1 Fiche produit Services numériques

1.1 Connectivité

Le produit est équipé d'une fonctionnalité qui, lorsqu'elle est activée, permet de se connecter au Cloud Swegon INSIDE lorsque l'on dispose d'un accès à Internet. Cette connexion s'effectue, soit via le point d'accès Internet local du bâtiment, soit à l'aide d'un modem fourni. En cas de connexion via le point d'accès Internet du bâtiment, le pare-feu local doit être configuré de manière à autoriser le trafic conformément aux paramètres du pare-feu. Cette fonctionnalité est désactivée par défaut et peut être activée dans le produit. En activant cette fonctionnalité, le client accepte les conditions générales du service numérique DS-23. Le client peut à tout moment désactiver la connexion au Swegon INSIDE Cloud dans l'interface utilisateur du produit.

1.2 Quelles données sont envoyées

Grâce à la connexion au Cloud Swegon INSIDE, le produit échange des données avec le Cloud Swegon INSIDE concernant certaines actions et certains paramètres du produit. Chaque point de données a des seuils différents pour l'envoi de données à Swegon, les données envoyées dépendent donc du type de point de données et de la configuration. Les données sont envoyées par intervalles, après quoi elles sont regroupées avec d'autres données de l'intervalle en question.

1.3 Qui a accès aux données

Les données envoyées au Cloud Swegon INSIDE sont utilisées par Swegon à des fins de performance, de fonctionnalité et de développement du produit. Swegon a donc le droit d'utiliser les données envoyées par tous les produits connectés au Cloud Swegon INSIDE. Les données sont utilisées conformément aux conditions générales DS-23 de Swegon et à notre contrat de vente avec le client.

1.4 Exigences

Pour connecter un produit au Cloud Swegon INSIDE, il faut une connexion Internet sécurisée via le réseau interne de l'établissement ou via le modem externe de Swegon. En plus d'une connexion Internet sécurisée, un certificat valide pour chaque produit individuel est également nécessaire pour autoriser le partage des données avec le Cloud Swegon INSIDE. Certains produits sont livrés avec un certificat valide en sortie d'usine, tandis que d'autres produits doivent être équipés d'un certificat pour être autorisés à partager des données.

Pour savoir si le produit est INSIDE Ready (c'est-à-dire prêt à partager des données) ou non, visitez INSIDE Ready | www.swegon.com.

1.5 Sécurité

Le produit Swegon INSIDE est connecté à azure IoT Hub. La connexion utilise MQTT et est sécurisée à l'aide de TLS et de certificats clients (MTLS). DigiCert sert d'autorité d'enregistrement et de gestion des clés. La plateforme cloud Swegon utilise les offres SaaS d'Azure pour l'hébergement des applications et des APIs. Les services numériques communiquent avec le Cloud Swegon INSIDE à l'aide de technologies standard telles que les APIs Rest et les files d'attente de messages. Les utilisateurs et les autorisations sont gérés par un fournisseur d'identité interne.

1.6 Paramètres du pare-feu pour Swegon Cloud

La solution cloud de Swegon utilise les services Microsoft Azure et les certificats de DigiCert pour sécuriser la connexion. Si le pare-feu utilisé par les produits autorise le trafic sortant vers l'internet, cela fonctionnera. Si le pare-feu est configuré pour contrôler le trafic sortant, les ports et destinations suivants doivent être autorisés. Seuls les ports 443 et 8883 sont utilisés pour le filtrage.

Domaine (y compris sous-domaine)	**Port**	**Protocole**	**Note**
***.azure-devices-provisioning.net** (dps-SwegonCloud-common-we.azure-devices-provisioning.net global.azure-devices-provisioning.net)	443 8883	https mqtt	Azure Device Provisioning Service
***.azure-devices.net** (iot-SwegonCloud-prod-we.azure-devices.net)	443 8883	https mqtt	Azure IoT Hub
***.blob.core.windows.net** (stswciotfilestorageprod.blob.core.windows.net)	443	https	Stockage Azure
clientauth.one.digicert.com	443	https	DigiCert Enrolment over Secure Transport (EST) pour l'enrôlement et le réenrôlement des certificats