IT Safety Manual
V 1.00

English

IMPORTANT

Read carefully before use!

Kathrein UHF RFID Reader

KATHREIN

Information provided in this manual is intended to be accurate and reliable. However, Kathrein Solutions GmbH assumes no responsibility for its use; nor for any infringements of rights of third parties which may result from its use. This document and the information contained in it are proprietary information of Kathrein Solutions GmbH and must be treated as confidential. Kathrein Solutions GmbH provides this document to its customers in connection with contacts of sale for the products described therein. If the person in possession of this document, being a legal or natural person, is not a contractual sales partner of Kathrein Solutions GmbH, or Kathrein Solutions GmbH has not intended him by other means as the recipient of the document and the information contained therein, the person in possession is hereby informed that the use of this document is unlawful and a violation of the rights of Kathrein Solutions GmbH.

Content

1 Preface

Dear customer,

Please follow all the information given in this guide. Kathrein Solutions GmbH has made every effort to ensure the information and descriptions are correct and complete. We reserve the right to make changes to this guide without prior notice. In particular, this applies to changes made due to technical advancements.

2 About this guide

This manual describes the functions and features of the Kathrein UHF RFID readers with regard to IT security. In addition to the devices themselves, the server-side IT remote station is also described.

It also provides detailed technical data to familiarise the user with the IT security requirements of Kathrein UHF RFID readers.

The target group of this manual is specialised personnel who install, configure and commission Kathrein UHF RFID readers. This document is valid for all Kathrein UHF RFID readers.

► For more information, visit our website www.kathrein-solutions.com.
The manuals are available for download at the internet product page.

3 Kathrein UHF RFID reader

These instructions apply to the following Kathrein UHF RFID readers:

Order number	UHF RFID reader
52010551 / 552	RRU 1400 RFID reader unit
52010288 / 296	RRU 4500 RFID reader unit
52010289 / 297	RRU 4560 RFID reader unit
52010290 / 298	RRU 4570 RFID reader unit
52010348 / 52010349	ARU 2400 antenna reader unit
52010664	ARU 2401 antenna reader unit
52010292 / 52010300	ARU 3500 antenna reader unit
52010340	ARU 8500 antenna reader unit

4 Introduction to the RFID system

An RFID system is comprised of the control computer of the reader, antennas, antenna connection cables and the tags. The figure below shows the schematic structure of the system:.

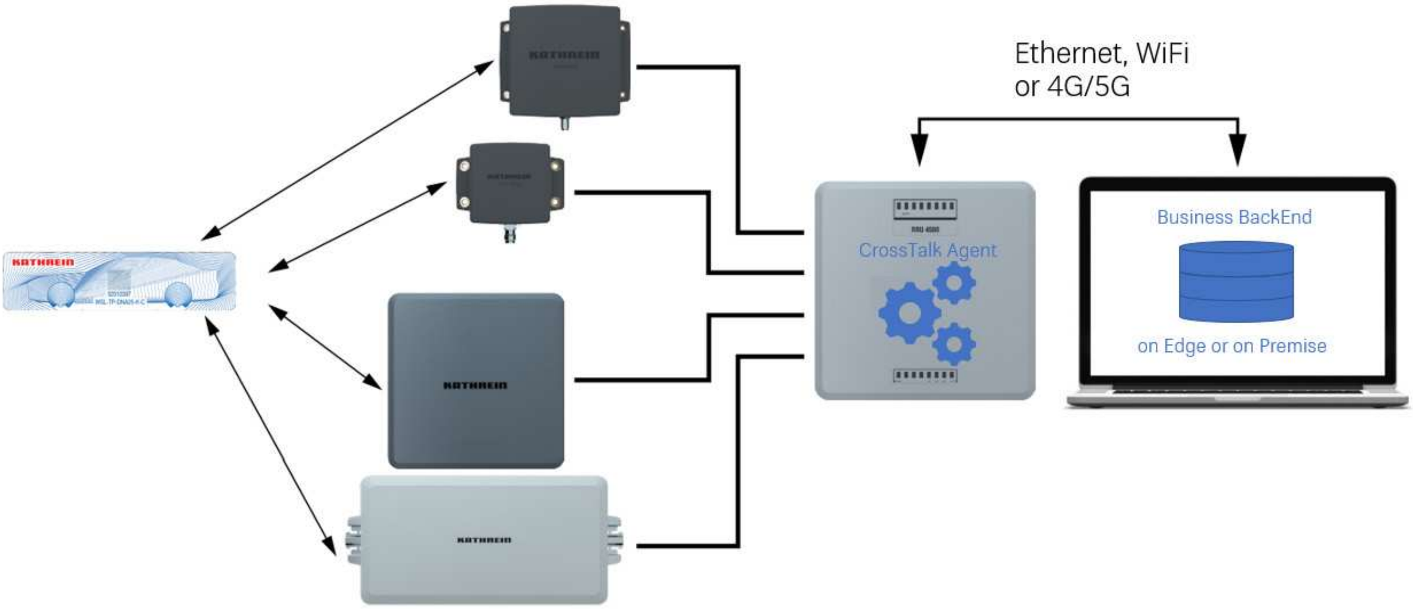


Figure 1: Example of an RFID system

The RFID reader is the central element here. It controls the UHF RFID antennas, which transform the wired transmission power into a radiated transmission power. This signal is used to transmit data to the passive (=battery-free) UHF RFID transponders. The reader can therefore both read data from the transponder and write data to the transponder.

As a rule, this data is used to identify objects such as containers, tools or vehicles. In addition to this identification data, further data can be stored that allows a more precise description of the object. Depending on the application, security-relevant access rights or parameters for payment can also be stored. In any case, data that needs to be protected.

Once the data has been received, it is processed in the reader CPU and prepared for distribution in an IT network. In addition to simple sorting and calculation functions, this also includes encryption and decryption operations.

Once the data has been processed, it is transferred to a backend system in an IT network. This is where the business logic is located, which can make decisions based on the data received from the transponders.

The requirements for IT security can therefore be divided into these three areas:

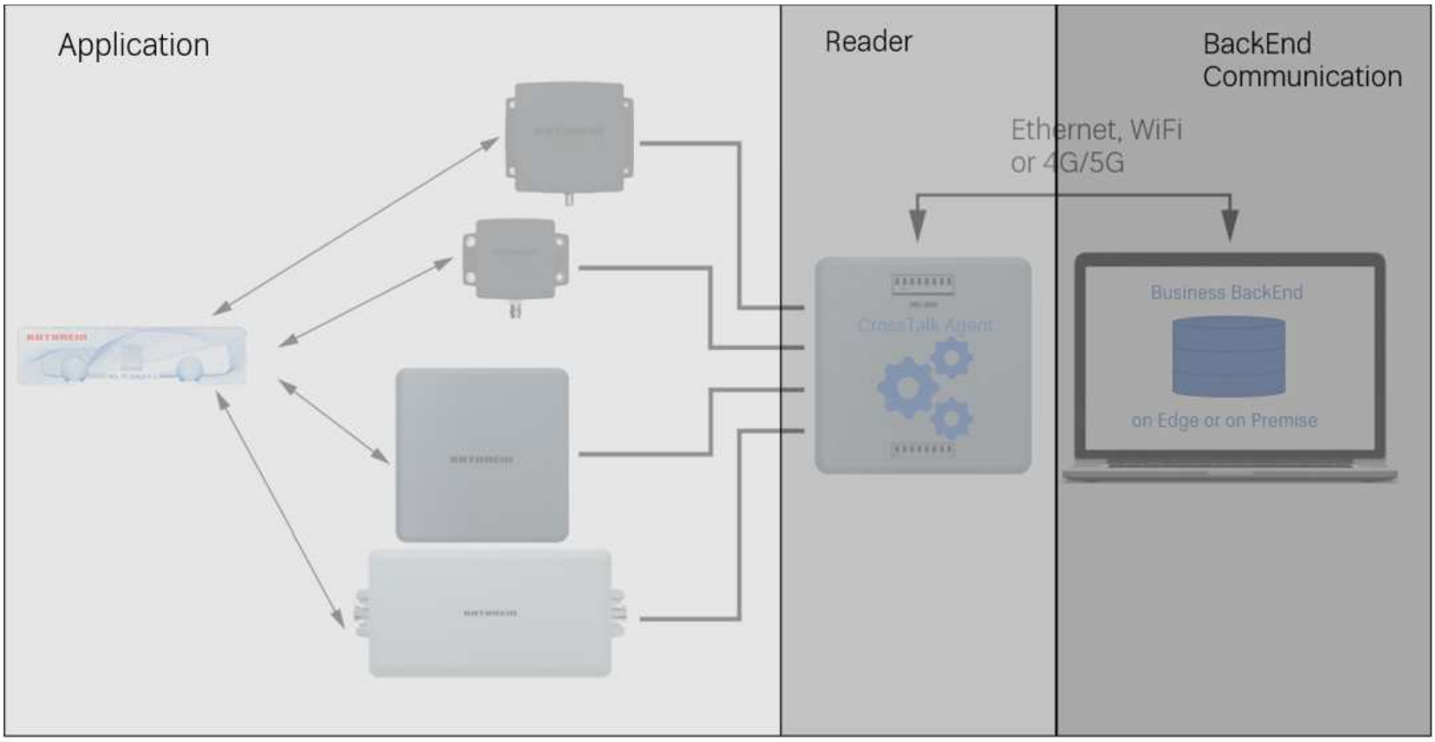


Figure 2: Categorisation of the IT security zones for an RFID system

As can be seen in the picture, there are three zones:

- the RFID application
- the RFID reader itself
- the communication to the back end

These zones also subdivide the various functions and parameters that Kathrein offers for IT security.

The rest of this section is organized in the order of these three zones.

5 IT security of Kathrein RFID reader

5.1 IT security in the RFID application

When accessing the transponders, the most important security aspects were already covered in the EPC Global Standard Gen2V2. For example, access to memory areas can be secured with a password. This password access can be cancelled or permanently requested. It is also possible to permanently delete the data of a transponder via a kill command.

As these and similar functions are well known, we will only refer here to the standard itself, which is explained in detail at GS1.

EPC UHF Gen2 Air Interface Protocol | GS1

Of course, the Kathrein readers implement these basic security requirements with all readers. For this purpose, the Kathrein Reader can be controlled via the Kathrein ReaderStart SW and the above-mentioned security features can be set or used. In addition, Kathrein offers security functions which are described below.

5.1.1 Authentication for RFID application

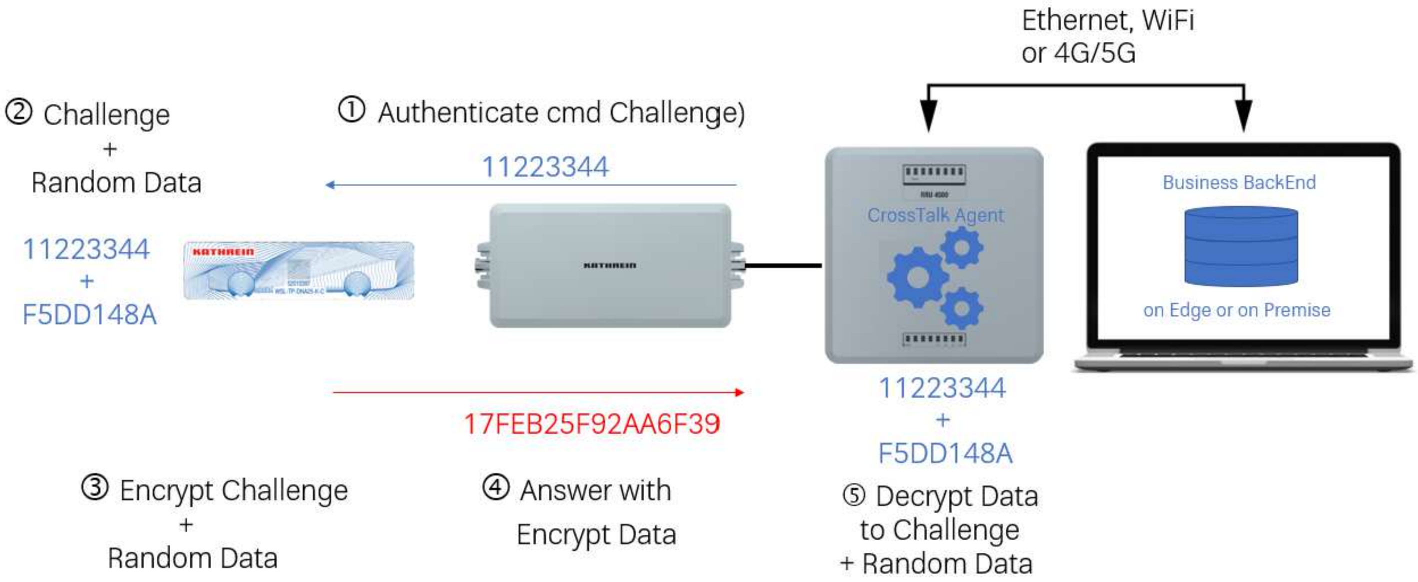
RFID is the standard when it comes to identifying parts and products. However, especially with high-priced or important products, there is always the question of whether the identification data is authentic.

A query for authentication of RFID transponders based on the EN 29167-10 standard is included in the basic command set of Kathrein readers and can be used for U Code DNA transponders, for example.

The UCode DNA IC combines advanced contactless performance with cryptographic security and enables a variety of smart city applications, such as asset tagging, automatic vehicle identification, access control and supply chain management. However, this functionality can be used in all other applications for encryption or authentication.

The advantage of this is that the authentication request is made directly on the reader. This makes the query quick and easy.

On Edge System Architecture – Authentifizierungs-Kommando



The authentication command is explained in 5 steps:

1. The reader selects a random but known data series after the command is called up. This series is called a challenge. This challenge, in this example "11223344", is then transmitted unencrypted on the air interface to the transponder
2. The RFID transponder accepts this command call and adds a purely random data series to the challenge - "11223344 + F5DD148A". This random data series is generated directly by the transponder and is reset with each call.
3. In the transponder IC, the complete data series from the challenge and random data is now encrypted with a predefined key A - "17FEB25F92AA6F39".
4. The transponder responds to the challenge command with the encrypted data series and transmits this data series back to the reader on the air interface
5. The reader decrypts the data series with the defined key A and thus finds the data for the challenge and the random data.

A repeated call with the same challenge always generates a different data series with random data in the transponder. This means that the transponder's encrypted response is different for each call, even if the same challenge is always used.
It is of course essential that the keys set in the reader and transponder are imprinted in secure areas.

5.1.2 Decryption und key-handling at RFID application

The most secure way to handle the encrypted data is in the back-end system itself. There, the keys can be accessed directly in a high-security area and the necessary calculations for decryption can be carried out.However, this solution is usually associated with very high costs for the required infrastructure.

A cost- and speed-optimised solution is achieved by immediately transmitting a pending decision based on this decrypted data at the reading location itself. This applies, for example, to access control systems that regulate the entry authorisation of vehicles. If a vehicle with registered authorisation is in front of a barrier, the opening of the barrier can be delayed if the connection to the backend is slow or the release calculations in the backend are delayed due to high demand.

To optimise this situation, the Kathrein RFID readers in the X5xx series have an integrated High Secure Memory (HSM) module. The keys are securely stored in this module and the calculation steps required to decrypt the data can also be carried out directly in this HSM module. This protects the stored data and keys from unauthorised access. If the HSM module detects unauthorised access, all stored data is immediately and irretrievably deleted. This is independent of whether the attack was carried out via the data interface or by mechanical or other means.

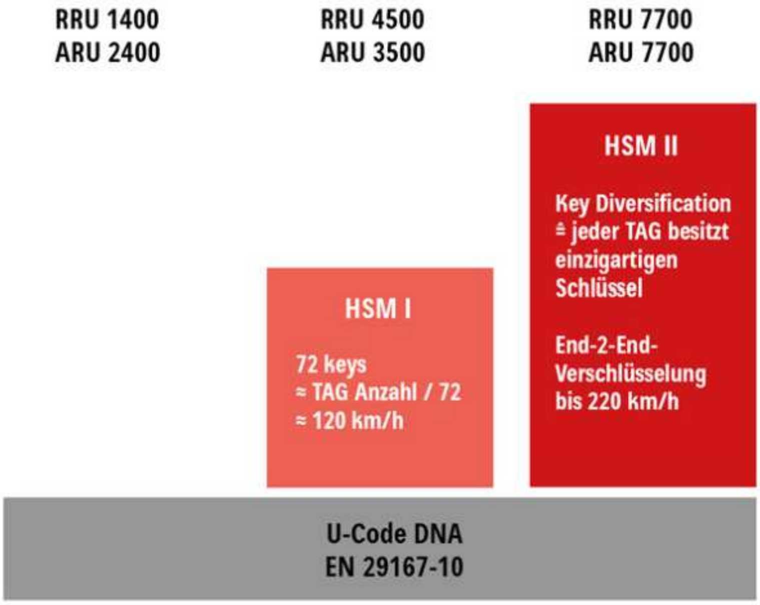
At the same time, the correct keys are also selected in the HSM module. The existing transponder population can be addressed with up to 72 different keys. If a key is compromised, only 1.4 % of the transponders are affected!

This makes it possible to quickly decrypt the data on site and at the same time keep the barriers to unauthorised access high.

In addition to the standard applications with x5xx readers, the ARU/RRU 7700 reader series can be used for higher requirements. On the one hand, the access speed to encrypted data has been increased once again. With this new HSM module, it is possible to read data from the transponder memory at the same time as decrypting data that has already been read. There is no need to focus on reading new data or decrypting data that has already been read, as this is done simultaneously.

The readers in the RRU 7700/ ARU 7700 series also feature dynamic key handling. With so-called key diversification, each individual transponder is assigned a unique key. If a key is compromised, only one transponder is affected.

The ARU / RRU 7700 RFID reader series with the new HSM module increases security while at the same time improving access times. In addition, high investments in complex network structures and backend systems can be avoided.



5.2 IT security with the Kathrein RFID readers

This section describes the security features offered by the Kathrein readers themselves. As the readers are very often prominently installed in publicly accessible areas, both mechanical and technical attacks must be taken into account.

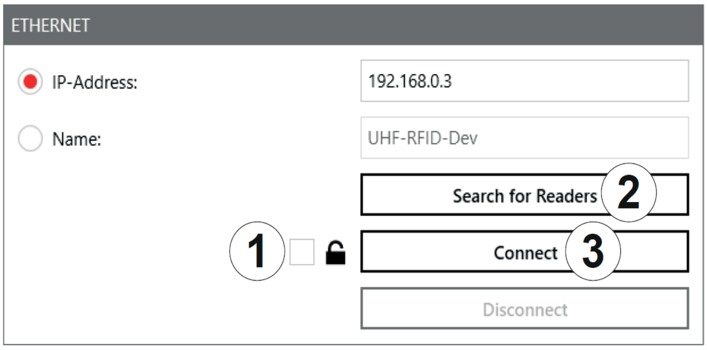
The individual measures are listed below without prioritising the order. In section "7.4 Application recommendation for IT security for Kathrein RFID readers", recommendations are listed for security measures for various applications. However, the security requirements are very individual. If required, you can obtain further information and support at
Support (kathrein-solutions.com)

5.2.1 IPv4 and IPv6 address space

The Ethernet connection is achieved by integrating the reader into an existing network or by directly connecting the reader and the control computer. To connect the reader directly to the PC, a cross-link cable is required, unless the LAN interface of the PC supports auto-mdi-x. Alternatively, it is possible to use two standard patch cables and a switch. The default IP address of the Kathrein RFID readers is 192.168.0.1. Other default values are:

Name	UHF-RFID-Dev
IPv4 adress	162.168.0.1
Subnet mask	255.255.255.0
Keep alive time	2000 ms
DHCP	inactive
IPv6 adress	z.B. fe::2d0:55ff:fe01:12c9/64

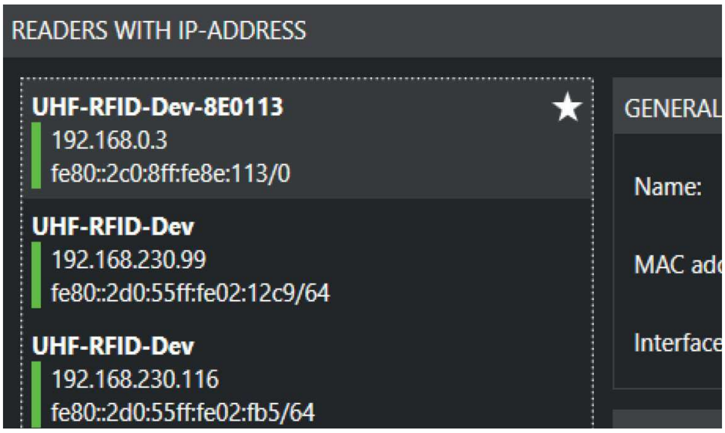
We recommend using the Kathrein ReaderStart SW to set up the Ethernet settings. There you will find the option to use a known IP to establish a connection to the reader and to search for unknown IP addresses. The lock symbol can be used to activate SSH connections and thus encrypt the data from the reader to the control computer or backend.


ETHERNET

● IP-Address: 192.168.0.3

○ Name: UHF-RFID-Dev

Unknown reader IP addresses are found using the search function. A broadcast command is used to force all connected readers to transmit their IPv4 and IPv6 addresses. The result is displayed as follows.



READERS WITH IP-ADDRESS

UHF-RFID-Dev-8E0113
192.168.0.3
fe80::2c0:8ff:fe8e:113/0

UHF-RFID-Dev
192.168.230.99
fe80::2d0:55ff:fe02:12c9/64

UHF-RFID-Dev
192.168.230.116
fe80::2d0:55ff:fe02:fb5/64

The values found can be accepted by clicking on them and the connection to the reader is established.
Further information on setting the IP addresses can be found in the Reader manual.

5.2.2 Secure connections with SSH

To ensure that the connection between the reader and the control computer is not visible, this connection can be encrypted using standard methods. It is sufficient to tick the lock symbol when connecting and the reader will request a password when connecting.

5.2.3 Login procedure

You can log in as an admin (root) with full access rights or as a user with reduced access.

The number of login attempts can be limited and a waiting time can be set, which must elapse before renewed access is permitted if the previous attempt has failed.

5.2.3.1 Passwords

A login name and password can be assigned for dialling in with an SSH connection. The password can also be reassigned after a successful connection with the reader.

Another password level is used to protect the configuration. If this is set, the user cannot make any changes to the setting parameters.

5.2.3.2 Certificate

The user can also choose whether a key file or a certificate is used instead of the password.

5.2.4 Port deactivation

Internal ports (UART board ports) can be deactivated to counter attacks at circuit board level. This prevents unauthorised access to the reader both during operation and when booting the reader.

External Ethernet ports can also be permanently deactivated. This is particularly important for the x5xx and x7xx readers, which have two Ethernet ports with an intelligent switch built in.

5.2.5 Limitation of simultaneous sessions

If SSH connections are used, it can be set that only SSH connections are possible on the reader. The number of sessions established at the same time can also be limited so that a maximum of only one session is possible.

5.2.6 Safety measures with wireless readers

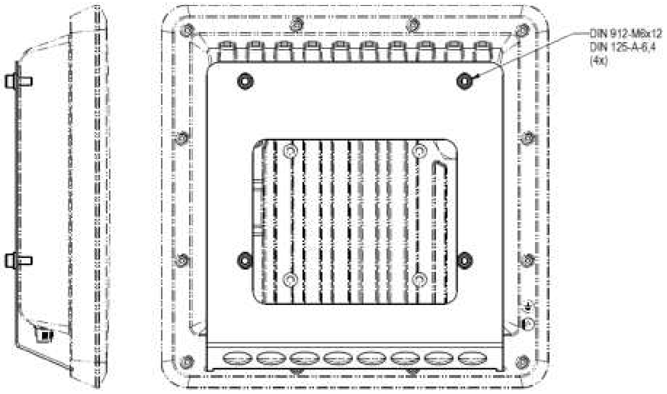
Suitable security levels are offered for the RRU 4560 (WLAN) and RRU 4570 (4G) readers, which prevent unauthorised access.

With the RRU 4560, the passwords are used for dialling in to recognised SSID networks. These passwords are only transferred between ReaderStart and the reader if an SSH connection is activated for the LAN port.

For the RRU 4570 with built-in 4G module, the access rights are managed via PIN, APN, user name and password. A complete description is not possible at this point. If required, please refer to the Reader manual or contact our support team.

5.2.7 Mechanical safety measures

To make it more difficult to access Kathrein readers that are freely accessible outdoors, Kathrein offers a vandalism protection that at least makes it more difficult to access or dismantle the reader.



The connectors are secured against loosening, as is the removal of the SIM card from the RRU 4570 reader. As the vandalism protection snaps directly into the back of the reader housing, mechanical attacks are only possible with extreme force. Dismantling the protection is time-consuming and prevents quick access to the reader.

5.3 Secure data transmission to backend systems

Efficient AutoID systems for automatic object identification and data capture as well as IoT (Internet of Things) systems require excellent hardware and at least equally excellent AutoID and IoT software. We offer such a software solution in addition to the hardware.

The CrossTalk software suite is one of the most advanced software systems for AutoID and IoT device management. The software can be customised almost at will to meet new challenges and can be used in a wide range of industries. It reduces running costs and accelerates data processing operations.

In addition, the CrossTalk Agent Edgeware, which can be installed directly on the UHF RFID reader, offers secure data transmission paths for business events to various backend systems.

These include:
- HTTP Post/Put
- TLS (https)
- Base authentication (user/password)
- API-KEY (inside http header)
- OAuth2 access token (inside http header)

MQTT Client:
- TLS (mqtts)
- Quality of service (QoS) levels 0-2

Further information on CrossTalk and the options for securing your IT landscape can be found on our homepage at Software (kathrein-solutions.com)

5.4 Application recommendation for IT security for RFID reader

This section lists recommendations for safety measures for various applications. However, safety requirements are very individual.

The application recommendations were categorised into 3 types of use:
- Inside buildings: acceptance of cordoned-off premises, access only for authorised personnel, therefore no need for hardening
- Within company premises: Assumption of cordoned-off outdoor area with external traffic possible (e.g. company car park, factory gate, etc.)
- Publicly accessible: Assumption that the readers are accessible to everyone (e.g. public car parks, etc.)

Measure	Inside of buildings	Within company premises	Publicly accessible
Set SSH password	x	x	x
Only allow secure connections	x	x	x
Distinction between admin / user	x	x	x
Set up a new user		x	x
Reject new users		x	x
Set configuration password		x	x
Limit the number of login attempts		x	x
Set duration between login attempts		x	x
Limitation of simultaneous sessions		x	x
Deactivate internal or external ports			x
Mechanical safety measures		x	x

If required, you can obtain further information and support from our Kathrein Training Academy or via the sales support.

Electronic equipment is not domestic waste – in accordance with directive 2002/96/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL dated 27th January 2003 concerning used electrical and electronic appliances, it must be disposed of properly. At the end of its service life, take this unit for disposal at a designated public collection point.