



**Described Version:** MPI2Sx Conversion Kit für die CRYPTO-BOX XS und Versa

**Also Applicable For:**

**Target Platforms:** Windows 32/64 Bit (Windows 7/Vista/XP, Windows Server 2008/2003)

**MARX Hardware:** CRYPTO-BOX® XS, CRYPTO-BOX® Versa

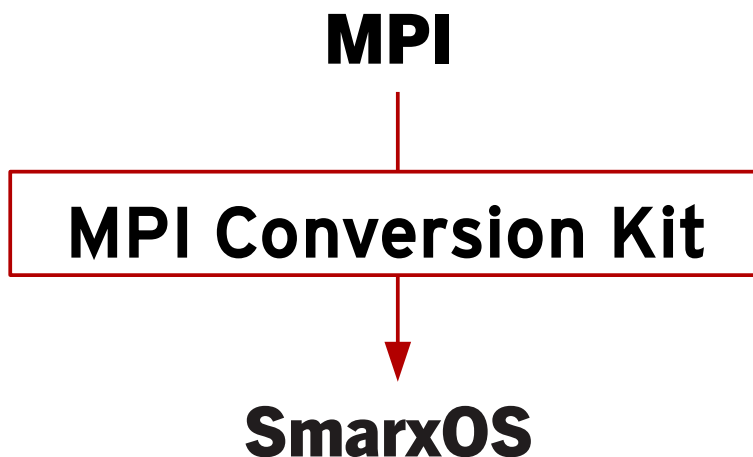
**Last Update:** 28 March 2012 by [Steffen Kaetsch](#)

## Konvertieren von MPI formatierten CRYPTO-BOX® USB Modulen zu SmarxOS®

Das MARX Programming Interface (MPI) wurde als erstes USB basierendes Format für die CRYPTO-BOX entwickelt. Ziel von MPI war es, die Kompatibilität zwischen den parallelen und seriellen Modellen der CRYPTO-BOX mit den USB-Varianten sicherzustellen.

Im Jahr 2005 hat MARX mit SmarxOS ein Nachfolgesystem entwickelt, welches für den Einsatz der USB-Version der CRYPTO-BOX optimiert wurde. MPI wird nicht mehr weiterentwickelt, daher empfiehlt sich ein Umstieg auf SmarxOS. Die Vorteile von SmarxOS gegenüber MPI werden in Kapitel 1 genauer erläutert.

Eine MPI-formatierte CRYPTO-BOX ist nicht kompatibel zu SmarxOS und umgekehrt. Mit MPI2Sx steht ein Tool zur Verfügung, welches eine einfache Konvertierung der CRYPTO-BOX von MPI zu Smarx ermöglicht - auch direkt bei Ihrem Kunden.



### CRYPTO-BOX®

- Schneller und einfacher Schutz von Windows-Anwendungen mit AutoCrypt.
- Individuelle Einbindung für alle gängigen Programmierumgebungen, inklusive .NET.
- Anpassung des CRYPTO-BOX Systems an kundenspezifische Anforderungen möglich.
- Plattform-Unabhängigkeit, unterstützt werden Windows, Linux und Mac OS X.
- Kurzes, robustes Metallgehäuse. Optional mit Kundenlogo oder Gravur.
- Serienmäßiger, interner Speicher von 4 bis 64 kB.
- Die CRYPTO-BOX ist netzwerkfähig und fern-programmierbar.
- Im Chip integrierte AES/Rijndael-Verschlüsselung.
- RSA-Support in Hardware (CRYPTO-BOX SC) oder auf Treiberebene (CRYPTO-BOX XS/Versa).



## Table of Contents

- 1. Warum Upgrade von MPI zu SmarxOS?.....3
  - 1.1 Installation .....3
- 2. Erzeugung des MPI2Sx Konvertierungstools.....4
  - 2.1 Voraussetzungen.....4
  - 2.2 MPI2Sx: Überblick, GUI- und Kommandozeilenmodus.....4
  - 2.3 Erzeugung des Konvertierungstools mit SxAF.....5
  - 2.4 Erzeugung des Konvertierungstools mit dem Kommandozeilentool SmrxProg.exe.....6
- 3. Konvertierung der CRYPTO-BOX mit MPI2Sx.....7
  - 3.1 GUI-Modus (mit grafischer Oberfläche).....7
  - 3.2 Stiller Modus (Steuerung per Skript oder aus anderen Anwendungen heraus).....7
- 4. FAQ - häufige Fragen.....9

## 1. Warum Upgrade von MPI zu SmarxOS?

Mit dem Umstieg von MPI auf das neue SmarxOS System erhalten Sie Unterstützung für alle aktuellen Plattformen und Compiler. MPI ist ein reines 32Bit-System Lösung und wird nicht mehr weiterentwickelt. Mit SmarxOS erhalten Sie nicht nur Bibliotheken und Beispiele für alle gängigen Compiler, sondern auch Unterstützung für 64Bit und weitere Plattformen wie Linux und MacOS. Durch die überarbeitete Speicherverwaltung über Partitionen lassen sich auf einfache Art und Weise mehrere Anwendungen mit nur einer CRYPTO-BOX schützen. Aber auch Nutzer der automatischen Verschlüsselung mit AutoCrypt profitieren von SmarxOS, da das neue SmarxOS-basierte AutoCrypt nicht nur mehr Schutzoptionen als sein MPI-Pendant bietet, sondern bereits ein System zur Kundenverwaltung und Verteilung von Updates enthält.

Feature	SmarxOS	MPI
Unterstützung für WEB API	Ja	Nein
Windows64, Windows Vista, Linux 32/64 and MAC OSX support	Ja	Nein
Volle .NET-Unterstützung, inkl. CBIOS4NET (objektorientierte, komponentenbasierte Syntax)	Ja	Nein
Einfacher Schutz meherer Anwendungen mit nur einer CRYPTO-BOX	Ja	Nein
Kontinuierliche Weiterentwicklung und Verbesserung durch das MARX-Entwicklerteam	Ja	Nein



Die CRYPTO-BOX Modelle 560/Net und Versa für den Parallelport können nicht zur Nutzung mit SmarxOS konvertiert werden.

### 1.1 Installation

Softwareschutz mit dem CRYPTO-BOX System beginnt mit dem Professional Protection Kit (PPK). Es enthält folgende Komponenten:

- Smarx PPK Control Center - ein Startmenü zum schnellen Zugriff auf alle verfügbaren Komponenten
- Das SmarxOS Application Framework (SxAF) - ein integriertes System zum Schutz von Software und digitaler Medien. Es enthält auch die AutoCrypt-Komponente (siehe *Error: Reference source not found*)
- Kommandozeilentools (als Alternative zum SxAF, insbesondere für Automatisierung und Skriptsteuerung)
- Tools für CRYPTO-BOX Treiberinstallation und Diagnose
- Bibliotheken und Beispiele für Einbindung in den Quellcode für Windows, Linux und Mac OS X
- Dokumentationen (Handbuch und API-Referenzen)

Um das Protection Kit zu installieren, legen Sie die PPK-CD in Ihr CD-ROM-Laufwerk ein, die Sie zusammen mit Ihrer CRYPTO-BOX Lieferung erhalten haben. Die Installation startet automatisch (andernfalls führen Sie bitte "start.exe" von der CD-ROM aus). Wählen Sie dann "Smarx® Professional Protection Kit installieren" aus und folgen Sie der Anleitung auf dem Bildschirm.

## 2. Erzeugung des MPI2Sx Konvertierungstools

### 2.1 Voraussetzungen

Die bestehenden MPI-formatierten CRYPTO-BOXen müssen die folgenden Voraussetzung erfüllen:

- a) Alle CRYPTO-BOXen besitzen denselben Rijndael Fixed Key. Standardmäßig ist dieser Schlüssel individuell für jeden Kunden von MARX, aber gleich für alle CRYPTO-BOXen eines Kunden. Daher ist dieser Punkt in den allermeisten Fällen zutreffend, außer bei Spezialfällen.
- b) Die CRYPTO-BOX Module besitzen die Firmware-Version 1.6 oder höher. Dies trifft in der Regel auf alle seit 2003 ausgelieferten Module zu.



**WICHTIG:** Die Konvertierung einer CRYPTO-BOX von MPI nach SmarxOS kann nicht rückgängig gemacht werden.

### 2.2 MPI2Sx: Überblick, GUI- und Kommandozeilenmodus

MARX bietet mit der Funktion MPI2Sx im SmarxOS Application Framework eine Möglichkeit, vorhandene CRYPTO-BOX Module die noch für das ältere MPI-System formatiert sind, nach SmarxOS zu konvertieren. Das ist auch direkt beim Endanwender möglich und hat den Vorteil, dass die CRYPTO-BOX nicht erst zurückgeschickt werden muß. Zusätzlich können Lizenzinformationen in die CRYPTO-BOX geschrieben werden, sodass die CRYPTO-BOX nach der Konvertierung sofort einsatzfähig ist. Die Möglichkeit, Lizenzen später über Remote Update (optional erhältlich) zu aktualisieren ist natürlich ebenfalls gegeben.

Zur Konvertierung benötigen Sie das "MPI zu SmarxOS Conversion Kit", welches Sie direkt bei MARX bestellen können (Kontaktinfos finden Sie auf der letzten Seite). Das Conversion Kit enthält bereits eine SmarxOS-formatierte CRYPTO-BOX. Diese hat dieselben Werte für den Rijndael Fixed Key und SCodeID1 (User-Passwort bei SmarxOS) wie Ihre bestehenden MPI-formatierten CRYPTO-BOXen. Zusätzlich erhalten Sie eine CDROM mit dem aktuellen SmarxOS Protection Kit (PPK) und eine weitere CDROM (Aufschrift "Confidential") mit dem SmarxOS Hardwareprofil (TRX-Datei), die für die Konvertierung benötigt wird.



**WICHTIG:** Geben Sie nie das Hardwareprofil Ihrer CRYPTO-BOX oder Key-Dateien, die Sie von MARX erhalten haben an Ihre Endkunden weiter!

Das Konvertierungstool MPI2Sx kann folgendermaßen erstellt werden:

- Erzeugung über die grafische Oberfläche des SmarxOS Application Frameworks (siehe Abschnitt 2.3) oder:
- Erzeugung über das Kommandozeilentool SmrxProg.exe (siehe Abschnitt 2.4)


Das damit erzeugte MPI2Sx Konvertierungsprogramm lässt sich entweder über seine grafische Oberfläche (siehe Abschnitt 3.1) oder über Kommandozeilen switches steuern, inkl. Auswertung der Fehlercodes (siehe Abschnitt 3.2).

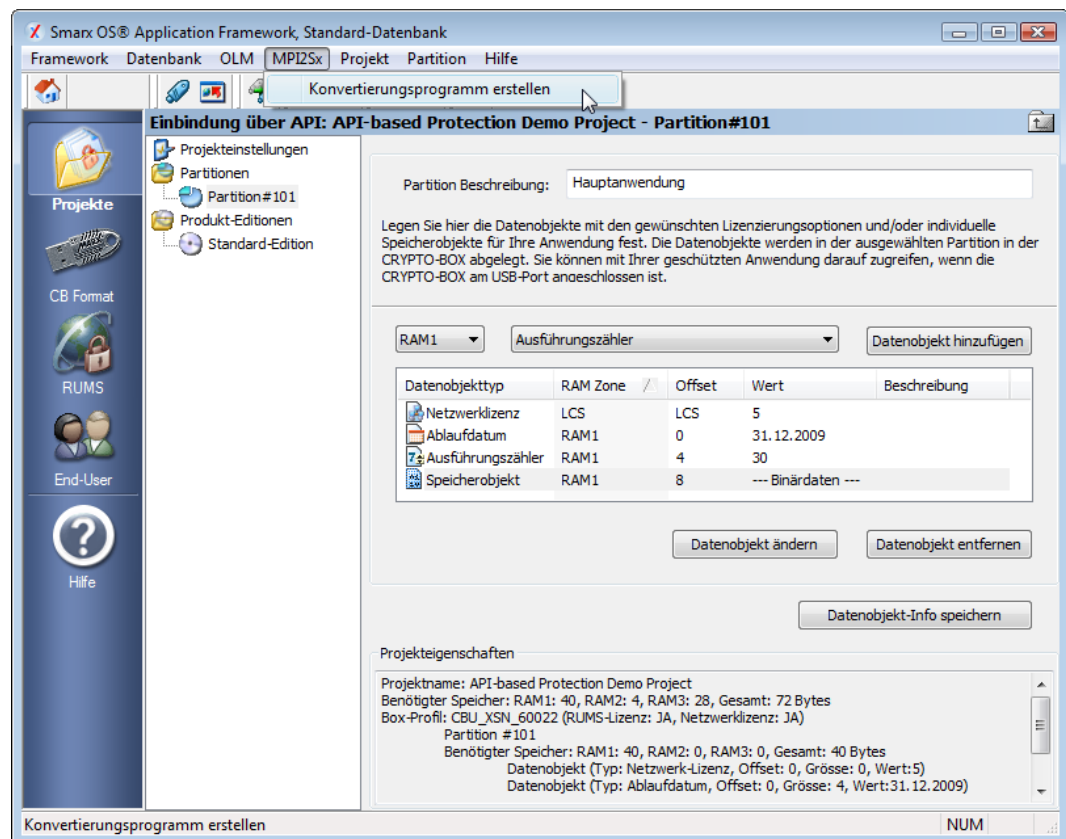
## 2.3 Erzeugung des Konvertierungstools mit SxAF

Um zu SmarxOS zu migrieren und Ihre bestehenden CRYPTO-BOX Module zu konvertieren, sind die folgenden Schritte nötig:

- Installieren Sie das SmarxOS Protection Kit von der CDROM wie in Abschnitt 1.1 beschrieben und starten Sie das SmarxOS Application Framework (SxAF) vom Control Center aus (weitere Details dazu finden Sie im beiliegenden Schnellstart-Handbuch, oder im Smarx Compendium ab Kapitel 3). Erstellen Sie Ihr gewünschtes Projekt mit dem SmarxOS Application Framework (entweder automatische Einbindung oder Implementierung über API, eine detaillierte Erklärung der beiden Optionen finden Sie im Smarx Compendium, Kapitel 4) und testen Sie den Schutz mit der enthaltenen SmarxOS-formatierten CRYPTO-BOX. Vergessen Sie nicht, Ihr Hardwareprofil von der zweiten CDROM (Aufschrift "Confidential") in Ihr Projekt zu importieren!

Nachdem Sie alle gewünschten Schutzoptionen gesetzt haben, können Sie Ihre Anwendung / Ihr Dokument schützen (nur wenn Sie AutoCrypt bzw. Document Protection einsetzen) und Ihre CRYPTO-BOX mit der Option "CB Format" im SxAF formatieren. Danach sollten Sie testen, ob alle Einstellungen richtig gesetzt sind und der Schutz mit der CRYPTO-BOX zu Ihrer Zufriedenheit arbeitet.

- Wenn Ihr Projekt wie gewünscht konfiguriert ist, können Sie das Konvertierungsprogramm erzeugen lassen. Öffnen Sie dazu das Projekt in SxAF und klicken Sie im Menü "MPI2Sx" auf den Punkt "Konvertierungsprogramm erstellen", oder die Schaltfläche  :



- Im folgenden Fenster werden Sie gefragt, ob Sie nur CRYPTO-BOX Module umprogrammieren wollen, die einen bestimmten Rijndael Private und/oder Rijndael Session Key haben. Dies kann nützlich sein,

wenn Sie die Möglichkeit der Konvertierung auf bestimmte CRYPTO-BOX Module beschränken wollen. Wenn Sie keine Einschränkungen wünschen, belassen Sie die Voreinstellung und klicken einfach auf "OK". Anschließend erscheint ein "Speichern Unter" Dialogfenster - wählen Sie den gewünschten Pfad und den Name für das Konvertierungstools aus und klicken Sie auf "Speichern". Im Ergebnis erhalten Sie das Konvertierungstool, welches Ihre bestehenden MPI-formatierten CRYPTO-BOX USB nach SmarxOS konvertiert und die im SxAF eingestellten Projekteinstellungen auf die CRYPTO-BOX überträgt.

Geben Sie Ihre geschützte Anwendung oder geschütztes Dokument, das MPI2Sx Konvertierungstool (inklusive der zugehörigen .409 und .407 Dateien) an Ihre Kunden weiter. Oder nutzen Sie das Tool selbst, wenn die CRYPTO-BOXen bei Ihnen sind. Die Benutzung des MPI2Sx Konvertierungsprogramms wird in Abschnitt erläutert.

- d) Zur Handhabung des MPI2Sx Konvertierungstools lesen Sie in Abschnitt 3 weiter.

## 2.4 Erzeugung des Konvertierungstools mit dem Kommandozeilentool SmrxProg.exe

Um zu SmarxOS zu migrieren und Ihre bestehenden CRYPTO-BOX Module zu konvertieren, sind die folgenden Schritte nötig:

- Installieren Sie das SmarxOS Protection Kit von der CDROM wie in Abschnitt 1.1 beschrieben. Das Kommandozeilentool SmrxProg.exe finden Sie im Protection Kit Control Center unter dem Punkt "Smarx Tools".
- Details dazu wie Sie eine passende XML-Datei zur Nutzung mit SmrxProg.exe erzeugen, finden Sie im Smarx Compendium, Kapitel 4.9 und Kapitel 7.4. Oder erstellen Sie eine angepasste XML-Datei in einem Editor - die Dateien SmrxProg\_Demo.xml, AC\_Local.xml oder AC\_Network.xml im SmrxProg-Ordner können Sie dabei als Prototyp verwenden. Testen Sie die erstellte XML-Datei zunächst mit der enthaltenen SmarxOS-formatierten CRYPTO-BOX.
- Wenn Ihre XML-Datei wie gewünscht konfiguriert ist, können Sie das Konvertierungsprogramm erzeugen lassen. Speichern Sie dazu die SmrxProg.exe, das Hardwareprofil (TRX-Datei) sowie die erzeugte XML-Datei im gleichen Ordner. Rufen Sie über die Konsole den folgenden Befehl auf:

```
SmrxProg.exe -extractMPI <TRX-Datei> <XML-Datei> <EXE-Datei>
```

Dabei ist:

- |             |   |
|-------------|---|
| <TRX-Datei> | die TRX-Datei, die Sie zusammen mit Ihrer kundenspezifischen CRYPTO-BOX erhalten (cbu_demo.trx beim Evaluation Kit)   |
| <XML-Datei> | die XML-Datei mit den Informationen zur Konfiguration der konvertierten CRYPTO-BOX - diese Daten werden nach dem Konvertiervorgang in die CRYPTO-BOX geschrieben. |
| <EXE-Datei> | Name des zu erzeugenden Konvertierungstools   |

Die Ergebnisse werden auf der Konsole angezeigt und in die Datei SMRXPROG.LOG ausgegeben.

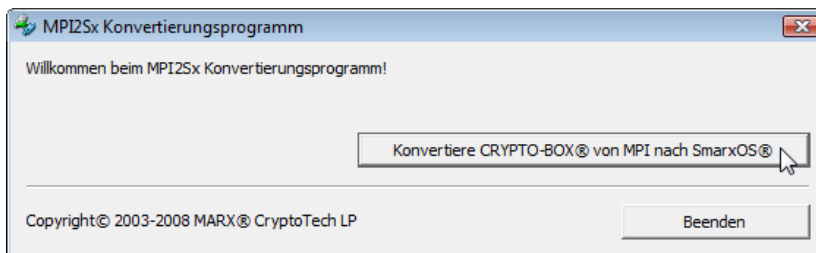


Eine detaillierte Beschreibung aller Optionen von SmrxProg.exe finden Sie in der Datei readme.txt im SmrxProg-Ordner des Protection Kits bzw. im Smarx Compendium, Kapitel 7.4.

## 3. Konvertierung der CRYPTO-BOX mit MPI2Sx

### 3.1 GUI-Modus (mit grafischer Oberfläche)

- a) Zum Konvertieren stecken Sie die MPI-formatierte CRYPTO-BOX an einen USB-Port, starten das Konvertierungstool und klicken auf den Button "Konvertiere CRYPTO-BOX von MPI-format nach SmarxOS".



Warten Sie bis die Konvertierung abgeschlossen ist, das kann bis zu 60 Sekunden dauern. Während dieses Vorgangs darf die CRYPTO-BOX nicht vom USB-Port entfernt werden! Wenn die Konvertierung erfolgreich beendet wurde, erhalten Sie die Nachricht "CRYPTO-BOX erfolgreich konvertiert!"

- b) Die konvertierte CRYPTO-BOX enthält bereits alle Einstellungen, die Sie im Projekt des SmarxOS Application Frameworks (oder in der XML-Datei wenn Sie SmrxProg.exe nutzen) vorgenommen haben.

### 3.2 Stiller Modus (Steuerung per Skript oder aus anderen Anwendungen heraus)

- a) Stecken Sie die MPI-formatierte CRYPTO-BOX an einen USB-Port.  
b) Rufen Sie das Konvertierungstool mit folgenden Parameterangaben auf:

```
{MPI2SxConvertTool}.exe -q
```

Dabei ist:

- {MPI2SxConvertTool} - Name des erzeugten Konvertierungstolls (wie in Abschnitt 2 beschrieben)
- -q - Stiller Modus (Quiet-Mode)

Rückgabewerte:

- Bei erfolgreicher Ausführung ist der Rückgabewert Null (0). Im Fehlerfall wird ein anderer Wert als Null zurückgegeben:

Fehlercode	Beschreibung
0x80000000	Erfolgreich
0x8000006B	Checksumme fehlerhaft
0x8000006C	Keine gültige CRYPTO-BOX angeschlossen
0x8000006E	Eine andere Anwendung greift auf die CRYPTO-BOX zu
0x8000006F	Interner Fehler: ungültiger Parameter

# MPI zu SmarxOS

0x80000071	Entschlüsselung der Daten fehlgeschlagen
0x80000072	CRYPTO-BOX wird nicht unterstützt, Firmwareversion ist kleiner als 1.6
0x80000073	CRYPTO-BOX ist nicht MPI-formatiert
0x80000074	Login fehlgeschlagen, falsches User Password (UPW)
0x80000075	Fehler bei der Formatierung der CRYPTO-BOX
0x80000076	Interner Fehler: Puffer ist zu klein
0x80000077	CRYPTO-BOX Speicher konnte nicht konfiguriert werden
0x80000078	Speicherplatz der angeschlossenen CRYPTO-BOX ist zu klein
0x80000079	Speichergröße der angeschlossenen CRYPTO-BOX wird nicht unterstützt
0x8000007A	Interner Fehler: Funktion ist nicht implementiert
0x8000008C	Unbekannter Fehler

## 4. FAQ - häufige Fragen

### 1. Kann ich die zu SmarxOS konvertierte CRYPTO-BOX auch wieder zurück nach MPI konvertieren?

Das ist nicht möglich, außer Sie senden die CRYPTO-BOX zurück an MARX.

### 2. Ich habe kundenspezifische Lizenzinformationen in der CRYPTO-BOX. Muss ich für jeden Kunden ein eigenes Konvertierungstool erzeugen?

Ja. Sie können die Erzeugung des Konvertierungstools automatisieren, wenn Sie das Kommandozeilentool SmrxProg.exe einsetzen (siehe Abschnitt 2.4)

### 3. Die CRYPTO-BOX lässt sich nicht konvertieren, ich bzw. mein Kunde erhält immer eine Fehlermeldung.

Prüfen sie in diesem Fall folgendes:

- Welche Fehlermeldung wird von Konvertierungstool ausgegeben?
- Wenn das Konvertierungstool eine Fehlermeldung ausgibt, dass keine CRYPTO-BOX gefunden wurde: Prüfen Sie, ob die CRYPTO-BOX Treiber korrekt installiert sind und die LED an der CRYPTO-BOX leuchtet. Sie können die korrekte Installation der CRYPTO-BOX mit dem Tool "MARX Analyzer" prüfen (auch beim End-User). Sie finden das Treibersetup "CBUSetup" und den MARX Analyzer unter [www.marx.com/downloads](http://www.marx.com/downloads).



In allen anderen Fällen wenden Sie sich bitte mit Angabe der Fehlermeldung an unseren Technischen Support.

### 4. Kann ich den Einsatz des Konvertierungstools auf eine bestimmte CRYPTO-BOX begrenzen?

Ab Protection Kit Version 5.74 ist es möglich, folgende Bedingungen vor der Konvertierung zu prüfen:

- CRYPTO-BOX Seriennummer (Boxname) muss bestimmten Wert haben
- Rijndael Private Key bzw. Rijndael Session Key muss bestimmten Wert haben. Diese Prüfung macht natürlich nur dann Sinn, wenn bei der MPI-formatierten CRYPTO-BOX einer dieser Werte kundenspezifisch programmiert wurde - standardmässig sind die Key-Werte für alle von MARX an einen Kunden gelieferten CRYPTO-BOX Module gleich.

## CRYPTO-BOX Datenblatt

	CRYPTO-BOX SC (CBU SC)	CRYPTO-BOX XS/Versa (CBU XS/Versa)
		
Controller-Chip	8/16 bit RISC Smartcard Prozessor	8 Bit Microcontroller mit USB Interface
Chip Zertifizierungen	EAL4+ / ISO 7816	WHQL (Microsoft)
Unterstützte Betriebssysteme	Windows 7/Vista/XP/2000, Linux, Mac OS X	Windows 7/Vista/XP/2000, Linux, Mac OS X
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, min. 32KByte frei	4, 32 oder 64 KByte
Lese-/Schreibrate interner Speicher	ca. 80kByte/s	ca. 1,3kByte/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	mehr als 1 Million Zyklen, 100.000 garantiert	
Datenerhaltszeit	minimum 10 Jahre	
Konformität und Zertifizierungen	FCC, CE (TÜV Rheinland), RoHS, USB-Logo	
Abmessung	15 x 6 x 38 mm	14 x 8 x 36 mm
Gewicht	10,5g	9,2g
Temperaturbereich	0°C bis zu +60°C	
Luftfeuchtigkeit	0% bis 95% relative Luftfeuchtigkeit	

### CRYPTO-BOX Zertifizierungen



Alle Marken, Warenzeichen und registrierte Warenzeichen sind Eigentum der jeweiligen Inhaber.

### CRYPTO-BOX Evaluation Kit

[www.marx.com/eval](http://www.marx.com/eval)

#### MARX Software Security GmbH

Vohburger Strasse 68  
85104 Wackerstein, Deutschland  
Phone: +49 (0) 8403 / 9295-0  
Fax: +49 (0) 8403 / 1500  
contact-de@marx.com

#### MARX CryptoTech LP

3355 Annandale Lane #2  
Suwanee, GA 30024 U.S.A.  
Phone: (+1) 770 904 0369  
Fax: (+1) 770 904 3893  
contact@marx.com

[www.marx.com](http://www.marx.com)