



securing
the digital world™

Application Notes

Pre-Boot Authentication AN-5

Purpose of Application: Secure UEFI Loader Kit - Operating System will start only when CRYPTO-BOX® is attached

Version: Smarx OS PPK 6.2

Last Update: 9 December 2014

Target Operating Systems: Windows 8/7 (32 & 64 bit)

Target Processor Platforms: Intel x86, UEFI capable

Supported Programming Tools: none required

Applicable for Product: CRYPTO-BOX® SC / XS / Versa

Secure UEFI Loader Kit: Pre-Boot Authentication with the CRYPTO-BOX®

The Secure UEFI Loader Kit implements an EFI Loader to the computer which checks for a CRYPTO-BOX on system cold boot and activates the standard Win UEFI Loader only if the valid CRYPTO-BOX was found.

It provides the following main features:

- Checking for valid Box Name or Unique Serial Number of the attached CRYPTO-BOX
- Allows to specify an alternative CRYPTO-BOX (“Super Key”) for administrative purposes
- Text messages displayed by the EFI Loader can be customized individually.



Table of Contents

- 1. UEFI Loader Kit: Overview.....3
- 2. Requirements.....3
- 3. Components and Usage.....3
 - 3.1. EFI Tool.....4
 - 3.2. EFI Installer.....5
- 4. System recovery.....5
- 5. FAQ (frequently asked questions).....6

1. Secure UEFI Loader Kit: Overview

The Secure UEFI Loader Kit is a supplemental tool which is part of the Smarx Protection Kit (PPK). It provides software manufacturers and distributors with the possibility to use the CRYPTO-BOX® for authentication prior to Operating System start (Pre-Boot Authentication). The same CRYPTO-BOX can be used for software protection and license management after system start.

2. Requirements



The Secure UEFI Loader requires a computer which is UEFI capable. Please check the documentation of your computer/mainboard for further information.

Currently only Windows 8 and Windows 7 are supported. Please [contact us](#) if you need support for other environments.

To enable UEFI boot following preparations must be made (Step-by-step instructions, settings and keys to be pressed may vary depending from the mainboard/computer manufacturer):

- Press DEL or F2 during system boot to enter UEFI setup
- Switch to Advanced Mode (press F7)
- Set options on <Boot> tab:
 - Fast Boot: <Enabled>
 - USB Support: <Full Initialization>
 - CSM (Compatibility Support Module):
 - ◆ Launch CSM: <Enabled>
 - ◆ Boot Device Control: <UEFI only> (or <both UEFI and Legacy>)
 - ◆ Boot from storage devices: <UEFI driver first>
 - Secure Boot:
 - ◆ OS Type: Windows OS



The system should be set to boot only from one (selected) Hard Drive. Boot from other devices (CDROM, USB flash drives, etc.) has to be disabled to prevent manipulations of the Loader by third persons.

Password protection on entering BIOS settings should be switched on.

3. Components and Usage

The Kit contains two command line tools:

- EFI Tool - Secure EFI Loader extraction and configuration utility
- EFI Installer - Loader installation utility

3.1. EFI Tool

The EFI Tool extracts the Secure EFI Loader (cbboot.efi) and injects the CRYPTO-BOX licensing information into it. The result is a customer specific loader.

This loader will either work with all CRYPTO-BOX units of one MARX customer, or can be limited to one specific unit (serial number is used for it).

Parameter description:

EFI_Tool.exe <TRX-file> [-SerNum:<serial number> [-SuperKey:<serial number>]] [<Lng-file>] [-Silent]

where:

<TRX file>	TRX file provided by MARX for your customer specific CRYPTO-BOX hardware (cbu_demo.trx for the CRYPTO-BOX shipped with the Evaluation Kit)
"SerNum"	(optional) specifies Serial Number of the CRYPTO-BOX to be verified
"SuperKey"	(optional, to be used with the "SerNum" option) specifies the emergency (SuperKey) CRYPTO-BOX Serial Number. The same SuperKey can be used for multiple loaders (for different CRYPTO-BOX units).
<serial number>	(optional) CRYPTO-BOX Serial Number as: <ul style="list-style-type: none">• 16-bytes HEX (Long Serial Number), "-" delimiter can be used (as displayed by MARX Analyzer)• 4-bytes HEX (DWORD, BoxName)• keyword "Auto" - to get Serial Number from the CRYPTO-BOX which is attached during EFI_Tool execution.
<Lng-file>	(optional) xml file with command line messages customization. See EFI_Lng.xml file for details - use this file as prototype for your own modifications.
"Silent"	(optional) Do not wait for key stroke after successful CRYPTO-BOX validation and proceed with system boot immediately.

Short explanation on how to use EFI_Tool:

- Place the EFI_Tool.exe, the TRX file for your CRYPTO-BOX units, and the XML file (if required) into the same directory.
- EFI_Tool.exe with parameters as described above
- The Secure EFI Loader (cbboot.efi) file will be generated, resulting output will be displayed on the console and also saved to the EFI_Tool.log file.

Examples:

EFI_Tool cbu_demo.trx

- extracts EFI loader and programs it to accept all CRYPTO-BOX units that match cbu_demo.trx profile

EFI_Tool cbu_demo.trx -SerNum:01020304

- extracts EFI loader and programs it to accept CRYPTO-BOX units with BoxName equal to 0x01020304 and matching cbu_demo.trx profile

EFI_Tool cbu_demo.trx -SerNum:01020304 -SuperKey:Auto

- extracts EFI loader and programs it to accept CRYPTO-BOX units with BoxName equal to 0x01020304 and matching cbu_demo.trx profile. Also, the Serial Number of the currently attached CRYPTO-BOX will be accepted ("Auto" option).



In case of error messages, have a look at the readme.txt file in EFI_Tool folder for return code description.

3.2. EFI Installer

The EFI Installer incorporates the EFI loader to the system partition of the target computer.



EFI Installer must be launched with admin rights.

Parameter description:

<EFI_installer> /i|/u [<path-to-loader>]

where:

/i Install the Loader

/u Uninstall Loader (restore system partition)

<path-to-loader> (optional) path to EFI loader (cbboot.efi is used as default)

Return codes:

On success 0 is returned, 1 in case of error.



To exclude any possibility of accidental replacement Secure EFI Loader with standard EFI loader during Windows Update process or its intentional replacement by potential intruder it is highly recommended to:

1. Disable automatic Windows Update on end-user's computer (switch it to manual mode)
2. Limit end-user's account with User level access rights (do not grant Admin level access rights to end-user)

Windows Update and system maintenance should be done by trusted System Administrator only.

4. System recovery

If something goes wrong (CRYPTO-BOX was lost, or the operating system does not start anymore after system update), then the Secure UEFI Loader can be removed manually from the system:

- Enter BIOS setting (Administrator needs to know the password) and allow boot from USB flash drive
- Boot from recovery USB flash drive (can be a flash drive with Windows 8/7 setup on it)
- Switch to command prompt - for example bootable USB stick with standard Windows setup:

- Boot from Flash Drive, choose Custom Installation
- When seeing “Select disk for system installation” dialog press Shift+F10: it will open console window
- Assign letter to system disk (disk where loaders are stored). For this purpose launch "diskpart" in console and do the following steps:
 - sel dis 0 (select disk with the system – volume size should be taken into account to choose the right disk)
 - sel par 2 (select partition named System, it is approx. 100Mb of size)
 - assign letter=e: (assign letter to the disk)
 - exit (complete diskpart session)
- Now restore (copy) the original EFI loader:
copy E:\EFI\BOOT\second.efi E:\EFI\Microsoft\BOOT\bootmgfw.efi



To create a bootable USB flash drive for system recovery, RUFUS utility can be used:

<http://rufus.akeo.ie>

Brief instructions for RUFUS:

Select - flash drive

- system image (loaded iso file)

- Partition Scheme: GPT partition scheme for UEFI computer

Then press Start

5. FAQ (frequently asked questions)

1. When using the EFI_Tool.exe to generate the Secure UEFI Loader, I always get an error message “Error: Decryption of 'C:\...\CBUxxxx.trx' failed - your CRYPTO-BOX(R) firmware 2.2 or higher should be attached”!

To generate these tools it is necessary to attach a CRYPTO-BOX to the computer which matches to the specified TRX-file.

2. When launching the EFI_Tool.exe with my customer specific TRX file as parameter, I get “Error: EFI not licensed”!

The UEFI Loader Kit is available as an option. Please contact your MARX distributor for more information and an offer. The CRYPTO-BOX from the Evaluation Kit and the cbu_demo.trx file can be used for testing purposes.

3. After I have updated my Windows, the Pre-Boot Authentication does not work anymore – the computer even boots without CRYPTO-BOX!

During update, Windows may have removed the UEFI Loader and restored the standard settings. In that case, please install the loader again with EFI_install.exe. Note: Windows Update and system maintenance



securing
the digital world™

Application Notes

Pre-Boot Authentication AN-5

should be done by trusted System Administrator only.



4. I have lost my CRYPTO-BOX for booting the computer! How can I restore the system?

This task has to be done by the System Administrator! Please refer to chapter 4 for instructions on system recovery.

5. Is the UEFI Loader Kit compatible with Linux or Mac OS X?

Currently only Windows is supported. Please [contact us](#) if you need support for other platforms.

CRYPTO-BOX® Data Sheet

	CRYPTO-BOX SC (CBU SC)	CRYPTO-BOX XS/Versa (CBU XS/Versa)
		
Controller chip	RISC Smart Card Processor with USB Interface	RISC Smart Card Processor with USB Interface
Chip certification	EAL4+	EAL4+
Supported operating systems	Windows, Linux, macOS, iOS, Android	Windows, Linux, macOS, iOS, Android
In hardware implemented algorithms	AES 128 Bit, RSA (up to 2048 Bit key length), others (for example: ECC) on request	AES 128 Bit in hardware, RSA up to 2048 Bit key length on driver level
Memory size (complete)	72KByte, ca. 32KByte free	4, 32 or 64 KByte
Internal memory read/write performance	ca. 80kByte/s	ca. 12kByte/s
Password (PIN/PUK)	up to 16 Byte length	
Case & LED	Designer metal housing, cast zinc, with LED display of operating status, eye for key ring/lanyard	
Connector	USB Type A	
Memory programming	minimum 100,000 write cycles	
Data retention time	minimum 10 years	
Conformity & Certifications	FCC, CE, RoHS, WEEE, USB logo	
Dimensions	14 x 7 x 32,5 mm / 0.55" x 0.28" 1.28"	14 x 7 x 32,5 mm / 0.55" x 0.28" 1.28"
Weight	7,5g	7,5g
Temperature	-10°C to +70°C / 14°F to 158°F	
Humidity	0% to 95% relative humidity	

CRYPTO-BOX Certifications



All brands, trademarks and registered trademarks are the property of their respective owners.

Evaluation Kit

www.marx.com/eval

MARX Software Security GmbH

Vohburger Strasse 68
85104 Wackerstein, Germany
Phone: +49 (0) 8403 / 9295-0
Fax: +49 (0) 8403 / 9295-40
contact-de@marx.com

www.marx.com

MARX CryptoTech LP

489 South Hill Street
Buford, GA 30518 U.S.A.
Phone: (+1) 770 904 0369
Fax: (+1) 678 730 1804
contact@marx.com