SECURE COMMUNICATION IN WURM PLANTS

Measures for secure data transmission via the CAN bus are continuously adjusted in order to adapt to the increasing networking of devices and systems. We pay special attention to interfaces to the outside world. These interfaces could be potential targets for unauthorised access to data communication and require special security measures. The configuration of our gateways is part of our strategies to defend your data against external attacks.

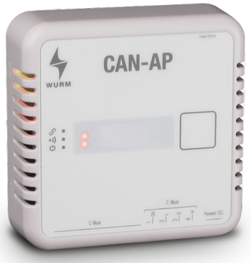
For wireless access to your Wurm plant via our app Frida we have developed the module CAN-AP, which can easily be implemented.

Wireless interfaces need to be particularly protected against external attacks. For this reason we use the Bluetooth® LE as wireless technology. In contrast to W-LAN, the communication range of BLE is only a few metres. Access to devices is only possible from close proximity to the refrigeration plant. These spatial limitations and further highly effective authentication mechanisms reduce the danger of potential intruders.

If the CAN-AP is additionally set to “inactive” (default setting), communication (limited in time) is only possible by manual operation – which means that the protection factor is enhanced further still.

These and other interlinked measures for enabling the best possible protection of customer data are the work of a team of experienced Wurm developers. They constantly observe developments in the fields of cybercrime and security technologies.

The high competence and continuously expanding technological knowledge of our experts ensure that your data are in good hands at Wurm.



SYSTEMATIC SECURITY

- Sophisticated security architecture with various interlocking measures ensures the best possible protection of your data. Key objectives of IT security – such as availability, confidentiality and integrity – are fulfilled.
- The complex security structure is continuously adjusted to incorporate technological innovations and new risk factors.
- All customer and plant data are stored on our own redundant Wurm servers in Remscheid.
- Sophisticated encryption methods as well as multi-stage authentication procedures ensure safe connections to connected branches / plants.
- Our web applications are based on the secure https protocol.
- Gateways by Wurm are configured in such a way that they ensure the same safety standard, independently of the platform.
- Interfaces to the outside world are given particular protection.

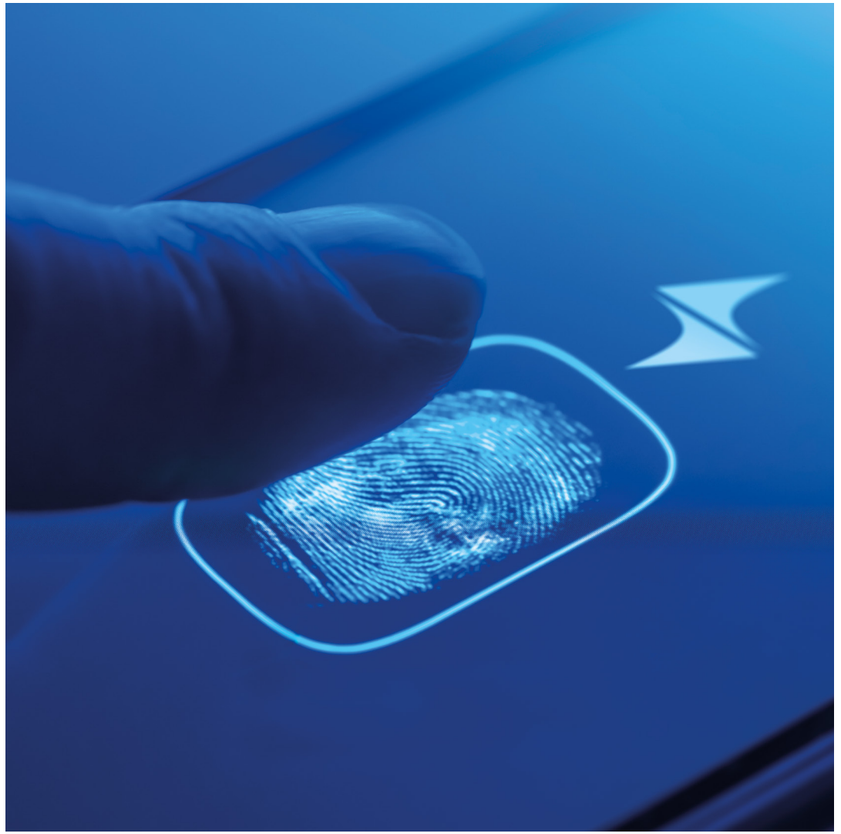
WURM SYSTEME

Wurm GmbH & Co. KG Elektronische Systeme
Morsbachtalstraße 30
D-42857 Remscheid

Tel: +49 (0) 2191 - 8847 300
Fax: +49 (0) 2191 - 8847 9300
Email: info@wurm.de

FSC
www.fsc.org
RECYCLED
Papier aus Recyclingmaterial
FSC® C010193

024A-EN



SECURITY FOR YOUR DATA

WURM SYSTEME

YOUR DATA SECURITY IS OUR TOP PRIORITY

In times of increasing global interdependence and digitalisation, IT security and data protection are of prime importance.

As a high-tech company, it is the responsibility of Wurm GmbH & Co.KG to develop efficient solutions to protect our clients and their data.

We do everything to realise the central goals of IT security most efficiently: Availability, confidentiality and integrity. Individual measures alone are not enough to achieve this; interrelated mechanisms need to be implemented in internal processes and Wurm products.

Wurm has had a complex security structure in place for many years which is adapted continuously to technological progress and to constantly changing risk factors.

This includes, inter alia, storage of all customer and plant data on our own redundant servers, sophisticated encryption methods for secure connections to connected branches and multi-stage authentication methods.

In this flyer, you will get an overview of those measures implemented at Wurm for your safety and for data security.

WURM DATA CENTER – THE CORE OF OUR SERVER CONCEPT

The Wurm DATA CENTER is the core of our system. From there, the data of all connected plants are provided for monitoring with Wurm solutions.

To protect your data we have put together a sustainable package of measures. It includes access control, sophisticated authorisation concepts, regular employee training and intelligent attack-defence systems.

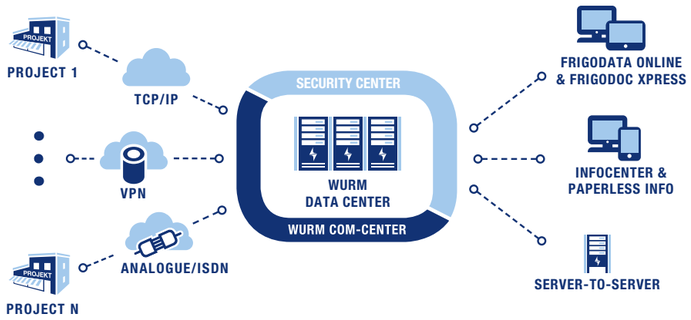
With the management of individual user identities and the configuration of access authorisation, the SECURITY CENTER creates the indispensable conditions for individual authentication when logging in to the Wurm system.

Discipline-specific access rights will only be given to users that are authorised to access the respective project.

Our customers can choose between various options to log in to the Wurm system depending on their needs and specific requirements: for example, by using our app OneID or via SMS and email.

For our web applications we only use the secure https protocol and further security mechanisms. All Wurm gateways are protected against password attacks (brute force) by specific safety precautions.

All data are safely stored on Wurm servers. The server environment is subject to regular certifications by TÜV (the German technical inspection authority).



SECURE TRANSMISSION OF YOUR DATA

Gateways play a key role in data transmission. The various gateway models provided by Wurm all have implemented security mechanisms that guarantee the same security standard, independently of the individual platform.

The effectiveness of our safety measures is regularly examined by external security experts. The demanding examination requirements have always been fulfilled by each of our devices.

All gateways are delivered with an individual password for each discipline exclusively to the responsible service company. If the service partner changes Wurm changes existing passwords. Thanks to closed ports on our gateways and VPN routers there are as few weak points as possible for hacker attacks.

The configuration of the email client in a specific gateway is only designed for sending out fault messages. This prevents the receipt of damaging emails with malware or spyware.