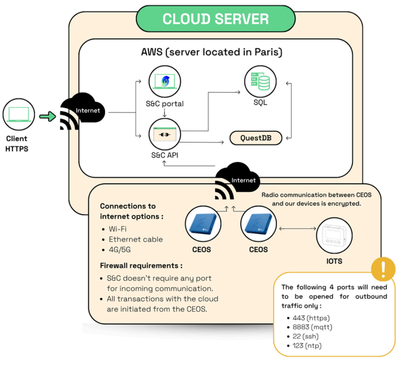
GTB Light - Sécurité et conformité



1. Sécurité et protection des données

La GTB Light a été conçue pour minimiser toute vulnérabilité.

CLOISONNEMENT ET LIMITATION DES RISQUES 1

- Chaque CEOS possède une identité et des identifiants uniques.
- Aucune donnée sensible ou partagée n'est stockée sur un CEOS.
- Les identifiants sont chiffrés dans le stockage persistant.
- Chaque CEOS dispose d'une clé de chiffrement unique, accessible uniquement en mode sécurisé.
- Mode sécurisé : impossible de démarrer un CEOS sans un firmware signé

MISES À JOUR SÉCURISÉES (OTA) 2

- Toutes les mises à jour nécessitent un paquet signé par un certificat DigiCert.
- Aucune injection de code malveillant possible.

SÉCURISATION DES COMMUNICATIONS 3

- CEOS n'est pas accessible directement depuis Internet (pas d'ouverture vers le WAN).
- Toutes les communications sont initiées par le CEOS.
- En cas d'attaque, la connexion CEOS peut être coupée immédiatement pour repasser en mode manuel.

CHIFFREMENT DES COMMUNICATIONS RADIO 4

- Toutes les communications entre CEOS et les appareils connectés sont chiffrées.
- La GTB Light repose principalement sur un écosystème d'objets radio en Z-Wave et Zigbee, deux protocoles sécurisés par nature. Contrairement aux protocoles filaires qui, sauf exception, ne disposent pas de mécanismes de sécurité intrinsèques, la sécurité dépend du réseau dans lequel ils sont intégrés.

2. CONNECTIVITÉ SÉCURISÉE ET INTEROPÉRABILITÉ

ARCHITECTURE EN PARALLÈLE AVEC VOS SYSTÈMES

La GTB Light fonctionne en parallèle des moyens de commande existants.
En cas d'incident, il suffit de désactiver CEOS pour revenir au fonctionnement manuel.

CONNEXION LIMITÉE ET SÉCURISÉE

Seuls quatre ports doivent être ouverts en sortie :

- 443 (HTTPS)
- 22 (SSH)
- 123 (NTP)
- 8883 (MQTT)

INTEROPÉRABILITÉ AVEC LES TECHNOLOGIES EXISTANTES

- Intégration cloud via API REST.
- CEOS communique en Modbus, Z-Wave, Zigbee.
- Aucune installation logicielle sur site requise, tout est full SaaS.

3. CONFORMITÉ ET MAINTENANCE SIMPLIFIÉE

CONFORMITÉ AUX RÉGLEMENTATIONS

- La GTB Light respecte les standards ISO, RGPD et cybersécurité.
- Smart & Connective est engagée dans une démarche de certification continue.

MAINTENANCE AUTOMATISÉE ET SIMPLIFIÉE

- Mises à jour automatiques et sécurisées.
- Besoin d'intervention sur site restreint.
- En cas d'anomalie, les logs permettent un diagnostic rapide et efficace.

4. DÉPLOIEMENT ET EXPLOITATION OPTIMISÉS

DÉPLOIEMENT RAPIDE

- Installation en quelques jours.
- Aucune infrastructure lourde requise

EFFICACITÉ OPÉRATIONNELLE

- Automatisation des mises à jour et supervision à distance.
- Gain en efficacité énergétique et conformité au décret BACS.

5. Rappel des protocoles terrains

La GTB Light utilise principalement les protocoles Zigbee et Z-Wave, des protocoles radio sécurisés, rapides à déployer, et parfaitement adaptés à la rénovation et aux bâtiments <5000 m².

Protocole	Chiffrement	Authentification	Sécurité globale
Modbus	✗ Non	✗ Non	Très faible
BACnet	⚠ Optionnel (BACnet/SC)	⚠ Optionnel	Moyenne
LON	⚠ Optionnel (128 bits)	⚠ Optionnel	Moyenne
LoRa	✓ AES-128	✓ Oui (via LoRaWAN)	Bonne
Z-Wave	✓ AES-128 (S2)	✓ Oui (S2)	Très bonne
Zigbee	✓ AES-128	✓ Oui	Très bonne
KNX Secure	✓ AES-128	✓ Oui	Très bonne
KNX classique	✗ Non	✗ Non	Aucune sécurité

Conclusion : Les protocoles Zigbee et Z-Wave permettent une architecture décentralisée, économique, sécurisée, et parfaitement adaptée à une stratégie de massification rapide et fiable de la GTB.

NOTE : LES PROTOCOLES FILAIRES TERRAIN CLASSIQUES NE SONT PAS PAS SÉCURISÉS "BY DESIGN", LA SÉCURITÉ DÉPEND DONC DU RÉSEAU SUR LEQUEL ILS SONT.

6. Directive RED (2014/53/UE) & nouvelles exigences RED2

DIRECTIVE RED ACTUELLE : Tous les équipements radio (comme les CEOS, capteurs, contrôleurs) sont conformes à la directive 2014/53/UE (RED), via les tests réalisés par les fabricants et intégrés au processus CE.

RED 2, AOÛT 2025 : Impose plus de sécurité logicielle et cybersécurité embarquée ; de résilience aux attaques et de conformité logicielle pour les objets connectés.

SMART & CONNECTIVE CERTIFIÉE RED2 SUR SON AUTOMATE CEOS :

Protection complète des données

Échanges chiffrés de bout en bout entre les CEOS et la plateforme Cloud Smart & Connective.

Mises à jour automatiques et sécurisées

Mises à jour logicielles et firmware des automates CEOS déployées automatiquement et de manière transparente par Smart & Connective, sans intervention requise sur site.

Avant chaque installation, le firmware est vérifié et validé cryptographiquement grâce à une signature numérique émise par un tiers de confiance : **DigiCert**.

Sécurisation du firmware et du matériel

Chaque automate intègre un système d'amorçage sécurisé (secure boot) et des mécanismes de signature du code.

Authentification par clé privée unique (ED25519)

Chaque automate CEOS possède une **clé privée unique** ED25519*, générée et stockée localement de manière sécurisée.

Elle permet l'authentification cryptographique avec nos serveurs, assurant que seuls les équipements légitimes peuvent établir une connexion.

*Rapidité et robustesse, elle offre une protection contre les attaques de type usurpation ou intermédiation (man-in-the-middle).