Chaine de Sécurité MICRO-SESAME

Interface Logiciels / Matériels

MICRO-SESAME, automates et lecteurs PROXILIS

Garder le contrôle à tous les niveaux

Dans une logique de sécurité sans faille, protéger l'accès au bâtiment ne suffit pas. Il est également important de mettre en place des mécanismes pour vérrouiller le système de sécurité lui-même.

Sur toute l'architecture TIL TECHNOLOGIES, du serveur jusqu'au badge utilisateur, des solutions vous sont proposées pour prévenir aussi bien les pannes que les erreurs humaines, les malveillances (internes comme externes) ou le piratage.

La chaine de sécurité

1. Infrastructure informatique et réseau

- Architecture électronique centralisable dans des baies et locaux sécurisés : les lecteurs sont raccordables jusqu'à 600 m des automates UTIL / TILLYS et des modules spécialisés.
- Redondance Serveur SAFEKIT, pour reprise automatique sur pannes matérielles, sans rupture de service ni perte de données.
- Réseau dédié pour la sécurité.

2. Accès aux applicatifs et à la supervision

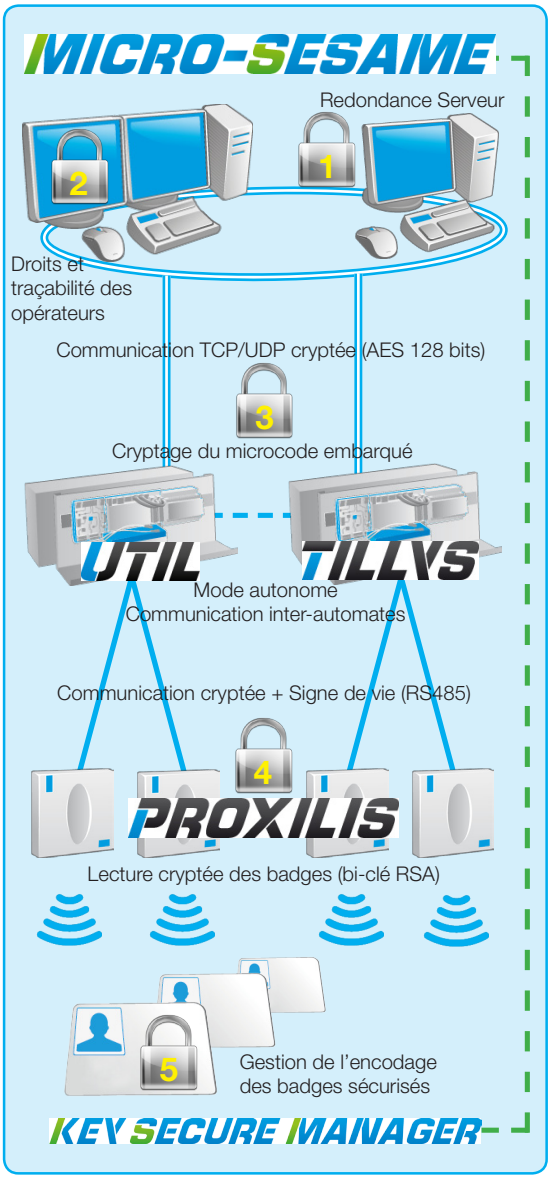
- Accès au superviseur logiciel MICRO-SESAME par mot de passe et intégration annuaire LDAP.
- Gestion fine des droits opérateurs : niveaux d'affichage et accès aux fonctionnalités logicielles selon des profils précis.
- Traçabilité des actions opérateurs dans une interface dédiée.

3. Automates et électronique de contrôle-commande

- Cryptage des communications entre le serveur et les automates en AES128 bits.
- Remonté des informations de panne ou de malveillance (arrachement ou ouverture de coffret).
- Protection du microcode embarqué (fonctions de commandes) par cryptage AES128 bits.
- En cas de coupure réseau ou serveur, fonctionnement autonome des UTIL et TILLYS + communication directe entre les automates.
- Possibilité de redondance d'UTL.

4. Lecteurs de contrôle d'accès

- Communication sécurisée entre les automates et les lecteurs (RS485 crypté), avec signe de vie.
- Lecture des badges avec cryptographie asymétriques (bi-clé RSA). Certification EAL4+.
- Lecteurs «transparents» pour les zones non-sécurisées : seule la tête de lecture est à l'extérieure, le firmware reste à l'intérieur du bâtiment.



5. Encodage de badges sécurisés

- Technologies Desfire EV1, ICAO et tous badges professionnels sécurisés (ex : carte agent du Ministère de l'Intérieur).
- Logiciel KEY SECURE MANAGER, pour la maîtrise par le client final des clés de cryptage qui protègent l'accès à chaque application du badge.

Standards
- EN50133
- IEC 60839-11-1

Référentiels
- SEVESO
- FDA21
- Carte Agent Ministériel
- ANSSI - guide sans contact

Common Criteria EAL 4+

Conforme aux exigences du Ministère de l'Intérieur

Contact Commercial > info@til-technologies.fr
Contact Marketing > marketing@til-technologies.fr