

Securing visual programmed projects

## Using the CRYPTO-BOX to protect LabView Projects



**Described Version:** LabVIEW 8.20

**Also applicable for:** LabVIEW 7.x and up

**Target platforms:** Windows Vista/XP/2000, Linux, MacOS

**MARX hardware:** CRYPTO-BOX USB



### Quick and efficient hardware based software protection!

MARX provides LabVIEW developers with a robust and reliable way to integrate protection to their software and intellectual property. With the CRYPTO-BOX USB state-of-the-art hardware system, the SmarxOS API, and further MARX solutions and technologies, LabVIEW applications will be protected against piracy and unauthorized usage in the most efficient way.

- 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 of on-board memory
- Reliable communication and CRYPTO-BOX identification



Download

**Download the latest Application Notes:**

**[www.cryptotech.com/AN](http://www.cryptotech.com/AN)**

## 1. Introduction: LabVIEW brief overview

LabVIEW (**L**aboratory **V**irtual **I**nstrumentation **E**ngineering **W**orkbench) is a platform and development environment for a visual programming language from National Instruments [www.ni.com/labview/](http://www.ni.com/labview/).

It is commonly used for data acquisition, instrument control, and industrial automation on a variety of platforms (Microsoft Windows, UNIX, Linux, and Mac OS). The graphical programming language used in LabVIEW, called “G”, is a dataflow language. The graphical approach allows non-programmers to build programs by simply dragging and dropping virtual representations of the lab equipment with which they are already familiar.

## 2. LabVIEW - platform independent extendable environment

LabVIEW offers an extensive support for accessing instrumentation hardware. Various drivers and abstraction layers allow standard software interfaces to communicate with hardware devices and save program development time. A new hardware driver topology (DAQmxBase), provides platform independent hardware access to numerous data acquisition and instrumentation devices.

In terms of performance, LabVIEW includes a compiler that produces native code for the CPU platform. The executable runs with the help of the LabVIEW run-time engine, which contains some precompiled code to perform common tasks that are defined by the G language. The runtime engine reduces compile time and also provides a consistent interface to various operating systems, graphic systems, hardware components, etc. A benefit of the LabVIEW environment is the platform independent nature of the G-code, which is portable between the LabVIEW systems for different operating systems.

## 3. Customizing and extending LabVIEW environment with external APIs

LabVIEW is an open development environment capable of calling external code such as DLLs, ActiveX, and .NET assemblies. LabVIEW for Windows 95 and Windows NT has a Call Library Function that you can use to access 32-bit DLLs. Because a DLL uses a format that is standard among several development environments, developer is able to use almost any development environment to create a DLL that LabVIEW can call: <http://zone.ni.com/devzone/cda/tut/p/id/3009>

LabVIEW supports ActiveX automation as both the client and the server. This means that LabVIEW can be used to interface with other programs from the LabVIEW programming interface. LabVIEW can act as the automation client and request information of the automation server (the other program). Likewise, other ActiveX automation clients can interface with the LabVIEW ActiveX automation server. Common programs that are used to do this are Microsoft Visual Basic and Microsoft Visual C++ : <http://zone.ni.com/devzone/cda/tut/p/id/2983>

With the release of LabVIEW 7 Express, you easily can connect to the new .NET technology as a .NET client. You can create instances of .NET classes and invoke methods to set and obtain properties on them from LabView. The usage paradigm is similar to that of ActiveX automation Vis. In addition to the ability to call .NET assemblies, LabVIEW 8.20 supports .NET user interface controls in the front panel, .NET events, and allows the user to easily import a Web Service

**Download the latest Application Notes: [www.cryptotech.com/AN](http://www.cryptotech.com/AN)**

## 4. Protecting LabVIEW applications with the CRYPTO-BOX USB 2

The CRYPTO-BOX offers a professional and secure protection for software and intellectual property. The functions utilized by the SmarxOS API are:

- 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.
- 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.

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 SmarxOS API enables application developers to implement product specific and highly efficient protection strategy of any complexity. Smart support for demo and full-operating versions of the program, online features activation, remote update scenarios, etc. can be integrated. See SmarxOS PPK Manual Part IV for more details.

MARX provides a wide range of methods for easy integration of CRYPTO-BOX USB support to LabVIEW-related products. The full set of SmarxOS API features including Network License Management and Remote Update are directly available for LabVIEW developers in form of:

- C/C++ static libraries
- Dynamically linked libraries (sample code included in the SmarxOS Protection Kit)
- ActiveX objects (sample code included in the SmarxOS Protection Kit)
- .NET managed classes
- Available wrappers for widely used programming languages as Delphi, Java, or Visual Basic.

MARX supports all major platforms. So the same code can be used for protecting LabVIEW software on Windows, Linux, or Mac OS X systems.

**Download the latest Application Notes: [www.cryptotech.com/AN](http://www.cryptotech.com/AN)**

## 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](http://www.cryptotech.com/AN)