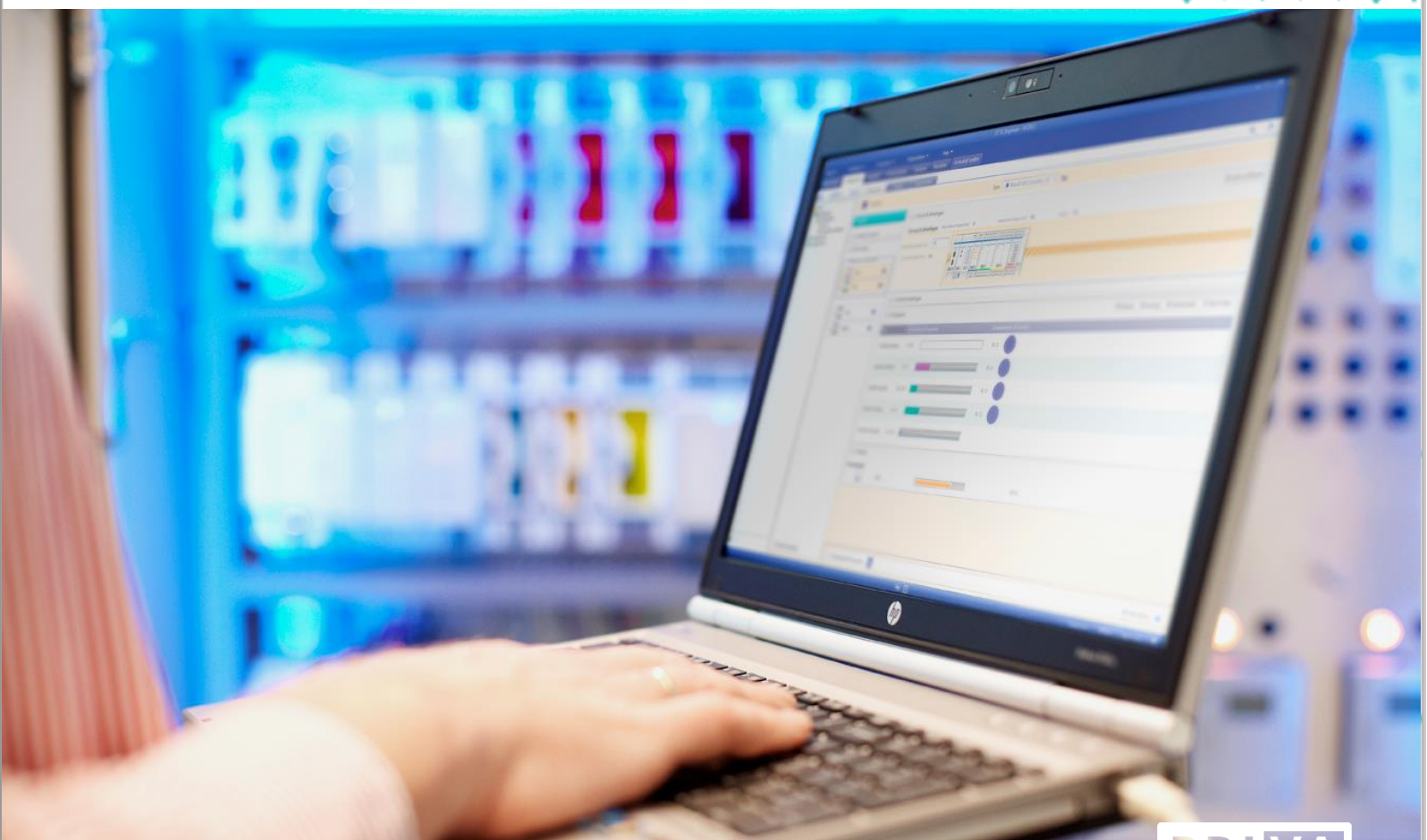
>

Cloud security

Discover how Priva secures your data

Whitepaper



This Cloud security whitepaper provides a general overview of the information security measures taken by Priva for our Cloud services.

This is a public document in order to provide clarity to Priva's customers and partners by being transparent on which security measures are implemented and managed within the Priva Cloud services. In case of additional questions, please contact Priva's Security, Quality and Compliance (SQC) team via sqc@priva.com.

Table of contents

1. 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.

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.

2. Secure Cloud services

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.

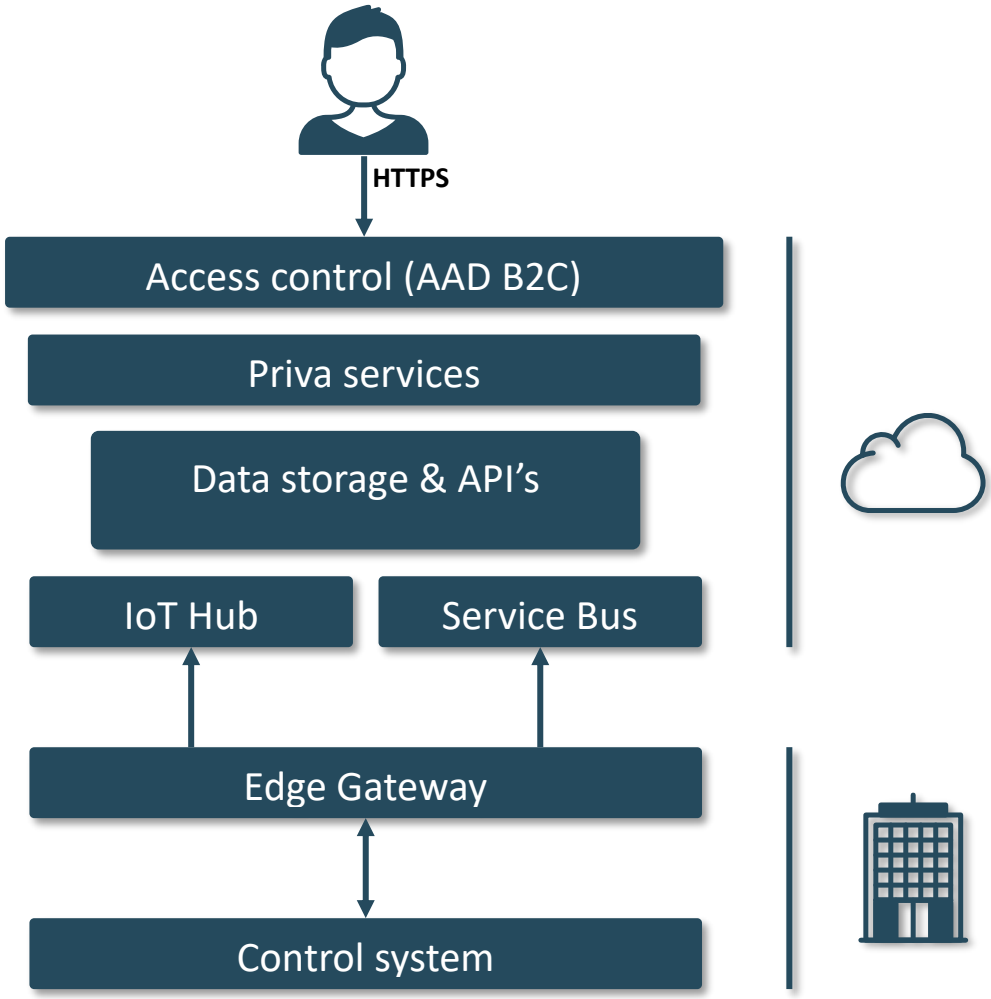
On top of Microsoft Azure, we have developed our Priva Cloud services. Microsoft Azure provides us with secure data centers, secure physical infrastructure and standard components. This means Priva can focus on secure software design, secure coding and secure configuration of our Cloud services. During 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.

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 **Edge Gateway**. In the **Cloud** the data is stored and the services are hosted. This is also where users access their services. See the picture below for the service architecture overview. The security of each of these components within the service architecture is discussed next.



3.1 The control system

The control system is the network of controllers that controls the climate installation. Generally, controllers and other related devices have limited security. The network traffic between control system components is often also unencrypted due to the use of unencrypted protocols and the need for interconnectivity. Those 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.

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

3.2 The 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. Any communication between the control system and the Cloud is always initiated by the Edge Gateway.

LAN2 is for connecting the Edge Gateway to the technical network. To connect with the other devices, LAN2 has ports open to inbound traffic.

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

We use standard Microsoft components to communicate between the control system 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 such as VPN, our architecture uses a message-based system, so there is no full data link between the control system and the outside world. Only very limited relevant data is exchanged.

3.3 Security of the Cloud; access control

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 use Access Control, which enables administrative users of an organization to control which accounts have access to which features and locations. 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 What endpoints do Priva services use?

To connect to the services in the Cloud, our Edge Gateway uses Fully Qualified Domain Names (FQDNs). The full overview of specific FQDNs is available in the Edge Gateway documentation.

3.5 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.

3.6 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 infrastructur