White Paper

API Implementation WP-1

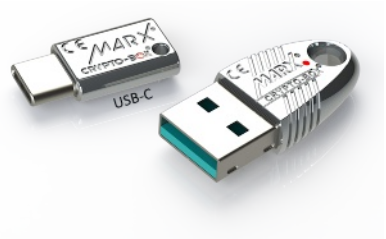
Subject: CRYPTO-BOX implementation into the source code with Smarx OS API
Version: Smarx OS PPK 8.14 and up, Smarx OS 4 Linux Package 1.22 and up, Smarx OS 4 Mac Package 2.49 and up
Last Update: 21 February 2024
Target Operating Systems: Windows, Linux, macOS, iOS, Android
Target Processor Platforms: Intel x64/x86, ARM 64/32
Access to source code needed (of protection application): ☑ Yes ☐ No
Supported Programming Tools: see chapter 5.1 in this document
Applicable for Product: CRYPTO-BOX® SC / XS / Versa

Implementation with API

The integration directly into the application source code using the Smarx®OS API unleashes the full power of the CRYPTO-BOX® and provides the most flexible way to protect your software and data against piracy and unauthorized usage.

This document describes how to get started with the API integration, and where to find the required libraries and tools in our Protection Kit.

Even if you are working with the API integration already, or if you are planning to revise your API implementations soon, this document will provide you with valuable information about the most recent changes and give you useful tips and references.



CRYPTO-BOX® Key Features

- Quick and easy protection of Windows applications with AutoCrypt
- Individual implementations with API for all common programming languages
- Multi-platform support: Windows, Linux, macOS, Android, ...
- Unique and stable metal case, optional with customer-specific color and labeling
- Network and remote update capability
- AES/Rijndael encryption on-chip
- RSA support on-chip (CRYPTO-BOX SC) or on driver level (CRYPTO-BOX XS/Versa

Order your CRYPTO-BOX Evaluation Kit now – or contact us for any questions:

www.marx.com/eval

MARX Software Security GmbH
Vohburger Strasse 68
85104 Wackerstein, Germany
Phone: +49 (0) 8403 / 9295-0
contact-de@marx.com

MARX CryptoTech LP
489 South Hill Street
Buford, GA 30518 U.S.A.
Phone: (+1) 770 904 0369
contact@marx.com

www.marx.com

Table of Contents

1. The meaning of “Implementation with API”....3
1.1. Overview....3
1.2. Automatic Protection and Implementation with API....3
2. Recommended Steps for Protecting Applications with API....3
3. Smarx®OS as Basis for the CRYPTO-BOX Integration....4
3.1. Overview....4
3.2. Smarx®OS API Subsets....4
3.2.1. Smarx®API....5
3.2.2. AC API....5
3.2.3. SmarxCpp....5
3.2.4. CBIOS4NET/Smarx4NET....6
3.2.5. CBIOS API....6
3.2.6. CBIOS Networking....6
3.2.7. DO API....6
3.2.8. RFP API....6
3.2.9. Extended API (XSMRX)....6
3.2.10. Smarx Cloud Security (WEB API)....6
4. Using the Smarx®OS API under Different Environments....6
4.1. Overview....6
4.2. Static Libraries (C/C++, Delphi)....7
4.3. Dynamic Libraries (DLL)....7
4.4. .NET....7
4.4.1. Smarx4NET....8
4.4.2. CBIOS4NET....8
4.5. COM/ActiveX....9
5. How to Find the Corresponding Library and Sample Code for Your Environment....9
5.1. Overview about Supported Environments....9
5.2. Obtaining the required Library/Samplecode from the Protection Kit....10
5.2.1. Windows....10
5.2.2. Linux....10
5.2.3. Mac (macOS/OS X)....11
5.2.4. iOS....11
5.2.5. Android....11

1. The meaning of "Implementation with API"

1.1. Overview

Hardware-based protection requires your protected applications and/or data files to have a corresponding CRYPTO-BOX attached to the computer (or a computer within the network) in order to function normally. The protected software will check for the presence of the CRYPTO-BOX. If the CRYPTO-BOX is not found, the program can switch to a demo mode or even refuse to work (completely or partially, depending on your protection strategy). If the CRYPTO-BOX is attached, the program will communicate with it, performing more detailed verification of information stored in the CRYPTO-BOX, such as:

- Verification of serial number (BoxName) or Developer ID
- Using the hardware-based encryption engine to decrypt information during application run-time
- Querying license information from the internal memory of the CRYPTO-BOX during application run-time

All these, as well as many other unique CRYPTO-BOX features, can be used to build a reliable protection strategy. Data can be encrypted using the CRYPTO-BOX internal on-board encryption. This approach guarantees an extremely reliable protection model: Encrypted data files can be viewed only when a corresponding CRYPTO-BOX is attached to the end user's computer. More limitations can be added, e.g., expiration dates: The end user will be able to use the software only until a defined date is reached. MARX provides you with a convenient way to update such expiration dates remotely (see *RUMS Application Notes* for more details).
Implementation with API means that all this functionality mentioned above can be added directly into the source code of the application by using predefined API calls (see chapter 3.2 for details).

1.2. Automatic Protection and Implementation with API

When protecting your software with the CRYPTO-BOX, you have two basic choices:

- Automatic protection of your compiled executable - see separate *AutoCrypt Application Notes* for further details.
- Implementation into the source code of your application through API.

Implementation into source code through the API is a feature targeted at developers who need maximum security and flexibility for their applications. It provides a product-specific and highly efficient protection strategy. For instance, you can integrate smart support for demo and full-product versions of the program, online feature activation, remote update scenarios, and much more.

It is possible to combine both AutoCrypt and API implementation, for instance if you want to take advantage of the encryption options offered by AutoCrypt. Or you can consider AC API which combines the simplicity of AutoCypt with the flexibility of API implementation. This is especially helpful if your type of application is not compatible with the AutoCrypt Wrapper. See chapter 3.2 for more details.

2. Recommended Steps for Protecting Applications with API

To protect your application with API, we recommend the following steps:

1. Make yourself familiar with our API (see chapter 3 and 4 in this document, and *Smarx Compendium* chapter 10). Select your preferred API and check out the sample code for your environment (see chapter 5.2) Now choose your own protection strategy.
2. Check our hints for secure implementation in the *Smarx Compendium* chapter 17 and the sample code for secure implementation in the Smarx OS Protection Kit (PPK) which can help you to significantly increase the protection level of your implementation:
   [PPK root]\SmarxOS-Samples\Security\ProtectUPW
   [PPK root]\SmarxOS-Samples\Security\.NetProtection (for .NET developers)

3. The easiest way to configure the CRYPTO-BOX with the protection and licensing setting required by your protected application is the usage of the Smarx Application Framework (SxAF, see *Smarx Compendium* chapter 4.5):
   - Make sure that the Smarx OS PPK is installed on your computer. Start the “MARX PPK Control Center” and go to “Quick Access” → “SxAF”.
   - Create a new SxAF project and specify *Implementation with API* as project type.
   - Choose the project-specific values for the CRYPTO-BOX, such as label and AES keys.
   - Select your project's licensing strategy by defining one or more partitions to hold data objects with licensing information, which can be expiration dates, counters, network licenses and/or customer specific memory objects (see *Smarx Compendium* chapter 4.5.5 for further details).
   - Use the “CB Format” option in SxAF to format your CRYPTO-BOX units with the project settings.
   - Optionally, you can export your project settings into an XML file to use with command line based tools for automated CRYPTO-BOX formatting (see *Smarx Compendium* chapter 4.9 for further details).
4. If you plan to update your CRYPTO-BOX later at your end-user's site, you can create the Remote Update Tool for this project and ship it together with the CRYPTO-BOX to your end-users (see *Smarx Compendium* chapter 4.10.3 for more information).
5. Test all licensing options carefully.
6. Ship your protected application, along with the CRYPTO-BOX and supplemental files (drivers, network server for network licensing if applicable). MARX provides an easy-to-use redistribution setup. See our *Application Notes “Driver Installation”* for further instructions.

3. Smarx®OS as Basis for the CRYPTO-BOX Integration

3.1. Overview

Smarx®OS is the basic input-output system of the CRYPTO-BOX system. It is used for communication with the CRYPTO-BOX within all components available in the *Professional Protection Kit (PPK)*, such as:

- Libraries provided by MARX for API implementation
- Smarx Application Framework (SxAF)
- Command Line Tools

Smarx OS supports all popular platforms:

- Windows 64/32 bit
- Linux 64/32 bit, x86 and ARMv7/ARMv8)
- macOS (ARM64 and x86_64)
- iOS (libraries/sample code can be provided on request, please *contact us*)
- Android (libraries/sample code can be provided on request, please *contact us*)
- Others - please contact us and provide your specs/requirements

Many programming environments (IDE’s) for these platforms are supported, see chapter 5 for more details.

3.2. Smarx®OS API Subsets

Smarx OS consists of several APIs providing a different subset of functionality. Not all API subsets are available for each platform/compiler.

The following tables provides an overview about available Smarx OS APIs for the CRYPTO-BOX system:

Smarx®OS Interface	Platform	Language	Environment
Smarx API Simple protection API with SxAF projects	Windows, Linux, macOS, Android, iOS (*)	C++ 11, C# 4.0+, Delphi, VB, Python, Cocoa	MSVS 2013+, gcc 5.4+, Xcode 9+, Embarcadero Delphi 10+, Python 3.8/3.9
AC API (**) Simple automatic protection API with SxAF/AutoCrypt Wizard projects			
CBIOS API, DO API Advanced protection API	Windows, Linux, macOS, Android, iOS	C#, F#, C/C++, Java, Delphi, VB, VBA, Swift, LabVIEW, MATLAB, VFP, Scala, DMD, IVFortran, DarkBASIC, REALbasic	MSVS 6+, Builder 6+, Delphi 5+, gcc 4+, Xcode 9+ and others
RUMS API Simple remote update API with SxAF projects	Windows, Linux, macOS, Android, iOS (*)	C/C++, Delphi	MSVS 6+, Builder 6+, Delphi 5+
RFP API Advanced remote update API	Windows, Linux, macOS	C#, C/C++, Delphi, VB	MSVS 6+, Builder 6+, Delphi 6+, Xcode 10+

* Windows, Linux (Intel/ARM) and macOS (Intel/ARM) platforms are supported now, other platforms can be supported on request.
** AC API is a part of Smarx API

See chapter 5.2 in this document for information on obtaining libraries and sample code for your preferred interface.

3.2.1. Smarx®API

This is a high level API layer for the CRYPTO-BOX SC, XS and Versa models which exposes a more simple and user friendly programming interface to developers than other Smarx OS based APIs (CBIOS, see below).

Please refer to the *Smarx Compendium* chapter 11 for more details about the Smarx API.

3.2.2. AC API

The AC API (Smarx AC) introduces a higher abstract layer allowing developer with only one function call implemented into the source code of his application to:

- Start periodic validation of the license information stored in the CRYPTO-BOX (e.g. expiration date, counters, etc.) for both local and network scenarios
- Add exit event notification (AppExitEvent) with exception argument

AC API supports C/C++ (Visual Studio 2013/gcc 6.0/Xcode 9 and higher), C# (Visual Studio 2013 and higher), Delphi (Embarcadero Delphi 10 and higher), Python (3.8 and 3.9 on x86_64 platforms) under Windows, Linux and macOS. Licenses for AC API can be defined with AutoCrypt Wizard or SmrxProg command line tool. Further details can be found in the Readme file in the corresponding AC API sample folder (see chapter 5.2).

3.2.3. SmarxCpp

This is an object oriented implementation of CBIOS (Networking)/DO APIs mentioned below for C++ developers (MS Visual Studio 2013/gcc 5.4/Xcode 9 or higher). Refer to the *Smarx Compendium* chapter 10.13 for details.

3.2.4. CBIOS4NET/Smarx4NET

This is an object oriented, components based implementation of CBIOS (Networking)/DO/RFP APIs mentioned below for .NET developers (C#, VB.NET etc. for .NET Framework or .NET Core). Please refer to the *Smarx Compendium* chapter 10.13.2 for more details.

3.2.5. CBIOS API

This is the basic API for the CRYPTO-BOX SC, XS and Versa models. It includes functions for CRYPTO-BOX search and identification, access to its internal memory and encryption functions.
Please refer to the *Smarx Compendium* chapter 12 for more details about the CBIOS API.

3.2.6. CBIOS Networking

A special subset of the CBIOS API allowing access the CRYPTO-BOX on networks and perform network licensing - defining a number of running instances of the protected application to be run in a network. Please refer to our White Paper "Network Licensing" for more information about accessing the CRYPTO-BOX in networks.

3.2.7. DO API

The Data Objects (DO) API is a subset of the CBIOS API which provides a convenient way to create and access various objects for licensing purposes, such as expiration dates, counters, passwords or self-defined objects.
Please refer to the *Smarx Compendium*, chapter 14 for more details.

3.2.8. RFP API

The Remote Update API allows to update the CRYPTO-BOX directly on the end-user side. It is intended for customers who prefer API integration instead of using tools provided by MARX (RUMS component in SxAF or "RU_Tool.exe" command line tool, see separate *RUMS Application Notes* for details).
Please refer to the *Smarx Compendium*, chapter 15 for more information on the Remote Update technology.

3.2.9. Extended API (XSMRX)

Provides CRYPTO-BOX formatting features for customers who prefer API integration instead of using tools provided by MARX (SxAF or "SmrxProg.exe" command line tool).

Please refer to the *Smarx Compendium*, chapter 16 for more details.

3.2.10. Smarx Cloud Security (WEB API)

Authenticate users via Internet/Intranet and update the CRYPTO-BOX. Ideal for online licensing and subscription services.

For detailed description and Developer's Guide, see the *Smarx Cloud Security White Paper*.

4. Using the Smarx®OS API under Different Environments

4.1. Overview

Depending on the platform (OS) and programming environment used, the Smarx OS API libraries are provided in different formats, such as:

- Static libraries
- Dynamic libraries (DLL)
- .NET assembly (Managed DLL)
- COM/ActiveX
- Native DLL/SO

For an introduction into accessing the CRYPTO-BOX via API, we strongly recommend you to read the *Smarx Compendium* chapter 10.

4.2. Static Libraries (C/C++, Delphi)

Static libraries are the most secure way of linkage. They are provided for most of the supported programming environments under Windows, Linux and macOS platforms, including: Microsoft C/C++, Borland C Builder, Delphi environments, and GCC.

If you are working with Visual Studio 2013 and later or Delphi 10.1 and later, you can consider using our high level Smarx API (see chapter 3.2.1 or SmarxCpp (see chapter 3.2.3).

See the *Smarx Compendium* chapter 11 for a description of the Smarx API.

If you are using other or older environments, or you don't want to use Smarx API: many environments are supported by the CBIOS (Networking)/DO/RFP API (see chapter 3.2.5 to 3.2.8).

- See *Smarx Compendium* chapter 12 for an introduction to the CBIOS API and implementation details.
- See *Smarx Compendium* chapter 13 for details on CBIOS Networking.
- See *Smarx Compendium* chapter 14 for details on the DO API.
- See *Smarx Compendium* chapter 15 for details on the RFP (Remote Update) API.

4.3. Dynamic Libraries (DLL)

Dynamic libraries (DLLs) allow easy, but less secure linkage. DLL based implementation should be considered only if for some reason no other options can be used (static library, COM). When using DLL try to improve the level of protection and licensing logic for your application (using hardware based encryption, keeping vital data in the CRYPTO-BOX, using parallel threads, etc.), making it difficult to emulate this logic by replacing the DLL. DLLs are provided for Windows (x64 and x86).

The *Smarx OS CBIOS API Reference* contains a detailed description of the API calls within the CBIOS API and the CBIOS Network API (see chapter 3.2.5 and 3.2.6) for developers working with Visual Basic.

4.4. .NET

MARX provides .NET developers with an object oriented, component based approach, simplifying integration of protection and licensing to .NET applications. C# programming community got used to object oriented component based way of software development (main benefit of .NET).

If you are working with Visual Studio 2013 and later, you can consider using our high level Smarx API (see chapter 3.2.1 which is based on CBIOS4NET. See *Smarx Compendium* chapter 11 for a description of the Smarx API.

If using old environment (Visual Studio <2013) or customer specific protection and licensing logic is required, then consider using CBIOS+DO API, rather than Smarx API. CBIOS+DO API is available for .NET developers in Smarx4Net or CBIOS4NET assemblies. See the ".NET interfaces for developers" table on the next page for more details.

Both interfaces combine all Smarx programming interfaces under one roof for .NET platform:

- CBIOS (network mode)
- DO API (including CDO support)
- RU API (Remote Update API)

They cover the following types of MARX hardware:

- CRYPTO-BOX® SC (CBU SC)
- CRYPTO-BOX® XS and Versa (CBU)

The CBIOS4NET/Smarx4NET API Reference contains an introduction into CBIOS4NET/Smarx4NET and a detailed description of its Classes.

This table provides an overview about .NET interfaces for developers:

IDE	.NET	Local & Net Mode	Plat form	Additional Redistribu table **	PPK Assembly	\SDK Path	MSI / MSM (Redistributable)
MS VS 2013+	4.5.1+	*	Any CPU	-	Smarx4Net.dll	\dotNET 4.5\Any CPU	\SMARX4NET\ SMARX4NET.msi SMARX4NETMergeModule .msm
	Smarx4 NetCore 2.1+				Smarx4NetCore. dll	\dotNET Core\Any CPU	-
	4.x	+	x86, x64 (for .NET 2.0-3.5, a platform specific loader CBIOSLoader .cs is required)	VC Redist 2013	CBIOS4NET.dll	\dotNET 4\x86\signed \dotNET 4\x64\signed	\CBIOS4NET\ CBIOS4NET_x86.msi, CBIOS4NET_x86_x64.msi CBIOS4NetMergeModule. msm
				VC Redist 2010		\dotNET 4\Obsolete\x86 \dotNET 4\Obsolete\x64	\Obsolete\CBIOS4NET\ CBIOS4NET_x86.msi, CBIOS4NET_x86_x64.msi CBIOS4NetMergeModule. msm
	2.0 - 3.5			VC Redist 2005	CBIOS4NET.dll CBIOS4NET64.dll	\dotNET 2\asm signed	
MS VS 2010 - 2012	4.x			VC Redist 2010	CBIOS4NET.dll	\dotNET 4\Obsolete\x86 \dotNET 4\Obsolete\x64	
	2.0-3.5			VC Redist 2005	CBIOS4NET.dll CBIOS4NET64.dll	\dotNET 2\asm signed	
MS VS 2005 - 2008							

* Smarx4Net requires CBIOS Network Server for both local and network mode

** Included to MSI/MSM

The following two chapters explain the differences between Smarx4NET and CBIOS4NET.

4.4.1. Smarx4NET

Compared to the legacy CBIOS4NET interface (the corner stone of Smarx4NET, see chapter 4.4.2), the new Smarx4NET is based on fully managed code which makes the implementation more flexible. There is no need for VC Redistributables anymore.

It supports standard C# applications as well as .NET Core applications, and is ideal for protecting multi-device, multi-platform applications for desktop and mobile usage. Smarx4NET runs in network mode, which requires an installation of the CBIOS Server (either on the same computer or in the network). See our White Paper *"Network Licensing"* and the *CBIOS Server readme file* for installation instructions.

A Smarx4NET package which contains documentation, libraries and sample code can be found in our *Download section*. Please refer to the included readme file for the latest information and updates.

4.4.2. CBIOS4NET

CBIOS4NET was the first interface for C# developers. The CBIOS4NET assemblies are based on unmanaged code which requires installation of corresponding Visual C/C++ Redistributable components. Furthermore, a Loader is required to load platform specific CBIOS4NET components (32 or 64Bit).

CBIOS4NET allows direct access to the CRYPTO-BOX on the local USB port (Smarx4NET too, but the CBIOS Network Server needs to be installed and running on the same computer).

If you are starting a new project, we recommend to use Smarx4NET because it offers more flexibility such as AnyCPU support and pure managed code, as well as .NET Core support.
If you are already using CBIOS4NET or need direct access to local USB port, you can stick with CBIOS4NET. If you want to switch to Smarx4NET, slightly refactoring of your code is required, plus using network mode instead of local mode. More details can be found in chapter 4 of the readme file in the *Smarx4NET package*.

4.5. COM/ActiveX

COM/ActiveX is the Windows platform specific interface standard. This interface format is universal and can be used from almost any Windows programming environment. Required Smarx OS ActiveX objects are installed and properly registered by our driver setup utility (CBUSetup.exe, see separate Application Notes *"Driver Installation"*).

Native DLL/native SO are specific to Java environment (Windows and Linux correspondingly).

5. How to Find the Corresponding Library and Sample Code for Your Environment

5.1. Overview about Supported Environments

The following table contains programming environments currently supported by Smarx®OS APIs:

Smarx®OS library	Target audience	Smarx OS Interfaces	Platform	Language	Environment
SmarxCPP static library	If you develop apps in C++ 11, you can use: 1. AC API – implement protection with only one function call 2. Smarx API - validate license with only one call using higher abstract layer (see ch. 4.2) 3. SmarxCPP - develop your licensing model with enhanced C++ classes	Smarx API, AC API, RUMS*, CBIOS, DO API	Win, Linux, macOS, Android*, iOS*	C++ 11	MSVS 2013+, gcc 6.0+, Xcode 9+, QT 5+
Smarx API dynamic library	For Delphi, VB and Python	Smarx API	Win, Linux, macOS	VB, Delphi, Python	MSVS 2013+, Embarcadero Delphi 10+, Python 3.8/3.9
CBIOS static library	For C/C++, Delphi, Swift, COBOL, MATLAB, IVFortran developers	CBIOS, DO, RUMS API	Win, Linux, macOS, Android, iOS	C/C++, Delphi, Swift, COBOL, MATLAB, IVFortran	MSVS 6+, Builder 6+, Delphi 5+, gcc 4+, Xcode 4+ and others
CBIOS dynamic library	For: LabVIEW, VFP, DMD, DarkBASIC, REALbasic developers	CBIOS, DO API	Win, Linux, macOS	LabView, VFP, DMD, DarkBasic, REALbasic	*
CBIOS4NET assembly	For .NET developers See chapter *4.4* for details and differences between Smarx4Net and CBIOS4NET Note: Smarx API (Higher abstract layer) is implemented only for CBIOS4NET	Smarx, *RUMS, CBIOS, DO, RFP, DP API	Win x64/x86	C#, VB, C++.NET	.Net Framework, MSVS2005+
Smarx4Net / Smarx4NETCore assembly		CBIOS, DO, RUMS API	Any CPU	C#, VB, C++.NET	.NET Framework 4.5+(Smarx4NET) .NET6.0+ (Smarx4NETCore)
JNI CBIOS dynamic library	It is for Java, Scala developers	CBIOS, DO API	Win, Linux, macOS	Java, Scala	Java 6+ SDK, Eclipse SDK 3.7+

Smrxw COM library	Obsolete COM model. To be considered for VBA development only	CBIOS, DO API	Win	(Any) VBA, C#, VB, C++.NET, Delphi	*
RFP static library	RFP API allows to update the CRYPTO-BOX directly on the end-user side. In contrast to RUMS (see chapter *3.2*) it provides maximum flexibility. Available for C/C++ and Delphi only.	RFP API	Win, Linux	C/C++	MSVS 6+, gcc 4+
RFP dynamic library			Win	Delphi	Delphi 6+
Smarx®OS Data Protection	If you distribute your software together with sensitive and valuable data files, you will require reliable protection not only for your app itself but also for the data files used by your app.	DP API	Win	C#, Delphi	MSVS 2005+, Delphi 7+

\+ - and higher
* - Can be implemented upon request

5.2. Obtaining the required Library/Samplecode from the Protection Kit

All libraries and samples for the supported environments can be found in the Smarx OS Protection Kit (PPK), which will be delivered together with the CRYPTO-BOX Evaluation Kit or with the first CRYPTO-BOX order you received from MARX.

In all Smarx OS API packages (for Windows, Linux and macOS) there are 2 folder: /sdk and /samples. Take the sample code from the "Samples" section and select the corresponding libraries for your compiler version from the "SDK" (libraries) section to make sure to have the correct library version for your compiler version! Refer to the included readme files for detailed information and implementation hints!
Please *contact us* if you need libraries or sample code for environments which are not listed in the Protection Kit.

5.2.1. Windows

First, you need to install the latest Smarx OS Protection Kit (PPK) which can be downloaded at https://www.marx.com/downloads (MyMARX account and a valid *Support Option* are required). After the installation has finished, click on the “PPK Control Center” shortcut on your desktop. The Control Center provides an overview of the installed PPK components, including a brief introduction and links to the components.

Click on the "Implementation with API" button, then on “Libraries/Samples”. For Windows there are two options:

a) Windows Libraries

Here you can select the required library for your platform. This library needs to be implemented into your project.

b) Windows Samples

Here you will find the sample code for your compiler which demonstrates the available API calls. These samples are a good starting point to get familiar with the Smarx API. For different API subsets (e.g. CBIOS and DO, see chapter *3.2* for more details) there may be different samples available.

5.2.2. Linux

The “Smarx OS 4 Linux” package which includes libraries and sample code for the supported Linux based environments (see chapter 5.1) can be downloaded at https://www.marx.com/downloads (MyMARX account

and valid support option is required to download it). Please refer to the included readme file for further details.

The *Smarx Compendium*, chapter 10.6 provides an introduction on Linux support.

5.2.3. Mac (macOS/OS X)

The "Smarx OS 4 Mac" package includes libraries and sample code for the supported Mac environments (see chapter 5.1). The package can be downloaded at https://www.marx.com/downloads (MyMARX account and valid support option is required to download it). Please refer to the included readme file for further details.

The *Smarx Compendium*, chapter 10.7 provides an introduction on Mac support.

5.2.4. iOS

The Smarx OS package for iOS contains the CBIOS Network Client for iOS. The sample code demonstrates interaction with a remote CBIOS Server over the network from iOS devices.

For more information on using the CRYPTO-BOX in networks, please read chapter 6 in the *Smarx Compendium*.

Please *contact us* to get iOS sample code.

5.2.5. Android

The Smarx OS package for Android contains libraries and a sample application demonstrating how to access the CRYPTO-BOX under Android in network or local mode. In network mode, it allows to query a CRYPTO-BOX which is connected to a remote CBIOS Server. For local access, a customized implementation of the USB stack based on libusb library is used. This requires root access on the Android device. Android SDK and Eclipse IDE are required.

Samples for both network and local mode can be provided on request. Please *contact us* for libraries and source code.