



Secure Demo Versions with the MARX CRYPTO-BOX USB

Described Version:	Smarx OS 2.21.7.110
Also applicable for:	Smarx OS 2.x and up
Target platforms:	Windows Vista 32/64 /XP/2000, Linux, Mac OS
MARX hardware:	CRYPTO-BOX® USB

Quick and efficient hardware based software protection!

Software and information piracy costs billions of dollars in annual losses to software vendors, distributors and content providers worldwide. The internet role in software and data distribution is growing rapidly and it increases the tenseness of the situation dramatically.

Hardware based protection can be used for creating robust and reliable secure demo versions of applications in a straightforward manner. While benefiting from strong and effective application protection provided by hardware based approach you can create flexible and secure demo versions with ease. The CRYPTO-BOX USB can make it happen!

- 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. Introduction.....2**
- 2. MARX CRYPTO-BOX® USB Solution Overview.....2**
- 3. Secure Demo Versions.....3**
- 4. Examples.....5**
 - 4.1 One example of how a customer could use AutoCrypt in their environment.....5
 - 4.2 One example of how API-protection could be implemented using the CRYPTO-BOX.....5
- 5. CRYPTO-BOX® USB (technical data).....6**
- Appendix.....8**
 - Appendix A – Distributors.....8
 - Appendix B - CrypToken Certifications and MARX Memberships.....8

1. Introduction

Software and information piracy costs billions of dollars in annual losses to software vendors, distributors and content providers worldwide. Internet role in software and data distribution is growing rapidly and it increases the tenseness of the situation dramatically.

On the other side Internet is highly attractive as a distribution tool and gives a decisive competitive advantage. Retail business hours are not an issue for you because your product will be available to customers 24/7 on the Internet. Internet is reducing distribution and administration costs as the customer can download the application directly from your server and evaluate it.

While easiness of your product evaluation gives you a strong benefit in a number of potential customers it implies that there is a special demo version of your application intended for evaluation purposes only. There is no sense for the customer to pay for your product otherwise. Depending on license agreement only proves you to be generous and sincere person but does not prevent your losses.

Common approach is to restrict demo application functionality until a valid serial number is purchased by the customer and used for product activation. But protecting software with serial numbers is rather weak strategy: personal serial numbers can be easily shared and even freely distributed over the Internet. Serial numbers can be considered more as legal and marketing control mechanism than actual protection. As a variant of this strategy a separate application demo build can be done which does not include restricted features at all. Full version of application is supplied to the customer along with serial number. But it complicates things just a bit as generally the full version can be easily downloaded from peer-to-peer networks or warez sites.

Another popular software based strategy assumes licensing software by binding it to a particular client's PC so there is no sense to share serial numbers. This strategy is more reliable; however it has two important disadvantages: support costs increase dramatically and low flexibility because switching to a different hardware requires re-activation.

Above mentioned protection strategies use software based approach and suffer from inherent to it ease of serial numbers replication and distribution. In the realm of hardware based protection such kind of issues does not emerge. Hardware based protection assumes a special hardware distributed to the users as a part of protected software/data package. It has no drawbacks of both serial numbers and PC binding strategies and provides the best and the most reliable solution for software vendors and content providers.

Hardware based protection can be also used for creating robust and reliable secure demo versions of applications in a straightforward manner. While benefiting from strong and effective application protection provided by hardware based approach you can create flexible and secure demo versions with ease.

The rest of the article is concerned in secure demo versions creation based on MARX CRYPTO-BOX USB state-of-the-art hardware system and offered by MARX reliable and proven solutions and technologies.

2. MARX CRYPTO-BOX® USB Solution Overview

Hardware based protection assumes that your protected applications and/or data files will require a corresponding CRYPTO-BOX® USB to be attached to the user's computer (or another network computer) in order for their normal functionality.

Protected software will check for the CRYPTO-BOX presence. If required hardware is not found, the program can switch to a demo/limited mode or even refuse to work (depending on your protection strategy).

If required hardware is attached, then the program will communicate with it, performing more detailed verification:

- Serial number;
- Access codes;
- Hardware based encryption;
- Internal memory

All these, as well as many other CRYPTO-BOX unique features can be used to build a reliable protection scenario.

Data files can be encrypted using CRYPTO-BOX internal on-board encryption. This approach guarantees an extremely reliable protection: encrypted data files can be viewed only with corresponding CRYPTO-BOX attached to the user's computer.

More limitations can be added, like, for example, expiration dates: your users will be able to view protected documents only by preset dates. MARX provides you with a convenient way to update such expiration date remotely (see below for more details).

Smarx OS® Professional Protection Kit (PPK) includes a comprehensive set of protection techniques and options based on CRYPTO-BOX® USB hardware for all major platforms.

Smarx OS® PPK provides you with:

- Full control over CRYPTO-BOX® USB hardware powerful features and capabilities via SmarxOS® API for Windows, Linux, and Mac OS X platforms and all major programming languages and technologies (ActiveX, .NET);
- High-level Smarx OS Data Objects API for expiration date, number of application executions (runs), application checksum and other common check-ups encountered in software protection realm;
- Automatic Protection with AutoCrypt which compress and encrypt your application, then wrap it inside a protective layer, preventing it from working unless a valid CRYPTO-BOX is attached;
- Remote Update Management System (RUMS) which provides a convenient way to remotely update Data Objects programmed inside the CRYPTO-BOX partitions and allows you to prolong the test period for evaluation or demo versions, change limitations for demo versions, or switch on/off particular features;
- Network License Management which allows Smarx OS-based applications to access a CRYPTO-BOX USB attached to any computer in a network and grants a very flexible mechanism of license management, allowing you to limit the number of network clients simultaneously logged onto a CRYPTO-BOX partition;
- Smarx OS Application Framework – a complete package for software vendors and distributors which automates your software and data protection scenarios;
- And other convenient tools and features.

3. Secure Demo Versions

Smarx OS® PPK gives you a great power to reliably check that correct CRYPTO-BOX USB is present and contains valid settings. If CRYPTO-BOX USB can not be detected your application logic can switch to demo version mode and restrict product functionality or refuse running and give informational message to the end-user. **This demo version is truly secure** as it is based on hardware key which can not be easily duplicated or substituted.

When protecting your software and creating demo versions you have two basic choices:

- Automatic protection
- Implementation into source code through API

Smarx OS PPK offers both options.

Automatic protection provides a fast, efficient and simple solution. You do not need to be a developer, spending time on understanding CRYPTO-BOX internals and incorporating corresponding code to your program. You do not need to have the source code at all. AutoCrypt Manager will do it for you in a snap! It will compress and encrypt your application, then wrap it inside a protective layer, preventing it from working unless a valid CRYPTO-BOX is attached. Many additional features and customizations are available. Still automatic protection implies that CRYPTO-BOXes are distributed along with your protected application even for evaluation purposes. AutoCrypt settings programmed in CRYPTO-BOX define restrictions of your product demo version. While your secure demo version functionality remains full-featured you are free to set trial period, number of allowed application executions, or other similar settings as defined by your marketing strategy. All those restrictions can be easily removed or changed via Remote Update after the customer paid for your product.

Implementation into the source code through the SmarxOS API is a feature targeted at developers who need maximum security and flexibility for their applications. Using the API you can implement a product-specific and highly efficient protection strategy. You can integrate smart support for demo and full-product versions of the program, online feature activation, remote update scenarios, and much more. Since Smarx OS allows you to protect up to 10 applications simultaneously with one CRYPTO-BOX USB, you can mix applications protected through AutoCrypt and API-protection on one CRYPTO-BOX. Currently MARX supports Windows, Linux and Mac OS X for API-protection implementations.

Besides other benefits manual protection allows you to create and distribute just one full-featured version of your product which behaves differently depending on CRYPTO-BOX USB availability and state. You can make your application freely available for download on your Internet site without worrying of software piracy and illegal software usage. Just those customers which purchased your software legally will get appropriate CRYPTO-BOX key to activate full version functionality. You determine what's possible and what isn't.

CRYPTO-BOX USB solution allows you to create very flexible protection strategies. Intelligent software protection using a CRYPTO-BOX key is the great software protection solution in particular for modularly designed products where each customer obtains only those components of the application that they need. It allows you to easily define more granular functionality restrictions than just demo / full version. The same CRYPTO-BOX USB can be used to protect your other products or software modules both current and planned to be developed in future. Let the customer evaluate your product and realize what functionality he really needs. You can easily configure CRYPTO-BOX USB for any set of functions this customer wants if it fits to your marketing strategy. **Everybody gets what they pay for – no more, no less.**

The CRYPTO-BOX key "decides" which parts of the application can be used, so creating a tailored application bundle for each customer requires very little effort. Do you want to set expiration date or number of application runs, limit the number of licenses, i.e. the number of workstations in a network allowed to run the software concurrently? No problem. You can configure the CRYPTO-BOX key accordingly to your needs. The customer will benefit from this sophisticated distribution approach. He pays only for what he really needs.

The CRYPTO-BOX system opens up all manner of possibilities. For example, "classical" hardware protection where the key has to remain connected to the computer all the time for the program to run. But you can also use **Network License Management** solution which allows your customers to run more than one instance of your software product concurrently on the network. Only one CRYPTO-BOX® storing network license counter (number of licenses you grant to the customer) is required. This hardware key has to be attached to any one of the network computers running Smarx OS® Network Server on it. And an entire network will be protected with only one CRYPTO-BOX!

You determine the number of workstations in the network on which your application may run. If desired, you can set an expiration date, an execution or a time limit on your program usage. Remote Update simplifies the distribution of updates and follow-up business (e.g. additional licenses) while the cost involved is negligible. Your marketing department benefits as well: you will obtain reliable customer data and be able to recognize market requirements early, thereby improving market information to assist your long-term marketing strategies.

SmarxOS provides you with a great feature of CRYPTO-BOX USB application partitions. You can view those partitions as separate virtual CRYPTO-BOXes sharing the same high level of security and reliability. It allows you to use just one CRYPTO-BOX hardware key for protecting a number of your separate applications and products. Combined with Network License Management solution it allows you to ship just one CRYPTO-BOX USB for the whole organization purchasing your product.

Smarx OS provides you with a very flexible mechanism of license management, allowing you to limit the number of network clients simultaneously logged onto a CRYPTO-BOX partition. It uses a special approach, called Smarx OS License Control System (LCS), to limit the number of applications of one type simultaneously logged into the partition of the attached CRYPTO-BOX. Any Smarx OS formatted CRYPTO-BOX has a special setting defined: Grant LCS to this CRYPTO-BOX or not.

The Smarx OS PPK includes all tools and components needed to support all popular licensing models. Network License Management allows you to support multi user licensing, while Smarx OS® Data Objects and Remote Update interfaces offer software renting, remote activation, subscriptions and Pay-per-Use models. Smartly applying and utilizing this functionality you can tremendously increase your sales.

What if your customer requires a new configuration, additional program functions or simply more licenses? The CRYPTO-BOX key can be updated over the Internet using Remote Field Programming. MARX provides you with **Remote Update Management System** (RUMS) to make CRYPTO-BOX USB remote updates an easy and quick task. Using the Remote Update Manager as part of the Smarx OS Application Framework (SxAF), you may prolong the test period for evaluation or demo versions, change limitations for demo versions, or switch on/off particular features. With the CRYPTO-BOX software protection system, you are the boss. You determine the number of program starts or limit the evaluation period to 30 or 60 days.

In contrast to conventional protection devices, CRYPTO-BOX USB can be kept continuously "up-to-date" via remote programming. This can occur over the Internet, by sending a password, or by phone.

That's flexible Electronic Software distribution in its purest form, allowing you to react quickly and easily to your customer's needs. That will put you one step ahead of the rest. Direct distribution combined with MARX CRYPTO-BOX USB hardware based protection allows you to increase your profits. Shipping costs and customs duty no longer apply.

Another side benefit: As soon as a customer contacts you to order an update or additional products, you receive reliable data on their needs and requirements. That's indispensable "fodder" for your marketing department and Customer Relation Management team. Only those who keep their finger on the pulse of their market and know their customer's requirements can look with confidence into the future of their business.

In addition to preventing piracy, Electronic Software Distribution strategies enable you to access new sales channels, improve customer relations and obtain valuable marketing data. Get 100% customer registration, sell updates (instead of just distributing them), and take advantage of LM/db, the invaluable License Management database for end user administration. Activate programs remotely using the Internet or sell your products as modular components and authorize them later, upon demand and after payment is received from your customers:

The CRYPTO-BOX makes it happen!

4. Examples

4.1 One example of how a customer could use AutoCrypt in their environment

Software Vendor A has spent a lot of time developing their software and now is ready for it to hit the market. Software Vendor A has a tight time line and needs a way to secure his application quickly so his customers can begin realizing the benefits of the software as soon as possible.

The company's sales model for this particular software product is to provide a demo version of the software, limited to ten uses, and then provide the customers with the option to upgrade to the full version for a one year term, with the option of renewing at the end of each year.

Software Vendor A decided to implement the CRYPTO-BOX and AutoCrypt to ensure that these requirements are met.

Using AutoCrypt Software Vendor A simply took their existing application and injected the necessary data-objects provided by AutoCrypt Manager to meet his requirements. Software Vendor A simply created a new project for this application, added his existing application to the project, selected the execution counter data object (set to 10 uses as listed in their requirements) and at the click of a button created a protected version of the software application. The last step was to format the CRYPTO-BOXes for this protected application. Software Vendor A was able to select the number of CRYPTO-BOXes he wanted to format and within minutes had demo versions of his software available for distribution.

The other requirement Software Vendor A had for his software was to prompt the users to upgrade for a one year subscription after their demo expired. He also used AutoCrypt (when formatting the execution counter data object) in order to create a message giving instructions on how to upgrade to a full one year license after the trial period was over.

Using RUMS (Remote Update Utility), the end user is able to simply read the message provided and request full usage of the software. Software Vendor A simply sends the customer the requested update using the expiration date data object and the Remote Update Utility. Next, the customer can automatically upgrade the software after paying and setting up the associated CRYPTO-BOX. The same series of events will happen once the expiration date for this specific customer is reached.

This is only one of the many examples of how our customers can use the quick and reliable AutoCrypt tool to secure their application and to ensure payment.

4.2 One example of how API-protection could be implemented using the CRYPTO-BOX

Software Vendor B has developed a set of tax preparation applications. Because of his high flexibility requirements he decided to implement the CRYPTO-BOX USB with API-protection as the protection scheme.

Software Vendor B knows that in order for his tax preparation software to become widely used by tax consultants he will need to provide an almost fully functional demo. All of his applications were developed using Microsoft Visual Studio .NET, which MARX supports, so there will be no additional work required to implement this protection scheme.

The only limitations Software Vendor B decided to have for his demo is that the tax documents are not printable and all internet based submission methods must be disabled. This was easily implemented using the Smarx OS CBIOS API. In other words: If there is no CRYPTO-BOX attached to the end user's USB port the software can be copied and is fully functional with the exception of the two limitations mentioned which, however, render the software useless to tax consultants.

Once a customer does decide to purchase, Software Vendor B simply gives a CRYPTO-BOX to the customer upon receipt of payment. Software Vendor B is able to protect all of his applications or application modules with one CRYPTO-BOX. Each CRYPTO-BOX supports up to 10 separate applications each with their own partition in CRYPTO-BOX memory.

The example above is a limited scenario where the CRYPTO-BOX API-protection scheme was applied. Since implementation through the API is so flexible the possibilities are virtually infinite.

5. CRYPTO-BOX® USB (technical data)

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 [Smarx OS 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	CRYPTO-BOX USB XL
Special feature	<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	
Windows, Linux, Mac OS Support	✓	✓	✓
Network license	<i>Floating</i>	✓	✓

<i>management</i>	<i>License</i>		
<i>License Control System (LCS)</i>		✓	✓
<i>Remote Update</i>	✓	✓	✓
<i>AutoCrypt (automatic protection)</i>	✓	✓	✓
<i>Implementation with API</i>	✓	✓	✓

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.