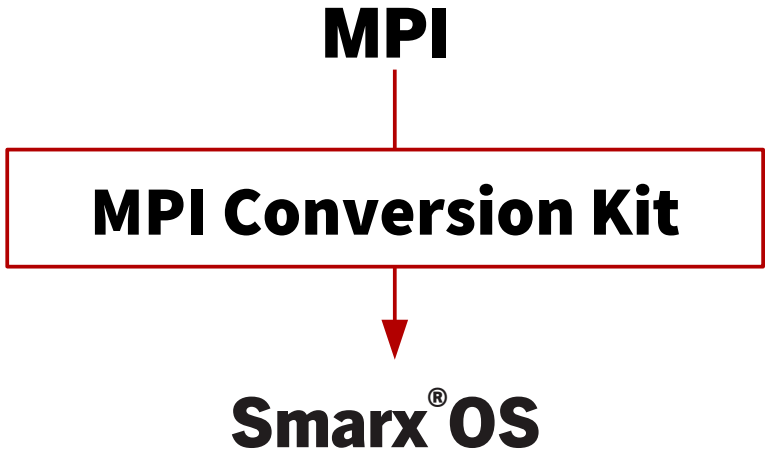
# MPI to Smarx®OS AN-3

**Purpose of Application:** Converting the CRYPTO-BOX XS and Versa from legacy MPI format to Smarx OS
**Version:** Smarx OS PPK 5.74 and later
**Last Update:** 15 November 2016
**Target Operating Systems:** Windows 10/8/7/Vista (32 & 64 bit)
**Target Processor Platforms:** Intel x86
**Supported Programming Tools:** none required
**Applicable for Product:** CRYPTO-BOX® XS / Versa, MPI Format

## Converting the MPI-formatted CRYPTO-BOX® XS or Versa to Smarx®OS

MPI (MARX Programming Interface) was developed as a "bridge" between the then-new CRYPTO-BOX for USB ports, and parallel- and serial port models. Its purpose, back in year 2000, was to provide an universal layer for various hardware platforms. Five years later, "the world was USB", and legacy ports became obsolete for the most part (we still support them, if the need will be).
Enter the Smarx System! It fully exploits the possibilities of what USB and modern security chips can offer. A plethora of features and add-ons is available, and constantly under development.
.NET support, 32/64 bit, Linux, Mac OS X, license management and remote field programming - you name it. Document- and media protection have been added, as well as sophisticated digital rights management gadgets and encryption capabilities.
Delve into our comprehensive PPK (Professional Protection Kit) and check out what makes your application iron clad secure *and* convenient for your customers!



# Table of Contents

## 1. Why should I upgrade from MPI to Smarx OS?

The purpose of this document is to explain the differences between a MPI formatted and a Smarx formatted CRYPTO-BOX. In addition, we demonstrate how you can easily upgrade your existing CRYPTO-BOX modules from MPI to Smarx OS.
MARX will continue to support and further develop the Smarx OS system.

| Feature | SmarxOS | MPI |
|---|---|---|
| WEB API Support | **Yes** | No |
| Windows 8/7/Vista (32/64Bit), Linux 32/64 and Mac OS X support | **Yes** | No |
| .NET Support, Support for Windows Store applications | **Yes** | No |
| Ability to protect multiple applications with a single CRYPTO-BOX | **Yes** | No |
| Continuous improvement and development by the MARX R&D team | **Yes** | No |

So what does all of this information have to do with you? If you are currently using a MPI formatted CRYPTO-BOX in your environment, MARX strongly recommends that you upgrade for all future releases. We discontinued MPI support and development back in 2005. By upgrading you will ensure that you are getting the most up to date support for the most widely used programming environments (including extended static libraries), support for new operating systems as they are released and the ability to fully exploit all of the functions that the CRYPTO-BOX has to offer.

The CRYPTO-BOX models 560/Net and Versa for parallel port cannot be converted to Smarx OS.

## 2. Generating the MPI2Sx Conversion Utility

### 2.1 Prerequisites

The existing MPI formatted CRYPTO-BOX USB units have to meet the following requirements:

a) All CRYPTO-BOXes have the same value of the Rijndael Fixed Key (by default this key is unique for every MARX-customer, but the same for all CRYPTO-BOXes of a customer).

b) The CRYPTO-BOX units which are subject to convert have firmware version 1.6 or higher. This is normally true for all units delivered in 2003 or later.

**IMPORTANT:** The conversion from MPI to Smarx OS cannot be reversed.

### 2.2 Installation

For the conversion you need the "*MPI to Smarx OS Conversion Kit*" which can be ordered directly from MARX (contact details can be found on the last page of this document). It contains one Smarx OS configured CRYPTO-BOX which has the same values for Rijndael Fixed Key and SCodeID1 (= User Password in Smarx OS) as your existing MPI formatted CRYPTO-BOX XS or Versa devices. Furthermore the Conversion Kit includes a CDROM with the latest Smarx OS Professional Protection Kit (PPK), and another one (labeled "Confidential") with the Hardware Profile (TRX file) needed for conversion.

**IMPORTANT:** Never disclose the Hardware profile (TRX file) or the RSA keys you received from MARX to your end-users!

Software protection and licensing with the CRYPTO-BOX always starts with the Professional Protection Kit (PPK). It contains the following main components:

- PPK Control Center - a start menu which provides access to all available options of the Protection Kit
- Smarx Application Framework (SxAF) - a project oriented, GUI based environment for software vendors and distributors which provides protection and licensing scenarios for software, data and media.
- Libraries and sample code for implementation with API for Windows, Linux, Mac OS X, iOS and Android
- Command line tools (as alternative to SxAF, especially for automation and controlling tasks within scripts or 3rd party applications)
- Tools for CRYPTO-BOX *driver installation and diagnostics*
- Documentation (*Compendium* and *API references*)

To install the PPK, please insert the CD-ROM into your CD-ROM drive. The graphical interface will start automatically (otherwise, please run the “start.exe” file on the CD-ROM). Select "Install Smarx® Professional Protection Kit" to start the installation process. After that, please follow the instructions.

### 2.3 MPI2Sx: Overview, GUI and command line mode

With the MPI2Sx conversion utility MARX offers a convenient way to convert existing CRYPTO-BOX units which were configured for the legacy MPI system to Smarx OS. This can be done even at the end-user side, so there is no need for the end-user to send the dongles back. Furthermore, MPI2Sx allows to update licensing information in the CRYPTO-BOX so that the unit is ready-to-use immediately after conversion. Of course, it is still possible to update licensing information later using Remote Update (available as an option).

There are two different ways to generate the MPI2Sx conversion utility:

- Using the GUI-based Smarx Application Framework (see chapter *2.4*)

or:

- Using the command line tool SmrxProg.exe (see chapter 2.5)

The MPI2Sx conversion utility itself can be either started in GUI mode (see chapter 3.1) or controlled via command line switches including return code evaluation (see chapter 3.2).

### 2.4 Generating the MPI2Sx conversion utility with SxAF

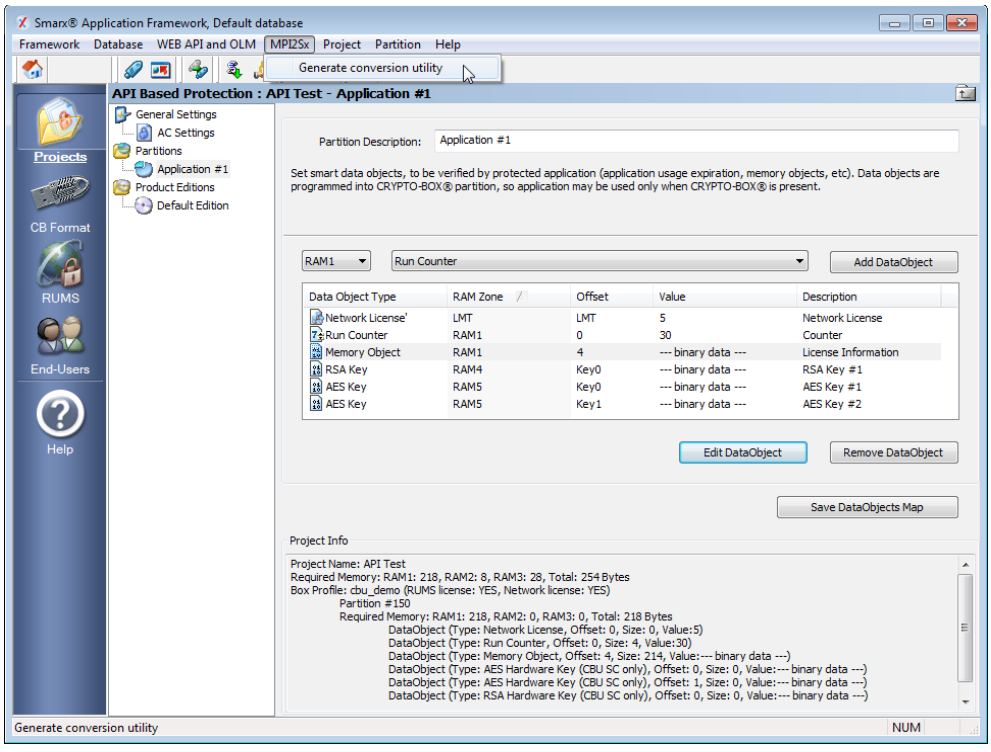
To migrate to Smarx OS and convert currently distributed MPI formatted CRYPTO-BOX units remotely, you need to:

a) Install the Smarx OS Protection Kit from the CDROM (see chapter *2.2*) and start the Smarx Application Framework (SxAF) from the Control Center (for more information how to use SxAF please refer to the

Smarx Compendium, chapter 3). Define the project you need in the Smarx Application Framework. It can be any available project type: AutoCrypt, Implementation with API, Document Protection or Media Protection - depending on your needs for protecting your software or content (see *Smarx Compendium*, chapter 4 for detailed description of all available protection options). Do not forget to specify the correct Hardware Profile (TRX file) inside the project!
After you have set up all necessary protection options, you can protect your application/document/ media content and format the Smarx OS CRYPTO-BOX which was included to the conversion kit using the CBFormat option of SxAF. Then its recommended to test if all protection options are working fine.

More information and instructions on creating projects and formatting CRYPTO-BOX units with SxAF can be found in the *Smarx Compendium*, chapter 4 or in our Application Notes for *AutoCrypt* or *Document Protection*. Check www.marx.com → Support → Documents to download the latest version of the Compendium and/or Application Notes as PDF file.

b) If everything is fine with your project, you can create the conversion utility. To do so, open your project and select "Generate conversion utility" in "MPI2Sx" menu, or click the button:




c) A new window opens which asks you if you want to verify the Rijndael Private Key and/or Rijndael Session of the CRYPTO-BOX which has to be converted. This can be useful if you want to limit the conversion to particular CRYPTO-BOX units. If you do not require such limitation, leave the default settings and click "OK". A "Save as" dialog will appear - specify the folder and the name for the conversion tool and click the "Save" button. As the result you will receive an executable file which can be used to convert MPI

formatted dongles.

d) Forward the protected application/document, the conversion utility and the .409 and .407 files to your enduser (or use the utility yourself if you are in the possession of the CRYPTO-BOX you want to convert).

e) Refer to chapter *3* for more details on how to use the MPI2Sx conversion utility.

### 2.5 Generating the MPI2Sx conversion utility with SmrxProg.exe

To migrate to Smarx OS and to convert currently distributed MPI formatted CRYPTO-BOXes remotely you need to:

a) Install the Smarx OS Protection Kit from the CDROM (see chapter *Error: Reference source not found*). The command line tool SmrxProg.exe can be found in the Protection kit Control Center under "Smarx Tools"

b) Details on how to generate an XML file for usage with SmrxProg.exe can be found in Smarx Compendium, chapter 4.9 and 7.4. Or create an individual XML file - the files SmrxProg_Demo.xml, AC_Local.xml or AC_Network.xml in the SmrxProg folder can be used as prototypes.

After you have set up your XML file, it is strongly recommended to test it with the SmarxOS CRYPTO-BOX which is included to the conversion kit to make sure that everything is working fine.

More information and instructions on creating projects and formatting CRYPTO-BOX units with SxAF can be found in the *Smarx Protection Kit Compendium*, chapter 4 or in our *Application Notes for AutoCrypt*.

c) If everything is fine with your XML file, you can create the conversion utility: store the SmrxProg.exe, the hardware profile (TRX file) and your XML file in the same folder. Then call SmrxProg with the following parameters:

SmrxProg.exe -extractMPI <TRX file> <XML file> <EXE file>

Where:

| | |
|---|---|
| <TRX file> | TRX file provided to you by MARX distributor together with your MPI2Sx Conversion Kit |
| <XML file> | XML file settings for the converted CRYPTO-BOX - this data will be written to the CRYPTO-BOX after conversion. |
| <EXE file> | File name of the generated MPI2Sx conversion utility. |

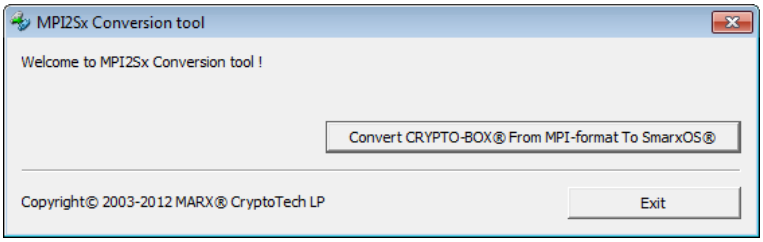
Results will be displayed on the console and directed to the SMRXPROG.LOG file.

A detailed description of all options available for SmrxProg.exe can be found in the readme.txt file in SmrxProg folder and in the *Smarx Compendium* chapter 7.4.

## 3. Converting CRYPTO-BOX units with MPI2Sx

### 3.1 GUI mode (with graphical interface)

a) Plug in the MPI-formatted CRYPTO-BOX, start the MPI2Sx executable and click the "Convert CRYPTO-BOX From MPI-format To Smarx OS" button.




Wait until the conversion process is finished, this may take up to 60 seconds (do not disconnect the CRYPTO-BOX!). When the conversion is finished you will receive a message "CRYPTO-BOX converted successfully!"

b) Now the converted CRYPTO-BOX will contain all information and Data Objects you specified in the project you created with the Smarx Application Framework (or in the XML file when SmrxProg.exe was used).

### 3.2 Quiet Mode (starting the conversion process via script or within other applications)

a) Plug in the MPI-formatted CRYPTO-BOX.

b) Call the MPI2Sx Conversion Utility with the following parameters:

{MPI2SxConvertTool}.exe -q

Where:

- {MPI2SxConvertTool} - Appropriate exe-file name (as described in chapter *2.5*)
- -q - Silent (quiet) mode

Return value:

- On success 0 (zero) is returned. If error has occurred return code will be other than zero:

| Return Code | Description |
|---|---|
| 0x80000000 | Successful |
| 0x8000006B | Wrong checksum |
| 0x8000006C | No valid CRYPTO-BOX was found |
| 0x8000006E | Some other CBIOS application is active or accesses the CRYPTO-BOX |
| 0x8000006F | Internal error: invalid parameter |
| 0x80000071 | Data decryption failed |
| 0x80000072 | Attached CRYPTO-BOX is not supported: firmware version is less than 1.6 |
| 0x80000073 | CRYPTO-BOX is not MPI formatted |
| 0x80000074 | Login to CRYPTO-BOX failed: wrong User Password (UPW) |
| 0x80000075 | Formatting error |
| 0x80000076 | Internal error: buffer is too small |
| 0x80000077 | CRYPTO-BOX memory redistribution failed |
| 0x80000078 | CRYPTO-BOX memory is too small |
| 0x80000079 | CRYPTO-BOX has unsupported memory size |
| 0x8000007A | Internal error: function is not implemented |
| 0x8000008C | Unknown error |

## 4. FAQ - frequently asked questions

**1. Is it possible to convert a Smarx OS CRYPTO-BOX back to MPI?**

This is not possible, except when sending the CRYPTO-BOX back to MARX.

**2. I need to write customer specific licensing information stored in the CRYPTO-BOX. Do I need to generate a separate conversion utility for each customer?**

Yes. But you can automatize the process of generating the conversion utility using the SmrxProg.exe command line tool (see chapter *2.5*).

**3. Does the MPI2Sx conversion utility preserve the data written in the internal memory of the MPI formatted CRYPTO-BOX during conversion?**

No, the data in the memory are overwritten with the data specified in the SxAF project where the conversion utility was created from (see chapter *2.4*). If you need help with transferring the data to the converted CRYPTO-BOX, please *contact us*.

**4. The CRYPTO-BOX cannot be converted - me resp. my customer always gets an error message when starting the conversion process.**

Please check which error message is displayed by the conversion utility. Please refer to our *technical support* and let us know the error message.

**5. Can I limit the usage of the conversion utility to a specific CRYPTO-BOX unit?**

Starting with Protection Kit version 5.74 it is possible to check the following conditions before conversion:

- Specific CRYPTO-BOX serial number (Boxname) value applies.
- Specific Rijndael Private Key resp. Rijndael Session Key value applies. Of course this check makes only sense, if one of these values was customer specific programmed for the MPI formatted CRYPTO-BOX. By default the key values are the same for all CRYPTO-BOX units delivered by MARX to one customer.

**6. For the MPI CRYPTO-BOX I had a Scode ID1 (SCODE_ID1) and a RAM Password (Password_MEM1) to access the internal memory. These values are not available for Smarx OS anymore – instead I have "UPW" and APW" values on the production sheet which came with the MPI2Sx Conversion Kit. I´m puzzled!**

SCODE_ID is equal to the User Password (UPW), Password_MEM1 is not available under Smarx OS anymore: It was emulated to ensure compatibility with the CRYPTO-BOX Parallel device at MPI times. A new value is the Administrator Password (APW), which is equal to the PASSWORD_MASTER under MPI (this value was not disclosed for MPI by default).

Application Notes

# MPI zu Smarx®OS AN-3

## CRYPTO-BOX® Datenblatt

| | CRYPTO-BOX SC (CBU SC) | CRYPTO-BOX XS/Versa (CBU XS/Versa) |
|---|---|---|
| |  |  |
| Controller-Chip | RISC Smartcard Prozessor | RISC Smartcard Prozessor |
| Chip Zertifizierungen | EAL4+ | EAL4+ |
| Unterstützte Betriebssysteme | Windows, Linux, Mac OS X, iOS, Android | Windows, Linux, Mac OS X, iOS, Android |
| In Hardware integrierte Algorithmen | AES 128 bit, RSA (bis zu 2048 Bit Schlüssellänge), andere auf Anfrage (z.B. ECC) | AES 128 Bit auf Hardwareebene, RSA (bis zu 2048 Bit Schlüssellänge, auf Treiberebene) |
| Speichergröße (insgesamt) | 72KByte, ca. 30KByte frei | 4, 32 oder 64 KByte |
| Lese-/Schreibrate interner Speicher | ca. 80kByte/s | ca. 12kByte/s |
| Passwort (PIN/PUK) | Bis zu 16 Byte Länge | |
| Gehäuse & LED | Designer-Metallgehäuse, Zinkguss, LED mit Anzeige des Betriebszustandes, Öse für Schlüsselring | |
| Steckverbindung | USB Typ A | |
| Programmierung des Speichers | minimum 100.000 Zyklen | |
| Datenerhaltszeit | minimum 10 Jahre | |
| Konformität und Zertifizierungen | FCC, CE, RoHS, USB-Logo | |
| Abmessung | 14 x 7 x 32,5 mm | 14 x 7 x 32,5 mm |
| Gewicht | 7,5g | 7,5g |
| Temperaturbereich | -10°C bis zu +70°C | |
| Luftfeuchtigkeit | 0% bis 95% relative Luftfeuchtigkeit | |

## CRYPTO-BOX Zertifizierungen

## Evaluation Kit

www.marx.com/de/store


**MARX Software Security GmbH**
Vohburger Strasse 68
85104 Wackerstein, Germany
Phone: +49 (0) 8403 / 9295-0
Fax: +49 (0) 8403 / 9295-40

**MARX CryptoTech LP**
489 South Hill Street
Buford, GA 30518 U.S.A.
Phone: (+1) 770 904 0369
Fax: (+1) 678 730 1804


www.marx.com