6.1. Communication

The communication tab groups together all the functions for establishing connections and configuring the interface cards. The various communication connections are grouped under 3 headers, COM for serial connections via the COM port (RS232/485/422), USB for connections up to version USB 2.0 and Ethernet for connections via TCP/IP.

When the connection is established, the program interrogates the information about the installed I/O cards. The information can be viewed and changed via the I/O card configuration.
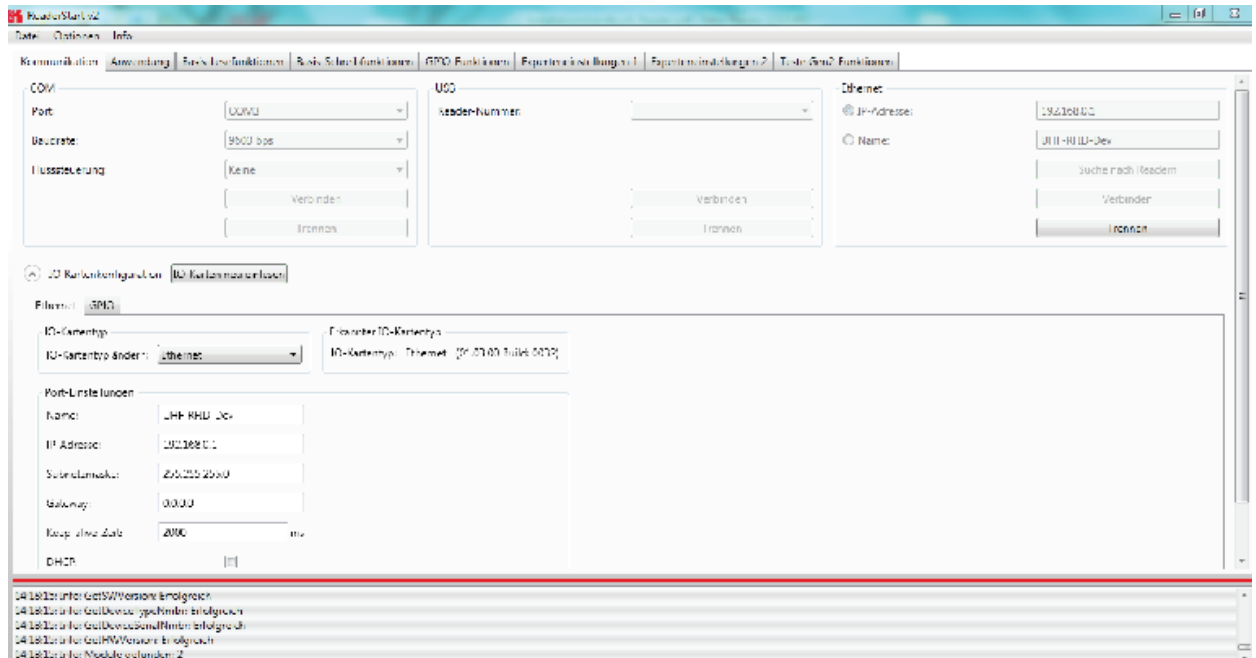
Figure: Tab for the Communication by Ethernet I/O card

6.1.1. COM header

The serial interface is used for communication with the reader via RS232, RS485 and RS422.

The RS485/RS422 interface card supports the standard data rates of the serial interface on a PC. A level converter is also required for communication to convert the RS232-compliant signal from the PC into a differential RS485/RS422 signal.

A serial COM port on the PC can be opened in this group box. For this purpose the correct serial interface must be selected in the *Port* drop-down list box. Only the ports available on the PC are displayed in this list box. It is not checked whether this port is already in use by other applications.

In the menu below the desired Baud rate must still be set, and if used, the flow control setting. The COM port is opened by clicking on the *Connect* button, which blocks it for other applications. If this port is already being used by another application, a corresponding error message is output. If the port is free, the reader can be operated using this port.

Pressing the *Disconnect* button breaks the connection and releases the interface again.

6.1.2.   USB header

If a RRU4 is connected to the PC via USB, the unit is installed in the system as a USB HID-compliant device. Correct logging in can be seen in the program if a reader number appears in the drop-down menu. This number is unique for each reader. If several readers are connected to the PC, the related reader can be selected on this menu. Clicking on Open now establishes the connection between the reader and PC.

6.1.3.   Ethernet header

The Ethernet connection can be achieved by linking the reader into an existing network, or by a direct connection between the reader and a control computer. For direct connection of the reader to the PC, a cross-link cable is required, unless the LAN interface on the PC supports "auto-mdi-x". Alternatively two standard patch cables and a switch can be used.

## 6.1.4.   Reader to factory default via TCP/IP- broadcast cmd

To reset the reader to factory default, the ReaderStart SW will send out a TCP/IP- broadcast cmd. This is only possible 20 seconds after power rebooting. For this select at the folder "Communication", press "Search for Reader".
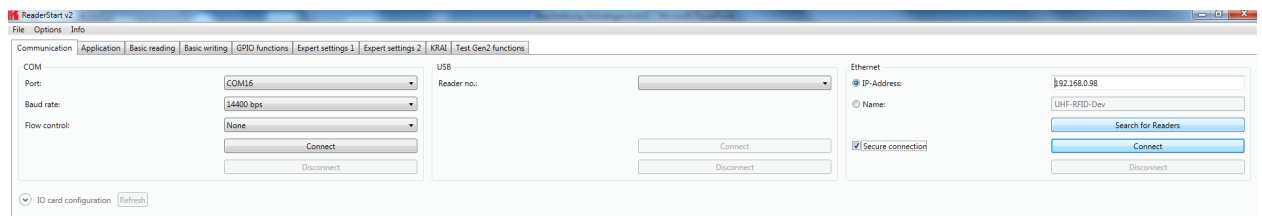
All reader in the network will be listed. Select the correct reader and press right mouse button.
The following question „Are you sure…." will be answered with „YES".
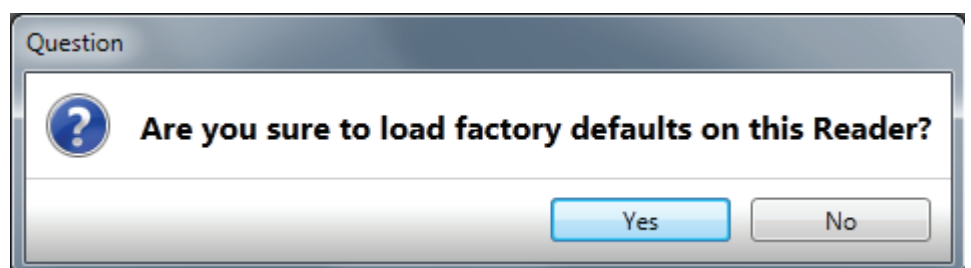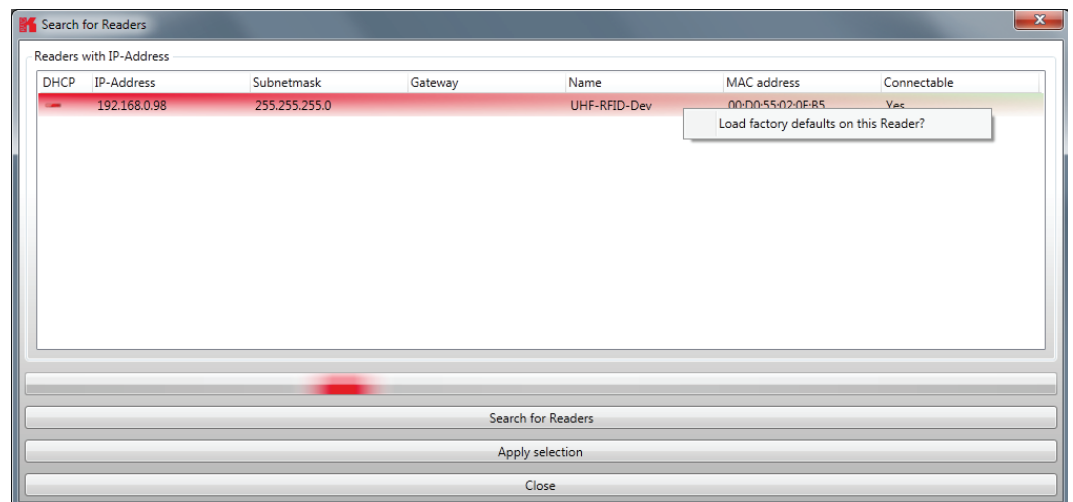
The user will be informed with the status messages about the progress of the reset process. The final message will be „Reader with IP Address 192.168.0.1 …. (???????????) .
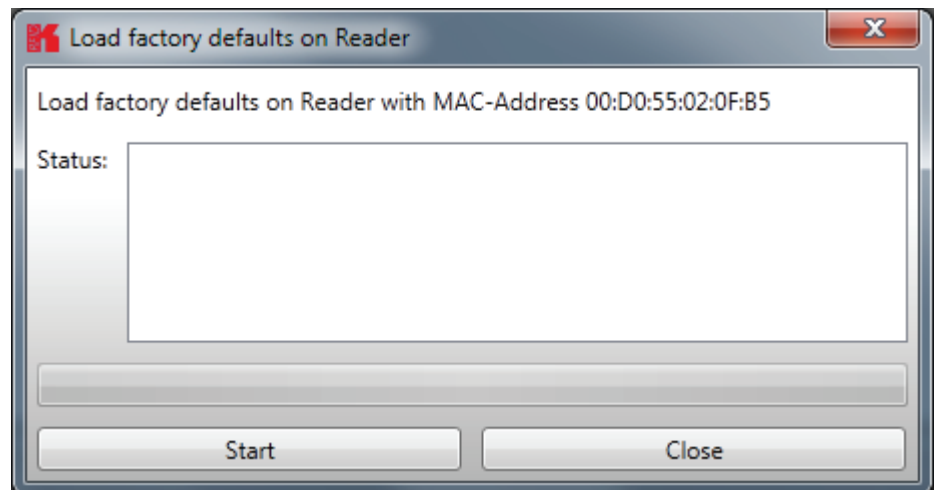
From reader firmware 2.04, the reader in the ex-works condition has the IP address 192.168.0.1 with the network mask 255.255.255.0. Reader versions earlier than this are configured for DHCP.

To integrate the reader into a corporate network, please contact your administrator who will be able to allocate you a spare IP address and assign the correct network mask. Alternatively the reader can also be configured to obtain an IP address automatically. For this service, referred to as DHCP, an appropriate DHCP server must be operating in the network. You can obtain more details about this from your network administrator.

Note

The IP addresses of the control computer and the reader must be in the same IP range, but they must not be the same. The network mask on the other hand must be identical.

In order to establish the connection to the reader, the program offers two options. On the one hand, it is possible to communicate directly with the reader by entering the IP address, on the other hand it is also possible to establish a connection using the reader's host name.
For the connection using a host name, there must be a correspondingly configured DHCP server and a DNS in the network. After power up, the reader makes a DHCP request and logs on to the DHCP server. This assigns the reader an IP address and reports the network name and IP address to the DNS server. If now the connection has been established, the IP address of the reader is determined by an enquiry on the DNS server.
The establishment of the connection is achieved if the establishment of the connection is selected under the Ethernet header, meaning the selection of the IP address or name. For this, the correct IP address or the host name of the reader must be entered in the corresponding field. Pressing the *Connect* button then opens the data channel to the reader.
If you wish to establish a connection via an IP address, the *IP address* field must be highlighted and this address entered in it. The connection is established by clicking on the *Connect* button.

6.1.5.   I/O card configuration

The communication interface settings can be changed using the *IO card configuration*. All available I/O cards are displayed here in the form of tabs. Clicking on the respective tab opens the associated card and displays all respective configuration parameters, together with the card type that was detected.

Under the *IO card type* header there is a drop-down menu, in which the card type can be set to *Auto detect, Card not used* or to the actual card type. Automatic detection restores the interface to the default settings. What these settings are is described in the following sections in relation to the interfaces. If the card type is set to not used, this interface can no longer to used.

All card-specific configuration parameters are displayed on the card sheet when the recognised card type is set. These parameters are described in the following sections for the respective card. The settings are saved to the reader by pressing the *Save changes* button.

Note

The new parameters, provided nothing to the contrary is specified for the specific card, become valid only when the reader has been restarted. If incorrect parameters are loaded, the reader can no longer be accessed!

6.1.5.1.   RS232

The serial interface supports communication to the EIA232 standard and, depending on the expansion stage, has five outputs for activation of LEDs. The configuration parameters are split between the *Port settings* and *Output* headers.

Figure: Configuration of the RS232 card

The communication parameters are grouped as follows:

1   Baud rate – the speed of the connection. All popular serial data rates up to 230,400 bps are supported

2   Data bits – the number of data bits transmitted per byte. The card supports 5 – 8 data bits.

3   Parity – a bit for security of the data transmission

If *None* is selected, this bit is not transmitted. For all other settings this bit is transmitted. The even or odd parity checks whether the number of bits including the parity bit is even or odd. Based on this information the recipient can determine whether a bit has been switched. Mark and space specify whether the parity bit should be transmitted with a fixed 1 or 0. In this case no data transmission security is achieved.

3   Stop bits – specifies whether the transmission of a byte should be terminated with one or two stop bits.

4   Flow control – for readers with the appropriate interface, this allows specification of whether the synchronisation between the PC and reader should be by software *None* or by hardware wires (*Hardware*).

Note

Note that for a point-to-point connection, the setting of this parameter must be the same for both participants, otherwise no connection can be established. RS232 readers, whose serial interface is performed via 4-pin M12 connector, do not support hardware flow control.

*The RS232 card has a further five outputs, which can be used for activation of LEDs. The configuration parameters for these outputs can be found under the **Output** header.*

Note

Not all reader hardware issues support this functionality. Please check the reader data sheet for information.

If the LEDs are present (only for ARU), the LED channels can be assigned various functionalities under this heading. Further parameters can be activated, depending on the function selected. The following functions are available:

1   Off – the selected LED is deactivated

2   On – the selected LED is always on

3   1Hz frequency – the selected LED flashes at a frequency of 1 Hertz

4   2Hz frequency – the selected LED flashes at a frequency of 2 Hertz

5   4Hz frequency – the selected LED flashes at a frequency of 4 Hertz

6   8Hz frequency – the selected LED flashes at a frequency of 8 Hertz

7   RF on – the LED lights up for *Turn-off time* milliseconds as soon as the radio frequency is present at the antenna *First antenna* to *Last antenna*.

8   Antenna error – the LED lights up for *Turn-off time* milliseconds as soon as an antenna error occurs at antenna *First antenna* to *Last antenna*.

9   Tag found – the LED lights up for *Turn-off time* milliseconds as soon as a tag is found at the antenna *First antenna* to *Last antenna*.

10   RF on – the LED lights up for *Turn-off time* milliseconds as soon as an operation on a tag was successful at the antenna *First antenna* to *Last antenna*.

11   Protocol access – the LED can be switched on and off directly via the protocol.

Default configuration:

Baud rate:	9600
Data bits:	8
Parity:	None
Stop bits:	1
Flow control:	None
LEDs:	Off

6.1.5.2.   GPIO

The GPIO card allows the reader to interact with its environment. In this tab, the inputs and outputs can be configured for the respective application under the headings *Input* and *Output*.

Note

Refer to the electrical characteristics of the inputs and outputs in the data sheet; if these characteristics are exceeded the card and the reader may be damaged.

Figure: Configuration of the GPIO card

Each input channel has two configuration parameters available. The *Invert logical input* option negates the electrical input signal and uses this status for processing in the reader. If the check is not set, the signal is used unchanged. Depending on the sensor being used (mechanical or electrical switch), a debounce time in milliseconds can be assigned to each channel.

The outputs from the card can be assigned various functions. Further parameters can be activated, depending on the function selected. The following functions are available:

1   Off – the selected output is deactivated

2   On – the selected output is always on

3   1Hz frequency – the selected output flashes at a frequency of 1 Hertz

4   2Hz frequency – the selected output flashes at a frequency of 2 Hertz

5   4Hz frequency – the selected output flashes at a frequency of 4 Hertz

6   8Hz frequency – the selected output flashes at a frequency of 8 Hertz

7   RF on – the output is active for *Turn-off time* milliseconds as soon as the radio frequency is present at the antenna *First antenna* to *Last antenna*.

8   Antenna error – the output is active for *Turn-off time* milliseconds as soon as an antenna error occurs at antenna *First antenna* to *Last antenna*.

9   Tag found – the output is active for *Turn-off time* milliseconds as soon as a tag is found at the antenna *First antenna* to *Last antenna*.

10   RF on – the output is active for *Turn-off time* milliseconds as soon as an operation on a tag was successful at the antenna *First antenna* to *Last antenna*.

11   Protocol access – the output is released and can be activated with all KBRP commands for GPIO.

Note

If the output is not set to protocol access, it cannot be accessed when processing action lists. See the **GPIO functions** *section for more details on action lists.*

Once all the settings have been performed, the changes are loaded to the reader by pressing the **Save changes** *button, and take effect immediately.*

Default configuration

No default configuration is provided for this card.

Note

If this card setting is changed from **Auto detect** *or* **Card not used** *to* **GPIO***, the reader must be restarted so that the card is correctly initialised.*

6.1.5.3.   RS485

In order to establish a serial symmetrical connection to the EIA-485 standard, a RS485/RS422 card is required for the reader. In addition to the parameters Baud rate, parity and stop bits, which are identical to RS232, the tab for configuration of this interface has certain other specific settings under the *Port settings* header.

The LED control is only possible with ARU reader.

Figure: Configuration of the RS485 card

The parameters have the following meaning:

1   Pull-up – when this parameter is set, the differential wires are pulled up with 120 Ohm to a fixed reference potential (+5 V and GND). This procedure is recommended when the signal ratios between the communications participants are critical.

2   Load resistor – terminates the differential wires against each other with 120 Ohm. This variant is required when the reader forms the end point of the network.

3   RS422 – activates the RS422 mode of the interface card. This changes over the connection from 2-wire for RS485 to 4-wire for RS422. This achieves a full duplex connection with differential RX and TX wires.

Note

Note that for a point-to-point connection or for connection of the participants in a network, the setting of this parameter must be the same for both participants, otherwise no connection can be established.

Default configuration:

Baud rate:	115200
Data bits:	8
Parity:	None
Stop bits:	1
Load resistor:	activated
RS422:	deactivated

6.1.5.4.   Ethernet

The parameters *Name*, *IP-Address*, *Subnetmask*, *Keep-alive time* and *DHCP* can be set for the Ethernet card on the reader.

The settings for the LED display are visible only if ARU reader.

Figure: Configuration parameters for the Ethernet module

The parameters have the following functions:

1 Name – Here the host name of the reader which is logged on to the DNS server is stated. The reader can be addressed by this name as an alternative to the IP address.

2 DHCP – activates the automatic issuing of an IP address by a DHCP server; if the network has a configured DNS server, the host name of the reader can also be used.

3 IP address – for manual issuing of the address. This parameter can be used only if the DHCP is deactivated

4 Subnet mask – for manual issuing of a network mask. This parameter can be used only if the DHCP is deactivated.

5 Keep-alive time – this time specifies the intervals of time at which the reader sends a data packet to check whether the receiver is still available. If the connection to the reader is broken, the reader shuts down the connection. If this parameter is deactivated (0 ms), the socket is shut down only when the reader is restarted.

Note

If no keep-alive time is set it may happen that the reader cannot take up any further connections because the existing connections have not been properly shut down (e.g. following a breakage in the wire). In this case the reader has to be restarted. It is recommended that the keep-alive time is used to check the connection between the reader and PC.

The data are saved in the reader by pressing the Save changes button. The data are however not loaded to the working configuration until the reader is restarted.

Note

If the interface is wrongly configured, no connection to the reader can be established. Please make a note of the data settings.

Default configuration:

Host name: UHF-RFID-Dev

IP address: 192.168.0.1

Subnet mask: 255.255.255.0

Keep-alive time: 2000ms

DHCP: deactivated

The IP addresses of the Linux Reader is now set via Reader Start Software.

6.2.   Application

The *Application* tab enables quick and easy configuration of the Kathrein RFID Reader for a selected application. The available applications are represented visually in the upper area of the tab by labelled pictograms. Under the *Settings* header, the number of tags expected, the antennas to be used, the parameter set in which the configuration should be saved and the values for *max. read frequency* and *max. read reliability* options are stated.
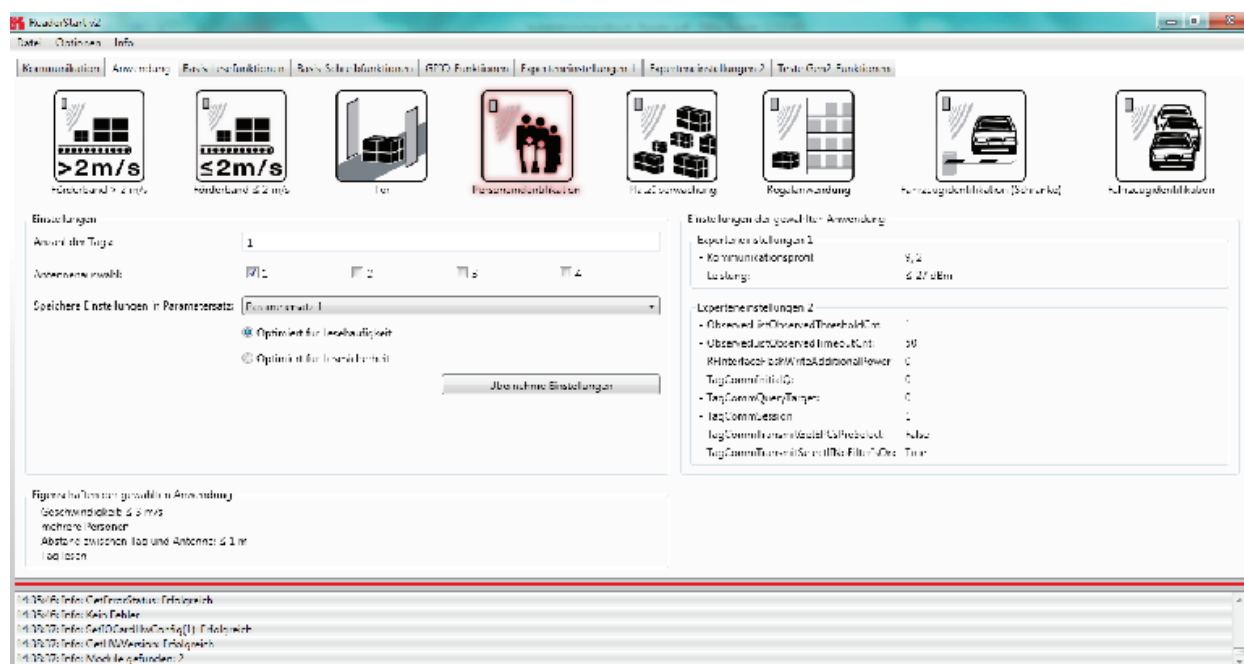

Figure: Application tab

When the button for the desired application is clicked, it glows green continuously. In addition the designation, the properties and the settings of the selected application are displayed in the respective fields.

The following applications are available for selection in version 2.00 of the *ReaderStart v2*:

- Conveyor belt > 2 m/s
  - o   Application for detecting individual tags in the antenna field on a conveyor belt moving at more than 2 m/s
  - o   the distance between the tags and the antenna is only a few centimetres
- Conveyor belt ≤ 2 m/s
  - o   Application for detecting and describing individual tags in the antenna field on a conveyor belt moving at less than or equal to 2 m/s
  - o   the distance between the tags and the antenna is only a few centimetres
- Gate
  - o   Application for detecting multiple tags in the antenna field as they pass through a gate
- Slot monitoring
  - o   Application for detecting and describing multiple tags in the antenna field, which are not moving
  - o   the distance between the tags and the antenna should be less than 1 m
- Vehicle identification
  - o   Application for detecting and describing multiple tags in the antenna field, which are moving at more than 14 m/s
  - o   the distance between the tags and the antenna should be less than a few metres

- Vehicle identification (barrier)

  o   Application for detecting and describing individual tags in the antenna field, which are not moving

  o   the distance between the tags and the antenna should be less than a few metres

- Shelving application

  o   Application for detecting and describing very many tags in the antenna field, which are not moving

  o   the distance between the tags and the antenna should be less than 1 m

- Personal identification

  o   Application for detecting multiple tags in the antenna field, which are moving at not more than 3 m/s

  o   the distance between the tags and the antenna should be less than 1 m

If there are more applications than fit on the screen, the buttons alongside the applications are activated to allow scrolling.

When the *max. read frequency* is set, for every detection (inventory) all tags are reset in order to read them afresh. Under some circumstances the time allowed for detecting the tags may be insufficient, so that some transponders are not detected. The frequency for detecting the tags should then be increased.

When the *max. read reliability* is set, tags that have already been read are not reset at every detection (inventory), provided they are still being supplied with power. This means that only those tags which have not yet been registered are detected. The confidence that all tags are read is thus increased.

Clicking on the *Apply settings* button saves the settings that were made, as well as the settings for the selected application, in the selected parameter set. This is done by first resetting them to the factory settings and thus overwriting the previous configuration. This must be acknowledged. Success is indicated by a the *Apply settings* button glowing briefly, and by display of a success message in the status window. If the process fails, the button glows briefly orange for a warning or briefly red for an error (and if the failure was due to an entry being omitted, in addition the field that is lacking the entry glows red), and by display of a warning description or error description in the status window.

If the settings have been loaded successfully, a switch can now be made to the *Basic reading* tab and the read process can be started.

Note

When there are more than one hundred tags in the field at the same time, the application can be optimized for Frequency of reading speed or reliability of reading.

When optimized for frequency of reading, the number of readings is maximized. In this case the same tag can be read several times, because all tags will be reset in the inventory, so that they will respond again. Because of reading the same tag multiple times in a scenario of moving tags it could happen that not all the tags crossing the antenna field can be read.

The frequency of detection of the same tag is increased.
Optimization for reliability of reading can be used to read as many different tags as possible.

When this setting is chosen, tags already detected are not read again in the next inventory as long as the tag is powered.

So only tags in the field that are not detected yet are read. The probability to read all the tags is increased.

6.3.   Basic read functions

This index card is divided into two columns, the first column contains a table with information about the read tags, and in the second column you can find the controls, which control the reading process.
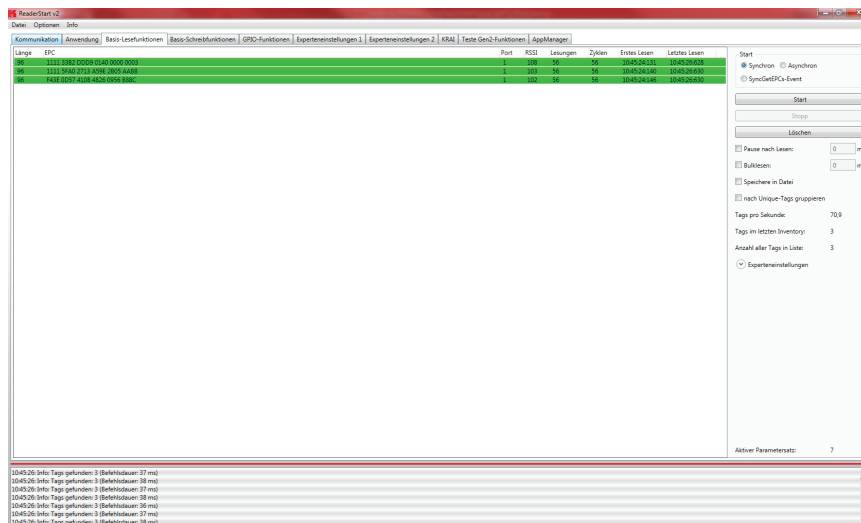

Figure: Basic read functions tab

The table next to the Electronic Product Code (EPC), you can find the following information:
1   Length - indicates the length in bits of the EPC, valid lengths 0-496 bit
2   EPC - EPC of the tag in hexadecimal representation
3   Antenna - tag was read over this antenna post, valid values 1-4
4   RSSI - is the unitless (shown as having no units) signal strength of the tag response, valid values 0-255
5   Readings - shows how many times this tag has been read successfully
6   Cycles - indicates how often an inventory was started
7   Last reading - is the timestamp of the last reading of the Tag
8   First reading - is the timestamp of the first reading of the Tag

The appearance and disappearance of the Tag is shown in colour in the field for better visual effect.
When a tag appears in the field, the row is represented by the green tag information, when it disappears the row is red.

The control of the reading process takes place in the second column of the index card. A distinction is made between two different modes. These can be selected by selecting „synchronous" and „asynchronous". The description of these two modes is done on the following pages.

The second column can be sorted by the read result (unique) tags. This is especially useful in multi-antenna applications. For example, with a gate application with 4 antennas read per pallet with 100 tags, then the maximum number of reading results will be 400. Since not all tags are read by all antennas, the reading results in general, will level off at about 250. In order to detect how many different tags have been read, the selection „sort by unique tags" can be made.

The row "number of unique tags" specifies how many different tags were read.

When the Tag count is very high (> 200) the detection of the tags can be speeded up, by commanding the reader may change to new "select command" (see EPC global standard (E)).

This can be tested by selecting "Expert Parameters" directly in read mode. If the read operation box is ticked with "Transmit Select If No Filter Is On", a "Select" is sent in each "Inventory". This means that all the tags that are defined at this time in the field will be reset. It can also happen that tags that have been read are sometimes reset and re-recorded again. In order to capture only new tags, a renewed "Select" can be prevented. This tick box is cleared on "Transmit Select If No Filter Is On" and thus all tags defined only once read. This selection result is that no time is lost due to a re-read. Please note, however, that tags in which the read operation was interrupted, they cannot be retrieved! Thus, it may be that not 100% of the tags are read. Therefore, this parameter should be used with care in order to achieve top results.
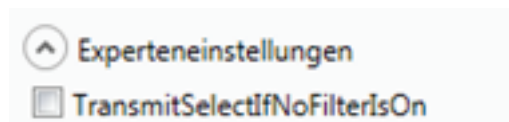
6.3.1. Display Tag phase and frequency

To display Tag phase and frequency during basic reading, the option "Show frequency and tag phase"
Should be selected in options menu.
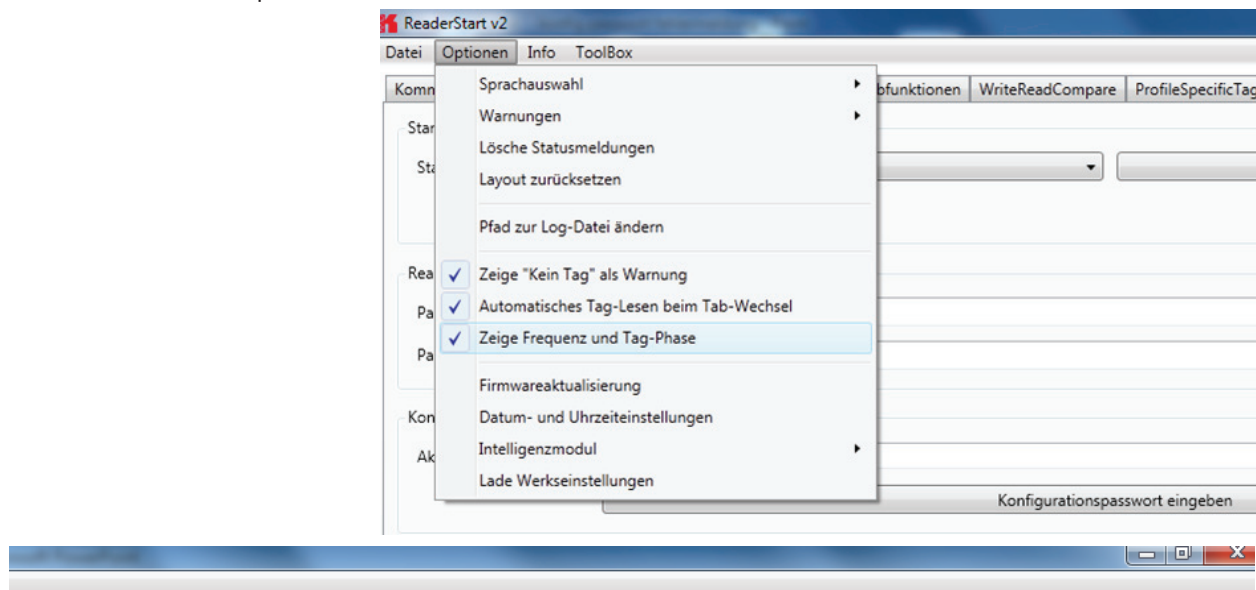
With the change of the tag phase, a movement of the transponder can be detected.

The frequency and the tag phase will be stored with all read results in CSV-format, if the button " Store to file" is selected

6.3.2.   Synchronous mode

This mode is intended for applications when the requirements for timing are not so demanding. This mode allows the facility to switch the carrier off during the idle times, thus saving power.

The inventory of the tags (the read process) is performed across all the antennas that are configured. Once all tags in the field have been read on the last antenna, data are sent to the PC. The inventory of the tags is then automatically retriggered by the PC.

The *Pause after reading* option specifies how many milliseconds the pause between two inventories should be. During this waiting time the carrier can be deactivated. See section ((B)) „configurational manual reader" for more information about switching off the carrier.

In order to keep the time between inventories as short as possible in synchronous mode, data transmission between the inventories can be dispensed with. That means that the reader saves all the tags that it finds in the field in its internal RAM. After a configurable time this results list is sent to the PC. This time is given in milliseconds by the *Bulk read* parameter.

The current reading performance is displayed under the item *Tags per second*.

Note
The read rate is influenced by many parameters; these include in addition to the selected broadcasting profile with the respective data rates also application-specific data such as how many tags the reader should expect in the field. You can optimise these parameters using the expert settings 1 and 2. There is more about this in the following sections. If you are unsure whether the settings you have chosen are optimum for your application, please contact KATHREIN Support.
If the tags that have been read are to be saved to a file, this can be done by activating the **Save to file** *option. The EPC, the length of the EPC, the antenna on which the tag was read, the RSSI valuetogether with the time stamp when the tag was read are saved.*
The data are then saved in a csv file in the Program directory. In the File menu, you can "change to the log file File / Options / Path" under the location of the CSV file. The file can opened or deleted in the context menu for this item.

6.3.3.   Asynchronous mode

This mode is intended for applications for which maximum performance is required.

The reader starts the inventory as quickly as possible, and at the end of an inventory it does not deliver every tag that was read to the PC, but only those that had newly appeared in the field or newly left it. This allows the time required for communication with the higher level to be minimised.

The timing of when a tag was reliably read in the field and when the tag no longer appears in the field can be defined more precisely using parameters. Details of these *ObservedThresholdCnt* and *ObservedTimeoutCnt* parameters can be found in section ((B)) „configurational manual reader".

Note
The read rate is influenced by many parameters; these include in addition to the selected broadcasting profile with the respective data rates also application-specific data such as how many tags the reader should expect in the field. You can optimise these parameters using the expert settings 1 and 2. There is more about this in the following sections. If you are unsure whether the settings you have chosen are optimum for your application, please contact KATHREIN Support.
If the tags that have been read are to be saved to a file, this can be done by activating the **Save to file** *option. The data are then saved in a csv file in the Program directory. The file can opened or deleted in the context menu for this item.*
Once the mode and the parameters have been selected, the read process can be started. Both modes are stopped by pressing the **Stop** *button. The* **Delete** *button removes all tag entries from the table.*

6.4.   Basic writing function

The *Basic writing* tab allows input of basic descriptions of tags. A fundamental distinction is maintained between synchronous writing - *write on command* - and asynchronous writing - *write on arrival*.
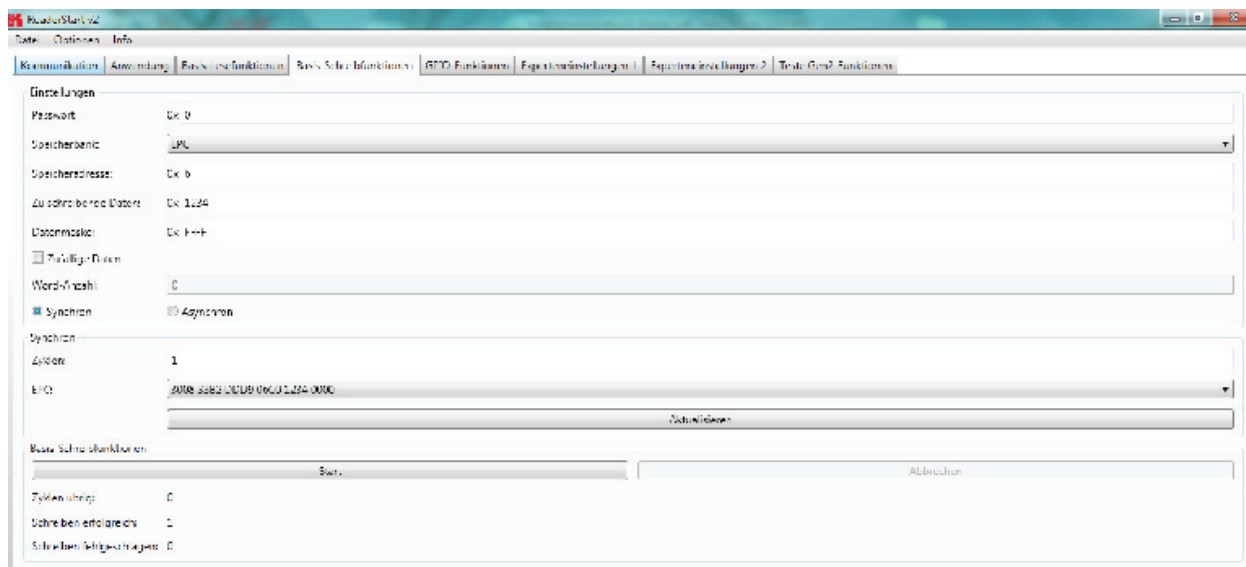

Figure: Basic write function tab

6.4.1.   Synchronous writing

In this type of writing the data can only ever be written selectively to one EPC. This is selected in the *EPC* ComboBox. Clicking on the *Refresh* button detects once again all tags in the antenna field and adds them to the ComboBox.

When all necessary data such as password, memory bank and memory address have been input a decision can be made whether to specify the data to be written or to generate them at random. If specified data should be written, optionally a data mask can be specified. When using random data, the number of them should be stated in words (16-bit).

Note

*Right-clicking on the **Data to write** field opens a context menu, which allows the selected EPC to be copied into this field.*

Note

*Right-clicking on the **Data mask** field allows this to be filled optionally with **0** or **F** according to the number of the data entered to be written.*

Clicking on *Start* starts the performance of the previously specified number of write attempts. The error-free completion of all write attempts is once again indicated by the button glowing green and by a message in the status window. If any necessary data are lacking, the button briefly glows red and the field lacking the data glows red somewhat longer. The associated error message appears in the status window.

The *Writing successful* and *Writing failed* fields indicate how often the write attempt succeeded or failed Hovering the mouse over the number of failed write attempts (provided indeed any failures did occur), calls up a window with detailed information.

## 6.4.2.	Asynchronous writing

In this type of writing the data is written to every EPC that occurs in the antenna field. When all necessary data (password, memory bank, memory address, data to be described - the input of the data mask is optional) have been input, clicking on Start starts the asynchronous write process. Successful and failed write attempts are shown in the respective fields. Hovering the mouse over the number of failed write attempts (provided indeed any failures did occur), calls up a window with detailed information.

Note

*Right-clicking on the **Data mask** field allows this to be filled optionally with **0** or **F** according to the number of the data entered to be written.*

6.5.   GPIO functions

Readers with GPIO functionality offer the facility to set up small controls which trigger the reader for instance by a light barrier or which trigger an action at the outputs of the reader by reading specific tags. Such an action might be switching an output to control the flow of goods.

The *GPIO function* tab allows the user of the program the facility to load or switch inputs and outputs manually. For more complex procedures, action lists can be created here, which execute a sequence of commands on the reader. This list can then be linked to various inputs.

This configuration sheet is divided into 5 different headers. In order to perform settings on a card, firstly the card number must be selected in the GPIO card drop-down menu. This shows only cards of this type.
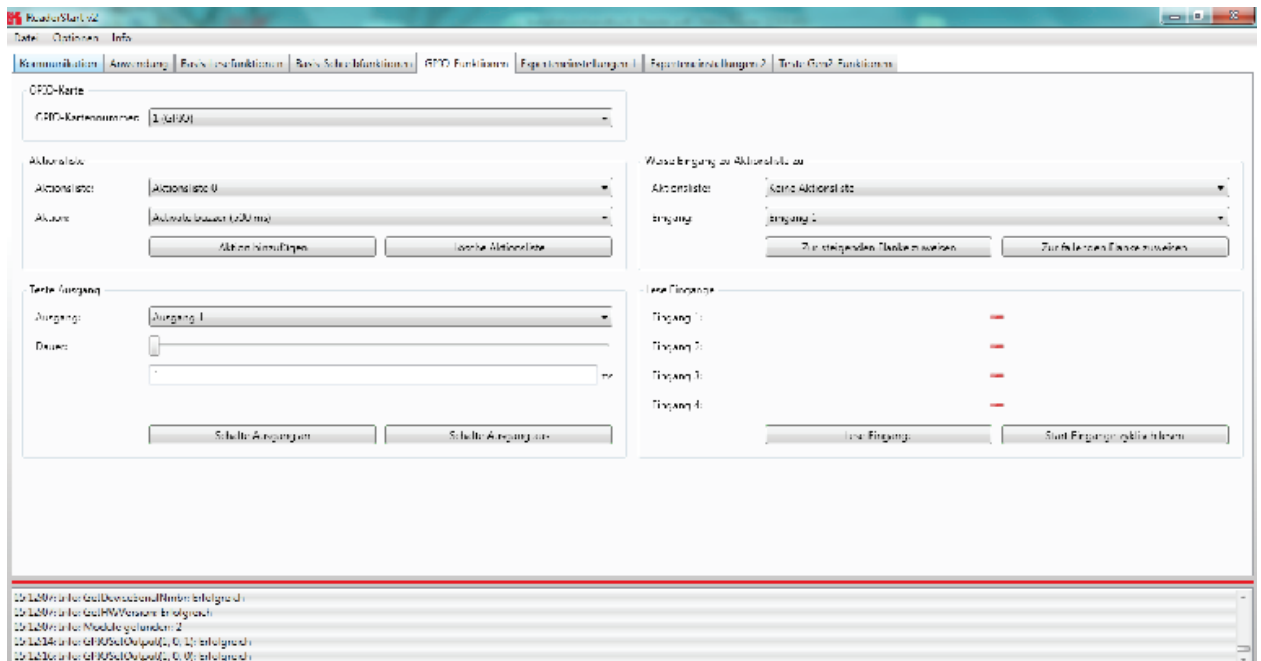

Figure: GPIO functions tab

The *Test output* header can be used in order to selectively connect an output manually. In order to enable this access, the respective output of this card must previously have been connected to protocol access (see I/O card configuration). The output in the drop-down menu is now selected in the header, and time is defined using the *Duration* parameter, until the output automatically returns to its idle mode. The connections can now be made using the *Set output on* and *Set output off* buttons.

The inputs to the reader can be interrogated under the *Read inputs* header. Whether an input is set or not is shown in the signal fields. A one-off read process can be triggered by pressing the *Read inputs* button. If this interrogation should be performed automatically, this process can be started by pressing the *Read inputs cyclic start* button.

To automate the processes, command sequences in the form of action lists can be stored on the reader. These are triggered by a change of flank at the selected input on the respective GPIO card.

The action lists consist of a sequence of individual actions, which can be loaded in the form of an ML file in the context menu of the *Action* item under the *Action list*. This file can be created or edited manually, using a text editor. The syntax can be seen from the example. The individual actions can be selected from the functions described in section 7 "Reader configuration".

The file is saved in the folder "..\My files\Kathren Sachsen GmbH\ReaderStart v2\" and can be edited using a text editor. In order to use the newly added actions in the program, the file must be reloaded into the context menu.

The action list must be selected from the drop-down list. The desired actions are now selected individually from the action list and added to the action list in the sequence in which they are to be executed. Pressing the *Clear action list* button clears down the selected list.

Note

When the action list has been created, it is assigned under the *Assign input to action list* header to an input and a selected flank. If it is desired to assign the list to both flanks, the assignment must be made once for the positive flank and once for the negative flank.

The assignment can be cancelled again by a restart/reset of the reader or by assignment of the *No action list* item.

The action lists that are created are stored only in the RAM of the reader. On restarting the reader these lists are deleted again.

For continuous operation of the reader, the commands for the digital inputs and outputs can be integrated into a software application. This application software can be run on an external PC or on the industrial PC ETL and ELC reader.

6.5.1.   Example of GPIO function

In the same menu, the basic functions of the GPIO card can be set.

First, the IO-card configuration is opened and the GPIO card set automatic detection on GPIO:

Here the global settings for the GPIOs are set.

Invertieren: when logically high level and high-level physica must be inverted

Debounce time   depending on the switching element at the entrance

Output ->TAG found „antenna mistake" ....

All these settings are global and apply to all configurations.

6.5.1.3.   Setting up a separate list ACTION

The Reader's launch SW sets in the folder „My Documents" or in the user's „Documents \ Kathrein Sachsen GmbH" to a directory where the system variables are stored. Here are inter alia the antenna list and the Action List for the inputs.

The approximately 150 reader commands with corresponding variance of the parameters do not allow for uniform list. A selection of all options is extensive. Therefore it is recommended to only list required in the application instructions.

To the Action List (ActionlistAction.xml) can use an XML editor to edit.

```xml
<?xml version='1.0' encoding='UTF-8'?>
<ActionlistActions>
  <!--Activate buzzer for 500 ms, CommandID: 0x0045, Parameter: 0x01F4-->
  <Action>
    <Description>Activate buzzer (500 ms)</Description>
        <CommandID>0045</CommandID>
    <!--LSB first-->
    <Parameter>F4</Parameter>
    <Parameter>01</Parameter>
  </Action>
  <!--Get EPCs, CommandID: 0x0101-->
  <Action>
    <Description>Get EPCs</Description>
        <CommandID>0101</CommandID>
    <!--LSB first-->
  </Action>
</ActionlistActions>
```

In this example, the commands „Buzzer" and were „Get EPCs" registered.
The CommandIds can be found in the Reader Protocol ((A)).

After editing, the action list it in the reader startup directory under
„My Documents" folder. The next time the reader start this software is active.

6.5.1.4.   Selecting commands from the ACTION list

The commands of the Action List are now under the menu item „GPIO functions / Action List" available at „action" all available commands are listed.

In the example, „Get EPCs"
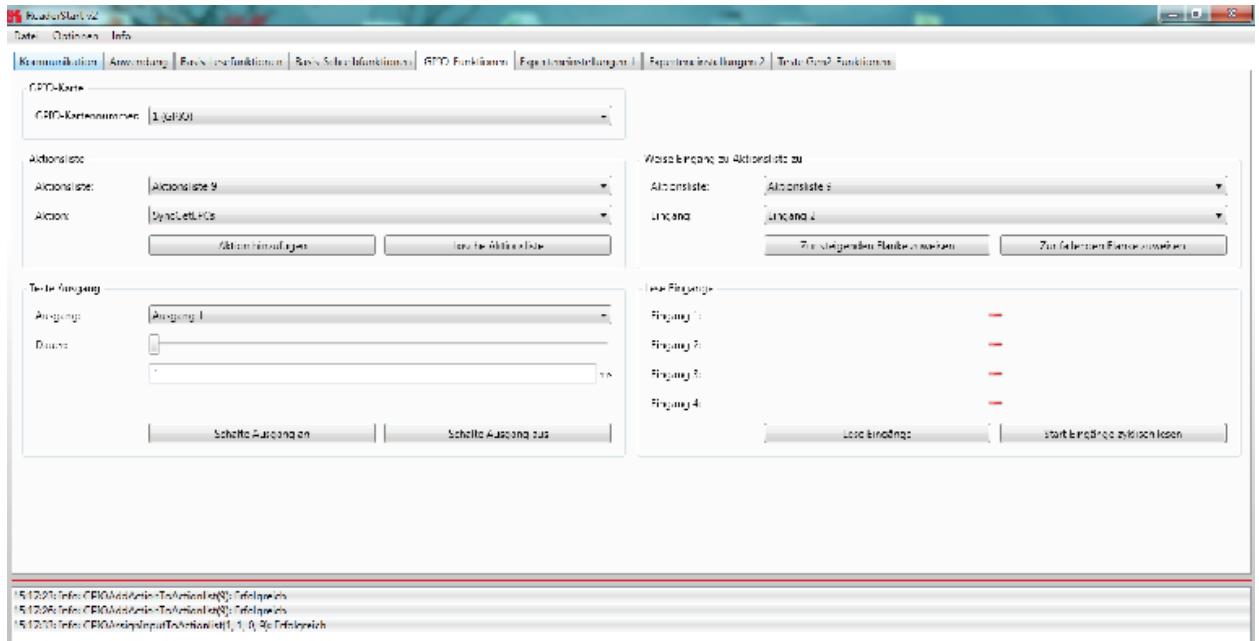
„Add Action" with the commands are written in chronological list of the selected action. Each command will be added in the system banner with the message
„GPIOAddActionToActionlist (9): Successfully" acknowledged.

6.5.1.5. Assigning the ACTION list to the respective inputs

Have been added, all of the commands to be executed, is in the menu box „way to input action list to" bring about the link to the inputs.

The action list (in this case 9) and the input (in this case 1) can be selected. Similarly, to determine whether to respond to the rising or falling edge is.
By clicking the „Apply" on the action list is associated with the input.

The Banner system will show „GPIOAssignInputToActionlist (1,1,5,9): Successfully" acknowledged.

Each rising edge is the command „Get EPCs" to send to the reader!

Note

With the Action List can only be basic logic operations. The inputs are linked with a defined EPC value is not possible.

6.6. Expert settings

The *ReaderStart v2* software is a powerful tool for configuration of the reader. It allows the reader to be customised to any application. The expert settings 1 and 2 allow the reader's RF interface and communications profile to be optimised to the tag so that the reader is optimally customised to the application.

6.6.1. Expert settings 1

There are eight parameter sets available for saving the configuration of the reader. All settings for the transmission power, the antenna multiplex configuration, the RF settings and the air interface parameters can be saved in these memory slots. Other parameters can be changed in *Expert settings 2*. See section ((B)) „configurational manual reader" for more information about the individual parameters.
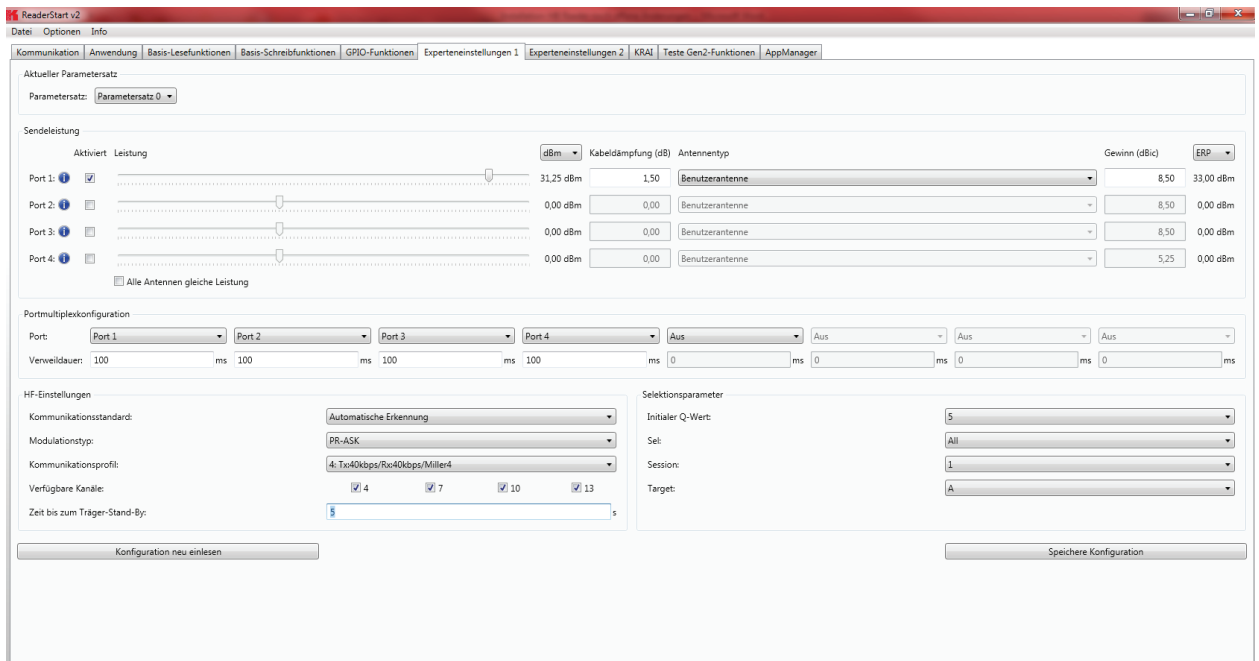

Figure: Expert settings 1 tab

Pre-setting can be selected under the *Current parameter set* header. This is done by selecting a parameter set in the drop-down menu. This parameter is now active and loaded, and the headers are updated. When all the desired changes have been made, they can be saved. The changes to the settings can be discarded by pressing the *Reload configuration* button. The parameter set can be reloaded by pressing the *Load factory defaults*.

Under the *Transmission power* header, the parameters of the transmission path can be entered; these include the transmission power, transmission channel (only ETSI) and spectrum. The applicable standards in the related approval region are to be observed when setting the transmission power.

Note

To operate the reader in accordance with the related national standards, the antenna gain and the cable attenuation must be taken into account in the transmission power setting. In no circumstances is it allowed to exceed the permitted transmission power. Failure to observe this instruction can result in non-compliant operation of the reader rendering void the unit's type approval.

6.6.1.1.   Transmission power

The radiated power is limited in Europe in accordance with ETSI 302208 to 2 W ERP. In the FCC / IC region, max. 1 W connected RF power applies with an antenna gain of 6 dBi. If the antenna gain is greater than 6 dBi, the RF power must be reduced accordingly. While the European standard refers to a half-wave dipole, FCC part 15 / RSS 210 refers to an isotropic radiator.

To set the transmission power, the length-dependent cable attenuation and the antenna gain must be included in the calculation of the transmission power. An example for the calculation of the transmission power for Europe and FCC / IC is given in the following.

The following applies to the European approval region:

$$P_{Reader} = P_{ERP} + D_{Kabel} - G_{HW}$$

P_{Reader}...Transmission power of the reader in dBm

P_{ERP}......Transmission power based on a half-wave dipole in dBm

D_{Kabel}.....Cable attenuation in dB

G_{HW}......Antenna gain based on a half-wave dipole

The cable attenuation is the length-dependent attenuation of the cable at the related frequency:

$$D_{Kabel} = l * D_{dB/m}$$

D_{Kabel}....Cable attenuation in dB

l..........Length in m

$D_{dB/m}$.....Attenuation in db/m at frequency

The antenna gain is stated in various different units. These units include dBi and dBic. The units dBi and dBic refer to an isotropic (spherical) radiator, where dBic refers to a circularly polarised isotropic radiator and dBi to a linearly polarised isotropic radiator.

In the European approval area, the radiated power must not exceed 2 W ERP. This figure refers to a half-wave dipole. The relationship shown below exists between an isotropic radiator (dBi) and a half-wave dipole.

$$G_{HW} = G_{isot} - 2.14dB$$

G_{HW}....Gain based on a half-wave dipole

G_{isot}....Gain based on an isotropic radiator in dBi

If the gain of the antenna is referred to the polarisation of a circular isotropic antenna (dBic), the linear gain of the antenna is 3 dB lower. As a result the transmission power can be increased by 3 dB.

$$G_{HW} = G_{isot} - 2.14dB - 3dB$$

G_{HW}....Gain based on a half-wave dipole

G_{isot}....Gain based on an isotropic radiator in dBic

In the FCC / IC approval region, the RF power connected at the antenna input must not exceed 1 W. If the gain of the antenna is higher than 6 dBi, the RF power connected must be reduced correspondingly. The reader's transmission power is then:

$$P_{Reader} = P_{cond} + D_{Kabel} \text{ with } P_{cond} \leq 1W \text{ and } G_{isot} \leq 6dB$$

P_{Reader}...Transmission power of the reader in dBm

P_{cond}......Power on antenna output in dBm

D_{Kabel}.....Cable attenuation in dBm

G_{HW}......Antenna gain in dBi

If the antenna gain is stated in dBic, the reader's transmission power can be increased by 3 dB.

The transmission power for the European variant can be set in 0.25-dB steps from 20 dBm to 33 dBm.

The heading provides separate fields for inputting the antenna gain and the attenuation.

Note

The antenna gain must be stated in dBic.

*The RFID reader's transmission power can be set separately for each antenna or all antennas at the same time. If the **All antennas same power** check box is set, the sliders for the other antennas are set to the same power when a slider for the power for antenna 1-4 is adjusted. If this check box is not selected, the power at the antennas can be set separately for each output.*

*Pre-defined antennas can be selected in the **Antenna type selection** drop-down menu. This selection sets the antenna gain in the program, and limits the transmission power to the maximum value permitted for this antenna. If **Custom antenna** is selected, the gain and power can be freely set.*

The context menu allows the XML file to be opened, and if changes are made to the file also allows it to be reloaded. When the file has been loaded, the changes are visible in the program.

right mouse -> open =, re-read and update!

6.6.1.2.   Antenna multiplex configuration

The sequence in which the antennas are used to read the tag can be set under this header. If this antenna is not activated, the system proceeds to the next entry on the multiplex list. For asynchronous operation of the reader, the exposure time on the antenna can also be specified. See section ((B)) „configurational manual reader", sections *MultiplexingAntennaport* and *MultiplexingExposureTime* for more details.

6.6.1.3.   RF settings

Depending on the approval region, the reader transmits in the frequency range 865 MHz to 868 MHz for Europe or 902 MHz to 928 MHz for USA / Canada.

In Europe the number of channels to be used can be limited. For this purpose the related check box for each channel the reader is to use must be selected on the *Available channels* list. In this manner it is possible to avoid from the start the usage of specific channels on which there is interference.

Each read command connects the channels under country-specific conditions and in accordance with the selected communications standard. The reader then starts to search through the channels in ascending order.

In the *Communication standard* drop-down menu, when necessary and when permitted by the reader, the reader can be switched to a different country-specific communications standard.The device version governs the communications standards that are permitted.

The modulation type can be switched between double sideband and PR-ASK modulation in this drop-down menu.

The communications profile is critical for the data rate and the read reliability. This option allows the technician to directly influence the performance of the reader and the spectrum of the signal. The profile names contain basic orientation on the transmission and reception data rates.

Note

A special data rate may be necessary, depending on the tag used. Please contact Kathrein (rfid@kathrein.de) for further details.

The "Time until carrier stand-by" parameter specifies how long the carrier of the reader remains active on the air interface after the last action. Once this time has elapsed the carrier is switched off.

6.6.1.4.   Selektionsparameter

Under this heading the user can configure the singularisation of the tags to the EPC standard ((E)). The parameters can be selected in the drop-down menu, and have the following meanings:

1   Initial Q value – reflects the number of tags expected in the field. (see ((B)) capital2.4.2. "*InitialQ*")

2   Sel – specifies whether other parameters are of interest for an inventory of the tag population, or not. (see ((B)) capital 2.4.10. "*QuerySel*")

3   Sessions - this configuration parameter instructs the reader the session with which it should work. (see ((B)) capital 2.4.3. "*Sessions*")

4   Target – specifies which tags in the population should participate in the inventory. (see ((B)) capital 2.4.9. "*QueryTarget*")

6.6.2.   Expert settings 2

The *Expert settings 2* tab is split into four headings for further configuration of the Kathrein RRU4 reader. The default parameter set can be changed, one parameter set copied into another,reader parameters read to determine their ID and select filter settings configured.
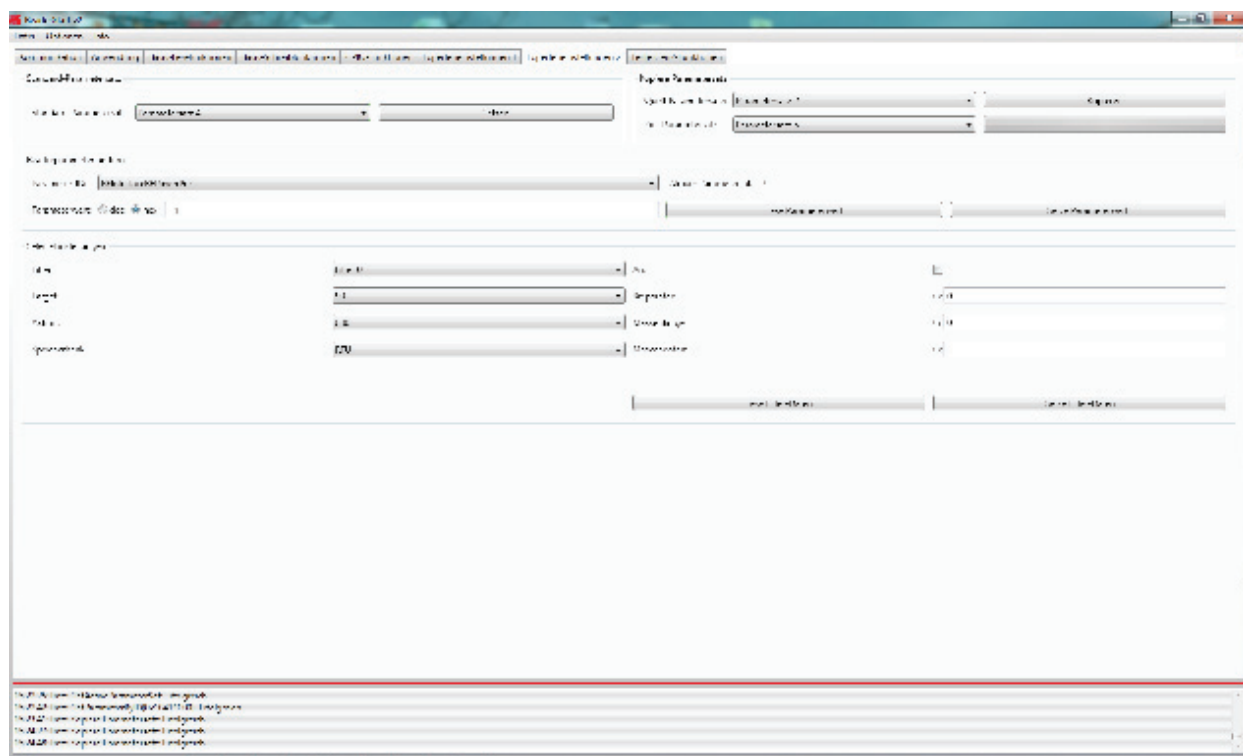

Figure: Expert settings 2 tab

The *Default parameter set* rubric allows configuration of the parameter set that is loaded from the EEPROM into the RAM when the Kathrein RRU4 reader is started.

The *Copy parameter set* header allows one parameter set to be copied into another. On successful completion of the copy operation, the *Copy* button glows green briefly and a corresponding message is displayed in the status window, otherwise the *Copy* button glows red.

The *Change reader parameter* header allows all the Kathrein RRU4 reader settings to be changed using their respective configuration IDs. After selection of the parameter ID, the corresponding value of the current parameter set of the Kathrein RRU4 reader is read by clicking on *Get parameter value* and displayed in the field parameter value, optionally as a decimal (*dec*) or hexadecimal (*hex*) value. A value that has already been read can be converted to *dec* or *hex* by pressing the radio button. The *Set parameter value* button writes the value stated in the *Parameter value* field into the selected parameter ID. The two actions (read and set) are shown by the respective buttons glowing the respective colour to indicate success and failure, and a message appears in the status window accordingly.

In the *Select settings* area, filters can be set which are brought into effect by means of a *Select* command. This offers the facility to filter out certain tags, or to detect only tags with certain defined data in the respective memory banks. Up to 32 filters can be set in total. Successful reading of the values of the selected filter and successful writing of the filter values is indicated by the respective button glowing green and a text appearing in the status field. Otherwise the respective button glows red and a description of the error is output.

6.7. Test Gen2 functions

This tab makes it possible to access individual functions of the reader. This includes, along with the functionality in accordance with the EPC-Gen2 standard, e. g.: read individual tags, describe tags, set and change passwords, and also select the antenna for the operation.

The user interface consists of the headers *Get all EPCs*, *Write EPC*, *Change password*, *Read/write data*, *Lock*, *Kill* and the display window for EPCs that have been read. The sections that follow explain this functionality in more detail.
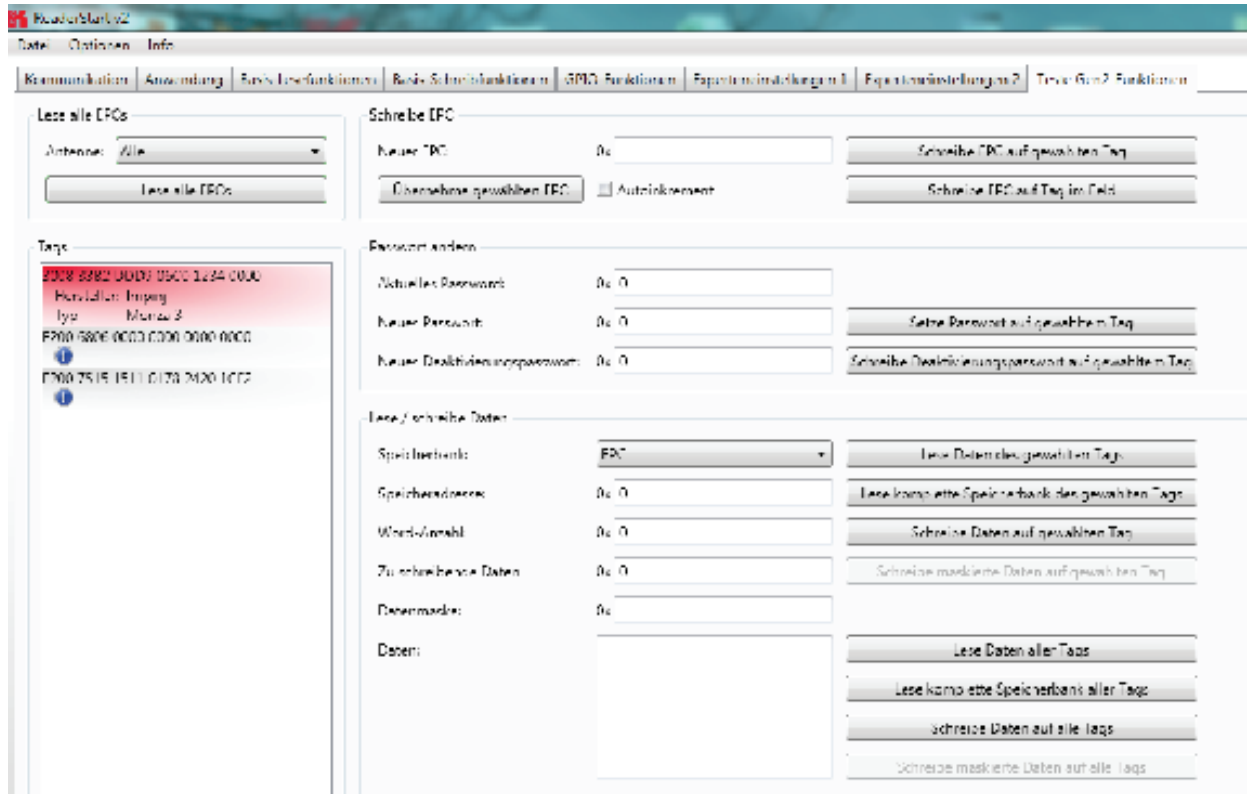
Figure: The Test Gen2 functions menu tab

Note

Additional information about the manufacturer and the chip type are displayed on the „i" symbol. Left click on this icon, this information can be retrieved.

6.7.1.   Get all EPCs

To read a tag in this menu, the *Get all EPCs* button must be clicked once the reader has been correctly configured. The reader now tries once again to read all the tags in the field of the selected antenna. If in the *Antenna selection* drop-down menu the number of antennas has been restricted, reading will now be performed using the currently selected antenna, or using the antenna selected with *All* in the *Expert settings 1*.

The EPCs from the tags read successfully are displayed in the field below. For the following operations, a tag can be selected from this list by clicking on it.

6.7.2.   Write EPC

The EPC of the tag can be altered as desired under this header. For this purpose an EPC in hexadecimal format must be entered in the *New EPC* field.

Note

Comply with the maximum EPC length supported by the tag - if this is exceeded the tag will return an error.

*If the requirement is only to amend an existing tag, this tag can be loaded to the field by pressing the **Apply selected EPC** button. Now the EPC can be changed manually, or by using the **Auto increment** option can be increased by one at each write event.*

*The write event itself can optionally be executed on this tag by pressing the **Write EPC to selected tag** button. At this time there may be several tags in the field, but at least one tag from the list must be selected. The second option is to write the specified EPC without a tag being selected. When using this function, make sure there just one single tag in the field.*

6.7.3.   Change password

The EPC standard see ((B)) specifies that the tag should have two modes, the *open* and the *secured state*. In the open state, operations can be performed on the tag if the associated memory areas are not secured with a password greater than 0. If a password has been set and the *Lock* header has been used to set the memory areas to password protected, the desired operation will not be executed, and the tag will report an access error. Normal access remains available in areas that are not blocked.

If when the tag is accessed the valid password is given, the tag switches into the secured state and access is available even in blocked areas. Setting the password and setting how individual areas are blocked is performed under the *Change password* and *Lock* headers.

Under the first header, the password for restricting access to the tag and the password for deactivation of the tag are set. The access password can be used to restrict access to the tag in the open state. Depending on the configuration under the *Lock* header, parts of the tag can be provided with completely or partially restricted access rights.

The deactivation password is required to deactivate the tag permanently by means of a Kill command.

Note

*After a **Kill tag** command, the tag will be unusable.*

*To change the password, the current password must be given. If no password has yet been set, the default value is 0. The new password is entered in the field of the same name, in hexadecimal format. Clicking on the **Set password on selected tag** button replaces the old password with the new password. The deactivation password is entered in the field of the same name by clicking on the associated button.*

*If the password is changed and the memory area in question is already protected by the access password, in addition to the new password the access password must be entered in the **Current password** field.*

6.7.4.   Read/write data

This header supplies detailed access to all the data areas of the tag. Access is obtained by entering the selected memory bank, the address within the memory bank and the number of words, expressed as 16-bit words.

If data are to be written, they must be entered in the *Data to write* field. The data mask allows only individual bits on the tag to be changed. To do this, the mask must be entered in the *Data mask* field. The reader uses this mask to change the data read from the tag at the points where 1 bits are written in the mask, and writes the result back into the tag. The desired data can optionally be written to a single tag in the field or to all tags in the field. If they are written to all tags in the field, these tags must all have the same configuration (lock and password).

The header also offers the facility to read data from the selected tag or from all tags in the field. If the tags in the field have differing passwords and are configured differently, the data must be read by individual tags.

The next section deals in more detail with the saving of the individual memory areas.

6.7.5.   Lock

The EPC Gen 2 standard provides security mechanisms for the tag data areas. This allows individual memory areas and functionalities of the tags to be provided with a password to protect it against access and/or changes.

Under the *Lock* header, the mask that specifies access to the areas in accordance with the EPC Gen 2 standard can be customised to suit the application. If no changes are required for an area, *No change* must be selected in the respective drop-down menu. The areas are grouped as follows:

1   Deactivate – specifies whether or not a deactivation password is necessary for deactivating the tag. Further details can be found in ((E)).

2   Access – specifies whether an access password is necessary for accessing a tag. If no access password is set, the TAG can be addressed in the open state condition. Further details can be found in ((E)).

3   EPC – allows specification of whether or not the access password is necessary for changing the EPC.

4   TID – this area contains general information about the tag. This area can also be protected against user access by setting the access password.

5   USER – if the tag has a memory area provided for user data, these can be protected by setting the access password.

The respective items in the drop-down menu are divided into access blocks, which prevent reading and writing, and write blocks.

Note

If the option with the suffix is permanently selected, this option can no longer be changed. Further details can be found in ((A)) „communication protocol".

*Clicking on the **Lock selected tag** button loads the mask that was created to the list of the selected tag. Alternatively all the tags in the field can be blocked, on the precondition that the tags all have the same password.*

Note

*Wrongly configuring the **Lock** header can render the tag unusable.*

## 6.7.6.	Kill

Pressing the *Kill selected tag* button, with the stated password, executes a Kill command on this tag. The *Kill all tags* button, with the stated password, attempts to execute a Kill command on all the tag in the field.

Note
For the deactivation of a tag, a deactivation password that is not 0 must have been set.

Note
*After a **Kill tag** command, the tag will be unusable.*

6.8. © KRAI-Settings

The basic settings of the reader parameters appear in this Installation Manual Reader from Chapter 6 "Descriptions and operation of the reader" and can be set and configured through the Reader Start Software.
© The KRAI-specific settings are explained in the following text. You can find this setting in the Reader Start Software section, under the tab "KRAI".
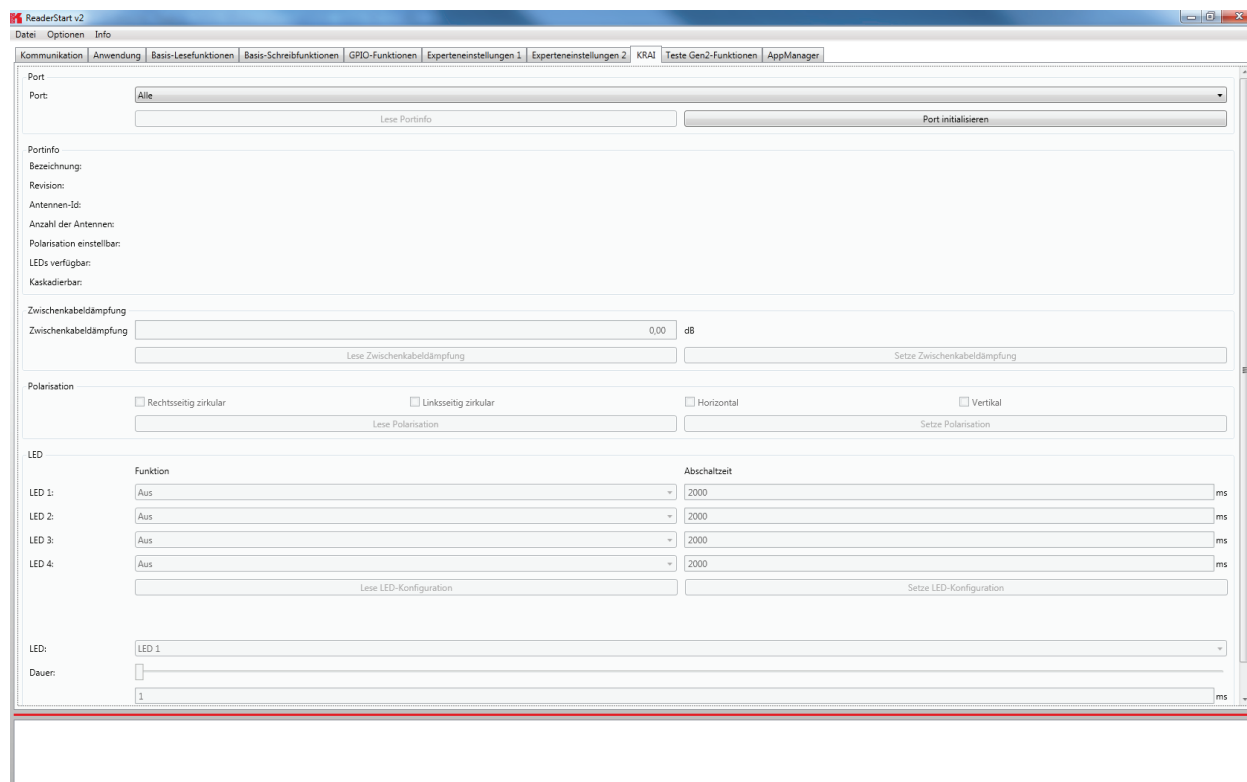
Figure: Overview of index card KRAI

The Reader recognises the connected antennas at boot up, but this can also be done manually by selecting a single port or through the "All" option from the dropdown menu section port. Initialize the button port then runs the query through the antennas in this / these ports.

When a port is selected from the drop-down list information on this port will be listed under port information specified in characteristics depending on the antenna type and features.

Port information which had been collected through initialisation can be called up by pressing the "Read port info" button. This action list is executed automatically by default for every port initialisation and port selection in the drop down menu.

The choice of configuration options depends on the types of the connected antennas. The category *polarisation* is for antennas with polarisation switching, and the cable attenuation category is available for use by SmartShelf antennas. Depending on the features that are integrated in the antennas LEDs can be controlled / configured under the section LED.
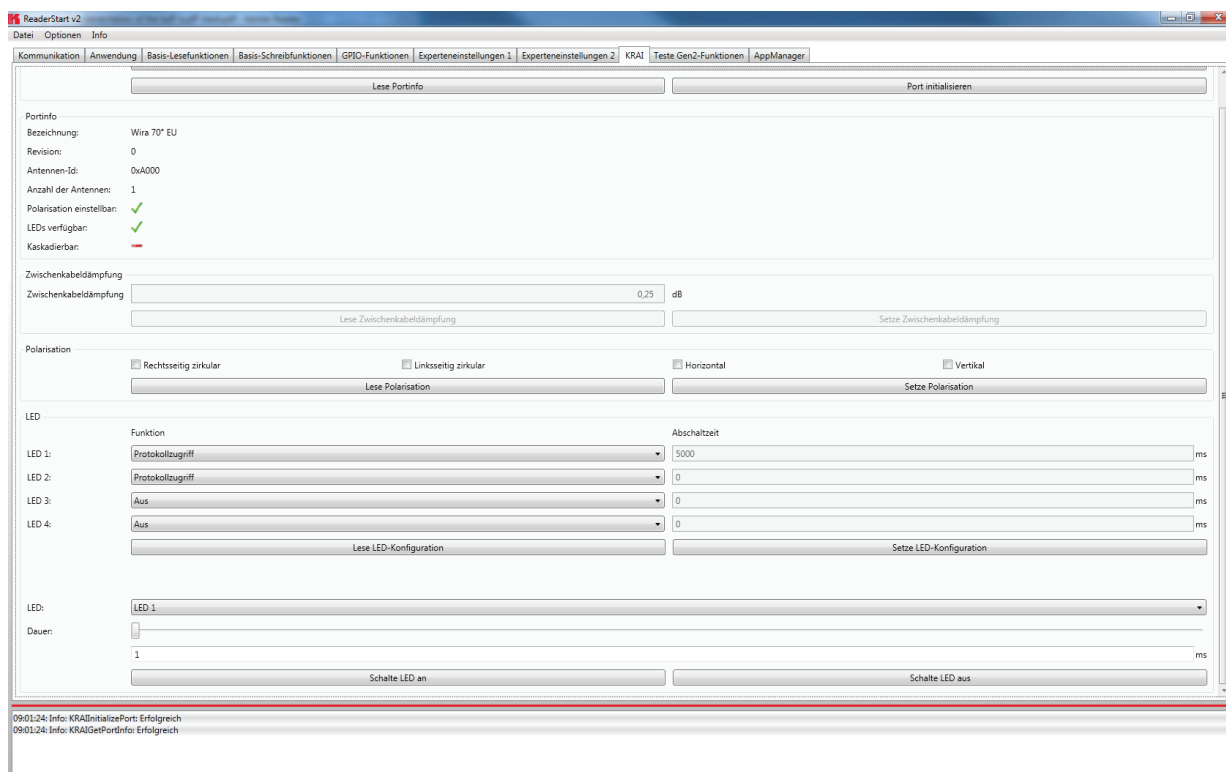
Figure: Example WIRA with KRAI function and LEDs

In the *polarisation* section, the polarisation modes RHCP, LHCP, and the *horizontal and vertical positions* of the panels can be set. If there are several types of polarisation selected at the same time in the check boxes, then the antenna configuration changes after every inventory (read cycle) in the specific given order.
Using the button *"Read Polarisation"* the stored information from the Reader can be called up and using the *"Set Polarisation"* button a new input configuration can be stored.

The configuration of the LEDs in the LED section is analogous to the description of the functions in Section 6.1 to the tab *communication, heading IO-Card configuration/RS232.* The features are as follows:

1 - Off - the selected LED is off

2 - On - the selected LED is always on

3 - RF on - the LED is active when the high frequency is fed to First to the Last antenna.

4 - Antenna Error - The error LED flashes/displays off-time in milliseconds when an error occurs in between the First and Last antenna

5 – Tag found - The error LED flashes/displays off-time in milliseconds whenever a tag is found on the antennas

6 - Operation successful tag - the output is active for milliseconds at switch off time as soon as an operation on the tag was successful on the First to the Last antenna.

7 - Protocol - the LED can be directly switched on and off via the protocol.

Reading and setting the configuration is done via the buttons *"Read LED Configuration"* and *"Set LED configuration"*. The configuration change is done immediately.

If the function access protocol for the LEDs is chosen, it can be adjusted in the submenu LED and residual period for the LED can be set. With buttons *"Switch LED On"* the LED is switched on for ms duration. The *"Switch LED Off"* button switches off the chosen LED.
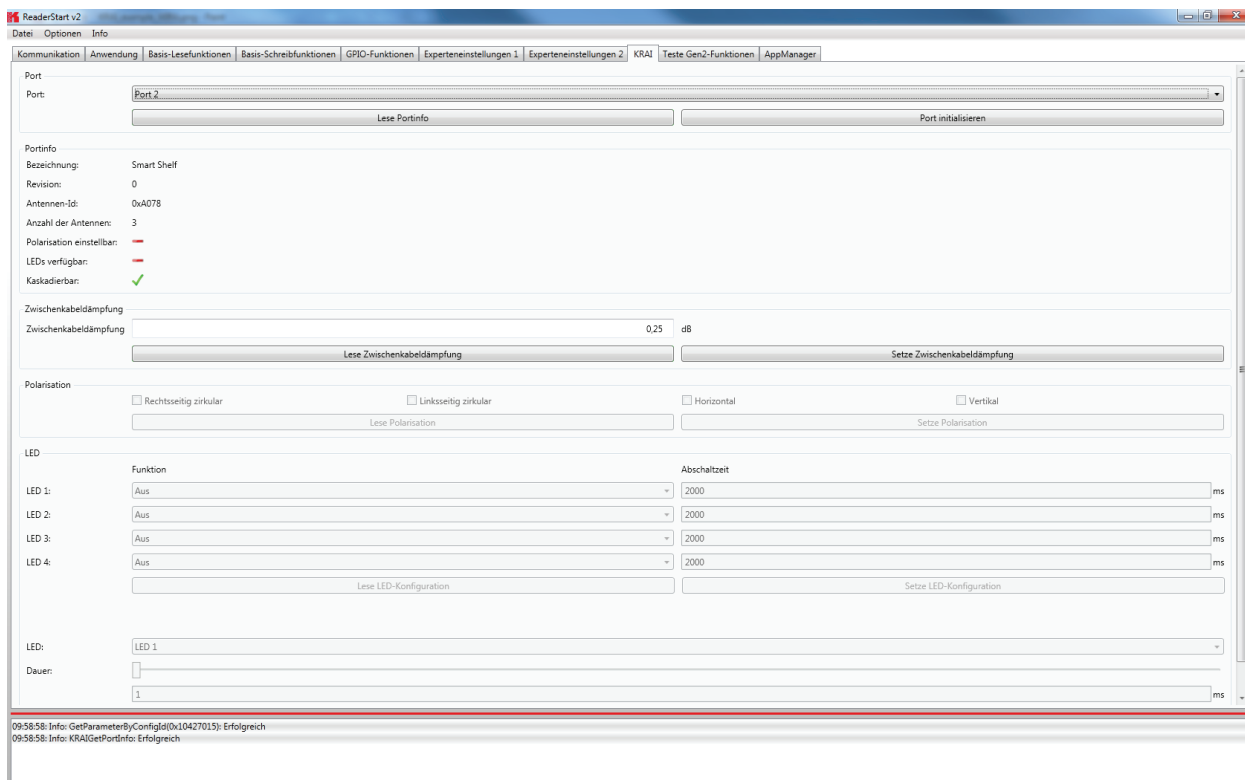

Figure: Example SmartShelf antenna with KRAI function without LEDs

For cascadable SmartShelf antennas an absolute attenuation value is to be entered under the heading "interim cable loss" (in 0.25 dB steps) for the lines between the antennas. The given value is set with "interim cable loss" to the reader. Conversely, this can be called up from the reader using the button "Read interim cable loss".

Note

For cascading smart shelf antennas, it is necessary to use cables with the same attenuation (cable length). Otherwise the TX-power of the antennas that is derived from the intermediate cable attenuation is not calculated correctly. Furthermore, the value of the intermediate cable loss should be correct, so that the output power can be correctly calculated and fed accordingly.

The libraries and headerfiles to support the software integration of the reader into existing applications can be found on the CD in the /API directory. The user can choose the appropriate library for the target system (windows/ linux/ ELC/ ETL).
As another way of integration the user can implement the KBRP protocol according to the specification ((A)).

The example projects are located in the directory RFIDDemoApp. They demonstrate the programming of applications for the reader under Windows, Linux and embedded Linux (ELC/ ETL) in C#, C++ and VB.Net. The examples are based on the use of library functions. This examples are console applications. They show how to establish an connection to the reader, read tags, use GPIOs and
how action lists are constructed.

6.9.   App Manager

The AppManager manages Linux application on the Linux part of the ELC and ETL Reader. To make this possible, each application must have the following structure:

```
<Configuration>
  <PlatformIDs>
        <!--SECO-->
        <PlatformID>E2C4D78C-C9FE-4594-8153-82B51312166E        </PlatformID>
        <!--KACOM-->
        <PlatformID>59E1F344-C5AE-4662-9A82-D5F265A16271</PlatformID>
  </PlatformIDs>
  <AppID>EC5BD95F-1296-4F94-957F-897219748C9C</AppID>
  <Name>Access Manager</Name>
  <Version>1.00.00.40</Version>
  <Start>startscript.sh</Start>
  <Stop>stopscript.sh</Stop>
  <IsAlive>isalivescript.sh</IsAlive>
        <!-- Optional -->
  <Install>installscript.sh</Install>
  <Uninstall>uninstallscript.sh</Uninstall>
</Configuration>
```

To transfer the application data to the reader, an FTP server can be started. Select "Start FTP Server" - this enables readers to start SW, in the menu "Options / Intelligence Module."

Access can then be made to the ftp://192.168.0.1 access in Windows Explorer. Please adjust the IP address, if you have set a different IP address on your system.
Alternatively, the app can be imported in the Linux system using the "install app" function.
For this purpose the app structure has to be packed in *.tar format.
Using the Reader Start software the applications can then be managed using the tab "AppManager"

6.10.   Access Manager

Kathrein RFID solutions are characterised by ease of use and intuitive operation. They have extensive capabilities for fast and secure ID applications of all kinds.
The devices of the ARU4 and RRU4 series have an optional integrated industrial PC platform based on Linux OS on which the complete application control can be run directly on the device. A permanent data connection is not necessary!

The application software Access Manager V 1.0 allows user-controlled input and configuration of the transponder data to be collected. Programming skills are not required! Digital inputs are thereby connected/linked to digital outputs and then to defined EPC and TID data dependent on transponders.

For flexible and efficient usage of the transponder, Kathrein RFID systems are equipped with up to 4 digital inputs that can be used to control features. This allows starting points of the application to be set, in which a photoelectric or inductive ground loop is requested to enable the reading process. When registered in the system transponder these can be detected and assigned to specific processes so that individual transponders are assigned appropriate authorisations. Depending on these decisions up to 4 digital outputs can be connected, e.g. to allow access by opening a barrier or a gate.

As an example, on the Kathrein RFID homepage a demo version of ACCESS Manager can be downloaded. This demo version is limited to 5 TAGs, and can be enabled if required for up to 500 transponders.
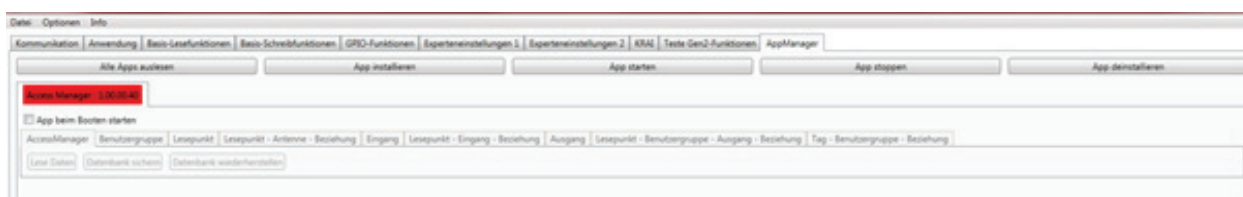
The ACCESS Manager is activated using the button "Start app". The signal bar in the indicator changes from red to green.
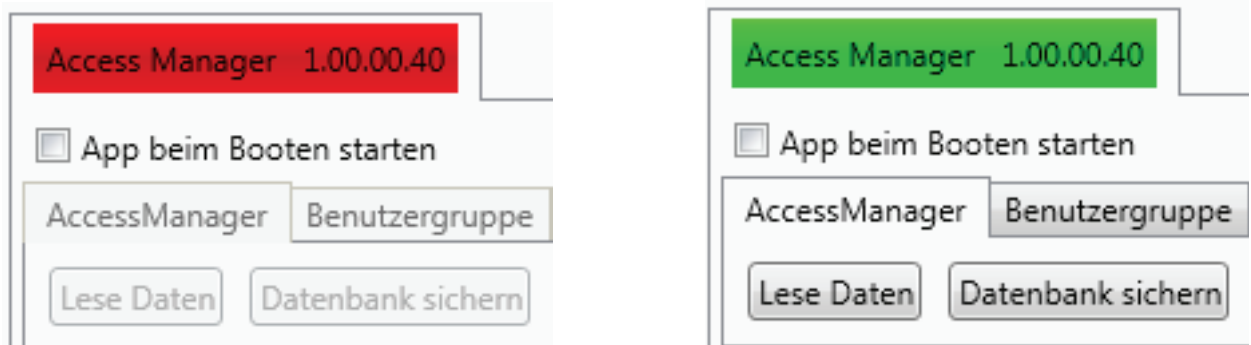
A tick in the "start app at boot" target application box will resume the app set after a power failure.
The example was set up based on the following scenario:

Vehicle detection for entry and exit in a parking garage
- 　　　3 user groups (standard, XXL parking; service staff)
- 　　　3 Entrances
- 　　　Standard Parking - Standard Parker and service staff
- 　　　XXL-Parking place - XXL-Parker and service staff
- 　　　Service Area – only service staff
- 　　　Each entrance has its own read point
- 　　　1 common exit – for all vehicles

6.10.1.　　　User Groups

Using "User Group / Add", the respective roles can be created and managed via delete / edit.

6.10.2. Reading point

On the input field "read point", the respective entrances and exits are recorded. At the same time the "read time" is set in msec.
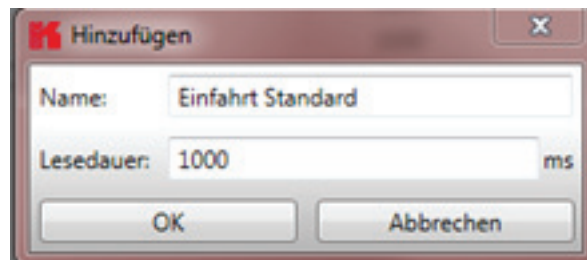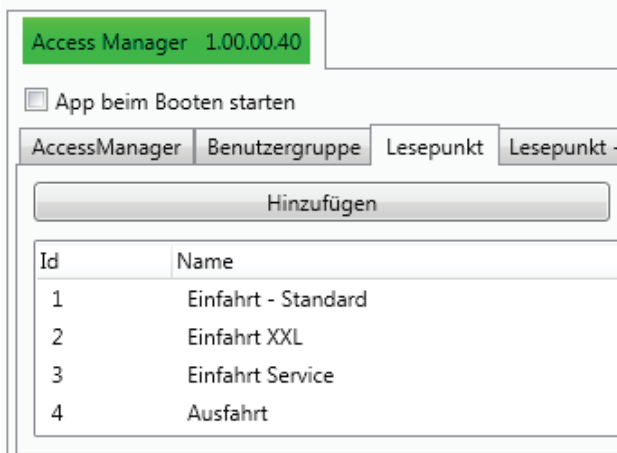
6.10.3. Reading point - Antenna relationship

The corresponding reading points are linked to the physical antennas with the "read point antenna" relationship.
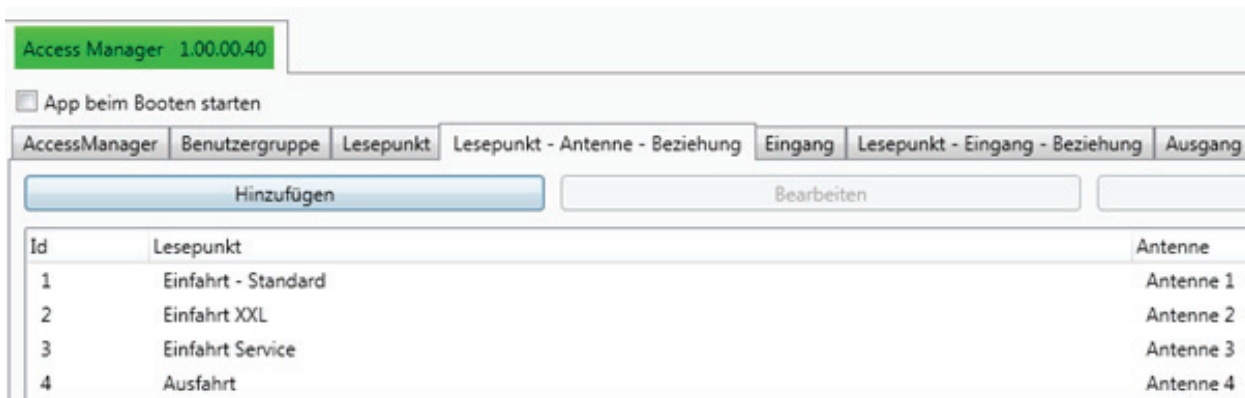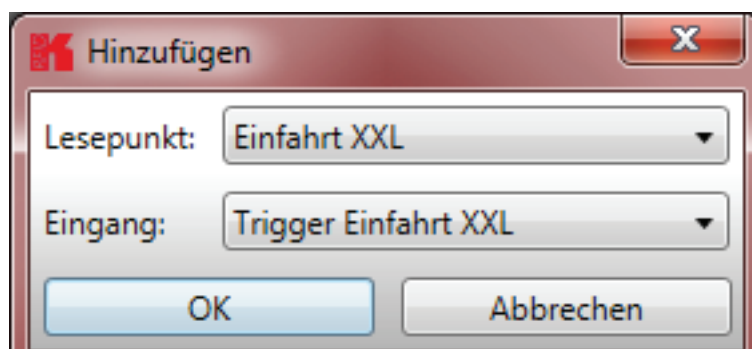

6.10.4. Entrance

The tab "Input" specifies the starting condition for the reading points. If e.g. the trigger is activated as inductive ground loop, the impetus for RFID reading is carried out via the associated digital input.

6.10.5. Reading point – entrance relationship

With the "read point – entrance relationship" the trigger is linked to the read point.
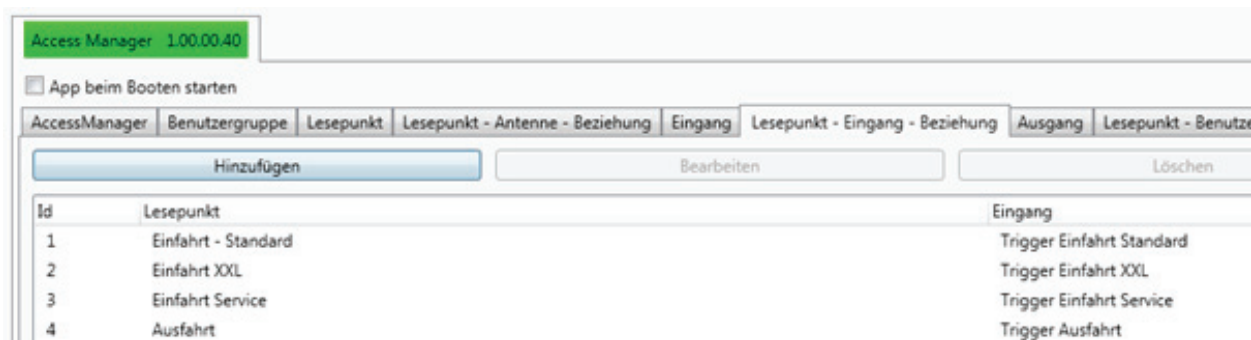
6.10.6. Output

Then, the digital outputs are allocated. This will then set which action should take place (here enable barrier = entrance open), and also which digital output is activated (output 1) and how long the switching pulse will be.
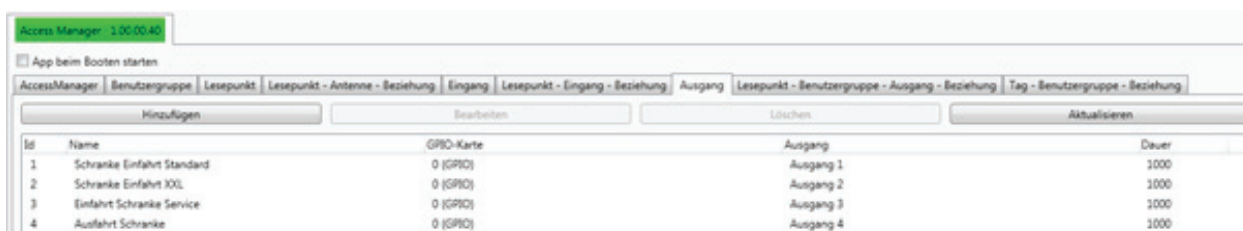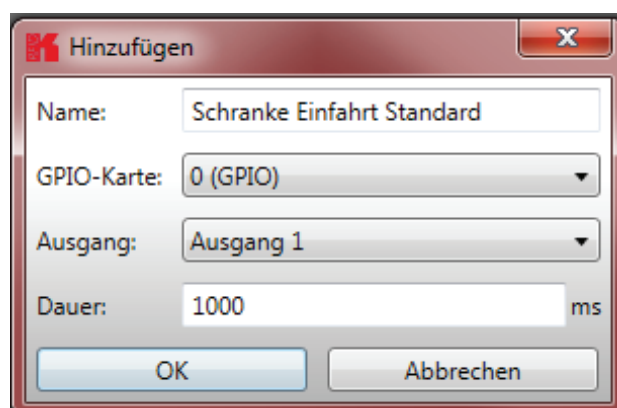
6.10.7. User Groups

The permissions are distributed through the relationship between reading points, user groups and the outputs. Here, of course, a user group (in this case service employees) can have access to multiple reading points.

6.10.8. Read point - User Group - Output - relationship

The next tab shows the allocation of read points, user groups and outputs.

Please note that all authorised users groups are also listed for each read point. Thus, in the example at the "entrance - standard" only "standard - Parker" can drive in "service employees". Should "XXL Parker" also be issued an access permit to this area of the car park, it must also be linked in.

6.10.9.   Tag – User Group relationship

Finally, the unique transponders are assigned to the respective representatives of the user group, so as to achieve an unambiguous classification and identification of vehicles and users.
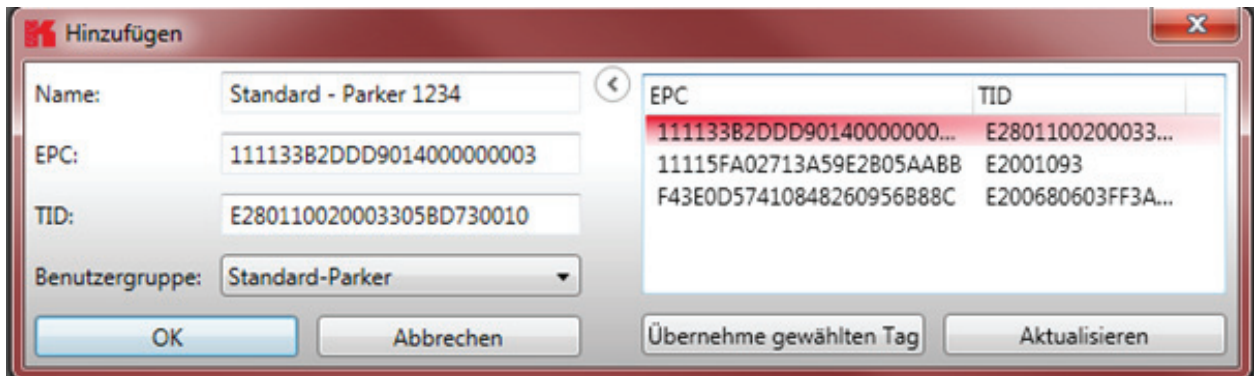
This can be either a "Name", "Username" or "ID".

After expanding the input mask using the ">" button, the current transponder is read. This can always be re-launched via the menu item "Update".

With "Accept the selected tag" the EPC and TID of the selected transponder is transferred to the mask.

At the end the tab "Tag-user Group relationship" is used to assign the user to his user group.

Thus authorisations and the unique identifier are defined by the transponder.

Since the processing of the Access Manager runs immediately into a SQL database on the Linux part of the reader, the transponder is also connected immediately. It is recorded in the corresponding driveways, after the triggering of the trigger and depending on its corresponding privileges, the barrier is opened or access is denied. Upon completion of processing, the Ethernet cable can be removed. The application runs autonomously on the Linux part of the Kathrein UHF RFID ETL / ELC Reader
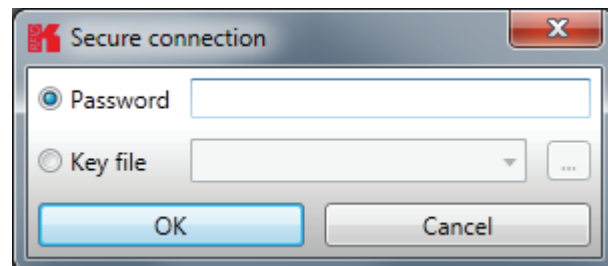
### 6.11.   Ethernet password

Secure Shell (SSH):

A secure shell connection can be established at the folder „Communication". For this, the option "Secure connection" has to be selected.
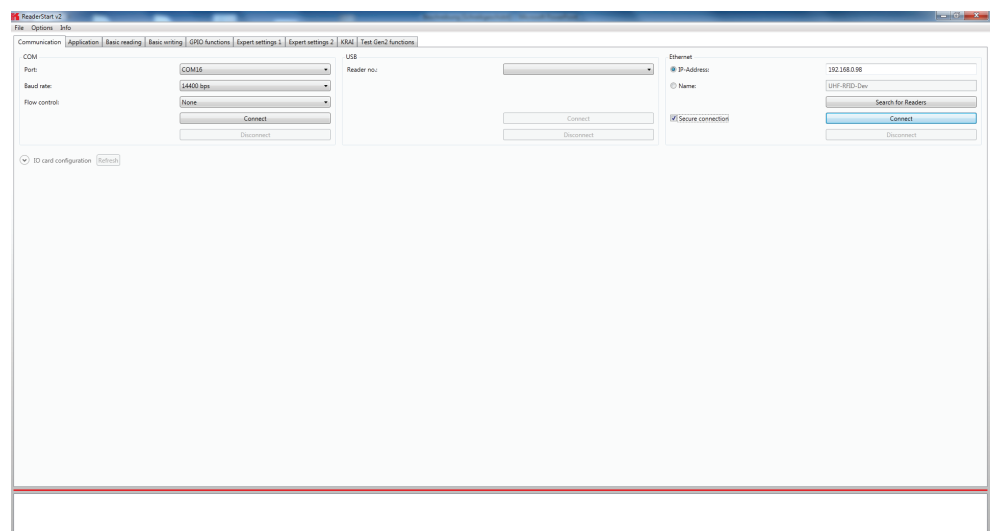
After selecting „Connect" a password is required to access. The default password is „UHF-RFID-Dev" .

Under „Options" > „Intelligence module" > „Secure connection config" the settings for the SSH can be installed.
The password can be changed with "Change Linux password"
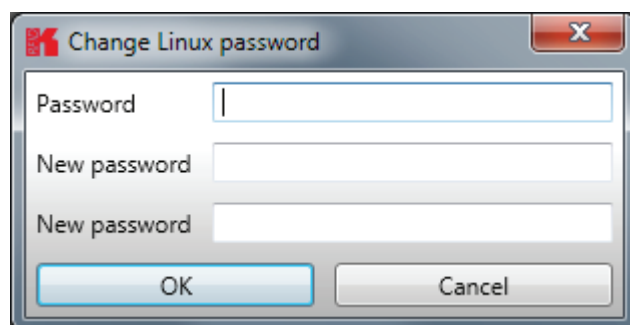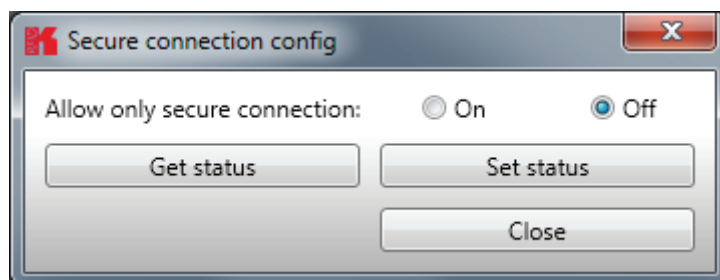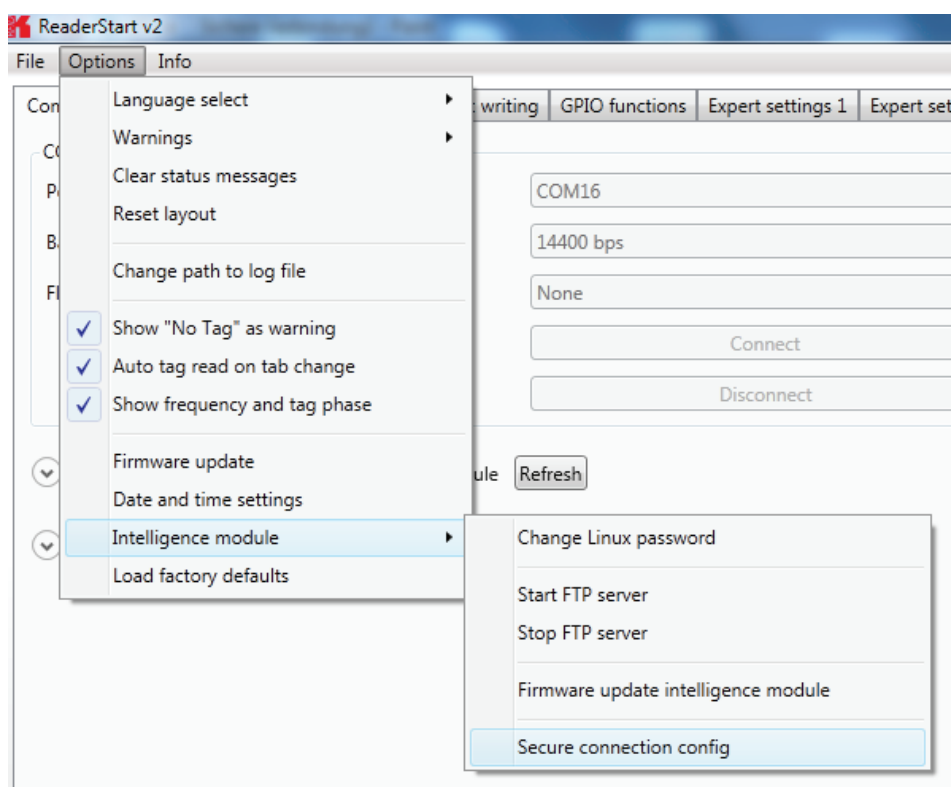
6.12. configuration password

The following commands will be protected against changing by the configuration password:

* SetCommunicationStandard

  * SetPortPower
  * SetCarrierFollowUpTime
  * SetPortMultiplexSequenceAndExposureTime
  * SetCableLossAndAntennaGain
  * SetETSIPortChannelList
  * SetETSIPortChannelSwitchingMode
  * SetProfile
  * SetModulationType
  * SetExtendedResultFlag
  * SetDefaultParameterSet
  * SetActiveParameterSet
  * SetParameterByConfigId
  * SetIOCardHwConfig
  * SetIOCardProtocolConfig
  * SetTime
  * SetAntennaMapping
  * LoadFactoryDefaults
  * FirmwareUpdatePrepare
  * SetSelSessionAndTarget
  * SetInitialQ
  * SetMaxAirCommErrors
  * SetASyncObservedListParameters

The configuration password can be set at "Expert settings2". To reset the password, a empty input will be set at the option "Set config password".
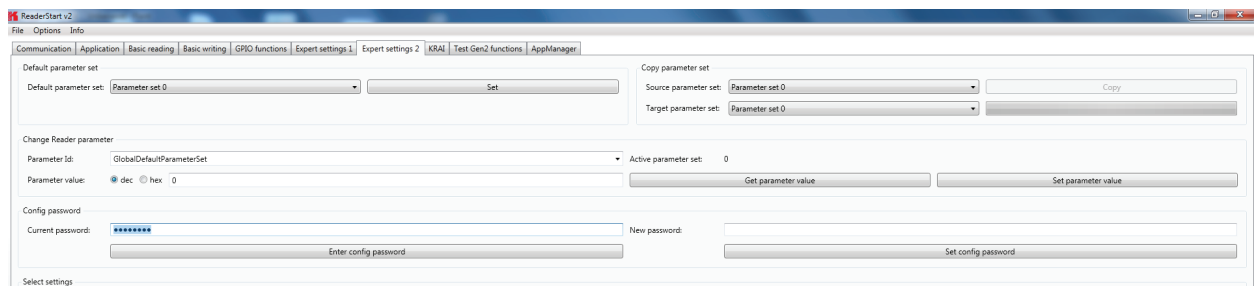
After entering the password you have 30 seconds to perform changes. Each time you save the changes, the expire time is extended by another 30 seconds. If you want to save changes after the 30 seconds, you get the system message „Access Denied".
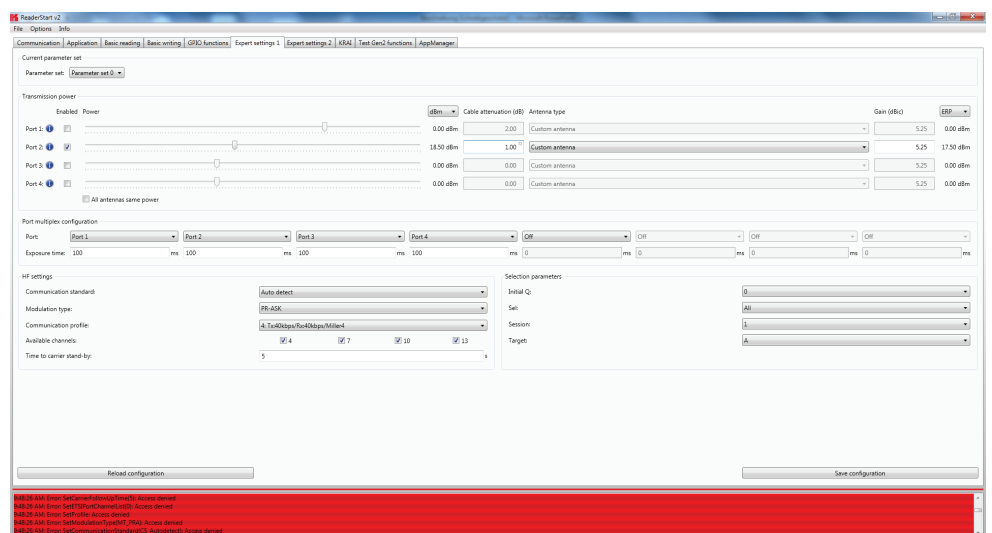
For the integration of the reader into an existing application on Windows, Linux for operation as a standalone device with embedded Linux appropriate libraries and header files are located on the CD in the subdirectory / API.
The user has the choice to use the appropriate target system library for Windows or Linux, or to implement KBRP according to the supplied protocol specification ((A)) in its target application.

The RFIDDemoApp directory contains sample projects for Windows, Linux and embedded Linux that demonstrate the programming in C #, C + + and VB.Net. These examples are based on the use of the library functions. This is a console application that shows how the connection is established to the reader and how tags are read, GPIOs used and action lists are built.

7.1.   Preparation

The examples have been tested on Windows 7 and Debian 6.0. Before the programs are compiled, the environment must be adapted. Copy the folder / AP and / RFIDDemoApp in your user directory. For the preparation of programs for an Embedded Linux, an Embedded Linux Development Kit must be installed. For more information on the installation, please see Chapter 7.6.

Note

The example is based on the connection parameters from the factory default settings of the IO cards. This may need to be adapted to your building in the reader and in the source code of the program.

The necessary libraries for the programs can either be stored in the respective program folder or the default library folder of the operating system.

Now, the programs can be created using the following procedure.

7.2.   Using the examples with Windows

The C #, C + + and VB.Net folder containing the example programs and project files for Visual Studio 2010 based on the ReaderDllDotNet. Download the appropriate project file and compile the program.

7.3.   Using the examples with Linux

The same source code can be used in Linux. A distinction is made as follows:

7.4.   Using the examples with Linux on a PC

The program is built in the / RFIDDemoApp / Linux with the command make. If the compiler finds all the necessary data, the program Console Linux demo is created in the same folder.

LibReaderLib.so the library from the / API / Linux as root (su + root password) is still needed for the program, this file can be copied to the / urs / lib (libReaderLib.so cp / usr / lib) or will be stored in the folder with the source code. Then the program with. / Console Linux demo can be started.

7.5.   Using on an embedded system

If the example is to be complied for the embedded system of an ETL or ELC reader, the ELDK must be installed for the corresponding target System on Linux. The process for this is described in Chapter 7.7. The cross compiler creates the program for the target system.

Note

The program created will only run on the target system.

To start the compilation process please use the file from the respective folder (RFIDDemoApp\RRU4-ELC-XX or ..\RRU4-ETL-XX).

The paths in the config.mk file must match those in your build system, so that the build process can be successful. If the build process is successful, the program can be transferred to the reader.

One way to transfer the data is described in Section 7.7.

7.6.   Installation Embedded Linux Development Kit (ELDK)

The ELDK is a development tool, which includes cross-compiler tools and furthermore useful programs, included already compiled for the target (eg libraries or user programs) provides.
The CD / DVD contains the information necessary for the installation of .iso files which were current at the time of creation of the CD / DVD. Newer versions can be downloaded at the following address

ftp://ftp.denx.de/pub/eldk/

(at the time of this writing, eg "version number" = 5.3). The directory structure is then given by

"Version-Nummer" → iso → eldk-"Versions-nummer"- "Architecture".iso

It is important to note that the type of Reader RRU4 ETL files with the extension "~ armv4t.iso" (eg eldk-5.2.1-armv4t.iso) and for readers of the type RRU4 ELC those ending with "~ armv7a.iso" (eg eldk-5.2.1-armv7a.iso) must be used.
To install the ELDK on the Linux system root privileges are required (su -> password). In the first step, you copy the .iso file to a temporary directory, eg / tmp

Now the .iso file can be mounted to a different directory eg / mnt / tmp directory (the directory if not available, create with mkdir / mnt / tmp)

mount -o loop /tmp/eldk-X.X.X-armvXX.iso /mnt/tmp

Next change to the mount directory

cd /mnt/tmp

and run the following command

./install.sh -s qte -r - armvXX

The ELDK is then installed by default in the / opt directory. There, the tools can be found. In the following directory

/opt/eldk-X.X.X/armvXX/sysroots/i686-eldk-linux

You will find the the Toolchain with the Cross-Compiler. In the following directory

/opt/eldk-X.X.X/armvXX/sysroots/armvXX-vfp-neon-linux-gnueabi

compiled tools can be found within the directory.
It is important that the last step is the unmounting of the .iso file
This can be completed using the following command

umount /mnt/tmp

The .iso file can then be deleted from the temporary folder.

rm -f /tmp/eldk-X.X.X-armvXX.iso

On the included CD/DVD is a file named "config.mk". This file is for the compilation of programs for the reader and is incorporated in the Makefiles (include config.mk)(see example below).

```
ELDK_SYSROOTS                    := /opt/eldk-5.1/armv7a/sysroots
ELDK_TOOLCHAIN_SYSROOT           := $(ELDK_SYSROOTS)/i686-eldk-linux
ELDK_ARM_SYSROOT                 := $(ELDK_SYSROOTS)/armv7a-vfp-neon linux-gnueabi
CROSS_COMPILE                    := arm-linux-gnueabi-
ARCHITECTURE_CFLAGS              := -march=armv7-a -mthumb-interwork

TARGET_ARCHITECTURE              := arm

ifndef NO_CROSS_COMPILE

AR        := ${CROSS_COMPILE}ar
AS        := ${CROSS_COMPILE}as
CC        := ${CROSS_COMPILE}gcc
CXX       := ${CROSS_COMPILE}g++
GDB       := ${CROSS_COMPILE}gdb
LD        := ${CROSS_COMPILE}ld
NM        := ${CROSS_COMPILE}nm
RANLIB    := ${CROSS_COMPILE}ranlib
LDCONFIG  := ${CROSS_COMPILE}ldconfig
STRIP     := ${CROSS_COMPILE}strip
OBJCOPY   := ${CROSS_COMPILE}objcopy

PATH      := $(ELDK_TOOLCHAIN_SYSROOT)/usr/bin/armv7a-vfp-neon-linux-gnueabi:$(PATH)

endif
```

In the config.mk paths are included for make, for example, where the compiler is required to find or libraries for the target (the ARM controller). Adaptations for the EDLK version (here eldk-5.1 or ARMv7A) or the directory structure may be necessary.

Note

The created program will run only on the target system.

To start the compile process, please use the make file from the respective folder (RFIDDemoApp \ RRU4-ELC-XX or .. \ RRU4 ETL-XX).

Note

The paths in the config.mk file must match those in your build system, for a successful build process.

When the build process was successful, the program can be transferred to the reader. A possible way to transmit the data is described in ().

7.7. Installation Linux application

The reader is equipped with a separate module, running a linux on it. That gives the user the opportunity to install an application that will start automatically after powering up the reader. The flash memory is divided into a writable and a read only part of the file system.

This application note describes how to install a user application to the non-volatile memory (flash) of the reader. To do this it is necessary to copy the application and the script, which starts the application, to the target and make both executable.

Requirements:
- RRU4-ETL-xx/ ARU-ETL-xx
- Ethernet connection to the reader
- For connecting to the Reader a client like putty ((F))
- ftp client e.g. ftp (for Windows you can use the Explorer)
- the user application

For writing and compiling an application please use the manual for the Reader.

First make a connection to the reader by opening a command shell:

```
C:\> putty –telnet ip_address          for xxxx-ETL-xx
C:\> putty -ssh ip_address              for xxxx-ELC-xx
```

where ip_address is the address of your reader. Per default this address is 192.168.0.1. The default login data is "root" with the password "UHF-RFID-Dev".

To copy a program to the reader ftp is used. Therefore the ftp server on the reader needs to be started. This can be done via telnet by calling

```
# /usr/rfid/ftpstart
```

from the command line.

Now it is possible to establish a connection to the reader via ftp. To do so, open another command-shell, go to the directory of the application to copy and start the ftp client e.g.:

```
C:\> ftp ip_address
```

where ip_address is the address of you reader. Login name is "root", no password is required. If there is a problem establishing the connection, check your firewall or ask your network administrator

To copy the application use

```
# put source /flash/destination
```

where source is the source filename and if necessary the directory from where to copy it. Destination should be the filename that it should be called on the target. It's important to copy the file into the "/flash" folder, because there is the writeable file system.

After the file is put in that folder, the ftp is not needed anymore. With

```
# /usr/rfid/ftpstop
```

the server can be stopped. The FTP service is also stopped after a reboot.

On reader side the application file needs the permission to execute for all intended users. To change the permission use

```
# chmod permission_owner permission_group permission_other application
```

where all permission_xxx consist of 3 bits, first read, second write and third execute. If the bit is set, the permission is granted otherwise it is not. At least the application should be executable. Application is the name of the application on the target. To give the permission to read and execute to all 3 groups it should look like this:

```
# chmod 555 application
```

So now we have an application in the non volatile memory on the target that is allowed to be executed. The next and last step is to make it bootable by default after power up. During boot process the script inittab is called. This script looks for a script named

startup

in the directory

/flash.

The linux will execute its content on every boot. Therefore we need to add the programcall in that script. Below is an example shown, how this can be done from the commandline on the reader:

```
root@UHF-RFID-Dev:~# echo  >> /flash/startup
root@UHF-RFID-Dev:~# echo  # now lets start the application >> /flash/startup
root@UHF-RFID-Dev:~# echo /flash/application >> /flash/startup
```

The first line adds a newline into the startup-File, the second adds a comment to it. The third line calls the application. When you need to modify the script, take use an editor that can handle Unix line breaks at the end of each line (0x0A), the normal windows carriage return and linefeed in the script won't work.

„communication protocol"	((A))	for software developers
„configurational manual reader"	((B))	for commissioning
„installation manual reader"	((C))	Setup and installation
"installation manual antenna"	((D))	Setup and installation
„EPCGlobal standard"	((E))	for software developers
„Putty is SSH and Telnet-Client"	((F))	for software developers

((E))   EPCTM Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID in version V1.2.0 : www.epcglobalinc.org

address	contact
Kathrein RFID	E-Mail: rfid-sales@kathrein-rfid.de
Kronstaudener Weg 1	Internet: www.kathrein-rfid.de
D-83071 Stephanskirchen	