

Cross-Platform Software Protection **CRYPTO-BOX® & Qt4**



Described Version:	Qt4 4.2.3
Also applicable for:	Qt4 4.x
Target platforms:	Windows Vista/XP/2000, Linux, MacOS
MARX hardware:	CRYPTO-BOX USB

Qt - Code Less! Create More!

Qt is a cross-platform application and user interface framework. Using Qt allows writing applications once and deploy them across many desktop and embedded operating systems without rewriting the source code. It includes an intuitive C++ class library, integrated development tools, high runtime performance and offers portability across desktop and embedded operating systems.

Qt and the SmarxOS Application Framework

The SmarxOS API is best applicable for cross-platform development, because it supports all common operating systems. This approach allows developers to use one source code for all platforms.



The CRYPTO-BOX:

- On-board encryption of data with Rijndael algorithm.
- Software-based authentication with RSA standard.
- Access control (PIN-based).
- Every CRYPTO-BOX USB has its own unique serial number.
- Encrypted EEPROM with on-board memory.
- Reliable communication and CRYPTO-BOX identification.
- and many more.



Download

Download the latest Application Notes:

www.cryptotech.com/AN



1. Introduction

MARX allows customers to add hardware protection to their software products running under all popular platforms:

- Windows 32 and 64;
- Linux 32 and 64;
- MAC OSX (Intel and PPC hardware architecture).

Even more - SmarxOS API is supported for all operating systems mentioned above as “one source code for all platforms”. This approach allows developers to use SmarxOS API for cross-platform development.

MARX recommends considering Trolltech Qt cross-platform GUI framework environment for this purpose. Samples demonstrating the usage of the SmarxOS API under Qt are available in the SmarxOS Protection Kit for the CRYPTO-BOX USB, please refer to the point "Software Protection for Developers SmarxOS API" in the Protection Kit Control Center.

2. Brief overview of Qt4

Qt (<http://www.trolltech.com>) is an open source C++ toolkit for cross-platform GUI application development. Since its commercial introduction in early 1996, Qt has formed the basis of many thousands of successful applications worldwide and proved itself to be a mature and robust solution. Qt is also the basis of the popular KDE Linux desktop environment, a standard component of all major Linux distributions.

Besides GUI framework Qt also includes C++ libraries for file handling, networking, process handling, threading, database access, XML processing, OpenGL integration and others.

Qt is currently supported for the following platforms:

- Microsoft Windows: Vista, XP, 2000
- Unix/X11: Linux, Sun Solaris, HP-UX, HP Tru64 UNIX, IBM AIX, SGI IRIX and many others
- Mac OS X: Mac OS X 10.3 +
- Embedded Linux: Linux platforms with frame buffer support

Development of Qt applications is supported by GUI (Graphical User Interface) layout and forms visual designer (Qt Designer), a set of internationalization tools (Qt Linguist) and comprehensive API documentation (Qt Assistant).

3. Adding hardware protection to Qt4-based projects

The CRYPTO-BOX USB offers quick and robust solution for software protection in Qt-based projects.

SmarxOS 32/64-Bit interface provides efficient, flexible, and convenient way to protect software and data against piracy and unauthorized usage, allowing developers to take advantage of all outstanding features CRYPTO-BOX USB hardware offers:

- On-board encryption of data with Rijndael algorithm (AES – Advanced Encryption Standard, official successor to the DES algorithm).
- 16 bytes key that never leaves the hardware platform, in OFB bit-stream cipher mode (Output Feedback Mode).
- Software-based authentication method supporting RSA standard (key length up to: 2048 Bits).
- Access control (PIN-based).
- Every CRYPTO-BOX USB (except USB Versa) has its own unique serial number.
- Encrypted EEPROM with 4 kByte of on-board memory (up to 64 kByte available on request).
- Reliable communication and CRYPTO-BOX identification.

As mentioned above, SmarxOS® API is supported for all major platforms: Microsoft Windows (Vista, XP, 2000), Linux, and Mac OS X (both Intel and PowerPC architectures).

Besides the full control over CRYPTO-BOX USB hardware SmarxOS API also provides a rich set of features for application developers:

- Sharing CRYPTO-BOX memory by different applications.
- Concurrent access to a CRYPTO-BOX by different processes/threads.
- Caching CRYPTO-BOX calls.
- Digital signature.
- Establishing secure communication channel, secure document submission, Remote Update.
- Network License Management and many others.

The full set of Smarx API software protection features (including networking, license management and comprehensive hardware control) is natively available for Qt developers.

SmarxOS API is available for Qt application developers as native (MinGW build on Windows) C/C++ static and dynamic libraries for all platforms. Libraries provide identical C/C++ API and share the same header files so the same software protection code can be used on all platforms. It entirely conforms to the cross-platform nature of Qt applications development and allows easy and reliable protection of crossplatform Qt applications with CRYPTO-BOX USB.

The same software protection code can be used on all platforms entirely conforming to the cross-platform nature of Qt application development.

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.cryptotech.com/eval
+49(0)8403 / 9295-19



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

MARX CryptoTech LP

4485 Tench Road #310
Suwanee, GA 30024 U.S.A.
Phone: (+1) 770 904 0369
Fax: (+1) 770 904 3893
info@cryptotech.com

www.cryptotech.com

Download the latest Application Notes: www.cryptotech.com/AN