

**Thema:** Hardwareprofil (TRX-Datei) zur Konfiguration der CRYPTO-BOX

**Version:** Smarx OS PPK 5.90 oder höher

**Zuletzt geändert:** 15. November 2016 von [Steffen Kaetsch](#)

**Ziel-Betriebssystem:** Windows, Linux, OS X

**Zielplattform:** Intel x86

**Unterstützte Programmierertools:** nicht erforderlich

**Anwendbar für Produkt:** CRYPTO-BOX® SC / XS / Versa

## Einsatz des CRYPTO-BOX® Hardwareprofils (TRX-Datei)

Das Hardwareprofil ermöglicht eine einfache und schnelle Konfiguration der CRYPTO-BOX mit kundenspezifischen Daten. Alle Zugriffsinformationen auf die CRYPTO-BOX sind in diesem Hardwareprofil gespeichert. Ein umständliche Eingabe der Zugriffspasswörter (User-Passwort und Administrator-Passwort) in den Tools des Smarx OS Protection Kits entfällt daher. Darüber hinaus bestimmt das Hardwareprofil, welche Zusatzoptionen des Smarx OS Protection Kits nutzbar sind, beispielsweise Remote Update (RUMS), Document Protection, Media Protection oder Pre-Boot Authentisierung.



### 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 macOS.
- 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).

## Inhaltsverzeichnis

1. Importieren des Hardwareprofils in das Smarx® Application Framework.....3
2. Nutzung des Hardwareprofils mit den kommandozeilenbasierten Tools.....4

## 1. Importieren des Hardwareprofils in das Smarx® Application Framework

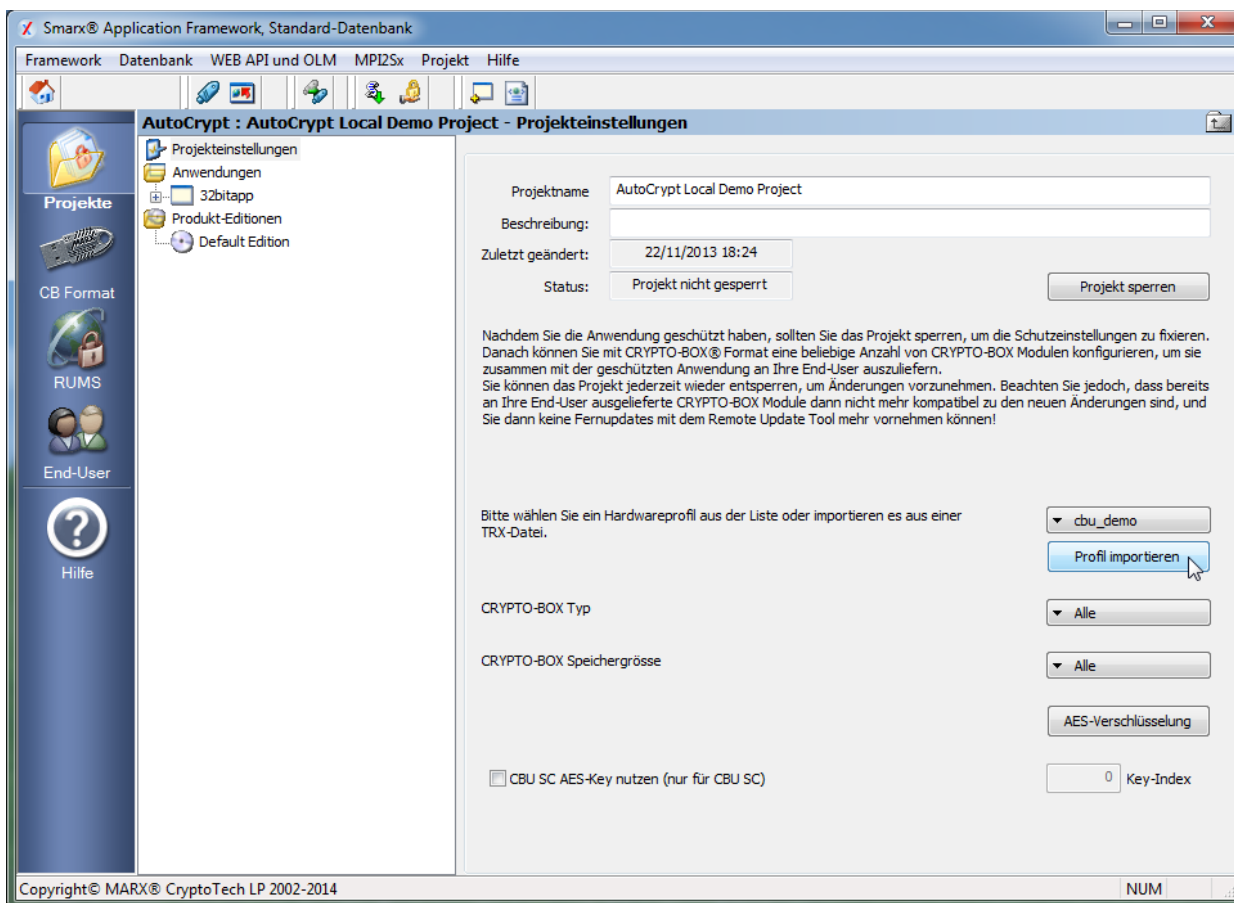


Das Hardwareprofil enthält die Zugriffscode für Ihre CRYPTO-BOX, geben Sie es daher keinesfalls an Ihre Endkunden weiter!

Das Smarx Application Framework (SxAF) ist die zentrale Schaltstelle zur Erstellung von Projekten für automatischen Schutz (AutoCrypt), Einbindung über API, sowie Document Protection. Weitere Details zum SxAF und den einzelnen Projekttypen finden Sie im [Smarx Compendium](#), Kapitel 4.

So importieren Sie das Hardwareprofil:

- Starten Sie das SxAF und erstellen Sie ein neues Projekt oder öffnen Sie ein bestehendes



- Wählen Sie im Verzeichnisbaum (mittleres Fenster) den Punkt "Projekteinstellungen"
- Klicken Sie im rechten Fenster auf "Profil importieren", um das Hardwareprofil zu laden.
- Legen Sie die CDROM mit der Aufschrift "Confidential" ein, die Sie zusammen mit Ihrer CRYPTO-BOX Lieferung erhalten haben. Wählen Sie die .trx-Datei auf der CDROM aus und klicken Sie auf "Öffnen"



Zum Import des Hardwareprofils muss eine zum Profil passende CRYPTO-BOX angeschlossen sein.

- Nach dem Import erscheint das Profil in der Auswahlliste und kann mit bestehenden und neuen SxAF-Projekten genutzt werden



Sie können einige Optionen des SxAF (z.B. RUMS und Document Protection) nur nutzen, wenn Sie eine Lizenz dafür erworben haben. Diese erhalten Sie von MARX oder Ihrem Distributor in Form einer aktualisierten TRX-Datei. Wenn Sie keine Lizenz haben, wird eine Fehlermeldung angezeigt.

## 2. Nutzung des Hardwareprofils mit dem AutoCrypt Wizard

Der AutoCrypt Wizard stellt den einfachsten und schnellste Weg zum Schutz von Windows-Anwendungen (.exe und .dll-Dateien) dar. Der Wizard führt Sie durch alle Schritte - vom Schutz der Anwendung über die Konfiguration der CRYPTO-BOX bis hin zu Remote Updates (optional). Weitere Details zur Nutzung des Hardwareprofils mit dem AutoCrypt Wizard finden Sie in den [AutoCrypt Application Notes](#), Kapitel 2.

## 3. Nutzung des Hardwareprofils mit den kommandozeilenbasierten Tools

Neben dem Smarx Application Framework (SxAF) stehen im Protection Kit diverse Kommandozeilentools zur Verfügung. Diese bieten mehr Flexibilität als die grafische Oberfläche des SxAF. So können Sie auch von externen Anwendungen oder Batch-Dateien heraus aufgerufen werden. Damit ist eine Anbindung an nahezu jedes bestehende Distributionssystem und ein hoher Grad an Automatisierung möglich.

Sie finden die Kommandozeilentools im Smarx Protection Kit unter:

`[Smarx OS PPK Installationsordner]\Tools\`

oder durch Klick auf die Schaltfläche "Treiber & Tools" im Control Center des Protection Kits.

Folgende Tools sind verfügbar:



- AC\_Tool.exe - automatischer Schutz von Anwendungen (analog zu AutoCrypt im SxAF)
- SmrxProg.exe - Konfiguration der CRYPTO-BOX (analog zu CB Format im SxAF)
- RU\_Tool.exe - Remote Update Tool (analog zu RUMS im SxAF)
- Doc\_Tool.exe - automatischer Schutz von Dokumenten ( analog zu Document Protection im SxAF)
- EFI\_Tool.exe und EFI\_Installer.exe – Secure EFI Loader (Pre-Boot Authentisierung mit der CRYPTO-BOX)

Details zum Aufruf des Hardwareprofils über die Kommandozeilentools finden Sie in der Readme-Datei im Ordner des jeweiligen Tools und im [Smarx Compendium](#), Kapitel 6.



Sie können einige Tools (z.B. RU\_Tool.exe oder Doc\_Tool.exe) nur nutzen, wenn Sie eine Lizenz dafür erworben haben. Diese erhalten Sie von MARX oder Ihrem Distributor in Form eines aktualisierten Hardwareprofils (.TRX-Datei). Wenn Sie keine Lizenz haben, wird eine Fehlermeldung angezeigt.

## 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
Lesen-/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



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

### Evaluation Kit

[www.marx.com/de/store](http://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

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