PRIVA CLOUD COMPUTING:

NOTRE CATALOGUE DE SERVICES DIGITAUX

POURQUOI LE CLOUD ?

Le concept du “Cloud” est simple : au lieu d’acheter et de maintenir de vastes infrastructures informatiques, les entreprises peuvent utiliser le “Cloud” pour externaliser le stockage, la communication et le traitement de leurs données. Pour les propriétaires d’immeubles ou les gestionnaires d’installations, l’accès à distance aux données, aussi simple qu’une application smartphone standard, est particulièrement intéressant. La rapidité, la simplicité d’accès du Cloud contribue à l’amélioration du confort des occupants, la bonne gestion des bâtiments, l’optimisation énergétique de ceux-ci.

Bien que le confort soit l’une des clés d’une entreprise performante, l’optimisation et l’entretien des systèmes de climatisation demeure un processus complexe qui exige une attention de tous les instants.

La capacité de gérer votre bâtiment à tout moment, n’importe où et depuis n’importe quel appareil est un gage essentiel d’efficacité. La possibilité de réunir sur une seule plateforme digitale plusieurs disciplines est un autre ingrédient clé. Nous pouvons utiliser les technologies modernes pour valoriser les énormes quantités de données qu’un bâtiment génère afin de le rendre Smart.

Le Cloud nous permet d’atteindre ces objectifs. Il a le pouvoir de traiter les données et, parce qu’il est accessible depuis toutes les interfaces, il facilite la coopération. Il rend le bâtiment plus éco-responsable en limitant les trajets des sociétés de maintenance. De ce fait, les problèmes sont détectés et résolus de manière rapide et efficace. Cette amélioration de la gestion quotidienne conduit à des niveaux de confort plus élevés à l’intérieur du bâtiment et à une augmentation générale de ses performances : c’est ce que nous appelons créer un climat propice à la croissance et au développement.

QUELS SONT LES AVANTAGES ?

Chez Priva, nous nous efforçons de développer des produits et services qui permettent à nos clients de créer un environnement propice à la croissance. Nous employons une large gamme de technologies pour rendre ces produits et services aussi puissants et simples à utiliser que possible. Le Cloud est une technologie clé qui permet d'offrir une expérience utilisateur exceptionnelle n'importe où, n'importe quand et depuis n'importe quel appareil.
Cette démarche offre les avantages suivants :

N'IMPORTE QUAND, N'IMPORTE OÙ, N'IMPORTE QUEL APPAREIL

CONFORT DES OCCUPANTS

ALERTES EN TEMPS RÉEL

MAINTENANCE PROACTIVE

AMÉLIORATION CONTINUE

SERVICES AMÉLIORÉS

PLATEFORME CLOUD : **MICROSOFT AZURE**

Notre technologie contrôle les fonctions vitales l'environnement des utilisateurs, votre bâtiment. La sécurité de ces produits et services, et les données qu'ils contiennent, est essentielle aussi bien pour vous que pour Priva. Nous vous expliquons les mesures de sécurité que nous avons prises :

Nous construisons tous nos services en utilisant la plate-forme Azure de Microsoft. Ce choix s'explique par les mesures de sécurité complètes que Microsoft a prises et par les composants standard qu'il fournit. De cette façon, nous pouvons nous concentrer sur la valorisation de vos bâtiments, tout en laissant les experts de Microsoft se concentrer sur la sécurité des services et des données. La sécurisation des logiciels est en effet une tâche que nous avons choisi de laisser à notre partenaire expert dans ce domaine. En sa qualité de fournisseur de plateformes de premier plan, Microsoft a l'envergure nécessaire pour investir dans la sécurité de produits aussi complexes que les services logiciels.

Et ce niveau de sécurité est perceptible. Au total, Azure est conforme à plus de 75 normes locales, régionales et mondiales, offrant ainsi un niveau de sécurité et de conformité qu'aucune autre entreprise ne pourra jamais atteindre avec son propre service informatique.

Les mesures de sécurité étendues prises par Microsoft s'appliquent également aux services de Priva. Vous trouverez des informations détaillées sur les efforts de sécurité de Microsoft sur le Microsoft Trust Center.

>

SÉCURISEZ VOTRE **OR**

La sécurité du Cloud est comparable à celle d'un coffre-fort de banque. Vous pouvez garder votre or sous votre lit, où il restera près de vous, mais les serrures n'empêcheront d'entrer que les gens honnêtes. Si quelqu'un veut vraiment entrer dans votre maison par effraction, il n'a besoin que d'outils de base et d'attendre le moment opportun.

Une autre solution consiste à entreposer votre or dans un coffre-fort de banque et à confier la sécurité de cette valeur à une entreprise dont l'expertise est de garder vos objets de valeur en sécurité. Le résultat ? Il est maintenant infiniment plus difficile de voler votre or.

OÙ VOULEZ-VOUS CONSERVER VOTRE **OR ?**

LA SÉCURISATION DES DONNÉES AU COEUR DES **SERVICES PRIVA**

L’infrastructure qui régie les services digitaux Priva peut être divisés en plusieurs étapes sur le plan de la sécurité. Tout commence avec le système de contrôle. Le Cloud Connector relie le système de contrôle au Cloud. C’est dans le Cloud que sont sauvegardées les données et que sont hébergés les services. C’est également là que les utilisateurs accèdent à leurs services. La sécurité de chacune de ces étapes est abordée ci-après.

LE SYSTÈME DE CONTRÔLE

Le système de contrôle consiste en un réseau de régulateurs qui gèrent les installations climatiques. En général, les contrôleurs d’immotique ne sont pas sécurisés et les protocoles de base de l’immotique, comme le BACnet, n’ont aucune option de chiffrement. Aussi les contrôleurs Priva et leurs communications mutuelles ne sont pas sécurisés.

Les systèmes immotiques doivent toujours utiliser un réseau technique spécialisé qui assure la sécurité en séparant le système immotique de tout accès extérieur possible. C’est pourquoi ces systèmes ne doivent jamais être installés sur des réseaux disposant d'un accès Internet.

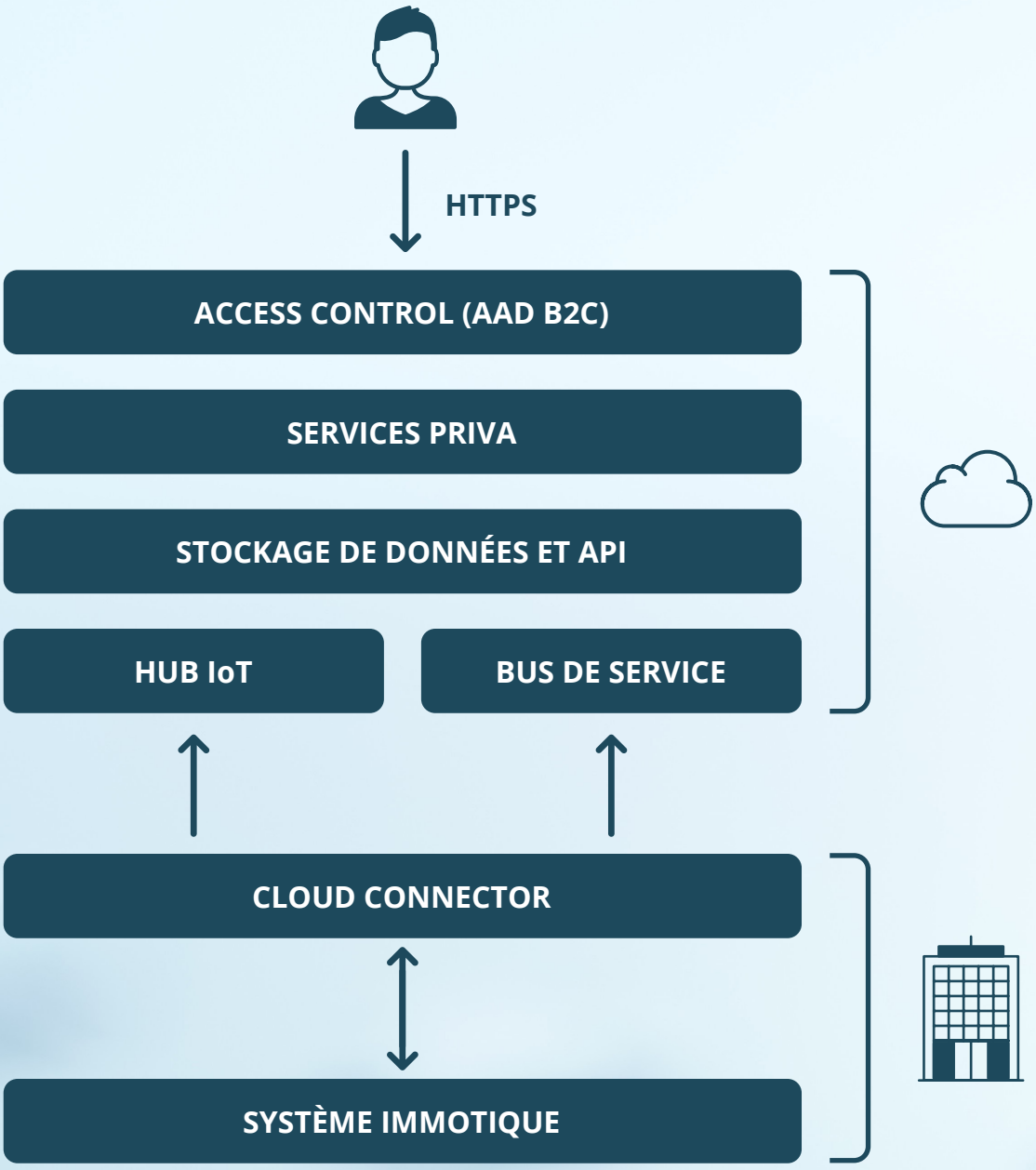
LE CLOUD CONNECTOR

Bien sûr, pour utiliser les services sur le Cloud, le système de contrôle doit se connecter à Internet. Nous utilisons donc le Cloud Connector pour fournir une interface sécurisée entre le système de contrôle et Internet. Pour ce faire, ce dispositif n'a que des connexions sortantes et aucune connexion entrante. Toute communication entre le bâtiment et le monde extérieur est donc toujours initiée par le Cloud Connector. En effet, du point de vue d'Internet, cet équipement n’a pas d’existence. Et il est impossible d'attaquer ce qui n'existe pas.

Cela signifie également qu'aucun port entrant n'a besoin d'être ouvert. Les ports sortants doivent en revanche être ouverts. Voici les ports qui sont utilisés et leur finalité : **Port 443 (HTTPS), Port 5671 (AMQP) and 8883 (MQTT), Port 9354 (SBMP)**.

Nous utilisons des composants Microsoft standard pour communiquer entre le bâtiment et le Cloud. Plus précisément, nos services utilisent le hub IoT et le bus de service de Microsoft Azure. Contrairement à d'autres méthodes d'accès aux systèmes immotiques comme le VPN, cette architecture utilise un système de messagerie, de sorte qu'il n'y a pas de liaison de données complète entre le bâtiment et le monde extérieur. L'échange de données pertinentes est très limité.

ARCHITECTURE
DES SERVICES PRIVA



LA SÉCURISATION DES DONNÉES AU COEUR DES **SERVICES PRIVA**

SÉCURITÉ DU CLOUD

La principale défense contre l'accès non autorisé des utilisateurs à nos services Cloud est une couche d'authentification basée sur le protocole OAuth2. Nous utilisons Azure Active Directory B2C (AAD B2C) comme fournisseur d'identité et une implémentation Identity Server qui fournit les règles d'autorisation pour ces identités. Nous sécurisons la communication avec tous nos services via HTTPS (TLS v1.2 ou supérieur) et notre couche d'authentification ne fait pas exception.

Après qu'un utilisateur s'authentifie avec AAD B2C, ses droits sont encodés dans un Token Web JSON et signés en utilisant une clé privée. Chaque fois qu'une de nos applications souhaite accéder à vos données, elle doit présenter le jeton au service qui le stocke. Le service vérifiera alors si le jeton n'a pas été altéré, en utilisant une clé publique et si l'utilisateur a le droit d'accéder à la ressource demandée.

Les utilisateurs des services Priva sont habitués au contrôle d'accès, qui est l'aperçu que nous avons construit à partir de cette couche d'authentification. Il permet aux utilisateurs administratifs d'une entreprise de contrôler les comptes qui ont accès à des fonctions et à des bâtiments spécifiques. Au point de vente, nous donnons tous les droits à l'acheteur du service, après quoi il peut inviter d'autres personnes et contrôler leurs droits.

Pour ce qui est de la conformité, Microsoft a pris d'importantes mesures pour satisfaire aux normes et à la législation. Des normes comme la norme ISO/CEI 27018 et le règlement général sur la protection des données (RGPD) garantissent la sécurisation des données personnelles et des mots de passe. La conformité fait d'ailleurs l'objet d'audits réguliers. Comme nous travaillons avec AAD B2C comme fournisseur d'identité, toutes les données concernant cette identité sont stockées chez Microsoft et sont conformes à ces normes.

NOTRE SOLUTION VERSUS VPN

Les VPN sont souvent utilisés dans l'automatisation des bâtiments pour gérer ou accéder à distance aux systèmes de contrôle. Les services de Priva présentent plusieurs avantages majeurs par rapport au VPN traditionnel. Les VPN sont des tunnels sur Internet, mais la communication à l'intérieur n'est souvent pas sécurisée, et dans de nombreux cas, il s'agit d'une liaison de données complète. Donc, si un intrus franchit le tunnel ou y accède, tout ce qui se trouve sur le réseau est accessible.

Avec les services de Priva, il n'y a pas de tunnel qui relie de nombreuses fonctions importantes, peut-être entre différents bâtiments, ou en dehors de votre propre contrôle, et où il est possible de pénétrer par effraction. C'est donc une solution beaucoup plus sûre. De plus, il n'y a pas d'installation ou de configuration complexe nécessaire, donc moins d'erreurs et de points faibles potentiels.

> QUELS SONT LES ADRESSAGES UTILISÉS PAR LES SERVICES PRIVA ?

Pour se connecter aux services du Cloud, notre Cloud Connector utilise des noms de domaine entièrement qualifiés (FQDN). L'aperçu complet des FQDN spécifiques est disponible dans la documentation et vous trouverez ci-dessous un extrait des FQDN :

*.servicebus.windows.net
*.azure-devices.net
*.azurewebsites.net
*.blob.core.windows.net
*.priva.com


FACILITER
LA VIE DE
NOS CLIENTS

À QUI APPARTIENNENT LES DONNÉES ?

La propriété des données est un sujet difficile dans le monde entier, car légalement, il est impossible de posséder des données. Les données ne sont que des 1 et des 0, elles n'ont pas de limites clairement définies, donc leur propriété ne peut pas être définie. Mais vous pouvez posséder les droits pour l'utiliser.

Les données dans nos systèmes sont constituées principalement de mesures et de réglages concernant le climat. La politique complète de Priva concernant l'utilisation de ces données est décrite dans les Conditions générales d'utilisation. En bref, notre politique stipule que les données appartiennent à ceux qui possèdent le système qui les génère. Nous nous réservons toutefois le droit d'utiliser ces données à des fins de R&D après les avoir anonymisées.

OÙ VOS DONNÉES SONT-ELLES STOCKÉES ?

Tous nos services Cloud sont hébergés dans la région Europe de l'ouest de Microsoft Azure. Actuellement, les centres de données de cette région sont implantés près d'Amsterdam, aux Pays-Bas. Toutefois, à des fins de récupération en cas de sinistre, les centres de données sont jumelés à ceux de la région de l'Europe du Nord d'Azure qui sont tous physiquement implantés à Dublin, Irlande, ou à proximité de cette ville. En cas d'urgence, vos données peuvent être transférées entre ces deux centres de données. Ces transferts de données utilisent toujours l'infrastructure de communication privée de Microsoft.

LE GOUVERNEMENT AMÉRICAIN PEUT-IL ACCÉDER AUX DONNÉES COMMERCIALES OU DE CONSOMMATION EUROPÉENNES ?

Selon le RGPD, le partage de données stockées dans l'UE sur la base d'une décision d'un gouvernement étranger ou d'un organe judiciaire n'est autorisé que s'il existe un traité avec ce gouvernement, donc dans un cadre juridique que l'UE a accepté. Le non-respect de ces règles peut entraîner de lourdes amendes pour l'entreprise. Cela reste un point litigieux entre l'UE et le gouvernement américain. Microsoft a également montré à maintes reprises son engagement à sécuriser les données de ses clients, en luttant contre les demandes de partage de données, souvent avec succès.


#CLIMATE-AS-A-SERVICE

CREATING
> A CLIMATE
FOR GROWTH

PRIVA

Consultez le site www.priva.com pour trouver les coordonnées des bureaux ou des partenaires Priva de votre région.

Suivez **Priva Building Automation** sur LinkedIn Twitter.