Individuelle Software
und Elektronik GmbH

Osterstraße 15
26122 Oldenburg
T +49 441 68006-0
F +49 441 68006-10
E info@ise.de

FAQ on IT security

1. Security and threat protection

How is my data protected against loss?

Our databases are backed up daily digitally in encrypted form on both internal servers and external analogue tapes. The data can be restored retroactively for up to six months.

How does the SMART CONNECT KNX Remote Access access my network?

The SMART CONNECT KNX Remote Access uses the Internet access of the network in which it is a participant and the DNS server to connect to the portal server.
When using the „Search links automatically" function in the SDA portal, a search for devices in the remote access network is triggered through SSDP.

Are operating systems and applications regularly updated?

Regular updates are carried out, including on individual packages in the event of security vulnerabilities. A standard package manager (APT) for operating system and software updates is used for this.

How are threats identified and eliminated?

Our monitoring system immediately triggers an alarm if our services fail. Special services notify us if security vulnerabilities are detected in third-party components we use. We also carry out regular checks for weaknesses using suitable tools.

How are the security and stability of SDA services ensured?

Once a year, we subject the SDA system and the SMART CONNECT KNX Remote Access to a penetration test by external, specialised testers. The results are evaluated and, if necessary, corresponding measures are derived and implemented.

How is login secured?

You need your user name and password to log in to both the SDA portal and the SDA Windows client for connection between remote access and the portal server.
The password must meet special complexity requirements, which are regularly updated. You can find the current requirements when assigning your password in the SDA portal.
Two-factor authentication is not yet available at this time.

Individuelle Software
und Elektronik GmbH

Osterstraße 15
26122 Oldenburg
T +49 441 68006-0
F +49 441 68006-10
E info@ise.de

FAQ on IT security

2. Data privacy

How is my data protected against misuse?

All data collection and storage is subject to the GDPR, the implementation of which is ensured by internal processes and responsible roles in the company.
Communication via SDA is encrypted using the current versions of various protocols:
Communication via our server is encrypted using the current versions of various protocols:
1. TLS is used to call the SDA portal in the browser. HTTPS is enforced here; no unsecured connections are possible.
2. OpenSSL is used for connection between SMART CONNECT KNX Remote Access and SDA portal server.
Sensitive data such as access data is never saved as plain text and is also masked in log files. This means it cannot be traced by anyone, not even our employees.
Only selected employees can access our servers, databases and logs. Physical access to our server rooms and offices is secured and restricted to certain employees (depending on sensitivity).

What happens in the event of information security incidents?

In the event of an incident such as customer data theft as a result of security vulnerabilities in the components we use, we immediately notify our customers, the responsible authorities and other affected groups. The security vulnerability will be closed or its impact minimised within 72 hours of the release of a patch or other action by the manufacturer.

Is there a programme for raising awareness of information security?

Our employees receive regular training on information security from our external data protection officers.

Are external analysis tools like Google Analytics used?

No, we do not use any external analysis tools.

Where are the SDA servers located and are the data centre operators certified?

All of our servers are located in Germany. Our service providers are certified at least in accordance with ISO/IEC 27001 and ISO 9001.

Individuelle Software
und Elektronik GmbH

Osterstraße 15
26122 Oldenburg
T +49 441 68006-0
F +49 441 68006-10
E info@ise.de

FAQ on IT security

3. Availability and failure safeguarding

How high is the availability of SDA services?

On average, our service availability is 99.9%. This does not include announced outages due to maintenance work. If there are unexpected, server-related outages, the server can be changed at any time within 15 minutes.

What happens in the event of an SDA service outage?

If our servers unexpectedly fail (average availability is 99.9%), our standby service is automatically notified. This service will carry out a root cause analysis, troubleshooting, restoration of regular operation and customer support. For prolonged outages, we will always notify our customers and, if necessary, other affected groups.

4. General information

How does SDA work? Which systems are involved and what do the data flows look like?

Information on this can be found in the SMART CONNECT KNX Remote Access product manual and the data privacy statement. (Download)

Can the connection be made via a proxy server or is a direct Internet connection required?

To use the SDA services, the SMART CONNECT KNX Remote Access must have a direct Internet connection. Connection via a proxy server is not supported.