CREATING
A CLIMATE
FOR GROWTH

PRIVA

THE TECHNOLOGY BEHIND OUR CLOUD-BASED PORTFOLIO

DISCOVER HOW PRIVA SECURES YOUR DATA

WHY THE CLOUD?

The concept of the Cloud is simple: Instead of purchasing and maintaining vast IT organizations, companies can use the Cloud to outsource data storage, communication and processing. For building owners or facility managers the remote access of energy and process data via the Cloud is of particular interest as it helps to improve occupant comfort.

While comfort is one of the keys to a high-performance organization, optimizing and maintaining climate systems to provide optimal comfort levels remains a complex process that requires frequent attention.

Being able to manage your building any-time, anywhere and on any device is a key ingredient to achieving good comfort in that building. Being able to work together with different disciplines is another key ingredient. Finally, we can use modern technologies to use the huge amounts of data that a building generates to optimize it's functionality.

The Cloud enables us to achieve these things. It has the processing power to handle the data, and because it is accessible from anywhere, facilitates cooperation and access to the building anywhere and at any time.

As a direct result, problems are being detected and solved in a quick and efficient manner. This efficieny leads to higher comfort levels inside the building and an overall increase in performance: We call this a climate for growth.

#PRIVA SERVICES

> **NO** UPFRONT INVESTMENTS
> **NO** MAINTENANCE
> **NO** WORRIES - JUST THE RIGHT CLIMATE AT **ALL** TIMES!

WHAT ARE THE BENEFITS?

At Priva, we strive to develop products and services that enable our customers to grow their business. We use a variety of technologies to make these products and services as powerful and yet simple to use as possible. The cloud is a key technology to enable great user experiences anywhere, at any time and on any device. This translates into the following benefits:

ANYTIME, ANYWHERE,
ANY DEVICE

OCCUPANT
COMFORT

REAL-TIME
ALERTS

PROACTIVE
MAINTENANCE

CONTINOUS
IMPROVEMENT

IMPROVED
SERVICES

CLOUD PLATFORM:
MICROSOFT AZURE

Our technology controls functions that are vital to the core business of those who use them. Security of these products and services - and the data that they contain - is critical. For that reason we want to explain the security measurements we have taken:

We build all our services using Microsoft's Azure cloud platform. We chose Azure because of the extensive security measures that Microsoft has taken and the standard components that Microsoft provides. This way, we can focus on creating value for our customers, leaving the experts at Microsoft to focus on the security of services and data. Making software secure is an immense and expensive task that requires specialized knowhow. As a leading platform provider, Microsoft has the scale to invest in the security of something as complex as software services.

And it shows. In total, Azure is compliant with more than 75 local, regional and worldwide standards; thus providing a level of security and compliancy that no single organization could ever reach with their own ICT department.

The extensive security measures that Microsoft has taken also apply to Priva's services. Detailed information on Microsoft's security efforts can be found at the Microsoft Trust Center.

>

SECURING YOUR **GOLD**

The security of the Cloud is analogous to a bank vault.
You can keep your gold under your bed, where it is near you, but locks will only keep out honest people. If someone really wants to break in to your house, they only need basic tools and good timing to do so.

Alternatively, you could store your gold in a bank vault and pay an organization whose specific purpose it is to keep your valuables safe. The result? It is now infinitely harder to steal your gold.

WHERE WOULD YOU STORE YOUR **GOLD?**

A DETAILED LOOK AT THE **SECURITY OF PRIVA SERVICES**

Priva services - and the infrastructure behind them - can be divided into multiple steps in terms of security. It starts with the control system. The cloud connector connects the control system to the cloud. In the coud the data is stored and the services are hosted. This is also where users access their services. The security of each of these steps is discussed below:

THE CONTROL SYSTEM

The control system is the network of controllers that controls the climate installation. Generally, building automation controllers are not secured and the core protocols of building automation such as BACnet have no option for encryption. Priva's controllers and the communication between them are also not secure.

Building automation systems should always use a dedicated technical network that provides security by means of separating the building automation system from any possible means of outside access. Building automation systems should never be on networks with internet access.

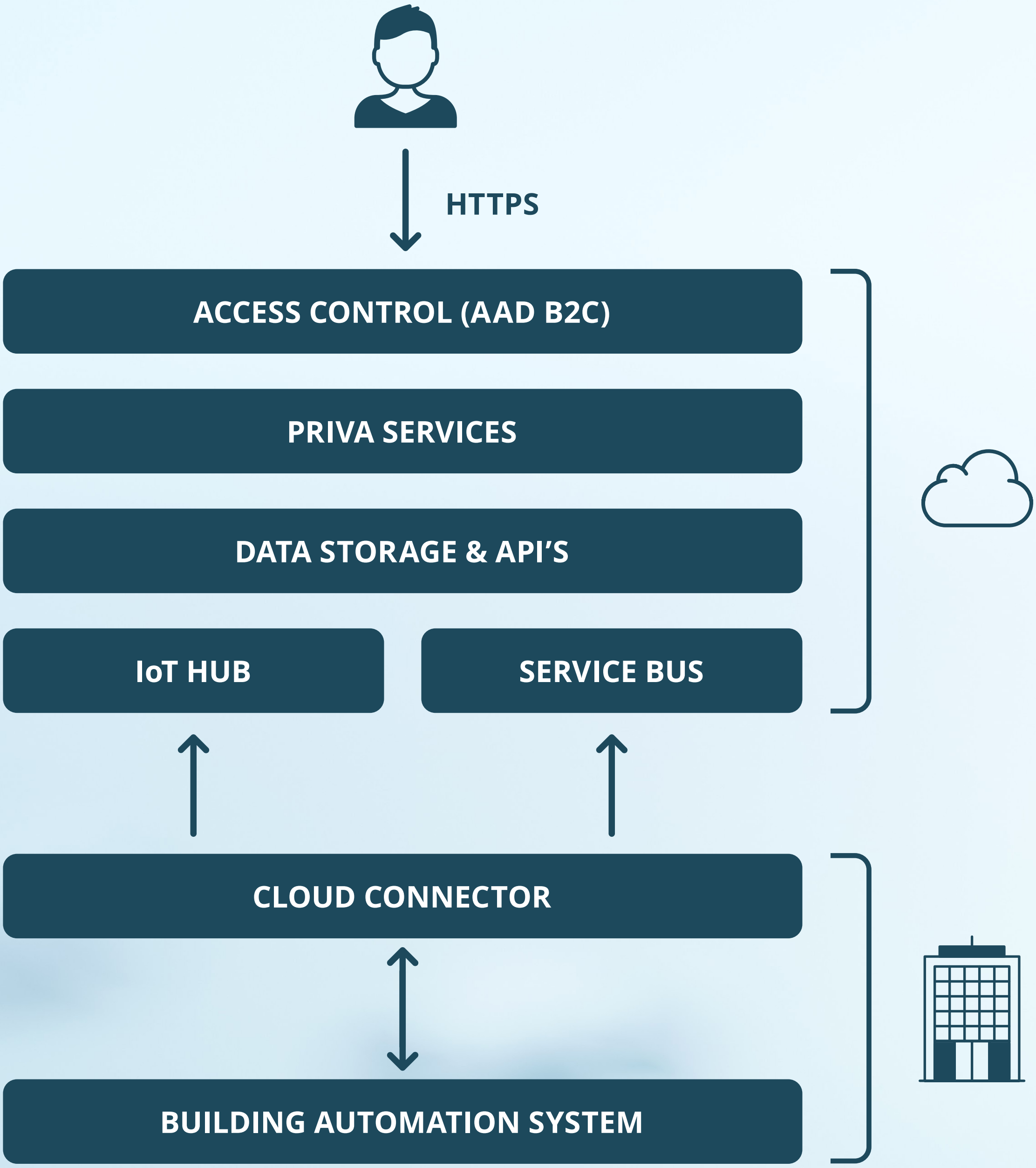
THE CLOUD CONNECTOR

Of course, in order to use cloud services, the control system has to connect to the internet. So we use the cloud connector to provide a secure interface between the control system and the internet. To achieve this, the cloud connector only has outgoing - and no incoming connections. Any communication between the building and the outside world is thus always initiated by the cloud connector. In effect, from the perspective of the internet, the cloud connector does not exist. And you cannot attack something that does not exist.

That also means no incoming ports need to be opened. Outgoing ports do need to be opened. The ports that are used, and what they are used for: **Port 443 (HTTPS), Port 5671 (AMQP) and 8883 (MQTT), Port 9354 (SBMP)**.

We use standard Microsoft components to communicate between the building and the cloud. Specifically, our services use Microsoft Azure's IoT Hub and Service Bus. The data that travels between the cloud connector and the cloud is secured by encryption. In contrast to some other methods of accessing building automation systems such as VPN, this architecture uses a message-based system, so there is no full data link between the building and the outside world. Only very limited relevant data is exchanged.

PRIVA SERVICES
ARCHITECTURE



A DETAILED LOOK AT THE SECURITY OF PRIVA SERVICES

SECURITY OF THE CLOUD

The primary defense against unauthorized user access to our cloud services is an authentication layer based on the OAuth2 protocol. We use Azure Active Directory B2C (AAD B2C) as our identity provider and an Identity Server implementation that provides the authorization rules for these identities. We enforce communication with all our services is done via HTTPS (TLS v1.2 or higher); and our authentication layer is no exception.

After a user authenticates with AAD B2C its permissions are encoded in a JSON Web Token and signed using a private key.
Whenever one of our applications wants to access your data, it must present the token to the service that stores it. The service will then check if the token was not tampered with, using a public key and if the user has permission to access the requested resource.

Users of Priva services will be familiar with Access Control, which is the overview we built based on that authentication layer. It enables administrative users of an organization to control which accounts have access to which features and buildings. At the point of sale, we give full rights to the buyer of the service, after which they can invite others and control their rights.

Regarding compliance, Microsoft has taken extensive measures to comply with standards and legislation. Standards like ISO/IEC 27018 and GDPR legislation make sure that personal data and passwords are secured.
Compliance is regularly audited. Because we use AAD B2C as our identity provider, any data regarding that identity is stored with Microsoft and are compliant with these standards.

OUR SOLUTION VERSUS VPN

VPNs are often used in building automation to remotely manage or gain access to control systems. Priva's services have several major benefits over traditional VPN. VPNs are tunnels over the internet, but the communication within them is often not secured, and in many cases, it is a full data link. So if anyone breaches the tunnel, or gets access, everything on the network is compromised.

With Priva's services, there is no tunnel – that connects many important functions, perhaps over buildings, or outside your own control – to be broken into. This is a much more secure solution. Also, there is no difficult setup or configuration needed, so less errors and potential weak points.

> WHAT ENDPOINTS DO PRIVA SERVICES USE?

To connect to the services in the cloud, our cloud connector uses Fully Qualified Domain Names (FQDNs). The full overview of specific FQDNs is available in the documentation. Below you can find an extract of FQDNs with wildcards:

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

MAKING OUR CUSTOMERS’ LIVES EASIER

WHO OWNS THE DATA?

Ownership of data is a difficult subject around the world, because legally, owning data is not possible. Data is just 1's and 0's, it doesn't really have clearly defined boundaries, so ownership cannot be defined. But you can own the rights to use it.

The data in our systems are mostly measurements and settings regarding climate. Priva's full policy regarding the use of that data is described in the Terms & Conditions. In short, our policy is that the data belongs to those who own the system that generates it. We do however retain the right to use this data for R&D purposes after it has been anonymized.

WHERE IS YOUR DATA STORED?

All our cloud services are hosted in Microsoft Azure's West Europe region. The datacenters in this region are currently physically located in/near Amsterdam, The Netherlands. For disaster recovery purposes however, the datacenters are paired with those in Azure's North Europe region which are physically located in/near Dublin, Ireland. In emergency situations your data might be transferred between these two datacenter locations. These data transfers always use Microsoft's privately owned communication infrastructure.

CAN THE US GOVERNMENT ACCESS EUROPEAN COMMERCIAL OR CONSUMER DATA?

According to the GDPR, sharing data stored in the EU based on a decision of a foreign government or judicial body, is only allowed if there is a treaty with that government, so inside a legal framework that the EU agreed to. Not complying can result in serious fines for the company. This remains a difficult issue between the EU and US government. Aside from the legislative side, Microsoft has also repeatedly shown its commitment to keeping the data of its customers secure, fighting requests for data sharing, often successfully.

#CLIMATE-AS-A-SERVICE

CREATING
> A CLIMATE
FOR GROWTH

PRIVA

See www.priva.com for contact information of a Priva office or partner for you region.

Follow **Priva Building Automation** on LinkedIn and Twitter