KIS.ME

Keep it simple. Manage Everything.

INTEGRATION GUIDE

Version 6, 01/2022

1 Network infrastructure

The devices (e.g. KIS.BOX and KIS.LIGHT) are using a local WiFi infrastructure to establish a connection to the cloud service (KIS.MANAGER). A 2.4 GHz network according to IEEE 802.11 b/g/n is required. The devices support WPA-PSK or WPA-2-PSK (CCMP). Only status information and metadata of the devices will be send to the cloud service. In addition, the devices can be controlled by the cloud service. Access to the cloud service is possible with a personal user account using a browser. Figure 1 shows the overall infrastructure of KIS.ME.

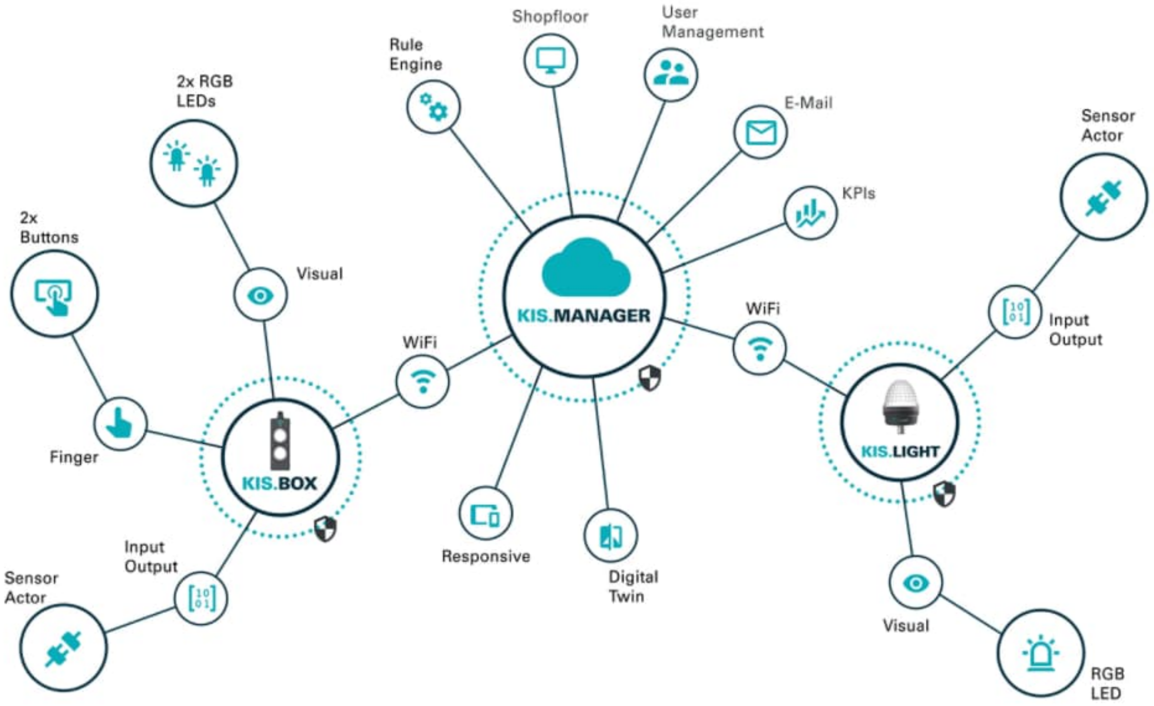

Figure 1: KIS.ME Infrastructure

A WLAN access point is required to use the devices within your network. It is recommended to use a separated network for this (e.g. a guest network). This means that the devices are logically separated from your internal infrastructure. Therefore no access to the internal network is possible. Figure 2 shows a common network infrastructure. The logical network infrastructure can be seen in Figure 3. A so-called VLAN (Virtual-LAN) or a DMZ (Demilitarized Zone) can be used to limit the logical access.

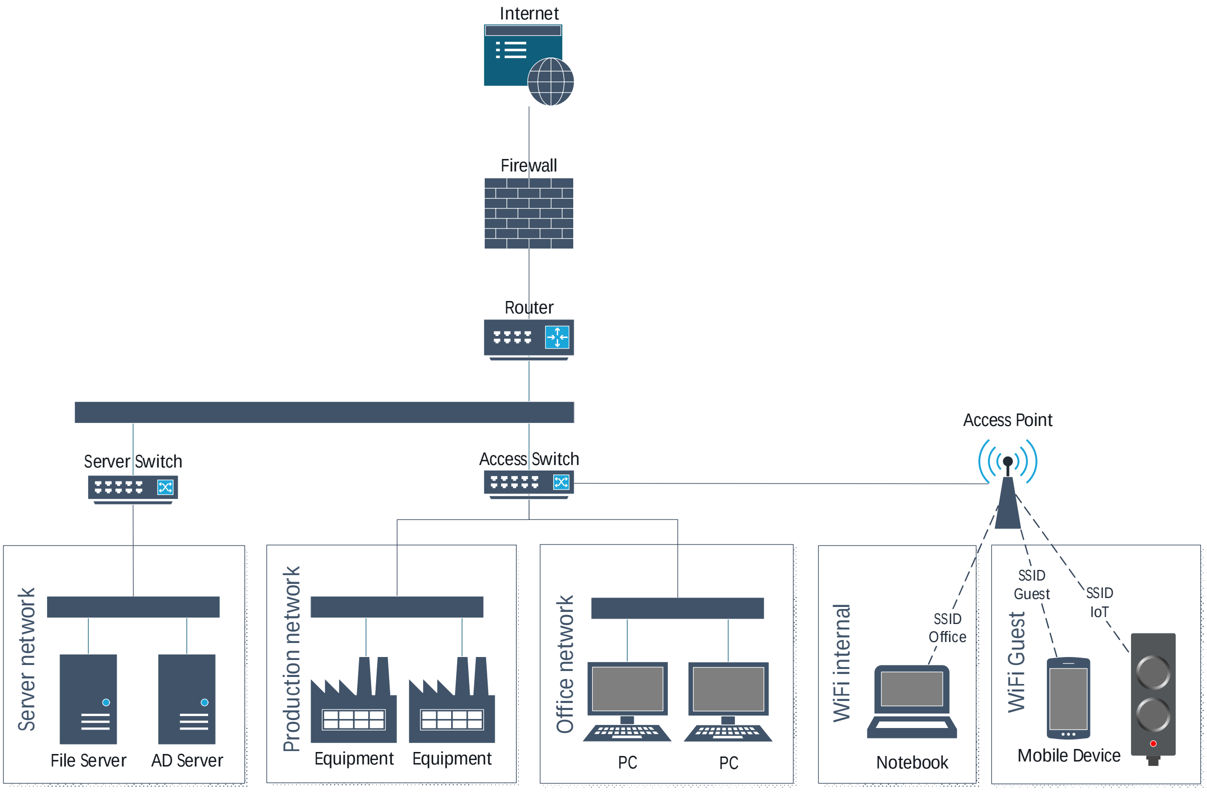

Figure 2: Physical network infrastructure

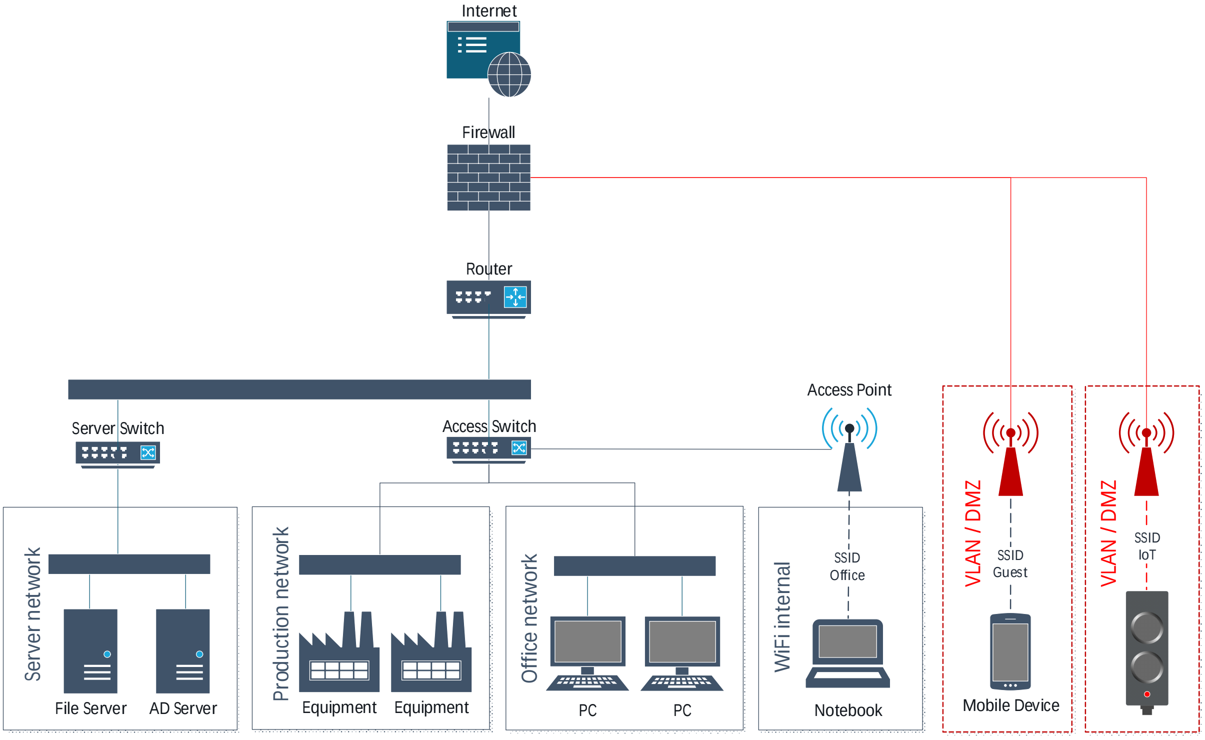

Figure 3: Logical network infrastructure

2 Firewall settings

2.1 KIS.ME devices requirements

For the KIS.ME devices to work properly, the usage of a few ports are required. So some settings in the firewall are necessary according to the table below:

Table 1 Overview Ports

Port	Protocol	Direction	Description
-	ICMP	Incoming	Ping
53	UDP + TCP	Outgoing	DNS
67	UDP	Outgoing	DHCP
68	UDP	Incoming	DHCP
123	UDP	Outgoing	NTP
443	TCP	Outgoing	HTTPS
8883	TCP	Outgoing	MQTT over TLS

ICMP

ICMP ping is not actively used by the devices, but it is allowed in both directions by the device firewall in order to be able to respond to pings (e.g. for network diagnostics).

DNS: Port 53 (UDP or TCP, at least one of them)

Probably only for internal network, but depending on the configuration.

DHCP: Port 67 and 68

Only required for the local network so that the devices can receive an IP address.

NTP: Port 123

Random servers are selected using these DNS names:

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

There is no restriction in the firmware. To change the NTP server address, these DNS entries have to be adjusted internally and redirected to the local NTP server if necessary.

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)

The Cloud-API is used by the devices to transmit the telemetry data. The data is encrypted by using MQTT over TLS. A certificate-based authentication is used for the Cloud connection.

MQTT over TLS: Port 8883

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

The devices send their telemetry data to the cloud server by using MQTT over TLS

2.2 KIS.MANAGER requirements

For the KIS.MANAGER to work properly, the usage of a few domains are required. So some settings in the firewall are necessary according to the table below:

Table 2 Overview Domains

Domain	**Description**
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

Which data are transmitted to the Cloud?

Only telemetry data of the KIS.ME devices will be transmitted to the Cloud
(e.g. Button_pressed, Set_Color_green etc ...).

Who has access to the data and for what purpose?

Only the tenant admin has access to the data. The admin has the possibility to add additional users with defined rights if this is necessary.

Is it ensured that the data will be processed in Europe (storage)?

The data are stored in the server infrastructure of the Microsoft Azure Cloud based in Ireland.

How and by whom is the Cloud-API used and how is the interface secured?

The Cloud-API is used by the devices to transmit their telemetry data. The data is encrypted by using MQTT over TLS. A certificate-based authentication is used for the cloud connection.

How does the multi-tenancy separation take place?

There are different types of a tenancy separation. Since it is a distributed system that uses different persistence services, the type of separation depends on the respective storage backend. An example is the use of separate database schemas for different tenants in SQL databases.

Is all data stored in encrypted form?

Yes, all data is saved in encrypted form. What the encryption looks like in practice depends on the respective storage backend.

What effects does it have on other tenants if a client's admin access has been compromised?

Should an attacker manage to obtain admin rights within a tenant, this would not affect other tenants.