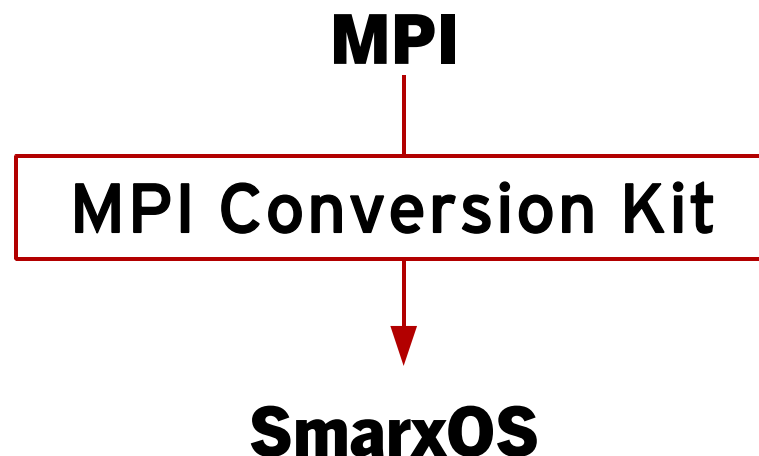


Konvertieren von MPI formatierten CRYPTO-BOX[®] USB Modulen zu SmarxOS[®]

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 dem SmarxOS ein Nachfolgesystem entwickelt, welches für den Einsatz der CRYPTO-BOX USB optimiert wurde.



Download der neuesten Application Notes:

www.marx.com/AN

1. Warum Upgrade von MPI zu SmarxOS?

1

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.

2. Schritte zur Konvertierung nach SmarxOS

2.1 Voraussetzungen

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

- 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.
- 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.

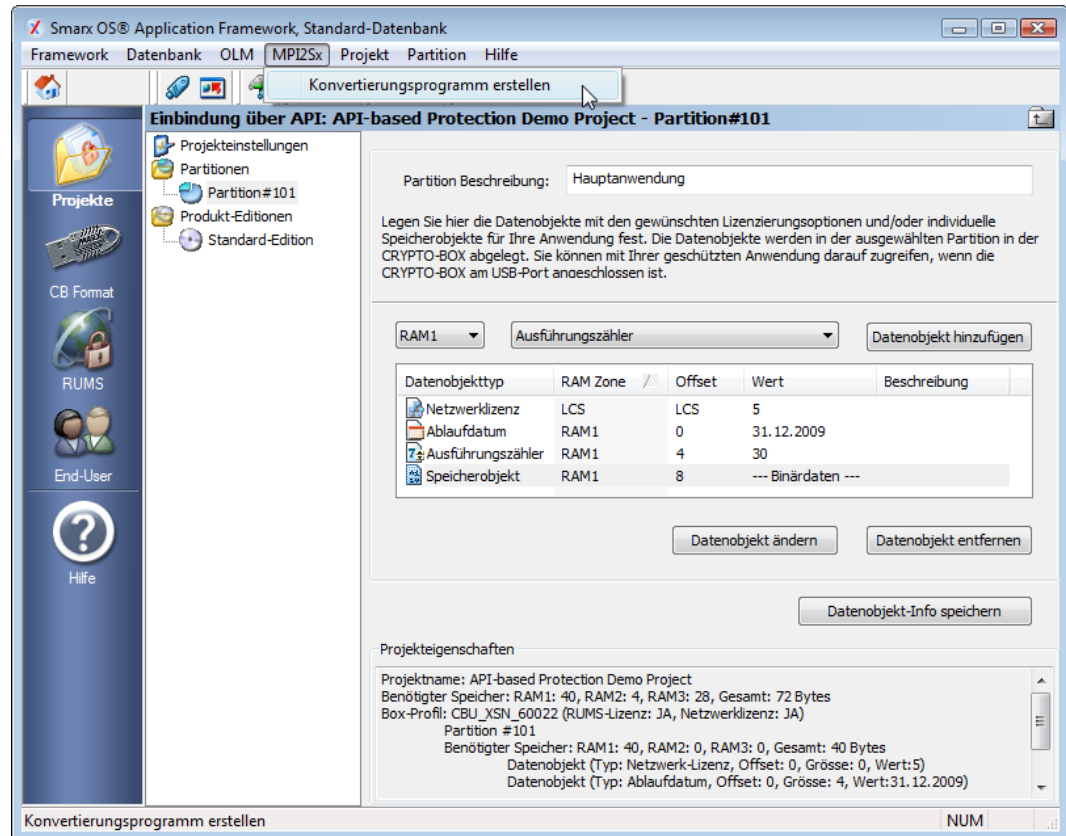
2. Schritte zur Konvertierung nach SmarxOS 2

2.2 Prozedur für die Migration von MPI zu SmarxOS

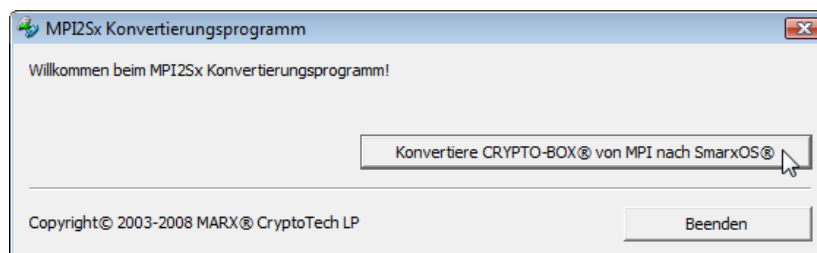
MARX bietet mit der Funktion MPI2Sx im SmarxOS Application Framework eine Möglichkeit, vorhandene CRYPTO-BOX Module die noch für das ältere MPI-System formatiert sind, nach SmarxOS umzuformatieren. Das ist auch direkt beim Endanwender möglich und hat den Vorteil, dass die CRYPTO-BOX nicht erst zurückgeschickt werden muß. Um zu SmarxOS zu migrieren und Ihre bestehenden CRYPTO-BOX Module zu konvertieren, sind die folgenden Schritte nötig:

- a) Bestellen Sie das "MPI zu SmarxOS Conversion Kit", welche bereits eine SmarxOS-formatierte CRYPTO-BOX USB enthält. Diese CRYPTO-BOX 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 mit dem SmarxOS Hardwareprofil (TRX-Datei), die für die Konvertierung benötigt wird.
- b) Installieren Sie das SmarxOS Protection Kit von der CDROM und starten Sie das SmarxOS Application Framework (SxAF) vom Control Center aus (weitere Details dazu finden Sie im beiliegenden Schnellstart-Handbuch, oder im SmarxOS Compendium ab Kapitel 2). Erstellen Sie Ihr gewünschtes Projekt mit dem SmarxOS Application Framework (entweder automatische Einbindung oder Implementierung über API, siehe Kapitel 3 bzw. 4 im Compendium) und testen Sie den Schutz mit der enthaltenen SmarxOS-formatierten CRYPTO-BOX. Vergessen Sie nicht, Ihr Hardwareprofil von der zweiten CDROM 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.
- c) 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  :

2. Schritte zur Konvertierung nach SmarxOS 3



- d) 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 Konvertierungstool 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 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.
- e) 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 nach SmarxOS".



2. Schritte zur Konvertierung nach SmarxOS 4

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!"

- f) Die konvertierte CRYPTO-BOX enthält bereits alle Einstellungen, die Sie im Projekt des SmarxOS Application Frameworks erstellt haben.



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

Securing the digital world

The CRYPTO-BOX® is ideal for

- **Software Protection**
- **License Management**
- **Remote Updates**
- **Web Security**
- **Secure Online Identification**
- **Access Control (online business)**
- **Content Protection (DRM)**

CRYPTO-BOX Evaluation Kit

www.marx.com/kit

+49(0)8403 / 9295-0



CRYPTO-BOX Datasheet

	CRYPTO-BOX 2	CRYPTO-BOX 2000
Controller chip	8/16 bit RISC Smart Card Processor Atmel AT90SC series with USB interface	8 Bit micro controller with USB interface
Chip certifications	EAL4+ / ISO 7816	WHQL (Microsoft)
Firmware	Proprietary MARX	Proprietary MARX
Supported operating systems	Windows Vista/XP/2000, Linux, MacOS X (in preparation)	Windows Vista/XP/2000, Linux, MacOS X
In hardware integrated algorithm	AES 128 bit, RSA up to 2048 bit key length, others (i.e. ECC) on request	AES 128 bit in hardware, RSA up to 2048 bit key length (on driver level)
Memory size	72Kbytes, minimum 32KBytes free	4, 32 or 64 KBytes
Reading / writing rate internal memory	Read: ca. 80Kbytes/s Write: ca. 30Kbytes/s	Read/write: ca. 1.3KBytes/s
Password (PIN/PUK)	Up to 16 bytes sequence	
Case & LED	Metal Designer Case, LED displays the operating mode, eye for key ring/lanyard	
Connector	USB Type A	
Memory programming	Typically more than 1 million cycles; 100 000 guaranteed	
Data durability	10 years	
Conformity & certifications	FCC, CE, RWTUEV, RoHS, USB Logo	
Dimensions	0.51" x 0.28" x 1.38" (13 x 7 x 35 mm)	0.51" x 0.32" x 1.38" (13 x 8 x 35 mm)
Weight	0.282 oz (8.0g)	0.326 oz (9.2g)
Temperature range	+32°F to +140°F (0°C to +60°C)	
Air humidity	0% to 95% relative humidity	

CRYPTO-BOX certifications



All trademarks used in this document are property of their respective owners.

MARX Software Security GmbH

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

www.marx.com

MARX CryptoTech LP

3355 Annandale Lane, Suite 2
Suwanee, GA 30024
Phone: (+1) 770 904 0369
Fax: (+1) 770 904 3893
info@cryptotech.com

Download the latest White Papers: www.marx.com/AN