

```

<!--Get EPCs, CommandID: 0x0101-->
<Action>
    <Description>Get EPCs</Description>
    <CommandID>0101</CommandID>
    <!--LSB first-->
</Action>
</ActionlistActions>
    
```

The example above shows the *Activate buzzer 500 ms* and *Get EPCs* actions.

16.7 Expert Settings 1

The ReaderStart software is a powerful tool for the reader configuration. 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.

There are eight parameter sets available for saving the reader configuration. It is possible to save all settings for the transmission power, the antenna multiplex configuration, the RF settings and the air interface parameters.

Other parameters can be changed in *Expert settings 2*.

- For more information about the individual parameters, refer to *Reader Configuration Manual for Kathrein RFID UHF Readers*.

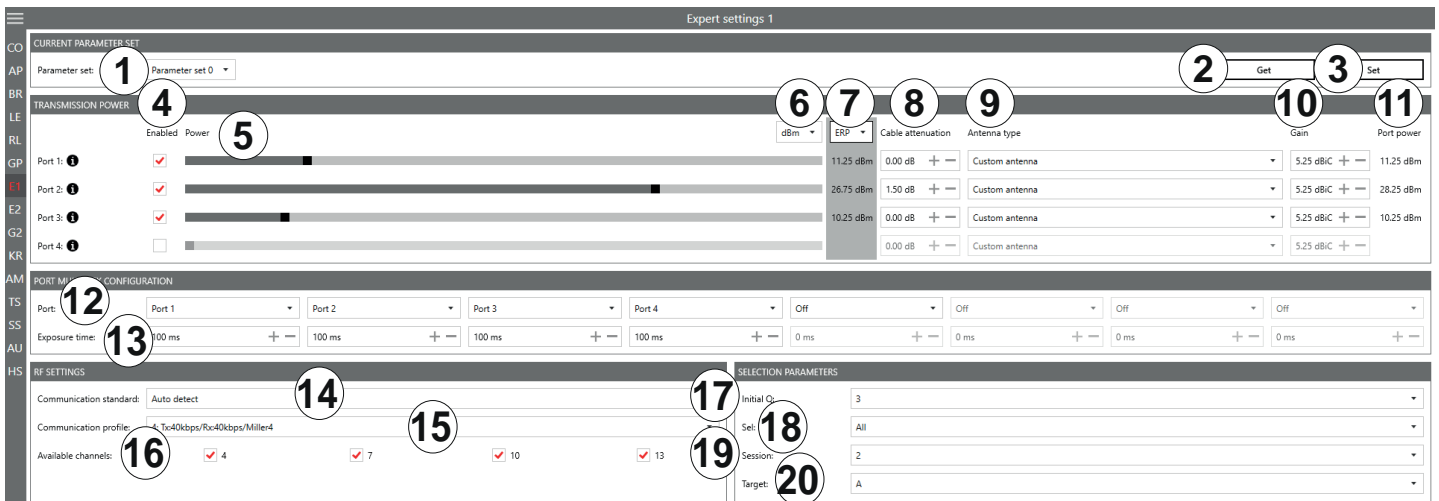


Fig. 67: Expert settings 1

①	<i>Parameter Set</i>	selects a parameter set
②	<i>Get</i>	reads the current settings of the selected parameter set in the system
③	<i>Set</i>	sets the parameters
④	<i>Enabled</i>	activates/deactivates the possibility to make changes in the port
⑤	<i>Power</i>	changes the power on the port (ERP)
⑥	<i>dBm/W</i>	switches between <i>dBm</i> and <i>W</i>
⑦	<i>ERP/EIRP</i>	switches between <i>ERP</i> and <i>EIRP</i>
⑧	<i>Cable attenuation</i>	selects cable attenuation in the range between 0 and 63.75 dB

⑨	<i>Antenna type</i>	selects the antenna type between pre-defined and custom antennas If the pre-defined antenna is selected, the programme sets the antenna gain to the maximum value permitted for this antenna. If <i>Custom antenna</i> is selected, it is possible to freely set the gain and power.
⑩	<i>Gain</i>	selects the antenna gain between -32.00 dBiC and 31.75 dBiC
⑪	<i>Port power</i>	shows the selected power on the port
⑫	<i>Port</i>	selects the antenna port or deactivates it If the antenna is not activated, the system proceeds to the next antenna in the <i>Port Multiplex Configuration</i> . ► For more details, refer to the Chapter MultiplexingAntennaport1...8 in the <i>Reader Configuration Manual</i> .
⑬	<i>Exposure time</i>	specifies the exposure time on the antenna; only used for asynchronous operation ► For more details, refer to the Chapter MultiplexingExposureTime1...8 in the <i>Reader Configuration Manual</i> .
⑭	<i>Communication standard</i>	selects a country-specific communication standard; the device version determines which communication standard is permitted
⑮	<i>Communication profile</i>	selects the profile for the data rate and 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.
⑯	<i>Available channels</i> (only available for ETSI readers)	selects the channel for the reader to use Depending on the region, the reader transmits in the frequency range 865–868 MHz for Europe or 902–928 MHz for USA/Canada. In Europe, the number of channels to be used can be limited. For this reason, it is necessary to check the related check box for each channel the reader is to use. This way, it is possible to avoid using specific channels on which there is interference.
⑰	<i>Initial Q</i>	reflects the number of tags expected in the field; see also Chapter InitialQ in <i>Reader Configuration Manual</i>
⑱	<i>Sel</i>	specifies whether other parameters are of interest for an inventory of the tag population or not; see also Chapter QuerySel in <i>Configuration Manual for Kathrein RFID UHF Readers</i>
⑲	<i>Session</i>	sets which session the reader is to work with; see also Chapter Sessions in <i>Reader Configuration Manual</i>
⑳	<i>Target</i>	specifies which tags in the population should take part in the inventory; see also Chapter QueryTarget in <i>Configuration Manual for Kathrein RFID UHF Readers</i>



To operate the reader in accordance with the related national standards, it is necessary to take into account the antenna gain and the cable attenuation in the transmission power setting.

- Do not exceed the permitted transmission power. Failure to observe this instruction can result in non-compliant operation of the reader leading the termination of the type approval.



To operate the reader in accordance with the related national standards, it is necessary to set the correct communication profile to use the correct frequency range.

- Make sure to operate the reader in the correct country-specific frequency range. Failure to observe this instruction can result in non-compliant operation of the reader leading the termination of the type approval.

16.7.1 Port Power

In Europe, the radiated power is limited 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, it is necessary to reduce the RF power accordingly. While the European standard refers to a half-wave dipole, FCC part 15/RSS 210 refers to an isotropic radiator.

To set the port power, it is necessary to include the length-dependent cable attenuation and the antenna gain into the calculation of the port power. An example for the calculation of the port power for Europe and FCC/IC is given below.

The following applies to the European approval region:

$$P_{\text{port}} = P_{\text{ERP}} + D_{\text{cable}} - G_{\text{HW}}$$

where P_{port} is the port power of the reader in dBm; P_{ERP} is the port power based on a half-wave dipole in dBm; D_{cable} is the cable attenuation in dB; G_{HW} is the antenna gain based on a half-wave dipole.

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

$$D_{\text{cable}} = l * D_{\text{dB/m}}$$

where D_{cable} is the cable attenuation in dB; l is the length in m; $D_{\text{dB/m}}$ is the 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.

$$G_{\text{HW}} = G_{\text{isot}} - 2.14 \text{ dB},$$

where G_{HW} is gain-based on a half-wave dipole and G_{isot} is 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 port power can be increased by 3 dB.

$$G_{\text{HW}} = G_{\text{isot}} - 2.14 \text{ dB} - 3\text{dB},$$

where G_{HW} is gain-based on a half-wave dipole and G_{isot} is gain-based on an isotropic radiator in dBi

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, it is necessary to reduce the RF power correspondingly. The reader's port power is then:

$$P_{\text{port}} = P_{\text{cond}} + D_{\text{kabel}} \text{ with } P_{\text{cond}} \leq 1\text{W} \text{ and } G_{\text{isot}} \leq 6\text{dB},$$

where P_{port} is the port power of the reader in dBm; P_{cond} is the power on antenna output in dBm; D_{cable} is the cable attenuation in dB; G_{HW} is the antenna gain in dBi.

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

The port power for the European variant can be set in 0.25-dB steps from 6 dBm to 33 dBm.

16.8 Expert Settings 2

The Expert settings 2 tab is divided into four sections for further configuration of the reader. In this tab, it is possible, for example, to change the default parameter set, copy one parameter set into another, read reader parameters to determine their ID and configure *Select Filter Settings*.

The screenshot shows the 'Expert settings 2' interface with the following sections:

- DEFAULT PARAMETER SET:** A dropdown menu for 'Default parameter set:' (currently 'Parameter set 0') and a 'Set' button.
- COPY PARAMETER SET:** Two dropdown menus for 'Source parameter set:' (currently 'Parameter set 0') and 'Target parameter set:' (currently 'Parameter set 0'), a 'Copy' button, and a progress bar.
- CHANGE READER PARAMETER:** A dropdown for 'Parameter id:' (currently 'GlobalDefaultParameterSet'), a radio button for 'Parameter value:' (currently 'dec'), a 'Get' button, and a 'Set' button.
- CONFIG PASSWORD:** Two input fields for 'Current password:' and 'New password:', and two 'Enter config password' buttons.
- SELECT FILTER SETTINGS:** Multiple dropdowns for 'Filter:', 'Target:', 'Action:', and 'Memory bank:', and input fields for 'On:', 'Bit pointer:', 'Mask length:', and 'Mask data:'. It also includes 'Save select filter data to file', 'Load select filter data from file', 'Get', and 'Set' buttons.

Fig. 68: Expert settings 2

16.8.1 Default Parameter Set

The *Default parameter set* allows configuration of the parameter set that is loaded from the Flash into the RAM when the reader is started.

The annotated screenshot highlights the following elements:

- 1:** The dropdown menu for 'Default parameter set:'.
- 2:** The 'Set' button for the default parameter set.
- 3:** The dropdown menu for 'Source parameter set:'.
- 4:** The dropdown menu for 'Target parameter set:'.
- 5:** The 'Copy' button.
- 6:** The progress bar for the copy operation.

Fig. 11: Expert settings 2: default parameter set and copy parameter set

①	<i>Default Parameter Set</i>	selects a default parameter set
②	Set	sets the selected default parameter set in the reader

16.8.2 Copy Parameter Set

The *Copy parameter set* allows one parameter set to be copied into another.

③	<i>Source parameter set</i>	selects the parameter set to be copied
④	<i>Target parameter set</i>	selects the parameter set into which the source parameter set is to be copied
⑤	Copy	<p>copies the parameter set</p> <ul style="list-style-type: none"> ▶ Click <i>Copy</i>. ☑ On successful completion of the copy operation, the <i>Copy</i> button briefly glows green and a corresponding message is displayed in the status field. ☑ If there is an error, the <i>Copy</i> button glows red, an error pop-up message appears and a warning is shown in the status field.
⑥		shows the progress of the copying process

16.8.3 Change Reader Parameter

Change reader parameter allows to change all reader settings using their respective configuration IDs.

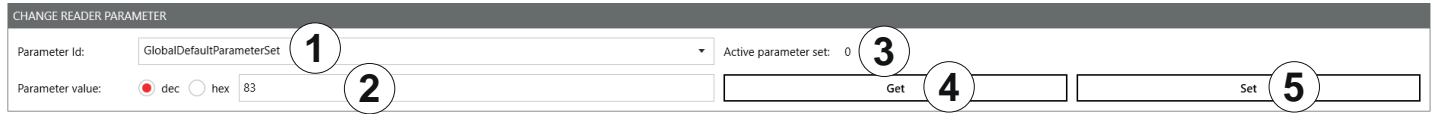


Fig. 12: Expert settings 2: change reader parameter

①	Parameter ID	selects the parameter ID
②	Parameter value	shows or sets the parameter value The value is either decimal or hexadecimal, it is possible to switch between <i>dec</i> and <i>hex</i> .
③	Active parameter set	shows the current active parameter set
④	Get	reads the value of the current parameter set of the reader and shows it at ②
⑤	Set	writes the parameter value (②) into the selected parameter ID (①)

16.8.4 Select Filter Settings

By means of these settings, it is possible to filter certain tags, e.g. to only read tags with the defined data in the respective memory banks. It is possible to set up to 32 filters.

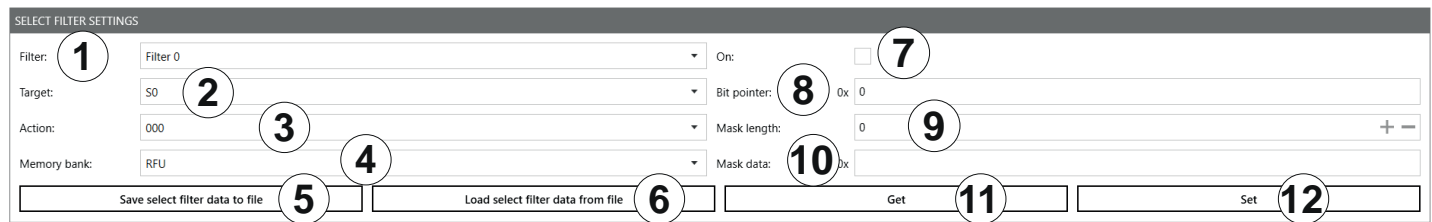


Fig. 69: Expert settings 2: select filter settings

①	Filter	selects a filter
②	Target	selects the tag target session ► Make sure the target matches the session set in ⑱ Fig. 67, p. 113.
③	Action	selects the action; see also <i>EPCglobal Gen 2 Specification</i> (p. 73) <div style="border: 1px solid gray; padding: 5px;"> <p>Tip ► To see the description of an action, hover over the <i>Action</i> field.</p> <p><input checked="" type="checkbox"/> ⇨ The description of the action appears in the tooltip:</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 5px;"> <p>Action: 100 Memory bank: EPC</p> <p>Matching: deassert SL or inventoried -> B Non-Matching: assert SL or inventoried -> A</p> </div> </div>
④	Memory bank	selects the memory bank (<i>RFU/EPC/TID/User</i>)
⑤	Save select filter data to file	saves the select filter data to file
⑥	Load select filter data to file	loads the select filter data from file
⑦	On	activates or deactivates the select filter
⑧	Bit pointer	sets from which memory address the filter compares the mask data

⑨	Mask length	sets the mask length (0–255)
⑩	Mask data	sets the data to be filtered
⑪	Get	reads the data of the filter selected at ①
⑫	Set	sets the select filter

Tip

In Generation 3 readers, select filter data are permanently stored in the reader, e.g. if the select filter has been activated, it is active after a reader restart.

16.8.5 Applying a Select Filter (Example)

You have the following results of the basic reading but you would like only the tags with the *FC28* in the memory address to take part in the inventory:

CO	AP	BR	LE	RL	EPC LENGTH	EPC	PORT	RSSI	RSSI DBM	READS	CYCLES	FIRST READ	LAST READ	FREQUENCY	TAG PHASE	MODE
					96	3034 F792 FC28 1800 001B CE7C	2	104	-64.7	250	3362	09:27:16:257	10:27:20:292	866.900 MHz	→	<input checked="" type="radio"/> Synchronous <input type="radio"/> Asynchronous <input type="checkbox"/> Listen for event <input type="button" value="Start"/> <input type="button" value="Stop"/> <input type="button" value="Clear"/>
					96	3034 F792 FC28 1800 001B CE7A	2	95	-71.3	252	3362	09:27:16:258	10:27:20:292	866.900 MHz	→	
					96	3034 F792 FC28 1800 001B CE7E	2	88	-76.8	252	3362	09:27:16:258	10:27:20:292	866.900 MHz	→	
					96	3034 F792 FC1A 31C0 0000 D47F	2	105	-63.7	117	3362	09:27:16:258	10:27:20:292	866.900 MHz	→	
					96	3034 F792 FC28 1800 001B CE73	2	87	-77.3	252	3362	09:27:16:258	10:27:20:292	866.900 MHz	→	
					96	3034 F792 FC28 1800 001B CE7C	2	104	-64.7	250	3362	09:27:16:257	10:27:20:292	866.900 MHz	→	

Fig. 13: Basic reading: select filter required

To do so, it is necessary to create a select filter. The advantage of this process is that the filtering takes place already at the air interface level.

To create the select filter as shown in the figure below:

SELECT FILTER SETTINGS

Filter: ① Filter 0 On: ⑤

Target: ② S2 Bit pointer: 0x 40 ⑥

Action: ③ 100 Mask length: 16 ⑦

Memory bank: ④ EPC Mask data: 0x FC28 ⑧

Save select filter data to file Load select filter data from file Get ⑨ Set

1. Select the filter you would like to save the filtering settings to under *Filter* (①).
2. Select the target (②). Make sure the target matches the session set in ⑨ Fig. 67, p. 113.
3. Select an action (③). In the example, the action is set to 100; see also *EPCglobal Gen 2 Specification*.
4. Select the *EPC* memory bank (④).
5. Activate the select filter (⑤).
6. Refer to the *EPCglobal Gen 2 Specification* to check from which bit pointer the filter will search for the value according to which you would like to filter the tags (*FC28* in the example); see pp. 44–46 in the *EPCglobal Gen 2 Specification V 2.0.1*. In the example, *FC28* is the third word in the EPC memory bank (bit pointer 0x00 is the CRC, bit pointer 0x10 is the PC, bit pointer 0x20 is the first EPC word). Therefore, *FC28* corresponds to the bit pointer 0x40.
7. Enter 40 at *Bit pointer* (⑥).
8. Enter the mask length at ⑦. In the example, *FC28* is one word, therefore, the value is 16.
9. Enter the value (*FC28*) at ⑧.
10. Click *Set* (⑨).
11. Go to *Expert settings 1*.
12. In *Selection Parameters*, set the value at target to *B*; see also *EPCglobal Gen 2 Specification*.
13. Start the reading in the *Basic reading* tab:

Basic reading											MODE		
	EPC LENGTH	EPC	PORT	RSSI	RSSI DBM	READS	CYCLES	FIRST READ	LAST READ	FREQUENCY	TAG PHASE	<input checked="" type="radio"/> Synchronous	<input type="radio"/> Asynchronous
CO	96	3034 F792 FC28 1800 001B CE7C	2	104	-64.7	309	3421	09:27:16:257	14:27:56:386	865.700 MHz	←	<input type="checkbox"/> Listen for event	<input type="button" value="Start"/>
AP	96	3034 F792 FC28 1800 001B CE7A	2	95	-71.3	311	3421	09:27:16:258	14:27:56:386	865.700 MHz	↓	<input type="button" value="Stop"/>	
BR	96	3034 F792 FC28 1800 001B CE7E	2	87	-77.3	311	3421	09:27:16:258	14:27:56:386	865.700 MHz	→		
LE	96	3034 F792 FC1A 31C0 0000 047F	2	105	-63.7	117	3421	09:27:16:258	10:27:20:292	866.900 MHz	←		
RL	96	3034 F792 FC28 1800 001B CE73	2	87	-77.3	311	3421	09:27:16:258	14:27:56:386	865.700 MHz	←		

⇒The reader only reads the tags with the filtered value (marked green). The tag without the filtered value is not read (marked red).

16.9 Test Gen 2 Functions

This tab makes it possible to access individual tag functions. In addition to the functionality in accordance with the EPC Gen2 standard, it is possible, for example, to read and write tags as well as set and change tag passwords.

The user interface consists of the fields *Get all Tags*, *Password for Operation*, *Write EPC*, *Read data*, *Write data*, *Change Password*, *Lock* and *Kill* that are described in the following chapters.

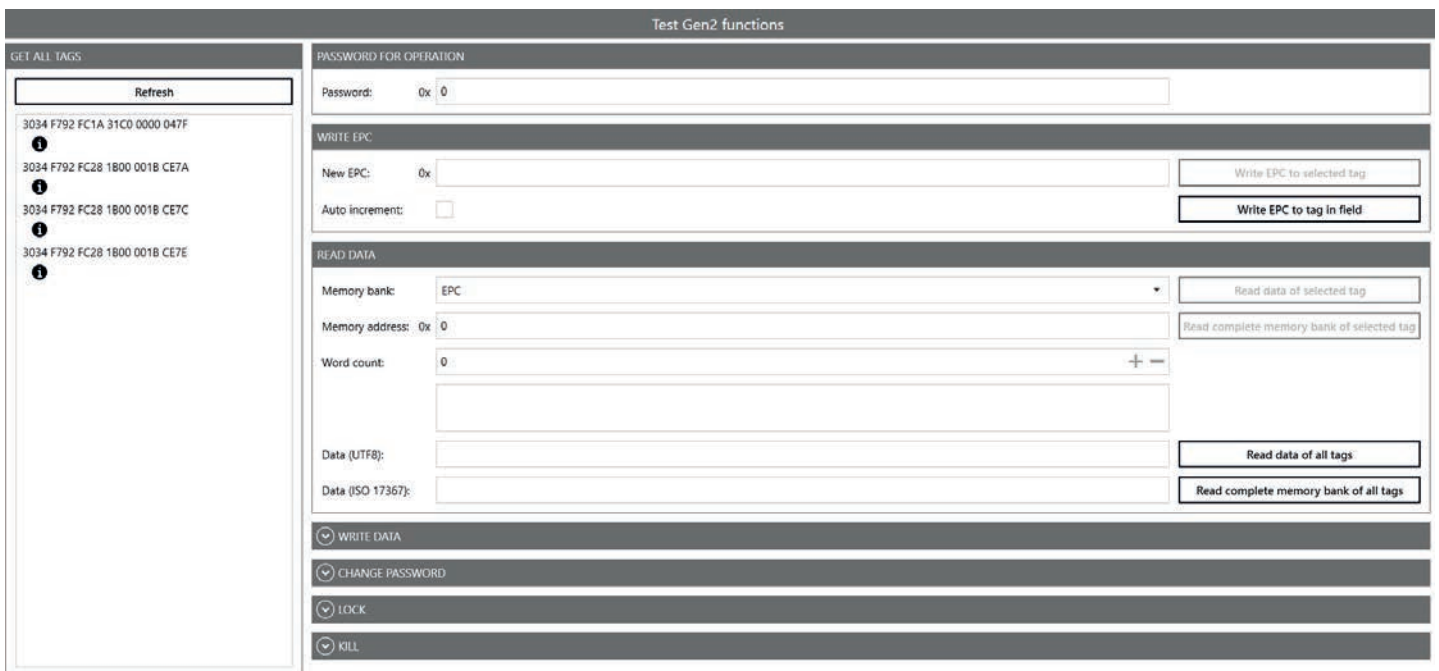


Fig. 70: Test Gen2 functions

16.9.1 Get All Tags

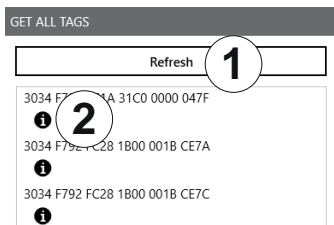


Fig. 71: Test Gen2 functions: Get all EPCs

①	<i>Refresh</i>	updates the tags read in the field ▶ For EPC-specific operations, click on a tag to select it from the list.
---	----------------	---

<p>② Info</p>	<p>shows the information about the tag manufacturer and the chip type</p> <p>► Click on the information symbol.</p> <p>⇒The information about the tag is shown:</p> <pre> 3034 F792 FC1A 31C0 0000 047F Manufacturer: Impinj Type: Monza R6 3034 F792 FC28 1B00 001B CE7A Manufacturer: NXP Type: UCODE 7 SL3S1204 3034 F792 FC28 1B00 001B CE7C </pre>
---------------	---

16.9.2 Password for Operation

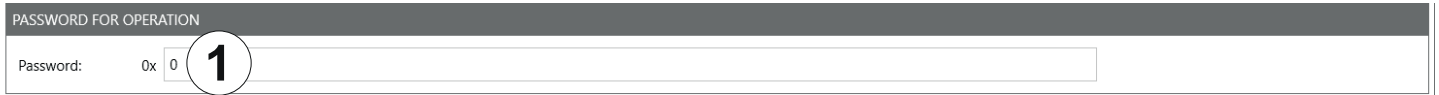


Fig. 14: TestGen2: password for operation

① <i>Password</i>	sets the password for the tag operation in the hexadecimal format
-------------------	---

16.9.3 Write EPC

In this tab, it is possible to change the EPC of the tag.

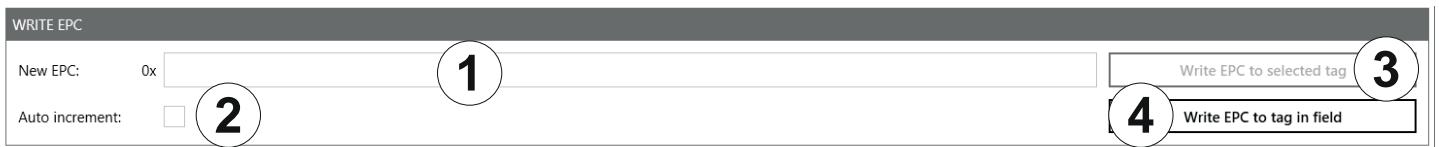



Fig. 72: TestGen2: write EPC

① <i>New EPC</i>	<p>enters an EPC in the hexadecimal format</p> <div style="border: 1px solid gray; padding: 10px; background-color: #f0f0f0;"> <p>! Make sure to comply with the maximum EPC length supported by the tag. If the maximum length is exceeded, the tag will return an error.</p> </div>
② <i>Auto increment</i>	activates or deactivates increasing the EPC by one with each successful writing process
③ <i>Write EPC to selected tag</i>	writes the EPC on the selected tag
④ <i>Write EPC to tag in field</i>	<p>writes the EPC entered in 1 to a single tag</p> <p>► When using this command, make sure there is only one tag in the field. Otherwise, an error message is displayed in the status field.</p>

16.9.4 Read Data

This group 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.

Fig. 73: TestGen2: read data

①	<i>Memory bank</i>	enters the selected memory bank
②	<i>Memory address</i>	enters the address within the memory bank
③	<i>Word count</i>	enters the number of words to read
④	<i>Data (UTF8)</i>	shows the data in the UTF8 format
⑤	<i>Data (ISO 17367)</i>	shows the data in the ISO 17367 format
⑥	<i>Read data of selected tag</i>	reads data from the selected tag
⑦	<i>Read complete memory bank of selected tag</i>	reads the complete memory bank of the selected tag; up to 255 words
⑧	<i>Read data of all tags</i>	reads data from all tags in the field <div style="border: 1px solid black; padding: 10px; margin-top: 10px;">  <p>If the tags in the field have different passwords and are configured differently, it is necessary to read the data from each tag individually.</p> </div>
⑨	<i>Read complete memory bank of all tags</i>	reads the complete memory bank of all tags in the field; up to 255 words

16.9.5 Write Data

WRITE DATA

Memory bank: EPC **1**

Memory address: 0x **2**

Data: **3** 0x 0

Data (UTF8): **4**

Data mask: **5** 0x 0


6 Write data to selected tag

7 Write masked data to selected tag

8 Write data to all tags

Write masked data to all tags **9**

Fig. 74: TestGen2: write data

1	<i>Memory bank</i>	enters the selected memory bank
2	<i>Memory address</i>	enters the address within the memory bank
3	<i>Data</i>	enters data to write in the hexadecimal format
4	<i>Data (UTF8)</i>	enters data to write in the UTF8 format
5	<i>Data mask</i>	enters the data mask The data mask allows only individual bits on the tag to be changed.
6	<i>Write data to selected tag</i>	writes data to the selected tag in the field
7	<i>Write masked data to selected tag</i>	writes the masked data to the selected tag
8	<i>Write data to all tags</i>	write data to all tags in the field <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> ! If the data are written to all tags in the field, make sure all the tags have the same configuration (lock and password).</div>
9	<i>Write masked data to all tags</i>	writes the masked data to the all tags in the field

16.9.6 Change Password

To change the password, enter the current password at ① in Fig. 74, p. 117. If no password has yet been set, the default value is 0.

Fig. 75: TestGen2: change password

①	<i>New password</i>	sets the new password in the hexadecimal format for the selected tag
②	<i>New kill password</i>	sets the new password to deactivate the selected tag
③	<i>Set password on selected tag</i>	replaces the old password by the new password for the selected tag
④	<i>Set kill password on selected tag</i>	replaces the old deactivation password by the new deactivation password for the selected tag

16.9.7 Lock


The *EPC Gen2* 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 *Lock*, it is possible to lock the memory banks.


The screenshot shows the 'LOCK' configuration window. It contains five dropdown menus, each with 'No change' selected. The dropdowns are labeled: Kill password (1), Access password (2), EPC memory bank (3), TID memory bank (4), and User memory bank (5). To the right of these dropdowns are two buttons: 'Lock selected tag' (6) and 'Lock all tags' (7).

Fig.76: TestGen2: Lock

①	<i>Kill password</i>	<p>specifies how the kill password is accessible</p> <ul style="list-style-type: none"> ► Select one of the following options from the drop-down menu: <table border="1"> <tbody> <tr> <td><i>No change</i></td> <td>the current setting for the kill password remains unchanged</td> </tr> <tr> <td><i>Accessible</i></td> <td>the kill password is readable and writeable from either the open or secured state</td> </tr> <tr> <td><i>Accessible with permalock</i></td> <td>the kill password is permanently readable and writeable from either the open or secured states and may never be locked</td> </tr> <tr> <td><i>Accessible with password</i></td> <td>the kill password is readable and writeable from the secured state but not from the open state</td> </tr> <tr> <td><i>Not accessible with permalock</i></td> <td>the kill password is not readable or writeable from any state</td> </tr> </tbody> </table> <ul style="list-style-type: none"> ► For more details, see <i>EPCGlobal Gen2 Specification</i>. 	<i>No change</i>	the current setting for the kill password remains unchanged	<i>Accessible</i>	the kill password is readable and writeable from either the open or secured state	<i>Accessible with permalock</i>	the kill password is permanently readable and writeable from either the open or secured states and may never be locked	<i>Accessible with password</i>	the kill password is readable and writeable from the secured state but not from the open state	<i>Not accessible with permalock</i>	the kill password is not readable or writeable from any state
<i>No change</i>	the current setting for the kill password remains unchanged											
<i>Accessible</i>	the kill password is readable and writeable from either the open or secured state											
<i>Accessible with permalock</i>	the kill password is permanently readable and writeable from either the open or secured states and may never be locked											
<i>Accessible with password</i>	the kill password is readable and writeable from the secured state but not from the open state											
<i>Not accessible with permalock</i>	the kill password is not readable or writeable from any state											
②	<i>Access password</i>	<p>specifies how the access password is accessible</p> <ul style="list-style-type: none"> ► Select an option from the drop-down menu; see the options at ①. ► For more details, see <i>EPCGlobal Gen2 Specification</i>. 										
③	<i>EPC memory bank</i>	<p>specifies how the EPC memory bank is accessible</p> <ul style="list-style-type: none"> ► Select one of the following options from the drop-down menu: <table border="1"> <tbody> <tr> <td><i>No change</i></td> <td>the EPC memory remains unchanged</td> </tr> <tr> <td><i>Writeable</i></td> <td>the EPC memory bank is writeable from either the open or secured states</td> </tr> <tr> <td><i>Writeable with permalock</i></td> <td>the EPC memory bank is writeable from either the open or secured states and may never be locked</td> </tr> <tr> <td><i>Writeable with password</i></td> <td>the EPC memory bank is writeable from the secured state but not from the open state</td> </tr> <tr> <td><i>Not writable with permalock</i></td> <td>the EPC memory bank is not writeable from any state</td> </tr> </tbody> </table>	<i>No change</i>	the EPC memory remains unchanged	<i>Writeable</i>	the EPC memory bank is writeable from either the open or secured states	<i>Writeable with permalock</i>	the EPC memory bank is writeable from either the open or secured states and may never be locked	<i>Writeable with password</i>	the EPC memory bank is writeable from the secured state but not from the open state	<i>Not writable with permalock</i>	the EPC memory bank is not writeable from any state
<i>No change</i>	the EPC memory remains unchanged											
<i>Writeable</i>	the EPC memory bank is writeable from either the open or secured states											
<i>Writeable with permalock</i>	the EPC memory bank is writeable from either the open or secured states and may never be locked											
<i>Writeable with password</i>	the EPC memory bank is writeable from the secured state but not from the open state											
<i>Not writable with permalock</i>	the EPC memory bank is not writeable from any state											
④	<i>TID memory bank</i>	<p>specifies how the TID memory bank is accessible</p> <ul style="list-style-type: none"> ► Select an option from the drop-down menu; see the options at ③. 										
⑤	<i>User memory bank</i>	<p>specifies how the User memory bank is accessible</p> <ul style="list-style-type: none"> ► Select an option from the drop-down menu; see the options at ③. 										
⑥	<i>Lock selected tag</i>	locks the selected tag with the settings from ①–⑤										

⑦	<i>Lock all tags</i>	<p>locks all the tags with the settings from ①–⑤</p> <div style="border: 1px solid black; padding: 10px; background-color: #f0f0f0;">  <p>▶ To lock all the tags, make sure that all the tags have the same password.</p> </div>
---	----------------------	---

16.9.8 Kill



▶ To deactivate a tag, set a deactivation password that is not 0; see ② in *Fig. 78, p. 120*.
After a kill command, the tag will be unusable!



Fig. 77: TestGen2: kill

①	<i>Kill selected tag</i>	executes a kill command on the selected tag
②	<i>Kill all tags</i>	executes a kill command on all tags in the field

16.10 @KRAI

This tab allows changing KRAI-specific settings. The @KRAI tab is divided into several sections. *Port* and *Port Info* are always available, other sections depend on the antenna connected to the reader, e.g. *Polarisation*, *Direction* etc.

The Reader recognises the connected antennas at boot up, but it is also possible to manually recognise a single port or all ports under *Port*. *Port Info* displays the information about the antenna.

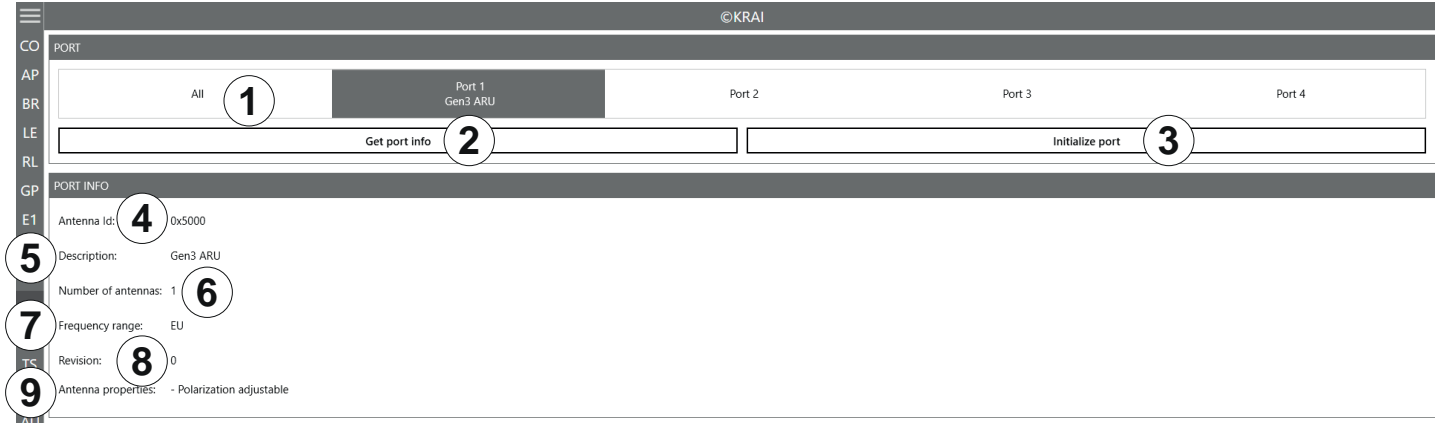


Fig. 78: @KRAI: polarisation

①	All/Port 1-4	selects either one or all antennas for <i>Initialise port</i> (③)
②	Get port info	retrieves port information for a selected @KRAI antenna
③	Initialise port	runs a query of the antennas on this port/these ports
④	Antenna Id	shows the antenna ID
⑤	Description	shows the description of the antenna
⑥	Number of antennas	shows the number of the antennas connected to the port
⑦	Frequency range	shows the frequency range the antenna operates in (<i>Global/EU/FCC</i>)
⑧	Revision	shows the hardware version of the antenna
⑨	Antenna properties	shows antenna properties, e.g. <i>polarisation adjustable</i> , <i>LEDs available</i>

Different configuration options are displayed, depending on the types of the connected antennas. The category *Polarisation* is shown for antennas with polarisation switching, the *Jumper Cable Attenuation* is available for smart shelf antennas, e.g. SMSH-30-30KRAI, *LED* is shown for @KRAI WIRA 70 and *Direction* for CSB KRAI antennas, e.g. WiRa 30°.

16.10.1 Polarisation

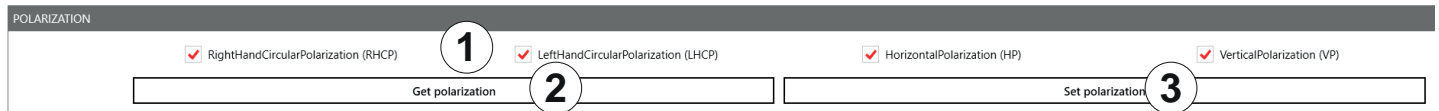


Fig. 79: @KRAI: polarisation

①		sets the polarisation of the antenna If there are several types of polarisation selected at the same time, the antenna configuration changes after every inventory.
②	<i>Get polarisation</i>	reads the current polarisation information of the antenna
③	<i>Set polarisation</i>	sets the polarisation on the antenna

16.10.2 LED

Depending on the features that are integrated in the antennas, it is possible to control/configure the LEDs.

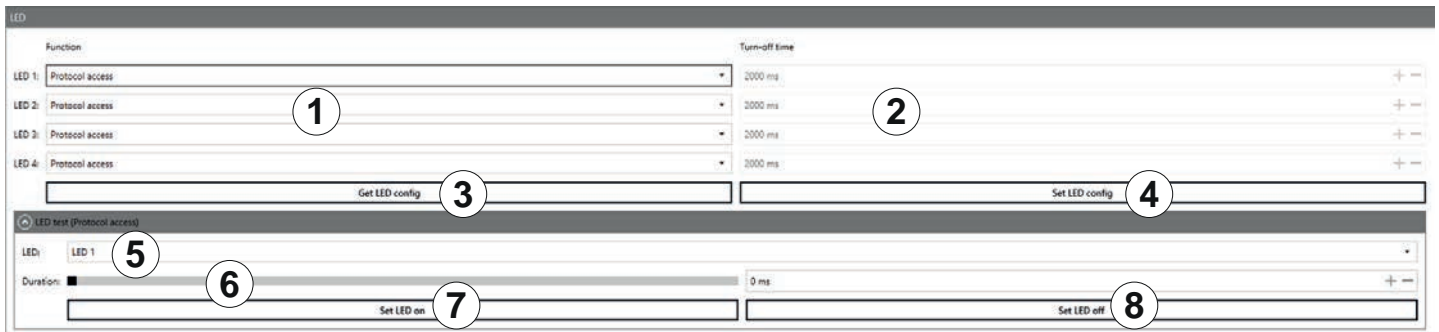


Fig. 80: @KRAI: LED

①	<i>LED 1-4</i>	selects the function of the LED 1-4 ► For functions, see Chapter <i>Selecting Functions</i> , p. 104
②	<i>Turn-off time</i>	sets the turn-off time for LED
③	<i>Get LED config</i>	shows the current LED configuration
④	<i>Set LED config</i>	sets the new LED configuration
⑤	<i>LED</i>	selects between LED 1-4
⑥	<i>Duration</i>	sets the duration of how long the LED is on; only if protocol access is selected in ①
⑦	<i>Set LED on</i>	switches the LED on for the duration in milliseconds selected in ⑥; if the duration is set to 65535 ms, the LED is permanently on
⑧	<i>Set LED off</i>	switches off the selected LED

16.10.3 Jumper Cable Attenuation

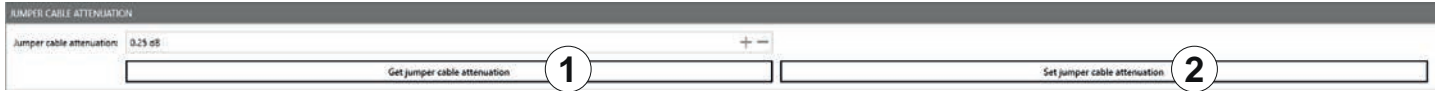


Fig. 81: @KRAI: jumper cable attenuation

①	<i>Get jumper cable attenuation</i>	reads the current jumper cable attenuation
②	<i>Set jumper cable attenuation</i>	sets the jumper cable attenuation

! 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 jumper cable attenuation is not calculated correctly.

16.10.4 Direction



Fig. 82: @KRAI: direction

①	<i>Left/Centre/Right</i>	sets the direction of the antenna If there are several types of direction selected at the same time, the antenna configuration changes after every inventory.
②	<i>Get direction</i>	reads the antenna direction(s) currently set in the antenna
③	<i>Set direction</i>	sets the selected direction(s) in the antenna

16.11 AppManager



This chapter gives a short overview of the apps, the requirements to operate them and the installation instructions.

► For more information on how to operate an app, refer to the user guide for the corresponding app.

16.11.1 Currently Available Apps

AccessManager

Automated vehicle identification (AVI) is one of the key markets that Kathrein Solutions is focusing on. AVI includes free flow identification, plaza and parking applications. For parking applications, Kathrein provides a specially configured software for access control called *AccessManager*.

The RRU 4xxx and ARU 3xxx series readers have a built-in industrial controller with Linux operating system. The entire application can be installed and configured directly on the reader. The system can be operated as an isolated solution without a network connection or alternatively via remote access over the network for configuration purposes or for database adaptations.

The *AccessManager* application software allows user-guided input and configuration of the transponder data that is to be captured. No programming knowledge is required in this case.

Flexible and efficient detection (e.g. of vehicles) is assured on the basis of the four digital inputs provided in Kathrein RFID systems which can be used for activation. A start point can be defined for the application in this way, whereby a light barrier or inductive ground contact is queried in order to activate the reading process.

Skidata

The Skidata app is a software-based solution that provides simple and easy interface integration of Kathrein RFID readers with Ethernet in the latest generation of Skidata barrier systems. With the Skidata app, the reader will become an officially certified SKIDATA compatible product.

Low Level Reader Protocol

Kathrein RFID readers are available with an optional LLRP (Low Level Reader Protocol) stack installable as an LLRP app. All readers with an integrated embedded Linux OS can be controlled via LLRP 1.0.1 port 5084 for easier integration. To specify air interface commands between readers and clients, LLRP is a ratified standard protocol from EPCglobal.

Profinet IO

The Profinet IO app allows the integration of a reader into a Profinet IO environment; the reader acts as an IO device. To run the app, a valid licence key is needed. Licence keys (either a full licence or a time limited demo licence) are bound to the specific reader the app is running on. For obtaining a licence key, the hardware key provided by the app is needed.

TagBlower

The TagBlower app can read tags asynchronously and generate messages, when a tag is coming or going. The app provides a server on a configurable port, where TCP clients can connect to receive those messages. The message format can be specified by the user by setting a coming and/or going datagram. A datagram consists of normal text and keywords.

16.11.2 Installing an App



This chapter describes installing an app shown on the example of *AccessManager*. You can install all other apps following the instructions described below.

- ✓ The *ReaderStart* software is installed.
- ✓ The reader is connected to a PC.

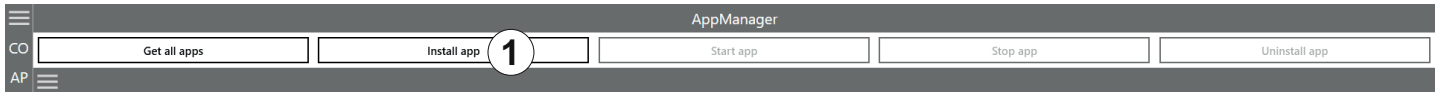


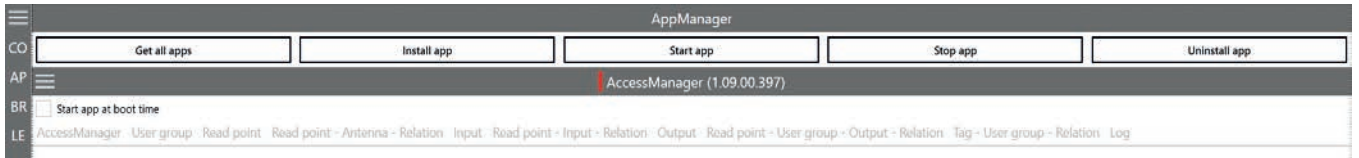
Fig. 15: AppManager: installing an app

1. Go to <https://www.kathrein-solutions.com/products/software/interface-software/accessmanager>.
2. Download the app.
3. If the downloaded app is in the zip format, extract a .tar file. Make sure not to extract the .tar file!
4. Start the *ReaderStart* software.
5. Go to the *AppManager* tab.
6. Click on *Install app* (①).
7. Select the file with the app. Make sure it is the .tar file.
8. Click *Open*.

⇒ A pop-up window to select the file with the app opens.

⇒ A pop-up message with the progress bar for the installation process appears for the duration of the installation.

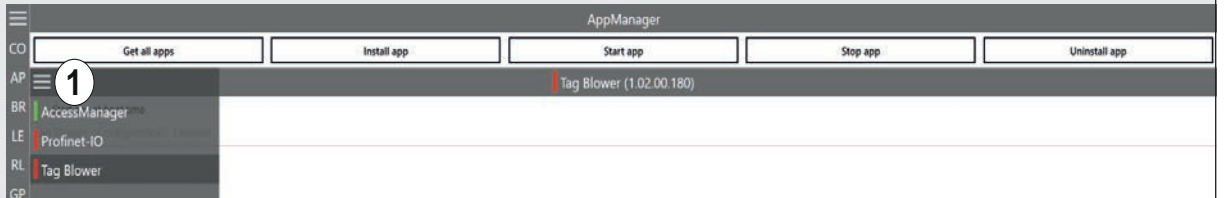
After the app has been successfully installed, the corresponding message is displayed in the status field and the app interface is shown in the *AppManager* tab:



Tip

- ▶ To see all the installed apps, click the menu symbol at (①).

☒ The installed apps are displayed:

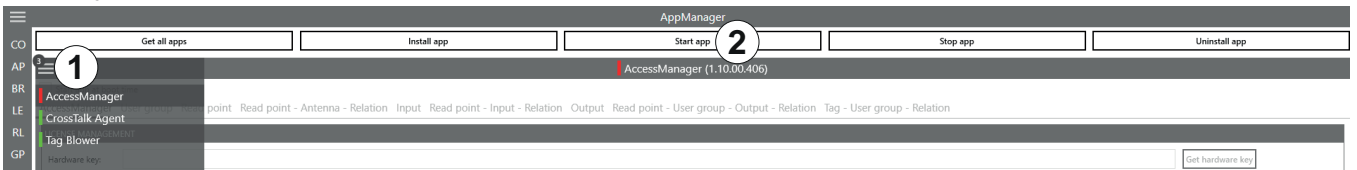


16.11.3 Activating an App License Key

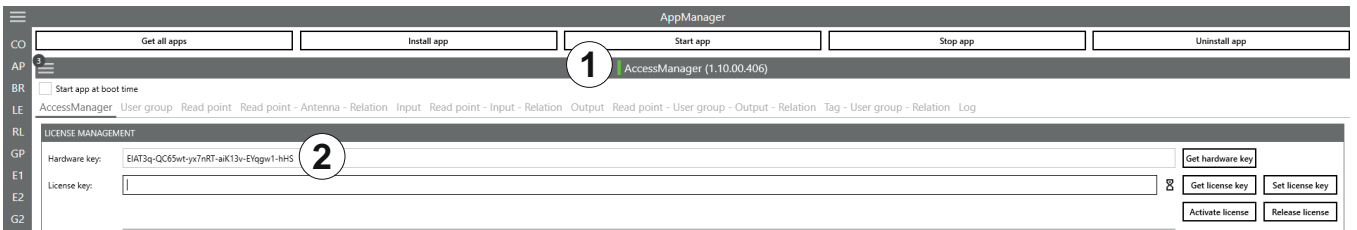
! This chapter describes activating the app license key shown on the example of *AccessManager*. You can activate all other apps in a similar way following the instructions described below.

- ✓ The *ReaderStart* software is installed and running on the PC.
- ✓ The reader is connected to the PC.
- ✓ The *AppManager* has been installed in the *ReaderStart* software, see *Installing an App*, p. 127.

1. Go to the *AppManager* tab.
2. To see all the installed apps, click the menu symbol at (1).
 - ⇒ The installed apps are displayed. The *AccessManager* is shown in red, which means the app has not been started yet:



3. Click *Start App* (2, see figure above).
 - ⇒ The *AccessManager* is started and is shown in green (1, see figure below). The hardware key is displayed at (2, see figure below):



! There are two options to activate the license key, one is a paid version, which you can only use if you have purchased the product and received the product key. There is, however, the demo version which is free of charge but limited to 8 hours if the app is running.

Activating the App License Key for the *AccessManager* Demo Version

There are two ways how to activate the license key for the *AccessManager* demo version, one using the Kathrein Solutions website and the *ReaderStart* software, the other using only the *ReaderStart* software.

Activating the App License Key for the *AccessManager* Demo Version By Using the Website and *ReaderStart*

This chapter describes how to activate the app license key using the Kathrein Solutions website and the *ReaderStart* software.

Fig. 83: *AccessManager*. Activating the app license key for the demo version using the website and *ReaderStart*

1. Copy the hardware key shown at ② (Step 3 in 17.11.3, p. 128).
2. Go to <https://www.kathrein-solutions.com/products/software/interface-software/accessmanager>.
3. Go to *AccessManager 1.10 Product Key Activation*.

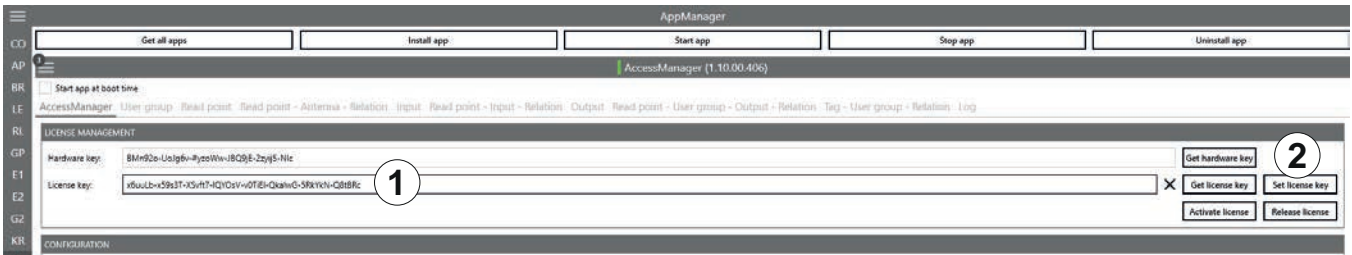
⇒The following is displayed:

4. If you have not purchased the *AccessManager* app, activate the *Demo* box (① in Fig. 87).
⇒The *Product key* field receives the *demo* entry and is deactivated (② in Fig. 87).
5. At *Hardware key* (③ in Fig. 87), enter the hardware key shown in *AppManager* (Step 3 in 17.11.3, p. 128).
6. Click *Activate*.

⇒A license key is generated. A pop-up window with the license key file in the PDF format appears (①). The license key is also displayed at (②):

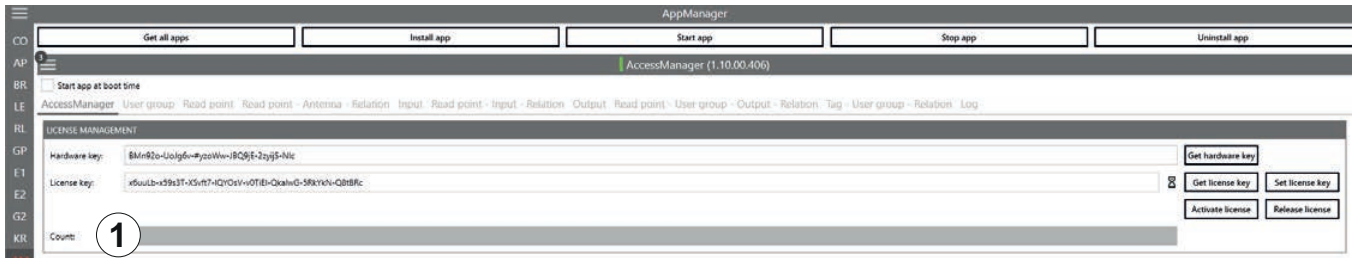
7. Copy the licence key from (②).

8. Save the PDF license key file (1).
9. Return to the *ReaderStart*, the *AppManager* tab.
10. Enter the license key copied from the website at *License key* (1):



11. Click *Set license key* (2).

⇒ The license has been activated for 8 hours if the app is running and the app can be used. You can see how much time you have left by checking the *Count* bar (1):



Activating the App License Key for the AccessManager Demo Version By Using the *ReaderStart* Software Only

This chapter describes how to activate the app license key using only the *ReaderStart* software.

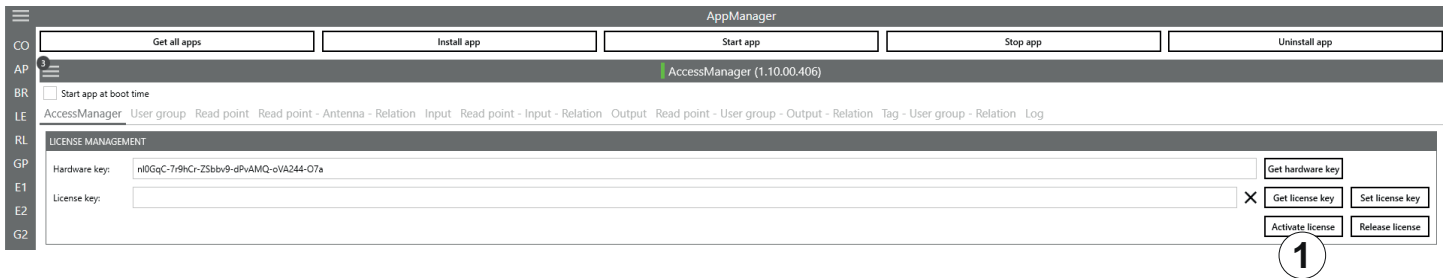


Fig. 16: *AccessManager*. Activating the app license key for the demo version using the *ReaderStart* software only

1. Perform Steps 1–3 in in 17.11.3, p. 128.
2. Click *Activate license*.
⇒ The following pop-up window appears:



3. Activate the *Demo* box (1).

⇒ The *Product key* field receives the *demo* entry and is deactivated (cf. 2 in Fig. 87). The hardware key is shows

at *Hardware key* (②):

Activate license

Product key: demo ① Demo

Hardware key: k*M*lg-yKx3Lx-e#gJ6x-Tvazri-7IZAP7-d8p ②

Comment:

License key:

Status: The product key or hardware key is invalid.

License: Save as PDF

③

4. Click *Get license online* (③).

⇒ If the operation has been successful, the tag count is shown at *Tag count* (④), the license key is shown at *License Key* (⑤), the *Status* (⑥) shows *Successful*:

Activate license

Product key: demo Demo

Hardware key: k*M*lg-yKx3Lx-e#gJ6x-Tvazri-7IZAP7-d8p

Comment:

Tag count: 5 ④

License key: zGmGtp-vWSPo5-EMaAir-mhmXm-1HjvoJ-uFpxul-HC#1ZS-e*mQGQ ⑤

Status: ⑥ Successful

License: Save as PDF ⑦

⑧

5. Activate the *Save as PDF* box (⑦) to save the license as a PDF file (cf. Step 8 in *Activating the App License Key for the AccessManager Demo Version By Using the Website and ReaderStart*, p. 129).

6. Click *Close* to close the window (⑧).

⇒ The license has been activated for 8 hours if the app is running and the app can be used. You can see how much time you have left by checking the *Count* bar (①) (cf. Step 11 in *Activating the App License Key for the AccessManager Demo Version By Using the Website and ReaderStart*, p. 129):

AppManager

Get all apps | Install app | Start app | Stop app | Uninstall app

AccessManager (1.10.00.406)

Start app at boot time

AccessManager User group Road point Road point Antenna Relation Input Road point Input Relation Output Road point User group Output Relation Tag User group Relation Log

LICENSE MANAGEMENT

Hardware key: BMn92o-UoJg6-#yzoWw-JBQ9E-2zjy5-Nlc

License key: x5ouLb-x59s3T-X5vt7-HQY0sv-vOTIE-QknhG-58kxNv-Q8BfC

Count: ①

Releasing the *AccessManager* License Key for the Demo Version

If you have purchased the app and want to activate the license on the same device, you will need to release the license key for the demo version. The same applies if you want to use the license on another device.

Releasing the *AccessManager* License Key for the Demo Version Using the *ReaderStart* Software Only

AppManager

Get all apps | Install app | Start app | Stop app | Uninstall app

AccessManager (1.10.00.406)

Start app at boot time

AccessManager User group Road point Road point Antenna Relation Input Road point Input Relation Output Road point User group Output Relation Tag User group Relation Log

LICENSE MANAGEMENT

Hardware key: BMn92o-UoJg6-#yzoWw-JBQ9E-2zjy5-Nlc

License key: x5ouLb-x59s3T-X5vt7-HQY0sv-vOTIE-QknhG-58kxNv-Q8BfC

①

Fig. 84: *AccessManager*: Release license

1. Click *Release license* (①).

⇒The following pop-up window appears:



2. Click *Yes* if you want to release the license. Click *No* if you want to cancel.

⇒The following pop-up window appears:



3. Click *OK*.

⇒The following pop-up window appears:

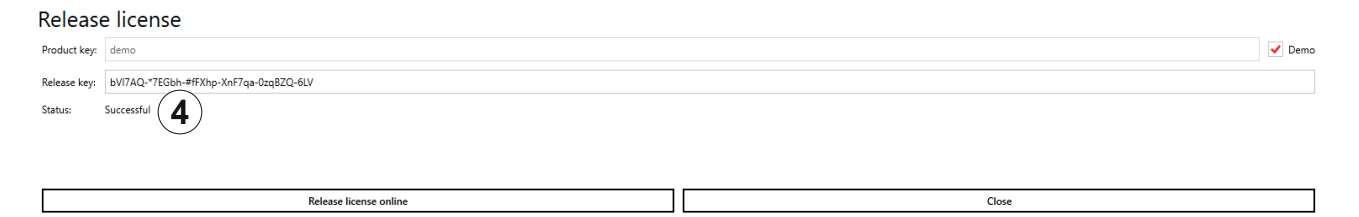


4. Activate the *Demo* box (①).

⇒The *Product key* field receives the *demo* entry and is deactivated (②), the *release key* is shown at (③), the *status* at (④).

5. Click *Release license online* to release the license.

⇒The *Status* changes to *Successful*:



6. Click *Close* to close the window.

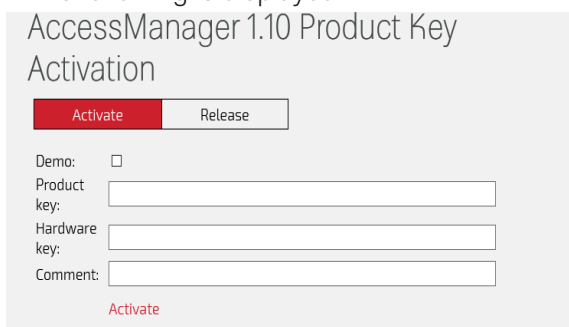
⇒The license has been released and the app can no longer be used, the count bar is not available.

Releasing the AccessManager License Key for the Demo Version Using the Website and ReaderStart

1. Perform Steps 1–4 in *Releasing the AccessManager License Key for the Demo Version Using the ReaderStart Software Only*, p. 131.
2. Copy the release key.
3. Go to <https://www.kathrein-solutions.com/products/software/interface-software/accessmanager>.

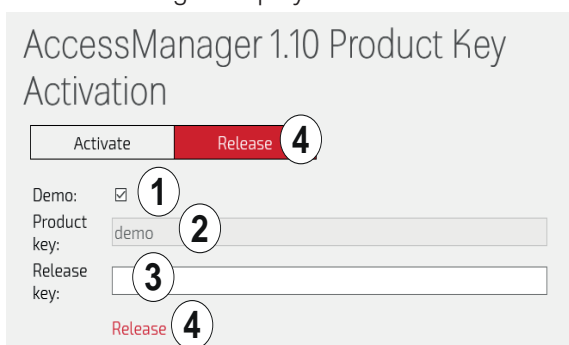
- Go to *AccessManager 1.10 Product Key Activation*.

⇒The following is displayed:



- Click *Release*.

⇒The following is displayed:



- Activate the *Demo* box (①).

⇒The *Product key* field receives the *demo* entry and is deactivated (②).

- At *Release key* (③), enter the release key copied from *AppManager* (Step 4 in *Releasing the AccessManager License Key for the Demo Version Using the ReaderStart Software Only*, p. 131).

- Click *Release* (④).

⇒The following is displayed:



- Click *OK* to close the message.

Activating the App License Key if You have Purchased *AccessManager*

If you have purchased the *AccessManager* app, there are two ways to activate the license key, one using the Kathrein Solutions website and the *ReaderStart* software, the other using only the *ReaderStart* software.

Activating the App License Key for the *AccessManager* App By Using the Website and *ReaderStart*

This chapter describes how to activate the app license key using the Kathrein Solutions website and the *ReaderStart* software.

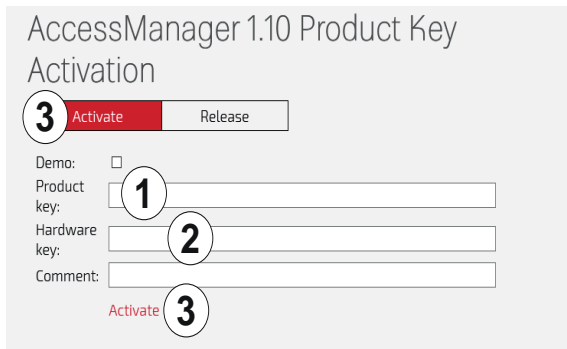
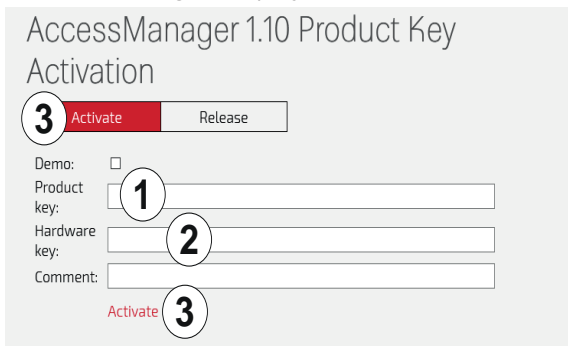


Fig. 85: *AccessManager*: Activating the app license key for the purchased version using the website and *ReaderStart*

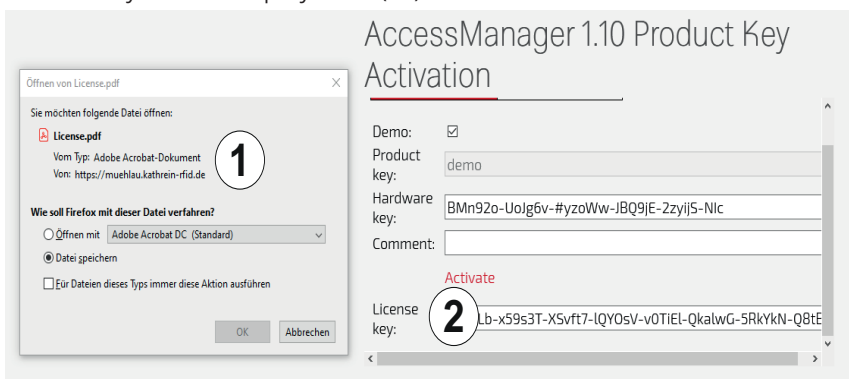
1. Copy the hardware key shown at ② (Step 3 in 17.11.3, p. 128).
2. Go to <https://www.kathrein-solutions.com/products/software/interface-software/accessmanager>.
3. Go to *AccessManager 1.10 Product Key Activation*.

⇒The following is displayed:



4. Enter the product key you have received when you purchased the app at ①.
5. At *Hardware key* (②), enter the hardware key shown in *AppManager* (Step 3 in 17.11.3, p. 128).
6. Click *Activate* at (②).

⇒A license key is generated. A pop-up window with the license key file in the PDF format appears (①). The license key is also displayed at (②):



Activating the App License Key for the *AccessManager* App By Using the *ReaderStart* Software Only

This chapter describes how to activate the app license key for the purchased *AccessManager* version using only the *ReaderStart* software.

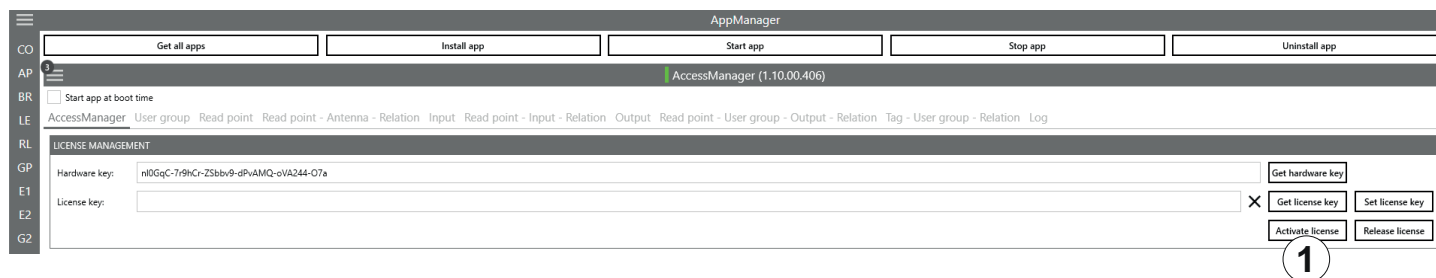


Fig. 86: *AccessManager*: Activating the app license key for the purchased version using the *ReaderStart* software only

1. Perform Steps 1–3 in in 17.11.3, p. 128.
2. Click *Activate license*.

⇒ The following pop-up window appears, the hardware key is shown at ②:

Activate license

Product key: ① Demo

Hardware key: k*M*lg-yKx3Lx-e#gJ6x-Tvazri-7IZAP7-dBp ②

Comment:

License key: ③

Status: ④

License: Save as PDF ⑤

⑥ ⑦

3. Enter the product key you have received when you purchased the app at ①.
4. Click *Get license online* (⑥).
 - ⇒ If the operation has been successful, the license key is shown at *License key* (③), the *Status* (④) shows *Successful*.
5. Activate the *Save as PDF* box (⑤) to save the license as a PDF file (cf. Step 8 in *Activating the App License Key for the AccessManager Demo Version By Using the Website and ReaderStart*, p. 129).
6. Click *Close* to close the window (⑦).

⇒ The license has been activated and the app can be used. You can see how much time you have left by checking the *Count* bar (①) (cf. Step 11 in *Activating the App License Key for the AccessManager Demo Version By Using the Website and ReaderStart*, p. 129).

16.12 TagScan

To represent the relationship between the tag phase and the RSSI value, it is possible to plot both values by means of the TagScan.

✓ There is only one tag in the field or a tag has been selected.

► Click *Start* to activate the TagScan.

⇒ The phase shifts are seen in the frequency switching. The RSSI value does not change because the transponder (tag) is not moved.

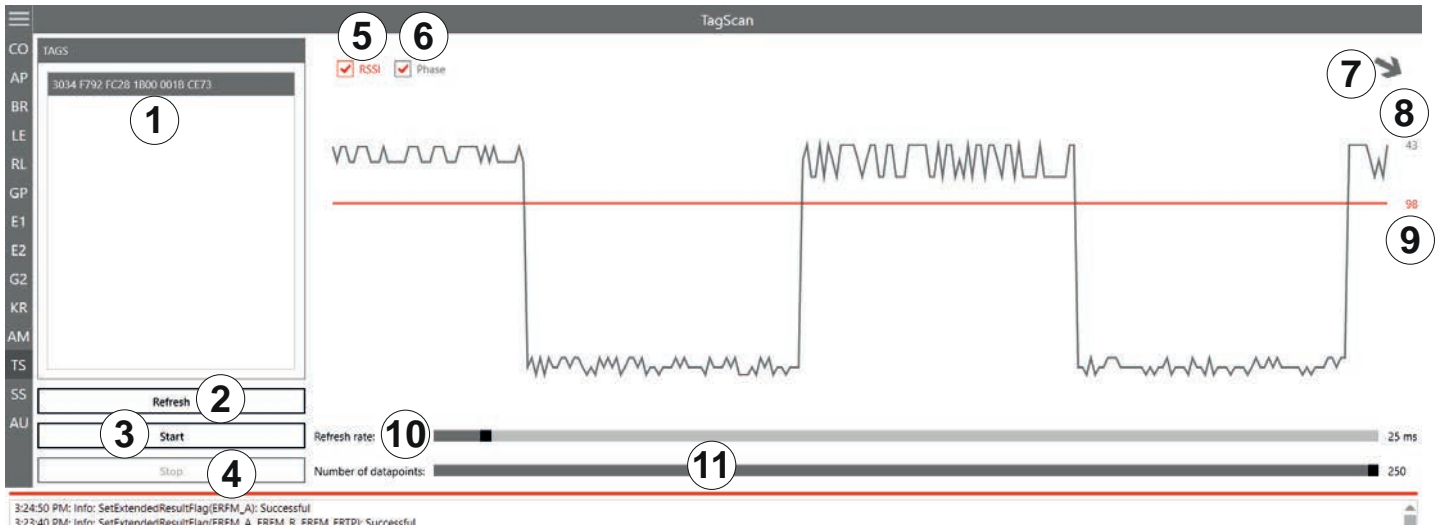


Fig. 87: TagScan: Phase shift (due to the channel change), transponder is not moved

①	<i>Tags</i>	shows the number of the tags present in the antenna field
②	<i>Refresh</i>	scans tags in the antenna field anew
③	<i>Start</i>	starts TagScan
④	<i>Stop</i>	stops TagScan
⑤	<i>RSSI</i>	activates/deactivates the presentation of the RSSI value in the graph
⑥	<i>Phase</i>	activates/deactivates the presentation of the phase in the graph
⑦		shows the phase in form of the rotating arrow
⑧		shows the current value of the phase
⑨		shows the current RSSI value
⑩	<i>Refresh rate</i>	sets the interval between the commands
⑪	<i>Number of data points</i>	sets the number of data points in the graph

Tip

► To eliminate the phase shifts, select only one transmission frequency under *Expert settings 1*; see *Expert Settings 1*, p. 110.

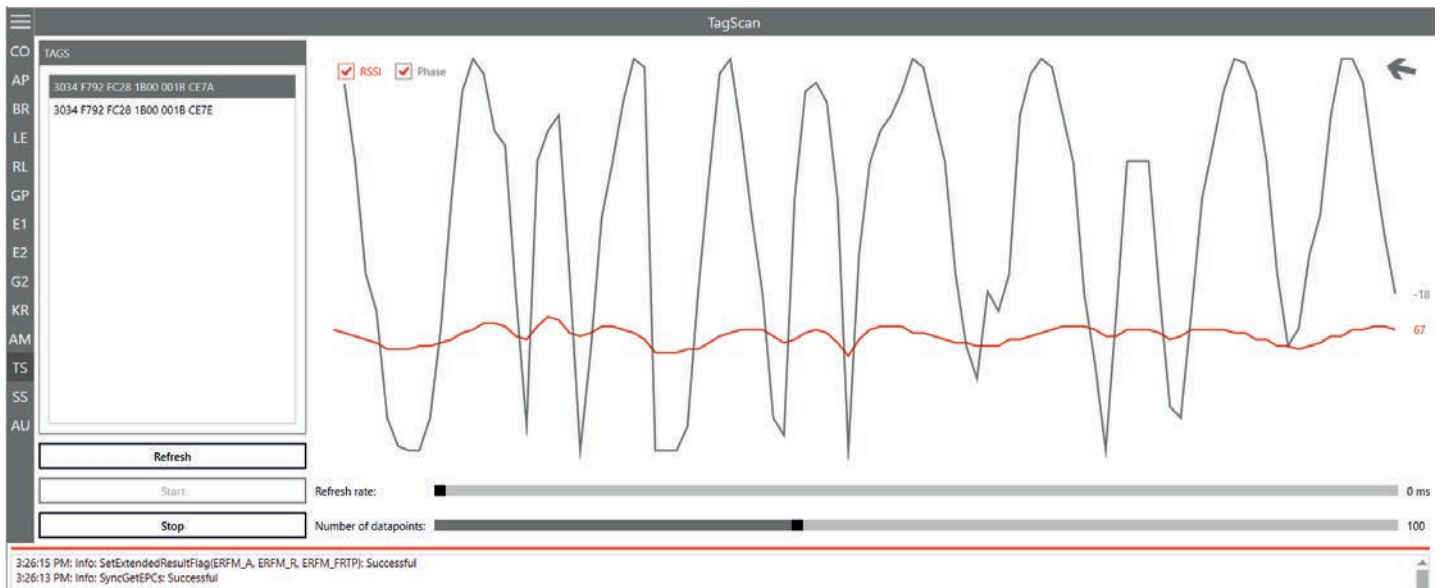


Fig. 88: TagScan: phase shift, transponder is moved

Transponder movement is indicated by the amplitude of the phase. The RSSI value changes in small steps. The direction of the movement is indicated by means of the rotating pointer.

16.13 Spectral Scan

It may happen that the RFID transmission to or from the transponder is disturbed by frequency interfering. *SpectralScan* shows a qualitative frequency spectrum. Due to the fact that it is received by means of the connected RFID antenna, the frequency assignment on location is made visible.

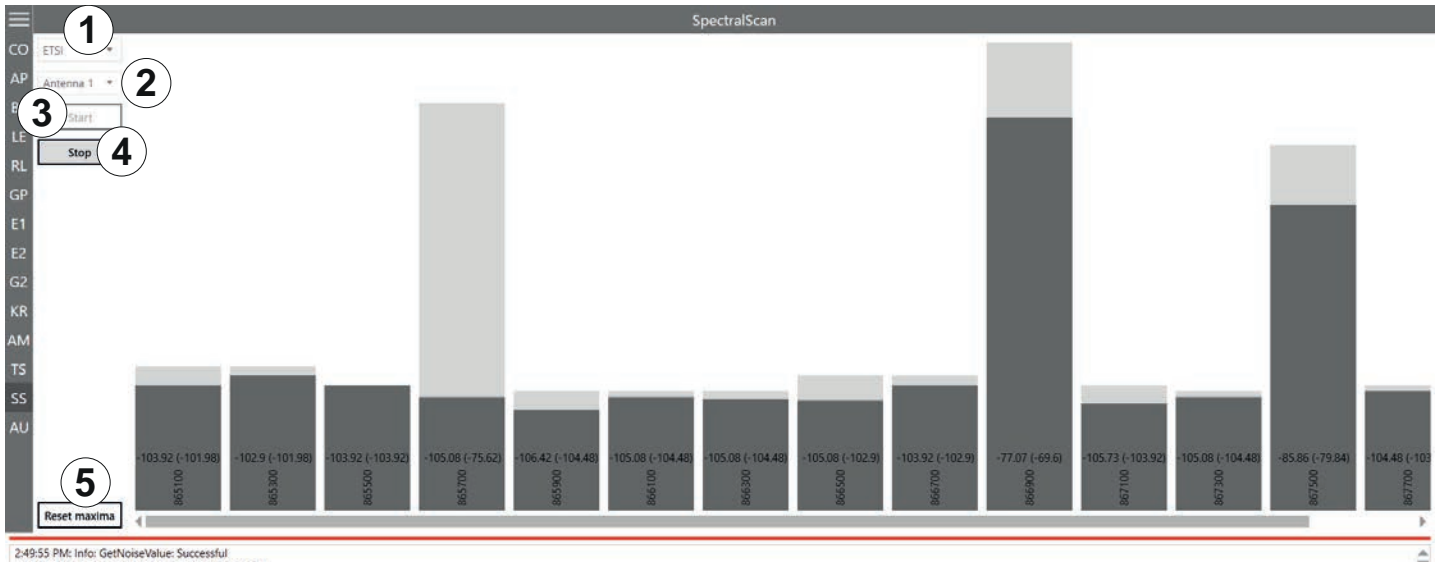


Fig. 89: SpectralScan

①	ETSI	selects the frequency area
②	Antenna 1-n	selects an antenna from the drop-down menu
③	Start	starts SpectralScan
④	Stop	stops SpectralScan
⑤	Reset maxima	resets maxima

If there is more than one reader, spectral scan shows which channels might be occupied by other readers. In Fig. 93, p. 137, the channels 4, 10 and 13 are occupied by other readers. If the user is not satisfied with the reading results and the interferences keep occurring, it is possible to deactivate channels on which the interference occurs (4, 10 and 13) and only activate the channel that is free (7) to achieve better reading results, see ⑩ in Fig. 66, p. 112.

16.14 Authentication

Using this function, it is possible to authenticate a tag.

The Authentication tab consists of 4 areas, *Get All Tags*, *Tags*, *Key* and functions that are described below.

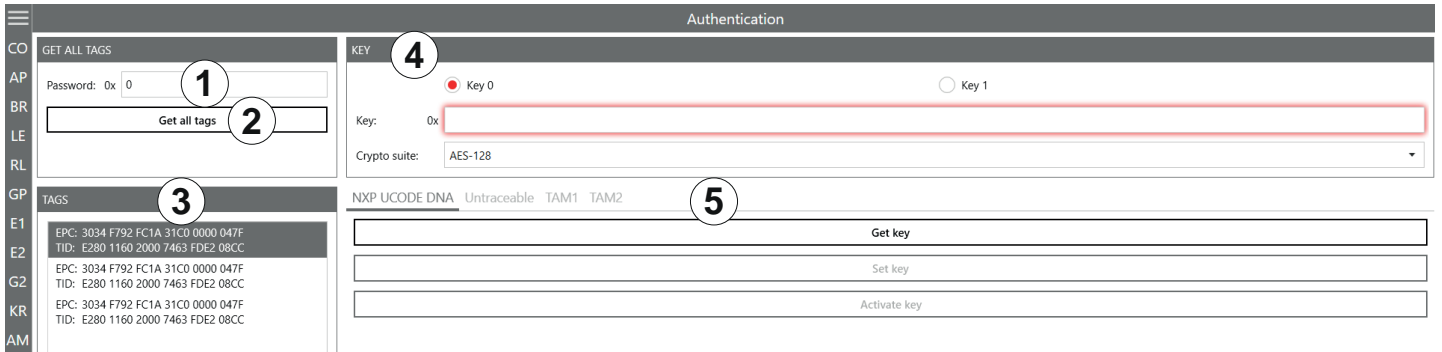


Fig. 90: Authentication

①	<i>Password</i>	enters the access password; see <i>Password for Operation</i> , p. 117
②	<i>Get all tags</i>	reads all the tags in the antenna field
③	<i>Tags</i>	shows all the detected tags
④	<i>Key</i>	see <i>Key</i> , p. 139; necessary for TAM1 and TAM2
⑤	<i>Functions</i>	see <i>Functions</i> , p. 140

16.14.1 Key

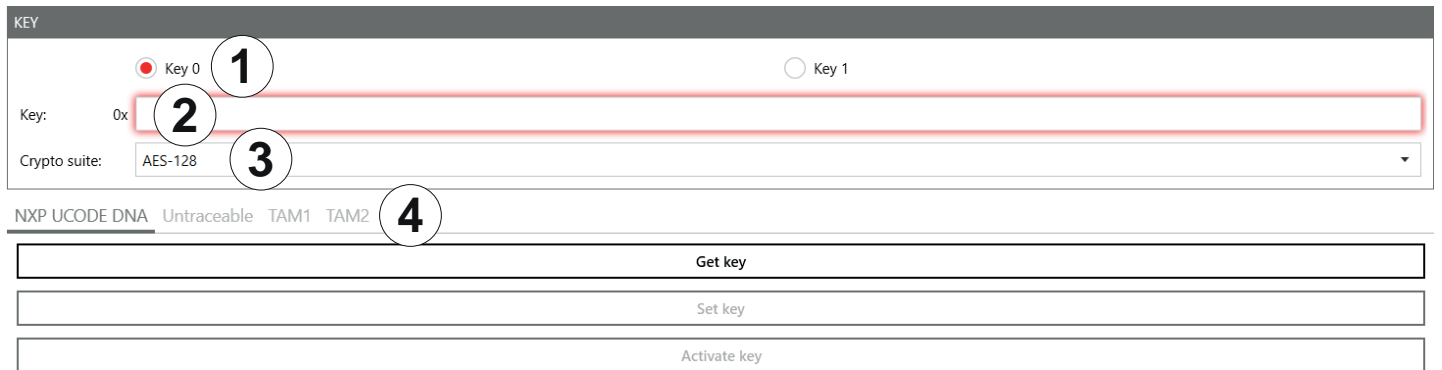


Fig. 91: Authentication: Key

①	<i>Key 0/Key 1</i>	selects a key for the authentication (<i>Key 0</i> is only used for TAM1, <i>Key 1</i> is used for both TAM1 and TAM2)
②	<i>Key</i>	enters the key selected in ①
③	<i>Crypto suite</i>	selects the crypto suite
④		see <i>Functions</i> , p. 140

16.14.2 Functions

NXP UCODE DNA

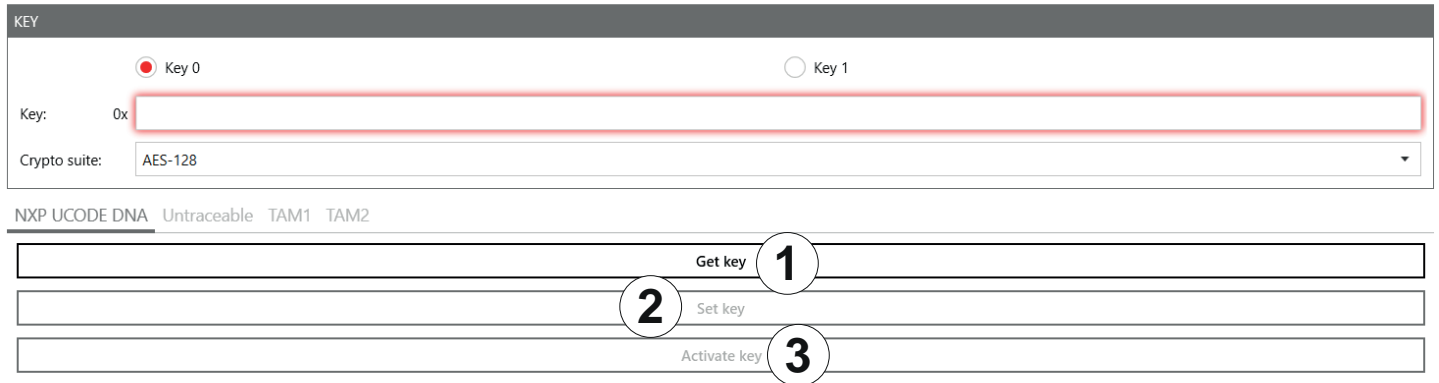


Fig. 92: Authentication: NXP UCODE DNA

①	<i>Get key</i>	reads key 0 or key 1 currently set in the selected tag; only if the key has not been activated
②	<i>Set key</i>	sets key 0 or key 1 on the selected tag
③	<i>Activate key</i>	activates key 0 or key 1 on the selected tag

Untraceable

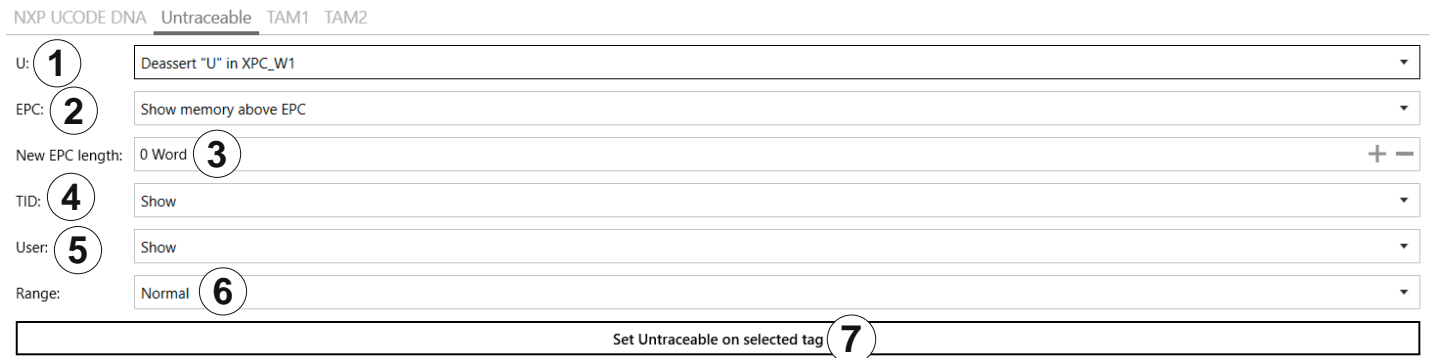


Fig. 17: Authentication: untraceable

①	<i>U:</i>	asserts or deasserts U in XPC_W1; see <i>EPCglobal Gen2 Specification, p. 106</i>
②	<i>EPC</i>	shows or hides memory above the visible EPC
③	<i>New EPC length</i>	sets new EPC length in words
④	<i>TID</i>	<i>Show</i> shows the complete TID
		<i>Truncated</i> shows the first two words in case of E2 and only one word in case of E1
		<i>Hide</i> hides the complete TID
⑤	<i>User</i>	shows or hides the user memory bank

⑥	Range	selects a range
		<i>Normal</i> the tag operates in the normal range
		<i>Toggle temporarily</i> The tag temporarily toggles between normal and reduced operating range but reverts to its prior persisting operating range when the tag loses power
		<i>Reduced</i> the tag operates in the reduced operating range
⑦	Set Untraceable on selected tag	sets settings 1–6 on the selected tag

TAM1

TAM1 is used to check whether the selected tag is authentic.

✓ The tag has at least one activated key, *Key 0* or *Key 1*.

The screenshot shows the 'KEY' configuration screen. At the top, there are two radio buttons for 'Key 0' (with a circled 1) and 'Key 1' (with a red dot). Below, the 'Key:' field contains the hexadecimal value '1111E2C068920000003A1E34C0501111'. The 'Crypto suite:' dropdown is set to 'AES-128'. Below the key configuration, there are tabs for 'Untraceable', 'TAM1', and 'TAM2'. A large button labeled 'Authenticate selected tag' (with a circled 2) is visible. Below this, three lines of data are shown: 'RRU → Tag: 09 68 EE D1 35 E5 E8 1E 14 A7' (with a circled 3), 'RRU ← Tag: A4 C1 96 45 0E D7 3B E7 0D 56 40 1F 60 CF BF B0' (with a circled 4), and 'AES Decryption: 96 C5 DB B1 17 41 09 68 EE D1 35 E5 E8 1E 14 A7' (with a circled 5).

Fig. 18: Authentication: key (TAM1)

	<i>Key</i>	see <i>Key</i> , p. 139
①	<i>Authenticate selected tag</i>	the reader sends the authenticate command to the selected tag; a pop-up message appears whether the authentication was successful or failed.
②	<i>RRU → Tag</i>	shows the random number sent to the tag by the reader
③	<i>RRU ← Tag</i>	shows the encrypted random number sent to the reader from the tag
④	<i>AES Decryption</i>	shows the data decrypted from ③ by means of the key entered at ② in <i>Authentication: Key</i> , p. 139; in the example above, this data contains the random number shown in ②

TAM2

TAM2 is used to read the data of the selected tag.

✓ *Key 1* has been activated.

Fig. 92: Authentication: key (TAM2)

①	<i>Profile</i>	selects a profile the data of which is shown
②	<i>Offset</i>	sets the offset for ⑤
③	<i>Block count</i>	sets how many bits rare to be read
④	<i>Protection mode</i>	selects the protection mode for the TAM2 authentication operation
⑤	<i>Read data of selected tag</i>	reads the data of the selected tag provided the correct key 1 has been entered at <i>Key</i>
⑥	<i>Data</i>	shows data read in ⑤

16.15 High Security Module (HSM)

The High Security Module tab is used to encrypt and decrypt data. In this tab, it is possible, for example, to set an AES key, to change a wrapping key and to create a public certificate.

The screenshot shows the 'High security module' interface with several sections:

- ENCRYPT / DECRYPT:** Includes fields for Key index (1), AES mode (CBC-128), IV, Ciphertext, and Plaintext. It has 'Decrypt' and 'Encrypt' buttons.
- RANDOM DATA:** Includes Random data length (1) and a 'Get random data' button.
- AES KEY MANAGEMENT:** Includes Key index (1), Wrapping key, and AES key fields, with a 'Set AES key' button.
- WRAPPING KEY MANAGEMENT:** Includes New wrapping key, Old wrapping key, and Private certificate fields, with a 'Set wrapping key' button.
- CERTIFICATE MANAGEMENT:** Includes an 'Old private certificate' field.

At the bottom, there are system logs: '10:26:23 AM: Info: HSMSetWrappingKey: Successful' and '10:26:19 AM: Info: HSMSetPublicCertificate: Successful'.

16.15.1 Encrypt/Decrypt

The *Encrypt/Decrypt* allows to decrypt or encrypt data.

The annotated screenshot highlights the following elements:

- 1:** Key index field.
- 2:** AES mode dropdown menu.
- 3:** IV input field.
- 4:** Ciphertext input field.
- 5:** Plaintext input field.
- 6:** Decrypt button.
- 7:** Encrypt button.

Fig. 93: HSM: Decrypt/Encrypt

①	<i>Key index</i>	selects a key from 0 to 71
②	<i>AES mode</i>	selects between the two encryption standards: <i>EBS-128</i> <i>CBC-128</i>
③	<i>IV</i>	enters data to write in the hexadecimal format
④	<i>Ciphertext</i>	enters data to decrypt in the 32 hexadecimal digit format (128 bit)
⑤	<i>Plaintext</i>	enters data to encrypt in the 32 hexadecimal digit format
⑥	<i>Decrypt</i>	decrypts the data entered in ④
⑦	<i>Encrypt</i>	encrypts the data entered in ⑤

16.15.2 Random Data

The *Random Data* generates a hexadecimal number.

Fig. 94: HSM: Random Data

①	<i>Random data length</i>	enters a digit between 1 and 100
②	<i>Random data</i>	shows the hexadecimal number generated in ③
③	<i>Get random data</i>	generates a random hexadecimal number based on the length entered in ①

16.15.3 AES Key Management

In the *AES Key Management*, enters a hexadecimal number.

Fig. 95: HSM: AES Key Management

①	<i>Key index</i>	enters a key between 0 and 71
②	<i>Wrapping key</i>	enters a wrapping key (the default wrapping key is 32 zero digits)
③	<i>AES key</i>	enters an AES key in the 32 hexadecimal digit format
④	<i>Set AES key</i>	sets the AES key entered in ③

16.15.4 Wrapping Key Management

In the *AES Key Management*, enters a hexadecimal number.

Fig. 96: HSM: Wrapping Key Management

①	<i>New wrapping key</i>	enters a new wrapping key in the 32 hexadecimal digit format
②	<i>Old wrapping key</i>	enters the old wrapping key
③	<i>Private certificate</i>	selects a private certificate
④	<i>Set wrapping key</i>	sets a new wrapping key entered in ①

16.15.5 Certificate Management

In the *AES Key Management*, enerates a hexadecimal number.

CERTIFICATE MANAGEMENT

Old private certificate: ① C:\Users\Fredrich\Desktop\ham2.pem

New public certificate: ② C:\Users\Fredrich\Desktop\ham.pub

Set public certificate ③

Fig. 19: HSM: Certificate Management

①	<i>Old private certificate</i>	uploads the old private certificate
②	<i>New public certificate</i>	uploads the new public certificate
③	<i>Set public certificate</i>	sets the public certificate

17 Contact Information

Kathrein Solutions GmbH

Kronstaudener Weg 1

83071 Stephanskirchen

Phone +49 (0) 8036 / 90 831 20

Fax +49 (0) 8036 / 90 831 69

Email: info@kathrein-solutions.com



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.