

NEW! Smart Application Framework
Optimized for VISTA

CRYPTO-BOX[®] Protection Kit



Quick Start Guide

Microsoft[®]
CERTIFIED
Partner

MARX[®]
CryptoTech[®]

Content of your Quick Start Guide:

- Smarx OS® Protection Kit installation
- Overview of available options of the Smarx OS Control Center
- Software protection in minutes with AutoCrypt

Your CRYPTO-BOX® Protection Kit includes:

- CRYPTO-BOX USB XS, Evaluation Version (same codes for all)
- OR: CRYPTO-BOX USB with your own customer-specific codes
- CD of the Smarx OS software
- Compendium (available in printed form and as a PDF file on CD).
The latest version always can be found on www.cryptotech.com

If something is missing, please contact us at:
+1 770 904 0369 or support@cryptotech.com

Installation (Windows Vista/XP/2000)

- Do not connect the CRYPTO-BOX to your PC yet!
- Place the CD in your CD-ROM drive. If the CD does not automatically start, trace to Start -> Run and enter X:\Setup (whereby „X“ stands for the letter assigned to your CD-ROM drive).
- From the menu, select Smarx OS® Professional Protection Kit and click on Install.
- Wait until the installation program has ended and the Smarx OS® Control Center appears.
- Now connect the CRYPTO-BOX to any free USB port - the Windows Hardware Wizard will start shortly thereafter. Click on Next to automatically install the driver.

Installation (Linux and Macintosh):

Notes on installing the libraries for developers using Linux and Mac OS can be found in the LINUX.TXT file and the MAC.TXT file in the main folder on the CD-ROM.

2

Driver Installation Utility
and Diagnostics Tools

3

Partition Editor

4

AutoCrypt Manager
as a part of SxAF

5

Document Protection
as a part of SxAF

6

Software Protection for Developers
SmarxOS® API (CBIOS, DO, RFP)

7

Network License Control
and User Limits



1

How To Start ?

SmarxOS® Demo

8

Data Protection API

9

Documentation

10

WEB API (WebSecurity)

11

Place Order

Request Quote

Copyright© 2002, 2007 MARX® CryptoTech LP

www.cryptotech.com

Exit

1 Quick start

A brief introduction to some of the features of this kit.

Options: Protection of applications with AutoCrypt, manual integration with the Smarx OS programming interface and Document Protection.

2 Driver installation and diagnostics tool

CBUSetup is used to install the CRYPTO-BOX drivers. You can deliver it together with your protected application or integrate it directly into your installation routine.

MarxProbe is used for diagnosing errors. In the event that the CRYPTO-BOX is not recognized by your system, you can run MarxProbe to perform an analysis of the system and create a report.

3 Partition Editor

The Partition Editor allows you to customize the way in which the CRYPTO-BOX memory is used for your application. The Partition Editor can be used to create, change and delete partitions for various applications such as AutoCrypt, integration with API, document protection and much more.

4 AutoCrypt Manager

With AutoCrypt, you can protect Windows applications in just a few minutes, without needing to access the source code of the application or having any programming skills. All of the steps are described in detail on the following pages.

5 Document Protection with DRM

Safe distribution of electronic documents with Document Protection. Only users with a valid CRYPTO-BOX USB connected to their PC can read the

encrypted documents. The documents also can include an expiration date and licenses can be renewed via remote updates (Digital Rights Management).

6 Manual integration for developers using the Smarx OS® programming interface

The Smarx OS API allows developers to fully exploit all the possibilities available with the CRYPTO-BOX USB by integrating within the source code of their applications. Examples for all common developing environments such as C++, .Net and Delphi are included.

7 License management in networks

Protect your application on all network PCs with just one CRYPTO-BOX.

8 Smarx OS® Demo

This allows you to test the functions of the Smarx OS programming interface

9 Data Security

The Smarx OS Data Protection API allows you to protect important informations, databases or tables.

10 Documentation

The Smarx OS Compendium as a PDF file, as well as information about the version of the Protection Kit.

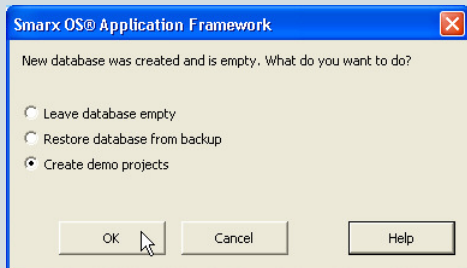
11 Web API

Users of a web application can be authenticated by their CRYPTO-BOX.

How to protect a Windows application in just a few minutes using AutoCrypt:

In the Control Center select **“AutoCrypt Manager as part of SxAF”** -> **“Launch Smarx OS Application Framework.”**

If you start the Smarx OS Application Framework (SxAF) for the first time the following window appears:



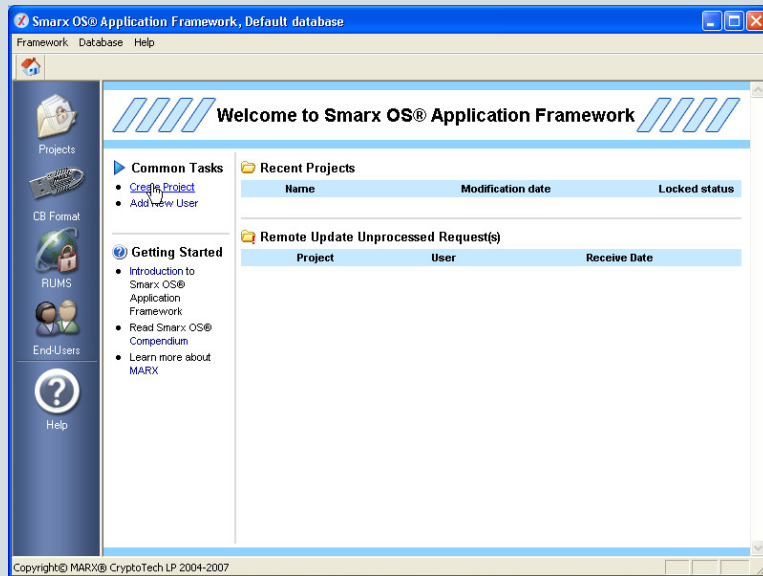
Choose the option **“Create demo projects”** and click **“OK”** to approve a new project creation.

Demo projects contain pre-settings, which are useful for a demo.

The main window of the Smarx OS Application Framework acts as control-center. Choose from the following options:

- Create new projects, or access the documentation and help file.
- Under **“Projects”** you can create new projects or change/delete existing projects.

- With **“CB Format”** you are able to configure the CRYPTO-BOX modules with your own project settings.
- **“RUMS”** allows you to process Remote Update Request from the end-user.
- Under **“End User”** you are able to save the data of your end-users, these facts can be assigned to a specific CRYPTO-BOX module – this is useful for Remote Updates.



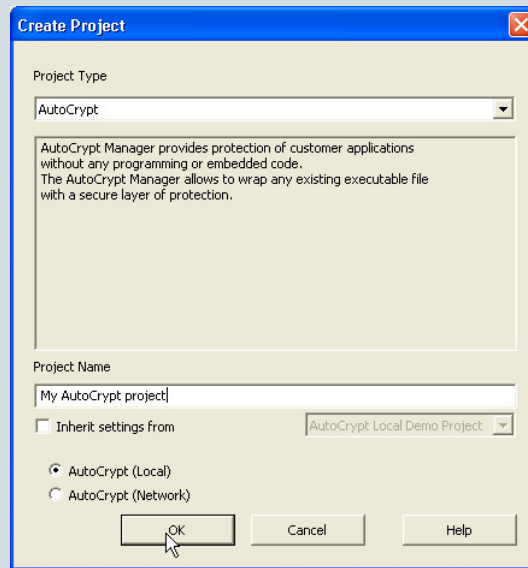
Click on the main menu **“Create Project”**. Choose as project type **“AutoCrypt”** and enter a project name.

In the lower field, you can select an existing project whose settings you would like to apply. This can be ignored for the time being.

Leave the setting **“AutoCrypt (local)”** (CRYPTO-BOX will be inquired directly on the local PC) and click **“OK”**, to get to the General Settings.

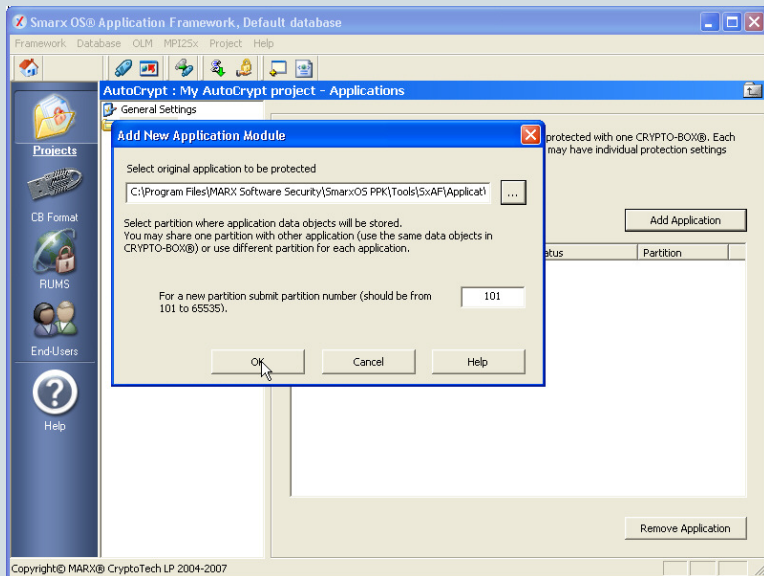
On the General Settings you can change the name of the project, add a description and choose the right hardware profile.

AutoCrypt uses hardware profiles in which the access codes for the CRYPTO-BOX are saved. If you have a CRYPTO-BOX Evaluation Kit, you are able to use the preset **“cbu_demo”** profile. If you already have customer-specific CRYPTO-BOX modules (e.g. Starter Kit), use the hardware profile from the supplied CD or request it directly from MARX. Click on **“Import profile”** and select the drive and folder path where your hardware profile is saved (e.g. CDROM-drive).

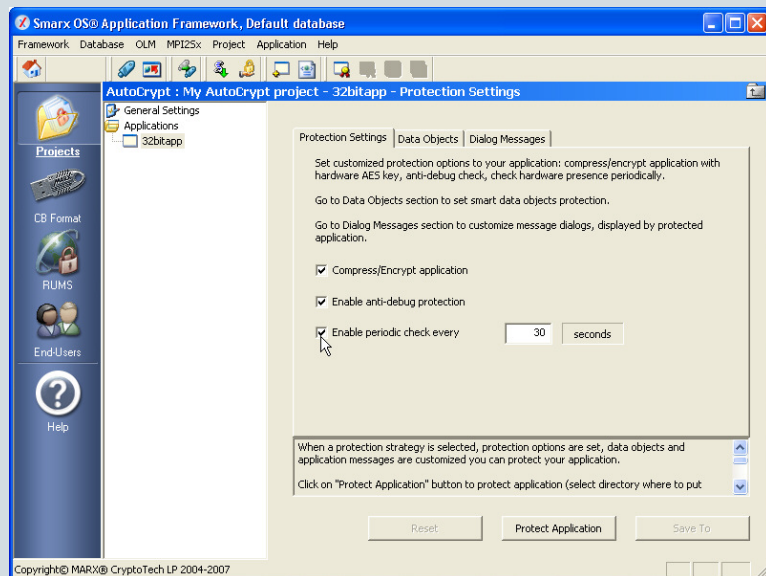


Afterwards click on the left section of the screen on **"Application"**. Now click on the **"Add Application"** button to select your application to be protected.

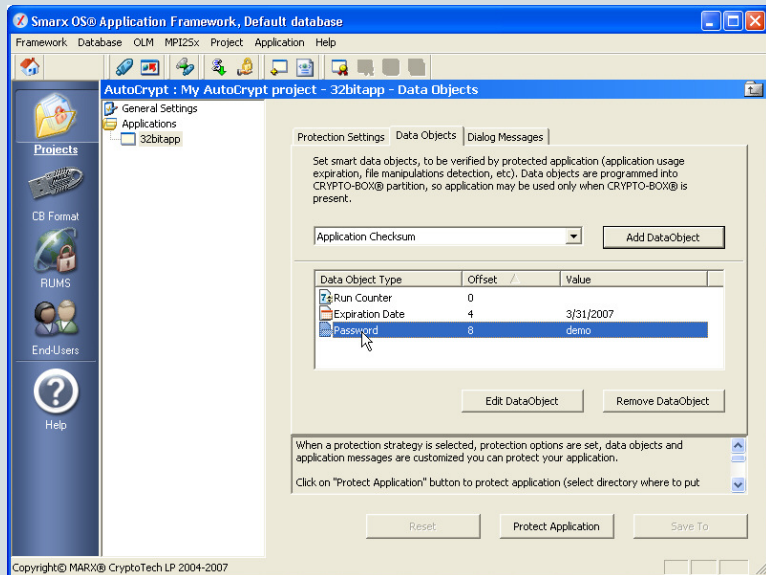
At the bottom you can specify the partition number to be used for saving the licensing options for your application on the CRYPTO-BOX. Do not change the default setting here. Now click on **"OK"** to switch to the screen with the protection and licensing option settings for your protected application.



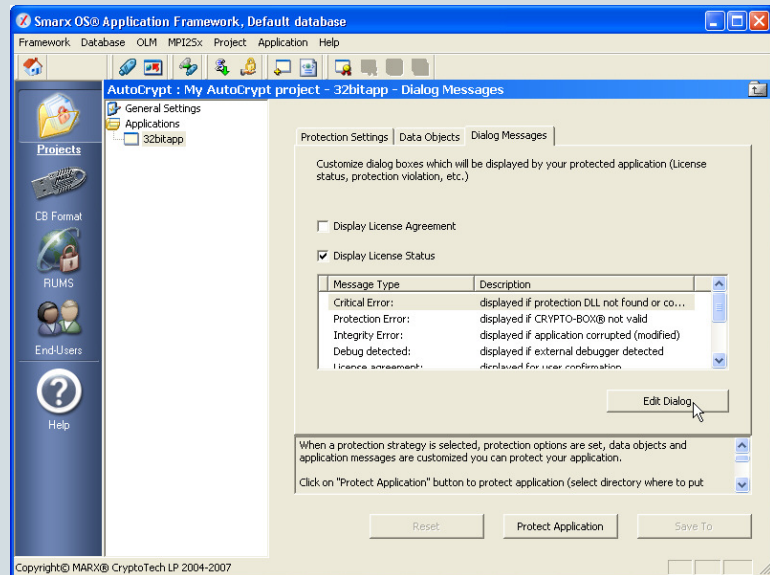
On this screen you will see options for determining the level of protection for your application. **"Compress-Encrypt application"** is used to automatically compress and encrypt your protected application. **"Enable anti-debug protection"** offers effective protection against debugging, as the application is not executed while a debugger is running on the system. When the **"Enable periodic check every"** option is selected, a check is made at regular intervals to verify that a CRYPTO-BOX is connected. This option definitely should be selected, however do not use too small of a value for the time interval (recommended intervals: 30 seconds or more).



In the center **"Data Objects"** you will see comprehensive licensing options such as placing a time limit on a license, limiting the number of program starts, additional password querying and much more. Click on **"Add DataObject"** to select or change the desired options, e.g. Expiration Days or Run Counter. Below you find an overview of the selected Data Objects.



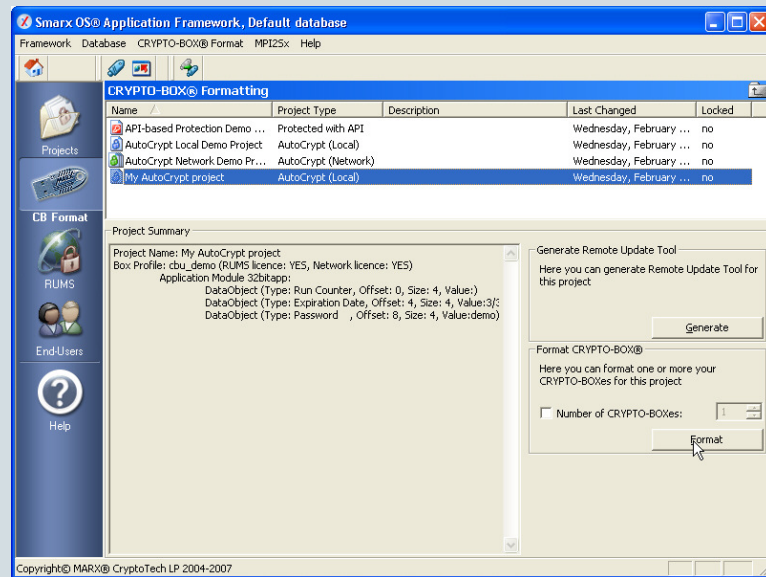
By selecting **"Dialog Messages"** you can configure those dialog boxes that your protected application is to output under certain circumstances (e.g. licensing information or if the CRYPTO-BOX was not found). To do this, select the desired message and click on **"Edit Dialog"**. If you select **"Display License Agreement"**, a license text will appear every time an end-user starts the program. The end-user will have to confirm their acknowledgment of this agreement in order to continue. If you activate **"Display License Status"**, every time before the program starts, the license status will be displayed (according to your settings under **"Data Objects"**). All Status texts and failure notices can be configured individually: to proceed select the requested notice and click on **"Edit Dialog"**.



Once you have configured all settings to meet your requirements, click on **“Protect Application”** to create the protected application. A window will appear, on which you can define the file name of your protected application and also the location where it should be stored. Afterwards click save.

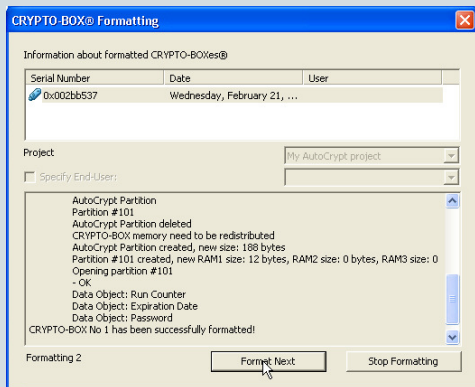
Your program is successfully protected! Now you can format one or more CRYPTO-BOX modules for use with your protected program. Therefore click on the left section of the menu bar on **“CB Format”**.

The following window provides an overview of all projects already created. Click on your created project – under **“Project Summary”** you will find all of your project settings.



Click on the button **“Format”** on the right side. Make sure that your CRYPTO-BOX is plugged into the USB-Port and click **“Format Next”**.

By request you are able to format further CRYPTO-BOX modules. Therefore click on **“Format Next”**, or to end click on **“Stop Formatting”**.



Congratulations!

You have successfully protected your application!

Now start the application and test all protection options.

Delivery to your customers

1. Your protected application.
2. Provide the CRYPTO-BOX drivers (simply use the CBUSetup.exe program for driver installation). More information can be found in the Control Center by clicking on **“Driver Installation Utility and Diagnostics Tools”**.
3. The CRYPTO-BOX.

The Smarx OS Protection Kit, however, offers you even more:

Several programs can be protected with one single CRYPTO-BOX, or update a license directly at the customers site via Remote Update. The Smarx programming interface provides unlimited opportunities for implementing individual protection and licensing options in the source code of your application. More information can be found in the Smarx OS Compendium.

A complete overview of all products can be found in our Web catalog at www.cryptotech.com.

Control Center: Main purpose

- Central control point for quick access to all Smarx OS Protection Kit applications.
- Provides you with a quick guide and overview of the individual options.

The main advantages of the AutoCrypt Manager

- Protect Windows applications in just a few minutes.
- Protected applications only can be executed with a matching CRYPTO-BOX.
- You do not need any source code or knowledge of programming.
- The AutoCrypt Manager offers comprehensive protection functions such as encryption, tampering detection and anti-debugging protection.
- Many licensing options are available, such as limitation of application runs, time limitation and password check.
- Protect several applications with a single CRYPTO-BOX.
- Take advantage of remote updating of CRYPTO-BOXes directly by your end-users.

Securing the Digital World

www.cryptotech.com

MARX Software Security GmbH
Vohburger Strasse 68
D-85104 Wackerstein
Germany
Phone: (+49) (0) 8403-9295 0
Fax: (+49) (0) 8403 -1500
support-de@marx.com



MARX CryptoTech LP
4485 Tench Road #310
Peachtree Commons Office Park
Suwanee, GA 30024 U.S.A.
Phone: (+1) 770 904 0369
Fax: (+1) 770 904 3893
support@cryptotech.com