The technology behind our cloud-based portfolio

Discover how Priva secures your data

Whitepaper

priva.com

Introduction

At Priva, we strive to develop products and services that enable our customers to grow their businesses. 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.

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. This document will introduce the technology behind our cloud-based portfolio and explain the steps we've taken to ensure your data is secure.

Contents

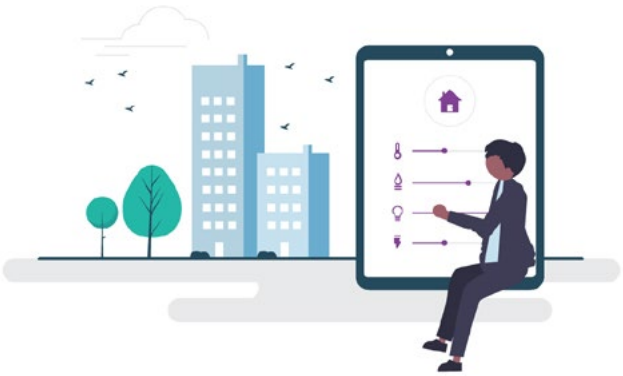
>

1.1 Why the cloud?

The concept of the cloud is simple: Instead of purchasing and maintaining vast IT infrastructures, companies can use the cloud to outsource data storage, communication and processing.

For building owners or facilities managers, the remote access to installation, comfort and energy data via the cloud is of particular interest as it helps optimize everything in the building and improve comfort for the occupants. Being able to manage your building anytime, anywhere and on any device is a key ingredient to achieving good comfort in that building.

The cloud offers big data intelligence, enabling you to process, analyze and save large data volumes. Therefore, problems are being detected and solved quickly and efficiently. This efficiency leads to higher comfort levels inside the building and an overall increase in performance: we call this a climate for growth.



1.2 What are the benefits?

The cloud is a powerful tool to support users in their processes and provides ease of use. At Priva, we use a variety of technologies to make our products and services as powerful and yet simple to use as possible.

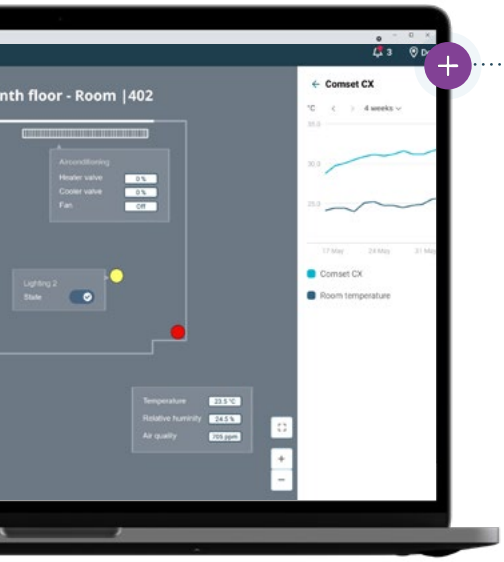
The cloud is a key technology to enable great user experiences anywhere. This translates into the following benefits:

1. **Being connected anytime, anywhere and from any device**
2. **Increase occupant comfort**
3. **Enable alarm handling**
4. **Support proactive maintenance**
5. **Making continuous improvements**

Building management and optimization is not a process best done behind a desk. It requires engagement with building users and tackling issues head on. Cloud-connected software allows you to monitor conditions, make adjustments, analyze performance and manage alerts.
That allows you to focus on your tasks – enabling you to solve issues quickly and efficiently.

Today, everything is connected. That also raises questions and worries about data security. With the cloud, security updates can be centralized and optimized. This minimizes the risks of outdated software solutions causing problems.

But these updates are about more than security. Technology is improving faster than ever. When implementing a BMS, you don't want it to be out of date the following year. Creating compatibility between technologies is necessary.



By using the cloud to uncouple the control system from the applications, any new technology can be integrated into the cloud environment without changing the local control system. This means that new technologies can be integrated in your BMS without problems.
Instead of the capabilities of your building being frozen in time from the design phase until it is renovated or rebuilt, it remains up to date at all times.

Technology is not the only thing that can change over time. Your needs may also change. In that case, you can easily consider adapting your services packages. There is no need for expensive or difficult changes to the local system that require all manner of experts. You are much more flexible to set the building to your needs.

Data is like any raw resource; it is only valuable when it is refined and easy to access in the right place. Using the cloud, you can browse data in a simple graph or perform complex analysis - without noticing the huge amount of processing power and complexity needed to process more data than your local device can handle.

>

1.3 In conclusion

Using the cloud ensures buildings that become more valuable, by supporting you and your processes better, unlocking the full potential of your data all whilst being easier to use and more secure, flexible and futureproof.

>

2. Cloud security

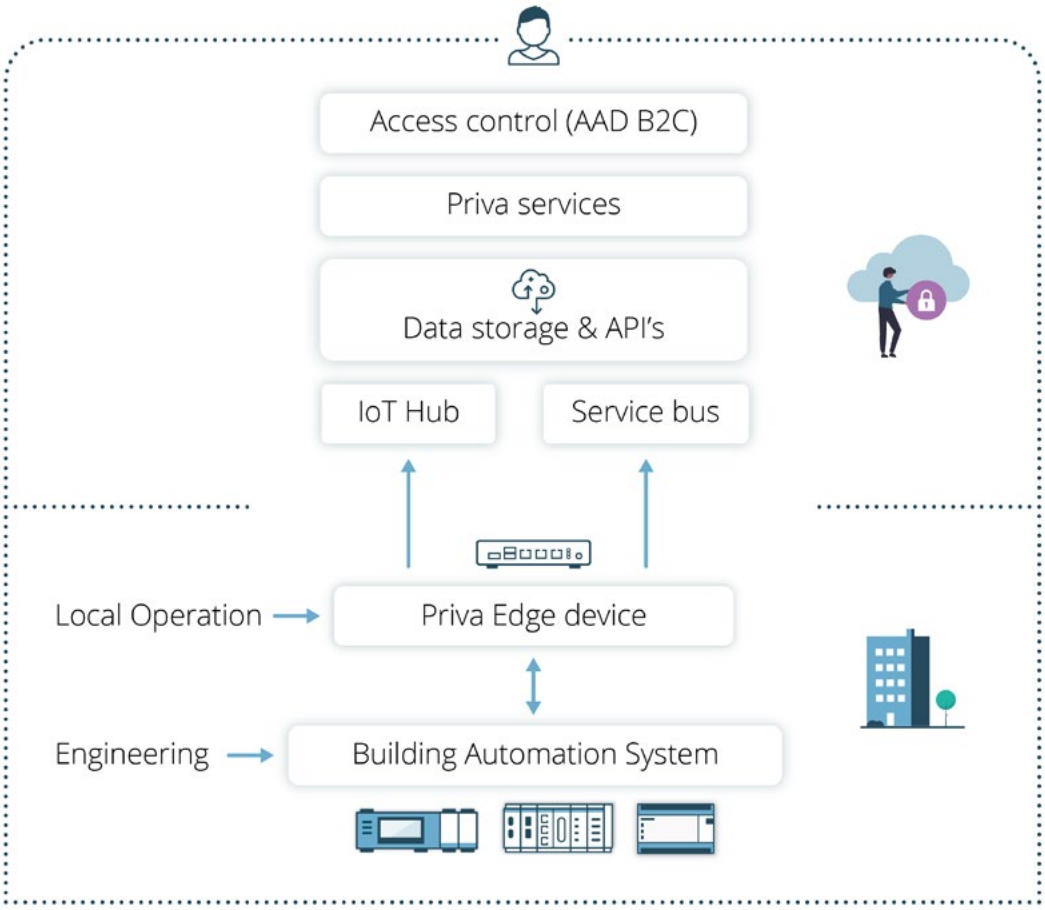
Developing secure cloud services is a challenging process that requires significant expertise and a secure and stable cloud platform. We use the Microsoft Azure cloud platform as a reliable foundation for all our cloud services. Microsoft Azure is a cloud platform that offers a high level of security as confirmed by the over 90 compliance certifications it holds. These certifications are listed on Azure's compliance documentation website. Detailed information on Microsoft's security measures can be found at the Microsoft Trust Center.

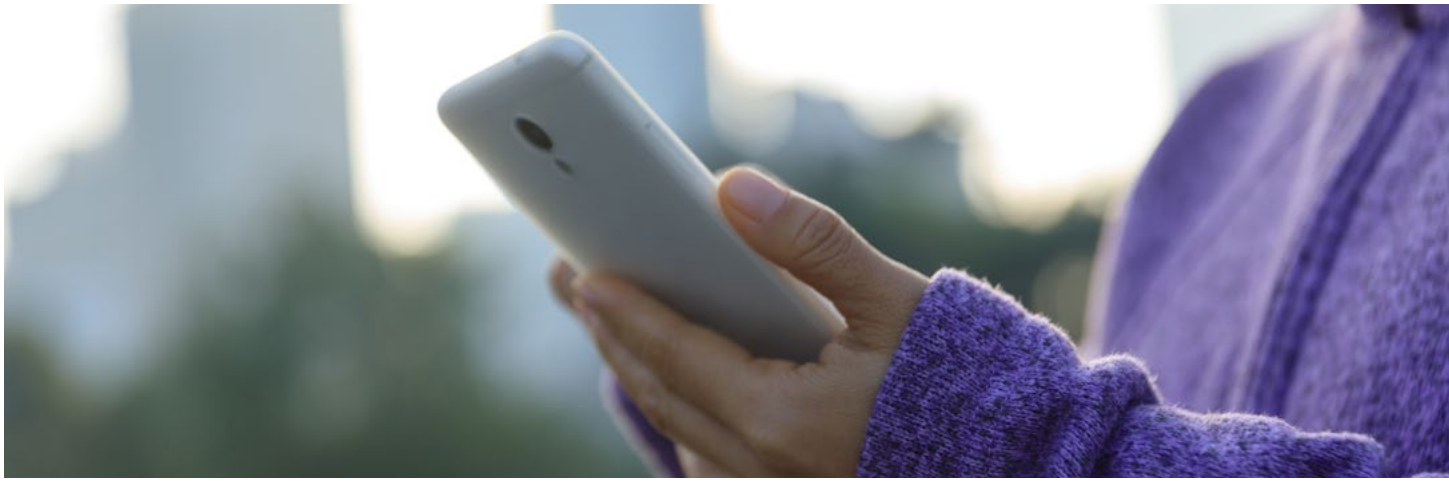
On top of Microsoft Azure, we have developed our Priva Digital Services. Microsoft Azure provides us with secure data centers, secure physical infrastructure and standard components. This means Priva can focus on secure software design, secure coding and secure configuration of our digital services. During the development and use of these services, we apply well-known security principles, such as 'security by design' and 'defense in depth'.

Our Architects and Security Specialists work closely with the development teams, so that information security is an integral part of the development process. During development, we continually test whether our products and services meet the required security level. This is done using risk assessments, automated tests and manual code reviews, in line with our software development policy and other information security policies.

To assure Priva (cloud) services are secure, Priva also hires independent ethical hackers to perform periodic penetration tests. Findings are investigated and resolved so that the security level is increased continuously. When a service or hardware device is adequately protected, the ethical hackers provide a TPM (Third Party Memorandum) to formally confirm their findings about the security level. In addition, Priva is ISO9001 and ISO27001 certified.

Priva's Service Architecture





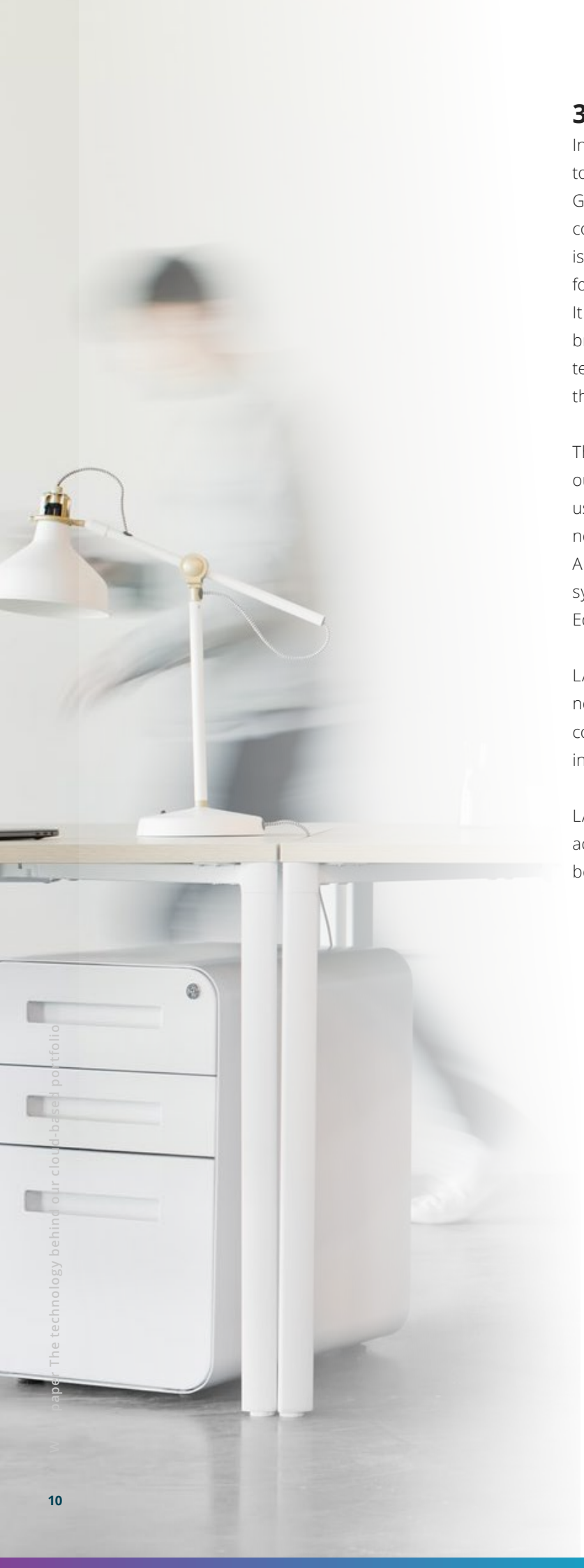
3. A detailed look at the security of Priva Services

Priva services - and the infrastructure behind them - can be divided into multiple security layers. It starts with the control system. The control system connects to the cloud through the Priva Edge Gateway. In the cloud the data is stored and the services are hosted. This is also where users access their services. The security of each of these components is discussed below.

3.1 The control system

The control system is the network of controllers that controls the climate installation. Generally, building automation controllers and other related devices have limited security. The network traffic between control system components is often also unencrypted. Building automation devices are expected to function 24/7 for more than a decade and, as such, are incredibly hard to keep up to date and secure during their entire lifespan.

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



3.2 The Priva Edge Gateway

In order to use cloud services, the control system has to connect to the internet. So we use the Priva Edge Gateway to provide a secure interface between the control system and the internet. The Priva Edge Gateway is a closed system that can only be configured and used for Priva services. Non-Priva software cannot be run on it. It uses three separate network cards that cannot be bridged to physically separate the internet from the technical network that our controllers use. This keeps the controllers logically separated from the internet.

The first network card, LAN1, is for connection to the outside world. To protect against potential intruders, it uses outbound connections and only uses the minimally necessary inbound connections (see the table below). Any communication between the building management system and the cloud is always initiated by the Priva Edge Gateway.

LAN2 is for connecting the Priva Edge Gateway to the network with the Building Automation System on it. To connect with the other devices, LAN2 has ports open to inbound traffic.

LAN3 is for service. On LAN3 the Local web UI can be accessed through which device and network settings can be accessed and changed.

	Accept inbound traffic	UDP Port	TCP Port	Purpose
LAN 1 /LAN 2/ LAN 3	Yes	68		DHCP (Client)
LAN 3	Yes		80	Local web UI
LAN 2	Yes	123		NTP
LAN 2	Yes	514		Rsyslog
LAN 2	Yes		1883	MQTT
LAN 2	Yes	1900		SSDP
LAN 2	Yes		5000/ 5001/ 5002/ 5003/ 5004	Functions of Building Operator Local or Building Operator Local Fallback
LAN 2	Yes	5353		mDNS
LAN 2	Yes	7650/ 7651/ 7660/ 7661		DDS
LAN 2	Yes	9508		PTP
LAN 2	Yes	15000/15001		Comprinet

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 network traffic between the Priva Edge Gateway and the cloud is encrypted. In contrast to some other methods of accessing building maintenance 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.

The network traffic between the Priva Edge Gateway and the cloud is encrypted.

The concept of the cloud is simple. Companies can use the cloud to outsource data storage, communication and processing...

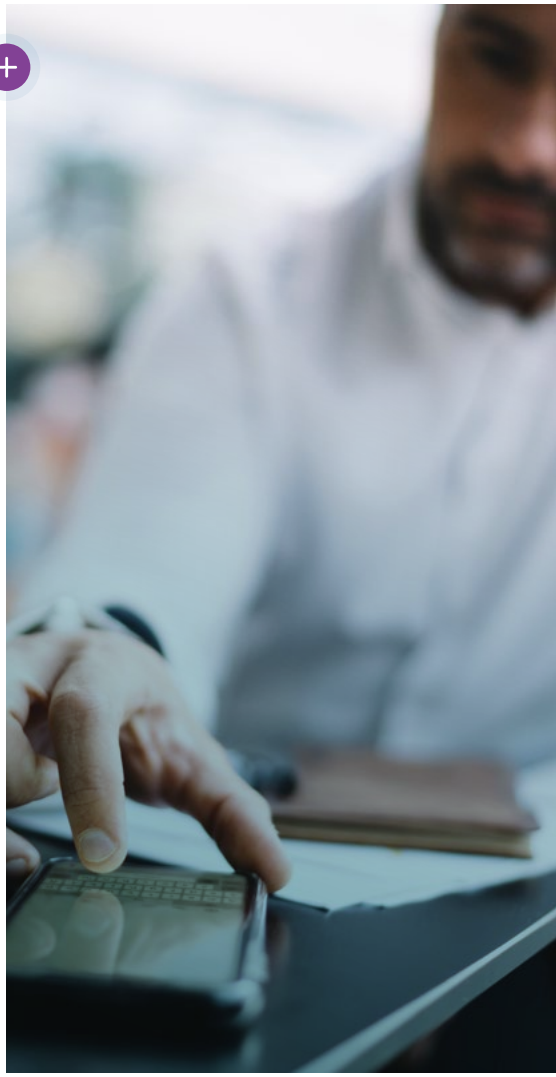
3.3 Security of the cloud

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 that communication with all our services is done via HTTPS (TLS v1.2 or higher).

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 enables administrative users of an organization to control which accounts have access to which features and buildings. At the point of sale, we give access rights to the buyer of the service, after which they can invite others and control their rights.

By default, MFA (Multi-Factor Authentication) is enabled for new users providing increased security during the login process. In addition to the user's password, MFA uses a second authentication factor like a text message with a one-time code to get access to the cloud services.
In addition, our services also support the use of the customer AAD, with which the customer can have more extensive control over the security policies.



3.4 Secured communications

Priva's Digital Services have several major security benefits over traditional connection methods. With Priva's Digital Services, there is no tunnel -that connects many important functions, perhaps over buildings, or outside your own control – to be broken into. Priva services use a messaging based system. Also, there is no difficult setup or configuration needed, which means less errors and potential weak points. Giving or revoking access with Access Control is so much easier over many buildings; no double logins or multiple passwords or people on a single account (for security).

3.5 What endpoints do Priva services use?

To connect to the services in the cloud, our Priva Edge Gateway 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**

3.6 Who owns the data?

Our policy is that the data belongs to whoever owns the system that generates it. We do however retain the right to use this data for development purposes after it has been made anonymous. Priva's full policy regarding the use of data is described in our general and service specific Terms & Conditions and our Privacy Policy.

3.7 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, these Microsoft 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.

PRIVA 10-2022

Get in touch

We love to hear from you!

Priva UK Limited
34 Clarendon Road
Watford
WD17 1JJ
United Kingdom

priva.com

#creatingaclimateforgrowth