ConnectedCooking HMP

Table of contents

1 Information on data security

Data security includes technical and organisational measures with the purpose of protecting data from unauthorised access and therefore from access, manipulation or removal of the data. The focus is on confidentiality, integrity and availability.

Confidentiality means that data can only be accessed by authorised persons. Another important aspect of data security is the integrity of the data, both against manipulation and against technical defects.

The confidentiality and integrity of the data is ensured by control mechanisms that prevent unauthorised access and thus also knowledge, manipulation or removal of the data:

a. Admission control
   - Restricted physical access to data centre
   - Server rooms only accessible to authorised personnel
   - Restricted access to rooms in which data material is stored

b. Access control
   - Separation of tasks/roles/responsibilities
   - Access to internal services for server administrators only possible via dedicated VPN
   - Concept for access authorisations with different access rights to data and functionalities

c. System access control
   - Users authenticated via user name and password
   - Guidelines for password design
   - Hardened server systems
   - Regular installation of the latest security updates
   - Regular penetration testing

d. Transfer controls
   - Extensive encryption
     Data is stored in the database in encrypted form
     All passwords are stored in encrypted form using a hash function
     All data transmissions are encrypted
   - Regular maintenance and testing of the systems

e. Input control
   - Access to the application is always logged

f. Availability control
   - Data protected against unintentional deletion or destruction for 6 months by regular backup copies

g. Separation of data for different purposes
   - Layered architecture separated into presentation, business processing and storage
   - Database servers are logically and physically separated and not part of the DMZ
   - Connections between different systems such as web (Internet), application and database servers are protected by firewalls with a stateful firewall.

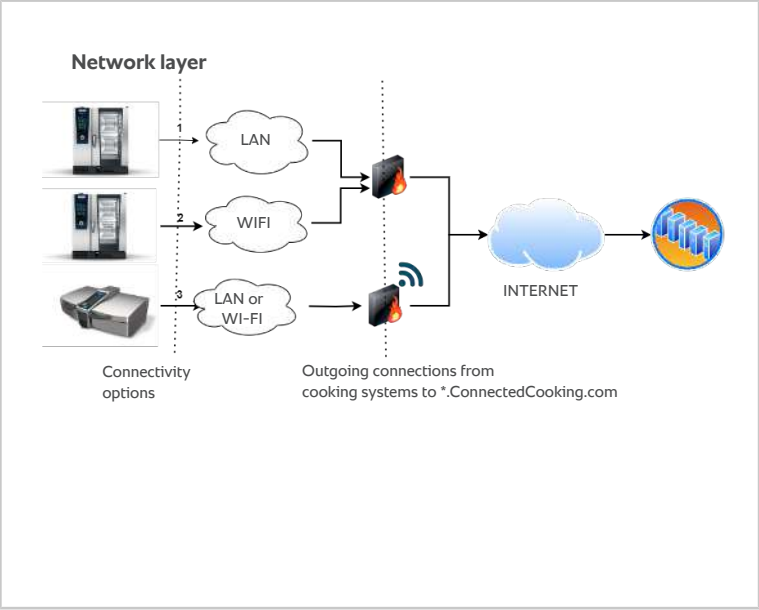
Ultimately, availability means that existing data can also be used if required. High availability is ensured by the redundant design of all network and server systems with load balancing.

2 Information on data transfer

RATIONAL cooking systems are connected to the Internet via Ethernet cable or WiFi, see connectivity options in Figure 1 below.

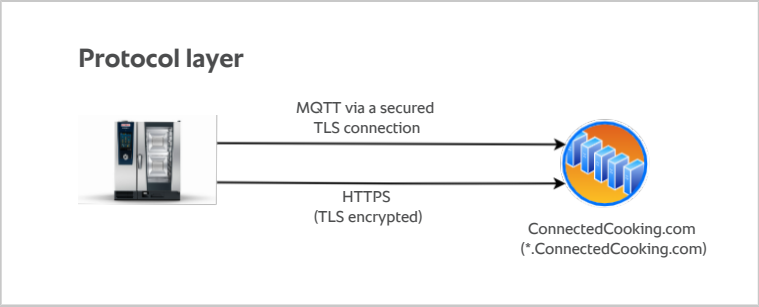
The cooking systems connected to the Internet in this way then establish a connection with the ConnectedCooking servers via the Internet. The relevant ports for the respective units are shown in the table of communication ports.

If possible, provide a separate network for the kitchen area that is physically or logically separated from the rest of the company network, e.g. using a VLAN.



Pict. 1: Network layer

All connections are encrypted using TLS 1.2 so that the transmitted data cannot be read by third parties.

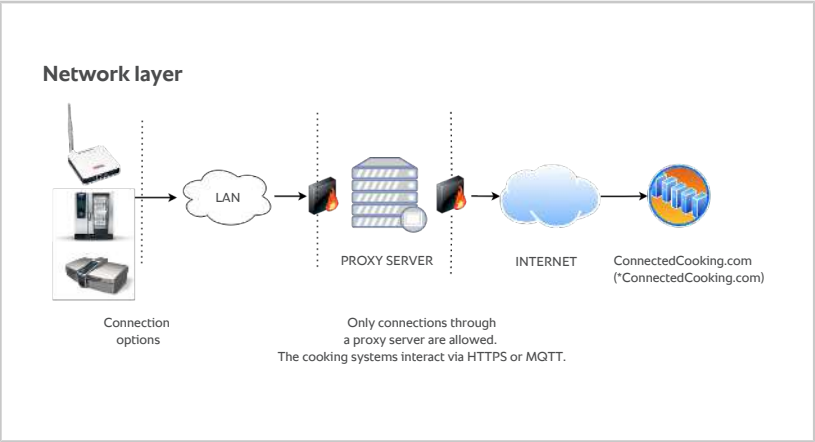


Pict. 2: Protocol layer

The pairing of the units and the subsequent communication are encrypted at all times.

3 Using a proxy server

RATIONAL cooking systems can establish a connection via a proxy server. Please note that we enable login via standard mechanisms on the proxy server. The communication must not be read (TLS inspection).



Pict. 3: Using a proxy server

- An exception rule for an MQTT connection is required to enable the connection through the proxy server, see Table 1: Communication ports.
- RATIONAL uses a self-signed TLS certificate to encrypt the connections.
- The The cooking system cannot establish a connection if a TLS or SSL inspection takes place between the ConnectedCooking server and the cooking system.

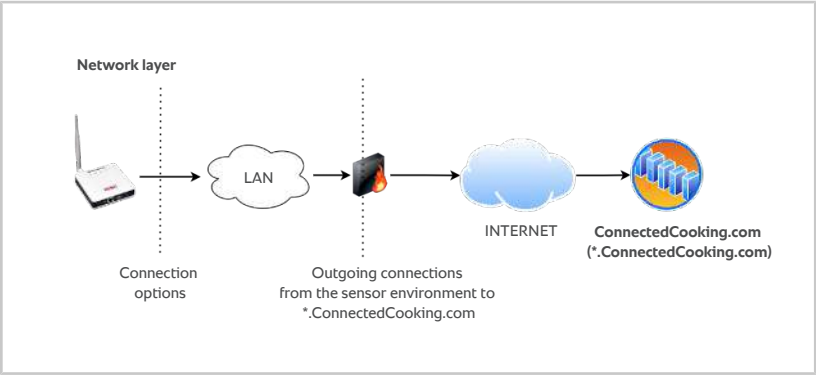
4 Access by ConnectedCooking users

ConnectedCooking users access ConnectedCooking with a desktop computer via the installed browser or with a smartphone or tablet via the Internet using an app.

The client (app or browser) establishes outgoing HTTPS connections with the ConnectedCooking servers and uses *.connectedcooking.com port 443 (HTTPs).

All connections are encrypted using TLS version 1.2 or higher. The Connected-Cooking servers only support connections with TLS 1.2 or higher. Insecure cipher suites are disabled.

5 Connection of ConnectedCooking Hygiene Management Pro sensors



Pict. 4: Networking of sensors for ConnectedCooking Hygiene Management Pro

When using the ConnectedCooking Hygiene Management Pro sensor network, a LoRa WAN gateway is connected to the Internet.

Data transmission between the sensors and the LoRaWAN gateway takes place via the ISM band, 868 MHz (ITU region 1) or 915 MHz (ITU region 2), as shown in Table 3: LoRa frequencies.

The LoRaWAN gateway obtains an IP address from the local network via DHCP.

The LoRaWAN gateway establishes an encrypted connection to the servers of the ConnectedCooking system and regularly transmits the sensor data to them, see table Communication ports. All connections are outbound only.

Ensure that your firewall is configured correctly to enable the transmission of sensor data to the cloud. All connections are encrypted with TLS so that the transmitted data cannot be read by third parties.

The data collected by the sensors is transmitted to the ConnectedCooking servers every 20 minutes via the LoRaWAN gateway.

6 ConnectedCooking support

The contact information for ConnectedCooking support and detailed documentation are available in ConnectedCooking under the support menu item.

7 Network requirements – ConnectedCooking Hygiene Management Pro

Requirements for successful integration of the RATIONAL unit into your network:

- Your unit is is equipped with a network connection or
- The unit has an internal Wi-Fi interface (e.g. iCombi Pro, iVario Pro or the additional Wi-Fi option for the iCombi Classic unit) or
- The Wi-Fi adapter option (RATIONAL 60.76.714) is installed.
- The unit displays the current date and time.
- The unit is equipped with the current software version, see Table 2.

The unit is connected to the Internet via:

- LAN: network connection socket with cable near the unit. It may be necessary to retrofit older unit models with an Ethernet connection.
- Wi-Fi (802.11b/g/n 2.4 GHz, WPA2): Good reception at the installation site via internal or external Wi-Fi interface.

The The cooking system is connected to the network as follows:

- LAN: an RJ45 cable connects the RATIONAL unit to a nearby network connection
- Wi-Fi: A built-in or external Wi-Fi interface (e.g. article no. 60.76.714, article no. 60.76.603) that connects to a Wi-Fi 802.11b/g/n (2.4 GHz) access point.
- All mains components must be installed in such a way that they are protected against splashes and water jets in accordance with the ambient conditions.

ConnectedCooking application:

To access ConnectedCooking, all you need is an Internet browser (Chrome, Firefox, MS Edge in the latest version) and access to *connectedcooking.com via port 443. ConnectedCooking does not install any programs on your computer.

Unit	Target	Protocol	Port	Direction	Description
SelfCookingCenter, VarioCookingCenter	*.connectedcooking.com	TCP	443	Outbound	HACCP data; Device data, if proxy server

Unit	Target	Protocol	Port	Direction	Description
iCombi Pro, iVario Pro					
SelfCookingCenter, VarioCookingCenter iCombi Pro, iVario Pro	*.connectedcooking.com	TCP	8883	Outbound	Device data
SelfCookingCenter, VarioCookingCenter iCombi Pro, iVario Pro	Customer DNS server	TCP/UDP	53	Outbound	DNS service
SelfCookingCenter, VarioCookingCenter iCombi Pro, iVario Pro	Customer DHCP server	UDP	68	Broadcast	DHCP service
iCombi-Classic	*.connectedcooking.com	TCP	8443	Outbound	HACCP data, Device data, if proxy server
iCombi-Classic	*.connectedcooking.com	TCP	8884	Outbound	Device data
iCombi-Classic	Customer DNS server	TCP/UDP	53	Outbound	DNS service
WGT-11	*.connectedcooking.com	TCP	8883	Outbound	MQTT
WGT-10	*.connectedcooking.com	UDP	1800/1801/1802	Outbound	Semtech UDP
WGT-10 WGT-11	0.pool.ubuntu.com	UDP/TCP	123	Outbound	Time server
WGT-10 WGT-11	1.1.1.1	ICMP	Ping	Outbound	Internet check
WGT-10 WGT-11	*.connectedcooking.com	TCP	443	Outbound	ConnectedCooking
SenseAnywhere	8.8.8.8	TCP/UDP	53	Outbound	DNS service

Unit	Target	Protocol	Port	Direc-tion	Descrip-tion
SenseAny-where	a.sa1.nl	TCP	80	Out-bound	Device data

Tab. 1: Communication ports

Unit	Min. required version	Availability
SelfCookingCenter	SCC_07-00-10-6.34 or higher	June 2022
VarioCookingCenter	VCC-01-02-04.7 or higher	June 2022
iCombi Pro	LM100-16.2.25 or higher	June 2022
iCombi Classic	LM200-8.0.0 or higher	June 2022
iVario Pro	LMX-2.10.0 or higher	June 2022

Tab. 2: Software versions

Region	Frequency (MHz)
EU	863-870
US	902-928
AU	915-928
CN	779-787, 470-510

Tab. 3: LoRa frequencies