESAME gère nativement cette fonctionnalité, directement dans les droits des identifiés. Les étages ou groupes d'étages sont vus comme des lecteurs de badges du bâtiment et peuvent donc être intégrés dans des groupes de lecteurs ou des profils d'accès.

La gestion multi-site dans un immeuble à plusieurs locataires permet de filtrer quel étage est géré par quel opérateur en rappelant qu'un UTL est mono-site. On peut par exemple organiser les étages ainsi :

- ▶ Le promoteur, gestionnaire principal peut gérer les droits d'accès de tous les étages
- ▶ Chaque locataire gère les droits d'accès uniquement à ces étages loués et aux étages communs (RDC/accueil, parkings, cantine...) et que pour son personnel grâce aux entités

Un locataire pourra ainsi octroyer des accès sur ses étages et sur la partie commune. Mais le gestionnaire principal de la tour gardera la main sur les plages horaires des étages communs.

Une UTL dédiée à la gestion d'ascenseurs est requise pour bénéficier de cette fonctionnalité.

ACCES VEHICULES ET GESTION DE PARKING

MICRO-SESAME peut superviser des lecteurs dédiés à l'accès des véhicules, comme des lecteurs longue distance (à télécommande ou à badges actifs) ou des lecteurs de plaques minéralogiques ou de QR Code.

Ces équipements facilitent la gestion des flux de véhicules, notamment aux heures de forte affluence, et apportent un plus grand confort pour les utilisateurs.

L'intégration dans MICRO-SESAME est transparente : les télécommandes ou les badges à longue portée font remonter un numéro comme n'importe quel autre badge, les plaques d'immatriculation sont directement gérées dans la fiche Identifié/Identifiant (jusqu'à 99 plaques minéralogiques par identifié).



Plus que contrôler les accès, cette gestion intégrée des identifiants permet aussi, par exemple de connaître :

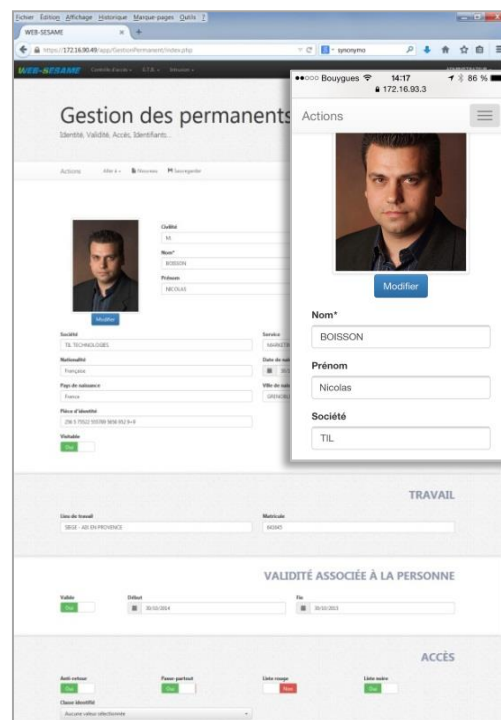
- ▶ Le nombre total de véhicules
- ▶ Les taux d'occupation par type de personnel, service ou société si parking commun
- ▶ Les volumes et durées d'occupation pour imputations ou refacturations...

GESTION WEB DES IDENTIFIES

Pour une exploitation simplifiée du contrôle d'accès, en plus des interfaces serveur et client lourd (fiche « Identifié » vue page 11), des interfaces web « légères » sont disponibles pour la gestion des identifiés et des visiteurs.

Depuis n'importe quel PC ou appareil mobile équipé d'un navigateur internet et d'une connexion, la nouvelle interface WEB-SESAME permet :

- ▶ La recherche et l'affichage de fiches « Identifiés » selon plusieurs critères
- ▶ La création ou modification de fiches, et notamment l'association d'une photo (prise rapide par smartphone ou tablette).
- ▶ L'attribution de profils d'accès et d'identifiants préexistants.
- ▶ L'import/export d'identifiés/identifiants



Ces mêmes fonctions sont disponibles pour la gestion des fiches visiteurs (externes au site).

D'autres interfaces de contrôle d'accès sont également disponibles en mode web, comme la gestion des rendez-vous (visiteurs externes) ou la consultation de l'historique de contrôle d'accès.

L'ergonomie de WEB-SESAME est optimisée pour une utilisation sur tablettes et smartphones (responsive):

- ▶ Ecrans auto-adaptatifs (résolution et orientation).
- ▶ Auto-complétion des champs et affichage photo.
- ▶ Boutons à cocher.

GESTION DES VISITEURS

PLANIFICATION DES RENDEZ-VOUS ET ACCUEIL DES VISITEURS

Sur un site équipé en contrôle d'accès, les personnes extérieures à l'entreprise doivent pouvoir être enregistrées, accompagnées, voire munies d'un identifiant, pour pouvoir circuler dans les zones qui lui sont autorisées. Cet objectif est demandé dans la politique de sécurité du client final ou imposé par la législation (guide ANSSI pour les OIV, OSE,...).

La gestion des visiteurs de **MICRO-SESAME** permet la planification, la gestion des flux des visiteurs l'optimisation des procédures d'accueil et allie flexibilité et sécurité. Pour s'adapter au mieux aux besoins, procédures et organisation du client final, la solution offre des paramètres généraux à prédéfinir (ex, limiter la durée d'un rendez-vous par défaut) et des limites fonctionnelles selon le profil opérateur de chaque demandeur, valideur, hôtesse d'accueil.

Cette option logicielle de **MICRO-SESAME** est réalisée à travers 3 interfaces dédiées :

- ▶ L'interface web **WEB-SESAME**,
- ▶ Des postes d'accueil (client lourd)
- ▶ Des bornes d'accueil (client lourd)

L'ergonomie de ces interfaces a été étudiée pour offrir une IHM épurée, un traitement accéléré avec :

- ▶ Accès aux onglets fonctionnels filtrés selon les droits opérateurs et données par défaut proposées ou imposées
- ▶ Ecrans web auto-adaptatifs à la résolution et à la navigation (portrait/paysage, disposition des champs selon largeur...)
- ▶ Saisie et recherche de visiteurs avec auto-complétion,
- ▶ Ajout de photo par prise instantanée (webcam, tablette ou smartphone)

L'interface **WEB-SESAME** est accessible à tous les utilisateurs autorisés avec leurs PC bureautiques munis d'un navigateur web depuis l'intranet de l'entreprise. Elle permet de créer des visiteurs, de planifier et/ou valider des rendez-vous et compléter les informations nécessaires (plage horaire, profil d'accès, accompagnant, fiche visiteur...).



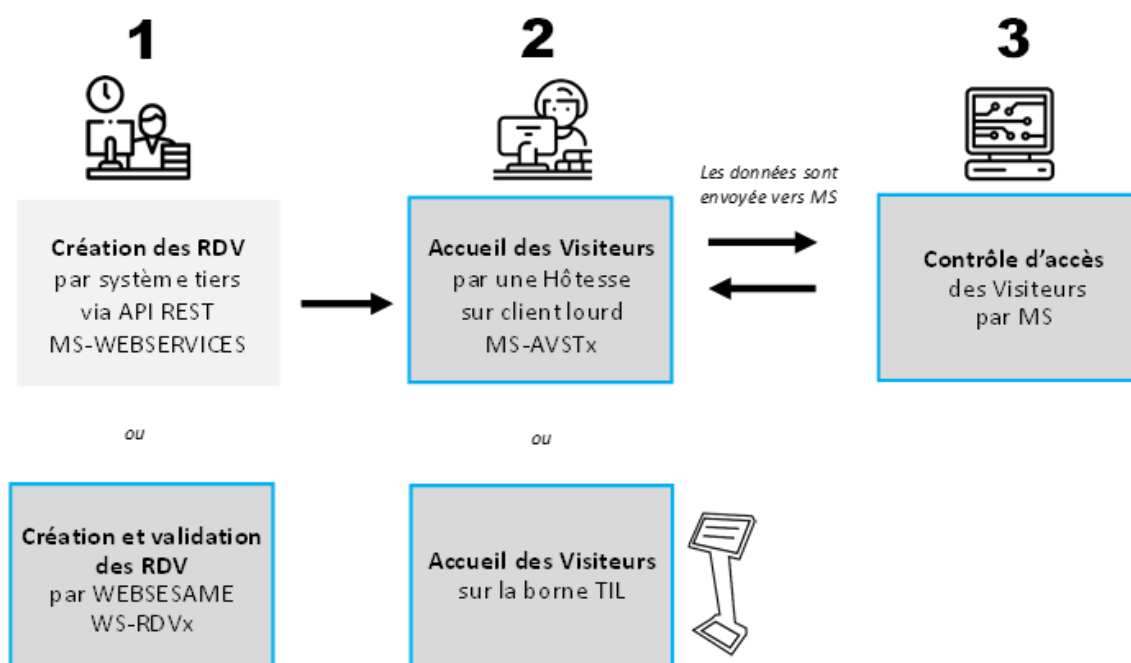
L'Accueil Visiteur, installé en postes client lourd à l'entrée physique du bâtiment, permet une grande fluidité et les opérations les plus complètes, de l'attribution à la restitution des badges aux visiteurs, la création de visites inopinées, le scan des papiers d'identité ou encore l'impression de badges/cartons personnalisés. Les postes « lourds » doivent être raccordés par réseau au serveur d'application MICRO-SESAME.

La borne d'accueil tactile, avec Scanner QR code intégré, offre 2 choix sur son écran :

- Pour le visiteur attendu qui scanne son QR code reçu par email
- Pour le visiteur inopiné qui crée sa fiche et sa demande de visite

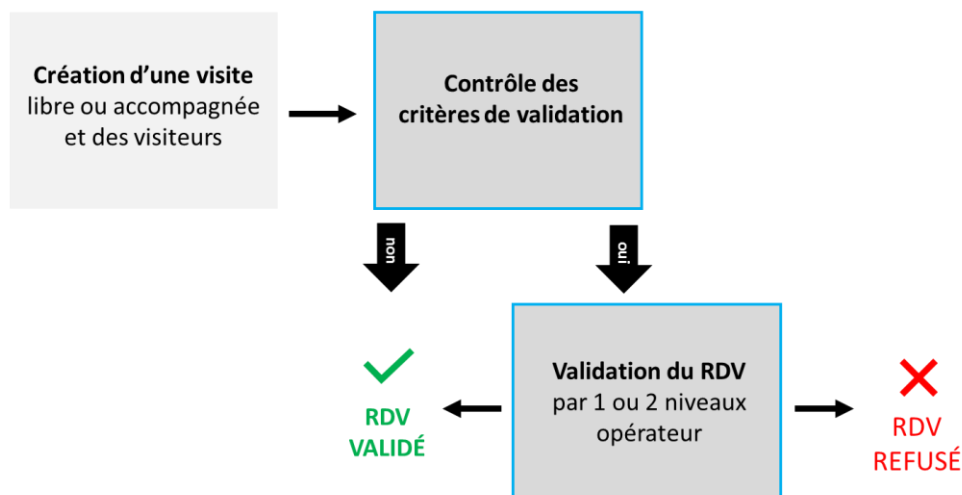
Il existe un document spécifique sur la gestion des visiteurs qui est disponible auprès de votre interlocuteur TIL habituel.

WORKFLOW SIMPLIFIE DE LA GESTION DES VISITEURS

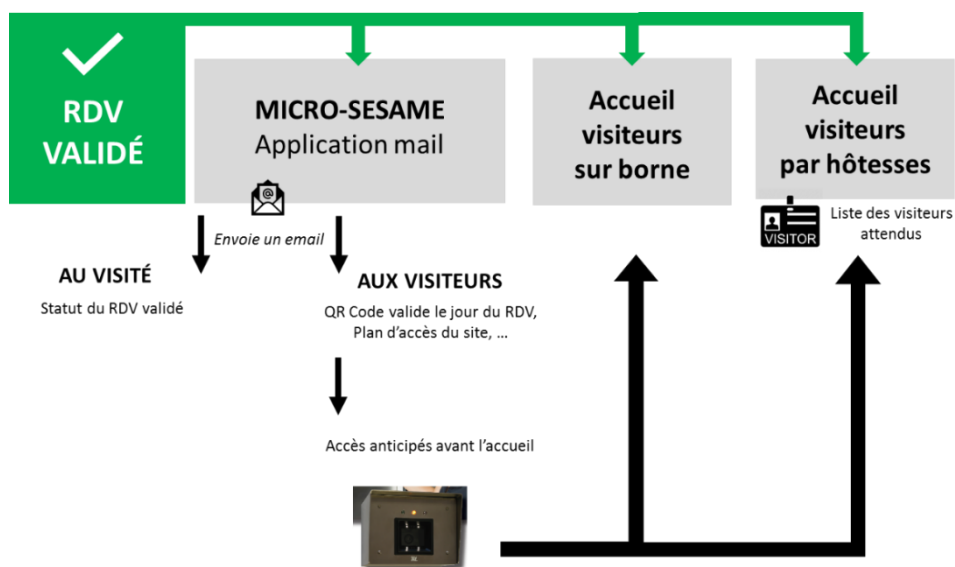


WORKFLOW DETAILLE DE LA GESTION DES VISITEURS

WEB SESAME



Si rendez-vous validé :



Cette solution offre les avantages suivants :

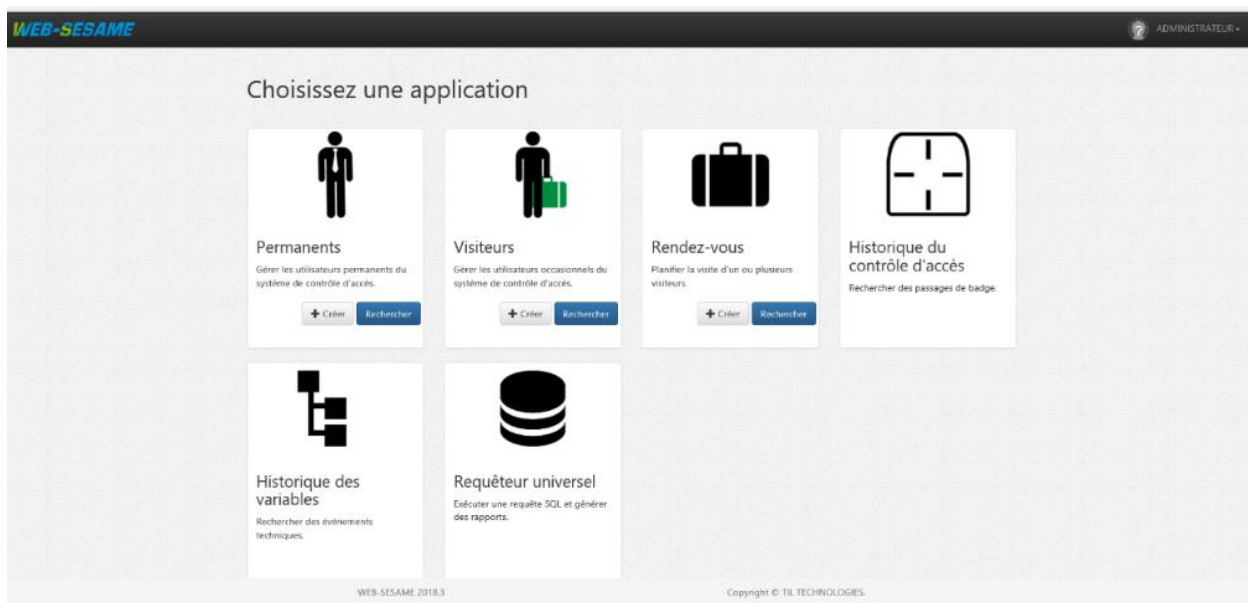
- ▶ Gérer des visiteurs par un workflow complet & intégré à la gestion des accès
- ▶ Optimiser, fluidifier, sécuriser l'accueil des visiteurs et leurs accès aux sites
- ▶ Offrir des visites libres ou accompagnées, Permettre de créer des rendez-vous inopinés
- ▶ Valider les rendez-vous selon des critères personnalisables par client
- ▶ Autoriser les visiteurs sur des accès anticipés (parkings,...)
- ▶ Créer des visites par les visités autorisés depuis leurs PC bureautiques
- ▶ Respecter les exigences de l'ANSSI (guide du sans contact)
- ▶ Offrir 2 types d'accueil visiteur (avec hôtesse et/ou borne) pour 2 problématiques (sécurité, coût)
- ▶ Edition de badges visiteurs personnalisés par client (charte graphique, nom, codes couleur, ...)

WEB-SESAME affiche deux icones pour la gestion des visiteurs : « Visiteurs » et « Rendez-vous »

LA GESTION DES VISITEURS permet la saisie de toutes les informations requises afin de créer les visiteurs éventuellement autorisés à circuler sur le site seul ou accompagné. La désignation des champs obligatoires à renseigner par les utilisateurs est paramétrable par les opérateurs MICRO-SESAME. Les possibilités de gestion d'accès sont limitées volontairement, par rapport à un poste lourd MICRO-SESAME, pour les adapter aux fonctions utiles à la gestion des visiteurs et au personnel qui utilisera l'interface (personnel hors accueil et service sécurité) :

- ▶ Profils d'accès parmi ceux autorisés pour les visiteurs
- ▶ Attribution d'un identifiant (badge) libre, parmi ceux créés pour les visiteurs
- ▶ Validité, Anti-retour, passe-partout, liste noire...
- ▶ Notion de « statut » visiteur que l'on peut rendre visible qu'aux opérateurs spécifiques

Cela permet de créer des droits d'accès limités pendant une période donnée



LA GESTION DES RENDEZ-VOUS permet de rechercher, créer des rendez-vous avec :

- ▶ La personne visitée, parmi les personnes autorisées avec statut « visitables »
- ▶ Les dates, horaires, et informations complémentaires (motifs des rendez-vous,...)
- ▶ Le ou les visiteurs sélectionnés à la suite de recherches, pour éviter les doublons, ou à défaut, en créant directement de nouveaux visiteurs dans une pop-up simplifiée
- ▶ Attribution de profils d'accès, parmi des profils autorisés aux visiteurs et des profils autorisés à l'opérateur (gestion multi-sites, notion de classification)
- ▶ Notion de Lieu de visite possible dans un champ avec liste déroulante prédéfinie pour des projets multi-sites. Pour notifier par email que les validateurs des sites concernés.
- ▶ Attribution d'accès anticipés pour rejoindre l'accueil depuis un parking avec des lecteurs QR code. Un QR code (ou code PIN) est envoyé par email au visiteur du rendez-vous
- ▶ L'accompagnant éventuel, parmi les accompagnants possibles. Dans ce cas, l'ouverture des accès demande un double badgeage, d'abord du visiteur, puis de n'importe personne avec le statut d'accompagnant dans un délai donné et les profils d'accès du visiteur et de l'accompagnant doivent être autorisés tous les deux.
- ▶ Annotation de consignes spécifiques si nécessaires



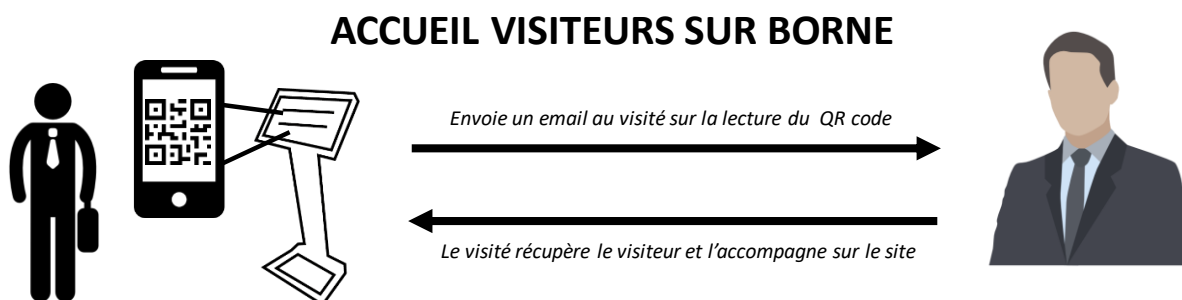
UNE FONCTION « VALIDATION DES RENDEZ-VOUS » est également disponible dans cette interface si les process internes de l'entreprise obligent une approbation par une ou deux tierces personne (officier de sécurité, responsable d'un service, ...) :

- ▶ Il est possible de gérer jusqu'à 2 niveaux de validation (opérateurs de niveau 1 & 2)
- ▶ Les critères de validation de chaque rendez-vous, qui vont le valider automatiquement ou par un ou deux opérateurs, sont configurables pour chaque client final par des requêtes basées sur des données liées au demandeur (service, statut...), à la visite (date, lieu...) ou aux visiteurs (nationalité, société...)
- ▶ Des notifications par emails personnalisables pourront être envoyées automatiquement aux personnes concernées (visiteur, visité, validateur) pour les informer du déroulement de la validation et du statut de la visite (en attente de validation, à valider, acceptée, refusée...).

Une fois le rendez-vous validée (automatiquement ou par opérateur), la visite n'est plus modifiable. Néanmoins, il est possible de dupliquer un rendez-vous validé.

ACCUEIL DES VISITEURS

WORKFLOW DETAILLE ACCUEIL DES VISITEURS SUR BORNE D'ACCUEIL :



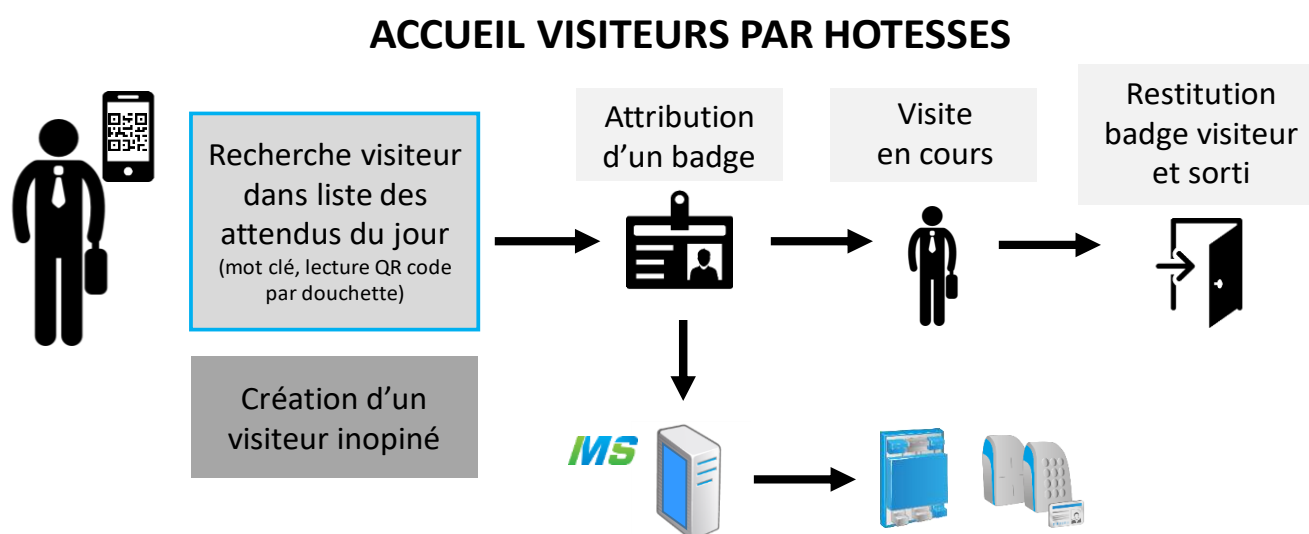
Borne tactile avec Scanner QR code intégré avec 2 choix sur écran d'accueil :

1. Pour le visiteur attendu qui scanne son QR code
2. Pour le visiteur inopiné qui crée sa fiche et sa demande de visite

Les avantages spécifiques de cette solution d'accueil des Visiteurs sur borne d'accueil :

- ▶ Gérer simplement l'accueil des visiteurs par un workflow allégé
- ▶ Réduire les coûts (personnel d'accueil, badges visiteurs, ...)
- ▶ Accompagner les visiteurs par les visités, seuls à avoir un badge & un droit d'accès
- ▶ Tracer les visites et entrées sur site des visiteurs avec l'historique de MICRO-SESAME

WORKFLOW DETAILLE ACCUEIL DES VISITEURS PAR DES HOTESSES AVEC POSTES D'ACCUEIL :



LES AVANTAGES SPECIFIQUES DE CETTE SOLUTION D'ACCUEIL DES VISITEURS PAR DES HOTESSES :

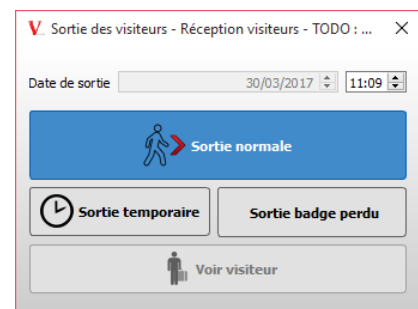
- ▶ Attribuer aux visiteurs un badge & droits d'accès téléchargés en moins de 10 s
- ▶ Lister, localiser les visiteurs présents sur site et leurs statuts (en attente, en cours, sortie, ...)
- ▶ Tracer les visites et tous les mouvements des visiteurs avec l'historique de MICRO-SESAME
- ▶ Plusieurs types de sorties possibles

LES PRINCIPALES FONCTIONS OFFERTES AUX HOTESSES AVEC L'APPLICATION ACCUEIL DES VISITEURS :

- ▶ Accueil et recherche rapide du visiteur
 - Recherche par nom du visité ou visiteur
 - Lecture du QR code du visiteur, reçu par email, via une douchette
 - Création possible sans rendez-vous préalable, si autorisée, d'une visite inopinée
 - Avec affectation de profils d'accès réservés aux visiteurs (parking visiteurs,...).
 - Avec durée de validité (acceptant plusieurs jours et sorties temporaires)
 - Avec ou sans escorte par un accompagnant habilité (double badgeage)
 - Possibilité de raccorder un lecteur OCR, pour remonter automatiquement des informations des cartes d'identité et passeports dans les champs de l'interface.
- ▶ Attribution d'un badge visiteur disponible par simple badgeage sur lecteur de table
- ▶ Mettre à jour l'état du visiteur : Faire entrer le visiteur ou placer le visiteur en attente (Visiteur enregistré mais en attente dans l'accueil visiteur du site).



- ▶ Plusieurs documents personnalisables peuvent être créés et imprimés pour les visiteurs entrants (carte de visite, bordereau de visite, plan du site, coupon autorisation véhicule, avec motif de visites, nom visité)
- ▶ Passerelles possibles avec des applications tierces (réunions, formations, ...) sur les visiteurs
- ▶ Faire sortir un visiteur et terminer une visite. Après la visite, il est nécessaire de déclarer la sortie du visiteur. Plusieurs types de sorties sont possibles :
 - Sortie normale : Clôture de la visite en cours. Le visiteur disparaît de la liste des visiteurs enregistrés. Le badge visiteur est à nouveau disponible et réutilisable
 - Sortie temporaire : Une fois que le visiteur a quitté temporairement le site, désactivation des accès. il doit être enregistré à nouveau à son retour
 - Sortie badge perdu : Le visiteur termine la visite sur site, mais son badge n'est pas rendu (ou cassé). La visite en cours est clôturée. Le visiteur disparaît de la liste des visiteurs enregistrés. Le badge non rendu attribué n'est plus attribuable.



- ▶ Lecteurs avec sortie automatique possible (Lecteurs avaleurs) sans passer par l'accueil
- ▶ Affichage d'une liste des visiteurs et leurs différents statuts
 - Visiteurs attendus : le visiteur est pré-enregistré et ne s'est pas encore présenté à l'accueil visiteur
 - Visiteurs en attente
 - Visiteurs entrés : le visiteur est enregistré et entré sur site et pas encore sorti
 - Visiteurs sortis
 - Visite dépassée : Lorsque l'heure prévue de fin de visite est dépassée, et si le visiteur n'a pas quitté le site, une alarme s'affiche et une icône signale le dépassement
- ▶ Edition d'historiques des visites ou de listes de visiteurs (attendus, en attente, sorties temporaires...) sur imprimantes ou exports en fichiers compatibles EXCEL.
- ▶ Synchronisation possible avec les calendriers Outlook grâce au fichier ICalendar (ICS) attaché au mail envoyé aux acteurs
- ▶ Purge possible des visiteurs qui ne sont pas venus à un rendez-vous

CONTROLE D'ACCES « OFFLINE »

GESTION DES CYLINDRES ET BEQUILLES MECATRONIQUES AUTONOMES

MICRO-SESAME gère nativement la logique de diffusion de droits d'accès « offline », c'est-à-dire sur des équipements mécatroniques autonomes (cylindres ou béquilles), non connectés au système en temps réel. Dans cette logique, les droits d'accès sont encodés directement par MICRO-SESAME dans les badges des utilisateurs, pour une durée de validité à définir.

Le rechargement périodique de ces droits nécessite le passage devant des bornes spécifiques reliées à **MICRO-SESAME** (liaison IP PoE).

Pour l'opérateur, l'attribution de droits sur ces accès non connectés s'effectue de manière complètement transparente, à travers la même interface « Identifié/Identifiants » avec laquelle il gère également les lecteurs connectés.

Cette flexibilité du système évite d'avoir deux interfaces ou de faire dialoguer deux bases de données. Elle permet aussi à ces accès autonomes, comme n'importe quel lecteur du site, de bénéficier de fonctionnalités **MICRO-SESAME** liés à la gestion multi-site et l'attribution de profils d'accès.

La gestion centralisée d'éléments mécatroniques autonomes apporte aussi des avantages pour la remontée d'informations.

En effet, à chaque passage d'un identifié sur une borne de rechargement, les éléments suivants sont récupérés vers **MICRO-SESAME** :

- ▶ Les historiques de passage badges.
- ▶ Les alarmes de pile basse.

Les fonctionnalités des « bornes offline » de TIL sont très évoluées :

L'encodage initial des badges ne nécessite pas un poste dédié mais peut s'effectuer directement lors du premier passage sur une borne de rechargement des droits.

En cas de perte de liaison entre une borne et le serveur MICRO-SESAME, celle-ci fonctionne de manière autonome (40 000 identifiés embarqués en local).



ENCODAGE DES BADGES

PERSONNALISATION ELECTRIQUE

La personnalisation électrique des badges (MS-ENCODBADGE) est une option logicielle de **MICRO-SESAME** permettant l'écriture de données dans les badges de la famille Mifare.

Le logiciel gère l'encodage de la plupart des formats : Mifare Classic, Mifare Desfire EV1, en définissant notamment l'emplacement (ex : secteur Mifare Classic, applications et fichiers Mifare Desfire) et le format des identifiants (décimal, hexadécimal, alphanumérique...).

Plusieurs applications avec de multiples Identifiants peuvent être encodés en une seule fois.

L'identifiant peut être généré par MICRO-SESAME ou fourni par une application tierce.

L'encodage physique peut être réalisé individuellement ou par série de badges, sur un encodeur de table ou directement dans une imprimante à badges avec un encodeur intégré. Dans ce cas, il est possible de réaliser simultanément, en automatique pour une population de personnes :

- ▶ La personnalisation graphique
- ▶ L'encodage multi-applications
- ▶ L'enrôlement de chaque badge à la personne associée

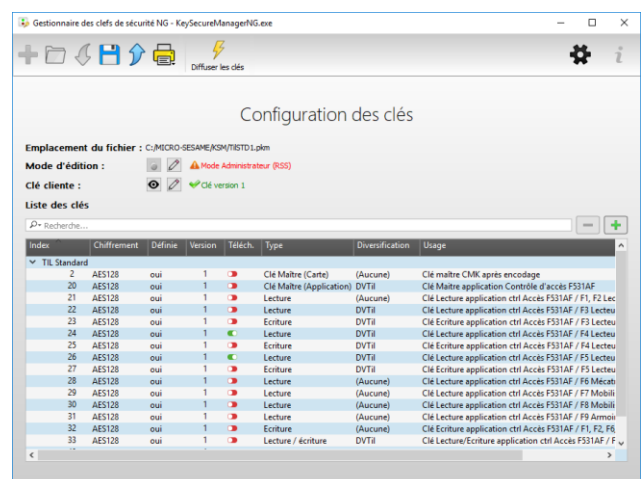
Cette solution offre : rapidité, simplicité, sécurité

GESTION DES CLES DES BADGES AVEC KSM

Le logiciel KEY SECURE MANAGER est un gestionnaire de clés de sécurité des badges. Il autorise un encodage sécurisé et entièrement sur mesure pour le client final :

- ▶ Configuration des clés (selon les formats et les types de clés utilisés) des badges.
- ▶ Génération des clés et fichiers de sauvegarde
- ▶ Génération du fichier associé à MS-ENCODBADGE pour l'encodage ou enrôlement physique du badge sur lecteur transparent d'un poste client MICRO-SESAME

Il existe une documentation KSM NG dédié plus détaillée.



PERSONNALISATION DES BADGES

La personnalisation des badges est une fonction intégrée de base à **MICRO-SESAME** permettant la création graphique (texte personnalisé selon données des fiches identifiées, texte fixe, logo, photo, pictogrammes, QR code, ...) et l'impression thermique.

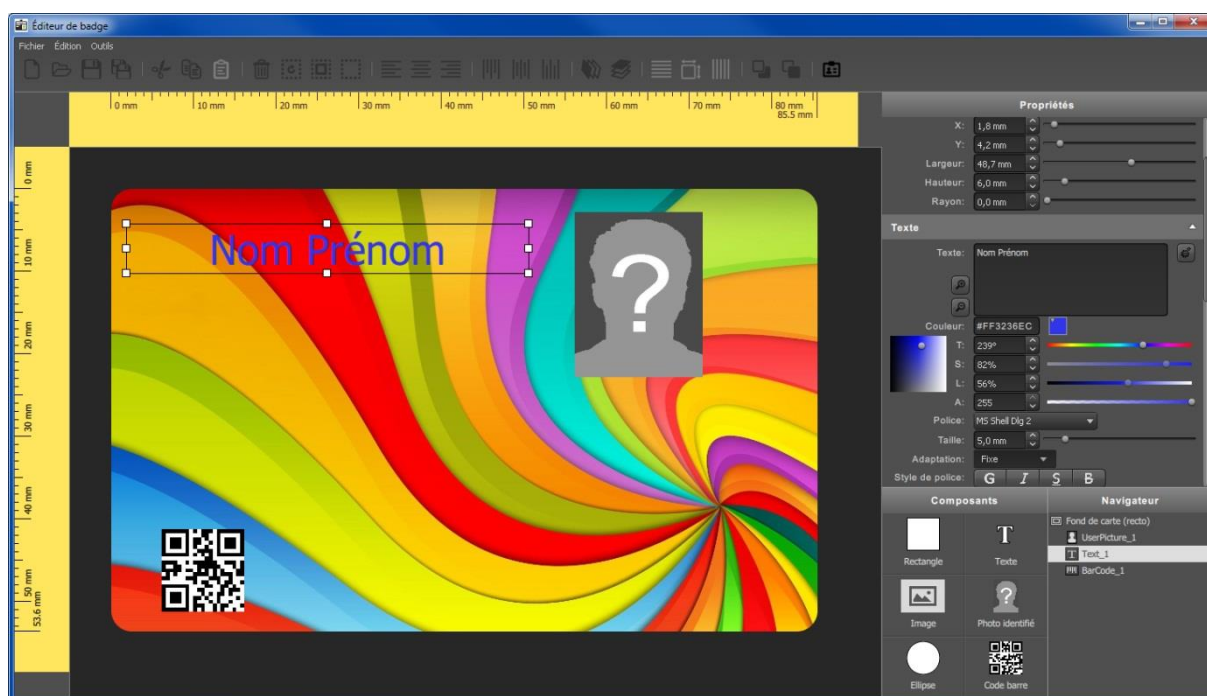
Il est possible de stocker pour chaque personne une photo provenant d'un fichier existant, d'un scanner, d'une source vidéo ou de n'importe quelle Webcam.

L'éditeur graphique de **MICRO-SESAME** permet de créer les fonds de carte sur simple ou double face, et de paramétrer différents libellés à imprimer (nom, service, habilitation...). Ces données imprimées peuvent être écrites avec tous les alphabets internationaux dont en particulier les alphabets arabes.

Il est possible par exemple d'ajouter à l'impression des pictogrammes symbolisant des habilitations spécifiques au porteur de la carte (habilitation électrique, atmosphère dangereuse, permis...)

L'éditeur de fonds de badges permet d'exporter des fonds de badges déjà créés pour les importer et les réutiliser sur d'autres sites du même client par exemple.

La solution permet de créer plusieurs fonds de badge au choix (permanent, temporaire, visiteur,...) avec des caractéristiques différentes et d'affecter le bon format par personne avant impression en série.

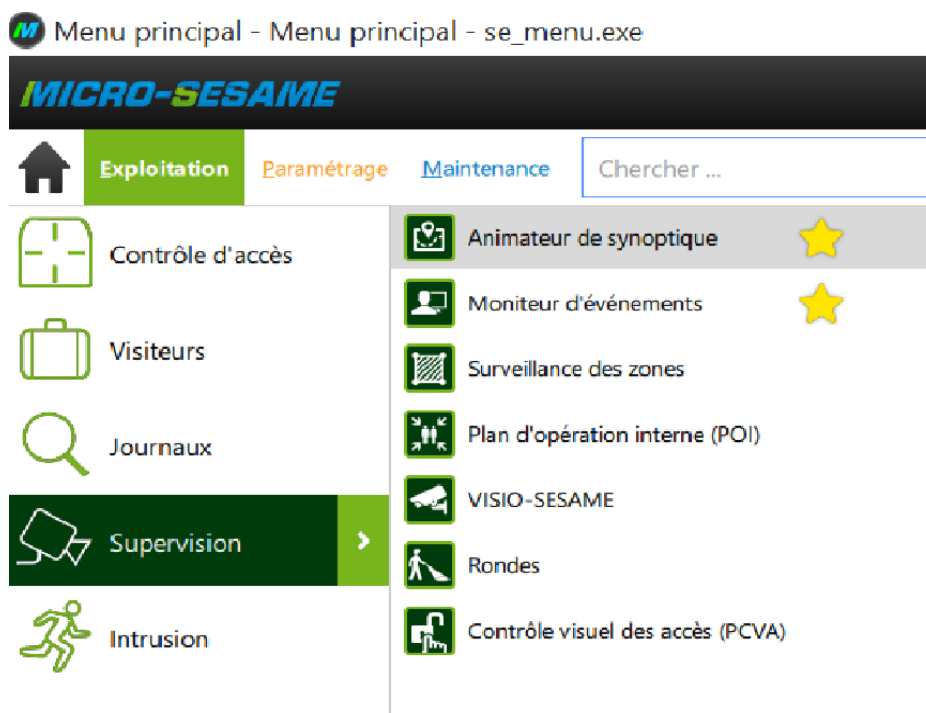


MONITORING & SUPERVISION


Moniteur d'événements temps réel, synoptiques graphiques, Surveillances des zones

MICRO-SESAME permet la surveillance des événements, alarmes, défauts du contrôle d'accès, intrusion, du système, de la gestion techniques et de lancer des actions associées (acquiescement, commandes diverses, visionner les flux vidéo, ...) grâce à ces fonctions :

- ▶ Animateur de synoptique
- ▶ Moniteur d'événements et d'alarme
- ▶ Surveillances des zones
- ▶ Gestion des zones POI (voir chapitre dédié)



ERGONOMIE GENERALE

- ▶ L'ergonomie des interfaces IHM est étudiée pour offrir une exploitation facile, rapide avec :
- ▶ Une seule IHM unifiée pour gérer toute la sûreté
- ▶ L'opérateur ne voit pas les fonctions, ni les données qui lui sont interdites
- ▶ Gestion multi-langues des IHM
- ▶ Chaque IHM dédiée à certaines fonctions (identifiés, POI, moniteur, synoptique, ...)
- ▶ Fonctions utilisées par une grande population accessibles en WEB (RDV, ...)
- ▶ Navigation et couleur séparée des applications : **Exploitation** – **Paramétrage** – **Maintenance**
- ▶ Un champ de recherche du Menu permet de retrouver facilement les fonctions disponibles
Affichage de l'opérateur connecté sur la barre du haut
- ▶ Notion de favori, raccourcis et liste des dernières applications récentes ouvertes dans le menu principal pour un accès rapide aux fonctions courantes 
- ▶ Gestion de l'autocomplétions permettant à l'utilisateur de limiter la quantité d'informations qu'il saisit avec son clavier, en se voyant proposer un complément qui pourrait convenir à la chaîne de caractères qu'il a commencé à taper
- ▶ Contrôle de cohérence des données en cours d'écriture selon le champ de saisies
- ▶ Notification aux opérateurs des erreurs, oublies selon saisie faite
- ▶ Possibilité de personnaliser la majorité des colonnes des formulaires de résultats :
 - Sélection des champs & données souhaités à l'affichage
 - Sauvegarde de leur position
 - Modification possible par l'exploitant à tout moment

Moniteur interactif des événements, alarmes

Le Moniteur interactif d'évènements centralise la surveillance de tous les évènements, alarmes, défauts reçus par MICRO-SESAME, les affiche en temps réel au fil de l'eau, et permet d'acquitter les alarmes, lancer des actions & télécommandes, forcer l'état des propriétés, ...

Chaque opérateur ne voit que ses sites, catégories d'évènements, ... autorisés. Dans tous les cas, toutes les apparitions, les acquittements et les effacements d'alarme sont horodatés et archivés en base de données pour consultation ultérieure (voir chapitres Historique & opérateur).

L'ONGLET FIL DE L'EAU

Monitoring - se_monitoring.exe

Filtres | Tous mes sites

2 alarmes

Propriétés

Date-Heure	Élément	Message
ven. 10 janv. 2020 11:31:13	Porte Entrée TIL Technologies	Effraction
ven. 10 janv. 2020 11:31:21	ADMINISTRATEUR	Connexion à l'application "Graphique / Courbe" avec le profil "Profil opérateur Administrateur"
ven. 10 janv. 2020 11:31:26	ADMINISTRATEUR	Déconnexion de l'application "Graphique / Courbe"

Détails

Porte Entrée TIL Technologies - Effraction
Le ven. 10 janv. 2020 11:31:13, la propriété est passée dans l'état. L'alarme est acquittée!

Actions

- Acquitter
- Visualiser la caméra
- Visualiser l'enregistrement
- Afficher le synoptique

Note associée à l'événement

Intrusion
Intrusion Radar
Incendie
Incendie RDC

Ajouter une note

Derrière l'événement, il y a moins d'une minute - 3 lignes

Monitoring - se_monitoring.exe

Filtres | Tous mes sites

6 alarmes

Propriétés

Date-Heure	Élément	Message
Thu 18 Jul 2019 10:57:05	ADMINISTRATOR	Connexion à l'application "Unit
Thu 18 Jul 2019 10:57:21	UTL	Compile LPU's
Thu 18 Jul 2019 10:57:32	LEC1	Dupond Ange : Passage autoris
Thu 18 Jul 2019 11:03:47	LEC1	Dupond Ange : Passage autoris
Thu 18 Jul 2019 11:03:50	LEC1	Dupond Ange : Passage autoris
Thu 18 Jul 2019 11:04:33	ADMINISTRATOR	Connexion à l'application "Zon
Thu 18 Jul 2019 11:05:32	ADMINISTRATOR	Connexion à l'application "App
Thu 18 Jul 2019 11:05:38	UTL	Compile LPU's
Thu 18 Jul 2019 11:05:41	Propriété	Daemons will apply changes to
Thu 18 Jul 2019 11:05:41	Programme de supervision	No main supervision program
Thu 18 Jul 2019 11:05:43	UTL	Start of the module download
Thu 18 Jul 2019 11:05:43	UTL	Start XML generation.
Thu 18 Jul 2019 11:05:43	UTL	No data to transfer.
Thu 18 Jul 2019 11:06:00	UTL	Start of the module download
Thu 18 Jul 2019 11:06:00	UTL	Start XML generation.
Thu 18 Jul 2019 11:06:00	UTL	1 module(s) to download
Thu 18 Jul 2019 11:06:00	UTLCSO	File sending to module(s) start
Thu 18 Jul 2019 11:06:02	UTLCSO	Start sending files to module:
Thu 18 Jul 2019 11:06:02	172.16.12.219 - Pourcentage d'identifiés utilisés	Creation 1 Update 0 Removal 0
Thu 18 Jul 2019 11:06:02	UTL	File sending to module(s) finis
Thu 18 Jul 2019 11:06:18	LEC1	Dupond Ange : Passage autoris
Thu 18 Jul 2019 11:06:21	LEC1	Dupond Ange : Passage interdi

Détails

Thu 18 Jul 2019 11:06:21
Passage sur le lecteur LEC1

Voir la fiche de l'identifié

Débloquer l'identifié (annule l'anti-retour)

Derrière l'événement, il y a 7 minute(s) - 23 lignes

« FIL DE L'EAU »

L'onglet « Fil de l'eau » remonte en temps réel tous les évènements de manière chronologique.

Il est possible de désactiver le défilement automatique des évènements pour laisser le temps à l'utilisateur de visualiser les évènements intervenus avant et après celui étudié.

Que la liste d'évènements soit importante ou pas, il est toujours possible de les filtrer selon :

- ▶ Le site (en gestion multisites)
- ▶ Le type d'évènements (passage autorisé ou interdit, alarmes, télécommandes, système, le dernier passage d'un identifié)
- ▶ Un mot clé dans la recherche rapide (nom,....)

« DETAILS »

Lors de la sélection d'un évènement affiché dans le fil de l'eau, la zone « Détails » permet de consulter des informations supplémentaires sur l'évènement et de voir les actions disponibles associées :

- ▶ Acquitter l'alarme : L'acquiescement d'une alarme, permet de s'assurer que l'opérateur l'a bien été prise en compte. La nécessité ou pas d'avoir à l'acquiescer est paramétrable pour chaque évènement typé en alarme.
 - Acquiescement unitaire / multiples sur alarmes par 1 ou X d'opérateurs autorisés selon les catégories des alarmes (CA, AI, ...) et leurs niveaux d'acquiescement (masque). Une alarme peut nécessiter d'être acquiescée par plusieurs intervenants.
 - Choix d'un clignotement ou pas sur les alarmes à acquiescer
- ▶ Lire une consigne,
- ▶ Visualiser la caméra en Live
- ▶ Visualiser l'enregistrement d'une séquence vidéo de l'alarme ou du passage de badge
- ▶ Afficher le synoptique associé à une alarme
- ▶ Sur passage de badge, accéder rapidement aux informations de l'identifié en ouvrant sa fiche et débloquer la sortie temporairement en cas d'alarme antipassback/anti-retour
- ▶ Sur changement d'une valeur, connaître l'état, forcer l'état, lancer une télécommande ...
- ▶ Affichage de la photo associée au dernier passage
- ▶ Ouvrir l'interface de prise de notes (libres ou liées à un évènement variable)

Distinguer les alarmes en fonction de leur gravité				Son Synthèse vocale	Son Nom	Son Répétition	Son Temporisation	Dernier changement
	Texte	Fond	Rendu					
5-10,12	#ffffff	#ff1a0d	Porte d'entrée - Effraction	<input checked="" type="checkbox"/>		En boucle	1000 msec.	il y a 1 heure(s) par ADMINISTRATOR
4	#ffffff	#ff4d26	Porte d'entrée - Effraction	<input checked="" type="checkbox"/>		En boucle	1000 msec.	il y a 1 heure(s) par ADMINISTRATOR
3	#000000	#ff7f3f	Porte d'entrée - Effraction	<input checked="" type="checkbox"/>		En boucle	1000 msec.	il y a 1 heure(s) par ADMINISTRATOR
2	#000000	#ffb259	Porte d'entrée - Effraction	<input checked="" type="checkbox"/>		En boucle	1000 msec.	il y a 1 heure(s) par ADMINISTRATOR
1	#000000	#ffe572	Porte d'entrée - Effraction	<input checked="" type="checkbox"/>		En boucle	1000 msec.	il y a 1 heure(s) par ADMINISTRATOR
0	#000000	#ffff7f	Porte d'entrée - Effraction	<input checked="" type="checkbox"/>		En boucle	1000 msec.	il y a 1 heure(s) par ADMINISTRATOR
*	#ffffff	#ff0000	Porte d'entrée - Effraction	<input checked="" type="checkbox"/>		En boucle	1000 msec.	il y a 1 heure(s) par ADMINISTRATOR

On peut distinguer les alarmes en fonction d'un niveau de gravité de 0 (le moins important) à 512 (le plus élevé).

Les codes couleurs des alarmes sont :

- ▶ Couleur de fond rouge et texte blanc : alarme en cours non acquittée (Couleur par défaut, et personnalisable). On peut distinguer ces alarmes à acquitter en fonction de leur niveau de gravité de 0 qui est personnalisable par :
 - Des couleurs de texte et fond de texte au choix et/ou
 - Des audios, sons au choix (synthèse vocale de Windows, fichier audio)
- ▶ Couleur de fond blanc et texte en noir : Une alarme non acquittable en cours
- ▶ Couleur de fond blanc et texte rouge : Alarme acquittée mais toujours en cours

L'ONGLET ALARMES

Donne une vue exhaustive des alarmes en cours ou qui n'ont pas encore été acquittées. Les alarmes acquittées et qui ne sont plus en cours disparaissent.

Les alarmes sont d'abord triées par ordre de gravité. La majeure partie des actions disponibles dans le fil de l'eau à propos des alarmes sont aussi disponibles dans cette vue avec en plus :

- ▶ Afficher la fenêtre courbe d'historique d'une alarme (voir chapitre Graphique / courbe)
- ▶ Accéder rapidement au paramétrage d'une propriété associée à l'alarme

ONGLET PROPRIETES :

Permet de surveiller, rechercher les différents types de propriétés, de surveiller leurs états (notification lors qu'une porte ouverte est détectée, par exemple), de les éditer et interagir avec.

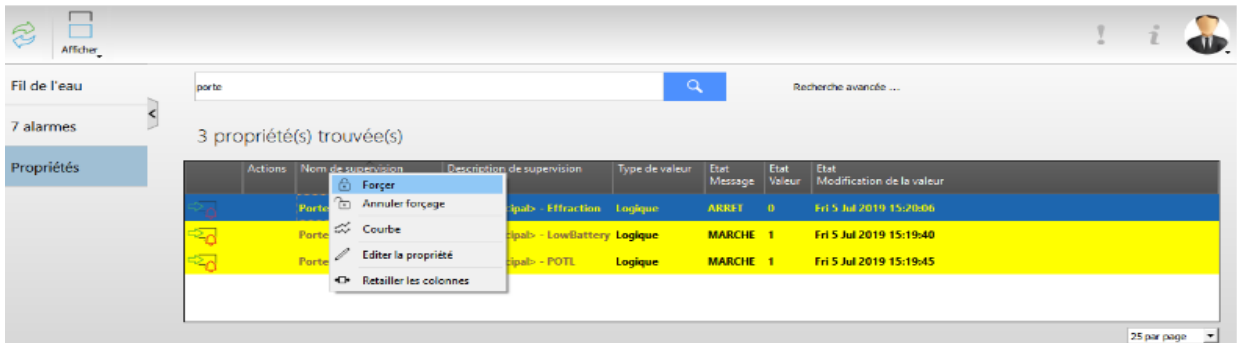
Un objet représente un élément installé sur site qui génère des informations (ex : une porte).

Les propriétés de supervision sont les différents états, télécommandes qui s'appliquent au sein d'un même objet (ex pour un objet porte : BP, Ventouse, Contact porte, POTL, Effraction, commande ouverture) et qui permettent de les piloter dans MICRO-SESAME.

Cette vue est utile à l'exploitant mais aussi à l'intégrateur lorsqu'il paramètre un site car elle permet de diagnostiquer son installation (ex: passer une télécommande, regarder un état, passer une autre télécommande, ouvrir un synoptique...).

Les actions possibles sur ces propriétés selon leurs types sont :

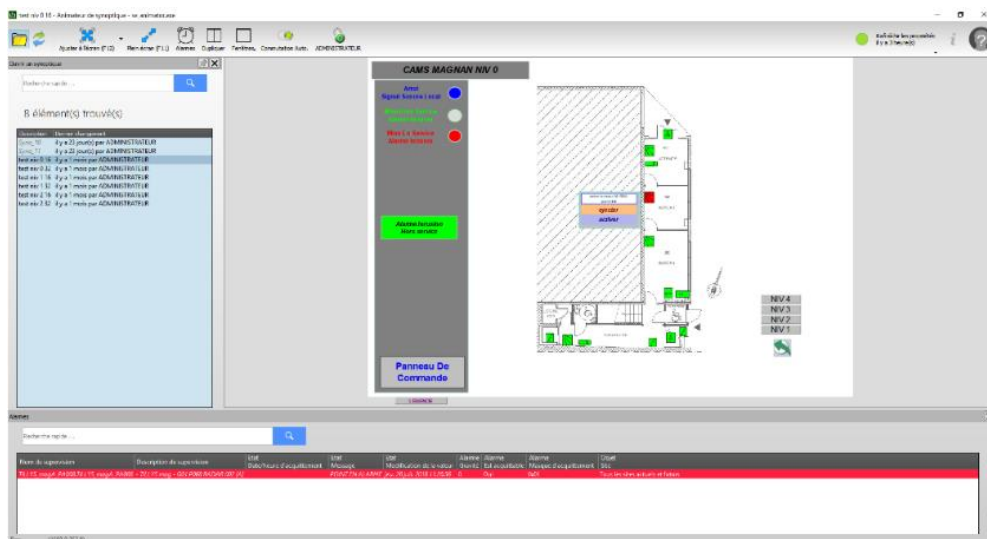
- ▶ Forcer : permet d'inhiber les propriétés, par exemple temporairement dans les cas d'une maintenance, d'un détecteur défaillant ...,
- ▶ Envoyer une commande ou une impulsion,
- ▶ Visualiser la courbe associée,
- ▶ Voir le synoptique associé,
- ▶ Editer la propriété



Les propriétés peuvent être affichées avec différents couleurs : Fond jaune texte marron si l'état d'une propriété a été forcé.

Animateur de synoptiques graphiques

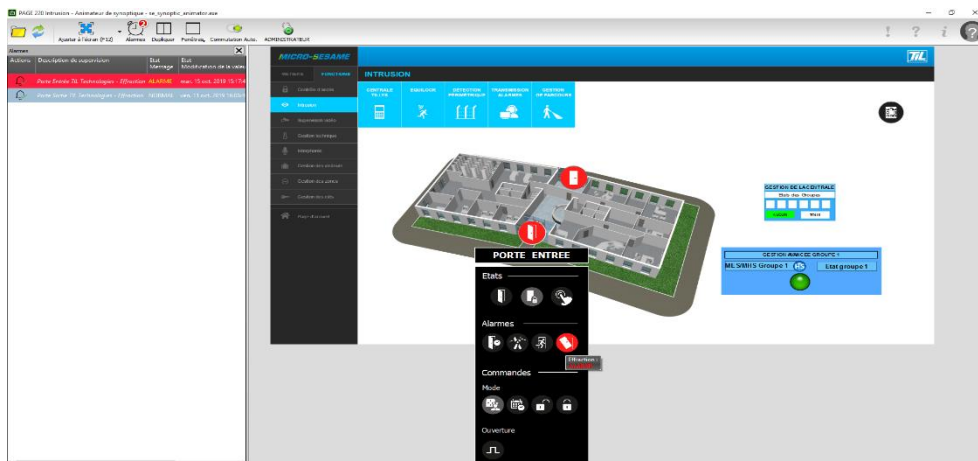
L'animation de synoptiques de **MICRO-SESAME** permet de personnaliser l'interface homme/machine selon les sites pour les fonctionnalités de surveillance (visualisation des alarmes, des états logiques et des valeurs numériques) et de réactions rapides des opérateurs (traitement des alarmes en respectant les consignes, lancer télécommandes, actions). Un synoptique est une représentation graphique de l'installation à superviser et est composée d'un ensemble d'objets graphiques sur des fonds de plan.



Les fonctionnalités associées aux synoptiques sont notamment :

EDITEUR & ANIMATEUR DE SYNOPTIQUES INTEGRE NATIVEMENT, RAPIDEMENT CONFIGURABLE ET HAUTEMENT PERSONNALISABLE GRACE A :

- ▶ La notion d'objets avec leurs propriétés (informations, états, commandes)
- ▶ Une bibliothèque de modèles d'objets prédéfinis, livrée avec MICRO-SESAME (UTL, porte, MAXIRIS, ...) qui intègrent la configuration métier et celle de supervision :
 - Paramétrage facile, rapide en glissant-déposant un objet à partir d'un modèle
 - Attribue automatiquement les automatismes, les entrées, sorties à câbler selon un schéma type avec des choix possibles à sélectionner par simple clic
 - Possibilité de changer l'image de l'objet en gardant toute la configuration
 - Ex avec l'objet « portes standards » : choix d'activer en entrée : contact position porte, commande, contact BBG, ou contact porte verrouillée
- ▶ La possibilité de créer, importer, copier des objets/propriétés personnalisés sur projet
- ▶ Le support du .SVG qui facilite l'import et l'export de plans de construction,
- ▶ La simulation possible depuis l'éditeur pour avoir un aperçu,



- ▶ Animer les objets selon les états des équipements (couleur, clignotement, message audio...)
- ▶ Réaliser des télécommandes, actions diverses depuis des objets, boutons par les opérateurs
- ▶ Utiliser la fenêtre des synoptiques pour naviguer d'un synoptique à l'autre conçus en arborescence (ex : une vue globale du site puis clic pour zoomer sur chaque bâtiment, puis une vue par étage du bâtiment, etc.)
- ▶ Disposer des fonctions de zoom avant et arrière sur un synoptique
- ▶ Ajuster rapidement le synoptique à l'écran ou de passer en mode plein écran par 2 raccourcis
- ▶ Gérer et superviser les alarmes directement depuis les synoptiques grâce à :
 - Une fenêtre spécifique détachable des alarmes avec widget / compteur et liste des alarmes (comme depuis le moniteur d'évènements) avec les différentes couleurs d'affichage selon leur état et leur acquittement
 - La possibilité d'acquitter les alarmes
 - L'ouverture des propriétés d'un objet
 - La visualisation des courbes correspondantes

Surveillance des zones

UNE ZONE EST UN LIEU CLOS (BUREAU, ETAGE, BATIMENT, ...) ET DOIT REpondre A DES REGLES PRECISES :

- ▶ Elle doit posséder un groupe de lecteurs en entrée
- ▶ Elle doit posséder un groupe de lecteurs en sortie
- ▶ Son étanchéité physique (mur) garantit son bon fonctionnement avec l'impossibilité d'entrer ou de quitter la zone sans être contrôlé.
- ▶ Un mécanisme d'unicité de passage des accès est nécessaire pour un comptage efficace

IL EXISTE PLUSIEURS TYPES DE ZONES AVEC LEUR GESTION PARTICULIERE :

- ▶ Comptage/ décomptage (en fonction des entrées et des sorties) des identifiés présents
- ▶ Anti-Retour (géographique ou temporisé)
- ▶ Plan d'opération interne (voir chapitre POI)
- ▶ Autres types de zones (ex : pour gérer des identifiés particulier comme ceux en liste noire)

Surveillance des zones - se_srvca.exe

Réorganisation par type Réorganisation par nom Impression par regroupement

Filtres & paramètres d'affichage Décompte total : 4

Délai de rafraîchissement 5 secondes Information(s) supplémentaire(s) à afficher : ...
 Fréquence de rafraîchissement 50 passages de badge Champ de regroupement Aucun regroupement
 Masquer les zones POI Déplier tous les noeuds à chaque rafraîchissement
 Liste noire

Recherche... Décompte total : 4

Zones de type 'zone de comptage' 4			Zones de type 'zone anti-retour' 0				Zones de type 'autre zone' 0			
Recherche...			Recherche...				Recherche...			
Nom	Société	Service	Nom	Société	Service	Horodatage	Nom	Société	Service	Horodatage
Zone Entreprise	4		tets AR	0			AUTRE ZONE	0		
REGAUDIE DE GIOUX GUILLAUME	TIL Technologies	Commercia								
MERISSE SAMUEL	TIL-TECHNOLOGIES	Projets								
BOUHAFS Cédric	TIL-TECHNOLOGIES	Commercia								
BERGONZO Nathalie										

Dernière mise à jour à 23:35:19

LA SUPERVISION DES ZONES GRACE A SA FENETRE DEDIEE PERMET :

- ▶ D'avoir la liste et comptage des personnes en temps réel par zone et type de zone
- ▶ D'imprimer et d'exporter en TXT et pdf ces listes
- ▶ D'offrir différents paramètres d'affichage

SUPERVISION VIDEO

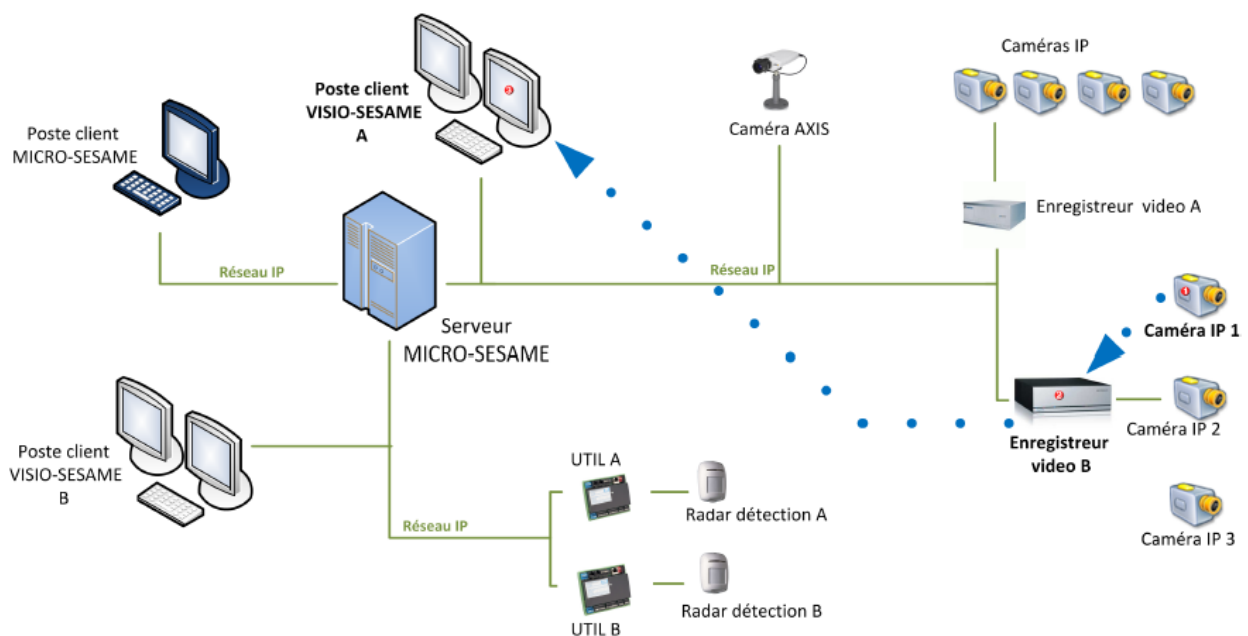
VISIO SESAME

L'OPTION LOGICIELLE MS-SCVXX VISIO-SESAME PERMET DE :

- ▶ Dialoguer, dans les 2 sens, avec de nombreux VMS, et enregistreurs vidéos numériques du marché via leurs SDK (ou une passerelle ASCII) interfacés avec **MICRO-SESAME**.
- ▶ Offrir la majorité des opérations d'exploitation courantes de la vidéosurveillance depuis n'importe quel poste **MICRO-SESAME** et de visualiser facilement les images de caméras connectées sur ces enregistreurs numériques (en direct ou enregistrées)

Et ceci avec plusieurs VMS en simultanées.

Toutes les fonctions de sécurité peuvent être pilotées depuis un superviseur graphique et vidéo unique, **MICRO-SESAME**, commun à tous les systèmes du bâtiment (contrôle d'accès, intrusion, incendie, gestion technique). L'exploitation devient beaucoup plus simple pour l'utilisateur. Les interactions entre la vidéo et les autres systèmes pouvant être complètement automatisées (actions sur alarmes ou sur événements), la rapidité et l'efficacité des traitements sont garanties. Afin d'assurer le bon fonctionnement, le poste client utilisant **VISIOSESAME** doit posséder deux écrans d'affichage.



LE FLUX DE DONNEES TYPIQUE ENTRE LE VMS ET MICRO-SESAME EST :

- ▶ La caméra de vidéosurveillance détecte les images à enregistrer
- ▶ L'enregistreur numérique enregistre les images détectées
- ▶ Le poste client VISIO-SESAME consulte directement les images en temps réel ou les images enregistrées en provenance de l'enregistreur, sans passer par le serveur MICRO-SESAME, en fonction du paramétrage dans le serveur MICRO-SESAME auquel le poste client accède
- ▶ Les images vidéo ne sont pas stockées sur le serveur ou client MICRO-SESAME mais uniquement sur les enregistreurs des VMS

LES FONCTIONNALITES OFFERTES PAR VISIOSESAME SONT :

RECEPTION & EMISSION D'ÉVENEMENTS, ALARMES AVEC PLUSIEURS VMS EN SIMULTANÉE :

- ▶ MICRO-SESAME -> VMS : déclenchement/arrêt enregistrement, pilotage dôme avec choix préposition et zoom, ...
- ▶ VMS -> MICRO-SESAME : alarme détection, défaut caméra, défaut enregistrement, enregistreur connecté, caméra connectée, ...

REDUCTION DU TEMPS DE PARAMÉTRAGE important liée à la fonction Vidéo avec :

- ▶ La notion d'objet « Caméra » dans l'éditeur des synoptiques
- ▶ L'import des libellés caméras des VMS

SUPERVISION DES ALARMES OPERATIONNELLES (détection d'activité par vidéo) et des alarmes de fonctionnement (perte de signaux vidéo ou autres pannes) en provenance des enregistreurs avec le moniteur d'événements, le bandeau d'alarme, temps réel comme toutes les autres

UNE FENÊTRE D'ARCHITECTURE MATÉRIELLE dédiée peut éventuellement s'afficher sur demande

PILOTAGE DES CAMÉRAS DOMES (zoom, choix d'une préposition prédéfinie) par une fenêtre dédiée

ZONE DE VISUALISATION DES CAMÉRAS ENTièrement PERSONNALISABLE selon des scénarios prédéfinis qui positionnent un ou plusieurs moniteurs dans différentes positions et différentes tailles (3 x 3, 2x 2,...). Il est possible d'ajouter autant de moniteurs que de sources. Les couleurs de la barre de titre du moniteur renseignent sur son contenu et son état.

VISUALISATION DE FLUX VIDEO EN DIRECT (Live) simultanés de plusieurs VMS en parallèle sur sélection d'icônes sur synoptiques d'exploitation, sur alarmes

DECLenchement D'ENREGISTREMENTS AUTOMATIQUE qui peut être réalisé par un événement (badgeage sur un lecteur donné), une alarme, un asservissement complexe, une commande manuelle opérateur depuis le synoptique en cliquant sur un bouton ou objet graphique, une commande depuis le Moniteur d'événements

GESTION DU MUR D'IMAGES (fonction matrice) qui permet de gérer un mur d'images constitué de plusieurs écrans et d'afficher une caméra dans une zone (appelée tuile)

L'**ANIMATEUR DE SYNOPTIQUE** permet, à partir d'un simple clic sur un objet d'un synoptique, de :

- ▶ Lancer un affichage d'une ou plusieurs caméras en direct
- ▶ Visionner d'une séquence enregistrée pour une source donnée
- ▶ Associer automatiquement des paramètres prédéfinis pour l'affichage (sélection d'un groupe de moniteurs, la préposition choisie, la source vidéo,...)

ASSERVISSEMENT D'UNE ACTION VIDEO à un événement ou à une télécommande d'un opérateur. Par exemple pré-positionnement automatique d'un dôme sur détection de badge interdit.

VISUALISATION DES SEQUENCES VIDEO ENREGISTREES associée à une alarme directement depuis la fonction « historique » de MICRO-SESAME qui assure la synchronisation des informations (fichier d'historique unique pour le contrôle d'accès, l'intrusion et la vidéo) et facilite ainsi grandement la recherche d'une séquence vidéo. Pas besoin de connaître la source, le nom de la caméra, l'heure, un clic sur ce symbole vidéo associé à l'alarme suffit et indique qu'il existe un enregistrement vidéo associé

UNE ZONE/BARRE D'ACTIONS RAPIDES, en bas de l'écran, offre, outre les touches magnéscope de gestion des enregistrements, des commandes directes actives selon votre enregistreur : Prendre une capture de l'image en cours, Activer l'enregistrement, Changement du mode de lecture, direct/enregistrement, Libérer un moniteur, ...

LES SOLUTIONS VMS INTERFACÉES A MICRO-SESAME

La liste des solutions, des versions compatibles et des fonctionnalités accessibles est en constante évolution. Il existe un guide spécifique sur **VISIO-SESAME** disponible auprès de votre interlocuteur TIL qui détaille la liste des VMS et leurs fonctions compatibles avec **MICRO-SESAME**. Selon les VMS, toutes les versions de SDK ne sont pas supportées et toutes les fonctionnalités ne sont pas disponibles. Il convient de valider auprès de TIL TECHNOLOGIES les compatibilités avant toute installation.

Il est fortement conseillé de consulter les prérequis informatiques pour les postes d'exploitation vidéo (surface d'écran, OS, carte graphique, carte réseau...) et pour le réseau (débit, latence, ...) indiqués par le constructeur de l'enregistreur vidéo auquel les postes clients VISIO-SESAME accèderont.

A titre indicatif, voici une liste de VMS intégrés à **MICRO-SESAME** :

- ▶ AXIS
- ▶ BOSCH BVMS
- ▶ GEUTEBRUCK Geviscope & G-Scope
- ▶ GENETEC Security Center & Omnicast
- ▶ VIDEOWAVE OneTrack
- ▶ MILESTONE XPROTECT (CORPORATE /EXPERT /PROFESSIONAL)
- ▶ HYMATOM VisioSpace
- ▶ CASD VISIMAX VM500
- ▶ VIVOTEK, AVIGILON, ARGOS via ASCII, (échange alarmes sans flux vidéo)

GEUTEBRUCK

Genetec



PLUG-IN MILESTONE

Pour les clients qui exploitent la VIDEO en priorité et souhaitent une supervision unifiée, MICRO-SESAME dispose de l'option **MS-MILESTONE-IP** qui intègre le PLUG-IN de MILESTONE ACCESS CONTROL, pour superviser le contrôle d'accès TIL depuis l'interface de supervision X-PROTECT de MILESTONE.

Cette interface, certifiée par MILESTONE, permet au superviseur VMS XPROTECT de :

- ▶ Gérer les alarmes de TIL (MICRO-SESAME -> X-PROTECT)
- ▶ Gérer les passages de badges avec Photos (MICRO-SESAME -> X-PROTECT)
- ▶ Lancer des télécommandes d'ouverture des accès gérés sur MICRO-SESAME (MICRO-SESAME <- X-PROTECT)

Milestone Verified


Confirmation of Compatibility

Partner: TIL Technologies

Partner Product: Milestone Access Control Plugin 2018.3.6
MICRO-SÉSAME 2018.4.0

Milestone Product XProtect®: Corporate 2019 R3

Date of Verification: 23-12-2019



POINTS DE CONTROLE VISUEL DES ACCES (PCVA)

Sur un accès équipé d'un lecteur de badges et d'une caméra vidéo, l'option **MS-CVA** permet, lorsqu'une personne badge, d'afficher simultanément la photo du titulaire du badge et l'image vidéo de l'accès.

En surimpression de la photo, une icône indique le statut du badge (autorisé, interdit, inconnu).

L'ouverture de la porte peut être manuelle ou automatique ou optionnelle selon le niveau de sécurité. D'autres actions peuvent être paramétrées, par exemple l'allumage de la lumière, l'affichage d'un message, la désactivation de la détection l'intrusion sur la zone...

GESTION INTRUSION

Il existe des documents spécifiques sur la gestion intrusion disponibles auprès de votre interlocuteur TIL habituel (Guide de paramétrage de l'intrusion, Principe de câblage de la détection intrusion, Guide de paramétrage sur la transmission, ...)

La fonction intrusion est native dans la solution TIL TECHNOLOGIES. Elle est mise en œuvre par :

LE SERVEUR MICRO-SESAME GERE LES UTILISATEURS ET LEURS DROITS INTRUSION CENTRALISES MULTI-CENTRALE.

Un utilisateur et son code d'identification est créé une seule fois pour X centrales :

UN "UTILISATEUR TILLYS" est une personne autorisée à s'identifier sur le clavier intrusion de la centrale **TILLYS**. Chaque utilisateur est associé à un profil intrusion, à des droits d'utilisation ainsi qu'à un code d'identification intrusion qui est généré automatiquement. Possibilité de dupliquer un profil intrusion

DROITS D'UTILISATION : Les droits d'utilisation sont les actions qu'un utilisateur est autorisé à effectuer à partir du clavier intrusion (accès au menu, mise en/hors service d'un groupe, effectuer une dérogation...etc.). Chaque utilisateur peut recevoir des droits différents

The screenshot shows a web application interface for user management. The title bar indicates the user is an administrator. The main content area is titled 'Identifié 1 sur 3' and shows a form for 'Identité du permanent' with fields for 'Civilité', 'Nom', 'Prénom', 'Id2', 'Société', and 'Service'. Below this, there are sections for 'Validité associée à la personne' (with a date range from 31/01/2017 to 31/01/2018), 'Visitable' (radio buttons for 'Oui' and 'Non'), and 'Statut' (a dropdown menu set to 'Normal'). A navigation bar at the bottom of the form includes tabs for 'Accès', 'Informations', 'Entités', 'Identifiants', 'Activité', 'Opérateur', and 'Intrusion' (which is currently selected). Below the navigation bar, there are fields for 'Nom court' (Id2), 'Codes d'authentification' (with an 'Afficher en clair' button), and a 'Télécharger' button labeled 'Accéder à la fenêtre de téléchargement'. A note indicates the last modification was 2 hours ago. Below this, it says '1 fonction(s) intrusion' with a green plus sign. A table lists intrusion functions with columns for 'Activée', 'UTL Activée', 'UTL Nom', 'Profil intrusion', 'Code d'authentification', 'Droits d'utilisation', and 'Création'. The table contains one row: 'Oui', 'Oui', 'Utlv3 Profil 2', '****', '12 élément(s)', and 'Il y a 7 heure(s) par ADMINISTRATEUR'. At the bottom, it shows '1 élément(s) sélectionné(s)' and a '25 par page' dropdown menu.

LES CENTRALES TILLYS NG fonctionnent de manière autonome avec leurs modes opératoires ayant été au préalable configurés et téléchargés depuis MICRO-SESAME. Chaque TILLYS NG a une capacité de :

- ▶ 32 Groupes de points/détecteurs
- ▶ 624 détecteurs / points
- ▶ 150 utilisateurs locales
- ▶ 8 fonctions claviers par bus, 16 fonctions sirènes
- ▶ Une fonction transmetteur IP « TIP » intégrée

DES CLAVIERS INTRUSION TACTILLYS NG, raccordés aux bus RS485 des TILLYS, pour l'exploitation local autonome d'une centrale intrusion en quelques clics. Chaque clavier peut être associé à une liste de groupes limitant les possibilités d'exploitation à une partie restreinte de l'installation

- ▶ Nouveau clavier moderne et ergonomique avec son écran tactile 7 pouces, installation en mode Portrait ou Paysage, son lecteur de badge en option dont la sécurité des clés est assurée par un coffre-fort HSM EAL5+

DES MODULES DEPORTES D'ENTREES surveillées / sorties, raccordés aux bus des TILLYS, sur lesquels sont connectés des capteurs, détecteurs et des actionneurs (sirènes, commande éclairage...)

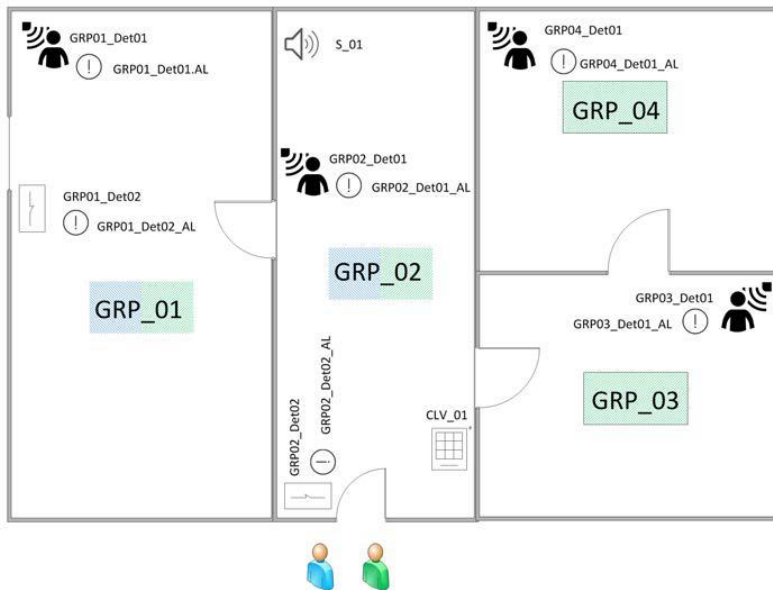
DES MODULES SPECIFIQUES INTRUSION haute sécurité **EQUILOCK** ayant 2 bus sécurisés de 32 petits transpondeurs adressables et intégrés dans les détecteurs

LA SOLUTION OFFRE UNE GRANDE RICHESSE & ADAPTABILITE FONCTIONNELLE NOTAMMENT GRACE AUX FONCTIONS SUIVANTES :

- ▶ Chaque point/détecteur doit être associé à un type de point qui conditionne le déclenchement d'une alarme. Les types possibles sont : Alarme intrusion, Alarme 24/24, Alarme intrusion silencieuse, Alarme technique, Défaut système silencieux, Appel d'urgence, Incendie
- ▶ Groupe de détecteurs définit un ensemble de détecteurs, points ayant un lien entre eux (bâtiment, étage, service, périmétrie, zone, ...) et bénéficiant d'un mode de gestion commun comme :
 - La mise en/hors surveillance
 - L'envoi de codes d'alarme vers un télésurveilleur
 - La gestion d'une ou plusieurs sirènes
 - La mise en œuvre de pré-alarme ou de mécanisme de dérogation



Nouveau clavier TACTILLYS NG (2020)



Ex :

Le profil 1 peut mettre en/hors service le GRP_01 et GRP_02.

Le profil 2 peut mettre en/hors service tous les groupes

POINTS EN DERANGEMENT : Un point en dérangement est un point qui générerait l'utilisateur dans certains cas spécifique (ex. Lors de travaux...etc.)

EJECTION : Fonction permettant d'exclure de la surveillance un point de manière définitive ou momentanée afin de permettre la mise en surveillance d'un groupe auquel il appartient et d'éviter le déclenchement systématique d'alarmes ou une action du télésurveilleurs notamment si le point est par exemple en dérangement ou peu important. On distingue plusieurs modes d'éjection (Éjection interdite, Éjection manuelle, Éjection automatique, Éjection avec réinjection automatique, Éjection permanente). Une action Ré-injection permet de mettre fin à l'éjection d'un point.

PRE-ALARME : correspond à une temporisation paramétrable qui permet, via une action brève des sirènes, d'avertir les occupants de l'imminence de la mise en surveillance du bâtiment tout en leur laissant la possibilité de relancer une dérogation

DEROGATION : Fonction qui consiste à repousser d'une durée paramétrable et sur demande explicite une mise en service automatique sur programme horaire (trigger). La demande est possible depuis le clavier intrusion par un utilisateur TILLYS ou par Microcode ou télécommande depuis le superviseur MICRO-SESAME

MISE EN SERVICE AVEC TRIGGER : Permet un lancement automatisé de la mise en surveillance d'un groupe de la centrale (ex : sur plages horaires). Les mises hors surveillance automatisées sont possibles mais à déconseiller pour des raisons évidentes de sécurité.

TEMPORISATION : Un groupe de points peut être temporisé d'une durée paramétrable en entrée ou/et en sortie pour permettre d'atteindre le clavier de mise en/hors surveillance quand ce dernier est en zone surveillée. Les valeurs des temporisations s'appliquent au groupe et le fait d'être temporisé en Entrée ou/et en Sortie se définit pour des points concernés du groupe.

MISE EN/HORS SURVEILLANCE : La mise en surveillance d'un ou plusieurs groupes est l'action de rendre opérationnelle la surveillance des points de type alarme intrusion liés à ce(s) groupe(s). La demande de mise en surveillance peut être effectuée de différentes manières :

- ▶ Par une opération d'un utilisateur sur un clavier intrusion TACTILLYS NG
- ▶ A l'aide d'une plage horaire
- ▶ Par toute autre action, asservissements configurés selon des entrées, événements, de tous les métiers (contrôle d'accès, intrusion, technique, incendie, ...)

ACQUITTEMENT d'un point en alarme depuis le superviseur (voir supervision)

INHIBITION d'un point ou un groupe de points rendu temporairement inopérant depuis le superviseur (voir supervision)

LA FONCTION TRANSMETTEUR IP « TIP » INTEGREE DE LA CENTRALE TILLYS NG :

La centrale **TILLYS NG** intègre une fonction transmetteur IP « **TIP** ». Elle permet la transmission des alarmes intrusion (et contrôle d'accès & techniques) vers un télésurveilleur par IP sous le protocole « **TIP** » de TIL, basé sur les standards ID-Contact ou CESA 200, et qualifié chez ESI et Azur soft.

Les principales fonctions liées à la transmission offrent une grande richesse, adaptabilité fonctionnelle :

LES CAPACITES DE CHAQUE UTL SONT DE :

- ▶ 4 destinataires & utilisateurs potentiels pour la réception des alarmes (centre de télésurveillance) et qui pourront effectuer des manipulations sur la centrale
- ▶ 8 profils d'appel de transmission des alarmes permettent de définir quel(s) destinataire(s) contacter et dans quel ordre
- ▶ 32 télécommandes : actions qui pourront être déclenchées par les utilisateurs

POLLING : permet au destinataire d'interroger la centrale périodiquement afin de détecter si cette dernière est toujours présent sur le réseau

TEST CYCLIQUE : la centrale réalise une transmission périodique vers un destinataire afin de vérifier le fonctionnement de la ligne de communication. La périodicité est paramétrable (heure précise, liée à la mise en service d'un ou plusieurs groupes, différent par destinataire)

TABLE DE CODAGE : Une table de codage est un tableau où l'on va définir un code événement pour chaque type d'alarme (intrusion, accès, incendie ...Etc.) qui sera envoyé au télésurveilleur. Ces codes sont donc à définir avec le télésurveilleur choisi

INTERPHONIE

EXPLOITER LES INTERPHONES DEPUIS MICRO-SESAME

MICRO-SESAME permet de dialoguer avec les centrales d'interphonie **COMMEND IP** (GE800, GE300, IS300, Virtuosis) permettant d'effectuer la majorité des opérations courantes de communication depuis n'importe quel poste d'exploitation

MICRO-SESAME :

- ▶ Affichage des appels interphones vers le poste maître.
- ▶ Traitement différencié selon 2 niveaux : communication normale ou urgence.
- ▶ Prise d'appel, interruption ou annulation.
- ▶ Virtualisation totale du poste maître (avec micro et haut-parleurs branchés directement sur le poste d'exploitation).
- ▶ Mise en communication de 2 postes (bouton direct dans la supervision graphique ou clavier du poste maître virtuel).
- ▶ Ecoute à distance.
- ▶ Transfert des appels du poste maître vers un autre poste (par exemple selon jour/nuit).
 - Import des abonnés
 - Appeler un abonné et décrocher/raccrocher
 - Notification d'appels (avec distinction entre normal et urgent)
 - Transfert d'appel de nuit
 - Possibilité de connexion au serveur d'interphonie



EXPLOITER LES INTERPHONES DEPUIS MICRO-SESAME

Avec l'intégration de l'interphonie dans **MICRO-SESAME**, les fonctions de communication sont pilotées depuis la même interface graphique que les autres systèmes de sécurité du bâtiment (contrôle d'accès, vidéo, GTB...).

Les actions sur évènement peuvent donc être complètement automatisées. L'exploitation devient beaucoup plus simple pour l'utilisateur et la rapidité des traitements est garantie.

Par exemple, l'appel interphone peut commander un asservissement vidéo pour un contrôle visuel instantané mais aussi commander l'éclairage.

Enfin, tous les appels et changements de statut sont également tracés dans l'historique **de MICRO-SESAME**.

PLAN D'OPERATION INTERNE (POI)

ASSISTANCE AUX EVACUATIONS ET AUX INTERVENTIONS DE SECOURS

Le POI définit les mesures d'organisation, les méthodes d'intervention et les moyens nécessaires que l'exploitant doit mettre en œuvre pour protéger son personnel, les populations et l'environnement. Il est principalement demandé pour les installations présentant les risques les plus importants, notamment les installations faisant l'objet d'un plan particulier d'intervention (PPI).

INTEGRATION DANS MICRO-SESAME

L'application d'assistance POI intégrée dans MICRO-SESAME intervient dans le processus de protection du personnel à travers des IHM, fenêtres dédiées simples et par les fonctions suivantes :

- ▶ Paramétrage des zones POI en 2 catégories : sécurisées et non sécurisées
 - ▶ Les zones sécurisées sont celles de rassemblement du personnel à l'abri des dangers
 - ▶ Les zones non sécurisées correspondent au reste du site
- ▶ Fourniture de la liste et nombre des personnes présentes sur site en temps réel par zone, avec affichage de leurs habilitations (si utilisé), selon leurs badgeages sur des lecteurs de badge
- ▶ Suivi en temps réel de la migration du personnel des zones de travail vers les zones sécurisées, après déclenchement du POI, pendant les exercices ou incidents
- ▶ Recherche d'une personne pour connaître sa localisation (zone sécurisée ou non)
- ▶ Edition du nom des personnes avec trombinoscope pour les zones sélectionnées
- ▶ Export pdf possible de la liste des personnes dans un répertoire donné
- ▶ L'exploitation et l'affichage des zones POI se lance depuis un synoptique ou le menu général



Pour faciliter le recensement sur les points de rassemblement (zones sécurisées), il est pratique d'utiliser le lecteur de badge portatif **MOBILIS**, prévu pour une utilisation extérieure. Plus besoin de câbler de lecteurs filaires, la lecture des badges est effectuée par les responsables d'évacuation.

CONTROLE DU TEMPS DE REPOS

RESPECT DE LA LEGISLATION DU TRAVAIL

L'article L3131-1&2 du code du travail français stipule que tout salarié bénéficie d'un repos quotidien d'une durée minimale de onze heures consécutives et d'un repos hebdomadaire d'une durée minimale de 35 heures consécutives.

MICRO-SESAME, à travers la fonction « **Contrôle du temps de repos** », vous permet de respecter le code du travail facilement en utilisant le contrôle d'accès du bâtiment.

L'analyse automatique des passages badges des salariés permet de calculer si ces temps de repos légaux, ou d'autres stipulés par l'entreprise, ont été respectés et offre plusieurs finalités au choix :

BLOQUER AUTOMATIQUEMENT LES ACCES aux salariés n'ayant pas respecté les délais adéquats entre sorties et entrées sur le site, de manière temporaire jusqu'à l'heure le respectant

SIGNALER L'INFORMATION D'INTERDICTION D'ACCES temporaire avec la date et l'heure de la prochaine autorisation d'accès aux exploitants dans la fiche identifié, avec ou sans blocage associé au choix

LE BLOCAGE TEMPORAIRE peut être supprimé manuellement par un opérateur habilité

GENERER DES RAPPORTS pour visualiser les anomalies sur les temps de repos

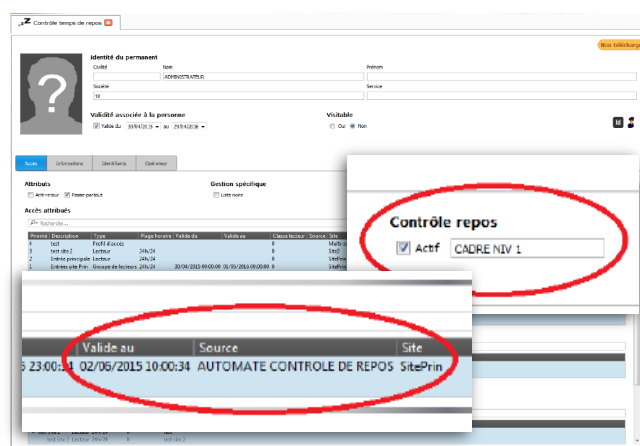
EVENEMENTS EXCEPTIONNEL : dans ce il est également possible de « débrayer » la fonction de contrôle du temps de repos pour tous les salariés

Pour traiter rapidement de grande population, la fonction de contrôle du temps de repos s'appuie sur la notion de « régimes de repos ». Chaque « régime de repos » nécessite de déclarer des lecteurs d'entrée/sortie, d'établir les durées & jours du repos, et les heures de début des calculs hebdomadaires et journaliers. Il est possible d'enregistrer plusieurs « régimes de repos » afin que chaque identifié soit contrôlé suivant les règles et lecteurs qui le concernent. Cette attribution peut être réalisée directement dans **MICRO-SESAME** ou, via une passerelle avec la base RH de l'entreprise.

Lorsque l'option est activée pour un salarié, les passages lecteurs refusés sont identifiés « hors plage » dans le moniteur d'évènement et l'historique **MICRO-SESAME**.

En ouvrant la fiche de l'identifié, il est possible de visualiser l'interdiction d'accès temporaire et de connaître la date et l'heure de la prochaine autorisation d'accès.

Si besoin, ce blocage temporaire peut être supprimé manuellement par un opérateur habilité.



Enfin, pour effectuer un suivi plus global des salariés par les services RH et Sécurité, le Requêteur universel de **MICRO-SESAME** permet de lancer des analyses hebdomadaires pour générer un fichier contenant tous les accès refusés « hors plage » (voir partie Historiques, Rapports et Requêteur).

GESTION DES PARCOURS

ASSISTANCE AUX RONDES TERRAIN

La Gestion des Parcours (**MS-PCR**) est une option logicielle de **MICRO-SESAME** permettant de créer des rondes et d'effectuer le suivi des rondiers (agents) amenés à effectuer les rondes sur un site en temps réel.

Une ronde de surveillance est un itinéraire prédéfini de lecteurs, sur lesquels les rondiers en charge de la ronde doivent présenter leur identifiant successivement. Cette option permet de contrôler la progression de plusieurs rondiers sur 64 parcours différents. (un agent/rondier par ronde).

LA GESTION DES PARCOURS peut utiliser les lecteurs déjà existants sur votre site sans lecteurs ou matériel spécifiquement dédié à la réalisation de rondes.

LA RONDE peut être réalisée sans droit d'accès aux lecteurs concernés mais dans ce cas sans accès autorisé. Le rondier peut utiliser son identifiant (badge) de contrôle d'accès pour réaliser la ronde.

DES DROITS OPERATEURS SPECIFIQUES existent pour la gestion des rondes (Accès à l'application et gestion des rondes, sans droits d'accès nécessaires) pour des opérateurs dédiés au profil restreint par exemple.

Pour lancer une ronde, sélectionner une ronde de la liste, et choisir le rondier en charge d'effectuer la ronde sur le terrain. Le temps défini entre chaque lecteur doit être respecté. En cas de dépassement de temps imparti entre 2 lecteurs, un événement ou une alarme est automatiquement déclenchée sur le moniteur d'événement, précisant le rondier et le parcours concerné. Sur alarme, les actions possibles sont : Acquitter, Afficher le synoptique, Visualiser la caméra associée dans **VISIOSESAME**.


The screenshot displays the MICRO-SESAME software interface. On the left, a sidebar shows 'Evénements' with 'Aucune alarme' and 'Etat des propriétés'. The main area features a table of events with columns for 'Date-Heure', 'Élément', and 'Message'. The 'Le moniteur d'événements' entry is highlighted. On the right, a detailed view of an alarm is shown, titled 'Ronde_1 - Temps dépassé', with a timestamp of 'Le mar. 30 oct. 2018 14:55:43' and the message 'la propriété est passée dans l'état 'L'alarme s'est déclenchée.''. Below the message, an 'Actions' panel offers options: 'Acquitter', 'Visualiser la caméra', 'Visualiser l'enregistrement', and 'Afficher le synoptique'.

Date-Heure	Élément	Message
jeu. 25 oct. 2018 10:..	Lect1	Rondier Paul : Passage autorisé
jeu. 25 oct. 2018 10:..	Ronde_1 - Id prochain lecteur	2
jeu. 25 oct. 2018 10:..	Ronde_1 - Id précédent lecteur	1
jeu. 25 oct. 2018 10:..	Ronde_1 - Nombre d'étapes terminées	1
jeu. 25 oct. 2018 10:..	Ronde_1 - Durée max étape	60
jeu. 25 oct. 2018 10:..	Ronde_1 - Date/heure de début de l'étape	1540457447
jeu. 25 oct. 2018 10:..	Lect2	Rondier Paul : Passage autorisé
jeu. 25 oct. 2018 10:..	Ronde_1 - Id rondier	0
jeu. 25 oct. 2018 10:..	Le moniteur d'événements	0
jeu. 25 oct. 2018 10:..	Ronde_1 - Id précédent lecteur	0
jeu. 25 oct. 2018 10:..	Ronde_1 - Nombre d'étapes terminées	0
jeu. 25 oct. 2018 10:..	Ronde_1 - Date/heure de début	0
jeu. 25 oct. 2018 10:..	Ronde_1 - Durée max étape	0
jeu. 25 oct. 2018 10:..	Ronde_1 - Date/heure de début de l'étape	0
jeu. 25 oct. 2018 10:..	Ronde_1 - En cours	Non

Un tableau dédié indique en temps réel les différentes informations et états des rondes :

- ▶ En cours, le rondier qui réalise la ronde,
- ▶ Le délai passé depuis le démarrage de la ronde,
- ▶ Le temps que le rondier a pour présenter son badge sur le prochain lecteur avec un code couleur de progression (verte, jaune, orange, rouge) selon le temps restant
- ▶ Le temps total pour chaque étape
- ▶ Le nombre total d'étapes
- ▶ L'étape actuelle
- ▶ Le dernier lecteur où l'identifiant du rondier a été détecté
- ▶ Le point ou l'identifiant du rondier doit être présenté

L'opérateur peut aussi accorder un délai supplémentaire pour le passage sur le lecteur (possible à tout moment), annuler la ronde.

Actions	Ronde	En cours	Rondier Nom/Prénom	Rondier Photo	Début	Temps restant	Durée max étape	Étape	Progression	Dernier lecteur	Prochain lecteur
■	Ronde_1	Oui	Rondier Paul		il y a moins d'u...	5m 44s <input type="text"/>	360 sec.	0/2	<input type="text"/>		Lect1

▶ Gestion des rondes : Onglet Rondes

HISTORIQUES, REQUETEUR & JOURNAUX

Ces fonctions sont intégrées nativement dans la solution **MICRO-SESAME**

HISTORIQUE

La fonctionnalité « **Historique** », depuis un poste client lourd, permet de consulter tous les événements inscrits dans la base de données. Elle trace à la fois l'exploitation du bâtiment (passages badges, alarmes techniques...), la vie du système et les actions des opérateurs.

La capacité de stockage n'est pas limitée. Par défaut, la durée de rétention des événements est réglée à 30 jours, mais cette valeur est paramétrable comme par exemple 3 mois, valeur utilisée par la CNIL.

Les critères de recherche et d'affichage des événements, alarmes, mouvements sont présentés par une vue globale avec des critères communs et par les onglets suivants correspondants à des types d'événements :

- ▶ Contrôle d'accès.
- ▶ Évènements techniques.
- ▶ Évènements système.
- ▶ Audit des modifications (actions des opérateurs).
- ▶ Fusion de tous les évènements.

Ces champs sont différents pour chacun des onglets. Par défaut, la période de recherche est positionnée sur l'heure en cours et sur les 7 derniers jours.

The screenshot shows the 'Historique' application window. At the top, there are search options: 'Période de recherche' (Pré définie, Durée, Avancée) set to '7 derniers jours', and 'Tri chronologique' (Normal, Inversé) set to 'Normal'. A 'Rechercher' button is present. Below this, there are several tabs: 'Contrôle d'accès', 'Evénements techniques', 'Evénements techniques (anciennes variables)', 'Evénements systèmes', 'Note', 'Audit des modifications', 'Fusion (tous les événements)', and 'Fusion (tous les événements, anciennes variables)'. The 'Evénements badges' tab is active, showing filters for 'Décision' (Autorisé, Attente, Interdit) and 'Raison' (toutes). There are also filters for 'Site', 'Type d'identifié', and 'Statut de l'identifiant'. A table header is visible at the bottom with columns: Date - Heure, Groupe de caméra, Décision, Raison, Commentaire lect, Norm, Prénom, 01 - Restauration, Type d'identifié, Site, and Id utilisateur.

La fonction Historique offre une finesse, une personnalisation et rapidité au client grâce à :

DES FILTRES SUR CERTAINES DONNEES (champs) : ils permettent d'éditer très précisément les événements recherchés. Pour avoir des choix rapides et pertinents de filtres, ces derniers peuvent être dans des listes déroulantes prédéfinies selon le paramétrage du système. Par exemple, le choix du site (en gestion multi-sites), du type d'identifié (visiteur ou permanent), du statut de l'identifiant (perdu, volé, actif...),

SAUVEGARDE ET NOMMAGE : Pour simplifier les besoins récurrents, il est possible pour chaque opérateur de sauvegarder et nommer les recherches types avec ses paramètres et filtres

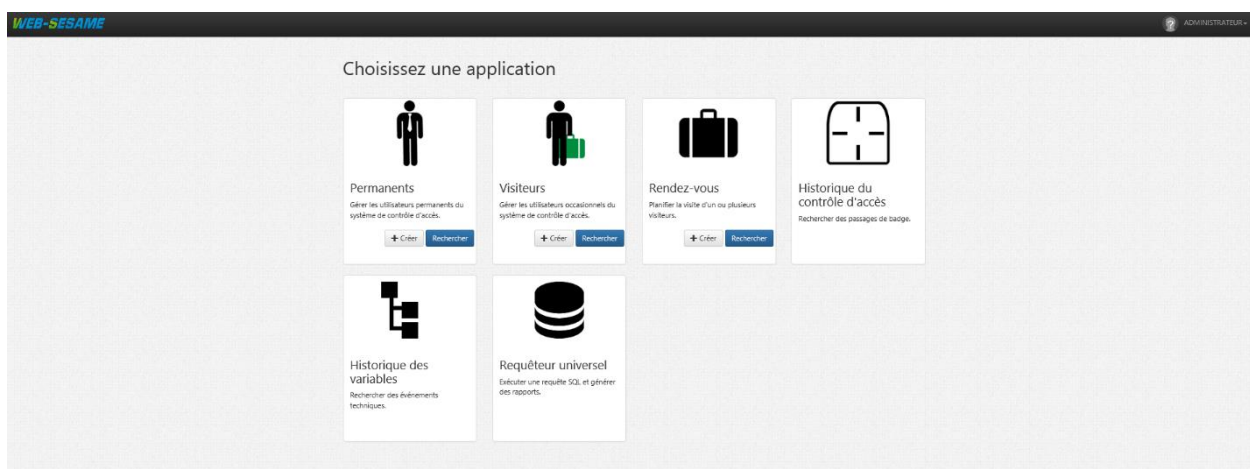
pré-remplis. Ces différentes recherches types sont enregistrées dans la fenêtre « filtres prédéfinis » avec le choix entre sauvegarde privée (visible que de l'opérateur qui l'a créée) ou public (disponible pour les autres opérateurs). Cela évite de ressaisir les mêmes critères de recherche à chaque fois et représente un gain de temps important

FILTRAGE de la visualisation des propriétés selon le droit « catégorie » de l'opérateur

AJOUT DE PRECISIONS SUR PASSAGES INTERDITS : site, identifiant inconnu, contrôle renforcé, passage contrôlé, pas d'accès

WEB-SESAME

Le portail **WEB-SESAME** propose entre autres ces 3 applications : Historique du contrôle d'accès, Historique des variables (propriétés), Requêteur universel



HISTORIQUE DU CONTROLE D'ACCES WEB-SESAME

L'interface Web de **MICRO-SESAME** inclut un onglet permettant de visualiser facilement l'historique de contrôle d'accès pour rechercher des passages de badge

Différents paramètres et filtres, date, type d'évènement (badges autorisés, interdits...), peuvent être appliqués pour faciliter la consultation des données. Les champs des résultats à afficher sont complètement paramétrables (civilité, nom, identifiant...).

HISTORIQUE DES VARIABLES / PROPRIETES WEB-SESAME

L'application Historique des variables (propriétés) permet la recherche d'évènements techniques liés au système de contrôle d'accès.

RÉSULTATS					
3 élément(s) trouvé(s)					
Date - Heure	Description de la propriété	Est une alarme	Forçage	Message	Nom de supervision
03/12/2018 à 17:56:09	Connexion avec MICRO-SESAME	Oui	Aucun changement	Déconnectée	UTL_1.connected
03/12/2018 à 17:55:58	Explication de la déconnexion	Non	Aucun changement	Aucune erreur	LINE_1.connectedReason
03/12/2018 à 17:55:58	Connexion avec MICRO-SESAME	Non	Aucun changement	Connectée	LINE_1.connected

5 par page

REQUETEUR UNIVERSEL WEB-SESAME

Accessible également depuis le portail **WEB-SESAME**, le Requêteur Universel est un utilitaire permettant l'extraction de tous types d'informations contenues dans la base de données **MICRO-SESAME** à travers l'exécution d'une requête SQL et la génération d'un rapport / résultat.

Le requêteur universel web offre les possibilités suivantes :

REQUETES : elles existent nativement dans le produit (voir liste ci-dessous) vous permettant d'avoir les recherches les plus courantes. Bibliothèque des requêtes disponibles dans : Serveur\ScriptsSql\SqlServer\Requestor\FR

RESULTAT, RAPPORT : il s'affiche directement dans l'IHM après exécution de la requête souhaitée. Il est possible d'exporter ce résultat dans un fichier au format CSV et pdf. Vous pourrez alors exploiter le fichier CSV depuis un tableur type Excel ou un éditeur de texte pour éditer des graphiques, faire des statistiques, ...

EXECUTION D'UN RAPPORT : sur changement de propriété et envoi par mail automatique

CREATION DE REQUETES PERSONNALISEES POSSIBLE :

- ▶ Par l'intégrateur, le client final, ayant une bonne connaissance du langage de script SQL, pour des requêtes simples à partir des exemples des requêtes existantes,

- ▶ Par TIL TECHNOLOGIES, sur projet, pour réaliser des requêtes plus complexes selon les besoins des clients, le schéma de la base de données & du contenu des tables (MCD) n'étant pas documenté

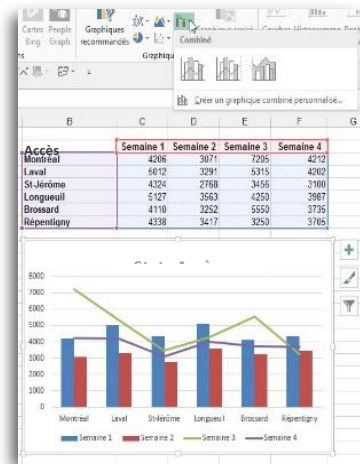
IMPORTER, EXPORTER DES REQUETES au format « fichier.json » . Il est possible d'importer une requête qui a été au préalable exportée d'un autre système MICRO-SESAME

FILTRES : La requête peut inclure des paramètres permettant de filtrer le résultat attendu selon par ex une date, heure, choix dans une liste déroulante (société, service, lecteur, ...), personne, ... Si un champ du filtre n'est pas rempli, cela concerne « tous » du champ concerné

OUTIL « EXTRACTEUR » : disponible dans la solution, permet de réaliser des rapports automatiques & périodiques de requêtes désirées dans des répertoires définis pour simplifier vos tâches dans des besoins récurrents

LISTE DES REQUETES EXISTANTES EN BIBLIOTHEQUE :

- 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 DE QUELQUES REQUETES POUR EXEMPLE :

- ▶ « Requête repos » : Liste des identifiés n'ayant pas respectés leurs temps de repos
- ▶ Requête « Identifié dévalider mois prochain » : Liste des personnes qui vont être invalide à une date donnée. Dans l'IHM de cette requête ci-dessous, vous trouvez les filtres : date début-fin, Matricule, Nom, prénom

GRAPHIQUES ET COURBES DANS MICRO-SESAME

MICRO-SESAME intègre une application Graphique/courbe qui permet de visualiser graphiquement l'évolution de variables numériques ou logiques suivant une période de temps définie et sous forme de courbes. Cette application offre les possibilités suivantes :

- ▶ Une période de recherche spécifique pour filtrer les données obtenues
- ▶ Les courbes - données obtenues sont exportables au format PDF ou un fichier.JSON à un emplacement choisi. Les fichiers .JSON peuvent aussi être utilisés pour l'import de paramètres externes
- ▶ Les graphes permettent de regrouper plusieurs courbes sous un même graphe
- ▶ Les caractéristiques suivantes d'affichage des courbes sont paramétrables :
 - Couleurs sur courbe, fond, axes, textes, seuils | Titre du graphique | Libellé de X et Y | Type de courbes parmi les 3 types de courbes disponibles au paramétrage :
 - Ligne : utilisées par les « propriétés » de MICRO-SESAME (Notion de 3 seuils possible avec nom et la valeur de chaque seuil)
 - Histogramme : générés à partir d'une requête SQL
 - Camembert : générés à partir d'une requête SQL

Graphique / Courbe

Courbe Graphe

Recherche

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

Heure	Valeur
08:00:00	100,0
10:00:00	50,0
12:00:00	25,0
14:00:00	20,0
16:00:00	10,0
18:00:00	5,0

Couleurs

Graphe :

Couleur Fond

Couleur Axe

Couleur Texte

Graphique / Courbe

Courbe Graphe

Recherche

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

Temps	Valeur
00:00:00	0,0
00:04:07	24,8
00:08:15	49,5
00:12:22	74,3
00:16:30	99,0

Couleurs

Graphe :

Couleur Fond

Couleur Axe

Couleur Texte

Couleur Courbe

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

PASSERELLES ET INTERFACES

SUPERVISEURS, AUTOMATES GTC, INCENDIE, INTRUSION, AFFICHAGE...

MICRO-SESAME dispose d'interfaces qui lui permettent de gérer de la biométrie, superviser d'autres équipements de gestion technique, de sûreté ou de sécurité ou de dialoguer avec d'autres applications du système d'information.

SUPERVISEURS, AUTOMATES GTC, INCENDIE, INTRUSION, AFFICHAGE...

MICRO-SESAME est capable de gérer les lecteurs biométriques de plusieurs marques & gammes : IDEMIA, STID, HANDKEY.

Pour la marque IDEMIA (ex MORPHO) :

- ▶ Lecteurs des séries SIGMA (empreintes digitales), MORPHOWAVE COMPACT (lecture à la volée sans contact des empreintes digitales,....
- ▶ L'enrôlement biométrique se fait à travers le logiciel MORPHOMANAGER d'IDEMIA.
- ▶ TIL a intégré la passerelle MORPHO-BRIDGE de MORPHOMANAGER pour envoyer les fiches personnes et l'identifiant créés dans MICRO-SESAME vers MORPHOMANAGER pour éviter une double saisie
- ▶ Solution biométrique avec :
 - badge + bio (1 :1) conforme recommandation CNIL AU52 : les empreintes sont dans le badge de chaque personne et pas dans une base de données centralisée
 - bio seul (1:N) soumis à plus de contraintes par la CNIL AU53 car les empreintes sont centralisées dans une base de donnée qui doit être protégée (voir RGPD)

Pour la marque STID :

- ▶ Lecteurs de la gamme ARCHITECT
- ▶ TIL a intégré les lecteurs biométriques en mode transparents avec le protocole conforme ANSSI (SCCPv1) et le protocole certifié ANSSI (SCCPv2)
- ▶ Solution biométrique avec badge + bio (1 :1) conforme recommandation CNIL AU52 : les empreintes sont dans le badge de chaque personne et pas dans une base de données centralisée

PROTOCOLES INFORMATIQUES STANDARDS

Il est possible d'interfacer des automates industriels ou systèmes de GTC en protocole **MODBUS IP** (Maître ou esclave), comme :



MICRO-SESAME dispose des protocoles **OPC UA** sécurisé serveur uniquement, ainsi que **OPC DA2**, client ou serveur. Ces protocoles sont très utilisés dans le monde de l'automatisme, permettant la liaison avec des systèmes de GTC ou GTB.

Il est ainsi possible d'interfacer :

DES SUPERVISEURS

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



DES AUTOMATES

- ▶ Schneider
- ▶ Schneider

DES CENTRALES INCENDIE COMPATIBLES AVEC MODBUS IP OU OPC

AUTRES INTERFAÇAGES TECHNIQUES

Par l'intermédiaire de modules spécifiques, du pilote générique texte ou des passerelles de synchronisation MS-SYNC et MS_RSYNC, de nombreux autres matériels ou systèmes tiers peuvent être interfacés à **MICRO-SESAME** (**limites fonctionnelles : nous consulter**) :

- ▶ Barrières, câbles de clôture et capteurs SORHEA
- ▶ Centrales intrusion GALAXY (document de référence à consulter)
- ▶ Autocomms AASTRA
- ▶ Ascenseurs SCHINDLER
- ▶ Gestion d'astreinte MEMOGUARD
- ▶ Systèmes PTI (Protection du Travailleur Isolé)
- ▶ ...

Honeywell
GALAXY



PASSERELLES AVEC APPLICATIONS DE GESTION, RESSOURCES HUMAINES, ANNUAIRES...

Dans de nombreux cas, il peut être intéressant de réaliser des échanges de données entre **MICRO-SESAME** et des bases de données qui gèrent les employés ou les usagers de l'entreprise (bases RH, annuaires etc.).

Automatiser la synchronisation de ces bases avec le système de contrôle d'accès est d'autant plus utile que le nombre de badges en circulation est important, car cela permet :

- ▶ D'éviter les doubles saisies (gain de temps important et précision)
- ▶ D'attribuer automatiquement des accès aux personnes en fonction de règles (alias) à définir par projet (selon leur service, leur fonction, etc.)
- ▶ Une prise en compte immédiate et automatique des mouvements d'arrivées ou départs du personnel, ce qui assure une sécurité optimale.

Avec les passerelles proposées par TIL, WEB SERVICES API REST ou MS-SYNCH(CSV), la mise à jour automatique des données peut être paramétrée pour intervenir à heure fixe ou à chaque modification du fichier source. Bien sûr, une synchronisation manuelle à la demande reste possible.

MICRO-SESAME supporte la synchronisation avec plusieurs sources différentes, chaque source pouvant disposer d'une configuration de synchronisation spécifique.

MICRO-SESAME peut aussi se transformer en fournisseur de données, pour délivrer à des systèmes tiers (Restauration, service d'impression, Gestion d'armoires à clés etc.) les données des personnels créées par le contrôle d'accès et l'encodage du badge multi-applications, avec les passerelles WEB SERVICES ou MS_RSINC(CSV). Micro-Sésame est à même d'alimenter des systèmes différents avec des données personnalisées pour chacune de applications tierces.

Cela permet de mettre à jour les bases des systèmes tiers automatiquement, et d'éviter aux usagers d'aller se faire enregistrer et enrôler leurs badges sur chaque système (plus de doubles saisies).

MESSAGERIE

MICRO-SESAME intègre une fonction d'envoi de mails sur alarmes par messagerie SMTP. Une alarme recensée sur le système (intrusion, contrôle d'accès, alarmes techniques) peut être envoyée par mail.

Il est possible également, suite à l'exécution d'un rapport avec le requêteur universel, de déclencher automatiquement son envoi par mail à des destinataires définis.

L'envoi par SMS n'est pas directement intégré à **MICRO-SESAME** et nécessite de prendre une solution tierce.

INTER-SYSTEMES

Il existe une passerelle (ISMS) qui permet l'échange de données par réseau IP entre plusieurs systèmes **MICRO-SESAME** indépendants (en protocole UDP). Les échanges de données sont basés sur le nom des propriétés.

Ex d'utilisation : Un client a plusieurs sites avec un serveur et un PC sécurité (PCS) d'exploitation par site. Le client a un réseau IP inter-site. Un site pourrait jouer le rôle de centralisateur des alarmes de synthèses le week-end et héberger un poste client capable de se connecter à tous les sites / serveurs (un seul à la fois). Ainsi, si une alarme de synthèse importante est envoyée du serveur X vers ce serveur central, l'opérateur central recevra cette alarme sur son poste d'exploitation du site. Il aura la consigne de se connecter sur le poste client banalisé en pointant vers le serveur X et gérer l'alarme avec tous les détails disponibles.