IT Sicherheits-Handbuch
V 1.00

Deutsch

Kathrein UHF RFID Reader

KATHREIN

Content

1 Vorwort

Sehr geehrter Kunde,

bitte beachten Sie alle Hinweise in dieser Anleitung. Die KATHREIN Solutions GmbH hat sich um Richtigkeit und Vollständigkeit der Angaben und Beschreibungen bemüht.

Wir behalten uns das Recht vor, Änderungen an dieser Anleitung ohne vorherige Ankündigung vorzunehmen. Dies gilt insbesondere für Änderungen, die dem technischen Fortschritt dienen.

2 Über dieses Handbuch

Dieses Handbuch beschreibt die Funktionen und Eigenschaften der Kathrein UHF RFID Reader in Bezug auf die IT-Sicherheit. Dabei werden neben den Geräten selbst auch die serverseitige IT-Gegenstelle beschrieben.

Darüber hinaus liefert es detaillierte technische Daten, um den Anwender mit den Anforderungen der IT-Sicherheit bei Kathrein UHF RFID Reader besser vertraut zu machen.

Die Zielgruppe dieses Handbuchs ist Fachpersonal, das die Kathrein UHF RFID Reader installiert, konfiguriert und in Betrieb nimmt. Dieses Dokument ist gültig für alle Kathrein UHF RFID Reader.

► Weitere Informationen finden Sie auf unserer Internetseite www.kathrein-solutions.com.
Die Handbücher stehen auf der Internet-Produktseite zum Download bereit.

3 Kathrein UHF RFID Reader

Diese Anleitung gilt für die folgenden Kathrein UHF RFID Reader:

Bestellnummer	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 Einführung in das RFID-System

Ein RFID-System besteht aus einem Steuerrechner oder BackEnd-System, dem Reader, Antennen und den Transpondern, auch TAGs genannt. Die folgende Abbildung zeigt den schematischen Aufbau des Systems.

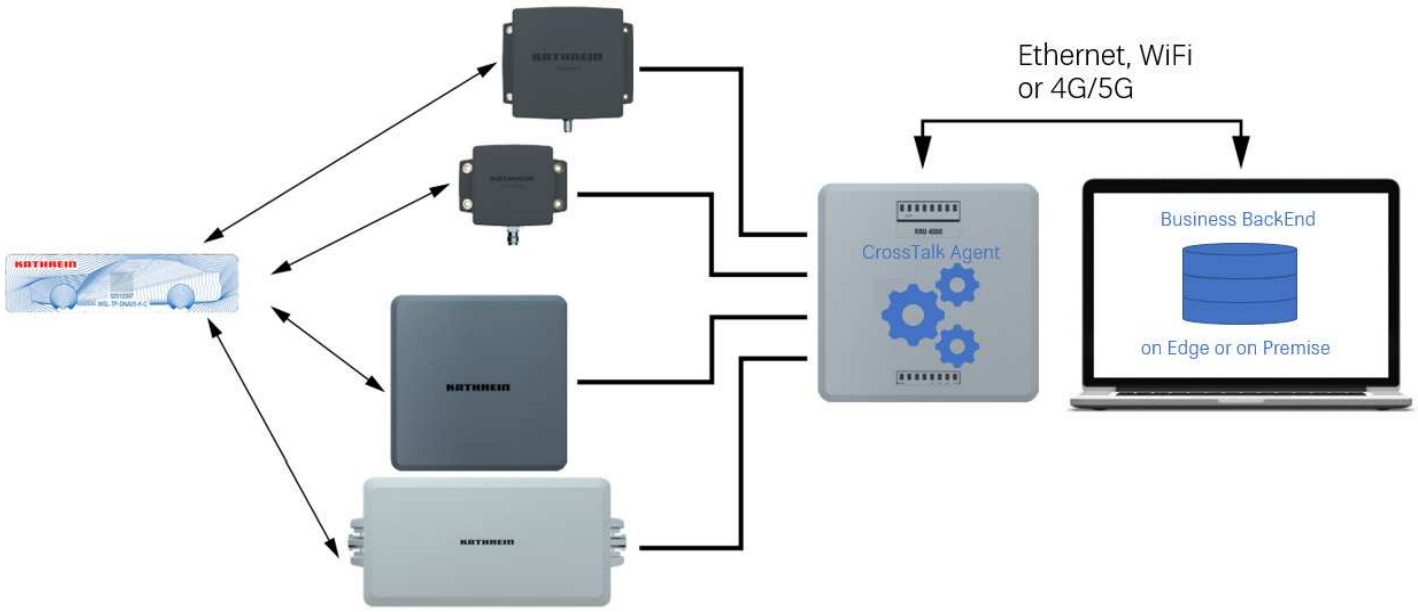


Bild 1: Beispiel für ein RFID-System

Der RFID-Reader ist dabei das zentrale Element. Er steuert die UHF RFID Antennen an, die die leitungsgebunde Sendeleistung in eine abgestrahlte Sendeleistung transformieren. Auf diesem Signal werden Daten an die passiven (=batterielosen) UHF RFID Transponder übertragen. Damit kann der Reader sowohl vom Transponder Daten auslesen als auch Daten auf den Transponder schreiben.

In der Regel stehen diese Daten für die Identifikation von Dingen, wie z.B. Behälter, Werkzeuge oder Fahrzeuge. Neben diesen Identifikations-Daten können weitere Daten gespeichert werden, die eine genauere Beschreibung des Objekts erlauben. Je nach Anwendung können dabei auch sicherheitsrelevante Zutrittsrechte oder aber auch Parameter für die Bezahlung hinterlegt sein. Nach dem Empfang der Daten werden sie in der Reader CPU verarbeitet und für die Verteilung in ein IT-Netzwerk eingebunden. Dies umfasst neben einer einfachen Sortier- und Berechnungsfunktion aber auch Ver- bzw. Entschlüsselung-Operationen.

Nachdem die Daten aufbereitet worden sind, werden sie in einem IT-Netzwerk an ein Backend System übertragen. Dort sitzt die Business-Logik, die aufgrund der empfangenen Daten aus den Transpondern Entscheidungen treffen kann.

Damit lassen sich die Anforderungen an die IT-Sicherheit in diese drei Bereiche einteilen.

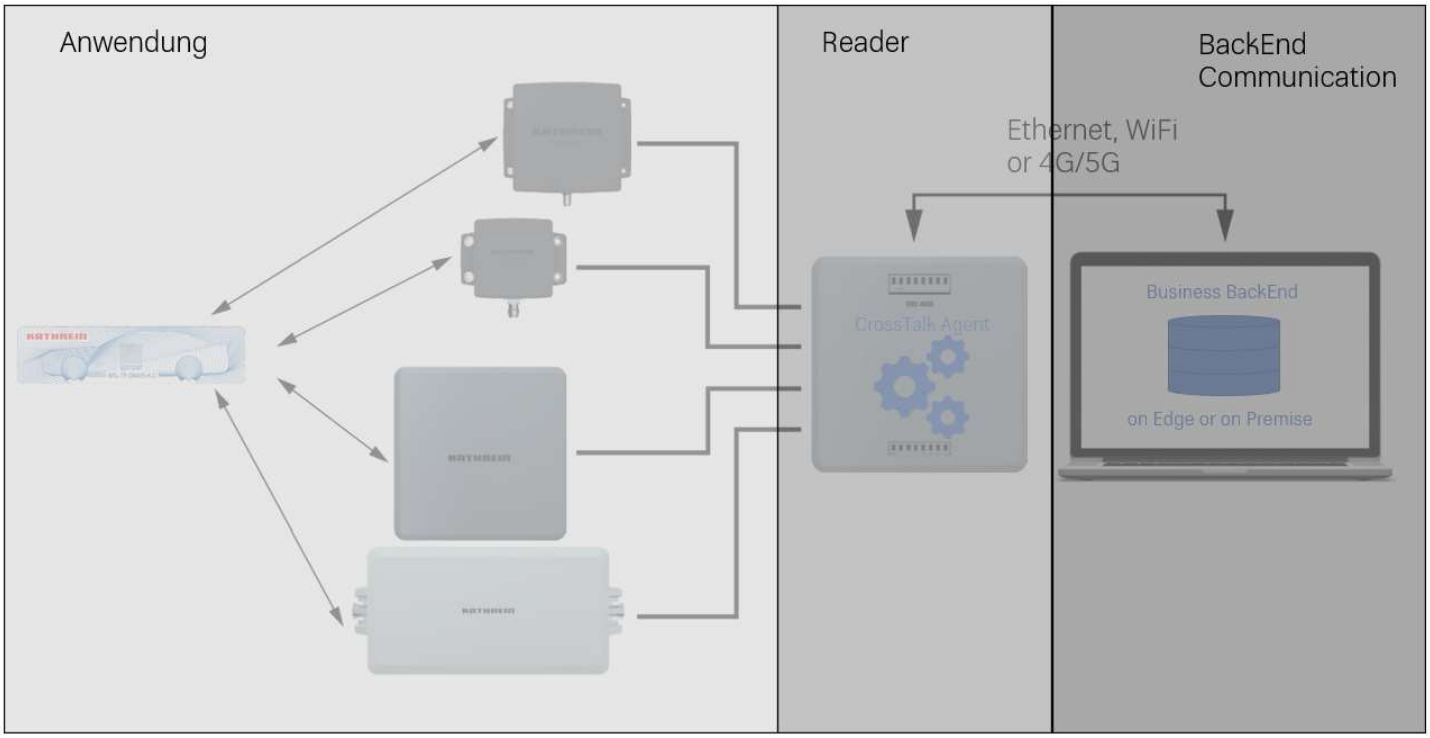


Bild 2: Einteilung der IT-Sicherheitszonen für ein RFID-System

Wie im Bild zu sehen, ergeben sich drei Zonen:

- die RFID Anwendung
- der RFID Reader selbst
- die Kommunikation zum BackEnd

Diese Zonen unterteilen auch die verschiedenen Funktionen und Parameter, die Kathrein für die IT-Sicherheit anbietet. Die weitere Betrachtung erfolgt in der Reihenfolge dieser drei Zonen.

5 IT-Sicherheit der Kathrein RFID Reader

5.1 IT-Sicherheit in der RFID Anwendung

Beim Zugriff auf die Transponder wurden bereits im EPC Global Standard Gen2V2 die wichtigsten Sicherheitsaspekte mit abgedeckt. So kann der Zugriff auf Speicherbereiche mit einem Passwort gesichert werden. Dieser Passwort-Zugriff kann wieder zurückgenommen werden oder permanent eingefordert werden. Ebenso ist es möglich, die Daten eines Transponders über einen Kill-Befehl dauerhaft zu löschen.

Da diese und ähnliche Funktionen hinlänglich bekannt sind, sei hier nur auf den Standard selbst verwiesen, der z.B. bei GS1 ausführlich erläutert wird .

EPC UHF Gen2 Air Interface Protocol | GS1

Natürlich setzen die Kathrein Reader diese Grundsicherheitsanforderungen mit allen Readern um. Dazu kann der Kathrein Reader über die Kathrein ReaderStart SW angesteuert werden und die o.g. Sicherheitseigenschaften gesetzt bzw. genutzt werden. Darüber hinaus bietet Kathrein Sicherheitsfunktionen an, die im Nachfolgenden beschrieben sind.

5.1.1 Authentifizierung bei RFID Anwendung

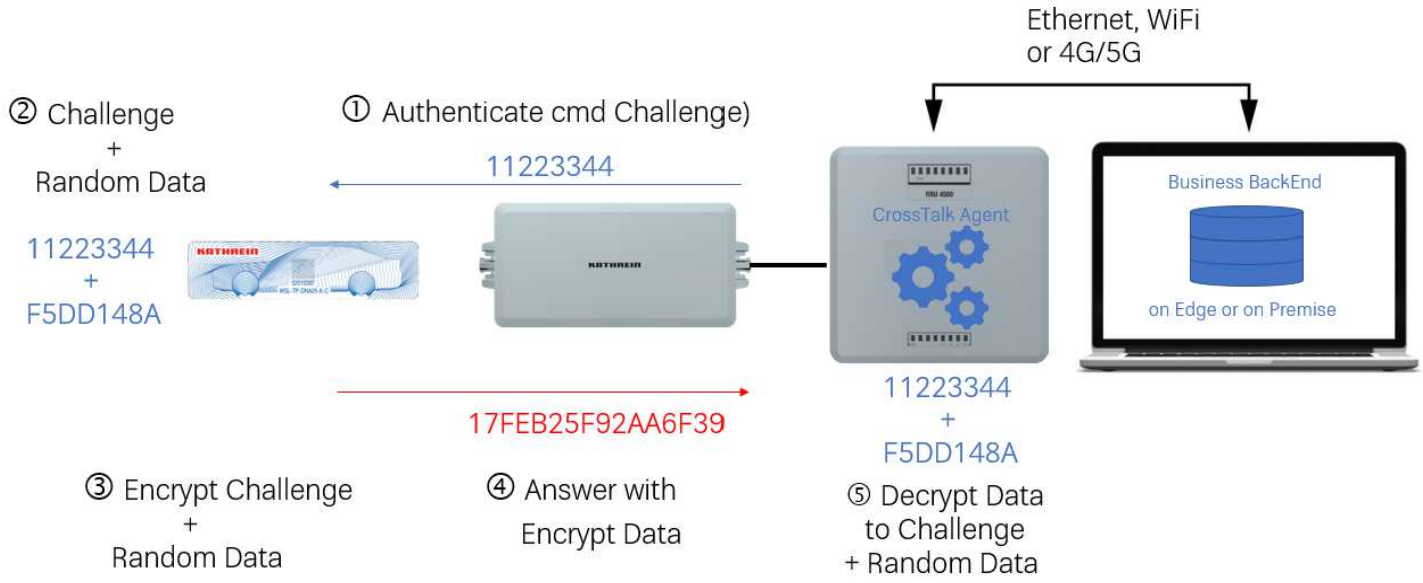
RFID ist gesetzt, wenn es um die Identifizierung von Teilen und Produkten geht. Dabei steht aber vor allem bei hochpreisigen oder wichtigen Produkten immer die Frage im Raum, ob die Identifizierungs-Daten auch authentisch sind.

Eine Abfrage zur Authentifizierung von RFID Transpondern auf Basis des Standards EN 29167-10 ist bei Kathrein Readern im Grund-Befehlssatz enthalten und kann z.B. für U Code DNA Transponder genutzt werden.

Dabei kombiniert der UCode DNA IC fortschrittliche kontaktlose Leistung mit kryptografischer Sicherheit und ermöglicht eine Vielzahl von Smart-City-Anwendungen, wie z. B. Asset-Tagging, automatische Fahrzeugidentifikation, Zugangskontrolle und Lieferkettenmanagement. Jedoch kann diese Funktionalität bei allen anderen Anwendungen zur Verschlüsselung oder Authentifizierung genutzt werden.

Der Vorteil dabei ist, dass diese Abfrage zur Authentifizierung direkt auf dem Reader passiert. Somit ist die Abfrage schnell und einfach möglich.

On Edge System Architecture – Authentifizierungs-Kommando



Das Authentifizierungs Kommando ist in 5 Schritten erklärt:

1. Der Reader wählt nach dem Befehlsaufruf eine zufällige, aber bekannte Datenreihe. Diese Reihe wird Challenge genannt. Diese Challenge, hier im Beispiel „11223344“, wird dann unverschlüsselt auf der Luftschnittstelle an den Transponder übertragen.
2. Der RFID Transponder übernimmt diesen Befehlsaufruf und addiert zur Challenge eine rein zufällige Datenreihe – „11223344 + F5DD148A“. Diese zufällige Datenreihe wird direkt vom Transponder erzeugt und bei jedem Aufruf neu gesetzt.
3. Im Transponder IC wird nun die komplette Datenreihe aus Challenge und Random Data mit einem vordefinierten Key A verschlüsselt – „17FEB25F92AA6F39“.
4. Der Transponder antwortet auf den Challenge-Befehl mit der verschlüsselten Datenreihe und überträgt diese Datenreihe auf der Luftschnittstelle zurück an den Reader.
5. Der Reader entschlüsselt die Datenreihe mit dem definierten Key A und findet so die Daten für die Challenge und die zufälligen Daten.

Bei einem wiederholten Aufruf mit derselben Challenge wird immer eine andere Datenreihe mit zufälligen Daten im Transponder erzeugt. Somit ist die verschlüsselte Antwort des Transponders bei jedem Aufruf unterschiedlich, auch wenn immer dieselbe Challenge benutzt würde.

Es ist natürlich essentiell wichtig, dass die gesetzten Schlüssel im Reader und in den Transpondern in sicheren Bereichen aufgeprägt werden.

5.1.2 Decryption und Key-Handling bei RFID Anwendung

Die sicherste Art, die verschlüsselten Daten zu behandeln, ist im BackEnd System selbst. Dort kann in einem Hochsicherheitsbereich direkt auf die Schlüssel zugegriffen werden und die notwendigen Berechnungen für die Entschlüsselung durchgeführt werden. Diese Lösung ist aber in der Regel mit sehr hohen Kosten für die benötigte Infrastruktur verbunden.

Eine kosten- und geschwindigkeitsoptimierte Lösung wird dadurch erreicht, dass eine anstehende Entscheidung auf Basis dieser entschlüsselten Daten sofort am Leseort selbst übermittelt wird. Dies trifft z.B. bei Zugangskontrollsystemen zu, bei dem die Einfahrtberechtigung von Fahrzeugen geregelt werden. Steht ein Fahrzeug mit eingetragener Berechtigung vor einer Schranke, so kann sich das Öffnen der Schranke verzögern, wenn die Verbindung zum Backend langsam ist oder die Freigabeberechnungen im Backend aufgrund hoher Nachfrage verzögert sind.

Um diesen Sachverhalt zu optimieren, haben die Kathrein RFID Reader der X5xx-Reihe ein High Secure Memory (HSM)-Modul eingebaut. In diesem Modul werden die Schlüssel sicher verwahrt und ebenso können die benötigten Berechnungsschritte zum Entschlüsseln der Daten direkt in diesem HSM-Modul vorgenommen werden.

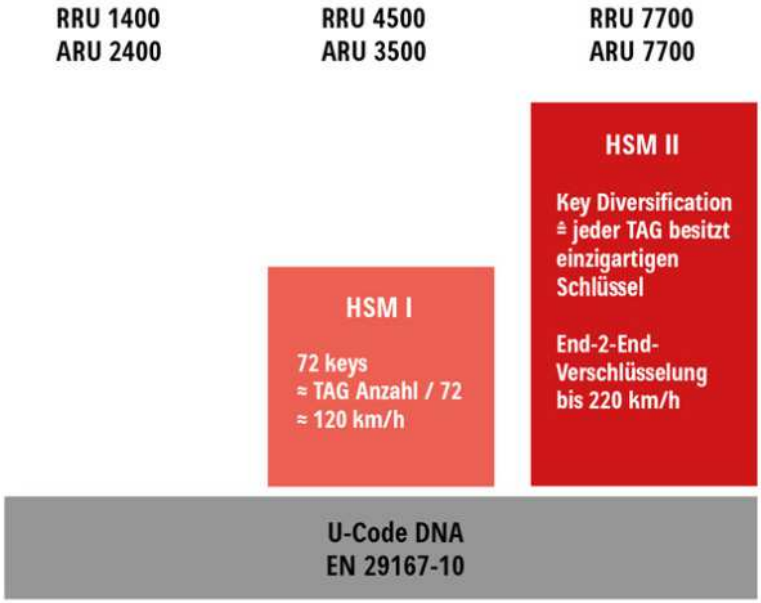
Dabei werden die gespeicherten Daten und Schlüssel vor unerlaubtem Zugriff geschützt. Stellt das HSM-Modul fest, dass ein unerlaubter Zugriff vorliegt, werden sofort alle gespeicherten Daten unwiederbringlich gelöscht. Dies ist unabhängig davon, ob der Angriff über die Datenschnittstelle oder aber auch durch mechanische oder andere Maßnahmen erfolgt ist.

Gleichzeitig erfolgt die Auswahl der richtigen Keys ebenso im HSM-Modul. Dabei kann die vorhandene Transponder-Population mit bis zu 72 unterschiedlichen Schlüsseln angesprochen werden. Wird dabei ein Schlüssel kompromittiert, sind nur 1,4 % der Transponder betroffen! Somit ist es möglich, die Daten vor Ort schnell zu entschlüsseln und gleichzeitig die Hürden für unerlaubten Zugriff hochzuhalten.

Neben den Standardanwendungen mit einem x5xx-Reader kann für höhere Anforderungen die Reader Reihe ARU/RRU 7700 genutzt werden. Zum einen konnte nochmals die Zugriffsgeschwindigkeit auf verschlüsselte Daten gesteigert werden. Mit diesem neuen HSM-Modul ist es möglich, dass das Lesen von Daten aus dem Transponderspeicher parallel mit der Entschlüsselung bereits gelesener Daten erfolgen kann. Eine Fokussierung aufs Lesen neuer Daten oder dem Entschlüsseln bereits gelesener Daten entfällt, da es gleichzeitig erfolgt.

Außerdem verfügen die Reader der RRU 7700/ ARU 7700 Serie über ein dynamisches Schlüssel-Handling. Bei der sogenannten Key-Diversification wird jedem einzelnen Transponder ein eindeutiger Schlüssel zugeordnet. Wird ein Schlüssel kompromittiert, so ist auch nur ein Transponder davon betroffen.

Die ARU / RRU 7700 RFID Reader Reihe mit dem neuen HSM-Modul steigert die Sicherheit, bei gleichzeitigen Verbesserungen der Zugriffszeiten. Zusätzlich können hohen Investitionen in aufwendige Netzwerkstrukturen und Backend-Systeme vermieden werden.



5.2 IT-Sicherheit mit den Kathrein RFID Readern

In diesem Abschnitt wird beschrieben, welche Sicherheitsfeature die Kathrein Reader selbst bieten. Da die Reader sehr oft prominent im öffentlich zugänglichen Bereich aufgebaut werden, müssen sowohl mechanische wie technische Angriffe berücksichtigt werden.

Im Nachfolgenden werden die einzelnen Maßnahmen ohne die Gewichtung der Reihenfolge aufgelistet. Im Abschnitt „7.4 Anwendungsempfehlung für IT-Sicherheit bei Kathrein RFID Reader“ werden Empfehlungen gelistet für Sicherheitsmaßnahmen bei verschiedenen Einsatzfällen. Jedoch sind die Anforderungen an Sicherheit sehr individuell. Bei Bedarf erhalten Sie weiteren Information und Unterstützung unter:

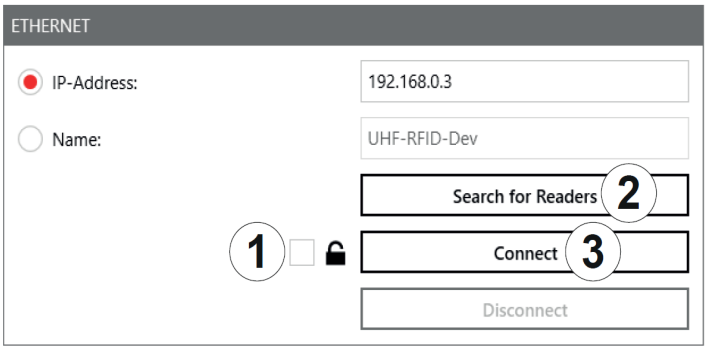
Support (kathrein-solutions.com)

5.2.1 IPv4 und IPv6 Adressraum

Die Ethernet-Verbindung wird durch die Einbindung des Lesegeräts in ein bestehendes Netzwerk oder durch die direkte Verbindung des Readers und dem Steuerrechner erreicht. Um das Lesegerät direkt mit dem PC zu verbinden, wird ein Cross-Link-Kabel benötigt, es sei denn, die LAN Schnittstelle des PCs unterstützt auto-mdi-x. Alternativ ist es möglich, zwei Standard-Patchkabel und einen Switch zu verwenden. Die Kathrein RFID Reader haben als Default IP-Adresse die 192.168.0.1. Weitere Default Werte sind:

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

Für die Einrichtung der Ethernet-Einstellungen wird die Kathrein ReaderStart SW empfohlen. Dort finden Sie die Möglichkeit, eine bekannte IP einzusetzen und damit eine Verbindung (3) zum Reader aufzubauen und um unbekannte IP-Adressen zu suchen (2). Über das Schloss-Symbol können SSH-Verbindungen aktiviert werden und damit die Daten vom Reader zum Steuerrechner oder Backend verschlüsselt



Unbekannte Reader-IP Adressen werden über die Suchfunktion (2) gefunden. Mittels eines Broadcastbefehls werden alle angeschlossenen Reader gezwungen, ihre IPv4 und IPv6-Adressen zu übermitteln. Das Ergebnis wird wie folgt angezeigt:

Durch Anklicken können die gefundenen Werte übernommen werden und die Verbindung zum Reader wird aufgebaut. Weitere Informationen zur Einstellung der IP-Adressen entnehmen Sie dem Reader Handbuch.

5.2.2 Sichere Verbindungen mit SSH

Damit die Verbindung zwischen Reader und dem Steuerrechner nicht einsehbar ist, kann diese Verbindung nach gängigen Methoden verschlüsselt werden. Es genügt beim Verbinden, den Haken beim Schloss-Symbol zu setzen und der Reader fragt beim Verbinden ein Passwort ab.

5.2.3 Login-Verfahren

Der Login kann als Admin (root) mit vollem Zugriffsrecht erfolgen oder als Anwender (user) mit reduziertem Zugriff. Dabei können die Anzahl der Einwahlversuche begrenzt und ebenso eine Wartezeit gesetzt werden, die verstreichen muss bis ein erneuter Zugriff erlaubt ist, wenn der vorhergehende Versuch fehlgeschlagen ist.

5.2.3.1 Passwörter

Für die Einwahl mit SSH-Verbindung kann ein Login-Name und ein Passwort vergeben werden. Nach erfolgreicher Verbindung mit dem Reader kann das Passwort auch neu vergeben werden.

Eine weitere Passwortebene wird für den Schutz der Konfiguration genutzt. Ist dieser gesetzt, kann der Anwender keine Veränderung an den Einstellparametern vornehmen.

5.2.3.2 Zertifikat

Ebenfalls kann der Anwender aussuchen, ob anstatt des Passworts ein Key-file bzw. ein Zertifikat genutzt wird.

5.2.4 Ports deaktivieren

Um Angriffen auf Leiterplattenebene zu begegnen, können interne Ports (UART Platinenports) deaktiviert werden. Damit ist sowohl im laufenden Betrieb als auch beim Booten des Readers ein unerlaubter Zugriff auf den Reader unterbunden.

Externe Ethernet Ports können ebenso dauerhaft deaktiviert werden. Dies ist vor allem bei den x5xx und 77xx Readern wichtig, die zwei Ethernetports mit einem intelligenten Switch eingebaut haben.

5.2.5 Begrenzung gleichzeitiger Sessions

Werden SSH-Verbindungen genutzt, kann eingestellt werden, dass ausschließlich SSH Verbindungen auf dem Reader möglich sind. Ebenso kann die Anzahl der gleichzeitigt aufgebauten Sessions begrenzt werden, so dass maximal eine Session möglich ist.

5.2.6 Sicherheitsmaßnahmen bei Wireless Readern

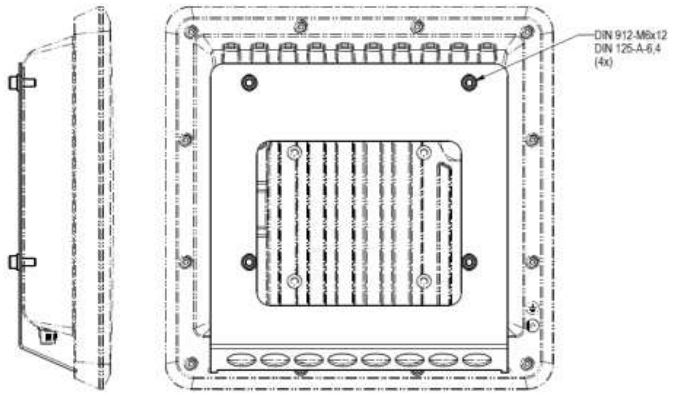
Für die Reader RRU 4560 (WLAN) und RRU 4570 (4G) werden passende Sicherheitsstufen angeboten, die den unerlaubten Zugriff unterbinden.

Beim RRU 4560 werden die Passwörter für die Einwahl bei erkannten SSID-Netzwerken genutzt. Dabei werden diese Passwörter nur zwischen ReaderStart und dem Reader übertragen, wenn eine SSH-Verbindung für den LAN-Port aktiviert ist.

Für den RRU 4570 mit eingebautem 4G Modul werden die Zugriffsrechte über PIN, APN, Username und Passwort verwaltet. Eine komplette Beschreibung ist an dieser Stelle nicht möglich. Bei Bedarf greifen Sie bitte auf das Reader Handbuch zu oder wenden sich an unseren Support.

5.2.7 Mechanische Sicherheitsmaßnahmen

Um den Zugang zu den Kathrein Readern zu erschweren, die im Außenbereich frei zugänglich sind, bietet Kathrein einen Vandalismus-Schutz an, der den Zugang oder Rückbau des Readers zumindest erschwert.



Dabei werden die Konnektoren gegen das Lösen gesichert und ebenso die Entnahme der SIM-Karte beim RRU 4570 Reader. Da der Vandalismus-Schutz direkt in die Gehäuserückwand des Readers einrastet, sind mechanische Angriffe nur mit äußerster Krafteinwirkung möglich. Ein Rückbau des Schutzes ist aufwändig und unterbindet schnelle Zugriffe auf den Reader.

5.3 Gesicherte Datenübertragung an Backend Systeme

Für effiziente AutoID-Systeme zur automatischen Objekt-Identifikation und Datenerfassung sowie IoT-Systeme (Internet of Things) bedarf es exzellenter Hardware und einer mindestens ebenso exzellenten AutoID- und IoT-Software. Dafür bieten wir neben der Hardware solch eine Softwarelösung an.

Die CrossTalk Software-Suite ist eines der fortschrittlichsten Software-Systeme zur AutoID- und IoT-Geräteverwaltung. Die Software lässt sich nahezu beliebig an neue Herausforderungen anpassen und in unterschiedlichsten Branchen einsetzen. Sie reduziert die laufenden Kosten und beschleunigt datenverarbeitende Prozesse.

Zusätzlich werden, mit der direkt auf dem UHF RFID Reader installierbaren CrossTalk Agent Edgeware, sichere Datenübertragungswege für Business Events an unterschiedliche Backend Systeme angeboten.

Dazu zählen:
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

Weitere Informationen zu CrossTalk und den Möglichkeiten zur Absicherung Ihrer IT-Landschaft finden Sie auf unserer Homepage unter:
https://www.kathrein-solutions.com/de/produkte/software

5.4 Anwendungsempfehlung für IT-Sicherheit bei Kathrein RFID Reader

In diesem Abschnitt werden Empfehlungen gelistet für Sicherheitsmaßnahmen bei verschiedenen Einsatzfällen. Jedoch sind die Anforderungen an Sicherheit sehr individuell.

Die Anwendungsempfehlung wurden in 3 Nutzungsarten kategorisiert:

- Innerhalb Gebäude: Annahme abgesperrter Räumlichkeiten, Zutritt nur für berechtigtes Personal, somit kein Bedarf zur Härtung
- Innerhalb Firmengelände: Annahme abgesperrter Außenbereich mit fremdem Personenverkehr möglich (z. B. Firmenparkplatz, Werkstor, o.Ä.)
- Öffentlich zugänglich: Annahme, dass die Reader sind für jedermann zugänglich (z. B. öffentliche Parkplätze, usw.)

Maßnahme	Innerhalb Gebäude	Innerhalb Firmengelände	Öffentlich zugänglich
SSH Passwort setzen	x	x	x
Nur sichere Verbindungen erlauben	x	x	x
Unterscheidung zwischen Admin / User	x	x	x
Neuen User einrichten		x	x
Neue User ablehnen		x	x
Konfigurations-Passwort setzen		x	x
Anzahl der Anmeldeversuche begrenzen		x	x
Zeitdauer zwischen Anmeldeversuche setzen		x	x
Begrenzung gleichzeitiger Sessions		x	x
Interne oder externe Ports deaktivieren			x
Mechanische Sicherheitsmaßnahmen		x	x

Bei Bedarf erhalten Sie weiteren Information und Unterstützung durch unsere Kathrein Training Academy:
https://www.kathrein-solutions.com/de/proserv/professional-service-ueberblick/training

Oder über die Support-Seite:
https://www.kathrein-solutions.com/de/support/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.

Kathrein Solutions GmbH, Kronstaudener Weg 1, 83071 Stephanskirchen, Germany, Phone +49 8036 90831 20, Fax +49 8036 90831 69