User Manual

MASDecryptor

2018.12.0

English

Table of Contents

Legal Disclosure

Information in accordance with section 5 TMG

femvenner GmbH

Lise-Meitner-Str. 2

24941 Flensburg

Contact

Telephone: +49 (0)461 16839627
E-Mail: webcontact@femvenner.de
Website: http://www.femvenner.de

Register entry

Entry in German Commercial Register
Register Number: HRB 10643
Register Court: Amtsgericht Flensburg

Represented by

Gunter Hinrichsen

Steffen Zscherneck

Matthias Jahr

VAT number

VAT identification number in accordance with
section 27 a of the German VAT act
DE 296134379

Disclaimer

Liability for Contents

The contents of our pages have been created with great care. However, we can not guarantee the correctness, completeness and actuality of the contents. As a service provider, we are responsible for our own content on these pages according to the general laws (§7 (1) TMG). According to §§ 8 to 10 TMG, however, we as a service provider are not obligated to monitor transmitted or foreign information or investigate circumstances which indicate an illegal activity. Obligations to remove or block the use of information according to general laws, remain unaffected. However, liability in this regard is only possible from the time of the knowledge of a specific infringement. In the event of a breach of the law, we remove these contents immediately.

Copyright

Our pages and their contents are subject to German copyright law. Unless expressly permitted by law (§ 44a et seq. of the copyright law), every form of utilising, reproducing or processing works subject to copyright protection on our pages requires the prior consent of the respective owner of the rights. Individual reproductions of a work are allowed only for private use, so must not serve either directly or indirectly for earnings. Unauthorised utilisation of copyrighted works is punishable (§ 106 of the copyright law).

Version 2.0.0 (12/04/2018)

Technical changes reserved.

The Use of Symbols

The following manual includes several symbols to make it easier to follow the instructions.

ⓘ	The information symbol indicates an additional information on the action of the programme or on the handling with the programme.
NOTICE	The NOTICE indicates an important information. Disregarding may cause the programme to not run properly.
➜	The arrow indicates a prerequisite for the following action. If this prerequisite is not given, the programme may can not follow with the given instructions.
✔	The check mark indicates the result of an action.

General Information

NOTICE	Modifications on the software, that are going beyond the scope that is presented in this document, are not permitted! Any consequences, that are referable to these modifications, will not be covered by the company.

1   About this Manual

This manual is addressed to users who are working with the **MultiAnalyzerSoftware** and the additional hardware decryption extension **MASDecryptor**.

This manual is an addition to the "User Manual – MultiAnalyzer" and contains further information about working with the hardware decryption extension **MASDecryptor** and its configurations.

The manual follows a logical order for a gradual induction. Before start working with the **MASDecryptor**, read this manual carefully.

Follow the instructions precisely.

2   About the MASDecryptor Extension

The **MASDecryptor** is a hardware decryption extension for the **MultiAnalyzerSoftware** (**MAS**). The **MAS** creates decryption requests and sends the requests to the **MASDecryptor** hardware. The hardware processes the requests and sends the results back. With the results the **MAS** is able to decrypt the received air interface encrypted protocol data.

The extension includes three components:

- **MASDecryptor Hardware**

  The hardware itself is connected to the PC via USB. Communication and power support is handled via USB.

- **AieSupport5V.dll**

  This is an extension plug-in. This plug-in takes the decryption requests from the **MAS** and sends the requests to the hardware. After the reception of the results, the decrypted data is sent back to the **MAS**.

- **MASDecryptor.exe**

  This programme is a service tool. The programme is used for firmware updates and configuration.

3   MASDecryptor

This chapter provides an overview of the **MASDecryptor** interface.

NOTICE	**MASDecryptor** works only with licenced dongle! Working with the **MASDecryptor** needs a valid **MultiAnalyzerSoftware** dongle. The option "Decryptor-HW" has to be enabled on the dongle (see chapter 4.2 Missing Dongle or Licence). In case the dongle has no licence available, ensure the dongle is updated with the latest licence.

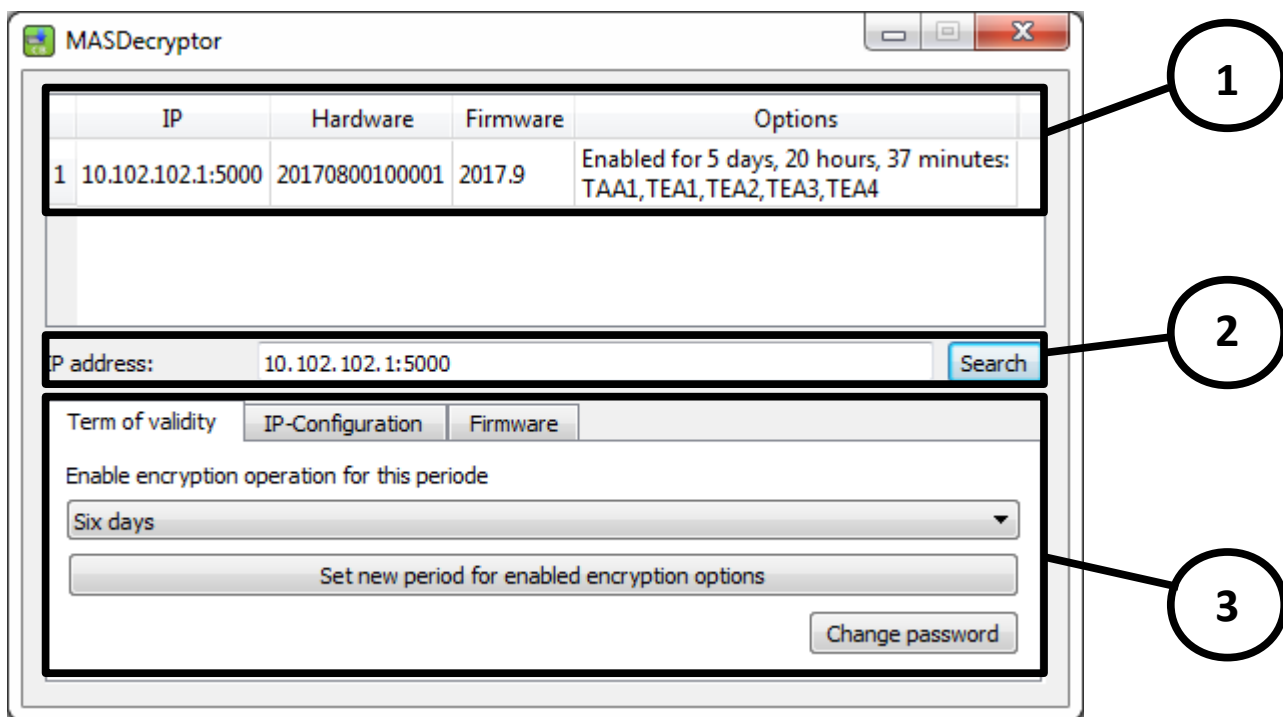*Illustration 1 MASDecryptor: Interface*

No	Description
1	Information about the found **MASDecryptor** hardware. This section shows the IP address, the serial number, the current firmware and the hardware status.
2	Text field to enter an IP address and a button to search for connected hardware.
3	Tap pages to enable safety-relevant algorithms, configure the IP address and to update the firmware. For more information see chapters (including subchapters): • 5 Firmware Update • 6 MASDecryptor IP Address • 7 Term of Validity

Table 1 MASDecryptor: Interface

4   Getting Started

To work with the **MASDecryptor**, the two software components **AieSupport5V.dll** and **MASDecryptor.exe** have to be installed in the corresponding **MultiAnalyzerSoftware** installation directory (typical: C:\Program Files\MultiAnalyzer). The installation can be done with the installer **MASDecryptorSetup.exe**. The hardware has to be connected via USB.

ⓘ   Windows usually installs all needed drivers by itself. A new "Remote Network Driver Interface Specification (**RNDIS**)" network interface turns up.

To run the **MASDecryptor.exe**, a licenced dongle is needed. Plug the dongle into the computer and ensure that the red LED of the dongle is switched on. If no light is on, check the dongle driver installation. If the message "No licence!" occurs, check the current licence. In both cases, see chapter 4.2 Missing Dongle or Licence.

NOTICE	**MASDecryptor** works only with licenced dongle! Working with the **MASDecryptor** needs a valid **MultiAnalyzerSoftware** dongle. The option "Decryptor-HW" has to be enabled on the dongle (see chapter 4.2 Missing Dongle or Licence). In case the dongle has no licence available, ensure the dongle is updated with the latest licence.

After starting the component **MASDecryptor.exe**, the connected device is displayed.

The **MASDecryptor** hardware is always delivered without encryption algorithm. To get the algorithm, a firmware update is needed (see chapter 4.3 Getting the Ordered Algorithm).

ⓘ   If no hardware is displayed, see chapter 4.1 Missing Hardware for more information.

4.1   Missing Hardware

A missing hardware can have different causes:

- Booting routine

  If the hardware is not directly displayed in the list after plug in, it may boots. After plugging in the hardware, wait about 30 seconds to let the hardware finish the booting routine.

- Windows driver works not properly

  If the hardware is still not listed, the windows driver may not work properly. In that case, (re)install the Windows driver. Use the "Install MASDecryptor-driver" within the Windows Start Menu (see 2).
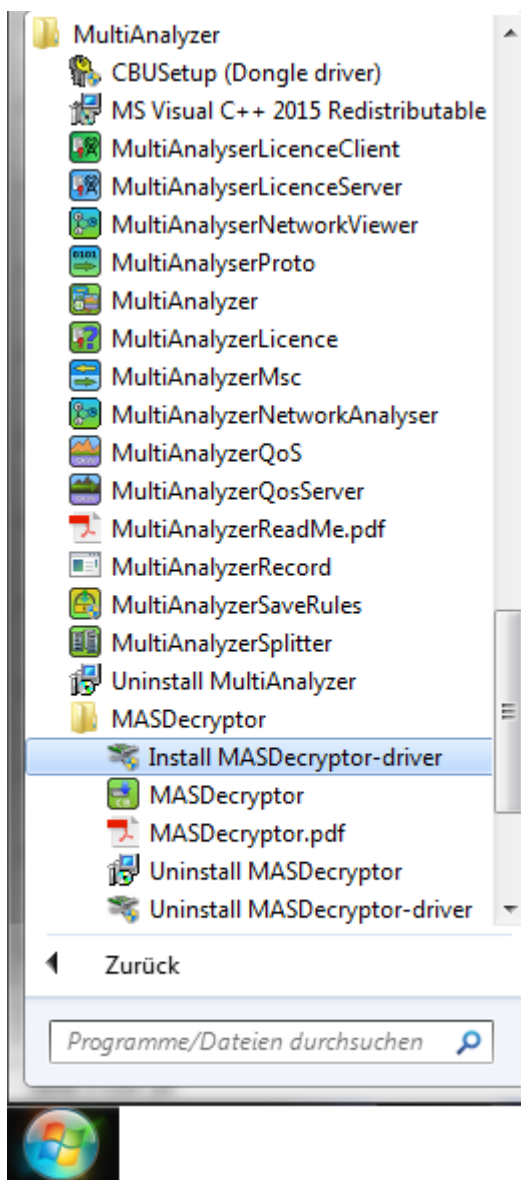
Illustration 2 Reinstall MASDecryptor Driver

4.2   Missing Dongle or Licence

If the programme exits with the message "No licence!" (see 3), this can have different causes:
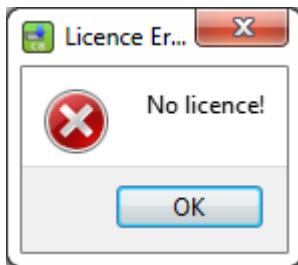

Illustration 3
MASDecryptor: No licence

- No dongle connected

    Ensure that a dongle is connected via USB, before running the programme.

- Dongle is not working

    Ensure that the dongle shows a red light. In case the dongle is not working, check the USB port. If the USB port is working, continue with the next point.

- No dongle driver installed

    In case the USB port is working but the dongle shows no red light, (re)install the dongle driver. Use the "CBUSetup (Dongle driver)" within the Windows Start Menu (see 4).
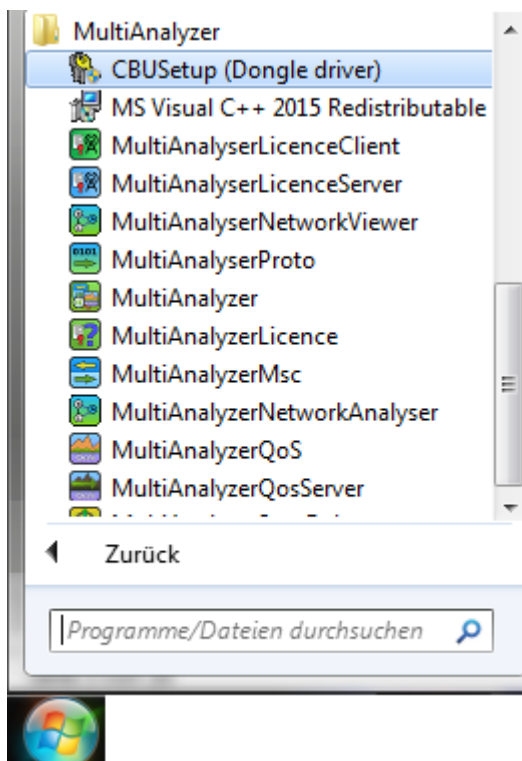

Illustration 4 Reinstall Dongle Driver

- No valid licence on dongle

    Open the **MultiAnalyzerLicence** and check the licence options of the connected dongle. The option "Decryptor HW" has to be valid (see 5).
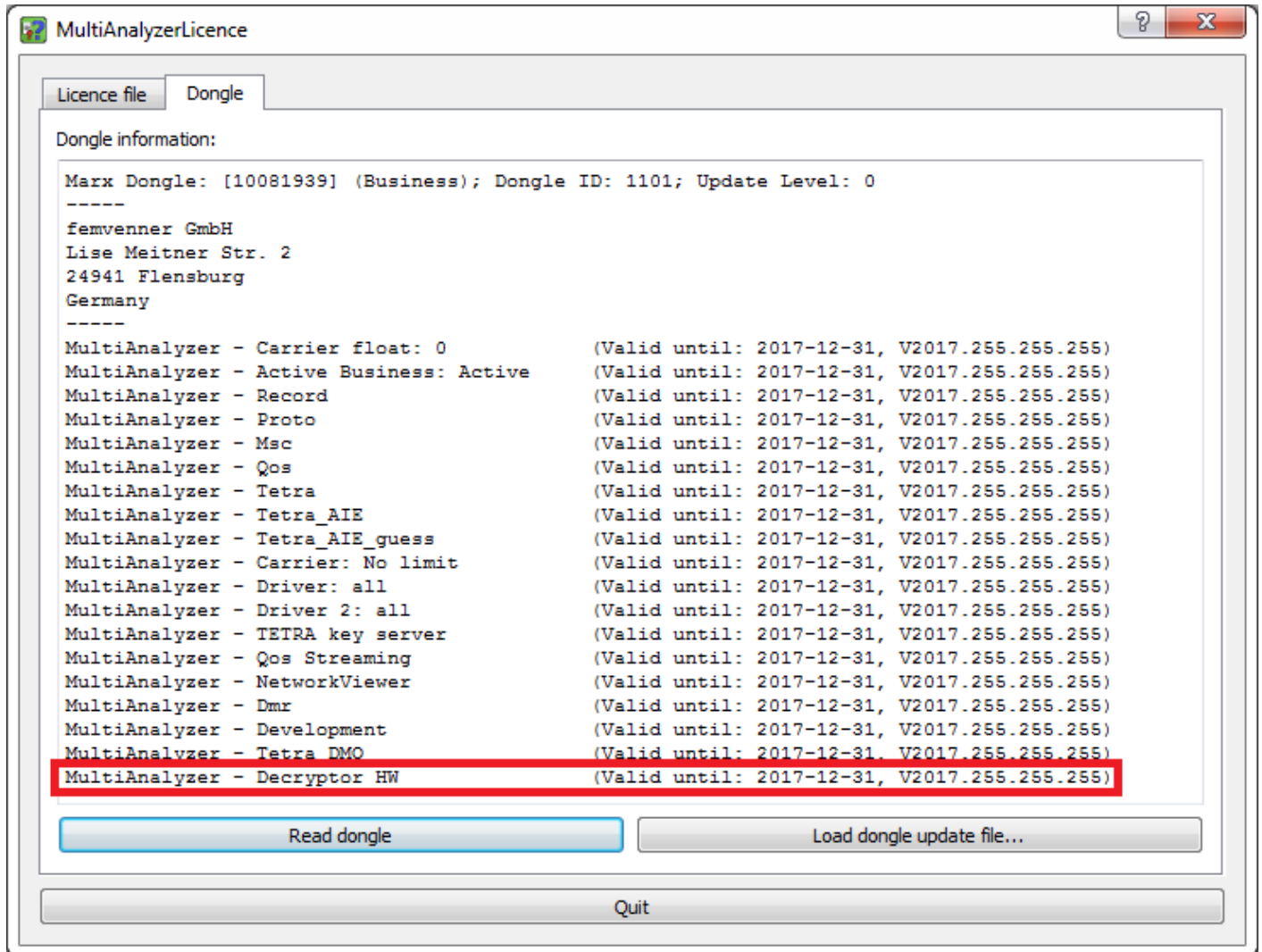

Illustration 5 MultiAnalyzerLicence: Check Licence Options Dongle

4.3   Getting the Ordered Algorithm

The **MASDecryptor** hardware is always delivered without encryption algorithm. The first step is to make a firmware update that implements the ordered algorithm.

To get this firmware, send the femvenner GmbH the signed agreement for limited application and if needed the TEA2 algorithm authorisation.

The postal address is:

femvenner GmbH

Lise-Meitner-Str. 2

24941 Flensburg

Germany

After acceptance, the femvenner GmbH will send the firmware update. For handling a firmware update see chapter 5 Firmware Update and chapter 5.1 Starting Firmware Update.

5   Firmware Update

A firmware update file has the suffix "*.mdhu" (**M**ultiAnalyzerSoftware **D**ecryptor **H**ardware **U**pdate). This update file is encrypted and unique for **MASDecryptor** hardware which is identified by the serial number. The decryption is only possible with a _unique_ hardware dongle. This can be one of the dongles, that were delivered with the **MultiAnalyzerSoftware** and are identified by the dongle number (in case of a subsequent order of the **MASDecryptor**, the update file can be generated matching to one of the already provided dongles).

NOTICE	Firmware update works only with matching hardware dongle!
	To decrypt the firmware update file, a matching hardware dongle is needed. For the update file decryption, use the dongle that is delivered with the software.

To process a firmware update, the following components are needed:

- the connected **MASDecryptor** hardware, to which the update file was bound

- the connected dongle, to which the update file was bound

- the running **MASDecryptor.exe**

5.1 Starting Firmware Update

If a valid **MASDecryptor** hardware IP address is set, the firmware update can be started.

(i)   For information about the IP configuration see chapter 6.1 Configuring the IP Address.

To start a firmware update, follow the next steps.

➔ **MASDecryptor.exe** is started.

➔ **MASDecryptor** hardware is connected.

➔ The firmware update dongle is connected.

➔ Firmware update file is present.

NOTICE	No firmware update possible with the wrong or without dongle!
	If no dongle or the wrong dongle is connected the **MASDecryptor** shows the message "No Dongle" or "Firmware update file does not match to the connected dongle!". Ensure that the right dongle is connected to the PC.

1. Open the tab page "Firmware" (see 6).
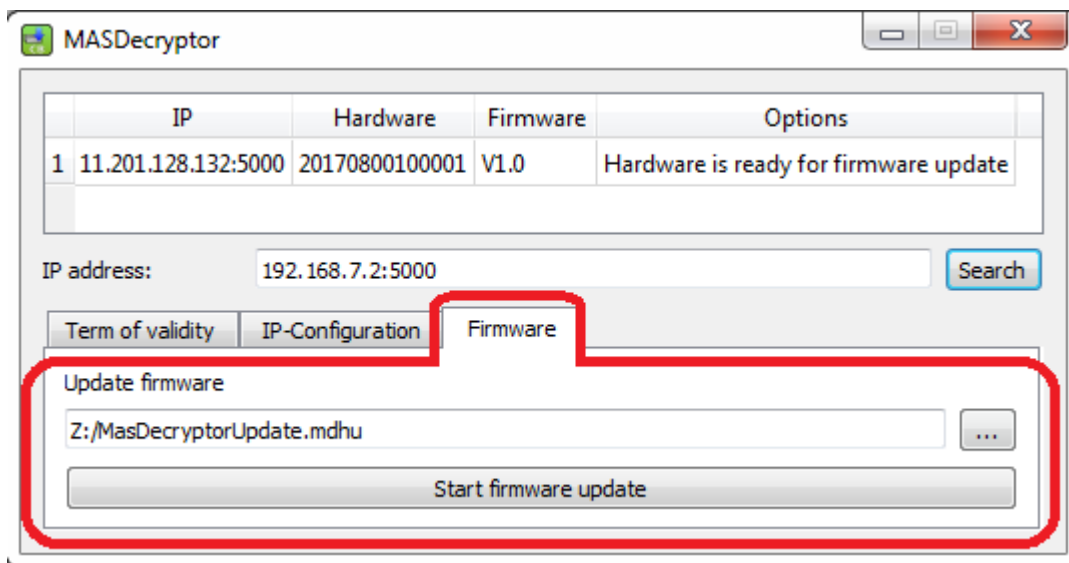
Illustration 6 MASDecryptor: Tab Page Firmware Update

2. To open the selection dialogue to select the update file, click on the button "…" (see 7).
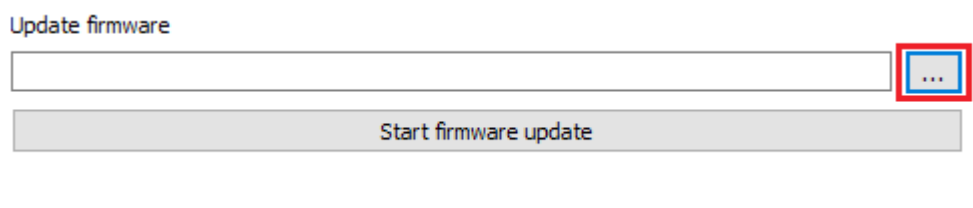

Illustration 7 MASDecryptor: Open Selection Dialogue

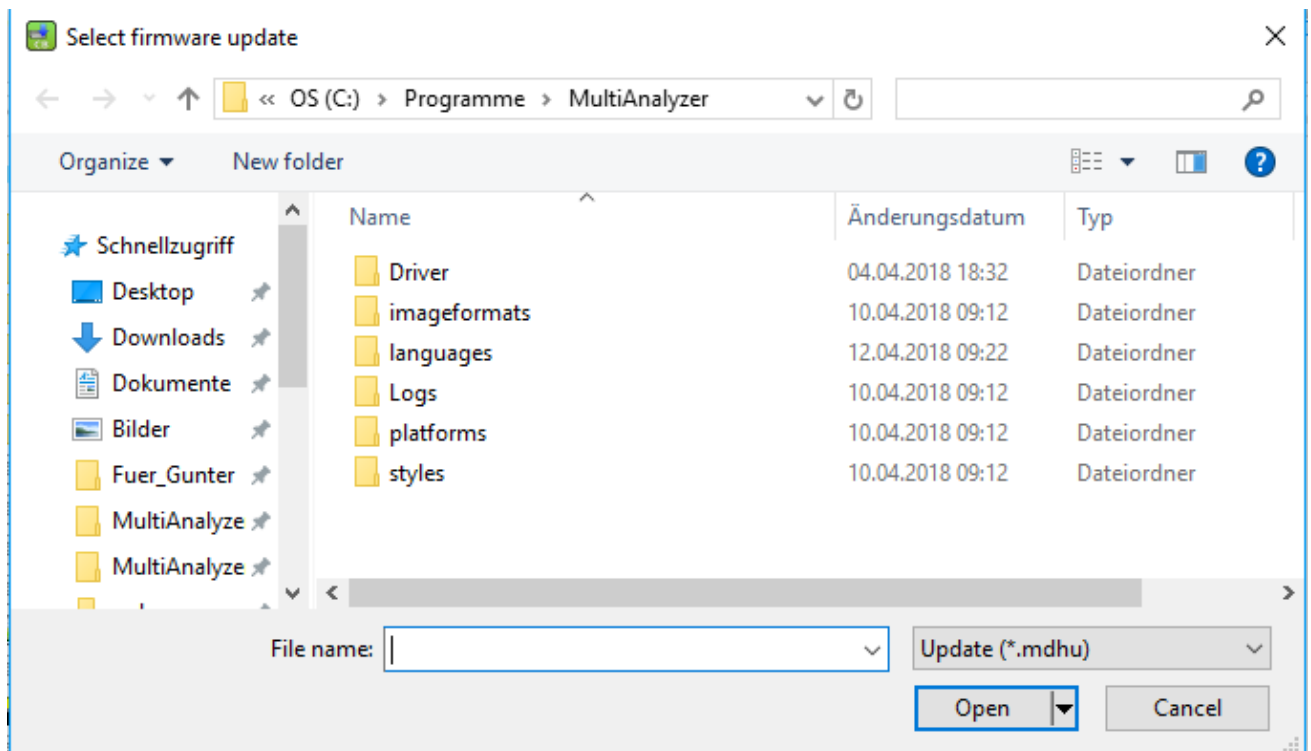✔ A selection dialogue opens to select the update file (see 8)

Illustration 8 MASDecryptor: Select Firmware Update File

3. To open the file, choose the file and click on the button *Open*.

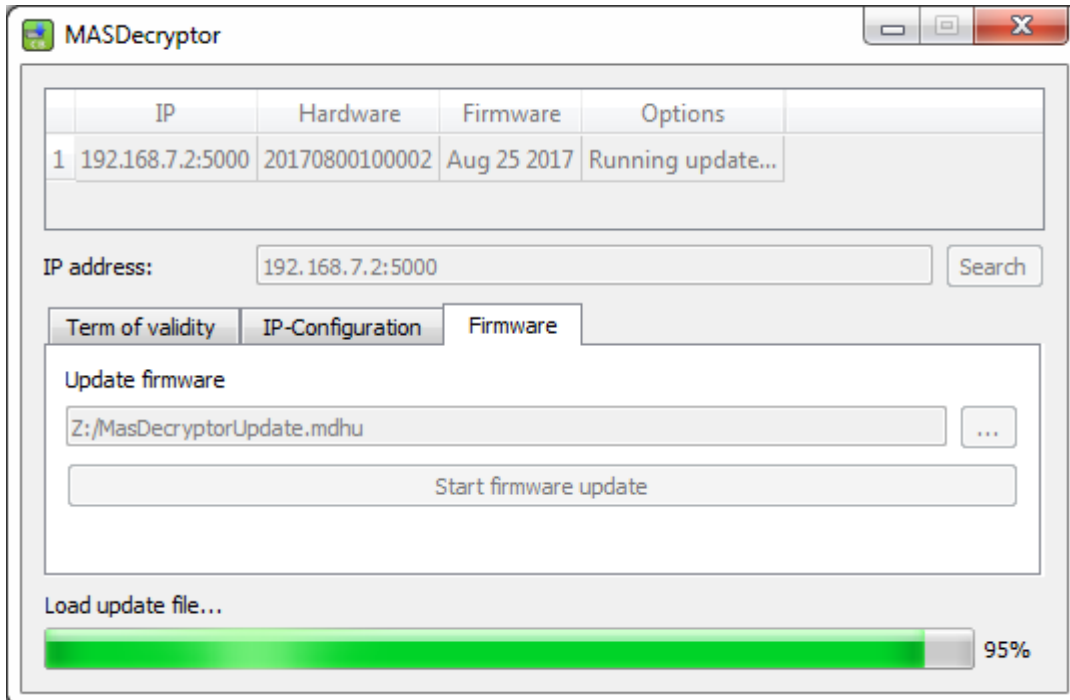✔ The service tool loads the firmware update and tries to decrypt it (see 9).

Illustration 9 MASDecryptor: Firmware Update File Loading

✔ After acceptance, the file is loaded to the hardware.

✔ After finishing loading, the hardware validates the firmware.

	Update fail because of invalid firmware file!
NOTICE	If the firmware is not suitable, the message "Update failed because image is invalid" appears. Select the correct firmware file and check the serial number of the **MASDecryptor** hardware.

4. To start the firmware update, click on the button *Start firmware update* (see 10).
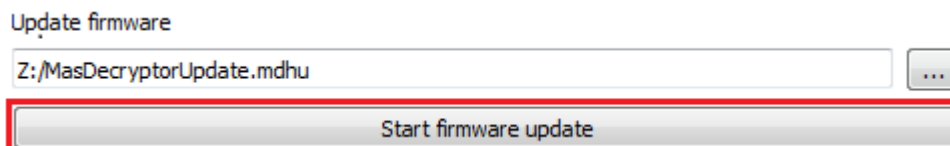
Illustration 10 MASDecryptor: Start Firmware Update

ⓘ This process may be password protected. For more information see chapter 8 Password Protection.

✔ If the validation was successfully completed, the firmware update starts.

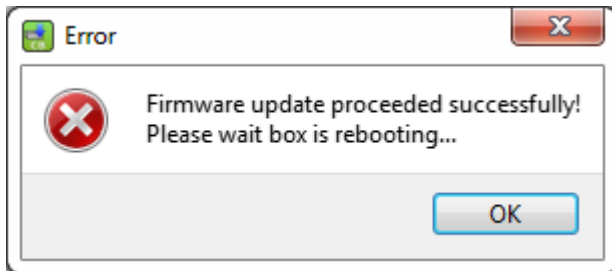|	Destruction of the software image!
NOTICE	The firmware update may includes several reboots of the hardware. Switching off the power or disconnecting the hardware may lead to a destruction of the software image that is installed on the hardware. Do not switch off the power or disconnect the hardware.

✔ The **MASDecryptor** shows the following message:

Illustration 11 MASDecryptor: Update Message

✔ The hardware reboots.

✔ The hardware is ready to use.

5.2   Meaning of Update Messages

Message	Cause	Solution
Firmware update proceeded successfully	Firmware update succeeded.	After an automatic reboot, the hardware is ready to use.
No valid destination IP address	Cannot connect to the **MASDecryptor** hardware.	See chapter 6 MASDecryptor IP Address.
Cannot connect: Target does not respond at given IP + port!	Cannot connect to the **MASDecryptor** hardware.	Check if the IP address and the port are correct. See chapter 6 MASDecryptor IP Address.
Unspecified error	General error.	Reboot the hardware and retry the firmware update. If this is unsuccessful too, contact the *femvenner GmbH*.
Protocol version not supported	The service tool and the firmware are not compatible.	Use a supported PC software.
Encryption fails	The service tool and the firmware are not compatible.	Use a supported PC software.
Client licence is blocked	The dongle is blacklisted.	Use an accepted dongle.
Cannot load image (File not completely loaded)	Error while loading or starting the update.	Reboot the hardware and retry the firmware update. If this is unsuccessful too, contact the *femvenner GmbH*.
Update failed because not supported	The **MASDecryptor** hardware does not support the firmware update.	Contact the *femvenner GmbH* .
Update failed because image is invalid	The firmware does not belong to the **MASDecryptor** hardware.	• Choose the correct firmware update. • Check the serial number.
Update failed because of update error	An update error occurred.	Reboot the hardware and retry the firmware update. If this is unsuccessful too, contact the *femvenner GmbH*.

Message	Cause	Solution
Cannot reconnect hardware!	The **MASDecryptor** hardware does not respond.	• Wait for 20 minutes. • Reboot the hardware. • Check if the firmware version has changed. • If not, retry the firmware update. If this is unsuccessful too, contact the *femvenner GmbH*.
No response from hardware!	The **MASDecryptor** hardware does not respond.	• Reboot the hardware. • Check if the firmware version has changed. • If not, retry the firmware update. If this is unsuccessful too, contact the *femvenner GmbH*.

Table 2 MASDecryptor: Meaning of Update Messages

6   MASDecryptor IP Address

To search for a hardware, a search request can be generated with the button *Search*. Also the IP address can manually be entered in the text field.

(i)   The default IP-Address is "10.101.101.101". The default port is "5000". Both are separated by a colon ":". The full IP-Address is written as "10.101.101.101:5000".

The upper field within the **MASDecryptor.exe** shows the information about the found **MASDecryptor** hardware. Besides the IP address this section shows the serial number, the current firmware and the options or the hardware status (see 12).
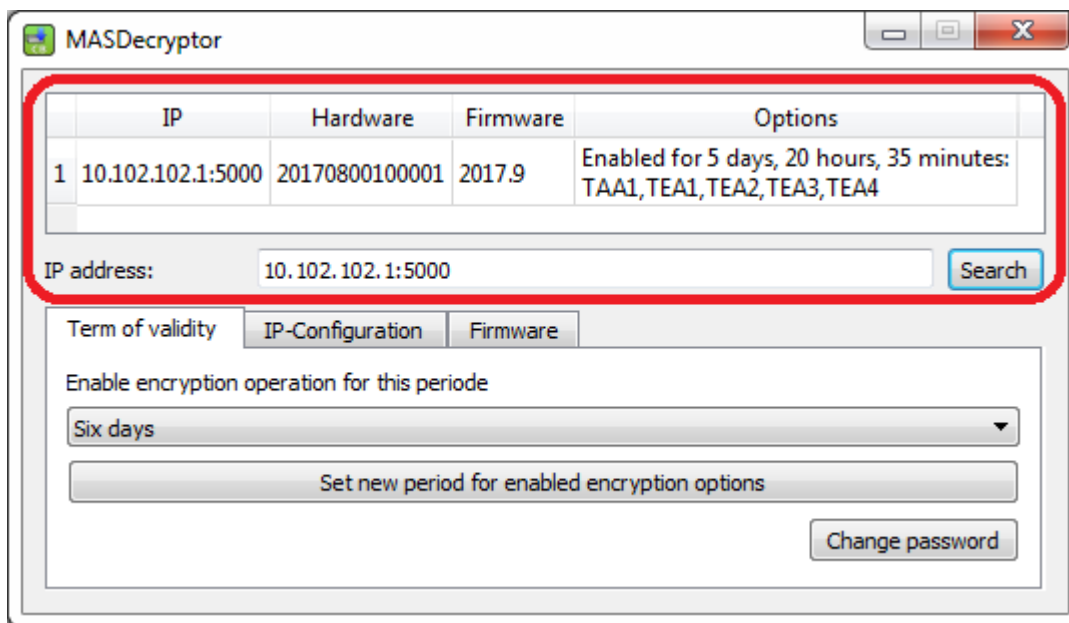
Illustration 12 MASDecryptor: Hardware Info

NOTICE	No displayed **MASDecryptor** data because of firewall or second instance! Displaying of no data can be caused by the firewall or a second running programme instance. Check the windows setting or the installed security suit for firewall options and make sure that only one programme instance is running.

To change the IP address, the tab page "IP-Configuration" can be used. For more in formation see chapter 8.1 Changing the Password.

(i)   If more than one **MASDecryptor** hardware is connected, the IP address must be changed.

6.1 Configuring the IP Address

If more than one **MASDecryptor** hardware is connected, the **MASDecryptor** hardware must have different IP addresses. The IP configuration option can be used to change this.

> (i) The default IP-Address is "10.101.101.101". The default port is "5000". Both are separated by a colon ":". The full IP-Address is written as "10.101.101.101:5000".

> (i) Regardless of a user-defined IP address, the default IP address retains as a second emergency fallback IP address within the **MASDecryptor**.

To change the IP address of the **MASDecryptor** hardware, follow the next steps.

➔ **MASDecryptor.exe** is started.

➔ **MASDecryptor** hardware is connected.

➔ A licenced dongle with the option "Decryptor HW" is connected (see chapter 4.2 Missing Dongle or Licence).

1. Open the tab page "IP-Configuration" (see 13).
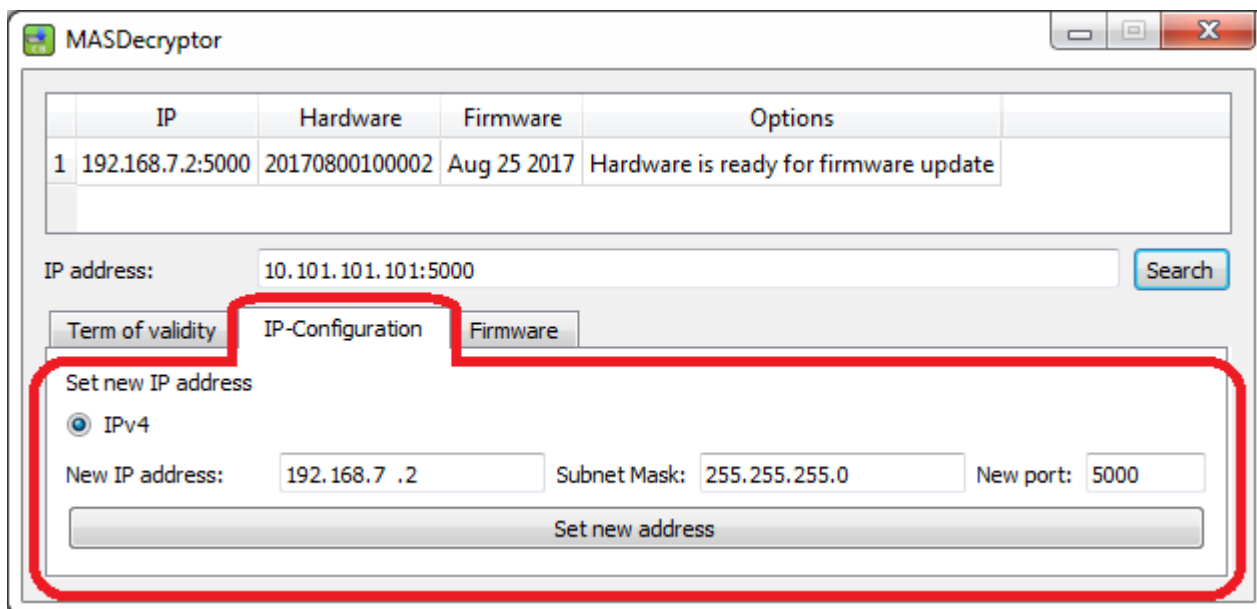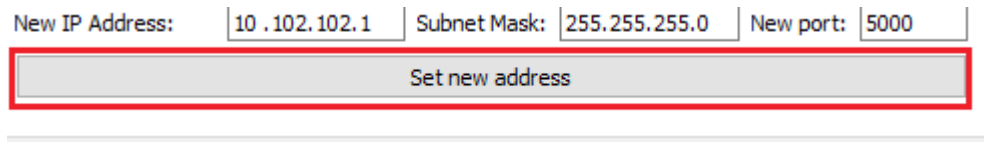
Illustration 13 MASDecryptor: IP-Configuration

2. Enter the new desired IP address, subnet mask and port into the dedicated fields.

> (i) Currently only IPv4 addresses are supported.

3. To confirm the changes, click on the button *Set new address* (see 14).

Illustration 14 MASDecryptor: Set New Address

ⓘ This process may be password protected. For more information see chapter 8 Password Protection.

✔ The IP address is changed.

6.2 Windows IP Address

If the settings of the RNDIS-Windows driver have not manually been changed, an address out of the desired range is automatically assigned to it. If no connection is possible but the **MASDecryptor** hardware is displayed, then the current Windows network configuration and adapter settings should be checked.

The **MASDecryptor** hardware is designed to work on a local PC. When operating in a network, the host Windows must be configured as a router. Under certain circumstances, this can lead to security problems. The *femvenner GmbH* does not recommend or provide support for this mode of operation.

7   Term of Validity

Within the tab page "Term of validity", a new runtime period for the used algorithms can be set.

The time is not limited to a specific date, but the overall use is limited. Each restart of the hardware costs 30 minutes of reliable running time. Every minute under power (used or unused) is deducted from the reliable running time. When the runtime has expired, the algorithms are no longer executed. This remains until the user extends the runtime again.

To change the runtime period for the algorithms, see chapter 7.1 Changing the Term of Validity.

NOTICE	Algorithms are only activated for a limited time! The **MASDecryptor** hardware contains safety-relevant algorithms. In order to limit unauthorised use in the event of a loss, these algorithms are always only activated for a limited period of time.

7.1   Changing the Term of Validity

To change the term of validity for the used algorithms, follow the next steps.

➔ **MASDecryptor.exe** is started.

➔ **MASDecryptor** hardware is connected.

➔ A licenced dongle with the option "Decryptor HW" is connected (see chapter 4.2 Missing Dongle or Licence).

NOTICE	The term of validity can only be set with a licenced dongle! The runtime can only be set with a dongle that has the option "Decryptor HW" activated. To avoid a loss of this protection, always keep the **MASDecryptor** and the dongle proctored.

1. Open the tab page "Term of validity" (see).
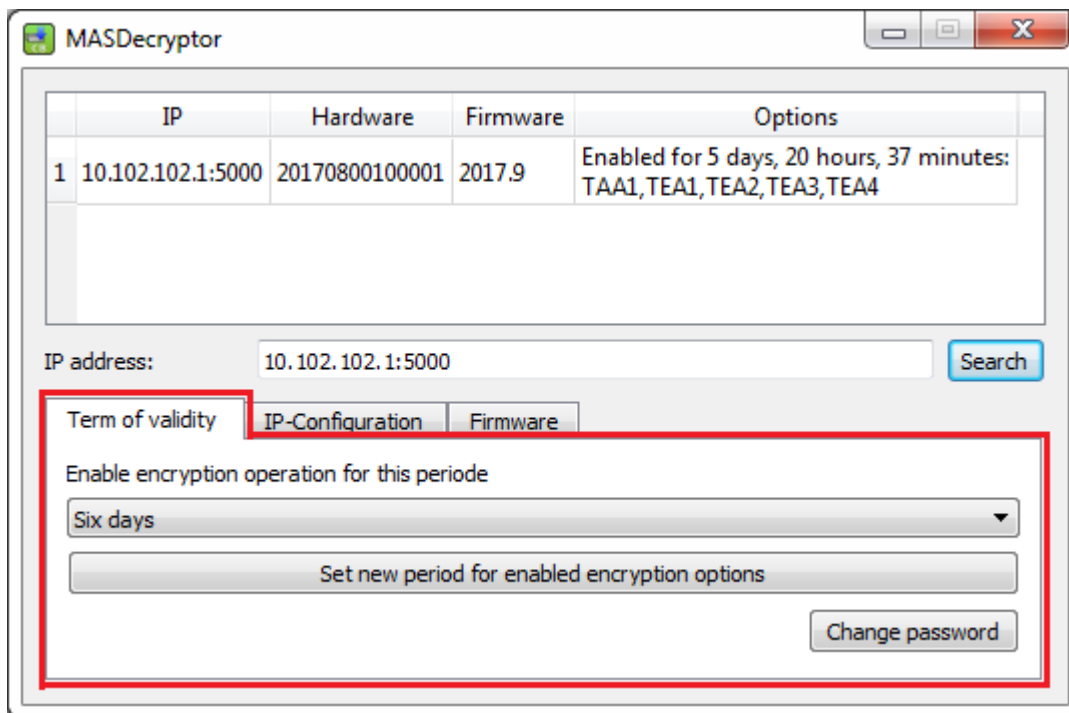
Illustration 15 MASDecryptor: Tab Page Term of Vadility

2. Choose a term from the drop-down list (see 16).
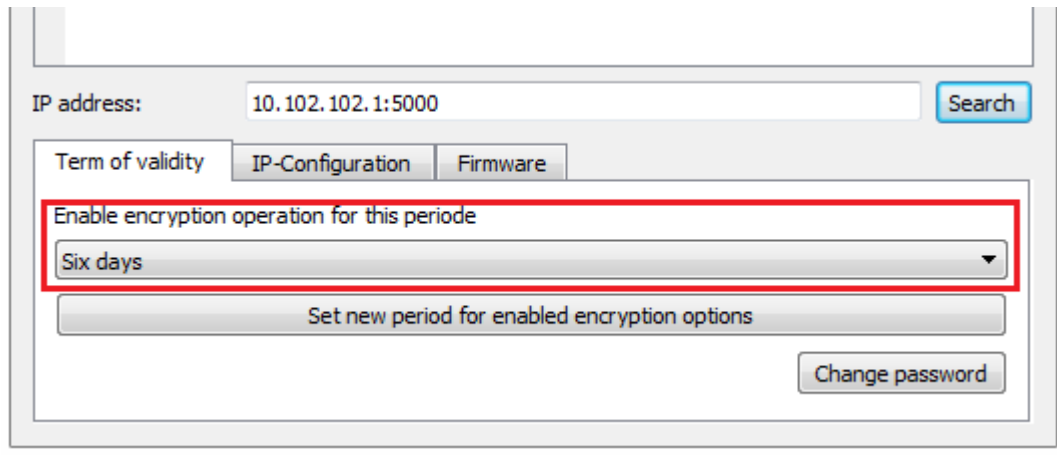
Illustration 16 MASDecryptor: Choose Runtime Period

ⓘ The item "Disable now" will disable the AIE algorithm. This makes sense if the box is no longer in use and the remaining time should be invalidated.

3. To confirm the changes, click on the button *Set new period for enabled encryption options* (see 17).
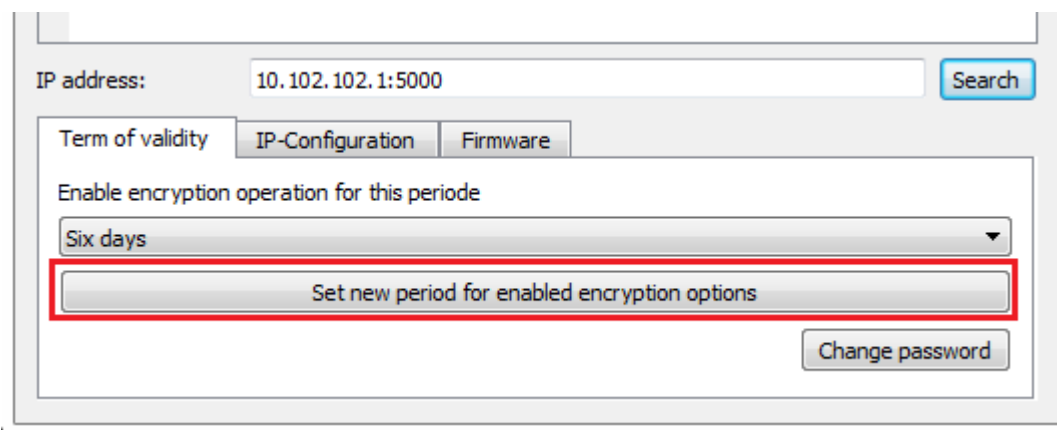
Illustration 17 MASDecryptor: Confirm Changes

ⓘ This process may be password protected. For more information see chapter 8 Password Protection.

✔ The runtime period is transmitted to the **MASDecryptor** hardware.

8   Password Protection

Tasks like 5 Firmware Update, 6.1 Configuring the IP Address and 7.1 Changing the Term of Validity can be password protected. No password is set at delivery. It is up to the user to change this. The password is stored on the dongle. So every dongle may has a different password. The password protects the use of the **MASDecryptor** dongle option.

To set, change or delete a password, see chapter 8.1 Changing the Password.

8.1　Changing the Password

The password can be set, deleted or changed at any time.

To change the password, follow the next steps.

➔ **MASDecryptor.exe** is started.

➔ A licenced dongle with the option "Decryptor HW" is connected (see chapter 4.2 Missing Dongle or Licence).

1. Open the tab page "Term of validity".

2. Click on the button *Change password* (see 18).
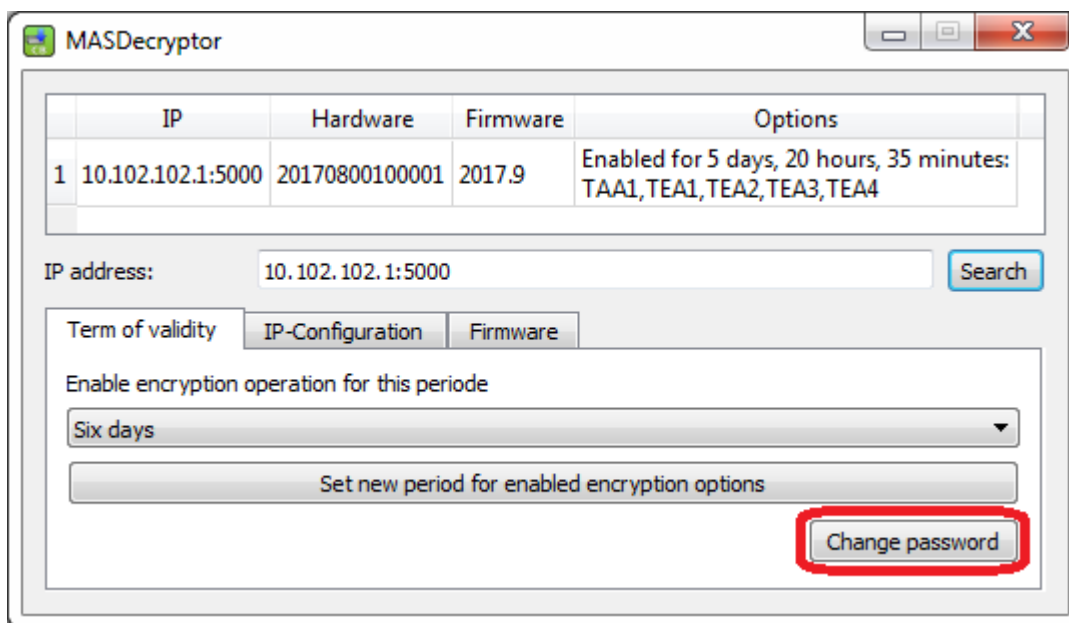
Illustration 18 MASDecryptor: Change Password

✔ A dialogue opens to change the password.
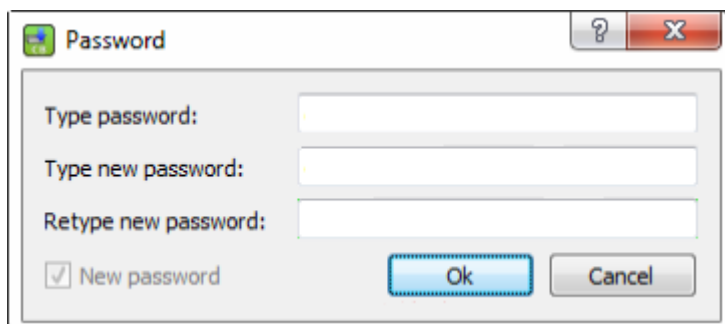
Illustration 19 MASDecryptor: Password Dialogue

3. Enter the old and the new password into the dedicated fields (see 20).
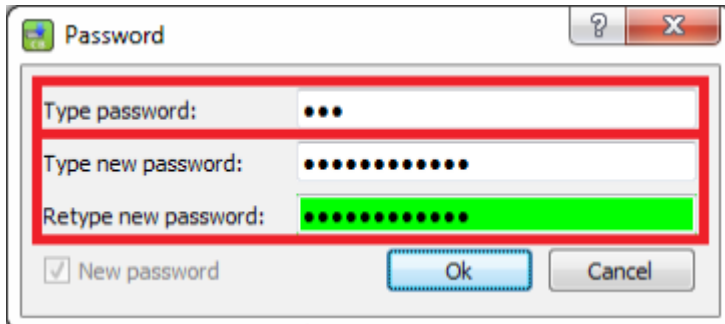
Illustration 20 Type Password

(i)   To change the password, the old password is required.

(i)   The new password is specified twice to avoid typos. A blank new password will remove the password protection.

4. To accept the new password, click on the button *Ok* (see 21).
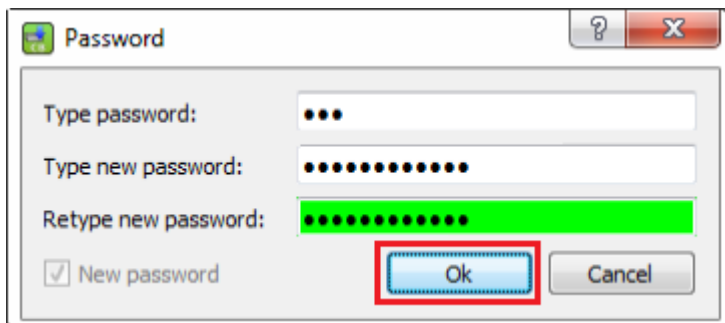
Illustration 21 Accept Password

✔ The password is changed.

✔ The password is stored on the dongle.

(i)   If the password has been forgotten, a dongle update can be requested from *femvenner GmbH* to reset the dongle.

9   Working with MASDecryptor

The installed component **AieSupport5V.dll** is used as a plug-in for the **MultiAnalyzerSoftware**, which is used as an interface to the **MASDecryptor** hardware. The hardware can handle up to sixteen different clients.

The following programmes from the **MultiAnalyzerSoftware** bundle can use the **MASDecryptor** as a client:

Programme	Description
MultiAnalyzer	The record programme only uses the **MASDecryptor** if the TETRA AIE Key Server is enabled. ⓘ An enabled Key Server uses one client instance.
MultiAnalyzerMsc	The programmes use the **MASDecryptor** while analysing the TETRA protocol.
MultiAnalyzerQoS	ⓘ Every analysing programme uses one client instance. After the analysis is finished the used client instance will be cleared.
MultiAnalyzerQosServer	Every TETRA stream uses a particular client instance from the **MASDecryptor**. ⓘ The number of TETRA streams determine the number of used client instances of the **MASDecryptor**.

Table 3 Working with MASDecryptor

9.1 Available Options

Depending on the firmware update level and the ordered options of the **MASDecryptor**, following encryption standards can be served by the hardware:

Option	Description
TAA1	The basic algorithms for TETRA. It includes following single algorithms: TB4, TB5, TB5, TB7, TA11, TA12, TA21, TA22, TA32, TA41, TA52, TA61, TA71, TA82, TA92, TA101.
TEA1	The KSS generation with TEA1 algorithm.
TEA2	The KSS generation with TEA2 algorithm.
TEA3	The KSS generation with TEA3 algorithm.
TEA4	The KSS generation with TEA4 algorithm.

Table 4 Available Encryption Standards

The available options and the term of validity are displayed in the service tool:
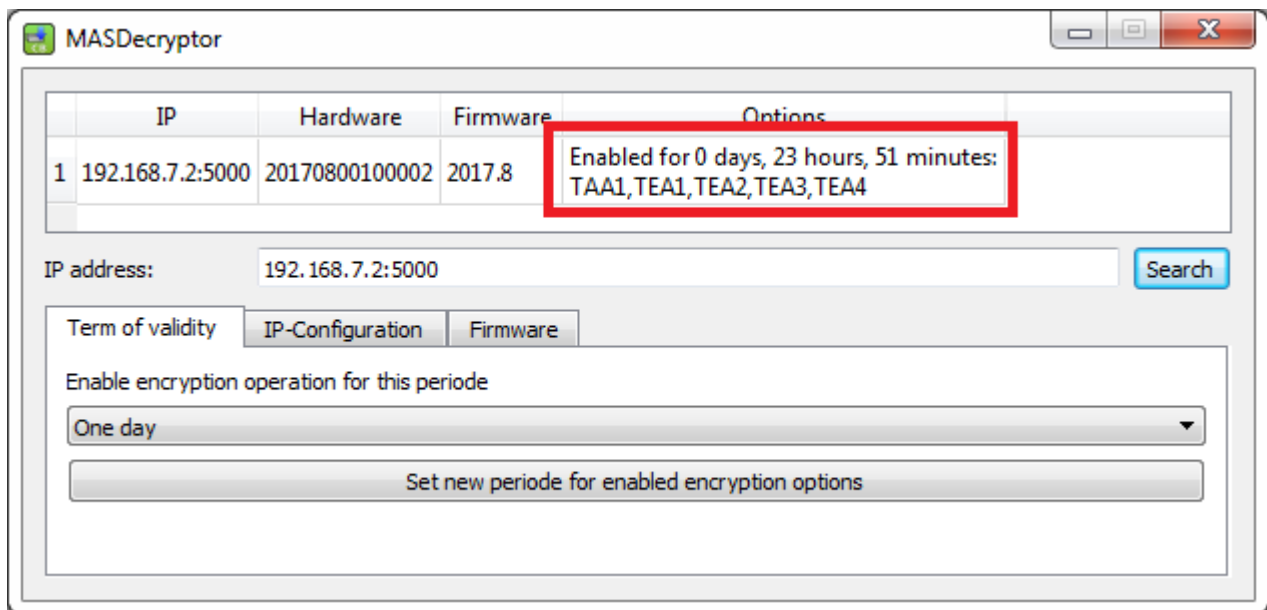
Illustration 22 MASDecryptor: Enabled Encryption Standards

ⓘ   For information about the term of validity, see chapter 7 Term of Validity.
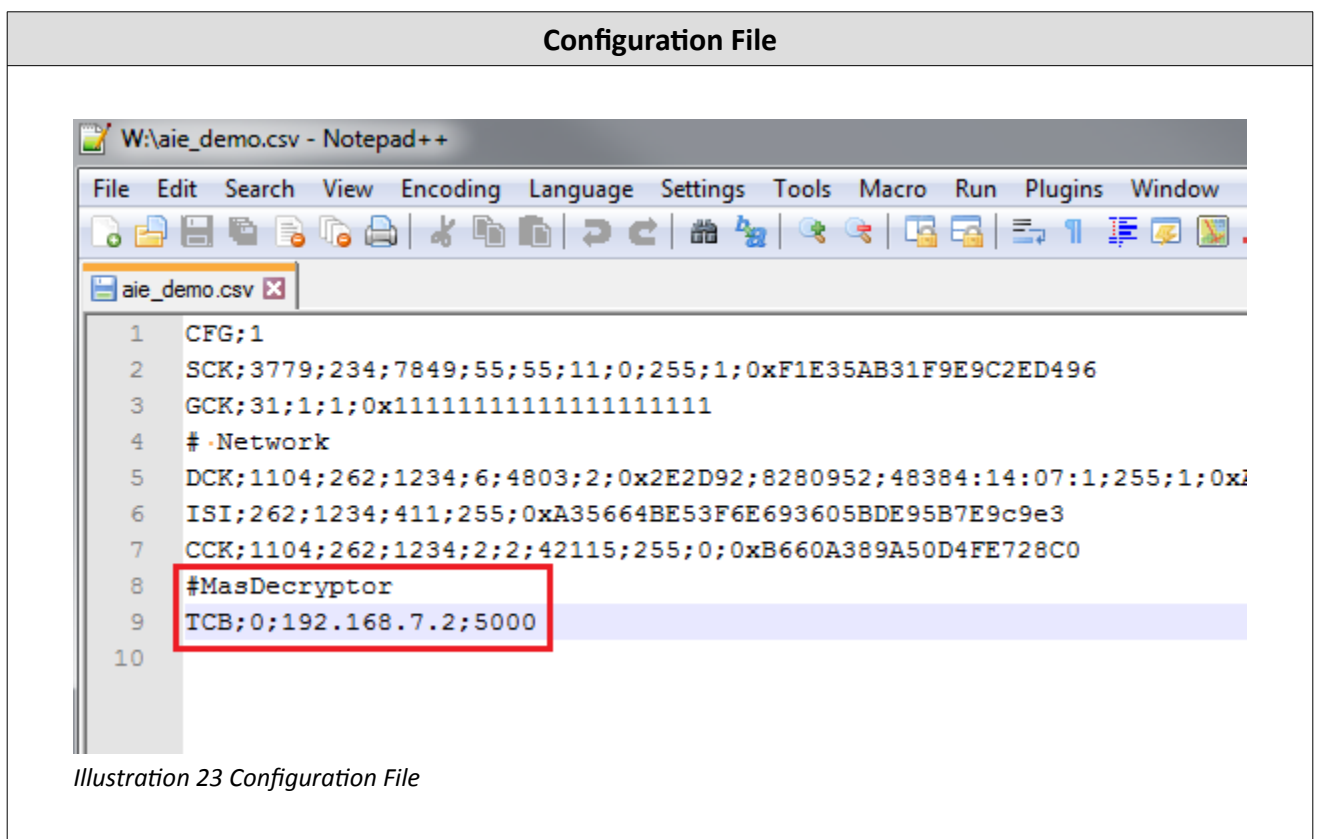
9.2 Configuring the MASDecryptor

To use the **MASDecryptor** hardware, the valid IP address and the port is needed. It is the same address as viewed in the **MASDecryptor.exe**, see chapter 6 MASDecryptor IP Address. The address is placed in the configuration file for encryption (*.csv).

The TETRA AIE Key Server of the **MultiAnalyzer**, the **MultiAnalyzerMsc**, the **MultiAnalyzerQoS** as well as the **MultiAnalyzerQosServer** supports the loading of the configuration file for encryption to get knowledge of the AIE configuration and the **MASDecryptor** connection settings. Internally the **AieSupport5V.dll** loads the configuration file and uses the IP address for the connection.

One line has to be inserted into the encryption file. The three arguments are separated by a semicolon ";" (see 23). The following table provides an overview about the information that have to be inserted into the file.

ⓘ   The default configuration line is: TCB;0;192.168.7.2;5000

Illustration 23 Configuration File

Argument	Description	
TCB	This is the keyword for the **MASDecryptor** address configuration.	
Address type	The address type contains the followed address from the **MASDecryptor**:	
	0	The address is in IPv4 format.
	1	**(NOT YET AVAILABLE)** *The address is in IPv6 format.*
IP Address + Port	The IP address and the port.	
	IPv4	The default address is "192.168.7.2". The default port is "5000". Both are separated by a semicolon ";". The full address is written as "192.168.7.2:5000".
	IPv6	**(NOT YET AVAILABLE)** *There is no default IPv6 Address. But the address is enclosed with brackets: "[" and "]". The default port is "5000". Both are separated by a semicolon ";". The full address is written as "[fe80::50fa:5aff:fedd:4cc7];5000".*

Table 5 Configuration File

The configuration file for the encryption can be loaded via the menu within the programme (see 24 and 25).
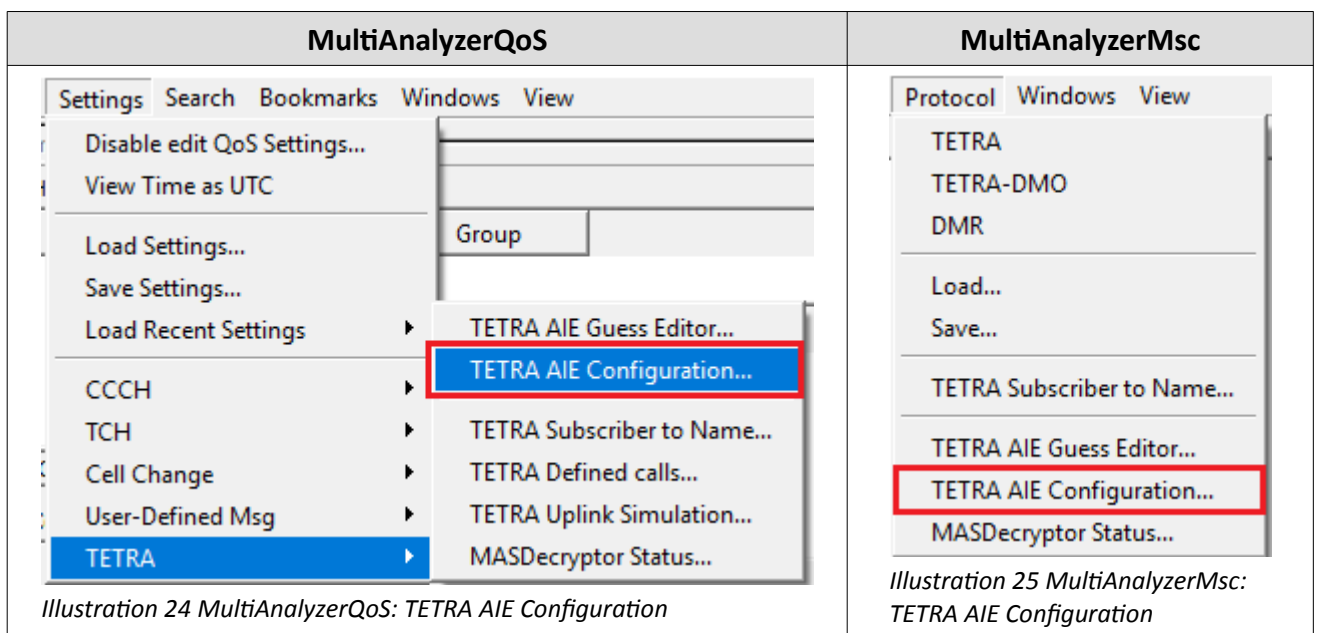
MultiAnalyzerQoS	MultiAnalyzerMsc
Illustration 24 MultiAnalyzerQoS: TETRA AIE Configuration	*Illustration 25 MultiAnalyzerMsc: TETRA AIE Configuration*

MultiAnalyzerQoS	MultiAnalyzerMsc
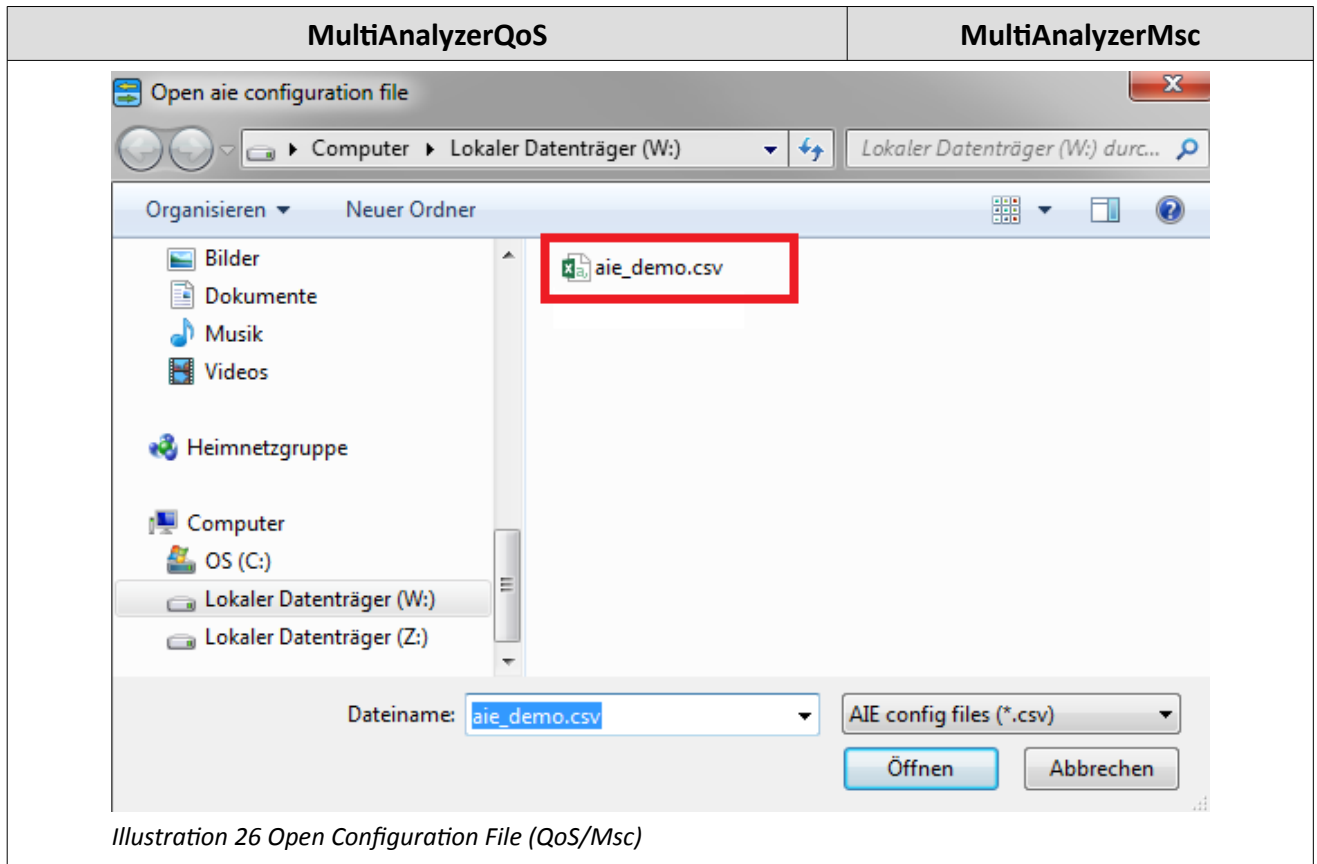
Illustration 26 Open Configuration File (QoS/Msc)

Table 6 Load Configuration File (QoS/Msc)

The programmes use the connection settings to connect to the **MASDecryptor** hardware. The **MultiAnalyzerMsc** is printing error messages if something is wrong or missing. Otherwise the enciphered messages and keys are displayed.

9.3   MASDecryptor Status

While the programmes **MultiAnalyzerMsc** or **MultiAnalyzerQoS** are analysing the data, the current status of the **MASDecryptor** can be displayed.

The information dialogue about the current **MASDecryptor** status can be called up via the menu within the programme (see 27 and 28).

Illustration 27 MultiAnalyzerQoS: MASDecryptor Status

Illustration 28 MultiAnalyzerMsc: MASDecryptor Status
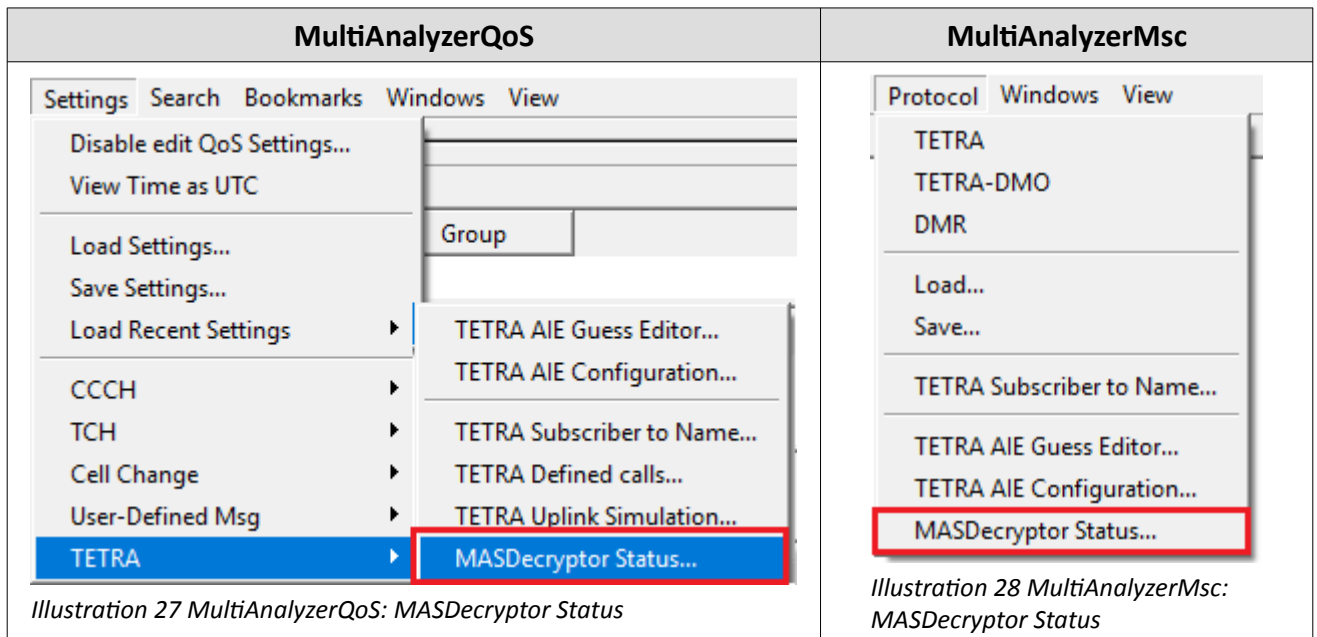
Table 7 MASDecryptor Staus (QoS/Msc)

The information dialogue shows the following data:
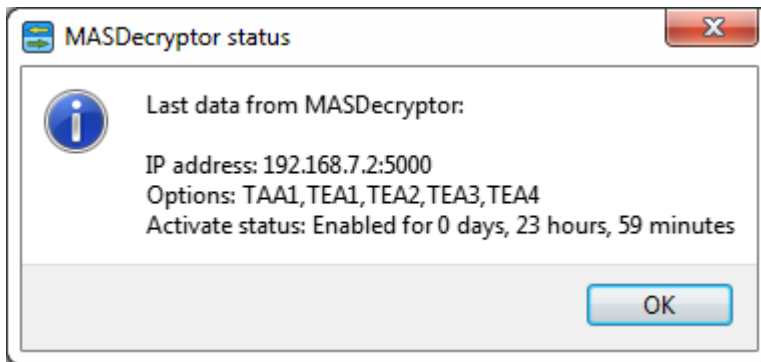
Illustration 29 MASDecryptor Status Enabled
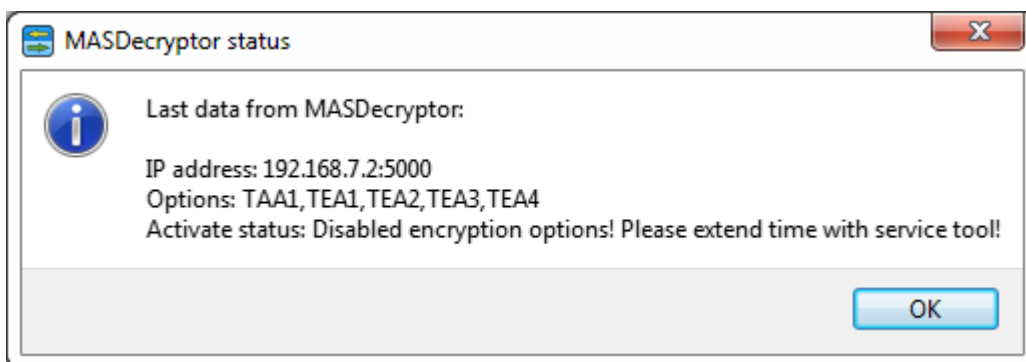
Illustration 30 MASDecryptor Status Disabled

Line	Description
Connection status	The connection status is shown if the programme analyses and displays recording data in real-time. (i) The connection status is not available if an offline analysis is running. After finishing the offline analysis, the data is displayed as long as the hardware is connected.
	Online — The hardware is used. Offline — The hardware is <u>not</u> used.
IP address	The configured (and used) IP address (see chapter <u>6 MASDecryptor IP Address</u> and <u>6.1 Configuring the IP Address</u>).
Options	The available option of the hardware and the term of validity.
Activate status	Message with activate option. The remaining operation time is displayed (see chapter <u>7 Term of Validity</u> and <u>7.1 Changing the Term of Validity</u>).

Table 8 Status Description

(i) If the runtime is expired, the "Activate status" is set to "disabled" (see 30). In this case see chapter <u>7.1 Changing the Term of Validity</u>.

10   Glossary

K

KSS	**K**ey **S**tream **S**egment	A separate KSS is produced to encrypt every timeslot for each different key to be used to encrypt PDUs in that timeslot. The KSS must have a sufficient length. The bits in the appropriate KSS are used to encrypt or decrypt the data of the control or traffic field.

T

TAA	**T**ETRA **A**uthentication **A**lgorithm	This algorithm set is intended for air interface security in TETRA products.
TAA1	**T**ETRA **A**uthentication and Key Management **A**lgorithm set **1**	
TEA	**T**ETRA **E**ncryption **A**lgorithm	The TETRA standard supports four AIE TETRA Encryption Algorithms (TEAs), these being TEA1, TEA2, TEA3 and TEA4. There are differences in the intended use and the exportability of equipment containing these algorithms. For example, TEA2 is intended for use by public safety users in Schengen and related European countries only; the others have wider applications ranging from general commercial use to public safety use in regions where TEA2 is not used.
TEA{1-4}		

11   Index

Illustration Index

Index of Tables