

First steps:

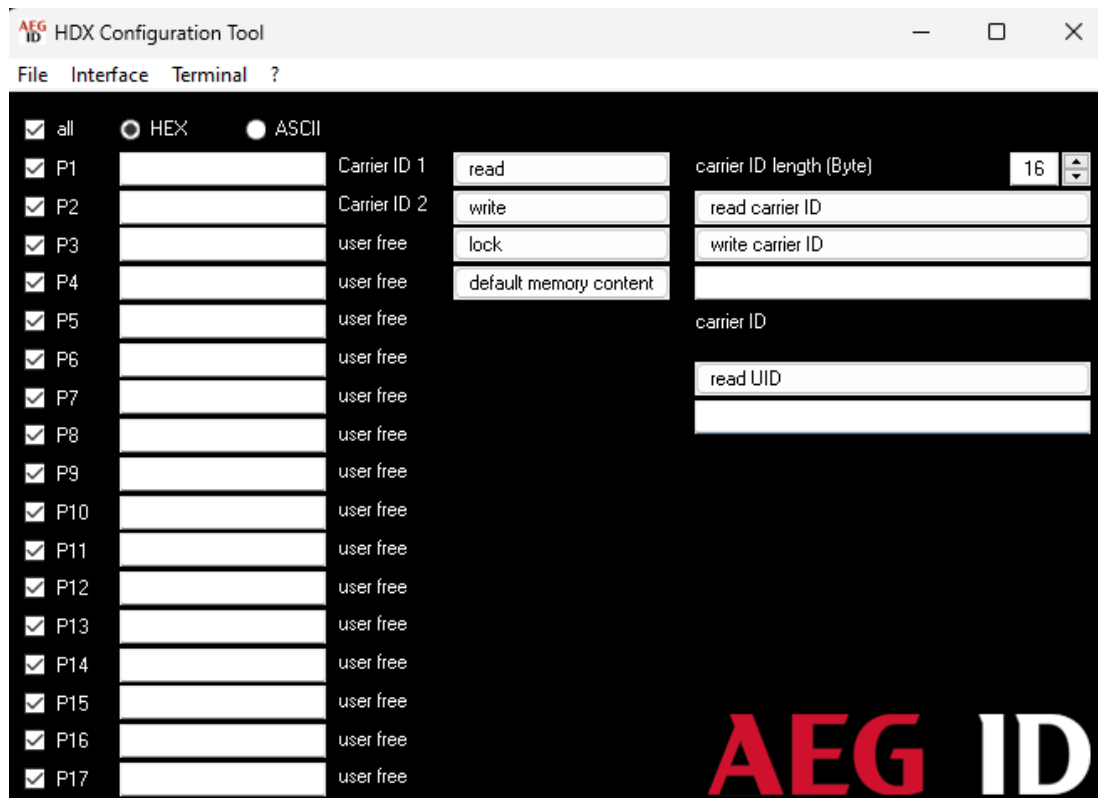
Plug in AEG ID reader ARE i2.0x or ARE i9x.

Note serial interface of PC

Start HDX configuration tool V026.exe

Please note the HDX configuration tool.ini file needs to be in the same folder as the .exe file

The program starts up like below.



General description of the program:

On the left side you see the memory map of AEG ID hdx multipage transponders. The pages can be selected individually.

Data can be displayed either in hex or ASCII by selecting the corresponding radio button.

Buttons “read, write, lock and default memory content” are to be used to check and change the data content of the chip displayed on the left side.

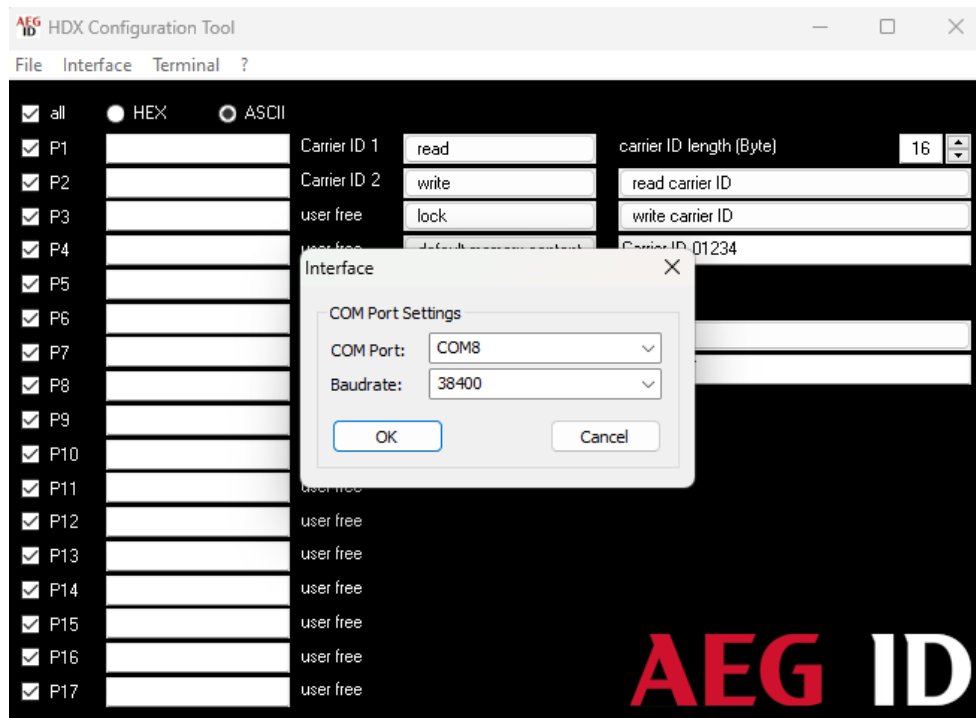
On the right side there is a special command to read and write a SEMI carrier ID residing in pages 1 and 2, depending on the setting of carrier ID length as defined by SEMI norms.

AEG ID hdx multipage transponders come with their own unique ID. This can be read by using the button read UID. Chip unique ID is used as a cyber security function.

Step by step instructions:

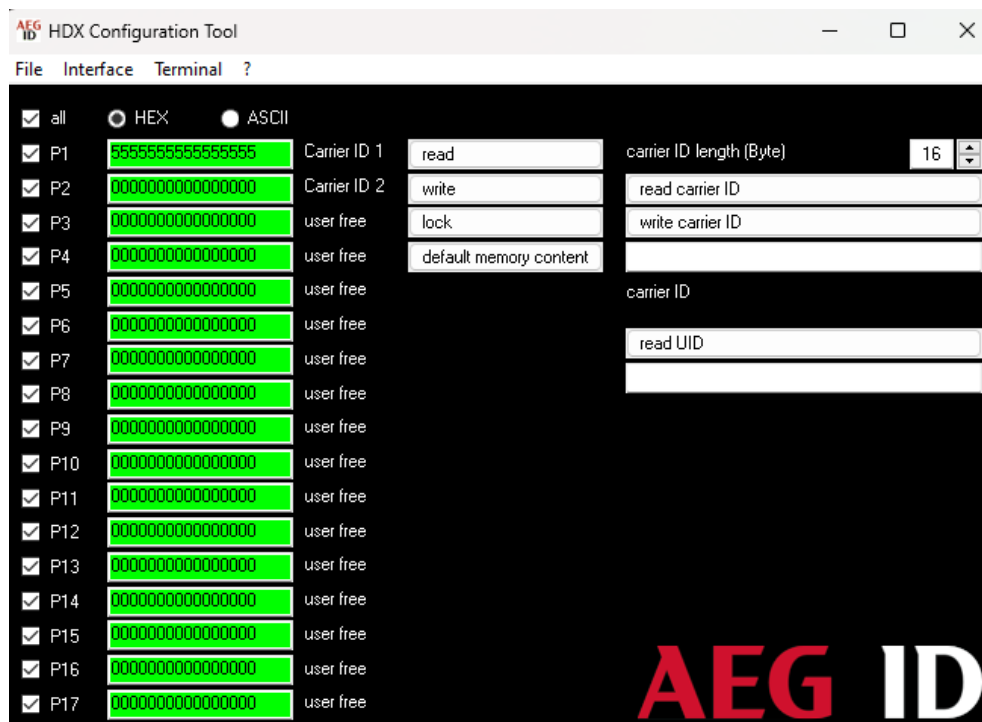
Open Interface

First you have to open the appropriate serial interface by pressing Interface. Select your interface and select 38400 as baud rate.



Read transponder memory

Button read triggers a read of all selected pages. Data is displayed either in hex or ASCII. Successful read of a page is displayed in green.

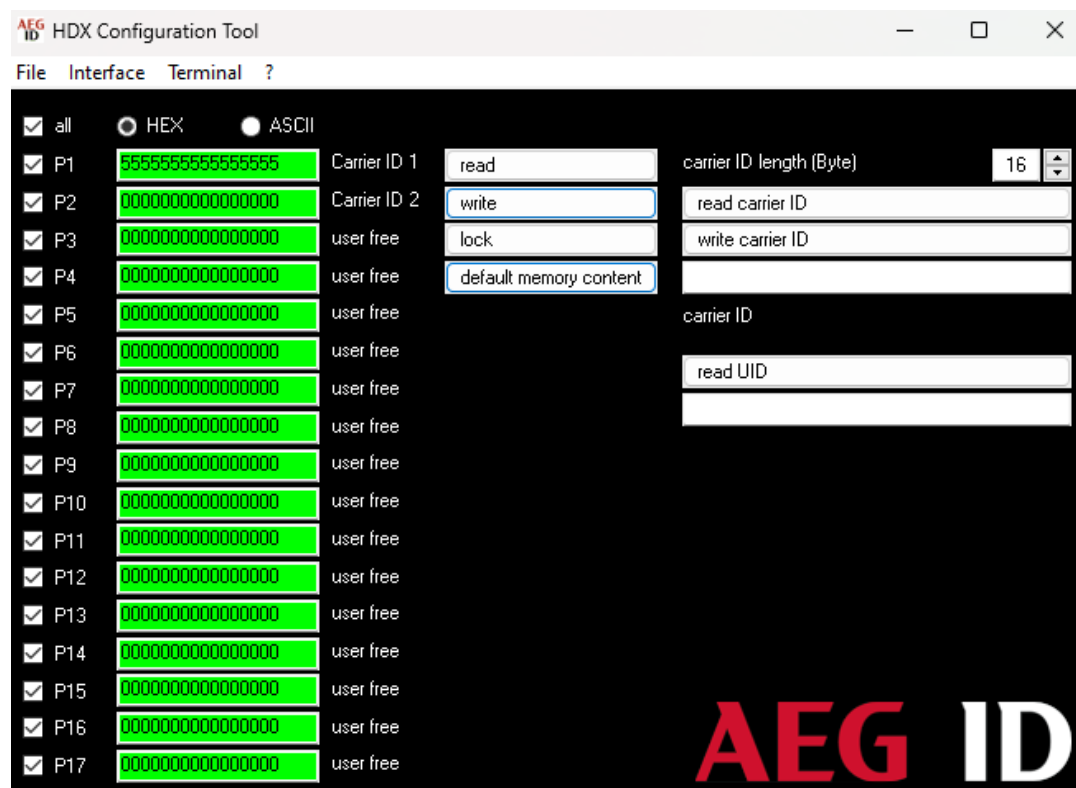


Editing data and writing to the chip

You can change the data content in the edit fields of the pages. In this example, data display is set to ASCII and the data content of pages 1 and 2 has been changed to below data. Button write triggers a write on all selected pages. Please note, in ASCII mode only printable characters are written. For non- printable characters, the data content of the chip remains unchanged.

Button default memory sets the entire memory back to its original content (Only in the edit fields, a subsequent write command has to be used to write this information to the transponder)

After pressing write, the data content is written to the transponder.

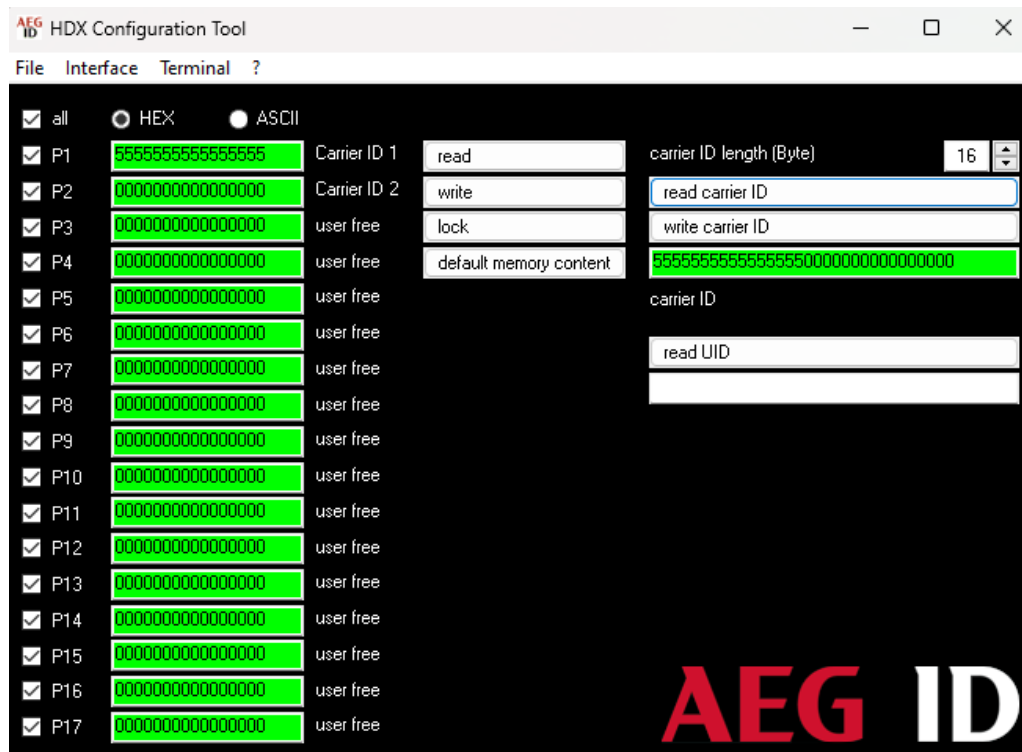


Locking chip memory to prevent data change

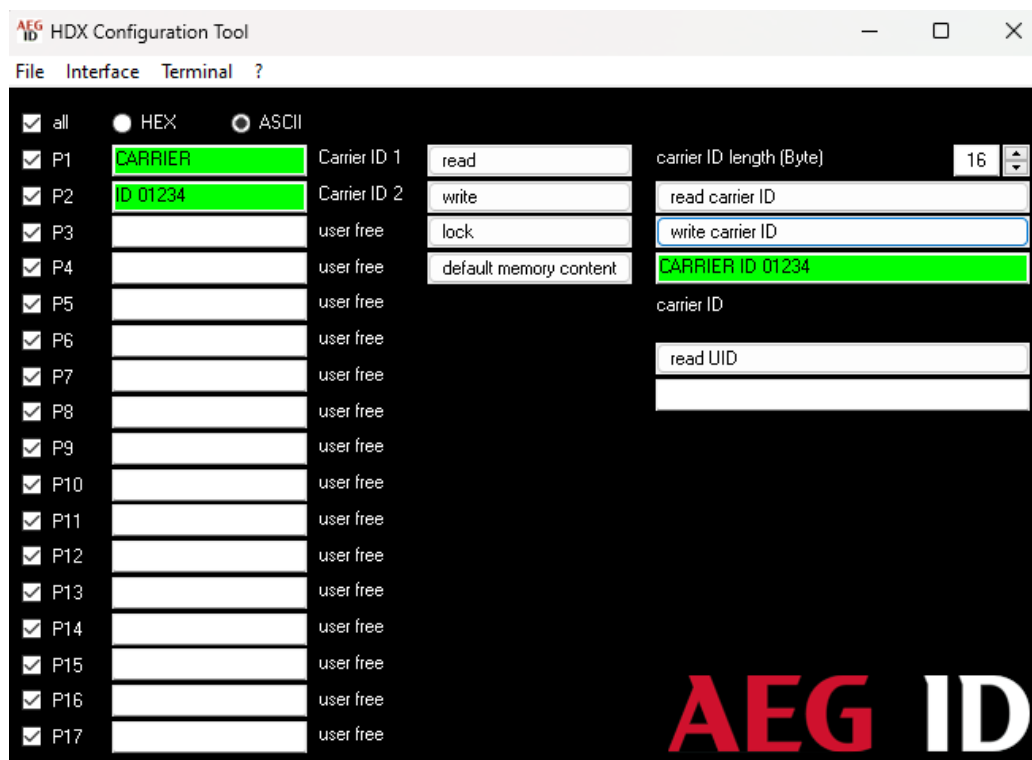
Button lock locks the memory for all selected pages. Be careful, this operation is non-reversible. Data for these blocks cannot be changed anymore.

Special feature for SEMI applications

Carrier ID length determines the length of the carrier ID. Button read carrier ID reads the data content from pages 1 and 2, depending on the setting of carrier ID length and displays it on the right side top edit field.

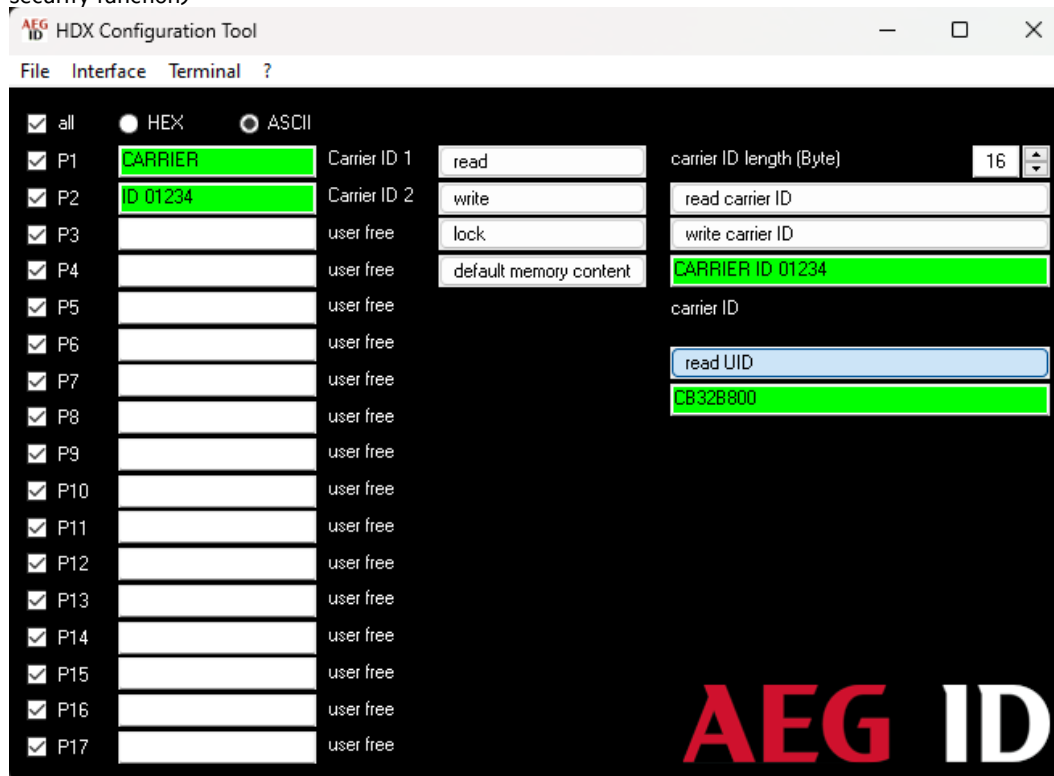


Data for Carrier ID can be changed in this edit field and written to the transponder by pressing write carrier ID.



Transponder unique ID (UID)

Button read UID reads the transponders unique ID. This unique ID can be used to encrypt data content for this individual transponder, making a copy of the data content useless as another transponder will have a different unique ID (-cyber security function)



The chip UID allows for any encryption method. It can be simple bit manipulations like AND, OR, XOR operations, it can be mathematical operations like adding or subtracting or the chip UID can be used as part of a AES 128 key. No matter how complicated the method for encryption is, it is always possible to determine, if the data in the transponder is the original intended data. Data copied to another tag or data changed in the tag can always be determined, thereby ensuring data integrity and security.

Terminal program

Pressing Terminal opens a simple terminal program on the right side. Here individual commands of AEG ID readers can be tested. In the example below, instruction “ruid” reads the chip UID.



1 Release, Change protocol

Revision:	Date:	Description of changes	Responsible
01	11.07.2024	First release	NK