



Smarx[®] API: extending D environment with external APIs

Described Version:	D 1.0
Also applicable for:	D 1.0
Target platforms:	Windows Vista 32/64 /XP/2000, Linux, Mac OS
MARX hardware:	CRYPTO-BOX [®] USB

Quick and efficient hardware based software protection!

D is a new general purpose systems and applications programming language. It combines the power and high performance of C and C++ with the programmer productivity of modern languages like Ruby and Python. Special attention is given to the needs of quality assurance, documentation, management, portability and reliability.

Only by protecting your software and/or data, you can guarantee that every single user has paid for your software and your intellectual property. MARX[®] provides D developers with robust and reliable way to integrate protection to their software and intellectual property. With the MARX CRYPTO-BOX USB state-of-the-art hardware system and based on it SmarxOS[®] API, solutions and technologies offered by MARX you will be able to protect your D applications against piracy and unauthorized usage in the most efficient way.

- On-board encryption of data with Rijndael algorithm
- Encrypted with 4kByte of on-board memory (up to 64 kByte available upon request)
- Reliable communication and CRYPTO-BOX identification



Table of Contents

- 1. Developing applications with D programming environment: brief overview.....2
- 2. SmarxOS® API: extending D environment with external APIs2
 - 2.1 Using External DLLs.....2
 - 2.2 Using COM.....2
- 3. Using MARX CRYPTO-BOX® USB with D projects.....2
- 4. Protecting your programs with SmarxOS® API.....3
- 5. CRYPTO-BOX® USB.....4
- Appendix.....5
 - Appendix A – Distributors.....5
 - Appendix B - CrypToken Certifications and MARX Memberships.....5

1. Developing applications with D programming environment: brief overview

D is a new general purpose systems and applications programming language. It combines the power and high performance of C and C++ with the programmer productivity of modern languages like Ruby and Python. Special attention is given to the needs of quality assurance, documentation, management, portability and reliability.

The D language is statically typed and compiles directly to machine code. It is multi-paradigm, supporting many programming styles: imperative, object oriented, and meta-programming. It's a member of the C syntax family, and its appearance is very similar to that of C++. Currently there are currently two implementations, the [Digital Mars DMD](#) package for Win32 and x86 Linux, and the [GCC D Compiler](#) package for several platforms, including [Windows](#) and [Mac OS X](#).

2. SmarxOS® API: extending D environment with external APIs

2.1 Using External DLLs

D provides an easy support for external DLLs:

<http://www.digitalmars.com/d/faq.html#omf>

"...There is one case where using existing C libraries does work – when those libraries come in the form of a DLL conforming to the usual C API interface. The linkable part of this is called an "import library", and Microsoft COFF format import libraries can be successfully converted to DMD OMF using the coff2omf tool..."

This approach is used to integrate CBIOS API calls into D. The latest SmarxOS® PPK contains CBIOS support for D implemented for Win32 platform.

2.2 Using COM

D environment for Win32 platform allows developers to create COM objects with D, however external COM objects are also supported from D programs:

<http://www.digitalmars.com/d/dll.html>

"...COM objects are analogous to D interfaces. Any COM object can be expressed as a D interface, and every D object with an interface X can be exposed as a COM object X. This means that D is compatible with COM objects implemented in other languages..."

This functionality allows D developers to use SMRXCOS interface to integrate MARX hardware protection to their programs.

3. Using MARX CRYPTO-BOX® USB with D projects

Only by protecting your software and/or data you, can guarantee that every single user has paid for your software and your intellectual property. MARX® provides D developers with robust and reliable way to integrate protection to their software and intellectual property. With MARX CRYPTO-BOX USB state-of-the-art hardware system and based on it SmarxOS® API, solutions and technologies offered by MARX you will be able to protect your D applications against piracy and unauthorized usage in the most efficient way.

MARX Professional Protection Kit introduces a comprehensive set of protection techniques and options based on CRYPTO-BOX® USB hardware. Before making any decisions about a strategy you're going to use to protect your applications and data, it's important to understand the main concepts.

4. Protecting your programs with SmarxOS® API

Adding API calls to your program, using SmarxOS® powerful features and capabilities you can implement product specific highly efficient protection/licensing strategy. You can integrate smart support for demo and full-operating versions of the program, online features activation, remote update scenarios, etc.

SmarxOS® API utilizes all outstanding functions the CRYPTO-BOX USB hardware including:

- On-board encryption of data with Rijndael algorithm (Advanced Encryption Standard (AES), official successor to the DES algorithm) with a 16 bytes key that never leaves the hardware platform, in OFB bit-stream cipher mode (Output Feedback Mode);
- The 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
- CRYPTO-BOX USB XL has integrated White Noise Random Generator (used for the purpose of random seed generation)
- Encrypted EEPROM with 4 kByte of on-board memory (up to 64 kByte available on request)
- Reliable communication and CRYPTO-BOX identification

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

API based protection is directly available for D developers with dynamic-link library included to SmarxOS PPK, implementing SmarxOS® API calls. See Chapters 4 and 8 of SmarxOS PPK Manual for more details.




5. CRYPTO-BOX® USB

The CRYPTO-BOX USB is the "short" answer to your questions about software protection under Windows, Mac OS or Linux.

- First key on market with AES/Rijndael implemented in hardware - encryption key never leaves hardware platform!
- RSA support for digital signatures and access control systems. *
- Ideal for establishing 2-Factor Authentication.
- Extremely short and robust metal case: shields electronic circuitry perfectly!
- Supports the [SmarxOS Application Framework](#), a sophistic all-in-one solution which protects software and data and provides flexible End-User Management, including Remote Updates.
- Complete operating system support: Windows XP/2000/NT4, Me/98, Microsoft .NET, Mac OS, Linux.
- Unique Serial number for every CRYPTO-BOX USB *
- Huge memory: from 4 to 64 kBytes. **
- Network support without hardware surcharge (protect your application with only one CRYPTO-BOX per network)
- Individual network license counter configuration for every CRYPTO-BOX USB possible - via License Control System (LCS®).
- Remotely programmable with Remote Update Management System, incl. network license counter reprogramming

* CRYPTO-BOX USB XS and XL only

** CRYPTO-BOX USB Versa only available with 4 kByte

			
Supported features	CRYPTO-BOX USB Versa	CRYPTO-BOX USB XS	USB XL
Special feature	<i>Extremely short! Ideal for notebook users</i>	<i>Extremely short! Ideal for notebook users</i>	<i>True White Noise Generator</i>
Metal case, perfectly shielded	✓	✓	✓
Unique serial number		✓	✓
AES/Rijndael on chip	✓	✓	✓
RSA support		✓	✓
Memory	4 kB	4 – 64 kB	4 – 64 kB
Windows, Linux, Mac OS Support	✓	✓	✓
Network license management	<i>Floating License</i>	✓	✓
License Control System (LCS)		✓	✓
Remote Update	✓	✓	✓
AutoCrypt (automatic protection)	✓	✓	✓
Implementation with API	✓	✓	✓

Appendix

Appendix A – Distributors

USA

MARX CryptoTech LP
 4485 Tench Rd. #310
Peachtree Commons Office Park
 Suwanee, GA 30024
 U.S.A.
www.cryptotech.com

Sales: sales@cryptotech.com
 Support: support@cryptotech.com
 Phone: (+1) 770-904-0369
 Fax: (+1) 770-904-3893
 Email: info@cryptotech.com

Germany

MARX Software Security GmbH
 Vohburger Strasse 68
 D-85104 Wackerstein
 Germany
www.marx.com

Sales: sales-de@marx.com
 Support: support-de@marx.com
 Phone: +49 (0) 8403 9295 14
 Fax: +49 (0) 8403 9295 29
 Email: contact-de@marx.com

Poland

Microplan Polska Sp. z o.o.
 Polwiejska 3
 PL-61-885 Poznan
 Poland
www.microplan.pl

Sales: Gregor Bigos
 Phone: +48 (0) 61 8518916
 Fax: +48 (0) 61 8518774
 Email: big@microplan.pl

Appendix B - CrypToken Certifications and MARX Memberships



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