Application Notes

AutoCrypt AN-1

Thema: Schneller Softwareschutz ohne Programmierkenntnisse mit AutoCrypt
Version: Smarx OS PPK V8.17 oder höher, AutoCrypt Package V1.5 oder höher
Zuletzt geändert: 21. November 2023 von Steffen Kaetsch
Ziel-Betriebssystem: Windows, Linux
Zielplattform: Intel x86/x64/ARM64
Quellcode der zu schützenden Anwendung erforderlich: ☐ Ja ☑ Nein
Anwendbar für Produkt: CRYPTO-BOX® SC / XS / Versa (USB-A und USB-C Varianten)

Automatischer Softwareschutz mit AutoCrypt

- Geringer Aufwand - Programm ist in wenigen Minuten geschützt
- Keine Programmierkenntnisse notwendig
- Kein Quellcode erforderlich
- Einsatz am Einzelplatz, als auch Schutz im Netzwerk (mit nur einer CRYPTO-BOX pro Netzwerk) möglich
- Lizenzierungsoptionen wie Ablaufdatum, Anzahl der Programmausführungen oder Anzahl der Netzwerklizenzen einfach definierbar
- Optional Aktualisierung von Lizenzierungsoptionen via Internet/Email über Remote Update
- Unterstützt werden Windows-Anwendungen (64 und 32 Bit Executables sowie DLLs) und .NET-Executables (inkl. .NET Core).

CRYPTO-BOX®

- Schneller und einfacher Schutz von Anwendungen mit AutoCrypt.
- Individuelle Einbindung für alle gängigen Programmierumgebungen
- Plattform-Unabhängigkeit, unterstützt werden Windows, Linux und macOS
- Netzwerkfähig und fern-programmierbar.
- EAL4+ zertifizierter Smartcard-Chip mit AES-Verschlüsselung in Hardware integriert
- RSA2048-Support in Hardware (CRYPTO-BOX SC) oder auf Treiberebene (CRYPTO-BOX XS/Versa).
- Anpassung des CRYPTO-BOX Systems an kundenspezifische Anforderungen möglich.
- Formschönes, kompaktes und stabiles Metallgehäuse, optional mit individueller Farbe oder Lasergravur
- Auch mit USB-C Stecker erhältlich.

Bestellen Sie noch heute Ihr Testpaket

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

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

www.marx.com

Inhaltsverzeichnis

1. AutoCrypt: Überblick

1.1. Auswahl der passenden AutoCrypt-Variante

Mit AutoCrypt können Anwendungen schnell und sicher geschützt werden. Es werden weder Eingriffe in den Quellcode, noch Programmierkenntnisse benötigt. Dazu wird in die Anwendung ein Schutzmechanismus eingebaut und sie zusätzlich komprimiert und verschlüsselt. AutoCrypt bietet vielfältige Schutz- und Lizenzierungsoptionen, mit denen Sie kreative Vertriebsstrategien verwirklichen können. Das beinhaltet zum Beispiel Ablaufdatum, Ausführungszähler, periodisches Überprüfen des Schutzes, Setzen von Passwörtern, Netzwerkunterstützung und vieles mehr.

Das Protection Kit (PPK) für die CRYPTO-BOX enthält 3 Versionen von AutoCrypt:

1.1.1. AutoCrypt Wizard

Dies ist der einfachste und schnellste Weg zum Schutz von Windows-Anwendungen. Der Wizard führt Sie durch alle Schritte - vom Schutz der Anwendung über die Konfiguration der CRYTO-BOX bis hin zu Remote Updates (optional). Die Projekt-Datei kann außerdem exportiert werden, um sie mit den Kommandozeilentools AC_Tool und SmrxProg (siehe *1.1.3*) einzusetzen.

Wenn Sie nach einer schnellen Schutzlösung suchen, die dennoch alle wichtigen Features unterstützt, ist AutoCrypt Wizard die richtige Wahl.

Eine detaillierte Schritt-für-Schritt-Anleitung zu AutoCrypt Wizard finden Sie in Kapitel *2.*

1.1.2. AutoCrypt SxAF

Diese Lösung ist im Vergleich zu AutoCrypt Wizard weniger intuitiv zu handhaben. Das SxAF bietet aber zusätzliche Lizenzierungsoptionen, wie die Unterstützung von Produkt-Editionen (siehe Kapitel *3.3.10*), sowie eine integrierte Datenbank mit Projekt- und End-User Management (siehe Kapitel *3.7*).

Wenn Sie diese zusätzlichen Funktionen benötigen, ist AutoCrypt SxAF die richtige Wahl für Sie.

Eine detaillierte Anleitung zu AutoCrypt SxAF finden Sie in Kapitel *3.*

1.1.3. Kommandozeilentools (AC_Tool, SmrxProg)

Die Kommandozeilentools machen vor allem dann Sinn, wenn Sie mehr Flexibilität – wie z.B. eine Automatisierung des Schutzvorgangs oder eine Anbindung an Ihr bestehendes Distributionssystems – benötigen. So kann zum Beispiel der Schutzvorgang von externen Anwendungen heraus aufgerufen und gesteuert werden. Die Projekt-Informationen liegen in Form von XML-Dateien vor, die sich z.B. von AutoCrypt Wizard oder AutoCrypt SxAF exportieren oder auch dynamisch aus eigenen Anwendungen heraus generiert werden können.

Während AC_Tool für den Schutz der Anwendung sorgt, dient SmrxProg zur Konfiguration (Formatierung) der CRYPTO-BOX mit den gewünschten Lizenzinformationen.

Weitere Details zu den Kommandozeilentools finden Sie in Kapitel *4.*

SmrxProg ist auch für Linux und macOS erhältlich, beachten Sie dazu bitte die entsprechenden Readme-Dateien in der „Smarx OS 4 Linux“ bzw. „Smarx OS 4 Mac“ Package. Diese können Sie im Downloadbereich von marx.com herunterladen (MyMARX-Login und gültiger Support-Vertrag werden benötigt).

1.2. Download und Installation von AutoCrypt

MARX® bietet zwei verschiedene AutoCrypt-Pakete an. Welches Paket Sie verwenden, hängt auch davon ab welche AutoCrypt-Variante Sie einsetzen wollen. Siehe dazu auch die Übersicht in *Kapitel 1.1*.

1. Wenn Sie einen schnellen Schutz wollen und Ihnen die Funktionalität des AutoCrypt Wizard ausreicht, oder Sie lediglich die jeweils aktuelle Version der Kommandozeilentools AC_Tool, SmrxProg und RU_Tool benötigen, ist die **AutoCrypt Wizard Package** ausreichend.
2. Im **Smarx OS Professional Protection Kit (PPK)** sind alle AutoCrypt-Varianten enthalten, inkl. AutoCrypt SxAF.

Das Smarx® OS Professional Protection Kit (PPK) und die AutoCrypt Wizard Package können Sie im Downloadbereich von marx.com herunterladen (MyMARX-Login und gültiger Support-Vertrag werden benötigt). Economy Support ist für Neukunden die ersten 45 Tage inklusive.

1.2.1. Smarx® OS Professional Protection Kit (PPK)

Laden Sie das „Smarx OS PPK“ im Downloadbereich von marx.com herunter. Starten Sie anschließend die Setup-Datei, um das PPK auf Ihrem PC zu installieren.
Sobald die Installation abgeschlossen ist, schließen Sie die CRYPTO-BOX an den USB-Port Ihres Computers an, Windows erkennt sie automatisch.

Das Smarx Professional Protection Kit enthält folgende Komponenten:

- Smarx PPK Control Center - ein Startmenü zum schnellen Zugriff auf alle verfügbaren Komponenten,
- AutoCrypt Wizard, siehe Kapitel *2;*
- Das Smarx Application Framework (SxAF) - ein integriertes System zum Schutz von Software und digitaler Medien. Es beinhaltet auch die AutoCrypt SxAF Komponente (siehe Kapitel *3*);
- Kommandozeilentools als Alternative zu AutoCrypt Wizard und SxAF, insbesondere zur Automatisierung und Anbindung an bestehende Systeme und Datenbanken (siehe Kapitel *4.1* und *4.2*);
- Tools für CRYPTO-BOX Treiber-, Netzwerkserverinstallation und Diagnose;
- Bibliotheken und Beispiele für Einbindung in den Quellcode für Windows, Linux und macOS (siehe dazu White Paper „Implementation with API“ unter www.marx.com → Support → Dokumente → White Papers;
- Dokumentationen (Handbuch und API-Referenzen).

Eine detaillierte Beschreibung aller Komponenten und Optionen des Smarx Professional Protection Kits finden Sie im "Smarx Compendium ". Sie können die jeweils aktuelle Version als PDF-Datei auf unserer Webseite (unter Support → Dokumente) herunterladen.

1.2.2. AutoCrypt Wizard Package

Laden Sie die „AutoCrypt Wizard Package“ im Downloadbereich von marx.com herunter. Entpacken Sie anschliessend das .zip-Archiv in einen beliebigen Ordner auf Ihrem Computer.

Vor Nutzung der AutoCrypt Wizard Package muss sichergestellt werden, dass der Treiber für Ihre CRYPTO-BOX auf Ihrem System installiert ist. Sofern Sie eine Internetverbindung haben, installiert Windows den Treiber automatisch beim ersten einstecken der CRYPTO-BOX. Alternativ können Sie unser Tool CBUSetup zur Treiberinstallation nutzen. Laden Sie CBUSetup herunter, entpacken Sie es und führen die Installation aus. Anschließend stecken Sie die CRYPTO-BOX in den USB-Port – sie wird automatisch erkannt.

2. AutoCrypt Wizard

2.1. AutoCrypt Wizard starten

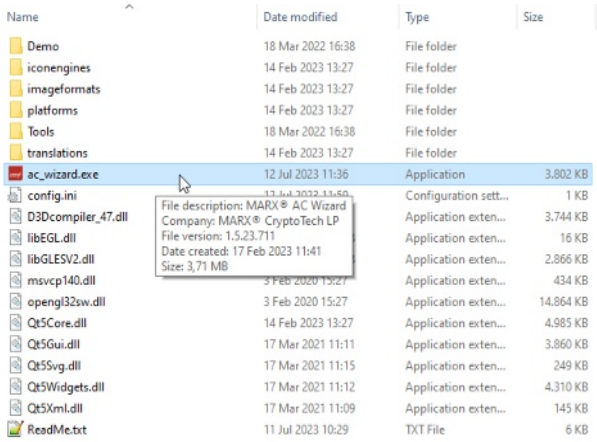
Je nachdem welches Paket Sie ausgewählt haben, (siehe Kapitel *1.2*), folgen Sie den Anweisungen in Kapitel *2.1.1* für die Installation des PPK, oder Kapitel *2.1.2* für die AutoCrypt Wizard Package

2.1.1. Smarx® OS Professional Protection Kit (PPK)

Nachdem Sie das PPK installiert haben, (siehe Kapitel *1.2.1*) klicken Sie auf dem Desktop auf den Link "PPK Control Center". Das Control Center zeigt eine Übersicht über die PPK-Komponenten an. Klicken Sie links auf "Schnellzugriff" und dann auf “AutoCrypt Wizard“.

2.1.2. AutoCrypt Wizard Package

Wenn Sie sich für die AutoCrypt Wizard Package entschieden haben, (siehe Kapitel *1.2.2*), starten Sie die Datei ac_wizard.exe im entpackten Ordner.



2.2. Anwendungen schützen

2.2.1. Schritte zum Schutz Ihrer Anwendungen

Wir empfehlen Ihnen die folgende Vorgehensweise:

1. Erstellen Sie ein neues AutoCrypt Wizard Projekt (siehe Abschnitt *2.2.2*). Ein Projekt enthält alle notwendigen Informationen zur Konfiguration der CRYPTO-BOX.
2. Fügen Sie die zu schützende(n) Anwendung(en) zum Projekt hinzu und wählen Sie die gewünschten Schutz- und Lizenzierungsoptionen. Eine Übersicht der verfügbaren Datenobjekte finden Sie im Abschnitt *2.2.5.*
3. Schützen Sie die Anwendung(en).
4. Konfigurieren (formatieren) Sie die gewünschte Anzahl an CRYPTO-BOX Modulen mit den Projekteinstellungen (siehe Abschnitt *2.3*).
5. Optional können Sie Ihr AutoCrypt Wizard Projekt zur Nutzung mit den Kommandozeilentools AC_Tool, SmrxProg und RU_Tool exportieren. Dies ermöglicht eine Automatisierung des Schutzvorganges, der Formatierung der CRYPTO-BOX Module und von Remote Update (siehe Abschnitt *4*). Nutzen Sie dazu die Option „Exportiere Projekt“ im AutoCrypt Wizard.
6. Wenn Sie Lizenzierungsoptionen später beim End-User aktualisieren möchten (z.B. Ablaufdatum oder Ausführungszähler), erstellen Sie zusätzlich das Remote Update Utility für das Projekt und liefern es zusammen mit der CRYPTO-BOX an Ihre End-User aus (siehe Abschnitt *2.5*).
7. Testen Sie den Schutz und die gewählten Lizenzierungsoptionen sorgfältig.
8. Liefern Sie die geschützte(n) Anwendung(en) zusammen mit der CRYPTO-BOX und ggf. zusätzlichen Dateien (CRYPTO-BOX Treiber, Netzwerkserver bei Netzwerkschutz) aus. MARX stellt dazu einfach zu handhabende Installationsprogramme zur Verfügung (siehe Abschnitt *5*).

2.2.2. Neues Projekt erstellen bzw. vorhandenes öffnen

Über den AutoCrypt Wizard Startbildschirm können Sie ein neues Projekt erstellen oder ein vorhandenes zur weiteren Bearbeitung öffnen. Wir empfehlen Ihnen, mit dem mitgelieferten Demoprojekt zu starten: klicken sie auf den Button „Bestehendes Projekt öffnen“ und wählen Sie das „AutoCrypt Demo Project“ aus.

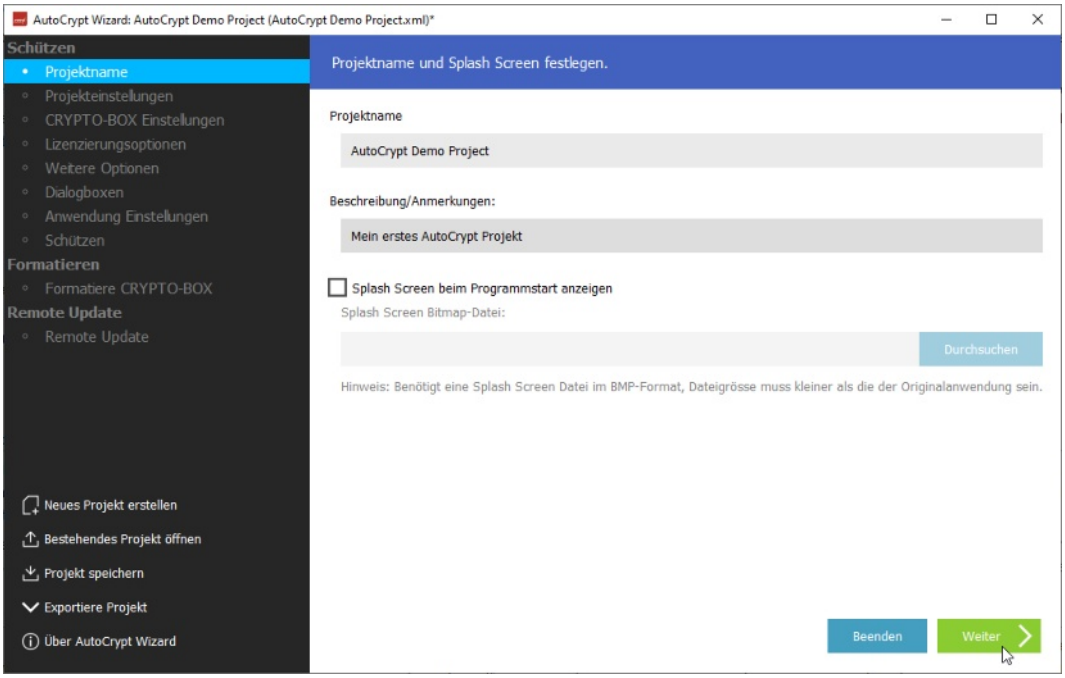
Geben Sie einen Projektnamen und eine Beschreibung (optional) ein.

Bei Bedarf können Sie einen Splash-Screen festlegen, der vor dem Start der geschützten Anwendung

angezeigt wird. Wählen Sie dazu eine Grafikdatei aus – diese muss im Bitmap-Format (.bmp) vorliegen und darf nicht größer als die zu schützende Anwendung sein.

Sie können beispielsweise die Windows-Anwendung „Paint“ nutzen, um ein beliebiges Bild als Windows Bitmap (BMP) Datei abzuspeichern. Verringern Sie ggf. die Auflösung oder Farbtiefe der Grafikdatei, um die Dateigrösse zu verringern.

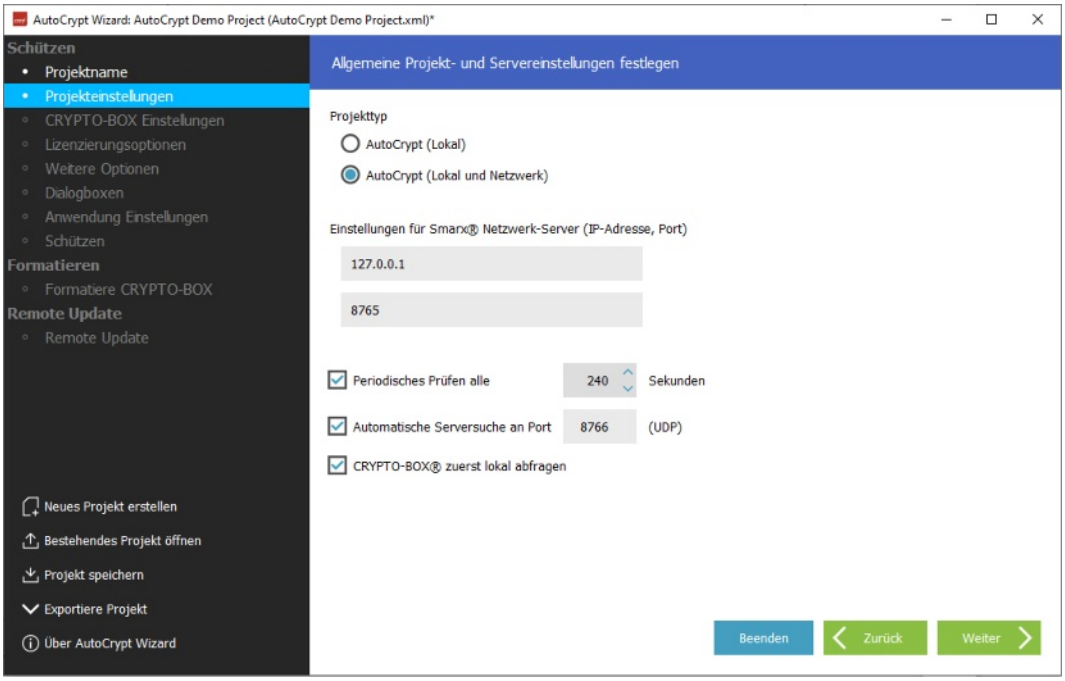
Bei .Net 6.0+ Anwendungen wird die Splashscreen-Option nicht unterstützt, die Splashscreen-Einstellungen werden in diesem Fall ignoriert



Klicken Sie auf „Weiter“, um die Projekteinstellungen anzupassen.

2.2.3. Projekteinstellungen

Wählen Sie zunächst im oberen Teil des Fensters den Projekttyp aus. AutoCrypt-Projekte können entweder lokal oder Netzwerk-basierend sein. Bei lokalen Projekten wird die Anwendung mit der am lokalen USB-Port des Computers angeschlossenen CRYPTO-BOX geschützt. Bei Netzwerkprojekten sind die Anwendungen über die an einem beliebigen Computer im Netzwerk angeschlossene CRYPTO-BOX geschützt, auf dem der „CBIOS Netzwerkserver“ läuft (siehe Abschnitt *5.1.4*) - Sie bestimmen dabei wie oft die Anwendung im Netzwerk ausgeführt werden darf. Wählen Sie das passende Verfahren: entweder „AutoCrypt (Lokal)“ für lokalen Schutz oder „AutoCrypt (Lokal und Netzwerk)“ bei reinen Netzwerkprojekten bzw. gemischten lokalen und Netzwerkprojekten.



Wenn Sie den Projekttyp „AutoCrypt (Lokal und Netzwerk)“ gewählt haben, können Sie darunter die Einstellungen zum Netzwerkserver angeben (IP-Adresse und Port); die voreingestellte IP-Adresse lautet „127.0.0.1“, der Port ist 8765. Anstelle einer IPv4-Adresse können Sie auch eine IPv6-Adresse oder den zugehörigen Computernamen angeben (zum Beispiel „PC-517“). Falls sich die Servereinstellungen später ändern, lassen sich diese später wieder zurücksetzen bzw. anpassen: sollte der Server an der angegebenen IP-Adresse nicht gefunden werden, öffnet die geschützte Anwendung automatisch einen Dialog, in dem die Servereinstellungen abgefragt werden.

Weitere Informationen zur Verwendung der CRYPTO-BOX im Netzwerk und zur Konfiguration des Netzwerkservers finden Sie im White Paper „Netzwerklizenzierung“ auf unserer Webseite.

Falls die Option „Periodisches Prüfen“ aktiviert ist, wird im festgelegten Zeitabstand das Vorhandensein der CRYPTO-BOX überprüft, solange die Anwendung läuft. Wenn die CRYPTO-BOX nicht gefunden wird, wird eine Fehlermeldung ausgegeben und die Anwendung beendet. Der Abstand zwischen den Prüfungen sollte mindestens 120 Sekunden oder mehr betragen. Es sind auch kürzere Werte möglich; das sollte aber nur dann gemacht werden, wenn es für die Lizenzierung wichtig ist.

Die letzten beiden Optionen sind nur im Netzwerkmodus verfügbar: automatische Serversuche via UDP bedeutet, dass die geschützte Anwendung selbständig nach vorhandenen CRYPTO-BOX Servern sucht (Server muss sich im selben Sub-Netz befinden). Die Standardeinstellungen für den UDP-Port ist 8766, Sie können ihn in der Serverkonfiguration ändern. Wenn die letzte Option "CRYPTO-BOX zuerst lokal abfragen" aktiviert ist, prüft die Anwendung zuerst, ob sich eine CRYPTO-BOX lokal am Computer befindet bevor eine Netzwerksuche gestartet wird.

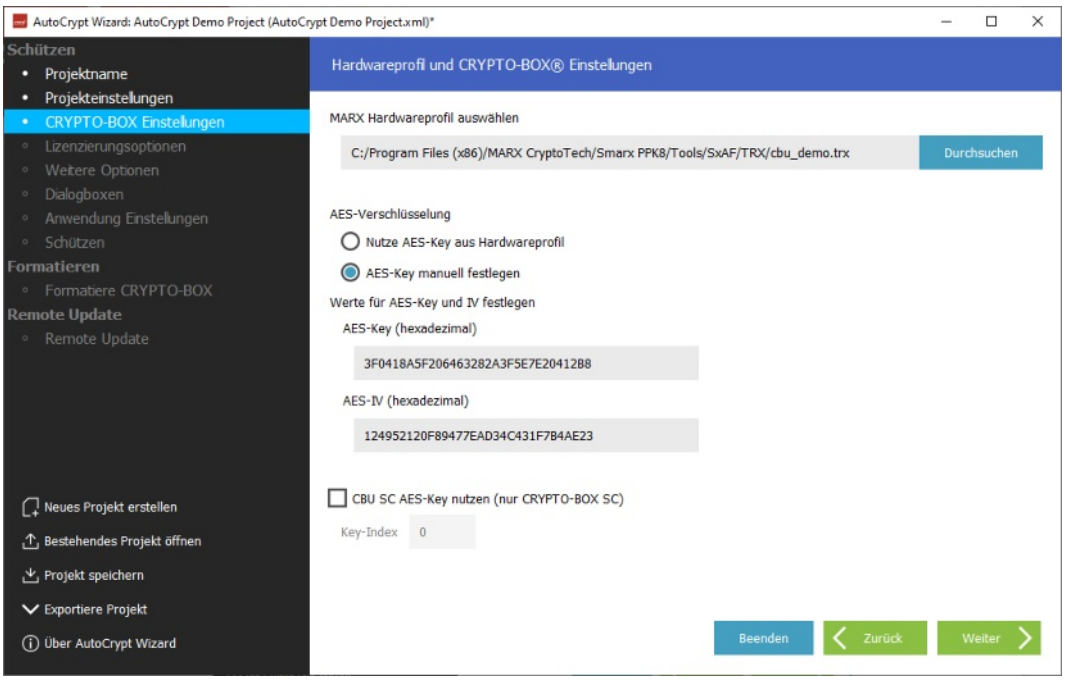
2.2.4. CRYPTO-BOX® Einstellungen

Im oberen Teil des Fensters wählen Sie das Hardwareprofil der CRYPTO-BOX für das Projekt aus. Das Hardwareprofil enthält die Zugriffspasswörter auf die CRYPTO-BOX . Wählen Sie das Profil „cbu_demo“ aus, wenn Sie die CRYPTO-BOX im Testpaket nutzen. Wenn Sie das „AutoCrypt Wizard Package“ nutzen, finden Sie die Profildatei im Unterordner „Demo“ in Ihrem entpackten Archiv. Haben Sie das PPK installiert, finden Sie den die Profildatei unter: [PPK Hauptverzeichnis]\Tools\SxAF\TRX

Haben Sie bereits kundenspezifische CRYPTO-BOX Module gekauft, verwenden Sie das Hardwareprofil (TRX-Datei), welches Ihrer ersten Lieferung beiliegt. Klicken Sie auf „Durchsuchen“, um Ihre kundenspezifische TRX-Datei zu laden.

Weitere Details zur Handhabung des CRYPTO-BOX Hardwareprofils finden Sie in dem White Paper "TRX Datei" auf unserer Webseite.

Unter „AES-Verschlüsselung“ können Sie die Werte für den AES/Rijndael-Schlüssel und den Initialisierungsvektor definieren, die zur Verschlüsselung der Anwendung verwendet werden. Mit „Nutze AES-Key aus Hardwareprofil“ verwenden Sie die vordefinierten Werte, die Ihnen von MARX für alle Ihre CRYPTO-BOX Module bei während der Produktion zugewiesen wurden. Oder Sie wählen mit „AES-Key manuell festlegen“ individuelle Werte für AES-Key und IV.



Alle geschützten Anwendungen werden automatisch komprimiert und verschlüsselt. Zur Verschlüsselung wird der AES Private Key der CRYPTO-BOX genutzt.

Mit der CRYPTO-BOX SC ist es möglich, mehreren Anwendungen verschiedene AES Keys zuzuweisen – bei Nutzung von ein und derselben CRYPTO-BOX. Aktivieren Sie dazu die Checkbox "CBU SC AES-Key nutzen". Mit dem Key-Index legen Sie fest, welcher Schlüssel-Platz genutzt werden soll.

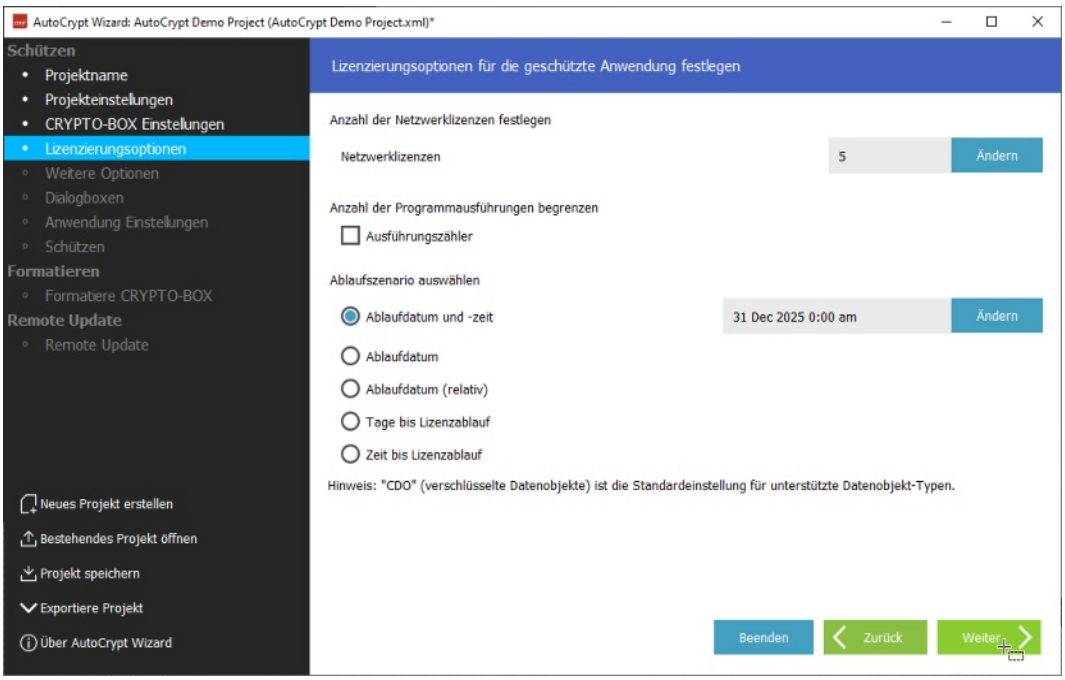
WICHTIGER HINWEIS:
Wenn Sie mehrere Anwendungen mit einer CRYPTO-BOX nutzen wollen, stellen Sie unbedingt sicher dass sie dieselben AES-Key-Werte für alle Projekte eingestellt haben! Wählen Sie in dem Fall entweder die Option „Nutze AES-Key aus Hardwareprofil“, oder legen Sie manuell dieselben Key-Werte für alle Projekte fest. Ausserdem müssen Sie sicherstellen, dass Sie bei allen Projekten unterschiedliche Partitionen zum speichern der Lizenzinformationen nutzen (siehe Kapitel *2.2.8*).

Alternativ können Sie AutoCrypt SxAF verwenden: dieses bietet die Möglichkeit, mehrere Anwendungen innerhalb eines Projekts anzulegen und zu schützen (siehe Kapitel *3.3.4*).

Eine Ausnahme ist die CRYPTO-BOX SC: hier können Sie für jedes Projekt einen eigenen AES-Key definieren. Aktivieren Sie dazu die Checkbox "CBU SC AES-Key nutzen".

Klicken Sie auf „Weiter“, um zu den Einstellungen der Lizenzierungsoptionen zu gelangen.

2.2.5. Lizenzierungsoptionen



Hier können Sie Lizenzeinstellungen für Ihre Anwendung vornehmen. Dazu legen Sie die Werte für Lizenz-Datenobjekte fest, zum Beispiel: Anzahl Netzwerklizenzen, Ablaufdatum, Ausführungszähler, und weitere.

Um ein Datenobjekt hinzuzufügen, aktivieren Sie es durch Klick auf das Auswahlfeld, klicken Sie auf „Ändern“ um den gewünschten Wert festzulegen und anschließend auf „Übernehmen“. Um ein Datenobjekt zu löschen, klicken Sie nochmal auf das Auswahlfeld.

Bei den Datenobjekten haben Sie die Wahl zwischen „CDO“ (Crypted DataObject = verschlüsseltes Datenobjekt) und unverschlüsseltem Datenobjekt („CDO“ deaktiviert). CDO bietet zusätzlichen Schutz gegen Manipulationen. Falls Sie verschlüsselte Datenobjekte zusätzlich per API abfragen wollen, beachten Sie die entsprechenden Hinweise in den Readme-Dateien unserer API-Beispiele, da nicht alle API-Bibliotheken CDO unterstützen, z.B. bei älteren oder exotischen Entwicklungs-umgebungen. Bei weiteren Fragen wenden Sie sich an unseren technischen Support.

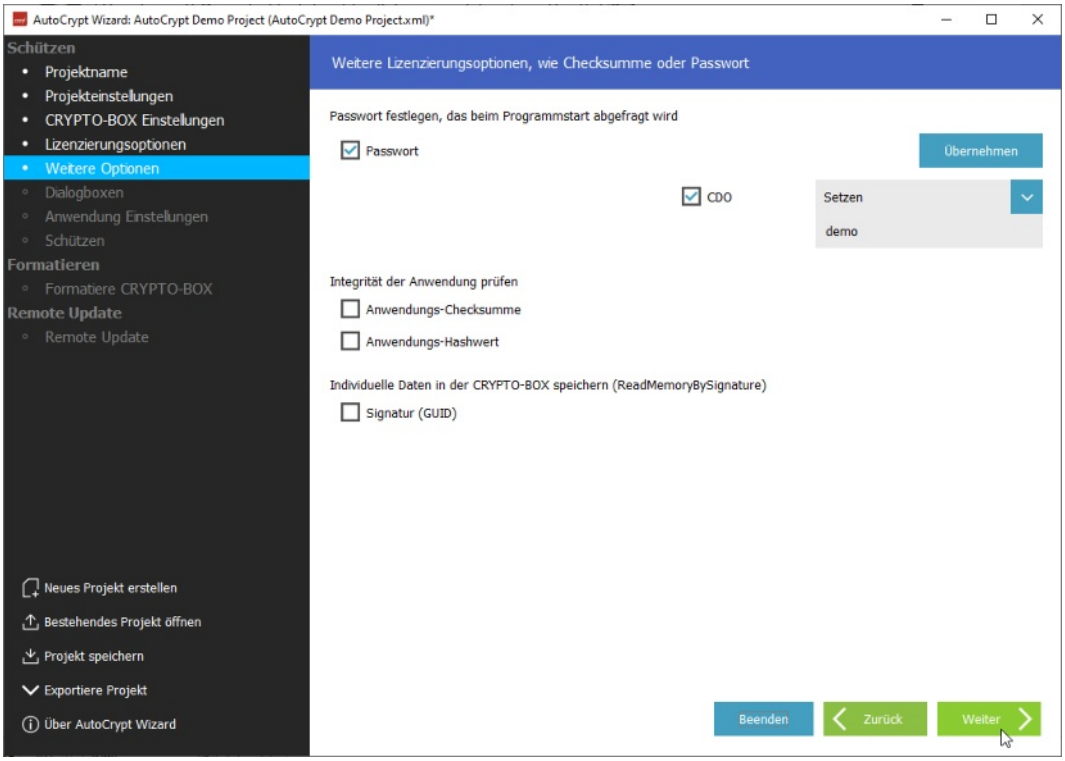
Folgende Datenobjekte stehen zur Verfügung:

Netzwerklizenz	Bestimmt wie oft die geschützte Anwendung im Netzwerk ausgeführt werden darf. Nur verfügbar wenn unter Projekteinstellungen der Projekttyp „AutoCrypt (Lokal und Netzwerk)“ gewählt wurde – siehe Kapitel *2.2.3*. **Wichtig:** Der Netzwerklizenz-Zähler wird nur von den CRYPTO-BOX Modellen SC und XS unterstützt. Die CRYPTO-BOX Versa unterstützt zwar auch den Netzwerkmodus, die Anzahl der Netzwerklizenzen ist jedoch immer unbegrenzt!
Ausführungszähler	Legt fest wie oft die geschützte Anwendung gestartet werden kann.
Ablaufdatum und -zeit	Genaues Ablaufdatum und Uhrzeit, nach der die geschützte Anwendung nicht mehr gestartet werden kann, z.B. 31. Dezember 2021 23:59:00
Ablaufdatum	Festes Ablaufdatum, z.B. 31. Dezember 2021. Dieser Datenobjekttyp ist veraltet und nur aus Kompatibilitätsgründen enthalten, bitte nutzen Sie stattdessen das Datenobjekt "Ablaufdatum und -zeit"
Ablaufdatum relativ	Das "Ablaufdatum relativ" legt fest, wie viele Tage die Anwendung ausgeführt werden darf, beginnend vom **ersten Start der Anwendung**
Tage bis Lizenzablauf	"Tage bis Lizenzablauf" legt fest, wie viele Tage die Anwendung ausgeführt werden darf, beginnend vom **Tag der Formatierung der CRYPTO-BOX** (siehe Kapitel *2.3*)
Zeit bis Lizenzablauf	Zeit (in Sekunden), die die geschützte Anwendung genutzt werden darf

Die Lizenz-Datenobjekte werden in der CRYPTO-BOX gespeichert. Sie können sie später direkt beim Kunden mit Remote Update aktualisieren – siehe dazu Kapitel *2.5*.

Klicken Sie auf „Weiter“, um zum Fenster „Weitere Optionen“ zu gelangen.

2.2.6. Weitere Optionen



Passwort
Hier können Sie ein Passwort festlegen, welches bei jedem Start der Anwendung abgefragt wird.

Checksumme
Dieses Datenobjekt prüft eine Checksumme ab, die über die geschützte Anwendung gebildet wurde. So kann beispielsweise festgestellt werden, ob die Anwendung manipuliert wurde. Die Anwendung wird dazu mit der in der CRYPTO-BOX gespeicherten Checksumme verglichen.

Anwendungs-Hashwert
Hier wird ein Hashwert über den Name der Anwendung gebildet, damit diese nicht nachträglich umbenannt werden kann. Die Anwendung wird dazu mit dem in der CRYPTO-BOX gespeicherten Hashwert verglichen.

WICHTIG:
Setzen Sie die Datenobjekte „Anwendungs-Checksumme“ und „Anwendungs-Hashwert“ nicht ein, wenn Sie vorhaben die geschützte Anwendung zu einen späteren Zeitpunkt zu aktualisieren bzw. gegen eine neuere Version auszutauschen (siehe Abschnitt *2.2.8*), da die neue Anwendung dann einen anderen Hashwert hat als den in der CRYPTO-BOX gespeicherten!

Signatur (GUID)
Diese Option ist für Softwareentwickler: Sie erlaubt das speichern eines individuellen Datenblocks bis zu 16 Byte Länge (zum Beispiel mit kundenspezifischen Daten) in der CRYPTO-BOX. Diese Daten können von der geschützten Anwendung ausgelesen werden – mit minimalem Aufwand!

Vorteil dieser Lösung: es sind keine Kenntnisse des CRYPTO-BOX API notwendig! Sie brauchen lediglich den Code aus unserem Beispielprogramm in den Quellcode Ihrer Anwendung zu implementieren.

Das Beispielprogramm und eine Readme-Datei mit Erläuterungen finden Sie im PPK:

[Smarx OS PPK Hauptverzeichnis]\SmarxOS-Samples\ReadMemoryBySignature

Das ganze funktioniert so: Nachdem die Prüfung der CRYPTO-BOX erfolgreich war, liest die mit AutoCrypt geschützte Anwendung die Daten aus der CRYPTO-BOX, entschlüsselt sie und schreibt sie in einen

Speicherpuffer, der mit einer individuellen Signatur versehen ist. Dieser Speicher kann durch den von Ihnen implementierten Code (siehe oben) ausgelesen und ausgewertet werden.

Klicken Sie auf „Weiter“, um zum Fenster „Dialogboxen“ zu gelangen.

2.2.7. Dialogboxen

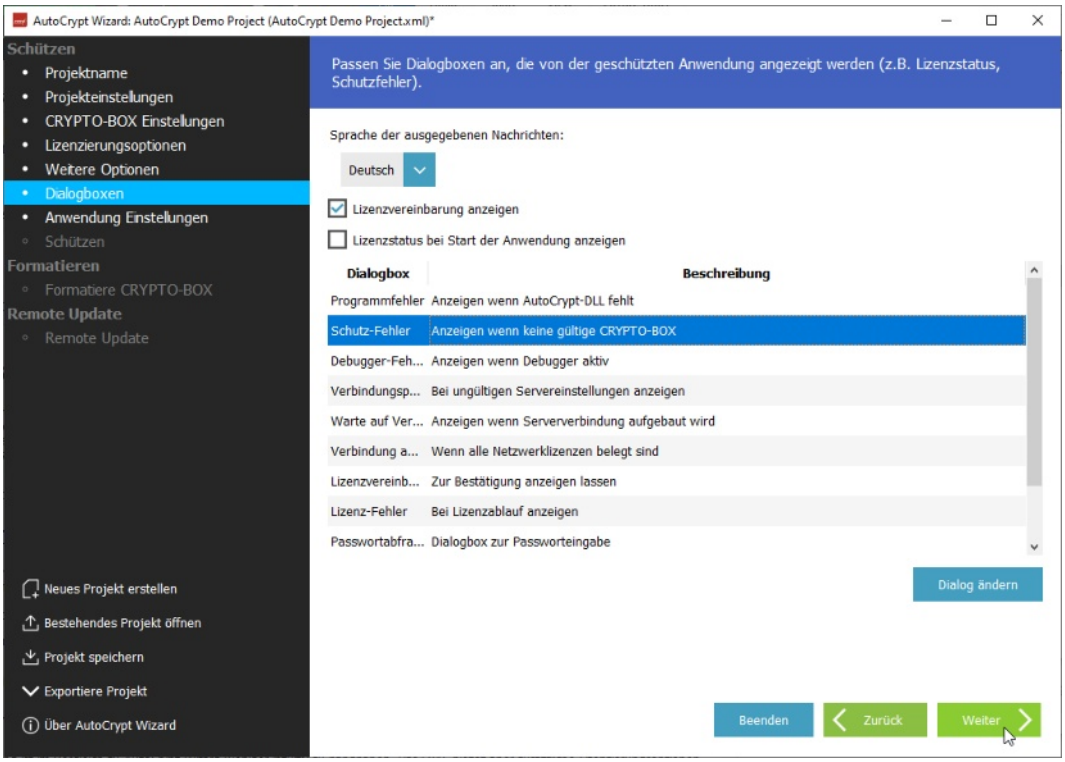
Für die geschützte Anwendung können Sie Dialogboxen individuell konfigurieren, die unter bestimmten Bedingungen ausgegeben werden, z.B. Lizenzstatus, Fehler- oder Warnmeldungen bei Lizenzverletzung, Meldung bei Lizenzablauf usw.

Wählen Sie dazu zuerst oben die gewünschte Sprache aus. Wählen Sie dann die gewünschte Dialognachricht aus der Liste aus und klicken auf „Dialog ändern“. Geben Sie dann den Dialogtitel und den Text ein, der erscheinen soll. Möchten Sie, dass bei einer bestimmten Bedingung keine Meldung angezeigt wird, lassen Sie die entsprechende Titelzeile und den Dialog leer.

Falls die Option „Lizenzvereinbarung anzeigen“ aktiviert ist, wird vor dem Anwendungsstart der von Ihnen vorgegebene Text mit Lizenzinformationen ausgegeben.

Falls die Option „Lizenzstatus anzeigen“ aktiviert ist, wird vor dem Start der Anwendung ein Hinweis eingeblendet wie oft bzw. wie viele Tage die Anwendung noch ausgeführt werden. Falls Sie keine Lizenzoptionen definiert haben (siehe Abschnitt *2.2.5*), ist diese Option deaktiviert.

Wenn sie die Dialognachrichten in einer anderen Sprache als Deutsch oder Englisch ausgeben wollen, überschreiben Sie einfach eine der beiden Voreinstellungen (Deutsch oder Englisch) mit Ihrer gewünschten Sprache.



2.2.8. Anwendung Einstellungen

Geben Sie oben zunächst Die Partition an, in der die Lizenzeinstellungen (siehe Kapitel *2.2.5*) gespeichert

werden sollen. Die Nummer muss zwischen 101 und 65535 liegen. Es empfiehlt sich, den voreingestellten Wert beizubehalten.

Wählen Sie dann Ihre zu schützende Anwendung aus. Es kann sich dabei um eine Windows .exe, .exe (.NET) oder DLL-Datei handeln (64 oder 32 Bit).

Zu Testzwecken können Sie die mitgelieferten Demo-Anwendungen und DLLs nutzen.

Bei Nutzung des **PPK** finden Sie diese unter:
[Smarx PPK Hauptverzeichnis]\SmarxOS PPK\Tools\SxAF\ Applicat“.

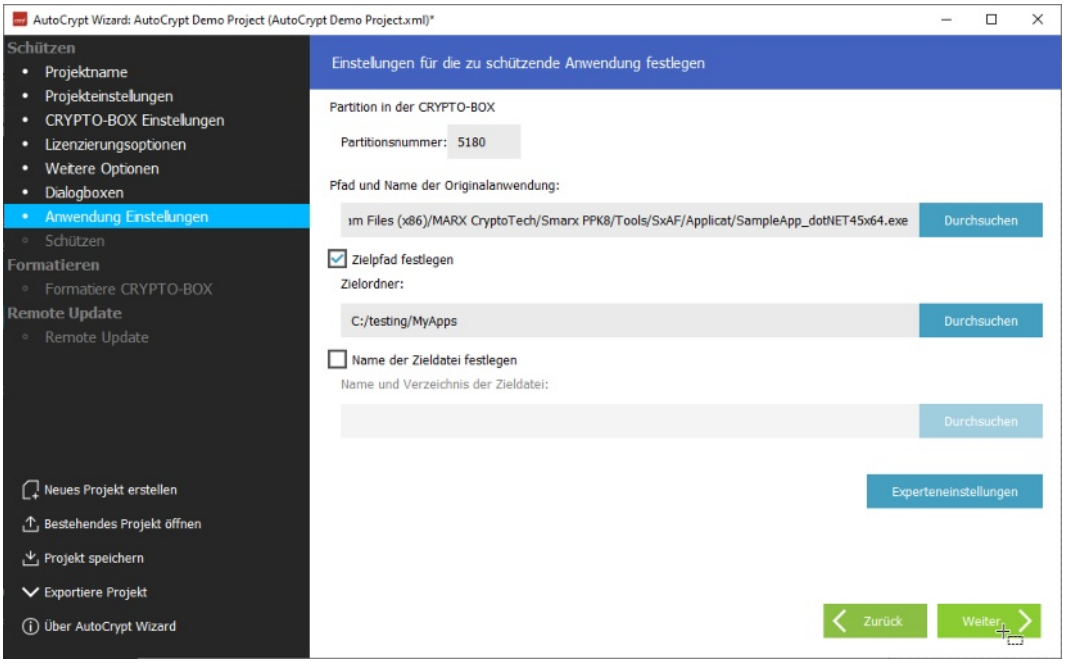
Bei der **AutoCrypt Wizard Portable Package** sind sie unter:

[AutoCrypt Package Hauptverzeichnis]\Demo

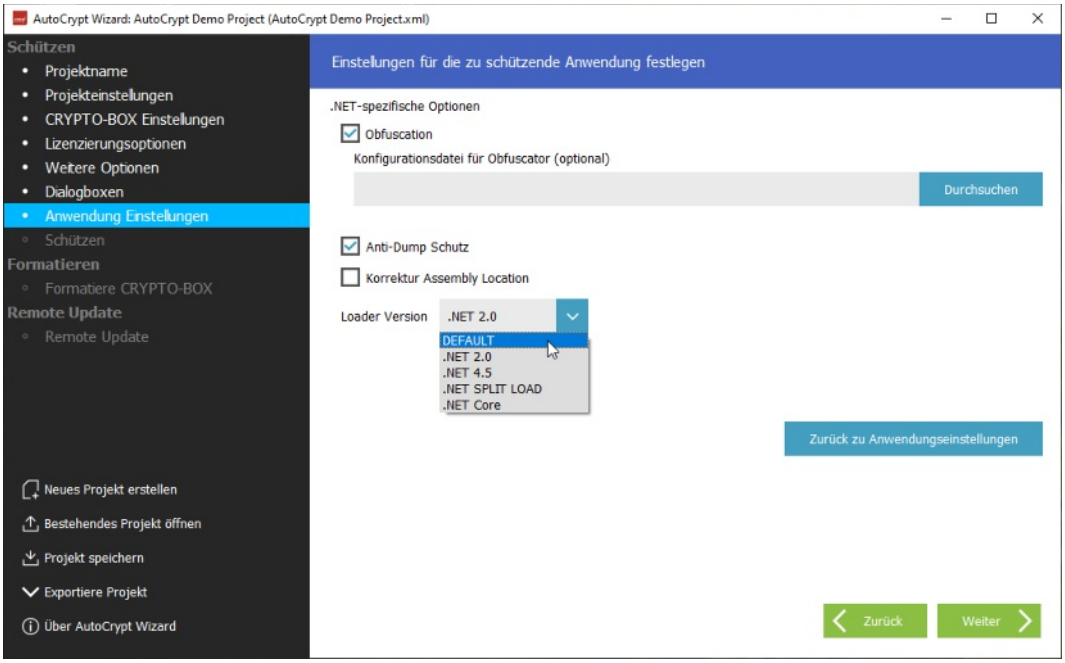
Wählen Sie hier die gewünschte Beispielanwendung, oder die Win32.dll/Win64.dll. Den Aufruf der geschützten DLL können sie mit DllLauncher.exe/DllLauncher64.exe testen.

Anschließend wählen Sie aus, wo die geschützte Anwendung gespeichert werden soll:

- Setzen Sie den Haken bei „Zielpfad festlegen“, wird die Anwendung im gewählten Zielpfad unter demselben Namen wie die Originalanwendung gespeichert.
- Setzen Sie den Haken bei „Name der Zieldatei festlegen“, können Sie zusätzlich den Dateiname der geschützten Anwendung ändern.



Wenn es sich bei Ihrer zu schützenden Anwendung um eine .NET-Anwendung handelt, haben Sie unter „**Experteneinstellungen**“ noch zusätzliche Optionen:



Bei Standard Win64/32-Anwendungen haben die Optionen unter „Experteneinstellungen“ keine Auswirkung.

- Mit „Obfuscation“ bietet AutoCrypt eine automatische Obfuscation der .Net-Anwendung an. Dazu wird im Hintergrund das Open Source Programm „Obfuscar“ genutzt. Weitere Details dazu finden Sie auf der Obfuscar-Webseite.
- Die Option „Anti-Dump Schutz“ erschwert das Dumpen von .Net-Anwendungen und sollte daher nur deaktiviert werden, falls die geschützte Anwendung nicht startet
- Die Option „Korrektur Assembly Location“ behebt das Problem, dass .Net-Anwendungen, die „Location Property“ nutzen um den Pfad der ausführenden Assembly zu erhalten - z.B. mit Assembly.GetExecutingAssembly() - nach dem Schutz von AutoCrypt nicht starten.
- Die Option „Loader version“ ermöglicht es, verschiedene Loader für .Net-Anwendungen auszuprobieren, beispielsweise wenn bei der Standardeinstellung (DEFAULT) die geschützte Anwendung nicht startet oder von Antivirus-Programmen irrtümlich als Schadsoftware erkannt wird. Folgende Optionen sind möglich:
  - DEFAULT (Standardeinstellung) – Automatische Erkennung: .NET_CORE für .Net 6.0+ Anwendungen (Bedingung: .exe, .dll und .runtimeconfig.json mit dem selben Name befinden sich im Verzeichnis der Originalanwendung), DOTNET_45 für .NET 4.x Anwendungen und DOTNET_20 für alle anderen Anwendungen
  - DOTNET_20 – forciert die Nutzung unseres älteren Loaders, der für .Net 2.0 Anwendungen entwickelt wurde (führt möglicherweise zu Inkompatibilitäten mit einigen .Net 4.x Anwendungen)
  - DOTNET_45 – Zur Nutzung mit Anwendungen, die mit .Net 4.x erstellt wurden
  - DOTNET_48 – Zur Nutzung mit Anwendungen, die mit .Net 4.8 erstellt wurden und TLS 1.2 Support benötigen
  - DOTNET_Core – forciert die Nutzung des Loaders für .Net Core Anwendungen (.NET 6.0 oder höher)
  - DOTNET_SPLIT_LOAD – Experimenteller Loader, um Fehlalarme von Antivirus-Software bei der

geschützten Anwendung zu umgehen. Dieser Loader ist nur für .Net 4.x-Anwendungen gedacht (beim DOTNET_Core Loader ist diese Funktionalität bereits im Loader integriert).

- Die Option „Kommandozeilenanwendung“ ist nur verfügbar, wenn der DOTNET_Core oder DOTNET_SPLIT_LOAD Loader ausgewählt wurde und ist bei Schutz von .NET-Kommandozeilenanwendungen zu aktivieren (Anwendungen ohne grafische Oberfläche)

Wichtige Hinweise zu .Net 6.0+ (.Net Core) Anwendungen:

1. Geben Sie bei .Net 6.0+ Anwendungen immer als Originalanwendung (siehe 2.2.8) die entsprechende .dll-Datei an, nicht die .exe! Die .exe ist bei .Net 6.0+ nur ein Loader, der die eigenliche Anwendung in der .dll-Datei lädt. AutoCrypt schützt die .dll und ersetzt die .exe mit einem eigenen Ladeprogramm. Falls die .exe angegeben wird, versucht AutoCrypt die zugehörige .dll zu schützen, sofern eine .NET 6.0+ Anwendung erkannt wurde.
2. Bei .Net 6.0+ Anwendungen muss die Zieldatei unbedingt denselben Namen haben wie die Originaldatei (siehe 2.2.8), sonst startet die geschützte Anwendung nicht!
3. .Net 6.0+ Anwendungen können Sie als Zielordner auch denselben Ordner wie die Originalanwendung angeben. In dem Fall ersetzt AutoCrypt die Originalanwendung mit der geschützten Dateien und verschiebt die Originaldateien in den Ordner _backup. Wenn Sie einen anderen Zielpfad wählen, vergessen Sie nicht immer die zugehörigen Runtime-Konfigurationsdateien in das Zielverzeichnis zu kopieren (.json-Dateien), sonst startet die geschützte Anwendung nicht!
4. .Net 6.0+ Anwendungen können nur mit der Option STANDARD oder DOTNET_Core geschützt werden, bei allen anderen Einstellungen startet die geschützte Anwendung nicht!
5. AutoCrypt kann .Net 5.0 Anwendungen nicht ohne weiteres schützen! Entweder Sie steigen auf eine neuere .Net-Version (6.0 oder höher) um, oder nutzen den in der AC_Tool Readme-Datei beschriebenen Workaround, um die .Net-Version in Ihrer Runtime-Konfigurationsdatei anzupassen. Siehe dazu Kapitel 4.1.

Wichtiger Hinweis zum DOTNET_SPLIT_LOAD Loader:

Mit der Option DOTNET_SPLIT_LOAD geschützte .Net 4.x Anwendungen benötigen unseren AC_Loader auf dem Zielsystem! AC_Loader ist im PPK enthalten:

[Smarx PPK Hauptverzeichnis]\Redistributable\AC_Tool\AC_loader.msi

Hinweis: AC_Loader installiert auch die CRYPTO-BOX Treiber, Sie brauchen daher nicht separat mit CBUSetup.exe installiert zu werden. Beachten Sie dazu die Hinweise in der AC_Loader Readme-Datei. AC_Loader unterstützt die Silent-Installation von msi-Paketen mit der /Quiet-Option.

2.2.9. Schützen

Stellen Sie sicher, dass die CRYPTO-BOX, die zu dem unter „CRYPTO-BOX Einstellungen“ (siehe Abschnitt *2.2.4*) festgelegtem Hardwareprofil passt am USB-Port angeschlossen ist und klicken Sie auf „Schützen“.

AutoCrypt komprimiert und verschlüsselt die geschützte Anwendung, der AES Rijndael Private Key der CRYPTO-BOX wird zur Ver- und Entschlüsselung genutzt (siehe Abschnitt *2.2.4*). Außerdem wird die Anwendung gegen Debuggen geschützt.

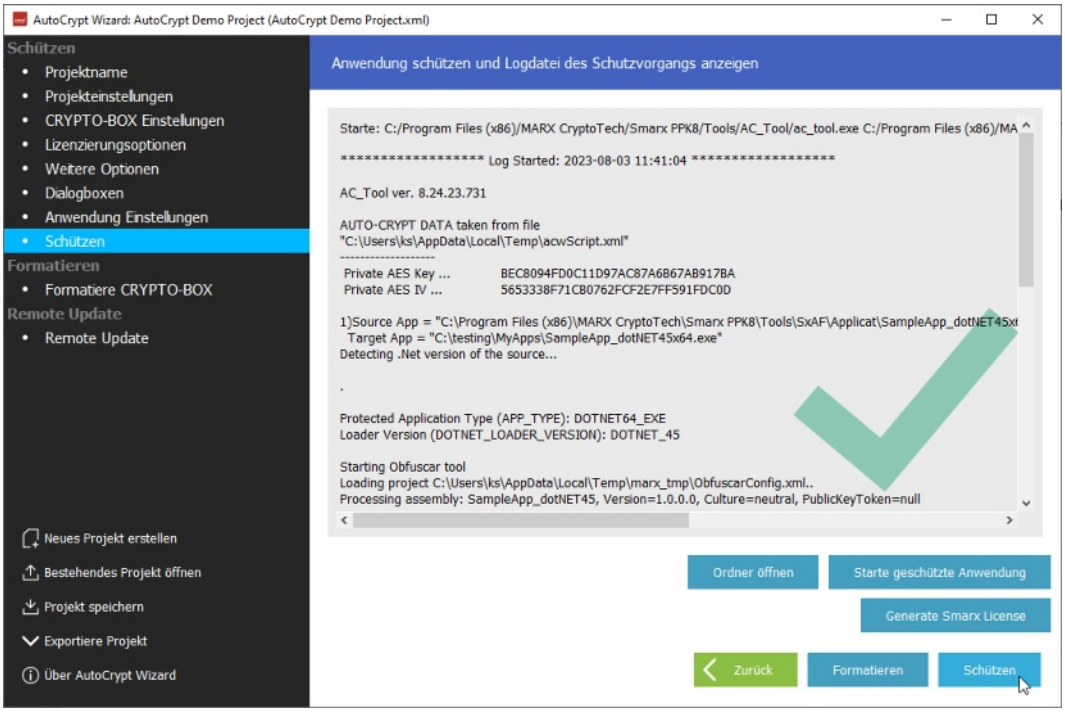
Sollte die geschützte Anwendung nicht lauffähig sein, nehmen Sie mit uns Kontakt auf – in vielen Fällen können wir AutoCrypt anpassen.

Falls Ihr Virenscanner bei der geschützten Anwendung Alarm schlägt, beachten Sie den FAQ-Eintrag Nr. 4 in Abschnitt 6.

Sie können den Schutzvorgang im Log-Fenster verfolgen, inklusive eventueller Fehlermeldungen. War alles erfolgreich, wird ein Haken angezeigt.

Klicken Sie jetzt auf den Button „Formatieren“, um fortzufahren.

Sie können den Schutz Ihrer Anwendungen mit der Kommandozeilenversion von AutoCrypt (AC_Tool.exe) automatisieren. AC_Tool.exe lässt sich über Kommandozeilenparameter steuern. Weitere Infos dazu finden Sie im Abschnitt *2.4*.



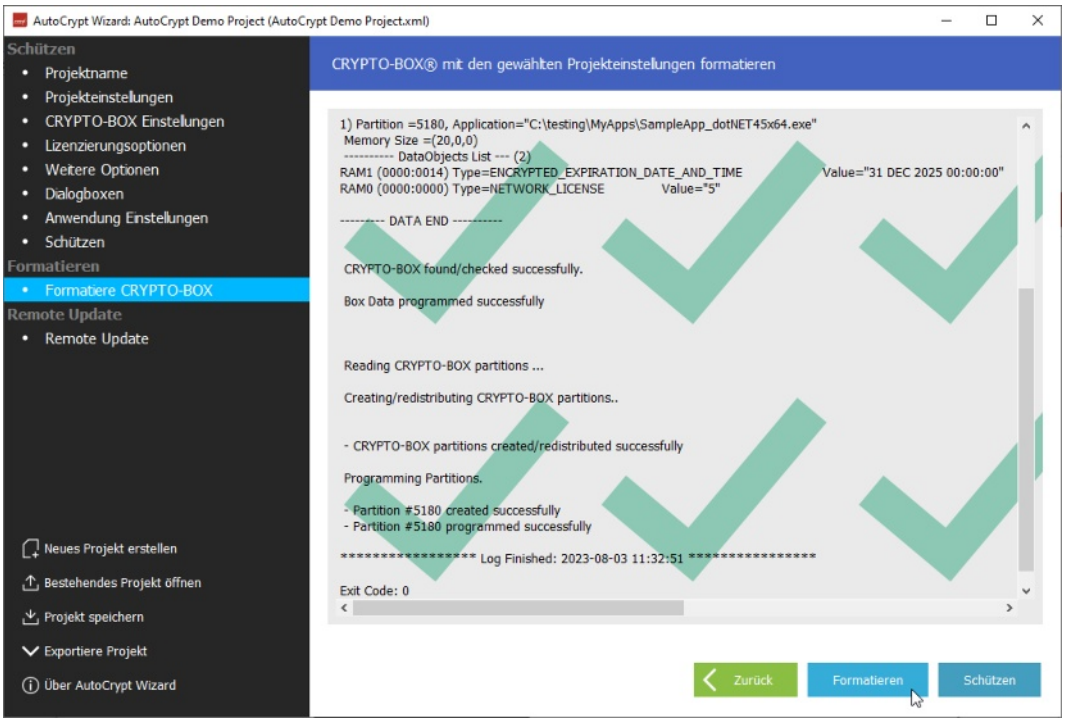
2.3. CRYPTO-BOX® formatieren

Nachdem sie die Anwendung erfolgreich geschützt haben, muss die die CRYPTO-BOX mit den von Ihnen festgelegten Lizenzdaten beschrieben werden.

Klicken Sie dazu den Button „Formatieren“. Sie können den Vorgang im Log-Fenster verfolgen. Hier werden auch mögliche Fehlermeldungen angezeigt. War alles erfolgreich, wird ein Haken angezeigt.

Zum formatieren mehrerer CRYPTO-BOX Module mit denselben Einstellungen stecken Sie einfach eine neue CRYPTO-BOX an und klicken erneut auf „Formatieren“.

Mit dem Kommandozeilenversion SmrxProg.exe) können Sie die Programmierung der CRYPTO-BOX automatisieren, z.B. zur Integration in Ihr bestehendes Vertriebssystem. Weitere Infos dazu finden Sie im Abschnitt *2.4.*



2.4. XML-Skript für Kommandozeilentools exportieren

Falls Sie den Anwendungsschutz und die Formatierung der CRYPTO-BOX in Ihre eigene Administrations- bzw. Distributionsstrategie integrieren wollen, bietet MARX die Kommandozeilentools AC_Tool und SmrxProg an. Mit dem Punkt „Exportiere Projekt“ in der Menüleiste unten links können Sie dazu Ihr AutoCrypt Wizard Projekt zur Nutzung mit dem Kommandozeilentools exportieren.

AC_Tool (dient zum Schutz von Anwendungen, siehe Abschnitt *4.1*) und SmrxProg (zum Konfigurieren der CRYPTO-BOX-Module, siehe Abschnitt *4.2*) sind Konsolenanwendungen, die Sie über Befehlszeilenparameter steuern. Diese Tools lassen sich von anderen Anwendungen aufrufen und über Skripte steuern. Auf diese Weise ist ein hoher Grad an Automatisierung möglich.

Der AutoCrypt Wizard selbst speichert die Projektdaten zwar auch in einer XML-Datei, deren Format ist jedoch nicht mit den Kommandozeilentools kompatibel.

2.5. Remote Update: CRYPTO-BOX® beim Endanwender aktualisieren

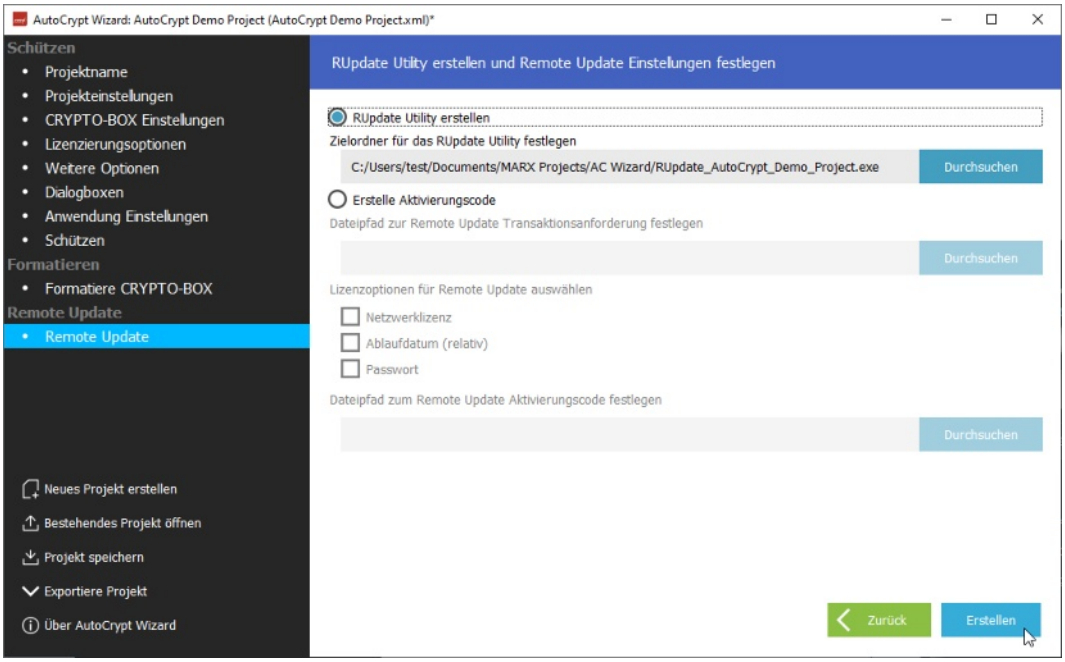
2.5.1. Remote Update Tool erstellen

Mit Remote Update können Sie die Lizenzinformationen in der CRYPTO-BOX direkt beim Endanwender aktualisieren. Das ganze geschieht über verschlüsselte Konfigurationsdateien, die z.B. einfach per Email verschickt werden können.

Dazu erstellen Sie das Remote Update Tool im AutoCrypt Wizard und liefern es zusammen mit der CRYPTO-BOX an Ihre Endanwender aus.

Klicken Sie dazu im AutoCrypt Wizard in der Navigationsleiste links auf den Punkt „Remote Update“.

Wählen Sie im rechten Fenster den Punkt „RUpdate Utility erstellen“ aus und geben darunter den Ordner an, in den das Remote Update Utility extrahiert werden soll, sowie den Dateinamen. Stellen Sie sicher, dass die CRYPTO-BOX, die zu dem unter „CRYPTO-BOX Einstellungen“ (siehe Abschnitt *2.2.4*) festgelegtem Hardwareprofil passt am USB-Port angeschlossen ist und klicken unten rechts auf „Erstellen“.



Im Log-Fenster werden Details und mögliche Fehlermeldungen angezeigt. War alles erfolgreich, wird ein Haken angezeigt.

Um das RUpdate Utility zu erstellen, wird eine RUMS-Lizenz benötigt (optional erhältlich).
Besuchen Sie www.marx.com → Shop → Lösungen → RUMS für weitere Details und Preise, oder wenden Sie sich direkt an MARX.
Wenn keine gültige RUMS-Lizenz vorliegt, wird im Log-Fenster die Meldung „Error: RUMS not licensed“ angezeigt.

Nachdem das RUpdate Utility erstellt wurde, klicken Sie auf „Zielordner durchsuchen“. Hier finden Sie 3 Dateien: das RUpdate Utility selbst (.exe-Datei), sowie 2 Sprachdateien. Senden Sie diese Dateien an Ihre(n) Endanwender, um Remote Updates für seine CRYPTO-BOX durchzuführen.

2.5.2. Transaktionsanforderung erstellen (Endanwender)

Um einen Remote-Update-Vorgang zu starten, schließt der Endanwender die CRYPTO-BOX an seinen Computer an und startet das RUpdate Tool. Hier klickt er anschließend auf “Erstelle Transaktionsanforderung”.

Es wird eine Datei mit der Endung .rutr erzeugt, diese schickt der Endanwender an Sie zurück (z.B. per Email).

Beim erzeugen der Transaktionsanforderung (*.rutr-Datei) wird wird eine spezielle Transaktions-ID in der CRYPTO-BOX gespeichert. Damit ist sichergestellt, dass nur die CRYPTO-BOX aktualisiert werden kann, mit

der die Transaktionsanforderung erzeugt wurde.

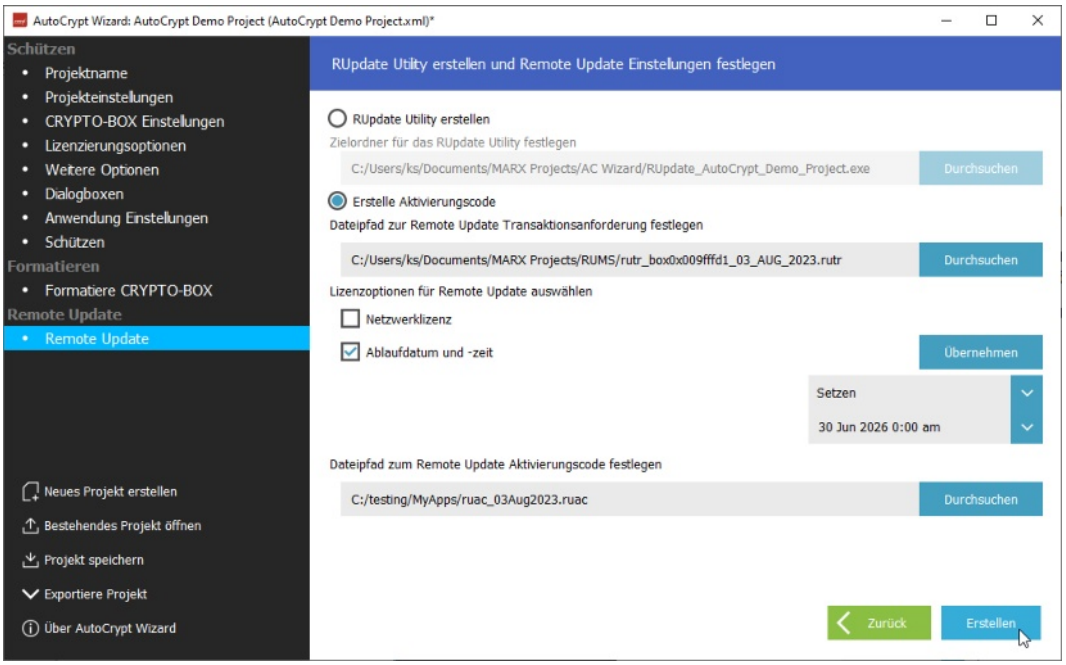
Sie können die Erzeugung der Transaktionsanforderung beim Endwanwender auch von Ihrer eigenen Software aus über Kommandozeilenparameter steuern. Eine detaillierte Beschreibung dazu finden Sie in den "*RUMS (Remote Update) Application Notes*".

2.5.3. Aktivierungscode erstellen (Software-Distributor)

Sobald Sie die Transaktionsanforderung (*.rutr-Datei) des Endanwenders erhalten haben, starten Sie den AutoCrypt Wizard, laden die Projektdatei (siehe Abschnitt *2.2.2*) und klicken in der Navigationsleiste links auf den Punkt „Remote Update“.

Wählen Sie nun die Option „Erstelle Aktivierungscode“ und wählen Sie darunter Transaktionsanforderung (.rutr) vom Endanwender aus. Anschließend haben Sie die Möglichkeit, die Datenobjekte in der CRYPTO-BOX zu ändern: wählen Sie die gewünschte Option aus und klicken auf „Ändern“. Sie können z.B. das Ablaufdatum verlängern bzw. auf „unlimitiert“ setzen, oder die Anzahl der Netzwerklizenzen erhöhen.

Abschließend wählen sie den Speicherort für den Aktivierungscode aus. Klicken Sie auf „Erstellen“, um den Aktivierungscode zu erzeugen. Diese Datei senden Sie an Ihren Endanwender.



Um den Activation Code zu erzeugen, muss eine CRYPTO-BOX am USB-Port angeschlossen sein (siehe Abschnitt *2.2.4*).

2.5.4. Ausführen des Aktivierungscodes (Endanwender)

Sobald der Endanwender den Aktivierungscode (*.ruac-Datei) von Ihnen erhalten hat (zum Beispiel per E-Mail), kann er die CRYPTO-BOX aktualisieren. Dazu startet er wieder das Remote Update Tool, schließt die CRYPTO-BOX an und klickt auf "Aktivierungscode ausführen". Die Transaktions-ID, die bei jeder Transaktionsanforderung erstellt und in der CRYPTO-BOX gespeichert wird, garantiert, dass jedes Update nur einmal ausgeführt werden kann.

3. AutoCrypt SxAF

3.1. SxAF starten

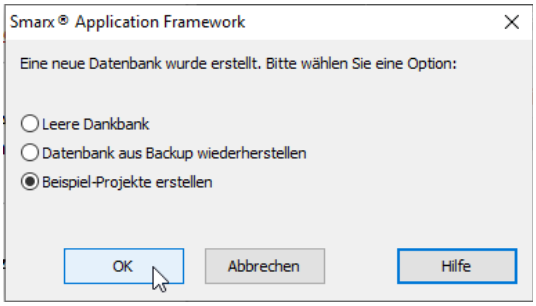
Nach der Installation des PPK (siehe Kapitel *1.2*) klicken Sie auf dem Desktop auf den Link "PPK Control Center". Das Control Center zeigt eine Übersicht über die PPK-Komponenten an. Klicken Sie links auf "Schnellzugriff" und dann auf “SxAF“.

3.2. Smarx Application Framework (SxAF)

Das Smarx Application Framework (SxAF) ist ein integriertes System zum Schutz von Software und Daten und arbeitet projektbasiert. Die Projekte werden in einer zentralen Datenbank gespeichert. SxAF ermöglicht:

- Automatischer Schutz Ihrer Anwendungen über eine grafische Oberfläche, inkl. Festlegung von Schutz- und Lizenzierungsoptionen und Dialogboxen
- Formatieren einer beliebigen Anzahl von CRYPTO-BOX Modulen passend zum Projekt
- Management von End-User Profilen
- Aktualisierung der in der CRYPTO-BOX gespeicherten Lizenzinformation direkt beim End-User (RUMS)

Wenn Sie das Smarx Application Framework (SxAF) zum ersten Mal starten, wird eine neue Datenbank angelegt; dazu erscheint der folgende Dialog:



Falls Sie sich für „Leere Datenbank“ entscheiden, wird die neue Datenbank lediglich das Hardwareprofil „cbu_demo“, jedoch keine Projekte enthalten.

Falls Sie stattdessen „Beispiel-Projekte erstellen“ wählen, werden zu Evaluationszwecken zwei Demoprojekte für AutoCrypt erzeugt (für lokalen und Netzwerkschutz).

Im Anschluss erscheint der Hauptbildschirm.

3.3. Anwendungen schützen

3.3.1. Schritte zum Schutz Ihrer Anwendungen

Wir empfehlen Ihnen die folgende Vorgehensweise zum erfolgreichen Schutz Ihrer Anwendungen:

1. Starten Sie das SxAF und erstellen Sie ein neues Projekt vom Typ "AutoCrypt" (siehe Abschnitt 3.3.2).
2. Fügen Sie die zu schützende(n) Anwendung(en) zum Projekt hinzu und wählen Sie die gewünschten Schutz- und Lizenzierungsoptionen. Eine Übersicht der verfügbaren Datenobjekte finden Sie im Abschnitt *3.3.6.*
3. Schützen Sie die Anwendung(en).
4. Konfigurieren (formatieren) Sie die gewünschte Anzahl an CRYPTO-BOX Modulen mit den Projekteinstellungen (siehe Abschnitt *3.4*).
5. Optional können Sie Ihre Projekteinstellungen in eine XML-Datei exportieren, um sie mit den Kommandozeilentools einzusetzen. Dies ermöglicht eine Automatisierung des Schutzvorganges und der Formatierung der CRYPTO-BOX Module (siehe Abschnitt *3.5*).
6. Wenn Sie Lizenzierungsoptionen später beim End-User aktualisieren möchten (z.B. Ablaufdatum oder Ausführungszähler), erstellen Sie zusätzlich das Remote Update Utility für das Projekt und liefern es zusammen mit der CRYPTO-BOX an Ihre End-User aus (siehe Abschnitt *3.6*).
7. Testen Sie den Schutz und die gewählten Lizenzierungsoptionen sorgfältig.
8. Liefern Sie die geschützte(n) Anwendung(en) zusammen mit der CRYPTO-BOX und ggf. zusätzlichen Dateien (CRYPTO-BOX Treiber, Netzwerkserver bei Netzwerkschutz) aus. MARX stellt dazu einfach zu handhabende Installer zur Verfügung (siehe Abschnitt *5*).

3.3.2. Neues Projekt erstellen bzw. vorhandenes öffnen

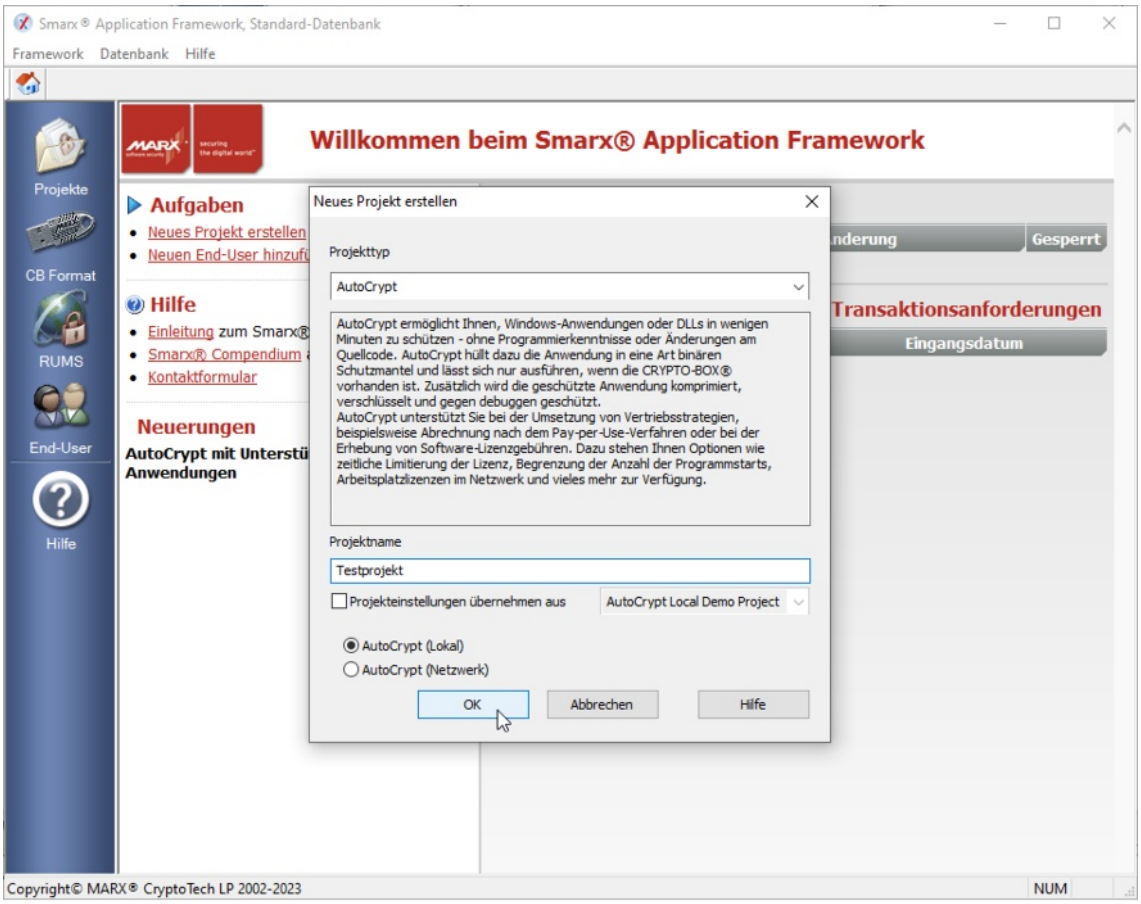
Starten Sie das Smarx Application Framework (siehe Abschnitt *3.1*). Im Hauptbildschirm können Sie ein neues Projekt erstellen oder ein vorhandenes zur weiteren Bearbeitung öffnen. Wenn Sie mit einem vorhandenen Projekt arbeiten (bzw. eines der Demoprojekte aus AutoCrypt evaluieren) wollen, klicken Sie auf das Register „Projekte” links in der Navigationsleiste, und wählen Sie das gewünschte Projekt aus.

Andernfalls klicken Sie auf den Button „Neues Projekt erstellen”, um ein neues Projekt anzulegen.

Geben Sie einen Projektnamen ein. AutoCrypt-Projekte können entweder lokal oder Netzwerk-basierend sein. Bei lokalen Projekten werden die Anwendungen über die an den lokalen PC angeschlossene CRYPTO-BOX geschützt. Bei Netzwerkprojekten sind die Anwendungen über die an den Server angeschlossene CRYPTO-BOX geschützt, Sie bestimmen dabei wie oft die Anwendung im Netzwerk ausgeführt werden darf. Wählen Sie das passende Verfahren: entweder „AutoCrypt (Lokal)“ für lokalen Schutz oder „AutoCrypt (Netzwerk)“ bei reinen Netzwerkprojekten bzw. gemischten lokalen und Netzwerkprojekten.

Über die Option „Projekteinstellungen übernehmen aus“ erzeugen Sie eine unabhängige Kopie eines vorhandenen Projektes, in die alle Anwendungen, Datenobjekte, Projekt- und Anwendungseinstellungen des Originalprojekts kopiert werden. Das neue Projekt ist vom gleichen Typ wie das Ausgangsprojekt (lokal bzw. Netzwerk).

Weitere Informationen zur Verwendung der CRYPTO-BOX im Netzwerk und zur Konfiguration des Netzwerkservers finden Sie im White Paper „Netzwerklizenzierung“ auf unserer Webseite.



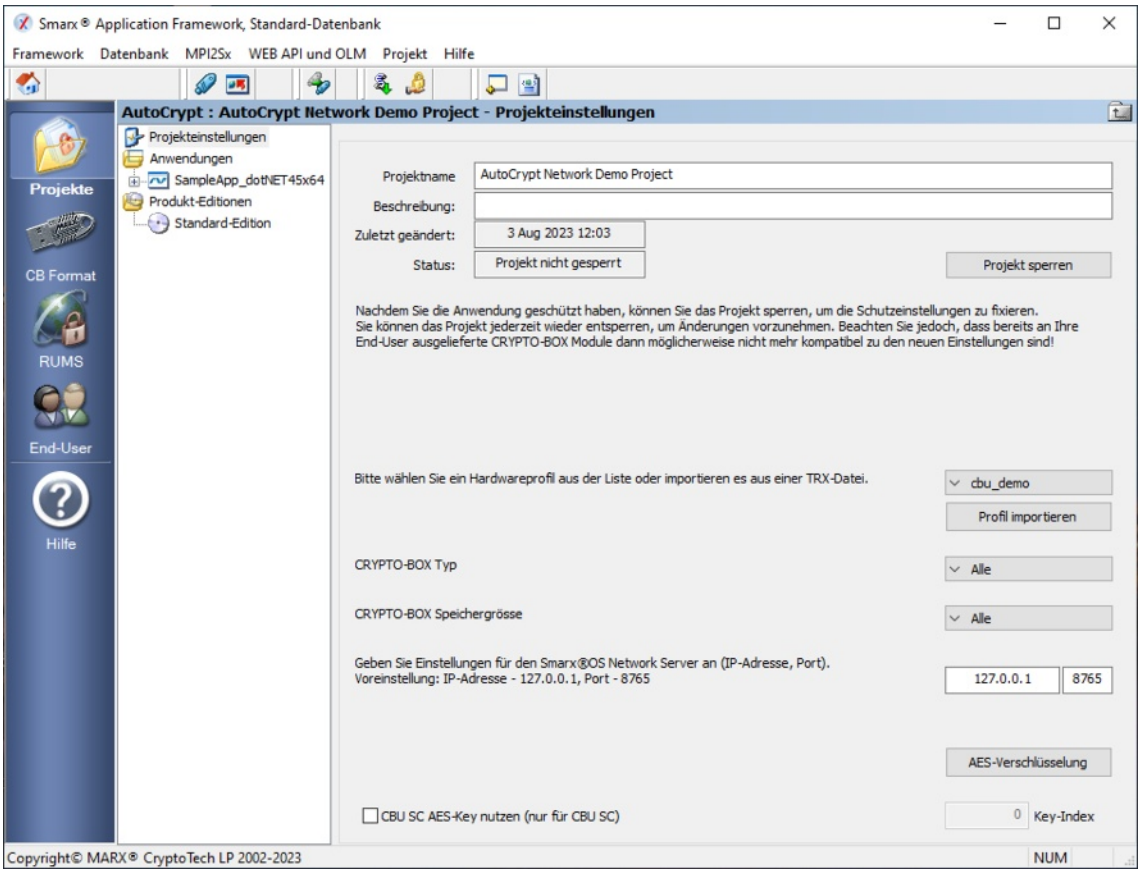
Klicken Sie im Anschluss auf „OK“, damit Sie die Projekteinstellungen anpassen können.

3.3.3. Allgemeine Projekteinstellungen

Mit dem Menüpunkt „Projekteinstellungen“ (im mittlerem Fenster) stellen Sie die Optionen für das

ausgewählte Projekt ein.

Hier können Sie zum Beispiel den Projektnamen und die Beschreibung eingeben oder verändern. Außerdem können Sie das Projekt sperren, so dass keine Änderungen erlaubt sind. Umgekehrt können Sie hier die Sperrung auch wieder aufheben, um die Einstellungen anzupassen. Beachten Sie jedoch, dass bei nachträglichen Änderungen am Projekt ein Remote Update von Lizenzierungsoptionen bei bereits ausgelieferten CRYPTO-BOX Modulen eventuell nicht möglich ist, falls die Projekteinstellungen nicht mehr mit der CRYPTO-BOX-Formatierung übereinstimmen!



Im unteren Teil des Fensters wählen Sie das Hardwareprofil der CRYPTO-BOX für das Projekt aus. Das Hardwareprofil enthält die Zugriffscodes, die die geschützte Anwendung benötigt, um auf die CRYPTO-BOX zugreifen zu können. Wählen Sie das Profil „cbu_demo“ aus, wenn Sie das Evaluation Kit nutzen. Haben Sie bereits kundenspezifische CRYPTO-BOX Module gekauft, verwenden Sie das Hardwareprofil (TRX-Datei), welches Ihrer ersten CRYPTO-BOX Lieferung beiliegt. Klicken Sie auf „Profil importieren“, um Ihre kundenspezifische TRX-Datei zu laden.

Weitere Details zur Handhabung des CRYPTO-BOX Hardwareprofils finden Sie in dem White Paper "TRX Datei" auf unserer Webseite.

Darunter können Sie den CRYPTO-BOX Typ und die Speichergröße festlegen. Diese Einstellungen sind optional: wenn Sie die Standardeinstellungen lassen, erkennt SxAF den CRYPTO-BOX Typ automatisch.

Bei einem Netzwerkprojekt können Sie darunter die Einstellungen zum Netzwerkserver angeben (IP-Adresse und Port); die voreingestellte IP-Adresse lautet „127.0.0.1“, der Port ist 8765. Anstelle der IPv4-Adresse können Sie auch eine IPv6-Adresse oder den zugehörigen Computernamen angeben (zum Beispiel „PC-517“). Falls sich die Servereinstellungen später ändern, lassen sich diese später wieder zurücksetzen bzw. anpassen: Wenn der Server an der angegebenen IP-Adresse nicht gefunden wird, öffnet die geschützte

Anwendung automatisch einen Dialog, in dem die Servereinstellungen abgefragt werden.

Über die Schaltfläche „AES-Verschlüsselung“ können Sie die Werte für den AES/Rijndael-Schlüssel und den Initialisierungsvektor definieren, die zur Verschlüsselung der Anwendung verwendet werden.

Alle geschützten Anwendungen werden automatisch komprimiert und verschlüsselt. Zur Verschlüsselung wird der AES Private Key der CRYPTO-BOX genutzt. Alle geschützten Anwendungen eines Projekts sind mit demselben AES Private Key verschlüsselt.

Mit der CRYPTO-BOX SC ist es möglich, mehrere Projekte mit verschiedenen AES Keys pro CRYPTO-BOX anzulegen. Aktivieren Sie dazu die Checkbox "CBU SC AES-Key nutzen". Mit dem Key-Index legen Sie fest, welcher Schlüssel genutzt werden soll.

WICHTIGER HINWEIS:
Jedes AutoCrypt-Projekt kann einen individuellen AES-Key nutzen. Beachten Sie jedoch: wenn eine CRYPTO-BOX für Projekt 1 formatiert wurde, kann sie nicht für Projekt 2 verwendet werden und umgekehrt, wenn die Projekte unterschiedliche AES-Keys haben. Wenn sie also mehrere (AutoCrypt) Projekte mit einer CRYPTO-BOX nutzen wollen, stellen Sie unbedingt sicher dass sie dieselben AES-Key-Werte für alle Projekte eingestellt haben!
Alternativ können Sie mehrere Anwendungen innerhalb eines Projekts anlegen und schützen, diese nutzen dann automatisch denselben AES-Key (siehe auch Abschnitt *3.3.4*).
Eine Ausnahme ist die CRYPTO-BOX SC: hier können Sie für jedes Projekt einen eigenen AES-Key definieren. Aktivieren Sie dazu die Checkbox "CBU SC AES-Key nutzen".

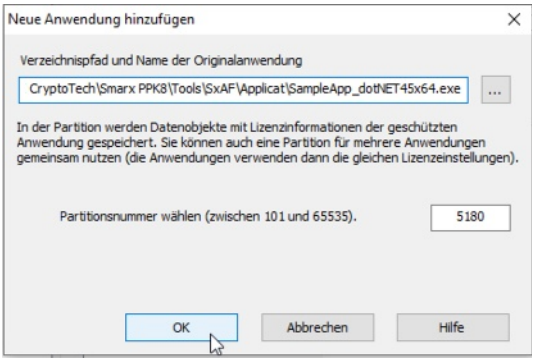
3.3.4. Anwendungen zum Projekt hinzufügen

Hier können Sie Anwendungen zu einem Projekt hinzufügen, sie entfernen oder editieren. Um das Projekt um eine neue Anwendung zu erweitern, klicken Sie auf „Anwendung hinzufügen“. Wählen Sie die Programmdatei (Dateinamen und Pfadname erforderlich) für die zu schützende Anwendung; es kann sich dabei um eine Windows EXE-, EXE.NET- oder DLL-Datei handeln (64 oder 32 Bit). Zu Testzwecken können Sie die mitgelieferten Demo-Anwendungen und DLLs nutzen. Diese finden Sie unter „\MARX Software Security\SmarxOS PPK\Tools\SxAF\ Applicat“.

Dann geben Sie die Nummer der CRYPTO-BOX-Partition an, in der die Schutzeinstellungen für die Anwendung (die Datenobjekte) gespeichert werden sollen. Die Nummer muss zwischen 101 und 65535 liegen.

Ein Projekt kann mehrere Anwendungen umfassen (EXE- bzw. DLL-Dateien), die mit einer CRYPTO-BOX geschützt werden. Die Lizenzoptionen für jede Anwendung werden in einer dedizierten Partition abgelegt, die für die jeweilige Anwendung eingerichtet wird. Die entsprechenden Partitionsnummern können Sie selbst festlegen (siehe oben). Die maximal mögliche Anzahl von Partitionen in der CRYPTO-BOX beträgt 32. Falls das nicht reicht, kann eine Partition von mehreren Anwendungen genutzt werden.

Mit der Option „Bestehende Partition nutzen“ können mehrere Anwendungen des aktuellen Projekts ein und dieselbe Partition gemeinsam nutzen und haben dann auch dieselben Schutz- und Lizenzierungsoptionen. Diese Option wird nur dann angeboten, wenn bereits eine Anwendung im Projekt vorhanden ist (alternativ können Sie auch die Update-Funktion verwenden, siehe Abschnitt *3.3.11*). Falls Sie verschiedene Datenobjekte und Schutzeinstellungen für Ihre Anwendungen definieren wollen, wählen Sie diese Option nicht und geben stattdessen eine neue Partitionsnummer an.



Beachten Sie die folgenden Hinweise zur gemeinsamen Nutzung von Partitionen:

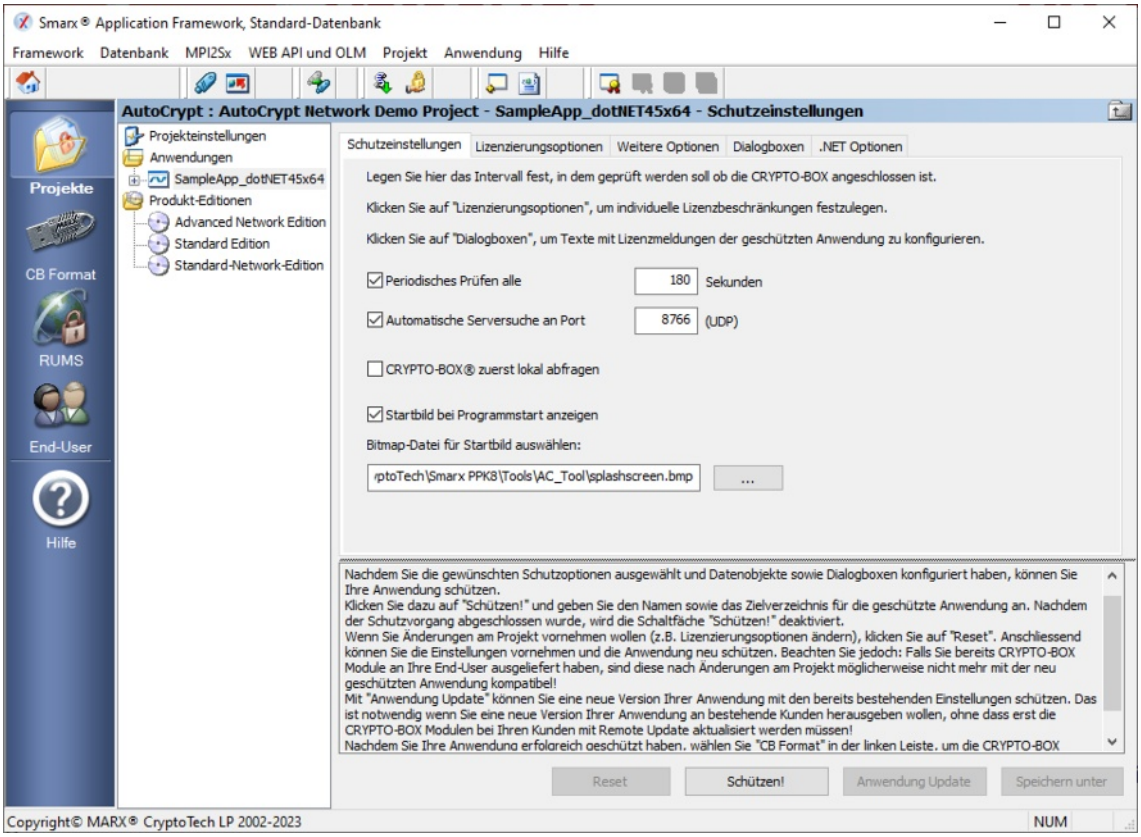
- Gemeinsam genutzte Partitionen können nicht die Datenobjekte „Anwendungs-Checksumme“ und „Anwendungs-Hashwert“ enthalten – und es können keine Partition gemeinsam genutzt werden, bei der diese Datenobjekte bereits vergeben sind.
- Verzichten Sie auf die gemeinsame Nutzung einer Partition bei mehreren Softwaremodulen, wenn diese gleichzeitig ausgeführt werden. Legen Sie stattdessen eine eigene Partition pro Modul fest.
- Wenn Sie etwas an den Datenobjekten einer gemeinsam genutzten Partition ändern, so ändern Sie diese Einstellungen automatisch für alle Anwendungen, die diese Partition nutzen. Beachten Sie das besonders dann, wenn Sie eine der Anwendungen die auf die Partition zugreift bereits an Ihre End-User ausgeliefert haben!
- Folgende Einstellungen können Sie immer individuell für jede Anwendung vornehmen, auch wenn diese eine Partition gemeinsam nutzen: Periodisches Prüfen / Lizenzstatus anzeigen / Lizenzvereinbarung anzeigen, sowie alle Anwendungsdialoge (Fehlermeldungen, Copyright, Texte für Schaltflächen und Links)

Klicken sie auf "OK", um zu den Schutz- und Lizenzierungseinstellungen zu gelangen.

3.3.5. Einstellungen für den Anwendungsschutz

Nachdem Sie die zu schützende Anwendung ausgewählt haben (siehe Abschnitt *3.3.4*), werden Sie automatisch zu den Schutzeinstellungen weitergeleitet. Alternativ klicken Sie links im Navigationsbaum auf die gewünschte Anwendung oder klicken Sie im rechten Fenster doppelt auf die Anwendung. Wechseln Sie jetzt zum Tab "Schutzeinstellungen".

Falls die periodische Prüfung aktiviert ist, wird in den vordefinierten Abständen das Vorhandensein der CRYPTO-BOX überprüft, solange die Anwendung läuft. Falls die CRYPTO-BOX nicht gefunden wird, wird die Anwendung beendet. Der Abstand zwischen den Prüfungen sollte mindestens 120 Sekunden betragen. Es sind auch kürzere Werte möglich; das sollte aber nur dann gemacht werden, wenn es für die Lizenzierung wichtig ist.



Die folgenden Optionen sind nur im Netzwerkmodus sichtbar:

- "Automatische Serversuche" via UDP bedeutet, dass die geschützte Anwendung nach vorhandenen CRYPTO-BOX Servern sucht (Server muss sich im selben Sub-Netz befinden). Die Standardeinstellungen für den UDP-Port ist 8766, Sie können ihn in der Serverkonfiguration ändern (siehe unser White Paper „Netzwerklizenzierung“ für weitere Details zum Netzwerkserver).
- Wenn "CRYPTO-BOX zuerst lokal abfragen" aktiviert ist, prüft die Anwendung zuerst, ob sich eine CRYPTO-BOX lokal am Computer befindet bevor eine Netzwerksuche gestartet wird.

Bei Bedarf können Sie einen Splash-Screen festlegen, der vor dem Start der geschützten Anwendung angezeigt wird. Wählen Sie dazu eine Grafikdatei aus – diese muss im Bitmap-Format (.bmp) vorliegen und darf nicht größer als die zu schützende Anwendung sein.

Sie können beispielsweise die Windows-Anwendung „Paint“ nutzen, um ein beliebiges Bild als Windows Bitmap (BMP) Datei abzuspeichern. Verringern Sie ggf. die Auflösung oder Farbtiefe der Grafikdatei, um die Dateigrösse zu verringern.

Bei .Net 6.0+ Anwendungen wird die Splashscreen-Option nicht unterstützt, die Splashscreen-Einstellungen werden in diesem Fall ignoriert

3.3.6. Lizenzierungsoptionen (Datenobjekte)

Im Tab "Lizenzierungsoptionen" können Sie Datenobjekte hinzufügen; diese können zum Beispiel

Ablaufdatum, Ausführungszähler, und weitere sein. Um ein Datenobjekt hinzuzufügen, aktivieren Sie es durch Klick auf das Auswahlfeld, und legen Sie den gewünschten Wert über den Button "Ändern" fest.

Bei den Datenobjekten haben Sie die Wahl zwischen „CDO“ (Crypted DataObject = verschlüsseltes Datenobjekt) und unverschlüsseltem Datenobjekt („CDO“ deaktiviert). Dies bietet einen zusätzlichen Schutz gegen Manipulationen. Falls Sie verschlüsselte Datenobjekte zusätzlich per API abfragen wollen, beachten Sie die entsprechenden Hinweise in den Readme-Dateien und unseren Beispielcode, da nicht alle API-Bibliotheken CDO unterstützen, z.B. welche für ältere oder exotische Entwicklungsumgebungen. Bei weiteren Fragen wenden Sie sich an unseren technischen Support.

Um ein Datenobjekt zu löschen, klicken Sie nochmal auf das Auswahlfeld und beantworten Sie die Frage nach dem Löschen des Datenobjekts mit "Ja". Folgende Datenobjekte stehen zur Verfügung:

Ablaufdatum und -zeit	Genaues Ablaufdatum und Uhrzeit, nach der die geschützte Anwendung nicht mehr gestartet werden kann, z.B. 31. Dezember 2025 18:00:00
Ablaufdatum	Festes Ablaufdatum, z.B. 31. Dezember 2025. Dieser Datenobjekttyp ist veraltet und nur aus Kompatibilitätsgründen enthalten, bitte nutzen Sie stattdessen das Datenobjekt "Ablaufdatum und -zeit"
Ablaufdatum relativ	Das "Ablaufdatum relativ" legt fest, wieviele Tage die Anwendung ausgeführt werden darf, beginnend vom **ersten Start der Anwendung**
Tage bis Lizenzablauf	"Tage bis Lizenzablauf" legt fest, wieviele Tage die Anwendung ausgeführt werden darf, beginnend vom **Tag der Formatierung der CRYPTO-BOX mit CB Format**
Zeit bis Lizenzablauf	Zeit (in Sekunden), die die geschützte Anwendung genutzt werden darf
Ausführungszähler	Anzahl der Starts der Anwendung
Netzwerklizenz	Bestimmt wie oft die geschützte Anwendung im Netzwerk ausgeführt werden darf.

3.3.7. Weitere Optionen

Der Tab "Weitere Optionen" bietet folgende zusätzliche Schutzoptionen.

Passwort

Hier können Sie ein Passwort festlegen, welches bei jedem Start der Anwendung abgefragt wird.

Checksumme

Dieses Datenobjekt prüft eine Checksumme ab, die über die geschützte Anwendung gebildet wurde. So kann beispielsweise festgestellt werden, ob die Anwendung manipuliert wurde. Die Anwendung wird dazu mit der in der CRYPTO-BOX gespeicherten Checksumme verglichen.

Anwendungs-Hashwert

Hier wird ein Hashwert über den Name der Anwendung gebildet, damit diese nicht nachträglich umbenannt werden kann. Die Anwendung wird dazu mit dem in der CRYPTO-BOX gespeicherten Hashwert verglichen.

WICHTIG:
Gemeinsam genutzte Partitionen (siehe Abschnitt *3.3.4)* können nicht die Datenobjekte „Anwendungs-Checksumme“ und „Anwendungs-Hashwert“ enthalten – und es können keine Partition gemeinsam genutzt werden, bei der diese Datenobjekte bereits vergeben sind!
Setzen Sie diese Datenobjekte ebenfalls nicht ein, wenn Sie vorhaben die Anwendung später zu aktualisieren (siehe Abschnitt *3.3.11*), da die neue Anwendung einen anderen Hashwert hat (als den in der CRYPTO-BOX gespeicherten)!

Signatur (GUID)
Diese Option ist für Softwareentwickler: Sie erlaubt das speichern eines individuellen Datenblocks bis zu 16 Byte Länge (zum Beispiel mit kundenspezifischen Daten) in der CRYPTO-BOX. Diese Daten können von der geschützten Anwendung ausgelesen werden – mit minimalem Aufwand!

Vorteil dieser Lösung: es sind keine Kenntnisse des CRYPTO-BOX API notwendig! Sie brauchen lediglich den Code aus unserem Beispielprogramm in den Quellcode Ihrer Anwendung zu implementieren.

Das Beispielprogramm und eine Readme-Datei mit Erläuterungen finden Sie im PPK:

[Smarx OS PPK Hauptverzeichnis]\SmarxOS-Samples\ReadMemoryBySignature

Das ganze funktioniert so: Nachdem die Prüfung der CRYPTO-BOX erfolgreich war, liest die mit AutoCrypt geschützte Anwendung die Daten aus der CRYPTO-BOX, entschlüsselt sie und schreibt sie in einen Speicherpuffer, der mit einer individuellen Signatur versehen ist. Dieser Speicher kann durch den von Ihnen implementierten Code (siehe oben) ausgelesen und ausgewertet werden.

3.3.8. Dialoge definieren

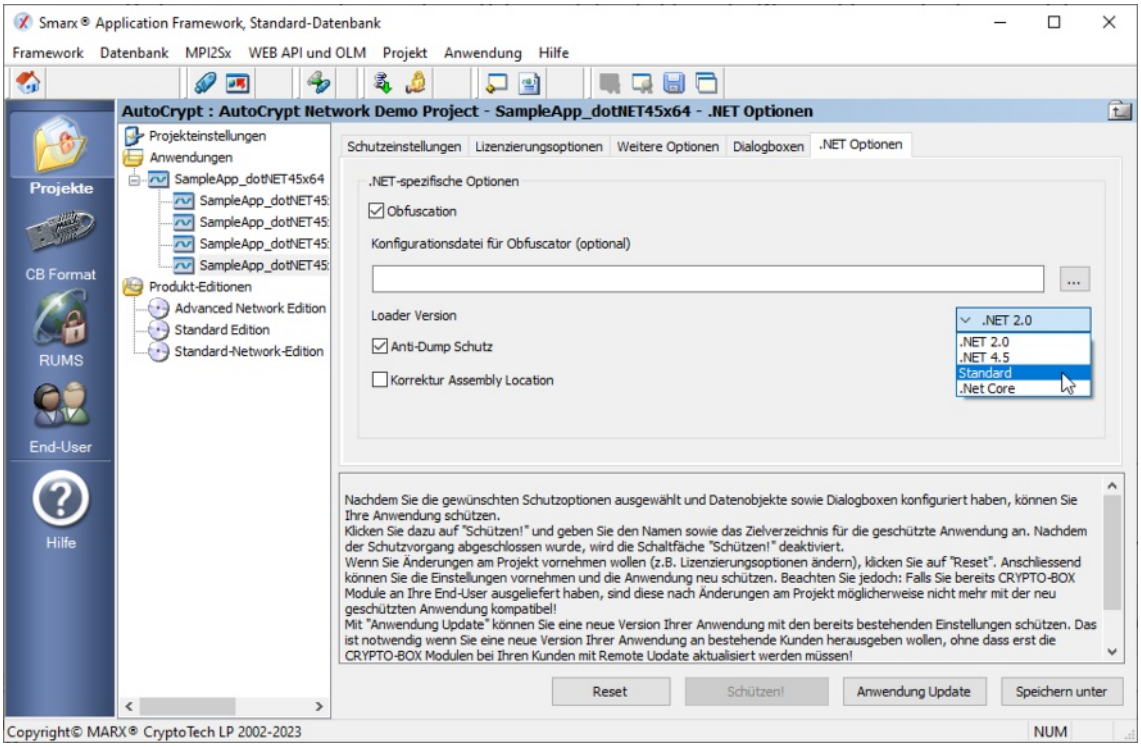
Für die geschützte Anwendung können Sie Dialogboxen individuell konfigurieren, die unter bestimmten Bedingungen ausgegeben werden, z.B. Lizenzstatus, Fehler- oder Warnmeldungen bei Lizenzverletzung, Meldung bei Lizenzablauf usw. Klicken Sie dazu auf das Register „Dialogboxen“, wählen die Meldung aus der Liste aus und klicken auf „Dialogbox ändern“. Geben Sie dann den Dialogtitel und den Text ein, der erscheinen soll. Möchten Sie, dass bei einer bestimmten Bedingung keine Meldung angezeigt wird, lassen Sie die entsprechende Titelzeile und den Dialog leer.

Falls die Option „Lizenzvereinbarung anzeigen“ aktiviert ist, wird vor dem Anwendungsstart der von Ihnen vorgegebene Text mit Lizenzinformationen ausgegeben.

Falls die Option „Lizenzstatus anzeigen“ aktiviert ist, wird vor dem Start der Anwendung ein Hinweis eingeblendet wie oft bzw. wie viele Tage die Anwendung noch ausgeführt werden.

3.3.9. .Net-Optionen

Handelt es sich bei Ihrer zu schützenden Anwendung um eine .NET-Anwendung, dann finden haben Sie bei dem Schutz- und Lizenzierungseinstellungen noch einen Punkt „.NET Optionen“ mit weiteren Einstellungen:



- Mit „Obfuscation“ bietet AutoCrypt eine automatische Obfuscation der .Net-Anwendung an. Dazu wird im Hintergrund das Open Source Programm „Obfuscar“ genutzt. Weitere Details dazu finden Sie auf der Obfuscar-Webseite.
- Die Option „Anti-Dump Schutz“ erschwert das Dumpen von .Net-Anwendungen und sollte daher nur deaktiviert werden, falls die geschützte Anwendung nicht startet
- Die Option „Korrektur Assembly Location“ behebt das Problem, dass .Net-Anwendungen, die „Location Property“ nutzen um den Pfad der ausführenden Assembly zu erhalten - z.B. mit Assembly.GetExecutingAssembly() - nach dem Schutz von AutoCrypt nicht starten.
- Die Option „Loader version“ ermöglicht es, verschiedene Loader für .Net-Anwendungen auszuprobieren, beispielsweise wenn bei der Standardeinstellung die geschützte Anwendung nicht startet oder von Antivirus-Programmen irrtümlich als Schadsoftware erkannt wird. Folgende Optionen sind möglich:
  - STANDARD (Standardeinstellung) – Automatische Erkennung: .NET_CORE für .Net 6.0+ Anwendungen (Bedingung: .exe, .dll und .runtimeconfig.json mit dem selben Name befinden sich im Verzeichnis der Originalanwendung), DOTNET_45 für .NET 4.x Anwendungen und DOTNET_20 für alle anderen Anwendungen
  - DOTNET_20 – forciert die Nutzung unseres älteren Loaders, der für .Net 2.0 Anwendungen entwickelt wurde (führt möglicherweise zu Inkompatibilitäten mit einigen .Net 4.x Anwendungen)
  - DOTNET_45 – Zur Nutzung mit Anwendungen, die mit .Net 4.x erstellt wurden
  - DOTNET_Core – forciert die Nutzung des Loaders für .Net Core Anwendungen (.NET 6.0 oder höher)
- Die Option „Console Application“ ist nur verfügbar, wenn der DOTNET_Core Loader ausgewählt wurde und ist bei Schutz von .Net-Kommandozeilenanwendungen zu aktivieren (Anwendungen ohne grafische Oberfläche)

Wichtige Hinweise zu .Net 6.0+ (.Net Core) Anwendungen:

1. Geben Sie bei .Net 6.0+ Anwendungen immer als Originalanwendung (siehe 2.2.8) die entsprechende .dll-Datei an, nicht die .exe, da sonst die geschützet Anwenudng nicht startet! Die .exe ist bei .Net 6.0+ nur ein Loader, der die eigentliche Anwendung in der .dll-Datei lädt. AutoCrypt schützt die .dll und ersetzt die .exe mit einem eigenen Ladeprogramm.
2. Bei .Net 6.0+ Anwendungen muss die Zieldatei unbedingt denselben Namen haben wie die Originaldatei (siehe 2.2.8), sonst startet die geschützte Anwendung nicht!
3. .Net 6.0+ Anwendungen können Sie als Zielordner auch denselben Ordner wie die Originalanwendung angeben. In dem Fall ersetzt AutoCrypt die Originalanwendung mit der geschützten Dateien und verschiebt die Originaldateien in den Ordner _backup. Wenn Sie einen anderen Zielpfad wählen, vergessen Sie nicht immer die zugehörigen Runtime-Konfigurationsdateien in das Zielverzeichnis zu kopieren (.json-Dateien), sonst startet die geschützte Anwendung nicht!
4. .Net 6.0+ Anwendungen können nur mit der Option STANDARD oder DOTNET_Core geschützt werden, bei allen anderen Einstellungen startet die geschützte Anwendung nicht!
5. AutoCrypt kann .Net 5.0 Anwendungen nicht ohne weiteres schützen! Entweder Sie steigen auf eine neuere .Net-Version (6.0 oder höher) um, oder nutzen den in der AC_Tool Readme-Datei beschriebenen Workaround, um die .Net-Version in Ihrer Runtime-Konfigurationsdatei anzupassen. Siehe dazu Kapitel 4.1.

3.3.10. Produkt-Editionen

Für Ihre Vertriebs- und Marketingstrategie kann es interessant sein, dass Sie verschiedene Lizenzierungsoptionen für ein und dasselbe Produkt definieren möchten. Dazu können Sie verschiedene Editionen festlegen.

Ein paar Beispiele:

- Advanced Edition: Nutzungsdauer 1 Jahr
- Platinum Edition: unlimitierte Nutzungsdauer

oder

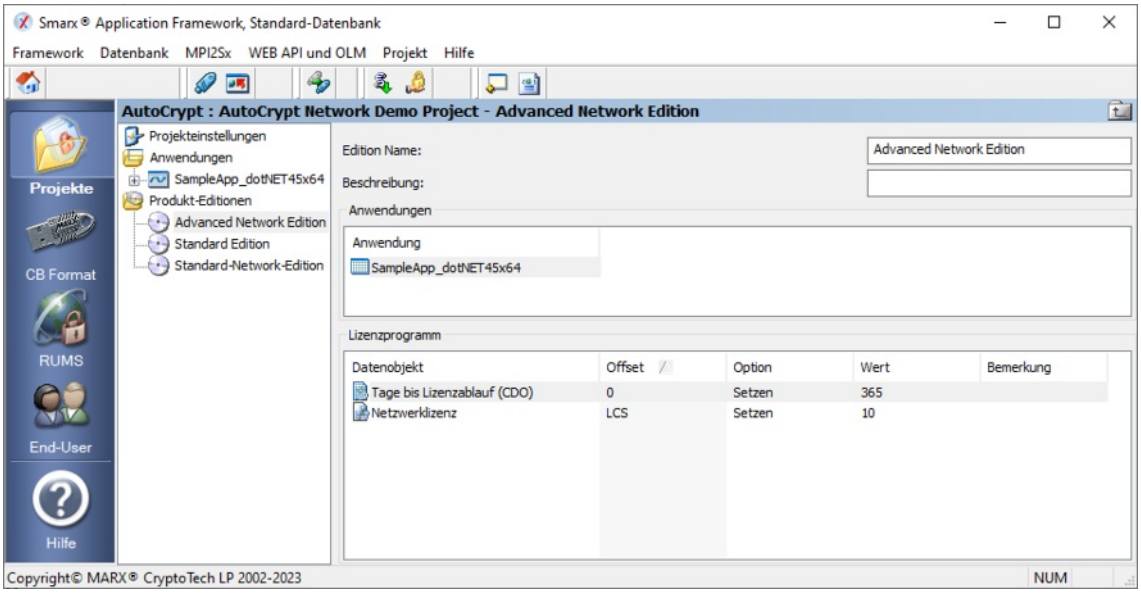
- Standard Network Edition: 5 Netzwerklizenzen für eine Nutzungsdauer von 6 Monaten
- Advanced Network Edition: 10 Netzwerklizenzen für eine Nutzungsdauer von einem Jahr
- Platinum Network Edition: 10 Netzwerklizenzen, unlimitierte Nutzungsdauer

usw.

Dazu brauchen sie lediglich die gewünschten Produkt-Editionen für Ihr Projekt festzulegen und die CRYPTO-BOX für den entsprechenden Kunden unter Angabe dieser Edition mit CB Format zu konfigurieren (siehe Abschnitt *3.4.1*). Standardmäßig ist nur eine Edition (Standard-Edition) angelegt.

Um eine neue Produkt-Edition zu definieren, klicken Sie auf den Eintrag "Produkt-Editionen" im mittleren Navigationsbaum. Wählen Sie "Neue Edition" um eine Edition anzulegen oder doppelklicken Sie auf eine bestehende Edition um deren Einstellungen zu ändern.

Sie können in einer Produkt-Edition nur Lizenzierungsoptionen ändern, die bereits in Ihrem Projekt vorhanden sind. Stellen sie daher sicher, dass Sie die gewünschten Lizenzierungsoptionen in Ihrem Projekt bereits definiert haben (siehe Abschnitt *3.3.6*), bevor Sie die Editionen anlegen.



3.3.11. Anwendung schützen

Um den Schutzvorgang für die Anwendung(en) zu starten, wählen Sie in der Baumstruktur die Anwendung aus und klicken Sie auf den Button "Schützen!“.

Daraufhin werden Sie gefragt, wo die geschützte Anwendung und die zugehörige DLL-Datei gespeichert werden soll. Geben Sie ein Verzeichnis an und klicken Sie auf "Speichern".

AutoCrypt komprimiert und verschlüsselt die geschützte Anwendung, der AES Rijndael Private Key der CRYPTO-BOX wird zur Ver- und Entschlüsselung genutzt (siehe Abschnitt *3.3.3*). Außerdem wird die Anwendung gegen Debuggen geschützt.

Sollte die geschützte Anwendung nicht lauffähig sein, nehmen Sie mit uns Kontakt auf – in vielen Fällen können wir AutoCrypt anpassen.

Falls die Anwendung bereits geschützt war, können Sie sie nur erneut schützen, wenn Sie vorher auf „Reset“ klicken. Mit „Speichern unter“ können Sie in Multi-User-Umgebungen die geschützte Anwendung (wenn diese von einem anderen Benutzer geschützt wurde) aus der Datenbank holen und auf Ihrem PC speichern. Weitere Informationen zum optional erhältlichen Multi-User-Einsatz des Smarx Application Frameworks erhalten Sie bei unserem Support.

Alle Informationen zu der geschützten Anwendung - und auch die geschützte Anwendung selbst - werden in der Datenbank gespeichert.

Die geschützte Anwendung können Sie nur zusammen mit einer CRYPTO-BOX einsetzen, die mit den passenden Lizenzdaten für die Anwendung konfiguriert (formatiert) wurde! Nutzen sie dazu die Option „CRYPTO-BOX Format“ im SxAF (siehe Abschnitt *3.4.1*).

Falls erforderlich, lassen sich die Lizenzierungsoptionen (zum Beispiel Ablaufdatum, Zähler oder Netzwerklizenzen) später über das Remote Update Management System (RUMS) aktualisieren.

Sie können den Schutz Ihrer Anwendungen mit der Kommandozeilenversion von AutoCrypt (AC_Tool.exe) automatisieren. AC_Tool.exe lässt sich über Kommandozeilenparameter steuern. Weitere Infos dazu finden Sie im Abschnitt *4.1*.

3.3.12. Neue Version der geschützten Anwendung verteilen

Wenn Sie Ihre geschützte Anwendung bereits an die Kunden ausgeliefert haben und jetzt ein Update verteilen möchten, können Sie die neue Version schützen und an Ihre Endanwender verteilen, ohne dass ein Update der CRYPTO-BOX notwendig ist! Öffnen Sie dazu das AutoCrypt-Projekt und rufen im Menü „Anwendung“ den Befehl „Update“ auf oder klicken auf das entsprechende Icon in der Symbolleiste. Wählen Sie dann die neue Anwendung aus und klicken Sie auf "OK". Anschließend klicken Sie auf "Schützen!" und speichern die geschützte Anwendung.

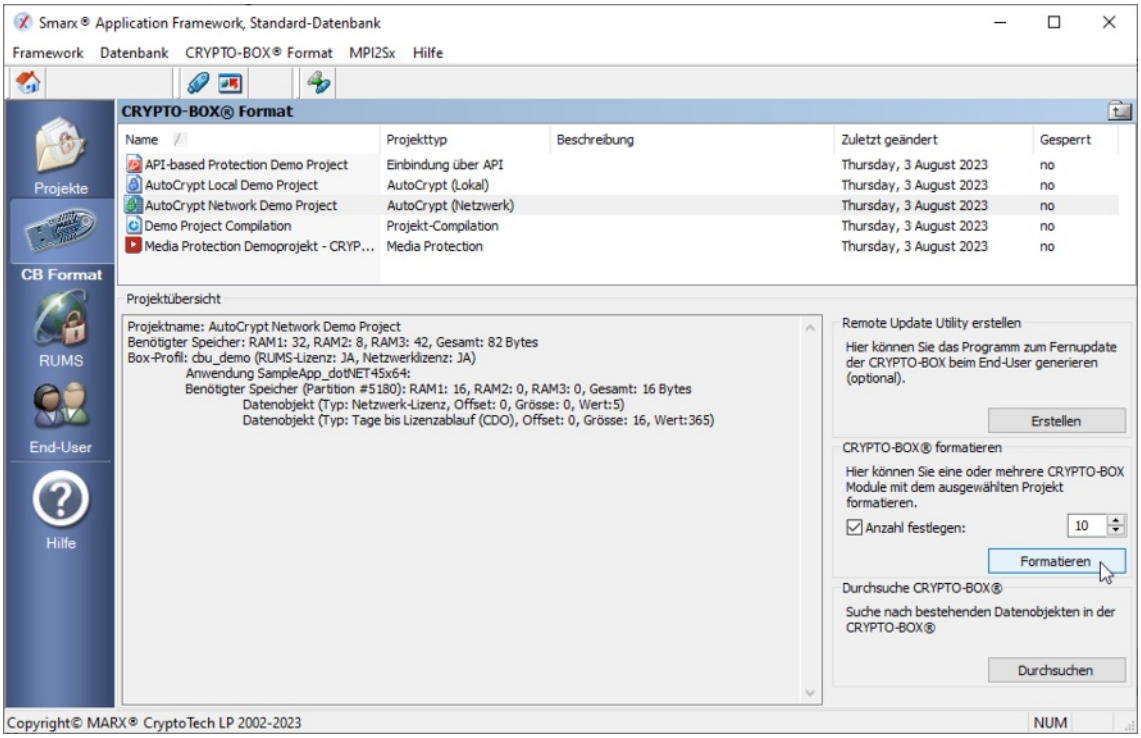
3.4. Konfiguration der CRYPTO-BOX®

3.4.1. CRYPTO-BOX® Format (CB Format)

Mit CRYPTO-BOX Format (CB Format) konfigurieren Sie die CRYPTO-BOX Module entsprechend Ihren Projekteinstellungen. Dabei werden Partitionseinstellungen und Lizenzinformationen, die Sie in Ihrem Projekt festgelegt haben in die CRYPTO-BOX geschrieben.

3.4.2. Projekt auswählen

Klicken Sie im SxAF ganz links in der vertikalen Leiste auf den Button “CB Format”. Wählen Sie oben im Fenster das Projekt aus, für das Sie die CRYPTO-BOX konfigurieren möchten. Im unteren Teil wird nochmal eine Zusammenfassung der Projekteinstellungen angezeigt.



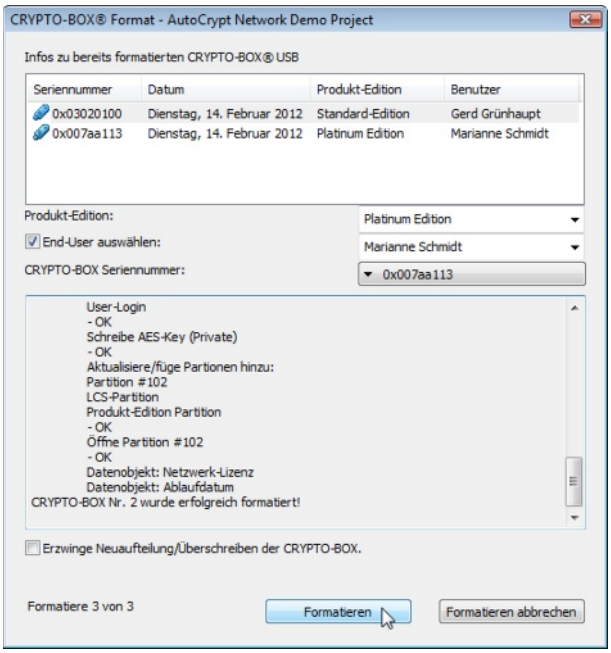
3.4.3. CRYPTO-BOX® formatieren

Legen sie unten rechts fest, wie viele CRYPTO-BOX Module sie für dieses Projekt formatieren wollen. Schließen Sie jetzt die erste CRYPTO-BOX an und klicken Sie auf "Formatieren". Im neuen Fenster sehen Sie die folgenden Optionen.

- **Infos zu bereits formatierten CRYPTO-BOX** - zeigt eine Liste der bereits formatierten CRYPTO-BOX, inkl. Seriennummer, gewählte Produkt-Edition und zugewiesener Benutzer (End-User)
- **Produkt-Edition** - wählen sie die gewünschte Produkt-Edition (siehe Abschnitt *3.3.10* für weitere Details zu Produkt-Editionen)
- **End-User auswählen** - aktivieren sie diese Checkbox, wenn Sie die formatierte CRYPTO-BOX einem bestimmten End-User zuweisen wollen (siehe Abschnitt *3.7* für weitere Details zum End-User Management). Dies ermöglicht es Ihnen, den End-user später bei Remote Updates anhand seiner CRYPTO-BOX zu identifizieren. Wenn Sie keine End-User angelegt haben, ist dieses Feld deaktiviert.
- **CRYPTO-BOX Seriennummer** - zeigt die Seriennummer der aktuell angeschlossenen CRYPTO-BOX an.
- **Erzwinge Neuaufteilung/Überschreiben der CRYPTO-BOX** - damit werden alle evtl. bestehenden Partitionen auf der CRYPTO-BOX gelöscht und nur die im Projekt angegebene angelegt.

Klicken Sie danach auf „Nächste formatieren“, um die Formatierung der ersten CRYPTO-BOX zu beginnen. Der Status des Formatiervorgangs wird in einem Fenster angezeigt. Sobald alle CRYPTO-BOX Module formatiert wurden, klicken Sie auf „Fertig“ oder auf "Formatieren abbrechen" (wenn sie weniger als die angegebene Anzahl an Modulen formatieren wollen), um das Fenster zu schließen.

Wenn Sie während der Formatierung eine Fehlermeldung erhalten, dass das Login auf die CRYPTO-BOX fehlgeschlagen ist, überprüfen Sie bitte ob Sie das zu Ihrer CRYPTO-BOX passende Hardwareprofil (TRX-Datei) im Projekt angegeben haben. Weitere Details dazu finden Sie im Abschnitt *3.3.3*.



Mit dem Kommandozeilentool SmrxProg.exe können Sie die Formatierung der CRYPTO-BOX über Skripte oder von anderen Anwendungen heraus steuern. Weitere Details dazu finden Sie im Abschnitt *4.2*.

Ändern Sie die Projekteinstellungen nach dem Formatieren der CRYPTO-BOX Module nicht mehr. Sonst können Sie die Lizenzeinstellungen möglicherweise nicht mehr mit RUMS aktualisieren!

3.5. XML-Skript für Kommandozeilentools erzeugen

Falls Sie den Anwendungsschutz und die Formatierung der CRYPTO-BOX in Ihre eigene Administrations- bzw. Distributionsstrategie integrieren wollen, bietet MARX die Kommandozeilentools AC_Tool und SmrxProg an.

AC_Tool (dient zum Schutz von Anwendungen, siehe Abschnitt *4.1*) und SmrxProg (zum Konfigurieren der CRYPTO-BOX-Module, siehe Abschnitt *4.2*) sind Konsolenanwendungen, die Sie über Befehlszeilenparameter steuern. Diese Tools lassen sich von anderen Anwendungen aufrufen und über Skripte steuern. Auf diese Weise ist ein hoher Grad an Automatisierung möglich.

Öffnen Sie das Projekt, das Sie exportieren wollen in SxAF und wählen im Menü "Projekt" den Eintrag "Erstelle XML-Skript für AC_Tool und SmrxProg" aus. Wählen Sie jetzt die dann die zu schützende Anwendung im Projekt aus, die Sie exportieren wollen, und geben den Ordner an, in dem die Anwendung gespeichert werden soll. Dann klicken Sie auf „Exportieren" und wählen einen Ordner für die XML-Datei aus. Das SxAF erstellt nun das XML-Skript und passt dabei automatisch den Pfad zur Anwendung an.

3.6. Remote Update Utility erstellen

Wenn Sie spätere Updates der Lizenzinformationen in der CRYPTO-BOX ermöglichen wollen, erstellen Sie zusätzlich das Remote Update Tool. Dieses Programm können Sie zusammen mit der CRYPTO-BOX an den Endanwender ausliefern.

Klicken Sie im SxAF ganz links in der vertikalen Leiste auf den Button "CB Format". Wählen Sie oben im Fenster das Projekt aus, für das Sie die CRYPTO-BOX konfigurieren möchten. Im unteren Teil wird nochmal eine Zusammenfassung der Projekteinstellungen angezeigt (siehe Abbildung in Abschnitt *3.4.2)*. Klicken Sie rechts unten auf „Erstellen" und geben Sie den Ordner an, in den das Remote Update Utility extrahiert werden soll, sowie den Dateinamen.

Eine detaillierte Beschreibung zu Remote Update finden Sie in den "*RUMS (Remote Update) Application Notes*", oder im *Smarx Compendium*, Kapitel 6.

Um das RUpdate Utility zu erstellen, wird eine RUMS-Lizenz benötigt (optional erhältlich). Besuchen Sie www.marx.com → Shop → Lösungen → RUMS für weitere Details und Preise, oder wenden Sie sich direkt an MARX. Ohne gültige RUMS-Lizenz ist der Button „Erstellen" ausgegraut.

3.7. End-User Management

Mit Hilfe des Smarx Application Framework könen Sie oder Ihr Vertrieb formatierte CRYPTO-BOX Module bestimmten End-Usern zuweisen. Die Zuweisung erfolgt während der Formatierung der CRYPTO-BOX (siehe Abschnitt *3.4.3*). Das erfordert allerdings, dass die End-User bereits in der Datenbank definiert sind. Falls Sie End-User-Beschreibungen in die Datenbank aufnehmen wollen, klicken Sie im Hauptbildschirm von SxAF auf der linken Seite auf „End-User".

Damit die End-User beim Formatieren der CRYPTO-BOX ausgewählt bzw. beim Remote-Update identifiziert werden können, reicht es die Namensfelder auszufüllen.

Wenn Sie End-User- und Lizenzierungsinformationen aus Ihrer eigenen Datenbank nutzen wollen, können Sie den Schutz der Anwendungen und die (kundenspezifische) Formatierung der CRYPTO-BOX an Ihr eigenes Vertriebssystem anbinden. Dazu nutzen Sie anstelle des SxAF unsere Kommandozeilentools "AC_Tool" und "SmrxProg". Weitere Details dazu erhalten Sie in Kapitel *4*.

4. Automatisierung mittels Kommandozeilentools

Mit den Kommandozeilentools AC_Tool.exe (zum Schutz von Anwendungen, siehe *4.1*) und SmrxProg.exe (zur Konfiguration der CRYPTO-BOX, siehe *4.2*) können Sie den Schutzvorgang weitgehend automatisieren. Das ist zum Beispiel ideal zur Integration in Ihre eigenen, existierenden Vertriebslösungen oder Datenbanken. Ihr Vertrieb profitiert ebenfalls: auf Knopfdruck kann so automatisch die geschützte Anwendung erzeugt und die dazu passende CRYPTO-BOX konfiguriert werden.

Die Kommandozeilentools sind sowohl im PPK als auch in der „AutoCrypt Wizard Package“ enthalten, siehe Kapitel *1.2* für Details.

4.1. AC_Tool - AutoCrypt Kommandozeilentool

Mit der Kommandozeilenversion von AutoCrypt (AC_Tool.exe) können Sie den Schutz Ihrer Anwendung über Kommandozeilenparameter steuern bzw. automatisieren.

AC_Tool finden Sie hier:

- Wenn Sie das **PPK** installiert haben, finden Sie AC_Tool im Control Center des Protection Kits unter dem Punkt „Treiber und Tools“ → „Kommandozeilentools
- Wenn Sie die **AutoCrypt Wizard Package** nutzen, finden Sie es im Unterordner „\Tools“

Parameter:

AC_Tool.exe <TRX-Datei> <XML-Datei>

Dabei ist:

<TRX-Datei>	CRYPTO-BOX Hardwareprofil, das Sie zusammen mit Ihrer kundenspezifischen CRYPTO-BOX erhalten (bzw. cbu_demo.trx beim Evaluation Kit)
<XML-Datei>	die XML-Datei mit den Schutzeinstellungen für die Anwendung und der Konfiguration für die CRYPTO-BOX; die Datei wird außerdem von SmrxProg.exe zur weiteren Programmierung der CRYPTO-BOX genutzt (siehe dazu die Beispieldatei AC_Test.xml)

Kurze Erläuterung zum Einsatz von AC_Tool:

- Nehmen Sie eine XML-Datei, die im AutoCrypt Wizard (siehe Abschnitt *2.2.1*) oder SxAF (siehe Abschnitt *3.3.1*) exportiert wurde. Oder erzeugen Sie eine angepasste XML-Datei in einem Editor (verwenden Sie z.B. die Dateien AC_Test.xml, AC_Local.xml und AC_Network.xml als Prototyp).
- Ist Ihre Anwendung eine .NET-Anwendung, enthält die Datei AC_Dotnet.xml nützliche Infos zu möglichen Konfigurations-Optionen für .NET-Anwendungen. **Beachten Sie dazu auch Kapitel 4 in der readme.txt in AC_Tool-Ordner!**
- Speichern Sie die TRX-Datei, die im vorhergehenden Schritt erzeugte XML-Datei sowie die Datei AC_Tool.exe im gleichen Ordner.
- Rufen Sie über die Konsole den folgenden Befehl auf: AC_Tool.exe <TRX-Datei> <XML-Datei>
- Die Ergebnisse werden auf der Konsole angezeigt und in die Datei AC_TOOL.LOG ausgegeben.
- Sollten Sie eine Fehlermeldungen erhalten, finden Sie in der beiliegenden Readme-Datei eine Liste der Fehlercodes und ihrer Bedeutung.

4.2. SmrxProg - CRYPTO-BOX® per Kommandozeile formatieren

SmrxProg ist ein Tool zur Formatierung (Programmierung) einer CRYPTO-BOX. Es lässt sich im Gegensatz zu

CRYPTO-BOX Format jedoch über Kommandozeilenparameter steuern und ist daher ideal zur Integration in kundenspezifische Lösungen zur Konfiguration von CRYPTO-BOX Modulen.

SmrxProg unterstützt:

1. Die Programmierung der zur Verschlüsselung verwendeten AES-Schlüssel der CRYPTO-BOX (private und Session-Keys: AES Key/IV);
2. das Erstellen von Partitionen im CRYPTO-BOX Speicher (Partitionsnummern zwischen 101 und 65535);
3. die Programmierung von Datenobjekten und Netzwerklizenzen für bestimmte Partitionen.

SmrxProg finden Sie hier:

- Wenn Sie das **PPK** installiert haben, finden Sie AC_Tool im Control Center des Protection Kits unter dem Punkt „Treiber und Tools“ → „Kommandozeilentools
- Wenn Sie die **AutoCrypt Wizard Package** nutzen, finden Sie es im Unterordner \Tools

Parameter:

SmrxProg.exe <TRX-Datei> <INI-Datei>

oder

SmrxProg.exe <TRX-Datei> <XML-Datei>

Dabei ist:

<TRX-Datei>	CRYPTO-BOX Hardwareprofil, das Sie zusammen mit Ihrer kundenspezifischen CRYPTO-BOX erhalten (bzw. cbu_demo.trx beim Evaluation Kit).
<XML-Datei>	Die XML-Datei mit den Schutzeinstellungen für die Anwendung und der Konfiguration für die CRYPTO-BOX; die Datei wird außerdem von AC_Tool.exe zum automatischen Schutz der Anwendung genutzt (siehe Abschnitt *4.1*).

Kurze Erläuterung zum Einsatz von SmrxProg:

- Nehmen Sie eine XML-Datei, die im AutoCrypt Wizard (siehe Abschnitt *2.2.1*) oder SxAF (siehe Abschnitt *3.3.1*) exportiert wurde. Oder erzeugen Sie eine angepasste XML-Datei in einem Editor (verwenden Sie z.B. die Dateien AC_Test.xml, AC_Local.xml und AC_Network.xml als Prototyp).
- Speichern Sie die TRX-Datei, die im vorhergehenden Schritt erzeugte XML-Datei sowie die Datei SmrxProg.exe file im gleichen Ordner.
- Rufen Sie über die Konsole den folgenden Befehl auf:
- SmrxProg.exe <TRX-Datei> <INI-Datei>
- bzw.
- SmrxProg.exe <TRX-Datei> <XML-Datei>
- Die Ergebnisse werden auf der Konsole angezeigt und in die Datei SMRXPROG.LOG ausgegeben.

Sollten Sie eine Fehlermeldungen erhalten, finden Sie in der beiliegenden Readme-Datei eine Liste der Fehlercodes und ihrer Bedeutung.

Die Readme-Datei enthält auch weitere Informationen zum Aufbau der XML-Datei.

5. Vertrieb Ihrer Software – Treiberinstallation und Netzwerkserver

Nachdem Sie die passende Schutzstrategie ausgewählt haben, Ihre Software geschützt und die CRYPTO-BOX formatiert haben, ist es an der Zeit, Software und Dongles an Ihre Kunden auszuliefern. Dabei ist es wichtig, die Treiber für die CRYPTO-BOX mitzuliefern. MARX stellt dazu das Programm CBUSetup zur Verfügung, das Sie entweder einfach in Ihre Installationsroutine integrieren, oder auch einfach separat beilegen können.

Beim Schutz im Netzwerk muss zusätzlich der Netzwerkserver installiert werden (siehe Abschnitt *5.1.4*).

5.1. CBUSetup: Treiberinstallation für Windows

Mit diesem Setup werden automatische alle benötigten Komponenten installiert, die für den Betrieb der CRYPTO-BOX auf dem PC des Endanwenders erforderlich sind – abhängig vom jeweiligen Windows-Betriebssystem. Der Installer ist ein selbstextrahierendes Programm, das alle zu installierenden Dateien enthält. Er erkennt automatisch das vorhandene Betriebssystem und installiert die entsprechenden Treiber (für Windows 32 und 64 Bit Versionen).

Es werden die CRYPTO-BOX Modelle SC, XS und Versa mit USB-Anschluss unterstützt.

Die jeweils aktuelle Version von CBUSetup.exe erhalten Sie auf www.marx.com.

Wenn Sie die Installation per CBUSetup in Ihre eigene Setup-Routine einbauen wollen, können Sie den so genannten “Quiet-Mode” (Stiller Modus) von CBUSetup nutzen (siehe Abschnitt *5.1.1)*.

5.1.1. Syntax

CBUSetup.exe /?	Zeigt den Hilfebildschirm an.
CBUSetup.exe /Q /CRYPTOKEN	Startet das Setup im "Quiet-Mode" und installiert den Treiber für die CRYPTO-BOX SC, XS und Versa
CBUSetup.exe /Q /CRYPTOKEN /DRIVERONLY -	Startet das Setup im "Quiet-Mode" und installiert nur den Treiber für die CRYPTO-BOX SC, XS und Versa ohne zusätzliche Komponenten (SMRXCOM ActiveX COM Objekt, ist für AutoCrypt nicht notwendig)
CBUSetup.exe /Q /U /CRYPTOKEN	Deinstalliert den Treiber der CRYPTO-BOX USB im "Quiet-Mode"

5.1.2. CBUSetup Exit-Codes

Wie bereits oben erwähnt, können Sie das Setup im „Quiet-Mode“ und im normalen Modus ausführen. Der „Quiet-Mode“ ist dann sinnvoll, wenn Sie CBUSetup in Ihre eigene Installationsroutine integrieren wollen. Durch die Analyse des Exit-Code von CBUSetup kann Ihr Installationsprogramm ermitteln, ob CBUSetup erfolgreich ausgeführt wurde.

CBUSetup liefert folgende Exit-Codes:

Exit-Code	Beschreibung
0	Kein Fehler aufgetreten.
-1	Der Installer konnte das Betriebssystem nicht erkennen.
-2	Abbruch der Installation durch den Benutzer.
-3	Falsche Betriebssystemversion.
-4	Interner Fehler im Setup – bitte wenden Sie sich an Ihren Distributor.
-5	CBUSetup wurde im "Quiet-Mode" gestartet, es wurde jedoch ein falscher Parameter

	angegeben. Starten Sie den Installer mit der Kommandozeilenoption „/?“, um sich über die korrekte Syntax zu informieren.
-6	Der Benutzer hat nicht die erforderliche Berechtigung, um den Treiber zu installieren. Bitte wenden Sie sich an den Systemadministrator.
-7	Der Installer konnte die Registrierung der Gerätetreiber nicht durchführen. Bitte starten Sie den Installer erneut. Falls weiterhin dieser Fehlercode gemeldet wird, nehmen Sie bitte Kontakt mit Ihrem Distributor auf.

5.1.3. CBUSetup als Windows Installer Merge Module

CBUSetup ist alternativ als Windows Installer Merge Module (CBUSetup.msm) verfügbar, welches in bestehende Windows Installer oder InstallShield Setups integriert werden kann. Es hat dieselbe Funktionalität wie CBUSetup.exe (siehe Abschnitt *5.1)*.

Die jeweils aktuelle Version von CBUSetup.msm erhalten Sie auf www.marx.com (MyMARX-Registrierung erforderlich).

5.1.4. Netzwerkserver installieren

Wenn Sie Ihre Anwendung im Netzwerk schützen wollen (siehe auch Abschnitt *3.3.2*), muss auf dem Computer im Netzwerk, an dem die CRYPTO-BOX angeschlossen ist, zusätzlich zu den CRYPTO-BOX Treibern auch der Netzwerkserver installiert werden. Dafür steht unter Windows ein Installationsprogramm für Windows (CBIOS Network Server.msi) zur Verfügung, alternativ ein Merge-Modul (CBIOS Network Server.msm) zur Integration in eigene Setups. Außerdem ist der Server für Linux und macOS erhältlich. Sie finden alle Server-Pakete auf unserer Webseite im Downloadbereich.

Detaillierte Informationen zur Verwendung der CRYPTO-BOX im Netzwerk und zur Konfiguration des Netzwerkservers finden Sie im White Paper „Netzwerklizenzierung“ auf unserer Webseite, sowie in der Readme-Datei, die dem Server beiliegt.

6. FAQ - häufige Fragen

1. Welche Dateitypen können mit AutoCrypt geschützt werden?

Sie können Windows 64 und 32 Bit EXE- und DLL-Dateien schützen, sowie .Net-Anwendungen. Seit der Protection Kit Version 5.90 werden RAD XE 64Bit Anwendungen, seit Version 7.0 .Net 4.x WPF Anwendungen und seit Version 8.17 .Net-Anwendungen unterstützt, die in .Net 6.0 oder höher (.Net Core) erstellt wurden. Wenn Sie Unterstützung für weitere Formate benötigen, wenden Sie sich bitte an unseren Support.

2. Ist AutoCrypt auch für Linux bzw. macOS verfügbar?

Bitte wenden Sie sich dazu an uns: https://www.marx.com/de/ueber-marx/kontakt

3. Meine Anwendung lässt sich schützen, startet aber nicht oder bringt eine Fehlermeldung.

Wenn Ihre geschützte Anwendung eine .Net 6.0 (oder höher) Anwendung ist und Sie nach dem Starten der Anwendung keinerlei Fehlermeldung erhalten haben, fehlen möglicherweise Dateien:

- Beachten Sie, dass Sie die zugehörigen Runtime-Konfigurationsdateien (.json-Dateien) vom Originalverzeichnis in das Verzeichnis mit den geschützten Dateien kopieren!
- Es fehlt die "Helper.dll". Diese Datei wird während des Schutzes automatisch im Zielordner erstellt. Bitte fügen Sie diese Datei ebenfalls zum Paket mit Ihrer geschützten Anwendung hinzu.

Eine weitere Möglichkeit warum die geschützte Anwendung nicht startet und Sie keine Fehlermeldung erhalten: die Werte für den Rijndael Private Key in Ihrem Projekt stimmen nicht mit denen in der angeschlossenen CRYPTO-BOX überein. Dies kann vor allem dann vorkommen, wenn Sie mehrere AutoCrypt-Projekte mit derselben CRYPTO-BOX nutzen. Stellen Sie in dem Fall für alle Projekte dieselben Wert für den AES-Key/Initialisierungsvektor in Ihrem Projekt ein.

Falls das nicht der Grund ist: bitte wenden Sie sich an unseren Technischen Support. In vielen Fällen können wir AutoCrypt anpassen, sodass Sie die Anwendung danach erfolgreich schützen können. Beachten Sie auch den Punkt 9 weiter unten.

4. Der Virenscanner meldet, dass meine geschützte Anwendung infiziert ist!

Es kommt gelegentlich vor, dass Virenscanner mit aktivierter Heuristik die geschützte Anwendung als infiziert erkennen (False Positive). Grund: Unser AutoCrypt-Wrapper nutzt zur Verschlüsselung der Anwendung Methoden, die auch teilweise von Schadsoftware eingesetzt wird. In diesem Fall gibt es folgende Möglichkeiten:

- Wenn Ihre Anwendung eine .NET 4.x-Anwendung ist, probieren Sie unseren DOTNET_SPLIT_LOAD Loader aus. Weitere Details dazu finden Sie in Kapitel 2.2.8 (bei Verwendung von AC_Tool beachten Sie die Erläuterungen in Kapitel 4.1 sowie Kapitel 3 in der AC_Tool Readme-Datei).
- Definieren Sie eine Ausnahmeregel im Virenscanner für Ihre Anwendung
- Die meisten Hersteller von Antivirus-Software bieten die Möglichkeit, als False Positive erkannte Anwendungen zu melden und auf ihren Server hochzuladen, damit diese in Zukunft nicht mehr als infiziert erkannt werden (Whitelisting).
- Signieren Sie Ihre geschützte Anwendung mit einem Code Signing Zertifikat.
- Überprüfen Sie, ob Sie in den Einstellungen des Virenscanners bestimmte Erkennungsmethoden deaktivieren können, insbesondere wenn diese häufig zu False Positive Meldungen führen.

5. Mein Kunde erhält beim Start der geschützten Anwendung immer die Fehlermeldung "Anwendung kann nicht gestartet werden (Dll fehlt oder beschädigt)".

Beim erstellen der geschützten Anwendung wird eine Datei fmteos.dll (bzw. fmteos64.dll für 64Bit-Dateien) mit erzeugt - liefern Sie diese unbedingt zusammen mit Ihrer geschützten Anwendung aus.

6. Ich bzw. mein Kunde erhalten beim Start der geschützten Anwendung immer die Fehlermeldung "CRYPTO-BOX® wurde nicht gefunden oder enthält keine gültigen Daten".

Prüfen sie in diesem Fall folgendes:

- Sind die CRYPTO-BOX Treiber korrekt installiert (siehe Abschnitt *5.1*) und leuchtet die LED an der CRYPTO-BOX? Sie können die korrekte Installation der CRYPTO-BOX mit dem Tool "MARX Analyzer" prüfen (auch beim End-User). Sie finden den MARX Analyzer im Downloadbereich von marx.com.
- Wurde die CRYPTO-BOX passend zur geschützten Anwendung konfiguriert?
  Für AutoCrypt Wizard: siehe Kapitel 2.3;
  Für AutoCrypt SxAF: siehe Kapitel *3.4.1;*
  Für AC_Tool.exe: siehe Abschnitt *4.2*.

7. Ich möchte meine AutoCrypt-Projekte sichern, um im Notfall ein Backup zu haben oder meine Projekte auf einen anderen Computer zu übertragen!

AutoCrypt Wizard: sichern Sie einfach die .xml-Datei Ihres Projekts (über den Punkt „Projekt speichern“). AutoCrypt SxAF: Sie können Ihre komplette SxAF-Datenbank sichern. Gehen Sie dazu im SxAF auf den Menüpunkt "Datenbank" → "Backup" und wählen Sie einen Speicherort aus. Sie können das Backup jederzeit über "Datenbank" → "Wiederherstellen" wieder einspielen oder auf einen anderen Computer übertragen. Wir empfehlen eine regelmäßige Sicherung der Datenbank, insbesondere vor der Installation einer neuen Version des Smarx OS Protection Kits (PPK).

8. Ich habe meine Anwendung mit der Einbindung über das Smarx OS API geschützt. Kann ich als zusätzliche Schutzmaßnahme meine Anwendung mit AutoCrypt verschlüsseln, um von Features wie Verschlüsselung und Debuggerschutz zu profitieren?

Das SxAF bietet die Verschlüsselung der .exe-Datei auch für API-Projekte an. Wenn Sie schon ein API-Projekt erstellt haben (siehe auch *Smarx Compendium*, Kapitel 4.5), finden Sie in den Projekteinstellungen zwei Schaltflächen: "AutoCrypt Einstellungen" und "Mit AutoCrypt schützen". Legen Sie zuerst die gewünschten Einstellungen, wie Dialogboxen und Verschlüsselungsoptionen fest und wählen Sie anschließend die zu schützende .exe-Datei aus. Bitte beachten Sie dazu auch Punkt 9 weiter unten.

Wenn Sie die AutoCrypt-Lizenzierungsoptionen (Ablaufdatum, Ausführungszähler, Netzwerklizenzierung, etc.) auch nutzen wollen, legen Sie stattdessen ein normales AutoCrypt-Projekt an wie in Abschnitt *3.3.2* ff. beschrieben. Beachten Sie jedoch folgendes:

- Lagern Sie bei der API-Einbindung die Abfragen mit dem Smarx API in einen eigene(n) Thread(s) aus und nutzen Sie unterschiedliche Partitionen in der CRYPTO-BOX.
- Wir empfehlen Ihnen, den Projekttyp "Compilation" im SxAF zu nutzen, um das API-Projekt und das AutoCrypt-Projekt zusammenzufassen. So brauchen Sie die CRYPTO-BOX nur einmal mit CB Format zu formatieren, anstatt zweimal (für das AutoCrypt- und das API-Projekt). Ausserdem prüft so das SxAF beide Projekte automatisch auf mögliche Überschneidungen/Inkompatibilitäten.

9. Ich habe mehrere Komponenten meiner Anwendung (mehrere EXE und/oder mehrere DLLs) mit AutoCrypt geschützt und habe das Problem, dass die Anwendung nicht mehr korrekt funktioniert oder eine Fehlermeldung kommt. Außerdem scheint die Lizenzierung (Ausführungszähler, Netzwerklizenzanzahl) nicht korrekt zu funktionieren!

Beachten Sie, dass Sie bestimmte Schutz- und Lizenzierungsoptionen nicht gleichzeitig für alle Komponenten/Anwendungsmodule verwenden (siehe auch Abschnitt *3.3.4*):

- Aktivieren Sie die Option "Periodisches Prüfen" nur bei einer geschützten Komponente (z.B. nur bei der EXE, nicht bei der EXE und weiteren geschützten DLLs)!
- Verwenden Sie die Option "Bestehende Partition nutzen" nicht gemeinsam für mehrere Komponenten, wenn diese gleichzeitig ausgeführt werden, da es sonst beim Ausführen beider Komponenten zu Fehlern kommen kann! Das gilt auch im Netzwerkmodus.
- Beachten Sie, dass wenn Sie Lizenzierungseinstellungen wie Zähler bis Lizenzablauf gemeinsam für mehrere Komponenten nutzen, werden diese beim Start jeder Komponente erneut herunter gezählt! Es empfiehlt sich daher, stattdessen eine eigene Partition pro Komponente festzulegen.