KIS.ME

Keep it simple. Manage Everything.

INTEGRATION GUIDE

Version 6, 01/2022

1 Netzwerk Infrastruktur

Die Geräte (z.B. die KIS.BOX und KIS.LIGHT) nutzen eine lokale WLAN-Infrastruktur, um eine Verbindung zum Cloud-Dienst (KIS.MANAGER) herzustellen. Ein 2,4-GHz-Netz nach IEEE 802.11 b/g/n ist erforderlich. Die Geräte unterstützen WPA-PSK oder WPA-2-PSK (CCMP). Es werden nur Statusinformationen und Metadaten der Geräte an den Cloud-Dienst gesendet. Außerdem können die Geräte über den Cloud-Dienst gesteuert werden. Der Zugriff auf den Cloud-Dienst ist mit einem persönlichen Benutzerkonto über einen Browser möglich. Abbildung 1 zeigt die gesamte Infrastruktur von KIS.ME.

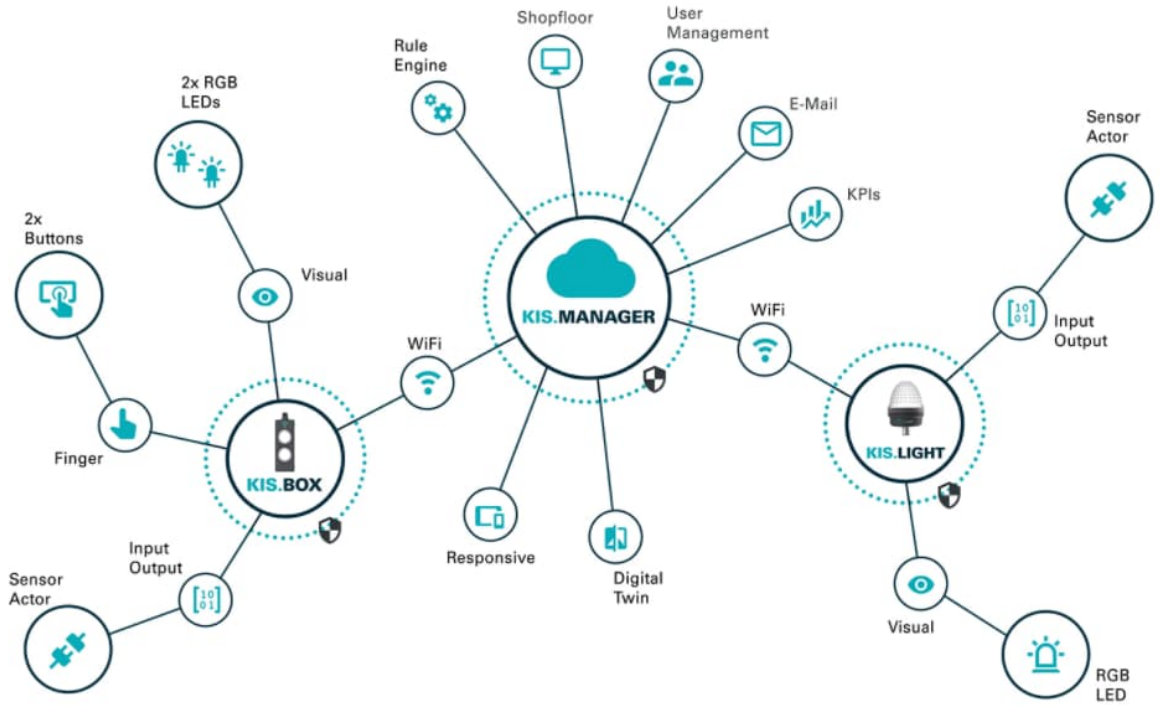

Abbildung 1: KIS.ME Infrastruktur

Für die Nutzung der Geräte innerhalb Ihres Netzwerks ist ein WLAN-Zugangspunkt erforderlich. Es wird empfohlen, dafür ein separates Netzwerk zu verwenden (z.B. ein Gastnetzwerk). Dies bedeutet, dass die Geräte logisch von Ihrer internen Infrastruktur getrennt sind. Somit ist kein Zugriff auf das interne Netzwerk möglich. Abbildung 2 zeigt eine übliche Netzwerkinfrastruktur. Die logische Netzwerkinfrastruktur ist in Abbildung 3 zu sehen. Zur Begrenzung des logischen Zugriffs kann ein sogenanntes VLAN (Virtual-LAN) oder eine DMZ (Demilitarized Zone) verwendet werden.

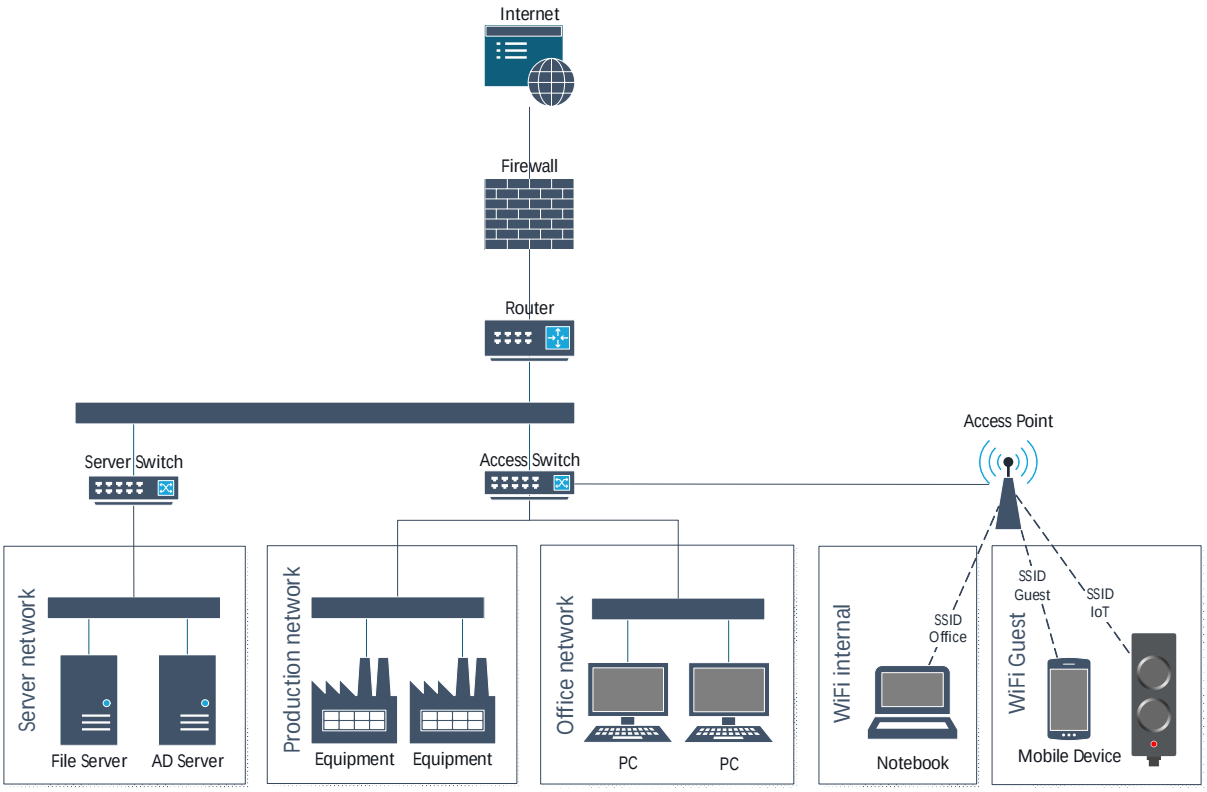

Abbildung 2: Physikalische Netzwerk Infrastruktur

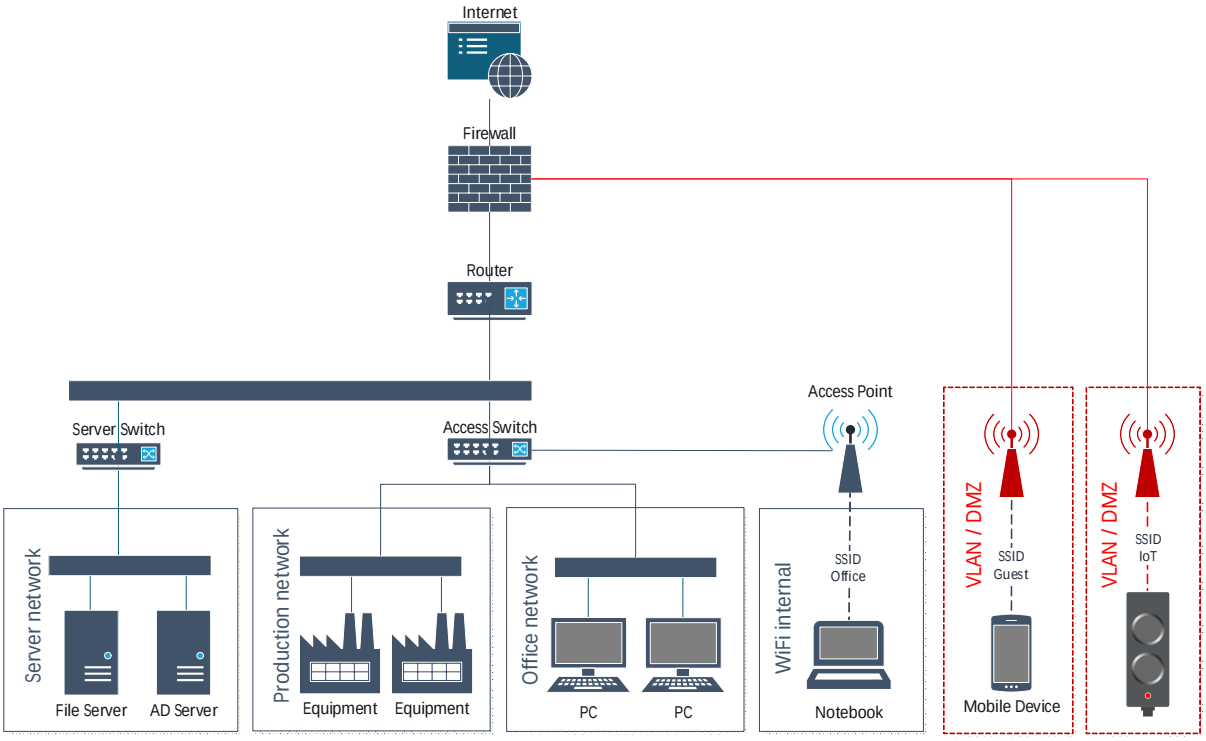

Abbildung 3: Logische Netzwerk Infrastruktur

2 Firewall Einstellungen

2.1 KIS.ME Geräte Anforderungen

Damit die KIS.ME-Geräte ordnungsgemäß funktionieren, ist die Nutzung einiger Ports erforderlich. Daher sind einige Einstellungen in der Firewall gemäß der nachstehenden Tabelle erforderlich:

Tabelle 1: Port Übersicht

Port	Protokoll	Richtung	Funktion
-	ICMP	Eingehend	Ping
53	UDP + TCP	Ausgehend	DNS
67	UDP	Ausgehend	DHCP
68	UDP	Eingehend	DHCP
123	UDP	Ausgehend	NTP
443	TCP	Ausgehend	HTTPS
8883	TCP	Ausgehend	MQTT over TLS

ICMP

Ein ICMP-Ping wird von den Geräten nicht aktiv genutzt, ist aber von der Geräte-Firewall in beide Richtungen zu erlauben, um auf Pings reagieren zu können (z.B. zur Netzwerkdiagnose).

DNS: Port 53 (UDP oder TCP, mindestens eines davon)

Voraussichtlich nur für das interne Netz erforderlich, je nach Konfiguration.

DHCP: Port 67 und 68

Nur für das lokale Netzwerk erforderlich, damit die Geräte eine IP-Adresse erhalten können.

NTP: Port 123

Es werden zufällige NTP-Server anhand dieser DNS-Namen ausgewählt:

- 0.europe.pool.ntp.org
- 1.europe.pool.ntp.org
- 2.europe.pool.ntp.org
- 3.europe.pool.ntp.org

Es gibt keine Einschränkung in der Firmware. Um die NTP-Serveradresse zu ändern, müssen diese DNS-Einträge intern angepasst und ggf. auf den lokalen NTP-Server umgeleitet werden.

HTTPS: Port 443 (Cloud-API + Firmware Update)

- iotrafi.centersightcloud.com (KIS.ME Cloud Service)
- bootstrap.centersightcloud.com
- connect.centersightcloud.com
- *.blob.core.windows.net (Firmware Update blob storage)

Die Cloud-API wird von den Geräten zur Übertragung der Telemetrie-Daten verwendet. Die Daten werden mit Hilfe von MQTT mittels TLS verschlüsselt. Für die Cloud-Verbindung wird eine zertifikatsbasierte Authentifizierung verwendet.

MQTT over TLS: Port 8883

- iotrafi-prod-iot-hub.azure-devices.net (Azure IoT Hub)

Die Geräte senden ihre Telemetrie-Daten per MQTT über TLS an den Cloud-Server.

2.2 KIS.MANAGER Anforderungen

Damit der KIS.MANAGER richtig funktioniert, ist die Nutzung einiger Domains erforderlich. Daher sind einige Einstellungen in der Firewall notwendig, die in der folgenden Tabelle aufgeführt sind:

Table 2: Domain Übersicht

Domain	Beschreibung
kismanager.kisme.com	KIS.MANAGER Domain
kismanager.rafi.de	KIS.MANAGER Domain
fonts.googleapis.com	Google fonts
api.locize.io	Locize translation service
*.Sectigo.com	Intermediate certificate authority
*.Comodoca.com	Intermediate certificate authority

2.3 FAQs

Welche Daten werden in die Cloud übertragen?
Es werden nur Telemetrie-Daten der KIS.ME-Geräte in die Cloud übertragen (z.B. Button_pressed, Set_Color_green etc ...).

Wer hat Zugriff auf die Daten und zu welchem Zweck?
Nur der Kunden-Admin hat Zugriff auf die Daten. Der Admin hat die Möglichkeit, weitere Benutzer mit definierten Rechten hinzuzufügen, wenn dies notwendig ist.

Ist sichergestellt, dass die Daten in Europa verarbeitet werden (Speicherung)?
Die Daten werden in der Serverinfrastruktur der Microsoft Azure Cloud mit Sitz in Irland gespeichert.

Wie und von wem wird die Cloud-API genutzt und wie ist die Schnittstelle gesichert?
Die Cloud-API wird von den Geräten zur Übermittlung ihrer Telemetrie-Daten genutzt. Die Daten werden mit Hilfe von MQTT über TLS verschlüsselt. Für die Cloud-Verbindung wird eine zertifikatsbasierte Authentifizierung verwendet.

Wie erfolgt die Mandanten-Trennung?
Es gibt verschiedene Arten der Mandatstrennung. Da es sich um ein verteiltes System handelt, das verschiedene Dienste nutzt, hängt die Art der Trennung vom jeweiligen Speicher-Backend ab. Ein Beispiel ist die Verwendung von separaten Datenbankschemata für verschiedene Mandanten in SQL-Datenbanken.

Werden alle Daten in verschlüsselter Form gespeichert?
Ja, alle Daten werden in verschlüsselter Form gespeichert. Wie die Verschlüsselung in der Praxis aussieht, hängt vom jeweiligen Speicher-Backend ab.

Welche Auswirkungen hat es auf andere Mandanten, wenn der Admin-Zugang eines Mandanten kompromittiert wurde?
Sollte es einem Angreifer gelingen, innerhalb eines Mandanten Admin-Rechte zu erlangen, so hat dies keine Auswirkungen auf andere Mandanten.