



# Digital Service IT SICHERHEIT

## Digital Service PREVISION

Im Zuge der vorrausschauenden Instandhaltung werden Daten Ihrer Wärmebehandlungsanlage zur Zustandsbeurteilung aufgenommen, gespeichert und analysiert. Dies geschieht unter Berücksichtigung aller sicherheitsrelevanten Aspekte.

## Was unternehmen wir für die **Sicherheit Ihrer Daten?**

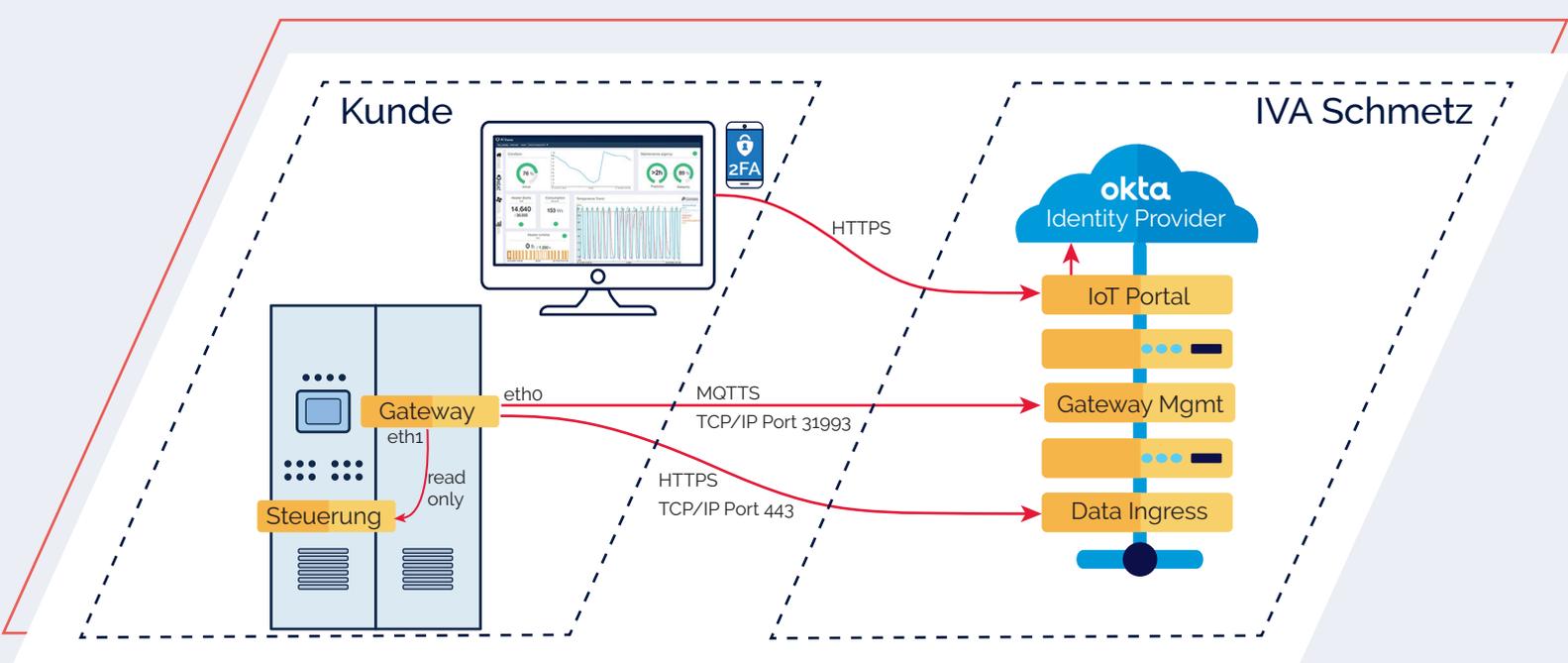
Wir implementieren auf allen Transferstrecken die heutigen Sicherheitsstandards und werden diese auch künftig regelmäßig dem technologischen Fortschritt anpassen.

### Kommunikation mit der Steuerung:

Es wird nur lesend, nicht schreibend auf die Steuerung zugegriffen. Wo die Kommunikationsprotokolle es steuerungsseitig ermöglichen wird gesichert authentifiziert kommuniziert.

### Kommunikation über das Internet:

-  **Verschlüsselt:** Sämtliche Datenübertragungen durch das Internet finden verschlüsselt statt. Es kommt eine 256-Bits starke AES Datenverschlüsselung zum Einsatz, die auf einer 2048-Bits RSA-Verschlüsselung für den Schlüsselaustausch beruht. Als mögliche Protokolle stehen TLS 1.3 und TLS 1.2 in dieser serverseitig präferierten Reihenfolge zur Verfügung.
-  **Authentifiziert:** Jedes IoT-Gateway verwendet einzigartige Credentials jeweils für die Authentifizierung gegenüber dem Gateway Management sowie dem Data Ingress. Die Identität eines jeden Nutzers des IoT Portals wird anhand von individuellen Credentials und zusätzlich mittels einer 2-Faktor-Authentifizierung gesichert.
-  **Autorisiert:** Eine Autorisierung findet mit jeder Interaktion statt, dabei ist es irrelevant ob diese vom IoT-Gateway oder einem menschlichen Nutzer ausgeht. Die zu prüfenden Berechtigungen werden penibel in mehrschichtigen Berechtigungsstrukturen entsprechend der Applikationen und Kundenberechtigungen abgebildet.



## IoT-Gateway → Gateway Management

Das IoT-Gateway kann vom Gateway Management Konfigurationsänderungen und Updates herunterladen, sowie über den Gerätezustand Bericht erstatten. Dies erfolgt über eine MQTTS Verbindung. Die Verbindung ist unidirektional und bedarf ausschließlich einer ausgehenden Portöffnung auf TCP/IP port 31993 sowie einer statischen, öffentlichen IP-Adresse zwecks Whitelisting.

## IoT-Gateway → Data Ingress

Das IoT-Gateway überträgt mittels HTTPS die gesammelten Daten an den Data Ingress Endpunkt. Die Verbindung ist unidirektional und bedarf ausschließlich einer ausgehenden Portöffnung auf TCP/IP port 443 sowie einer statischen, öffentlichen IP-Adresse zwecks Whitelisting.

## Kunden-Browser → IoT Portal

Der Zugang zum Dashboard erfolgt über eine Benutzernamen/Passwort Anmeldung mit zusätzlicher 2-Faktor-Authentifizierung. Als Identity Provider wird Okta in Verbindung mit 2FA eingesetzt.

## Was benötigen wir von Ihnen?

- ⊕ Einen Internetzugang mit statischer, öffentlicher IP-Adresse
- ⊕ Kabelgebundener Netzwerkanschluss zur störungsfreien Datenübertragung
- ⊕ Portfreigaben für TCP/IP Port 443 und TCP/IP Port 31993, jeweils vom IoT-Gateway-Netzsegment ins Internet

Noch Fragen?  
Wir sind da!

+49 (0) 231 92178-0  
info@iva-schmetz.de  
www.iva-schmetz.de