La technologie qu se trouve derrière notre portefeuille basé sur le cloud

Découvrez comment Priva sécurise vos données

WHITEPAPER

PRIVA The Experts' Choice

Table des matières

Introduction

Chez Priva, nous nous efforçons de développer des produits et des services qui permettent à nos clients de développer leurs activités. Nous utilisons différentes technologies pour rendre ces produits et services aussi efficaces et simples à utiliser que possible. Le cloud est une technologie primordiale pour assurer une expérience utilisateur exceptionnelle en tout lieu, à tout moment et sur tout appareil.

Notre technologie contrôle les fonctions indispensables à l'activité principale des personnes qui les utilisent. La sécurité de ces produits et services (ainsi que des données qu'ils contiennent) est primordiale. Ce document présentera la technologie derrière notre portefeuille basé sur le cloud et expliquera les étapes que nous avons suivies pour garantir la sécurité de vos données.

Pourquoi le cloud ?

Le concept du cloud est assez simple : Au lieu d'acheter et d'entretenir de grandes infrastructures informatiques, les entreprises peuvent utiliser le cloud pour externaliser le stockage, la transmission et le traitement des données.

Pour les propriétaires de bâtiments ou les gestionnaires des installations, l'accès à distance aux données d'installation, de confort et d'énergie via le cloud est particulièrement intéressant car il permet d'optimiser tout ce qui se passe dans le bâtiment et d'améliorer le confort des occupants. Pouvoir gérer votre bâtiment à tout moment, en tout lieu et sur n'importe quel appareil est primordial pour assurer un bon confort dans ce bâtiment.

Le cloud apporte avec lui l'intelligence du big data, ce qui vous permet de traiter, d'analyser et de sauvegarder de grands volumes de données. Par conséquent, les problèmes sont détectés et résolus rapidement, de manière efficace. Cette efficacité permet d'atteindre de meilleurs niveaux de confort dans le bâtiment ainsi qu'une augmentation générale de la performance. C'est ce que nous appelons un climat favorable à la croissance.

Quels sont les avantages ?

Le cloud est un outil efficace pour assister les utilisateurs dans leurs processus en plus d'être simple d'utilisation. Chez Priva, nous utilisons différentes technologies pour rendre nos produits et services aussi efficaces et simples à utiliser que possible.

Le cloud est une technologie primordiale pour assurer une expérience utilisateur exceptionnelle. Il présenté les avantages suivants :

1. Une connexion à tout moment, partout, depuis n'importe quel appareil
2. Un meilleur confort de l'occupant
3. Permettre la gestion des alarmes
4. Assurer une maintenance proactive
5. Apporter des améliorations de manière continue

Dans l'idéal, la gestion et l'optimisation des bâtiments ne se font pas derrière un bureau. Il faut s'engager auprès des utilisateurs des bâtiments et s'attaquer aux problèmes de front. Le logiciel connecté au cloud vous permet de surveiller les conditions, d'effectuer des ajustements, d'analyser les performances et de gérer les alertes.

Ce fonctionnement vous permet de vous concentrer sur vos tâches, et donc de résoudre les problèmes rapidement et efficacement.

De nos jours, tout est connecté. Ce qui soulève des questions et des inquiétudes par rapport à la sécurité des données. Avec le cloud, il est possible de centraliser et d'optimiser les mises à jour de sécurité. Cela permet de minimiser les risques de problèmes causés par des solutions logicielles obsolètes.

Mais ces mises à jour ne se limitent pas à la sécurité. La technologie s'améliore plus vite que jamais. Quand vous mettez en œuvre une gestion technique du bâtiment (GTB), vous n'avez pas envie qu'elle soit obsolète l'année suivante. Il est nécessaire d'assurer la compatibilité entre les technologies.

En utilisant le cloud pour détacher le système de contrôle des applications, toute nouvelle technologie peut être intégrée dans l'environnement cloud sans modifier le système de contrôle local. Ce qui veut dire que vos nouvelles technologies sont intégrables sans problème à votre GTB.

Plutôt que d'être figées dans le temps de la phase de conception à la rénovation ou la reconstruction, les capacités de votre bâtiment restent constamment à jour.

La technologie n'est pas le seul aspect qui peut changer avec le temps. Vos besoins sont également susceptibles de changer. Dans ce cas de figure, vous pouvez envisager d'adapter vos ensembles de services. Il n'est pas nécessaire d'apporter des modifications coûteuses ou compliquées au système local, qui nécessitent toutes sortes d'experts. En configurant le bâtiment selon vos besoins, vous êtes bien plus flexible.

Les données sont comme toute ressource brute. Elles n'ont de valeur que lorsqu'elles sont affinées et qu'on peut y accéder facilement au bon endroit. En utilisant le cloud, vous pouvez parcourir les données dans un simple graphique ou réaliser des analyses complexes, sans penser à la puissance de calcul et la complexité nécessaires pour traiter plus de données que ce que votre appareil local peut gérer.

En conclusion

L'utilisation du cloud permet d'accroître la valeur des bâtiments, en vous assistant mieux, vous et vos processus, et en libérant tout le potentiel de vos données. Il est également plus facile à utiliser, plus sûr, plus flexible et à l'épreuve du temps.

Sécurité du cloud

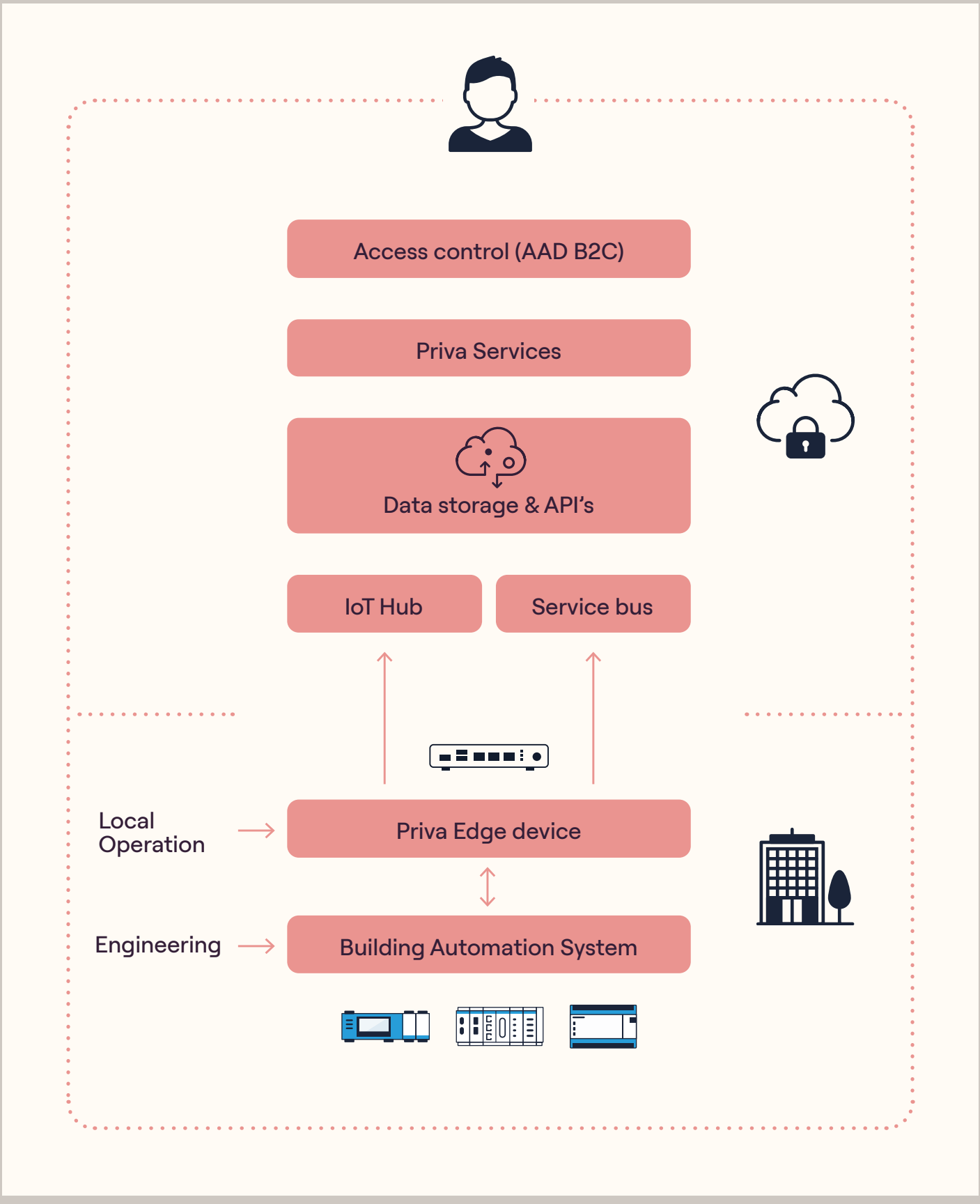
Le développement de services cloud sécurisés est un processus difficile qui nécessite une expertise importante, ainsi qu'une plateforme cloud sûre et stable. Nous utilisons la plateforme Microsoft Azure comme base solide pour tous nos services cloud. Avec plus de 90 certifications de conformité, cette plateforme cloud offre un niveau de sécurité élevé. Les certifications sont listées sur la page de documentation de conformité du site Web d'Azure. Des informations détaillées sur les mesures de sécurité de Microsoft sont disponibles sur le Portail de conformité Microsoft.

En plus de Microsoft Azure, nous avons développé nos propres services numériques Priva. Microsoft Azure nous fournit des centres de données, des infrastructures et des composants standards sécurisés. Par conséquent, Priva peut se concentrer sur la conception du logiciel, la génération d'un code sécurisé et la configuration sécurisée de ses services numériques. Lors du développement et de l'utilisation de ces services, nous appliquons des principes de sécurité bien connus, tels que la « security by design » (sécurité par la conception) et la « defense in depth » (défense en profondeur).

Nos architectes et spécialistes de la sécurité travaillent en étroite collaboration avec les équipes de développement, afin que la sécurité des informations fasse partie intégrante du processus de développement. Pendant la phase de développement, nous testons continuellement nos produits et services pour confirmer qu'ils répondent au niveau de sécurité requis. Cela se fait grâce à une évaluation des risques, des tests automatisés et des vérifications manuelles du code, conformément à notre politique de développement de logiciels et aux autres politiques de sécurité de l'information.

Pour garantir le fait que les services (cloud) Priva sont sécurisés, l'entreprise engage également des hackers éthiques indépendants pour effectuer des tests d'intrusion périodiques. Les résultats sont étudiés et les correctifs appliqués afin d'améliorer constamment le niveau de sécurité. Lorsqu'un service ou un dispositif matériel est correctement protégé, les hackers éthiques fournissent un TPM (pour Third Party Memorandum) afin de confirmer formellement leurs conclusions sur le niveau de sécurité. En outre, Priva est certifiée ISO9001 et ISO27001.

L’architecture du service Priva



Un regard détaillé sur la sécurité des services Priva

Les services Priva, ainsi que l'infrastructure sous-jacente, sont divisibles en plusieurs couches de sécurité. Tout commence avec le système de contrôle. Il se connecte au cloud en passant par le portail Priva Edge. Dans le cloud, les données sont stockées et les services sont hébergés. C'est également là que les utilisateurs accèdent aux services. La sécurité de chacun de ces composants est abordée ci-dessous.

Le système de contrôle

Le système de contrôle est le réseau de contrôleurs qui gère l'installation de la climatisation. En général, les contrôleurs d'automatisation des bâtiments et les autres dispositifs connexes ont une sécurité limitée. Le trafic réseau entre les composants du système de contrôle est également chiffré. Les dispositifs d'automatisation des bâtiments sont censés fonctionner 24 heures sur 24 et 7 jours sur 7 pendant plus d'une décennie et, à ce titre, il est extrêmement difficile de les maintenir à jour et de les sécuriser pendant toute leur durée de vie.

Les systèmes d'automatisation des bâtiments devraient toujours utiliser un réseau technique dédié qui assure la sécurité en séparant le système d'automatisation des bâtiments de tout moyen possible d'accès extérieur. Les systèmes d'automatisation des bâtiments ne devraient jamais être exécutés sur un réseau avec un accès à Internet.

Le portail Priva Edge

Pour utiliser les services cloud, le système de contrôle doit se connecter à Internet. Nous utilisons donc le portail Priva Edge pour fournir une interface sécurisée entre le système de contrôle et Internet. Le portail Priva Edge est un système fermé qui ne peut être configuré et utilisé qu'à l'aide des services Priva. Les logiciels qui ne sont pas de Priva ne peuvent pas être exécutés dessus.

Il utilise trois cartes réseau distinctes qui ne peuvent pas être pontées pour séparer physiquement Internet du réseau technique que nos contrôleurs utilisent. Cette mesure permet de séparer logiquement les contrôleurs d'Internet.

La première carte réseau, LAN1, est dédiée à la connexion au monde extérieur. Pour se protéger des intrus potentiels, elle utilise des connexions sortantes et n'utilise que les connexions entrantes minimales nécessaires (voir le tableau ci-dessous). Toute communication entre le système de gestion du bâtiment et le cloud est toujours initiée par le portail Priva Edge.

LAN2 se charge de connecter le portail Priva Edge au réseau sur lequel sur trouve le système d'automatisation des bâtiments. Pour se connecter aux autres dispositifs, LAN possède des ports ouverts au trafic entrant.

LAN3 est destinée au service. Sur la carte LAN3, il est possible d'accéder à l'interface utilisateur Web locale qui permet d'accéder aux paramètres du dispositif et du réseau, et de les modifier.

	Accepte le trafic entrant	Port UDP	Port TCP	Rôle
LAN 1/LAN 2/LAN 3	Oui	68		DHCP (Client)
LAN 3	Oui		80	Interface utilisateur Web locale
LAN 2	Oui	123		NTP
LAN 2	Oui	514		Rsyslog
LAN 2	Oui		1883	MQTT
LAN 2	Oui	1900		SSDP
LAN 2	Oui		5000/ 5001/ 5002/ 5003/ 5004	Fonctions de Building Operator Local ou Building Operator Local Fallback
LAN 2	Oui	5353		mDNS
LAN 2	Oui	7650/ 7651/ 7660/ 7661		DDS
LAN 2	Oui	9508		PTP
LAN 2	Oui	15000/15001		Comprinet

Nous utilisons des composants Microsoft standard pour assurer la communication entre le bâtiment et le cloud. Notre service utilise IoT Hub et Service Bus de Microsoft Azure. Le trafic réseau entre le portail Priva Edge et le cloud est chiffré. Contrairement à d'autres méthodes d'accès aux systèmes de maintenance des bâtiments, comme le VPN, cette architecture utilise un système basé sur les messages. Il n'y a donc pas de liaison de données complète entre le bâtiment et le monde extérieur. La quantité de données pertinentes échangée est très limitée.

"Le trafic réseau entre le portail Priva Edge et le cloud est chiffré."

Le concept du cloud est simple. Les entreprises peuvent utiliser le cloud pour externaliser le stockage des données, la communication et le traitement...

Sécurité du cloud

La principale défense contre l'accès d'utilisateurs non autorisés 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 de serveur d'identité qui génère les règles d'autorisation pour ces identités. Nous exigeons que la communication avec tous nos services se fasse par le protocole HTTPS (TLS v1.2 ou supérieur).

Lorsqu'un utilisateur est authentifié avec AAD B2C, ses autorisations sont encodées dans un jeton Web JSON et signées à l'aide d'une clé privée. À chaque fois qu'une de nos applications souhaite accéder à vos données, elle doit présenter le jeton au service qui les stocke. Le service vérifie ensuite si le jeton n'a pas été falsifié, à l'aide d'une clé publique, et si l'utilisateur est autorisé à accéder à la ressource demandée.

Les utilisateurs des services Priva connaissent bien Access Control. Il permet aux administrateurs d'une organisation de contrôler l'accès aux différentes fonctionnalités et aux différents bâtiments de chaque compte. Au point de vente, nous donnons des droits d'accès à l'acheteur du service, après quoi il peut inviter d'autres personnes et contrôler leurs droits.

Par défaut, la MFA (authentification multi-facteurs) est activée pour les nouveaux utilisateurs, ce qui apporte une sécurité supplémentaire pendant le processus de connexion. En plus du mot de passe de l'utilisateur, la MFA utilise un deuxième facteur d'authentification comme un SMS avec un code à usage unique pour autoriser l'accès aux services cloud.

En outre, nos services prennent également en charge l'utilisation de l'AAD du client, avec lequel le client peut avoir un contrôle plus étendu sur les politiques de sécurité.

Communications sécurisées

Les services numériques de Priva présentent plusieurs avantages majeurs en matière de sécurité par rapport aux méthodes de connexion traditionnelles. Avec les services numériques de Priva, il n'y a pas de tunnel (qui relie de nombreuses fonctions importantes, à travers des bâtiments, ou hors de votre contrôle) à percer. Les services Priva utilisent un système basé sur les messages. En outre, aucune installation ou configuration difficile n'est nécessaire, ce qui réduit drastiquement le risque d'erreurs et de vulnérabilité. Avec Access Control, il est bien plus simple de donner ou révoquer l'accès sur plusieurs bâtiments ; pas de double connexion, de mots de passe multiples ou de compte partagé par plusieurs personnes (pour la sécurité).

Quels points de terminaison utilisent les services Priva ?

Pour se connecter aux services sur le cloud, notre portail Priva Edge utilise des noms de domaine pleinement qualifiés (FQDN pour Fully Qualified Domain Names). L'aperçu complet des FQDN spécifiques est disponible dans la documentation. Vous trouverez ci-dessous un extrait des FQDN avec des caractères de remplacement :

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

Qui est le propriétaire des données ?

Selon notre politique, les données appartiennent à celui qui possède le système qui les génère. Toutefois, après leur anonymisation, nous conservons le droit d'utiliser ces données à des fins de développement. La politique complète de Priva concernant l'utilisation des données est décrite dans nos Conditions générales et Conditions spécifiques aux services, ainsi que dans notre Politique de confidentialité.

Où sont stockées vos données ?

Tous nos services cloud sont hébergés dans la région Europe de l'Ouest d'Azure. Les centres de données de cette région sont actuellement situés physiquement à/près d'Amsterdam, aux Pays-Bas. Toutefois, à des fins de reprise après sinistre, ces centres de données Microsoft sont jumelés à ceux de la région Europe du Nord d'Azure, qui sont physiquement situés à proximité de Dublin, en Irlande. 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.

Avez-vous besoin de plus d'informations ?

Avez-vous des questions ou souhaitez-vous en savoir davantage sur la manière dont nos solutions peuvent répondre à vos besoins spécifiques ?

Contactez-nous >

priva.com

PRIVA The Experts' Choice