Skalierbarer Softwareschutz und Flexible Lizenzierung

CodeMeter und CodeMeterAct

WIBU SYSTEMS

Version 1.0

Rüppurrer Strasse 52-54 | D-76137 Karlsruhe

Tel.: +49-721-93172-0 | Fax: +49-721-93172-22

E-Mail: info@wibu.de

Inhalt

1 Einleitung

Software steuert unser Leben. So findet man Software heute nicht nur auf den PCs in Büro und Kinderzimmer, sondern in jeglicher Art von Maschinen – angefangen von der einfachen Kaffeemaschine, in der ein programmierbarer Controller den Strichcode des eingegebenen Pads auswertet und dann Wassermenge und Temperatur steuert, bis hin zu Strickmaschinen, die so groß wie eine Halle sind. In den meisten Fällen liegt das Know-how zum großen Teil in der steuernden Software.

Der Siegeszug der Software in allen Bereichen des Lebens hat aber auch seine Schattenseiten. Eine Software ist einfach und ohne jeglichen Materialaufwand digital kopierbar. Die entstandene Raubkopie hat die gleiche Qualität wie die originale Software. Handelt es sich um eine reine Softwareanwendung, dann kann ein Raubkopierer mit dem Einsatz von wenigen Cent pro CD und Booklet, eine Software – weit unter dem Marktpreis – verkaufen, die vom Original nicht zu unterscheiden ist. Ein lukratives Geschäftsmodell, welches laut Statistiken in Asien extrem hoch verbreitet ist, genau genommen aber ein weltweites Phänomen darstellt.

Ist das Ganze mit einer Maschine oder einer Steuerung gekoppelt, dann werden die elektronischen und mechanischen Teile eins-zu-eins kopiert. Auch hier ist der materielle Einsatz für die Raubkopie deutlich geringer, als die Entwicklungskosten für Hard- und Software durch den Hersteller. Häufig merkt der Anwender, der die Raubkopie einsetzt, gar nicht, dass es sich um keine originale Maschine handelt, da neben den Eigenschaften auch das Branding kopiert wird. Der Hersteller erfährt von der Raubkopie erst, wenn der Anwender einen Supportfall hat, aber nicht als Kunde gelistet ist.

Neben der Vervielfältigung von Raubkopien ist auch die Entwicklung von Nachahmungen ein lukratives Geschäftsmodell für den Dieb des geistigen Eigentums. Hier wird das Know-how aus einer Anwendung durch Reverse Engineering herausgezogen und im eigenen Produkt wiederverwendet. Dies reduziert die eigenen Forschungskosten drastisch und hilft einen Rückstand am Markt mit einem großen Sprung aufzuholen.

Je mehr Anteile in Programmiersprachen geschrieben werden, die einen lesbaren Zwischencode erzeugen (z.B. .NET oder Java), umso einfacher ist das Reverse Engineering der fertigen Anwendung. Mittels aktueller Werkzeuge kann aus einer Anwendung wieder lesbarer Quellcode erzeugt werden. Aber auch Anwendungen, die in einer Hochsprache wie C, C++ oder Delphi entwickelt wurden, sind vor Reverse Engineering nicht gefeit.

Daher ist es essentiell die Forschungs- und Entwicklungsarbeit, die in den eigenen Produkten steckt, gegen Raubkopien und Nachahmungen zu schützen. Nur so kann ein Unternehmen seinen Marktvorsprung halten und seinen Umsatz realisieren.

2 Softwareschutz im Überblick

Mit dem Softwareschutz- und Lizenzmanagementsystem CodeMeter / CodeMeterAct können Sie Ihre Software sicher gegen Raubkopien und gegen Reverse Engineering durch Mitbewerber schützen.

Mit CodeMeter® / CodeMeterAct bietet Ihnen WIBU-SYSTEMS ein einheitliches System, das hardwarebasierten Schutz (Dongle - CodeMeter) und softwarebasierten Schutz (Aktivierung - CodeMeterAct) miteinander verbindet. Sie liefern Ihre Software als eine Anwendung aus und entscheiden pro Kunde, ob Sie Dongle, Aktivierung oder beides verwenden möchten.

Beim Einsatz von CodeMeter / CodeMeterAct spielen die Integration in Ihre Software, sowie die Integration in Ihre Prozesse (Backoffice Integration) eine wichtige Rolle. CodeMeter / CodeMeterAct bietet Ihnen umfangreiche Tools, einfache APIs und einen allumfassenden Support.

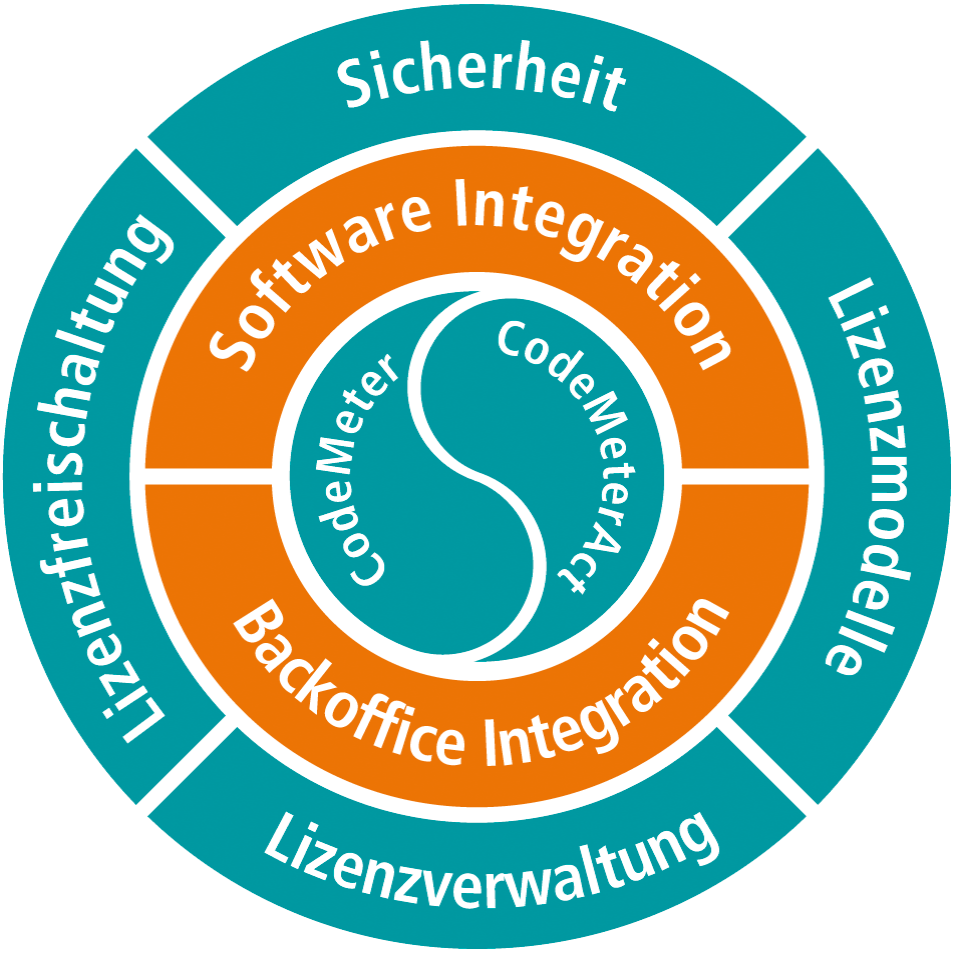


Abbildung 1: Softwareschutz mit CodeMeter / CodeMeterAct im Überblick

Sicherheit

Durch moderne Verschlüsselungsalgorithmen (AES, ECC und RSA), gepaart mit wechselnden Schlüsseln, bietet CodeMeter / CodeMeterAct ein Höchstmaß an Sicherheit, das in mehreren Hacker's Contests auch in der Praxis bewiesen wurde.

Lizenzmodelle

Mit CodeMeter / CodeMeterAct konnte bisher jedes auch noch so ausgefallene Lizenzmodell abgedeckt werden, von der Einzelplatz-Lizenz bis zu Overflow-Lizenzen im Netzwerk.

Lizenzverwaltung

Für die Verwaltung der erzeugten und verschickten Lizenzen bietet CodeMeter / CodeMeterAct eine datenbankbasierte Lösung, die einfach in bestehende Systeme integriert werden kann, sowie umfangreiche APIs für individuelle Anforderungen.

Lizenzfreischaltung

Die Freischaltung einer Lizenz erfolgt wahlweise durch die Programmierung eines Dongles am lokalen PC, durch die sichere Fernprogrammierung eines bereits beim Kunden befindlichen Dongles, durch die Internetaktivierung für einen PC sowie durch eine telefonische Aktivierung.

3 CodeMeter / CodeMeterAct

3.1 Ein Lizenzserver für alle Fälle

Die zentrale Komponente von CodeMeter / CodeMeterAct ist der CodeMeter Lizenzserver (CodeMeter.exe), der auf jedem Rechner läuft, auf dem eine geschützte Software verwendet werden soll. Diese Komponente ist für verschiedene Plattformen verfügbar. Der CodeMeter Lizenzserver stellt die Schnittstelle zwischen Ihrer Software und der Lizenz in einem Dongle (dem CmStick) bzw. in einer Aktivierungsdatei zur Verfügung.

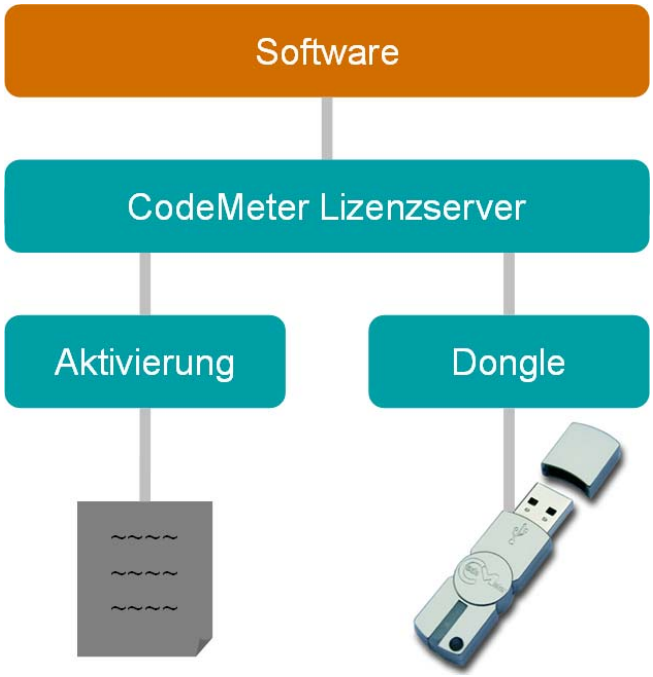


Abbildung 2: Einheitlicher Lizenzserver für CodeMeter / CodeMeterAct

Sie können wahlweise CmStick, Aktivierung oder beides verwenden. Der CmStick bietet Ihnen hierbei die höhere Sicherheit, da alle Ver- und Entschlüsselungen geschützt im CmStick durchgeführt werden.

3.2 Das CodeMeter Konzept

In einen CmStick, bzw. in eine Aktivierungsdatei können Sie viele Lizenzeinträge speichern. Im Dongle sind dies bis zu 4.000 und in der Aktivierungsdatei beliebig viele, nur durch den Platz auf der Festplatte begrenzt. Diese Lizenzeinträge bestehen aus einem Firm Code (FC), einem Product Code (PC) und einzelnen Optionen. Den Firm Code vergibt WIBU-SYSTEMS, den Product Code können Sie frei wählen.

Jeder Firm Code wird von WIBU-SYSTEMS einmal vergeben und an einen Master-Dongle, die sogenannte Firm Security Box (FSB) gebunden.

Dadurch stellt WIBU-SYSTEMS sicher, dass nur Sie als Besitzer der Firm Security Box in der Lage sind einen CmStick mit Ihrem Firm Code zu programmieren, bzw. eine Aktivierungsdatei zu erstellen. Das Programmieren, bzw. das Aktivieren ist durch Kryptographie abgesichert. Die dazu benötigten Schlüssel sind sicher in Ihrer FSB gespeichert.

Abbildung 3: Programmierung eines CmSticks

Zur besseren Übersicht werden die Lizenzeinträge in einem Container, dem Firm Item verwaltet. Jeder Lizenzeintrag wird Product Item genannt.

In einem CmStick können sich gleichzeitig Lizenzeinträge von verschiedenen Lizenzgebern befinden. Damit können sich mehrere Lizenzgeber einen CmStick teilen und Kosten sowie Bearbeitungsaufwand sparen. Der Lizenznehmer hat dabei den Vorteil, dass er alle Lizenzen in einem Dongle hat und so nur einen Anschluss belegt.

Bei CodeMeterAct können natürlich mehrere Lizenzdateien verschiedener Lizenzgeber gleichzeitig installiert sein.

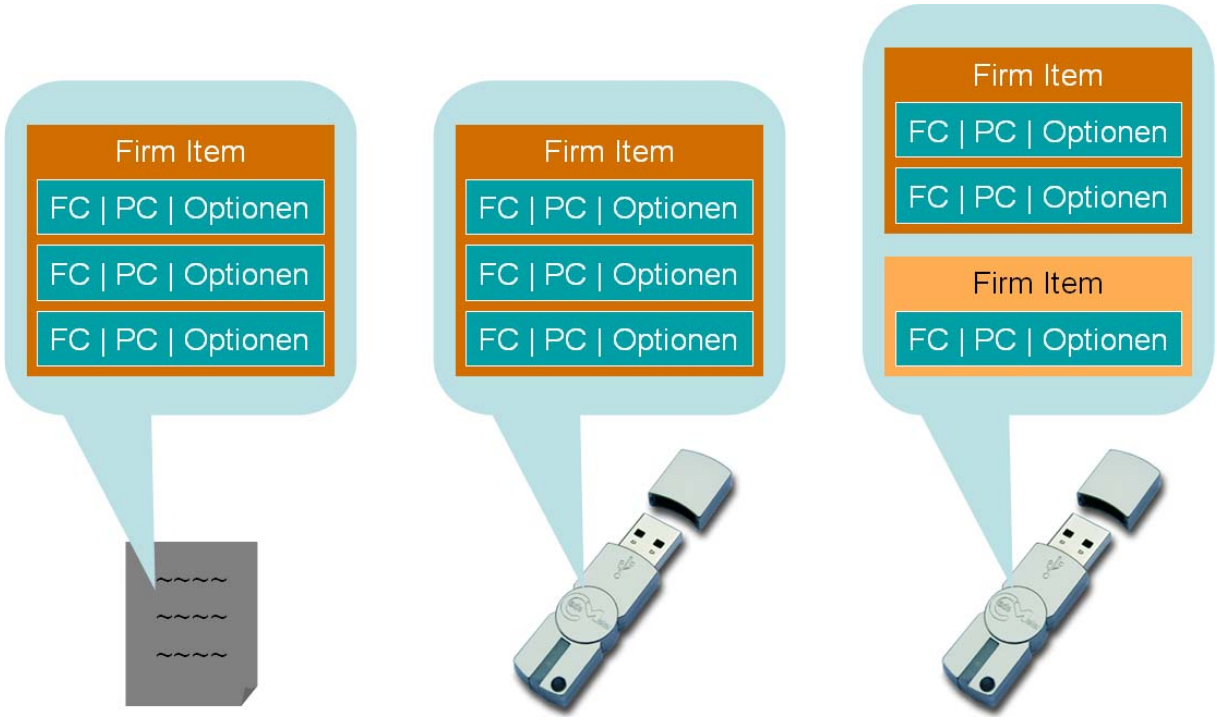


Abbildung 4: Aktivierungsdatei mit einem Firm Item, CmStick mit einem Firm Item, CmStick mit zwei Firm Items verschiedener Lizenzgeber

Jeder Lizenzeintrag kann verschiedene miteinander kombinierbare Optionen (Product Item Options) besitzen. Diese Optionen erlauben Ihnen für jeden Kunden individuelle Lizenzmodelle festzulegen. Alle Kunden erhalten die gleiche Software, und Sie legen die Lizenzoptionen im CmStick, bzw. in der Aktivierungsdatei fest.

Zum Anlegen, Ändern und Löschen der Optionen benötigen Sie in den meisten Fällen Ihre Firm Security Box. Damit stellen wir sicher, dass Ihr Kunde die von Ihnen verkaufte Lizensierung nicht selbstständig ändern kann. Lediglich die Option ‚Text' und ‚UserData' können ohne Firm Security Box geschrieben werden. Die Eigenschaften der einzelnen Optionen finden Sie in der folgenden Tabelle:

Product Item Option	Bemerkung	Lesen	Schreiben
Unit Counter	Zähler, Verwendung in Pay-Per-Use-, Pay-Per-Click-, Pay-Per-Print- oder Pay-Per-Start-Versionen	Ja	Reduzieren, ja / Erhöhen mit FSB
License Quantity	Anzahl der gleichzeitig benutzbaren Lizenzen, Verwendung für Floating Lizenzen im Netzwerk	Ja	Mit FSB
Activation Time	Aktivierungsdatum, Verwendung für zeitlich befristete Versionen	Ja	Mit FSB
Expiration Time	Ablaufdatum, Verwendung für zeitlich befristete Versionen	Ja	Mit FSB
Usage Period	Nutzungsdauer, Verwendung für zeitlich befristete Lizenzen, deren Startzeitpunkt noch nicht feststeht. (Demos, Backups)	Ja	Einmalig beim ersten Start
Feature Map	32-Bit Maske, Verwendung für Freischaltung von Features oder für Versionsverwaltung	Ja	Mit FSB
Customer Owned License Information	256 Byte Textfeld, Verwendung für kundenspezifische Daten (z.B. Name des Lizenznehmers)	Ja	Mit FSB
Text	256 Byte Textfeld, Verwendung als Anzeige im WebAdmin	Ja	Ja
User Data	256 Byte Daten, Verwendung zum Speichern von Konfigurationsdaten	Ja	Ja
Protected Data	128 x 256 Byte Daten, Verwendung zum Speichern von zusätzlichen Informationen im Binärformat	Ja	Mit FSB
Hidden Data	128 x 256 Byte Daten, Verwendung als Schlüsselquelle	Mit Passwort	Mit FSB
Secret Data	128 x 256 Byte Daten, Verwendung als Schlüsselquelle	Nein	Mit FSB

Tabelle 1: Product Item Options im Überlick

Der CodeMeter WebAdmin ermöglicht dem Anwender die Lizenzeinträge in einem CmStick einzusehen. CodeMeter WebAdmin ist im CodeMeter Lizenzserver integriert.

Abbildung 5: Beispiel des CodeMeter WebAdmin – zwei verschiedene Lizenzen

3.3 Betriebssysteme für CodeMeter / CodeMeterAct

CodeMeter / CodeMeterAct ist für viele Betriebssysteme verfügbar:

Betriebssystem	CodeMeter	CodeMeterAct
Windows 2000	Ja	Ja
Windows XP	Ja	Ja
Windows Vista	Ja	Ja
Windows 2000 Server	Ja	Ja
Windows 2003 Server	Ja	Ja
Windows 2008 Server	Ja	Ja
MacOS X	Ja	Ja
Linux	Ja[1)]	Ja[1)]
Sun Solaris 9	Ja	-
Sun Solaris 10	Ja	-
Windows XP Embedded	Ja	-
Windows CE 5.0	Ja	-
Windows CE 6.0	Ja	-

Tabelle 2: Unterstützte Betriebssysteme

[1] Siehe Release-Liste für detaillierte Information zu freigegebenen Distributionen

3.4 CodeMeter Bauformen

Die CodeMeter Hardware ist in einer großen Vielfalt für unterschiedliche Schnittstellen verfügbar:

	**CmStick**	Standard Version
	CmStick/M	Version mit zusätzlichem Flash Memory, um die Software direkt vom CmStick mobil starten zu können
	CmStick/ME	Metall-Edition, in edler Metallausführung, wahlweise mit Flash Memory
	**CmCard**	PCMCIA Karte, mit Flash Memory
	**CmCard/E**	Express-Karte für den Nachfolger des PCMCIA-Slots, mit Flash Memory
	**CmCard/SD**	SD-Card, geplant
	**CmASIC**	ASIC für die Integration auf eine eigene Platine

Tabelle 3: CodeMeter Bauformen

3.5 CodeMeterAct Bindungs-Schemata

Die Lizenzen in einer CodeMeterAct Lizenzdatei sind an einen PC gebunden. Aus bestimmten Eigenschaften des PCs, bzw. des installierten Betriebssystems, werden Informationen gebildet und als Host-ID verwendet. Diese Host-ID geht in den Freischaltcode ein. Nach der Aktivierung einer Lizenzdatei ist diese solange gültig, wie sich die verwendete Host-ID gar nicht bzw. innerhalb der von Ihnen zugelassenen Toleranzen ändert.

Bei den Schemata wird zwischen den Hardware-Bindungs-Schemata (echte Hardwareeigenschaften) und den Konfigurations-Bindungs-Schemata (konfigurierbare Eigenschaften) unterschieden.

3.5.1 Hardware-Bindungs-Schemata

Für die Hardware-Bindungs-Schemata stehen vier Eigenschaften der Hardware zur Verfügung, die beliebig miteinander kombiniert werden können:

Hardwareeigenschaft	Bemerkung
Network-Adapter (N)	Informationen über die Netzwerkkarte (Mac-Adresse)
Disk (D)	Informationen über die Festplatte (echte Seriennummer)
CPU (C)	Informationen über den Hauptprozessor (Type des Prozessors)
Bios (B)	Informationen über das Bios des PCs

Tabelle 4: Grundlegende Hardwareeigenschaften

Sie wählen eine beliebige Kombination der oben genannten Eigenschaften und legen fest, wie viele sich davon ändern oder nicht ändern dürfen. Empfohlene Schemata sind in der folgenden Tabelle zusammengestellt:

Schema	Bemerkung	Einsatz
N:1	Bindung an den Netzwerkadapter.	Große Unternehmen und KMU (kleine und mittelständische Unternehmen
DCBN:4	Bindung an Netzwerkadapter, CPU, Festplatte und Bios. Keine Toleranz gegenüber Änderungen der Hardware.	Small Office / Home Office, Spiele
DCBN:3	Bindung an Netzwerkadapter, CPU, Festplatte und Bios. Drei Eigenschaften müssen gleich bleiben, eine darf sich ändern.	Große Unternehmen, KMU, Small Office / Home Office
DCN:3	Bindung an Netzwerkadapter, CPU und Festplatte. Keine Toleranz gegenüber Änderungen der Hardware.	Große Unternehmen, KMU, Small Office / Home Office
DCB:2	Bindung an Netzwerkadapter, CPU und Festplatte. Zwei Eigenschaften müssen gleich bleiben, eine darf sich ändern.	Große Unternehmen, KMU, Small Office / Home Office
D:1	Bindung an die Festplatte	Home Office / Small Office

Tabelle 5: CodeMeterAct Hardware-Bindungs-Schemata

3.5.2 Konfigurations-Bindungs-Schemata

Im Vergleich zu den Hardware Eigenschaften ist die Bindung an die konfigurierbaren Eigenschaften deutlich schwächer. Die Eigenschaften sind außerdem auch nicht kombinierbar:

Schema	Bemerkung	Einsatz
IP-Address (IP)	In die Berechnung der Host-ID geht die IP-Adresse des PCs ein. Es wird dabei die IP-Adresse verwendet, an die der CodeMeter Lizenzserver gebunden ist.	Große Unternehmen, Small Office / Home Office
Machine-SID (MID)	In die Berechnung der Host-ID gehen die Machine-SID und die Domain-SID im Windows Netzwerk ein.	Große Unternehmen
None (Non)	Die Lizenzdatei ist nicht an einen PC gebunden und kann mit einem festen vorberechneten Code auf beliebig vielen PCs aktiviert werden. Dieser Modus geht aus lizenztechnischen Gründen nur mit zeitlich eingeschränkten Lizenzen. Dieses Schema kann für Demoversionen ohne Online-Aktivierung (nur Eingabe der Produktseriennummer und des Freischaltcodes auf der Verpackung) verwendet werden. Der Freischaltcode ist dann für alle PCs gleich. Nach Ablauf der Lizenz kann diese auf dem gleichen PC nicht noch mal verwendet werden.	Small Office / Home Office (Demos)

Serial (Ser)	Die Host-ID wird aus der Produktseriennummer berechnet. Damit ist diese für jeden Lizenznehmer anders. Die Host-ID ändert sich aber nicht mit dem Austausch von Rechner-Hardware. Dieses Schema ist als einfacher Lizenzschutz konzipiert. Zusätzlich kann der Lizenzgeber den Name des Lizenznehmers in die Lizenzdatei schreiben, diesen auslesen und in der Software oder auf Ausdrucken anzeigen. Dies lässt die Lizenz gefühlt individueller erscheinen und erhöht die mentale Barriere die Lizenz weiterzugeben. In diesem Schema können die Freischaltcodes vorberechnet werden. D.h. der Lizenznehmer erhält eine Produktseriennummer und einen Freischaltcode, gibt beides ein und die Software läuft ohne Online-Aktivierung.	Große Unternehmen

Tabelle 6: CodeMeterAct Konfigurations-Bindungs-Schemata

Das Bindungs-Schema wird unabhängig von der Software festgelegt und kann für eine schon für CodeMeterAct verschlüsselte Software nachträglich geändert werden.

Der Lizenznehmer erhält eine Lizenz-Informationsdatei, die die Information über das verwendete Schema enthält. Diese Lizenz-Informationsdatei kann zusammen mit der Software ausgeliefert (z.B. im Installationsprogramm), oder auch separat zum Lizenznehmer geschickt. Der Lizenzgeber legt damit für jeden Lizenznehmer das Schema individuell fest.

So erstellt der Lizenzgeber zum Beispiel eine CD, die für alle Kunden gleich ist und die eine Lizenz-Informationsdatei mit dem Schema DCBN:3 enthält. Diese bekommen alle Endkunden und alle mittleren und großen Firmenkunden. Schließt der Lizenzgeber jetzt einen Rahmenvertrag mit einem großen Firmenkunden, welcher den Einsatz von 100 Lizenzen in der Firma erlaubt und Online-Aktivierung ausschließt, dann schickt er diesem Firmenkunden lediglich eine neue Lizenz-Informationsdatei mit dem Bindungs-Schema IP-Adresse oder Serial, sowie eine Liste mit 100 Freischaltcodes.

4 Lizenzmodelle

Jeder Lizenzeintrag kann beliebig miteinander kombinierbare Optionen enthalten, die dem Lizenzgeber die Möglichkeit bieten, seine Lizenzmodelle mit CodeMeter / CodeMeterAct abzubilden. Die folgenden Lizenzmodelle sind abbildbar:

Lizenzmodell	Bemerkung
Standardlizenz	Realisiert als Eintrag aus Firm Code und Product Code. Je nach Implementierung in der Software muss die Lizenz am lokalen PC verfügbar sein oder kann auch auf einem Lizenzserver im Netzwerk gefunden werden. Sie können in der Software ebenfalls vorgeben, ob nur eine oder mehrere Instanzen gleichzeitig laufen dürfen.
Lokale Lizenz	Realisiert als Eintrag aus Firm Code und Product Code mit License Quantity = 0. Der CmStick, bzw. die Aktivierungsdatei muss dann lokal am selben PC verfügbar sein, auf dem die Software laufen soll. Bei Betrieb des CmSticks unter VmWare muss die Lizenz direkt in der Session verfügbar sein. Ein Sharing zwischen verschiedenen Sessions ist nicht möglich.
Floating Lizenz	Realisiert als Eintrag aus Firm Code und Product Code mit License Quantity = x. Dabei geben Sie mit x vor, wie oft die Software gleichzeitig betrieben werden kann. Sie können hierbei zwischen Zählung pro PC oder Zählung pro Instanz wählen.
Zeitlich limitierte Lizenz (fixes Datum) Demoversion Mietlizenz	Realisiert als Eintrag aus Firm Code und Product Code mit einem Ablaufdatum oder einem Nutzungszeitraum. Das Ablaufdatum, bzw. der Nutzungszeitraum wird bei CodeMeter gegen die interne Uhr im CmStick verglichen und ist damit gegen Manipulationen sicher. Bei CodeMeterAct wird das Ablaufdatum mit der PC Uhr verglichen. CodeMeterAct enthält Mechanismen, um das Zurückstellen der Uhr des PCs zu erkennen.
Pay-per-use Lizenz Pay-per-click Lizenz Demoversion (x-mal Starten)	Realisiert als Eintrag aus Firm Code und Product Code mit einem Unit Counter. Sie bestimmen, wann der Unit Counter heruntergezählt wird. Bei einer x-mal Starten Version geschieht dies beim Start der Anwendung. Bei einer pay-per-use oder pay-per-click Lizenz zählen Sie den Unit Counter vor oder nach der entsprechenden Aktion in Ihrer Anwendung selbst herunter. Bei verschiedenen Aktionen können Sie natürlich wahlweise den gleichen Counter oder verschiedene Counter reduzieren.
Laufzeit limitierte Lizenz	Realisiert als Eintrag aus Firm Code und Product Code mit einem Unit Counter (Wert = Laufzeit / Zeiteinheit). In der Software zählen Sie den Unit Counter pro Zeiteinheit um 1 herunter.
Funktional eingeschränkte Demoversion Modulare Lizenz	Realisiert als mehrere Einträge aus Firm Code und unterschiedlichen Product Codes. Jeder Product Code steht für ein Modul / eine Funktionalität. Durch das Programmieren der entsprechenden Product Codes können Sie eine individuelle Lizenz für den Lizenznehmer erstellen. In diesem Fall können Sie jedes Modul separat mit weiteren Optionen (z.B. Ablaufdatum) versehen. ODER Realisiert als Eintrag aus Firm Code und Product Code mit einer Featue Map. Jedes Bit in der Feature Map steht für genau ein Modul / eine Funktionalität. Durch das Programmieren der entsprechenden Feature Map können Sie die einzelnen Module / Funktionalitäten freischalten. Die Lizenzen für die einzelnen Module können auf verschieden CmSticks bzw. Lizenzdateien verteilt sein. So könnte die Basisversion mit Rechnerbindung laufen, während der Servicetechniker mit seinem CmStick Zugriff auf erweiterte Funktionen erhält.

Downgrade Lizenz	Realisiert als Eintrag aus Firm Code und Product Code mit einer Feature Map. Jedes Bit in der Feature Map steht für eine Version. So können Sie z.B. eine Floating Lizenz auf 3 PCs gleichzeitig inklusive einem Downgrade-Recht anbieten, d.h. der Lizenznehmer kann auf 3 PCs entweder die alte oder die neue Version starten, aber beide zusammen auf maximal 3 PCs gleichzeitig.
Cold-Standby Lizenz	Realisiert als Eintrag aus Firm Code und Product Code mit einer Usage Period. Der Backup-Dongle kann für eine von Ihnen definierte Zeitspanne ab dem ersten Start (z.B. 7 Tage) verwendet werden. Innerhalb dieser Zeit können Sie die originale Lizenz ersetzen und den Backup-Dongle wieder zurücksetzen.
Hot-Standby Lizenz	Realisiert als Eintrag aus Firm Code und Product Code in der Haupt-Lizenz und aus Firm Code und Product Code mit einem sehr hohen Unit Counter in der Backup-Lizenz in einem zweiten CmStick / auf einem zweiten PC. Über die Serversuchliste legen Sie die Reihenfolge der zu belegenden Lizenzen fest. Im Fall, dass der erste Server ausfällt, wird automatisch der zweite Server mit den Backup-Lizenzen verwendet. Sie kontrollieren regelmäßig den Zählerstand, um einen Missbrauch zu vermeiden.
Overflow Lizenz	Realisiert als zwei Einträge aus Firm Code und zwei verschiedenen Product Codes. Der Haupt-Eintrag enthält keinen Unit Counter und eine License Quantity entsprechend der gekauften Lizenzen. Der Overflow-Eintrag enthält einen hohen Unit Counter und eine License Quantity in Höhe der gewünschten Overflow Lizenzen. Wenn alle Haupt-Einträge belegt sind, verwenden Sie in der Software die Overflow-Einträge. Sie können dann selbst entscheiden, ob Sie dies in der Software anzeigen und die Software in diesem Fall künstlich verlangsamen wollen. Zusätzlich können Sie regelmäßig den Unit Counter kontrollieren und so nachweisen, wie häufig (oder wie lange) die Overflow Lizenzen verwendet wurden.
Rechnergebundene Lizenz	Realisiert mit CodeMeterAct und dem entsprechenden Bindungs-Schema (Hardware oder Maschine). Alternativ als Eintrag aus Firm Code und Product Code mit dem Speichern einer eigenen Host-ID als Protected Data. In der Software vergleichen Sie, ob die eigene gespeicherte Host-ID mit der aktuell für den Rechner berechneten übereinstimmt.
Named User Lizenz	Realisiert als Eintrag aus Firm Code und Product Code mit dem Speichern einer eigenen User-ID als Protected Data. In der Software vergleichen Sie, ob die eigene gespeicherte User-ID mit der aktuell für diesen Nutzer berechneten User-ID übereinstimmt.

Tabelle 7: Lizenzmodelle

Alle Lizenzmodelle sind miteinander kombinierbar. Mehrere Einträge - mit identischen Firm Code und Product Code - werden an einem Lizenzserver zusammengezählt. So können Sie z.B. zu einer Floating Lizenz weitere Floating Lizenzen für eine gewisse Zeit hinzufügen.

Abbildung 6: Acht Floating Lizenzen für „Produkt Eins", verteilt auf zwei Lizenzeinträge

5 Lizenzfreischaltung

5.1 Programmierung eines CmSticks

Zur Programmierung eines CmSticks benötigen Sie eine FSB, die Ihren Firm Code enthält (siehe 3.2 Das CodeMeter Konzept).

Die Programmierung kann über die folgenden Wege erfolgen:

- **Direkt** (der zu programmierende CmStick wird beim Lizenzgeber programmiert.)
- **Per Dateiaustausch** (der zu programmierende CmStick befindet sich bereits beim Lizenznehmer und wird remote umprogrammiert.)

Bei der direkten Programmierung befindet sich die FSB am lokalen PC oder an einem Lizenzserver im Netzwerk. Über die Zugriffskontrolle auf einem Netzwerkserver werden Berechtigungen vergeben, von welchem Rechner aus die FSB verwendet werden darf.

Abbildung 7: Programmierung eines lokal angeschlossenen CmSticks

Wie in Abbildung 7 dargestellt, wird in einen leeren CmStick ein Lizenzeintrag mit dem Firm Code aus der FSB programmiert. Natürlich kann der zu programmierende CmStick bereits Lizenzeinträge enthalten. Dabei ist es egal, ob diese eigene Lizenzeinträge mit dem gleichen Firm Code, oder Lizenzeinträge von anderen Lizenzgebern sind.

Bei der Programmierung per Dateiaustausch wird für den zu programmierenden CmStick eine Kontext-Datei erzeugt. Dabei ist es wiederum egal, ob der CmStick leer ist, eigene Lizenzeinträge oder fremde Lizenzeinträge besitzt. Die Kontext-Datei enthält die Seriennummer des CmSticks und den Inhalt des eigenen Firm Items, dem Lizenzcontainer in dem alle eigenen Lizenzeinträge zusammengefasst sind.

Über die FSB erzeugen Sie dann eine Update-Datei. Diese Update-Datei kann vom Lizenznehmer genau einmal in genau den dafür bestimmten CmStick eingespielt werden. Nach dem erfolgreichen Einspielen der Update-Datei wird ein Zähler im Firm Item erhöht. Durch das Erhöhen des Zählers wird die Update-Datei für ein weiteres Einspielen ungültig. Dies ist vor allem relevant, wenn die Update-Datei Programmierbefehle enthält, die einen weiteren Lizenzeintrag anlegen, einen Unit Counter um eine Anzahl an Einheiten erhöhen oder ein Ablaufdatum um eine Anzahl an Tagen nach vorne setzen.

Dieser Weg eignet sich sowohl für eine offline, als auch eine online Umprogrammierung von CmSticks. Im offline Fall schickt der Lizenznehmer die Kontext-Datei z.B. per Mail an den Lizenzgeber, oder lädt diese auf der Webseite des Lizenzgebers hoch. Auf dem gleichen Weg erhält der Lizenznehmer die Update-Datei vom Lizenzgeber zurück.

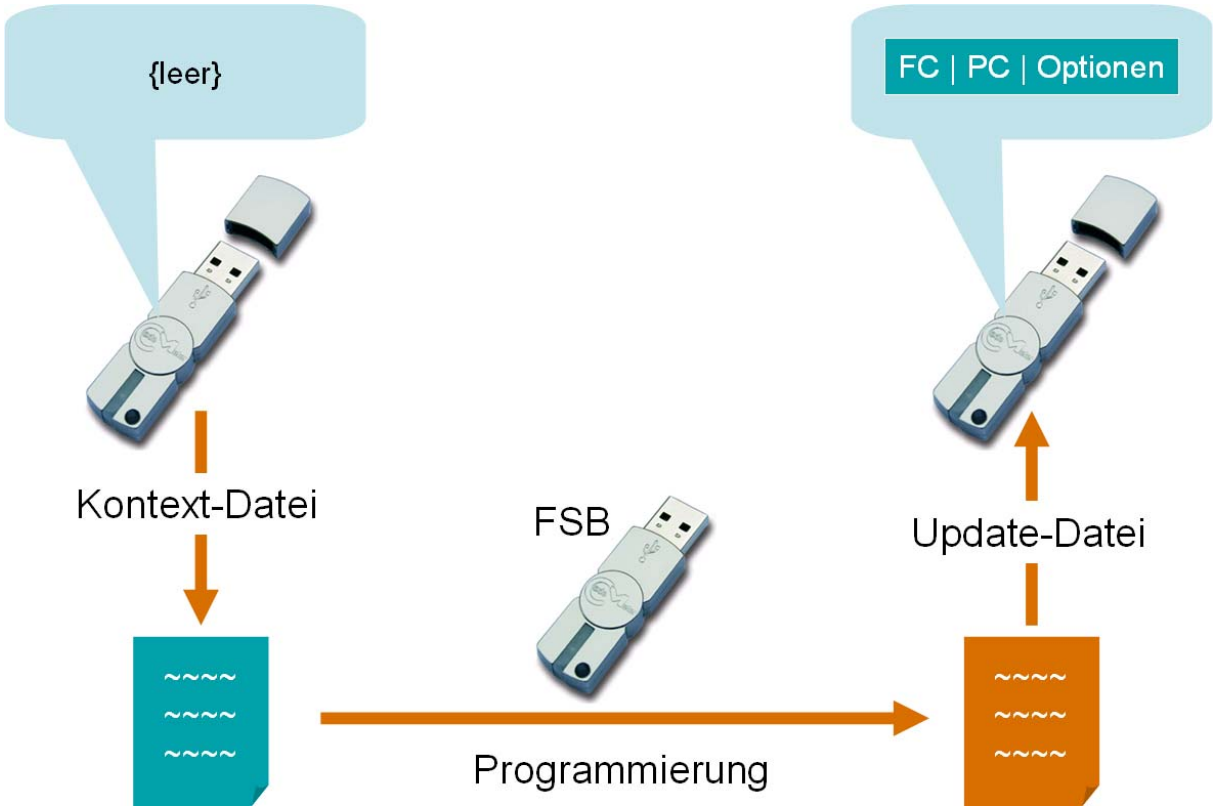


Abbildung 8: Programmierung mittels Update-Datei

Um den Umprogrammierprozess zu vereinfachen, kann sich der Lizenzgeber die nächste Kontext-Datei berechnen und diese gleich als Modifizierte Kontext-Datei aufheben. Dann entfällt das Erzeugen und Verschicken der Kontext-Datei auf der Seite des Lizenznehmers. Der Lizenzgeber verschickt lediglich seine Update-Dateien. Dies ist möglich, da für die Programmierung der eigenen Lizenzeinträge nur der Zustand des eigenen Firm Items (d.h. des Zählers im Firm Item) relevant ist. Sollte der CmStick zwischendurch von einem anderen Lizenzgeber umprogrammiert worden sein, behalten Ihre Update-Dateien, Kontext-Dateien und Modifizierten Kontext-Dateien weiterhin ihre Gültigkeit.

Im online Fall wird die Kontext-Datei auf der Seite des Lizenznehmers automatisch erzeugt und hochgeladen, die Update-Datei heruntergeladen und eingespielt und eine neue Kontext-Datei als Quittung erzeugt und hochgeladen. In diesem Fall hat der Lizenzgeber immer einen aktuellen Überblick, welche Lizenzen bei welchen Kunden bereits eingespielt sind.

Diese Funktionalität können Sie in Ihre Software integrieren oder Sie nutzen Standardsoftware von WIBU-SYSTEMS, die mit der CodeMeter Runtime installiert werden. Das Online Modul für den Lizenzgeber wird in Kapitel 8 Lizenzverwaltung - Backoffice Integration beschrieben.

5.2 Freischaltung einer CodeMeterAct Lizenz

5.2.1 Automatische Aktivierung

Anstelle eines CmSticks wird bei CodeMeterAct eine Lizenzinformationsdatei ausgeliefert. Diese ist vergleichbar mit einem leeren CmStick und enthält die Information über das CodeMeterAct Bindungs-Schema.

Bei der automatischen Aktivierung einer CodeMeterAct Lizenz wird aus der Lizenzinformationsdatei und der Host-ID eine Kontext-Datei erzeugt.

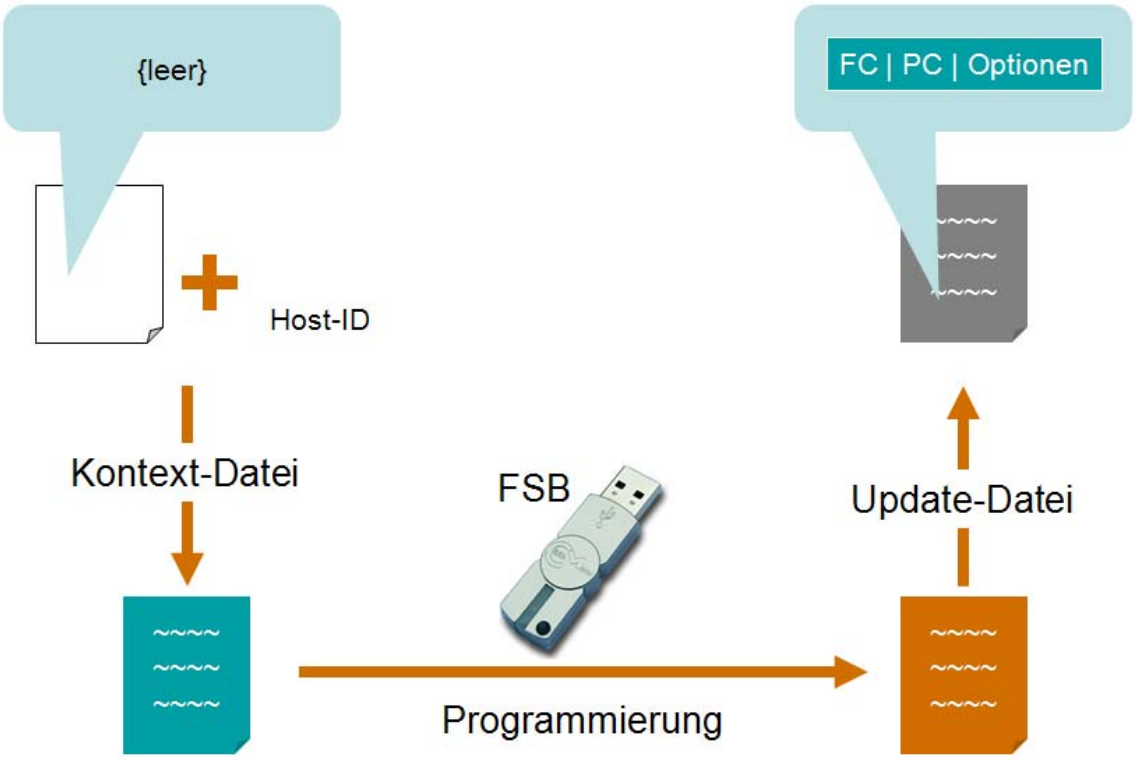


Abbildung 9: Automatische Programmierung einer CodeMeterAct Lizenz

Die erzeugte Kontext-Datei wird dann vom Lizenznehmer zum Lizenzgeber geschickt. In der Regel sollte Ihr Kunde dabei die Produktseriennummer als ‚Kaufnachweis' mitschicken. Dafür gibt es die folgenden Möglichkeiten:

- **Direkt aus Ihrer Software heraus per SOAP:** Sie erstellen automatisch die Kontext-Datei und spielen die Update-Datei ein. Über eine Fehlermeldungsschnittstelle (Dll) können Sie die Aktivierung auch sehr einfach in eine automatisch mit dem AxProtector geschützte Anwendung integrieren.
- **Direkt über eine Webseite:** Installierte CodeMeter Runtime erforderlich, der Lizenznehmer geht auf die Webseite, das Erstellen der Kontext-Datei und das Einspielen der Update-Datei erfolgen automatisch.
- **Indirekt über eine Webseite:** Der Lizenznehmer erstellt die Kontext-Datei selbst, lädt diese hoch, erhält die Update-Datei und spielt diese manuell ein. Damit ist es auch möglich eine Lizenz auf einem PC zu aktivieren, der über keinen direkten Internetzugang verfügt.

5.2.2 Telefonische Aktivierung

Die automatische Aktivierung erfordert einen verfügbaren Internetzugang. Dieser muss nicht zwingend am Rechner vorhanden sein, für den die Lizenz aktiviert werden soll, allerdings muss es eine Möglichkeit geben, zwischen diesem Rechner und einem Rechner im Internet Daten per Datei auszutauschen. Falls diese Voraussetzung nicht erfüllt ist, bietet WIBU-SYSTEMS Ihnen die telefonische Aktivierung.

Im Gegensatz zur automatischen Aktivierung ist die ausgelieferte Lizenzinformationsdatei nicht leer, sondern sie enthält schon einen großen Teil der benötigten Informationen. Lediglich ein letzter fehlender Teil der kryptographischen Schlüssel wird bei der Aktivierung übertragen.

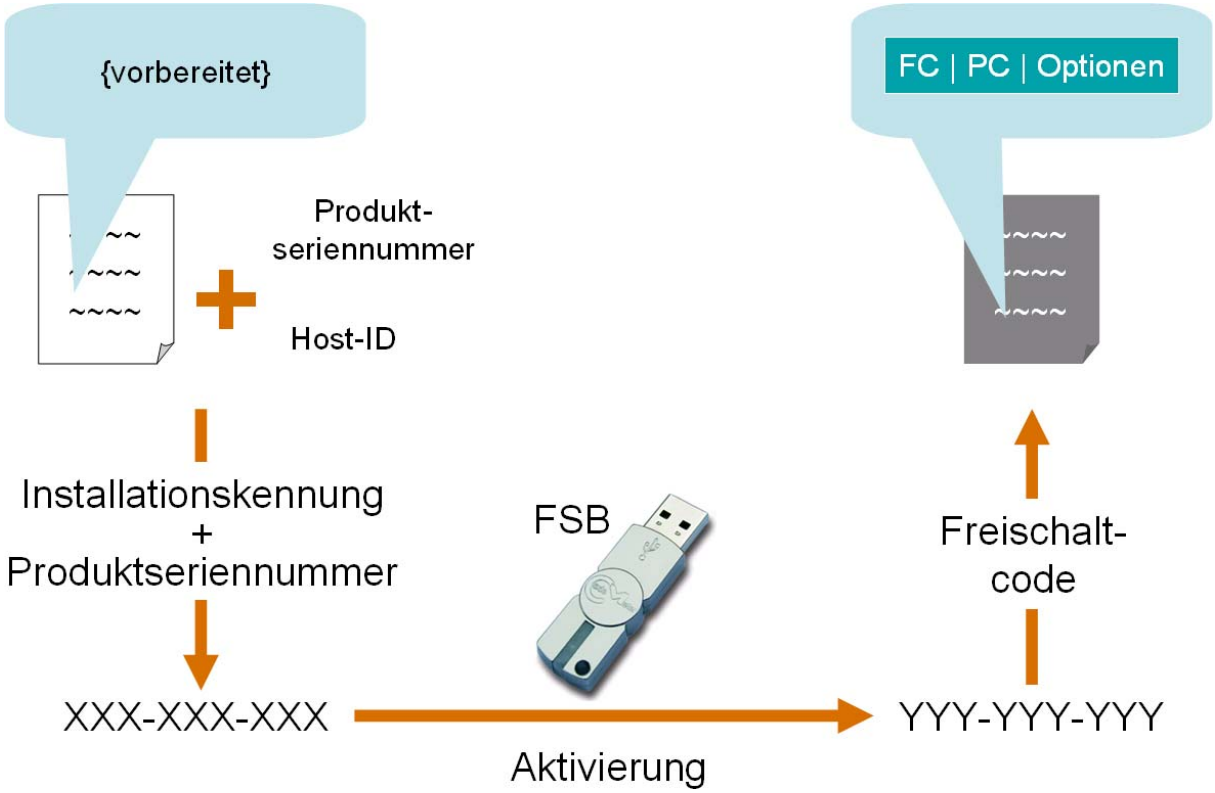


Abbildung 10: Aktivierung einer CodeMeterAct Lizenz per Telefon

Bei der telefonischen Aktivierung wird auf dem PC des Lizenznehmers aus der Host-ID und der Produktseriennummer eine Installationskennung für die vorhandene Lizenz-Informationsdatei berechnet. Diese Installationskennung und die Produktseriennummer nennt der Lizenznehmer dem Lizenzgeber am Telefon.

Der Lizenzgeber berechnet daraus innerhalb CodeMeter License Central (siehe 8. Lizenzverwaltung - Backoffice Integration) den Freischaltcode und übermittelt ihn an den Lizenznehmer, der diesen eingibt. Die Lizenz ist aktiviert.

Zur Implementierung der automatischen wie telefonischen Aktivierung stehen Ihnen API Funktionen zur Verfügung, die sich in Ihre Software integrieren lassen. Damit realisieren Sie den Aktivierungsprozess in Ihrem Corporate Design. Im Falle einer automatisch geschützten Anwendung (siehe 7.1 AxProtector) finden Sie ein Implementierungsbeispiel in der Fehlermeldungs-Dll.

Die telefonische Aktivierung lässt sich automatisieren. Anstelle einer Person beim Lizenzgeber wird ein Sprachcomputer oder eine Internetseite verwendet werden. In diesem Falle tippt der Lizenznehmer die Installationskennung am Telefon oder auf einer Internetseite ein und erhält das Ergebnis automatisch angesagt, bzw. angezeigt.

Bei der telefonischen Aktivierung besitzen Sie zwei grundlegende Möglichkeiten für die Codierung der Installationskennung und des Freischaltcodes:

- Alphanumerischer Modus: Verwendung von 32 alphanumerischen Zeichen (0..9, A..Z), Länge: 40 Zeichen
- Numerischer Modus: Verwendung von 10 Zahlen (0..9), Länge: 60 Zeichen

Der numerische Modus benötigt eine größere Länge, hat aber den Vorteil, dass der Installations-Code bei einer Anbindung an einen Sprachcomputer einfach über die Telefontasten einzugeben ist. Die telefonische Übermittlung des Freischaltcodes im numerischen Modus ist speziell international einfacher, da 10 Zahlen einfacher zu buchstabieren sind als alphanumerische Zeichen.

5.3 Mehrfache Aktivierung

Der Fall, dass ein CmStick ausfällt, tritt sehr selten auf. Vermeiden lässt sich dies durch einen Backup-CmStick, den man dem Kunden vorab zukommen lässt und der alle Lizenzen mit der definierten Nutzungsdauer (UsagePeriod) enthält. Häufiger hingegen kommt es vor, dass der PC, auf dem eine Lizenz aktiviert ist, aufgerüstet oder ausgetauscht wird. Damit wird die Host-ID geändert und eine erneute Aktivierung ist notwendig. Erfahrungswerte zeigen, dass man bei nicht toleranten Schemas eine Aktivierung pro Jahr benötigt, unabhängig davon, ob es sich um Business- oder Consumer-Produkte handelt.

Dafür kann bei der Konfiguration der Lizenz (siehe 8 Lizenzverwaltung - Backoffice Integration) angegeben werden, wie häufig die entsprechende Lizenz aktiviert werden darf. Ist die Anzahl an erlaubten Aktivierungen erreicht, kann der Mitarbeiter im Support des Lizenzgebers diese Anzahl für jede gekaufte Lizenz individuell erhöhen. Danach kann die Aktivierung entsprechend oft erneut durchgeführt werden.

Die erneute Aktivierung der gleichen Produktseriennummer und für die gleiche Host-ID wird nicht als mehrfache Aktivierung gewertet und kann auch durchgeführt werden, wenn die Anzahl der erlaubten Aktivierungen bereits erreicht ist. Sollte diese Produktseriennummer bereits auf mehreren Host-IDs aktiviert worden sein, gilt dieser Fall nur für die letzte zu dieser Produktseriennummer bekannte Host-ID.

Um den Missbrauch durch mehrfache Aktivierung einzuschränken, hat der Lizenzgeber die Möglichkeit, die Lizenzen mehr oder weniger hart zeitlich zu begrenzen:

- **Ablaufdatum**: In der Lizenz wird ein Ablaufdatum gesetzt. Die Lizenz verfällt dann automatisch zum Zeitpunkt des Ablaufs und muss neu aktiviert werden. Die Verlängerung der Lizenz kann der Lizenzgeber als automatisches Update in seine Software integrieren. In diesem Fall sieht der Lizenznehmer das Ablaufdatum im CodeMeter WebAdmin. Dies ist daher dafür geeignet, um Mietkauflizenzen zu realisieren, bei denen der Lizenznehmer die Mietperiode kennt.
- **CheckPoint**: In der Lizenz wird in einem Datenfeld ein zeitlicher CheckPoint definiert. Dies kann im Klartext („Nächstes Update am 31.08.2008“) oder verschlüsselt erfolgen. Die Software überprüft den CheckPoint selbst. Wenn der CheckPoint erreicht ist, versucht die Software, die Lizenz neu zu aktivieren. Dabei wird der alte CheckPoint gelöscht und ein neuer CheckPoint gesetzt. Die Reaktion auf Fehler („Lizenz konnte nicht erneut aktiviert werden.“) liegt komplett in Ihrer Software.

In beiden Fällen wird von Ihrer Software aus die Lizenz automatisch neu aktiviert. Wenn dabei die Host-ID nicht mit der aktuell für diese Produktseriennummer hinterlegten Host-ID übereinstimmt und die Anzahl der erlaubten Aktivierungen erreicht ist, kann die Lizenz nicht verlängert werden. Im Fehlerfall kann der Support die Anzahl der Aktivierungen erhöhen, oder er ändert das Bindungs-Schema für diesen Kunden individuell.

6 Sicherheit

6.1 Einsatz von Verschlüsselung

Die Sicherheit von CodeMeter / CodeMeterAct basiert auf Verschlüsselung. Die zu schützende Software, bzw. Teile der Software oder Daten in der Software werden vor der Auslieferung durch den Lizenzgeber verschlüsselt. Der Schlüssel zum Entschlüsseln ist in der Lizenz enthalten, die der Lizenzgeber dem Lizenznehmer erstellt. Auf der Seite des Lizenznehmers werden in der Software nur die Teile entschlüsselt, die gerade benötigt werden. Nach der Verwendung können diese Teile wieder verschlüsselt werden.

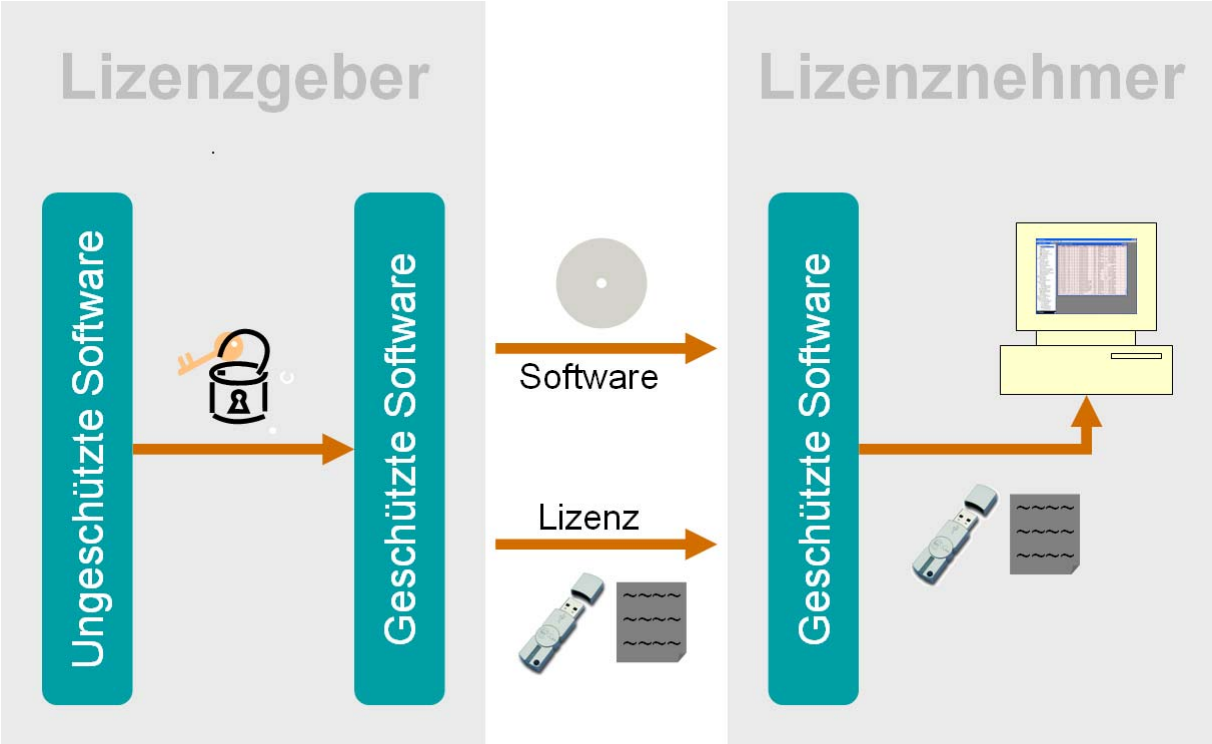


Abbildung 11: Sicherheit durch Verschlüsselung

CodeMeter und CodeMeterAct basieren auf denselben Prinzipien und bilden die gleichen Lizenzmodelle ab. Bei CodeMeterAct, das komplett im Speicher des PCs läuft, werden andere geheime Schlüssel und andere Verfahren verwendet als bei CodeMeter. Aus der Analyse von CodeMeterAct kann ein Cracker keine Rückschlüsse auf die sicher im Smartcard-Chip gespeicherten Schlüssel von CodeMeter ziehen.

6.2 Vorteile der Hardware

CodeMeter hat seine Sicherheit in mehreren Hackers' Contests auch in der Praxis bewiesen. „6 Monate Haltbarkeit war unser Ziel und nun gibt es seit mehr als 3 Jahren keine Cracks mehr von unserer Software. Dies hat unsere Erwartungen um ein Vielfaches übertroffen." wird ein Hersteller einer Musiksoftware zitiert, der sich für CodeMeter entschieden hat.

Hier kommen deutlich die Stärken von CodeMeter zum Vorschein. Die folgende Tabelle zeigt die sicherheitsrelevanten Punkte, bei denen der Dongle der Aktivierung deutlich überlegen ist.

Vorteil von CodeMeter	Bemerkung
Firmware läuft geschützt in der Hardware	Die Firmware, d.h. die Speicherung und Berechnung der Schlüssel und die entsprechende Entschlüsselung bzw. Verschlüsselung läuft sicher geschützt im Smartcard-Chip im CmStick ab. Dieser Teil kann vom Hacker nicht analysiert werden und stellt somit eine Black Box dar.
Hardware kann gesperrt werden	Wenn Sie innerhalb Ihrer Software einen Angriff erkennen (dies machen unsere Tools automatisch für Sie), dann haben Sie die Möglichkeit, ein Sperrkommando aus Ihrer Software heraus an den CmStick zu schicken. Dieses Kommando sperrt alle Ihre Lizenzen, d.h. die in Ihrem Firm Item. Sie können diese Lizenzen per Fernprogrammierung wieder freischalten, aber bis zur Freischaltung verhält sich der CmStick so, als wären diese Lizenzen (und damit die Schlüssel) nicht vorhanden. Der Hacker hat keinen zweiten Versuch.
Zähler können nicht durch ein Backup zurückgesetzt werden	Zähler werden sicher im Smartcard-Chip im CmStick gespeichert. Damit können diese nicht von außen manipuliert oder durch das Einspielen eines Backups wieder zurückgesetzt werden.
Gelöschte Lizenzen können nicht durch ein Backup zurückgesetzt werden	Lizenzen, die in einem CmStick gelöscht wurden sind nicht mehr vorhanden. Durch die Übermittlung einer fälschungssicheren Quittung ist der Lizenzgeber sicher, dass die Lizenz im aktuellen CmStick nicht mehr vorhanden ist und auch nicht wieder hergestellt werden kann.
Expiration Time und Usage Period werden gegen die interne Uhr überprüft	Alle verwendeten Zeiten wie Expiration Time und Usage Period werden gegen die intern im Smartcard-Chip laufende Uhr geprüft. Die eingetragenen Zeiten können nicht manipuliert werden; die interne Uhr kann nicht zurückgesetzt werden. Damit ist eine abgelaufene Lizenz nicht wieder herstellbar.
Einfacher Wechsel auf einen anderen PC	Ein Umzug der Software auf einen anderen PC ist problemlos möglich. Software installieren und den CmStick anstecken. Dies kann der Lizenznehmer selbst beliebig häufig durchführen, ohne dass er dazu den Lizenzgeber benötigt. Der Lizenzgeber kann sich auf der anderen Seite sicher sein, dass nach einem Wechsel auf einen anderen PC die Software nicht gleichzeitig noch auf dem alten PC ausgeführt werden kann.
Sicherheit vor Verlust der Lizenz durch Viren und andere Schadsoftware	Die Programmierung (Anlegen, Ändern, Löschen) einer Lizenz in einem CmStick ist durch Kryptographie abgesichert. Nur Sie mit Ihrer FSB können Einträge löschen. Damit ist kein Virus in der Lage die Lizenzen beim Lizenznehmer zu zerstören.

Tabelle 8: Vorteile der Hardware

6.3 Ein Lizenzeintrag - viele Schlüssel

Die Software wird zur Laufzeit auf dem PC des Lizenznehmers entschlüsselt. Die Kommunikation zwischen der Software und der Lizenz ist dabei verschlüsselt (bei CodeMeter bis in den CmStick hinein). Die verschlüsselte Kommunikation verhindert, dass mit einfachen Mitteln ein Record-Playback an der Schnittstelle zu einem Crack führt.

Um eine weitere Sicherheitsschicht einzufügen, verwendet WIBU-SYSTEMS das Konzept von wechselnden Schlüsseln.

Jeder Lizenzeintrag stellt einen Satz von 4 Milliarden verschiedenen Schlüsseln zur Verfügung, der zum Schutz der Software verwendet wird. Diese Schlüssel werden im CmStick / im CodeMeterAct Modul durch eine Ableitung gebildet. Dabei werden für CodeMeter und CodeMeterAct unterschiedliche geheime Schlüssel verwendet.

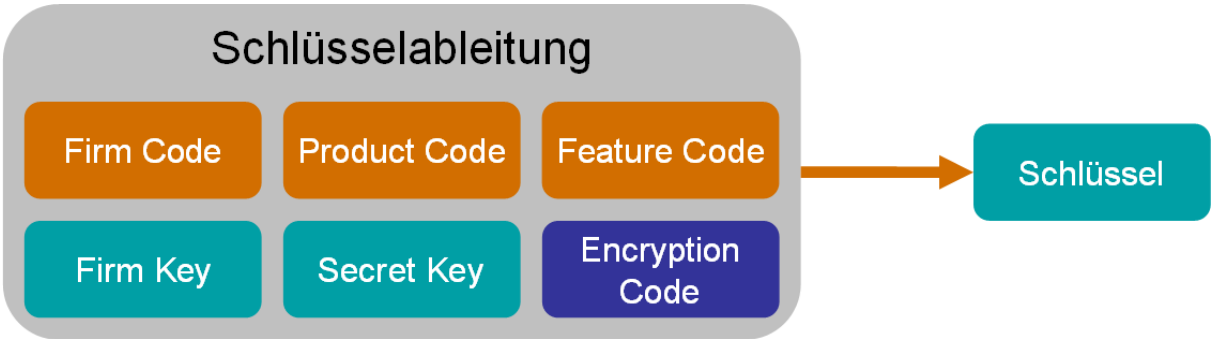


Abbildung 12: Schlüsselableitung

Firm Code, Product Code und Feature Code sind die sichtbaren Bestandteile des Schlüssels. Diese programmieren Sie in den CmStick bzw. die Lizenzdatei. Der Lizenznehmer sieht diese Bestandteile im CodeMeter WebAdmin, die den Lizenzeintrag charakterisieren.

Der Firm Key ist ein geheimer Bestandteil des Lizenzgebers. Der Lizenzgeber kann den Firm Key bei CodeMeter frei wählen und in seine FSB schreiben. In der Regel wird der von WIBU-SYSTEMS initial ausgelieferte Firm Key verwendet. Beim Programmieren eines CmSticks bzw. einer Lizenzdatei wird der Firm Key in diese übertragen.

Der Secret Key ist ein weiterer geheimer Bestandteil von CodeMeter / CodeMeterAct, der bei beiden Kopierschutzsystemen unterschiedlich erzeugt und verwendet wird.

Secret Key, Firm Key, Firm Code, Product Code und Feature Code sind für einen Lizenzeintrag fix. Der Encyrption Code hingegen kann zur Laufzeit geändert werden. Durch die Veränderung des Encryption Codes können Sie mit wechselnden Schlüsseln arbeiten.

Die Kunst besteht nun darin, das Konzept der wechselnden Schlüssel durch geeignete Methoden in Ihre Software zu integrieren. Z.B. durch die Verschlüsselung der gleichen Daten mit unterschiedlichen Schlüsseln vor der Auslieferung und der zufälligen Auswahl eines Schlüssels beim Entschlüsseln zur Laufzeit.

Bei der automatischen Integration mit dem AxProtector und der Integration mit dem Wibu Universal Protection Interface (siehe 7. Software Integration) brauchen Sie sich um diese Methoden gar nicht zu kümmern. Dies erledigen die Tools von WIBU-SYSTEMS automatisch für Sie. Und neue Methoden sind mit den Updates dieser Tools automatisch beim erneuten Verschlüsseln Ihrer Software integriert. Ohne dass Sie den Quelltext ändern oder Ihre Software neu kompilieren müssen.

6.4 CodeMeter und CodeMeterAct gleichzeitig

CodeMeter und CodeMeterAct basieren auf unterschiedlichen Schlüsseln. Daher können Daten, die für CodeMeter verschlüsselt sind, nicht mit CodeMeterAct entschlüsselt werden. Um dennoch ein sicheres und flexibles Lizenzmanagement zu ermöglichen, arbeiten die Tools von WIBU-SYSTEMS mit einer zweistufigen Verschlüsselung.

Verschlüsseln:

- Es wird ein zufälliger Schlüssel gebildet.
- Die Daten werden mit diesem zufälligen Schlüssel verschlüsselt.
- Der Schlüssel wird mit CodeMeter und / oder CodeMeterAct verschlüsselt (ggf. mehrmals mit unterschiedlichen Encryption Codes). Diese Schlüssel werden verschlüsselt als Schlüsselpool an die Daten angehängt.

Entschlüsseln:

- Es wird die passende CodeMeter oder CodeMeterAct Lizenz gesucht.
- Es wird aus dem Schlüsselpool ein für diese Lizenz passender Schlüssel ausgesucht.
- Mit dem ausgesuchten Schlüssel wird der eigentliche Schlüssel entschlüsselt.

- Mit dem eigentlichen Schlüssel werden die Daten entschlüsselt.

Diese zweistufige Verschlüsselung wird automatisch im AxProtector, bzw. im Wibu Universal Protection Interface verwendet. Damit erzeugen Sie eine Software, die wahlweise mit CodeMeter oder CodeMeterAct läuft. Neben dieser Flexibilität bietet die zweistufige Verschlüsselung auch einen deutlichen Performancegewinn gegenüber einer kompletten Verschlüsselung über den Dongle.

Natürlich können Sie das oben beschriebene Verfahren auch selbst in Ihrer Software implementieren.

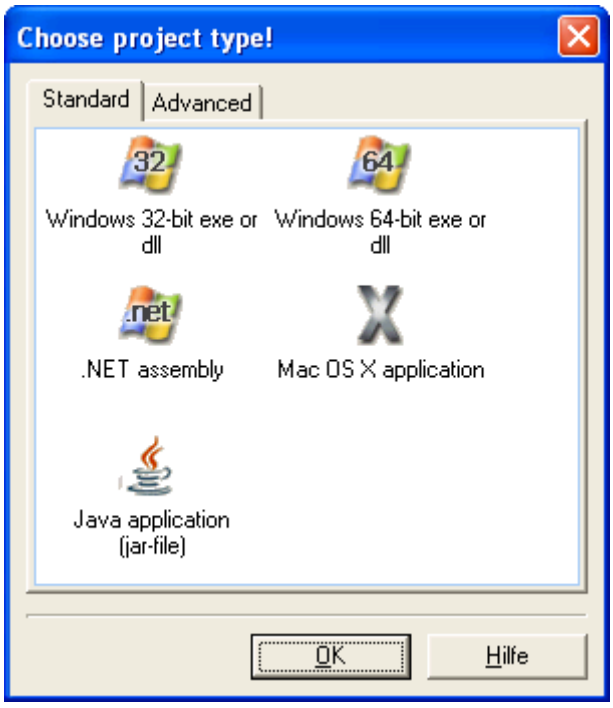
7 Software Integration

Für die Integration in die Software bietet WIBU-SYSTEMS Ihnen drei Möglichkeiten:

- automatisch mit dem AxProtector,
- individuell mit dem Softwareschutz-API Wibu Universal Protection Interface (WUPI) und dem darin enthaltenen IxProtector zum Schutz auf Funktionsebene,
- mit dem Kern-API.

7.1 AxProtector

Der AxProtector ist ein Werkzeug, das die fertige Anwendung (Exe, Dll oder Jar) nachträglich verschlüsselt.



Die Produktfamilie AxProtector umfasst:

- AxProtector (Schutz für native Windows 32-Bit und 64-Bit Anwendungen, Schutz für Mac OS X Anwendungen)
- AxProtector für .NET (Schutz für .NET Assemblies auf Methoden-Ebene)
- AxProtector für Java (Schutz für Java Anwendungen auf Klassen-Ebene)

Für die Verwendung des AxProtector stehen Ihnen eine grafische Oberfläche und ein Kommandozeilentool für die Integration in Ihre automatischen Build-Prozesse zur Verfügung.

Im AxProtector können Sie das Kopierschutzsystem wählen. Sie können eine Anwendung erzeugen, welche nur mit CodeMeter, nur mit CodeMeterAct oder mit beiden gleichzeitig funktioniert.

Der AxProtector bietet Ihnen einen sehr einfach zu implementierenden, sicheren Schutz gegen Raubkopien und Reverse Engineering. Sie nehmen einfach die kompilierte Anwendung und verschlüsseln diese mit dem AxProtector. Der AxProtector fügt selbstständig Code in Ihre Anwendung ein, der die verschlüsselten Teile zur Laufzeit entschlüsselt. Neben der Entschlüsselung enthält dieser Code auch Überprüfungen der Integrität der Anwendung sowie Erkennungsmechanismen für typische Hacker-Tools.

Im Fall des Erkennens von Hacker-Tools leitet der AxProtector sofort Gegenmaßnahmen ein, vom einfachen Beenden Ihrer Software bis zum permanenten Sperren der Lizenz. Dabei bestimmen Sie selbst, nach welchen Hacker-Tools gesucht wird und wie der AxProtector reagieren soll.

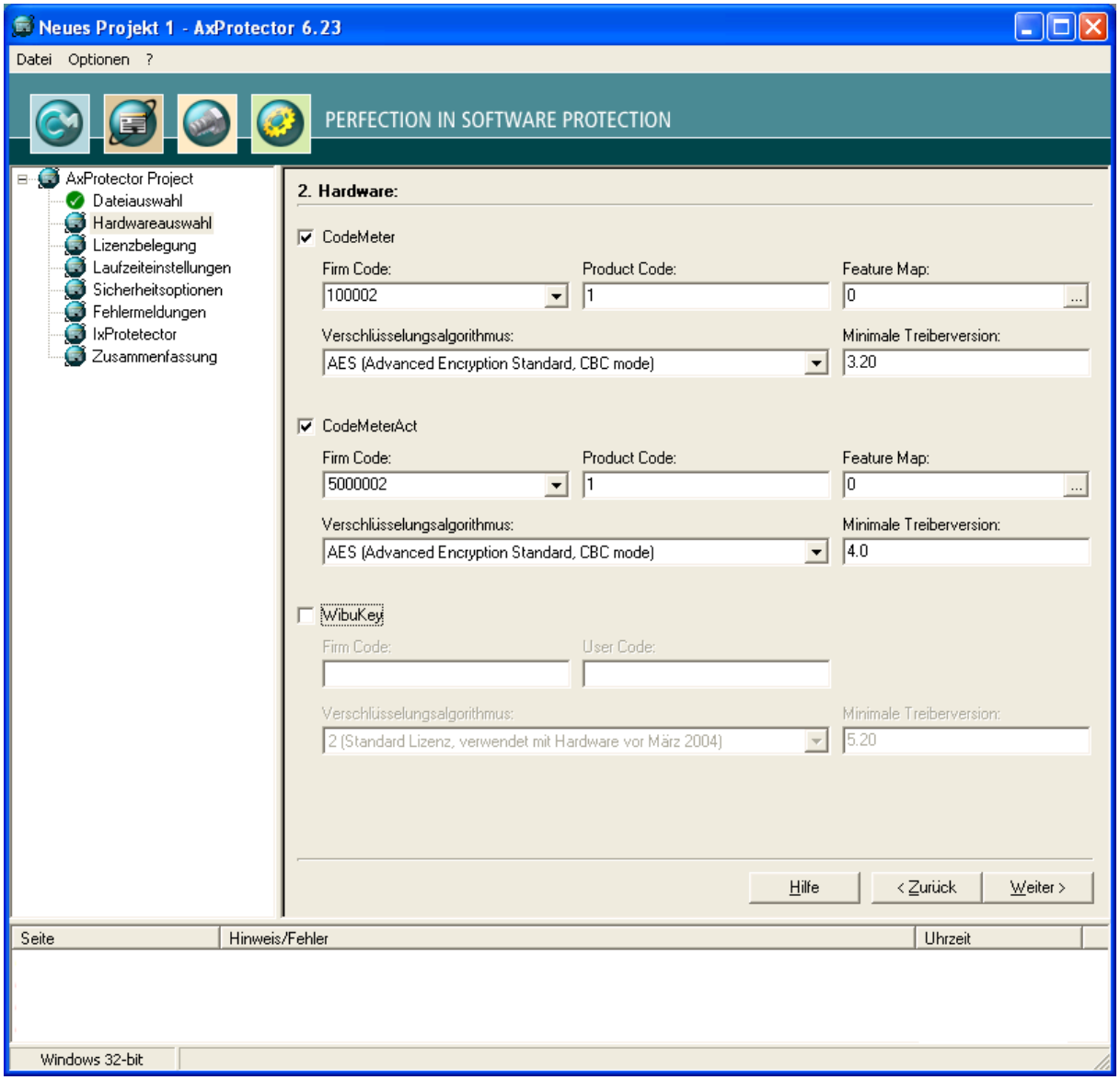


Abbildung 13: Auswahl von CodeMeter und CodeMeterAct im AxProtector

Zusätzlich zur Sicherheit bietet Ihnen der AxProtector auch viele Komfortfunktionen. Er belegt die entsprechende Lizenz automatisch auf dem Lizenzserver beim Starten der Anwendung und gibt diese beim Beenden wieder frei. Mit einer konfigurierbaren Laufzeit-Überprüfung (Intervall) stellt der AxProtector sicher, dass Ihre Software nur läuft, wenn sich die Lizenz permanent auf dem Rechner befindet (d.h. wenn der Dongle nicht abgezogen wird).

Auch im Fehlerfall entscheiden Sie selbst, wie sich Ihre Anwendung verhalten soll. Sie bestimmen, ob Fehlermeldungen angezeigt werden und wie diese aussehen. Über eine Dll-Schnittstelle können Sie die Fehlermeldungen selbst implementieren. Auf diesem Weg realisieren Sie zum Beispiel die Aktivierung einer Lizenz oder die Programmierung eines CmSticks in Ihrem eigenen Design mit den von Ihnen gewünschten Abläufen in einer automatisch geschützten Anwendung.

7.2 Das Softwareschutz-API: Wibu Universal Protection Interface (WUPI)

Der AxProtector bietet Ihnen einen umfassenden Schutz. Für alle Fälle, die nicht durch den AxProtector realisierbar sind, bietet Ihnen WIBU-SYSTEMS mit dem Softwareschutz-API Wibu Universal Protection Interface (WUPI) eine einfache Schnittstelle. Der Einsatz von WUPI ist in den folgenden Anwendungsfällen zu empfehlen:

- Schutz von einzelnen Modulen in Ihrer Software (einer ausführbaren Datei), die Sie separat lizenzieren wollen. Der AxProtector verschlüsselt eine ausführbare Datei immer komplett mit einer Lizenz.

Zusatzmodule, die andere Lizenzen benötigen und das entsprechende Fehlerhandling können Sie mit WUPI realisieren.

- Abrechnung von Aktionen (pay-per-use, pay-per-print, …) in Ihrer Software, bei dem Sie zu einem bestimmten Zeitpunkt einen Unit Counter herunter zählen wollen. Der AxProtector kann wahlweise beim Starten der Anwendung oder in einem von Ihnen definierten Intervall einen Unit Counter herunter zählen. Soll dies beim Eintreten eines Ereignisses erfolgen (falls Sie Ihre Software z.B. pro gedruckte Seite lizenzieren möchten, ist dies nach dem Ausdrucken einer Seite), dann bietet Ihnen WUPI hier ebenfalls einfache Funktionen.
- Erhöhung der Sicherheit Ihrer Anwendung, indem Sie selbst bestimmen, welche Teile Ihrer Software wann entschlüsselt und wann wieder verschlüsselt werden. Auch hier müssen Sie nicht auf die Sicherheit des AxProtectors verzichten, denn WUPI und der AxProtector können gleichzeitig verwendet werden.

WUPI ist für viele Programmiersprachen und Plattformen verfügbar. WUPI enthält einfache Funktionsaufrufe, die in einer Dll gekapselt sind. Während der Implementierung von WUPI arbeiten Sie mit IDs für Ihre einzelnen Module, d.h. Sie müssen Firm Code und Product Code, ja sogar das Kopierschutzsystem noch nicht festlegen. Nachträglich – durch den AxProtector – wird dann in der kompilierten Anwendung die WUPI-Dll gegen eine statische Implementierung ausgetauscht und die IDs in Firm Code und Product Code übersetzt. Dabei kann eine ID auch wahlweise CodeMeter und CodeMeterAct gleichzeitig unterstützen.

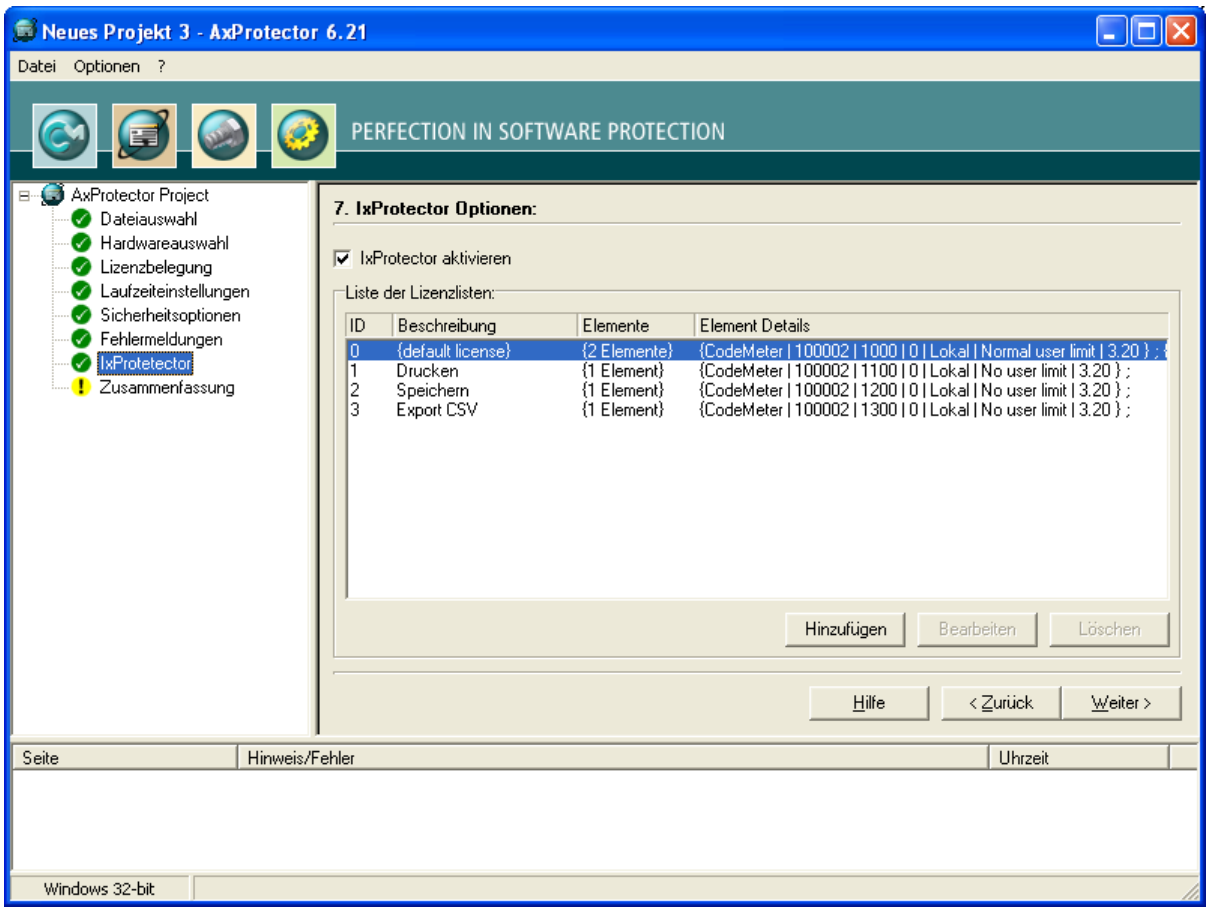


Abbildung 14: Nachträgliche Definition der Lizenzdetails mit dem AxProtector

Dieses Vorgehen hat viele Vorteile für Sie:

- Sicherheit einer statischen Bibliothek.
- Nachträgliche Bestimmung des Kopierschutzsystems, d.h. Sie können nachträglich zwischen CodeMeter und CodeMeterAct wechseln ohne neu kompilieren zu müssen.
- Trennung von Lizenzdetails und Implementierung vereinfacht die Implementierung.

- Ständig aktuelle Mechanismen (und damit aktuelle Sicherheit) durch neue Verschlüsselung mit dem AxProtector.

Die WUPI-Funktionen im Überblick:

Funktion	Bemerkung
WupiAllocateLicense (License: Integer)	Belegt die Lizenz, die im AxProtector mit der Id = LicenseId definiert wurde. Falls die Definition im AxProtector CodeMeter und CodeMeterAct enthält, dann wird die zuerst definierte Lizenz zuerst gesucht. Ist diese nicht vorhanden, dann wird die zweite Lizenz gesucht. Eine Definition kann beliebig viele optionale Lizenzen enthalten, auch mit dem gleichen Kopierschutzsystem.
WupiCheckLicense (LicenseId: Integer)	Führt kryptographische Funktionen aus, um die Lizenz zu überprüfen. Führt automatische ein WupiAllocateLicense durch.
WupiFreeLicense (LicenseId: Integer)	Gibt die Lizenz, die im AxProtector mit der Id = LicenseId definiert wurde, wieder frei.
WupiQueryInfoId (LicenseId: Integer, Type: Integer)	Entsprechend Type werden Informationen aus dem gerade belegten Lizenzeintrag abgerufen. Zum Beispiel: der Stand des Unit Counters, die gesetzte FeatureMap, die verbleibenden Tage bis zum Ablaufdatum.
WupiDecryptCode (FunctionId: Integer)	Die im AxProtector mit Id = FunctionId definierte Funktion wird entschlüsselt. Dieser Aufruf muss vor dem Ausführen einer verschlüsselten Funktion erfolgen, da die Software sonst abstürzen würde.
WupiEncryptCode (FunctionId: Integer)	Die im AxProtector mit Id = FunctionId definierte Funktion wird wieder verschlüsselt. Rufen Sie diese Funktion nach dem Ausführen Ihrer geschützten Funktion auf, damit diese wieder sicher geschützt im Speicher liegt.
WupiCheckDebugger (LicenseId: Integer)	Mit dieser Funktion können Sie den Debugger-Check aus dem AxProtector aufrufen. Sollte der Debugger-Check einen Debugger erkennen, kann (je nach gewählter Einstellung) die im AxProtector mit der Id = LicenseId definierte Lizenz permanent gesperrt werden.
WupiDecreaseUnitCounter (LicenseId: Integer, Units: Integer)	Mit dieser Funktion können Sie einen Unit Counter in der im AxProtector mit der Id = LicenseId definierten Lizenz die gewünschte Anzahl herunterzählen. Dies können Sie verwenden, wenn Sie eine Pay-Per-Click Funktionalität in Ihre Software integrieren möchten. Besitzt die Lizenz keinen Unit Counter, dann liefert die Funktion keinen Fehler zurück, d.h. Sie können durch die Programmierung der Lizenz festlegen, ob der Lizenznehmer eine Pay-Per-Click oder eine unlimitierte Lizenz erhält.
WupiGetNativeHandleId (LicenseId: Integer)	Mit dieser Funktion können Sie sich ein Handle holen, welches Sie in dem nativen API weiterverwenden können. Damit können Sie auf die erweiterten Funktionen des Low-Level API zugreifen.

Tabelle 9: WUPI-Funktionen im Überblick (Auszug)

7.3 Das Kern-API

Neben dem AxProtector und WUPI bietet Ihnen WIBU-SYSTEMS ein Kern-API, das Sie in allen anderen Fällen verwenden können.

CodeMeter / CodeMeterAct arbeiten mit diesem Kern-API. Lediglich der Firm Code unterscheidet sich bei den beiden Systemen. CodeMeterAct bietet zusätzliche Funktionen, die eine Integration des Aktivierungsprozesses in die eigene Software ermöglichen.

Der Einsatz des Kern-API ist in speziellen Anwendungsfällen empfohlen, z.B. zur verschlüsselten Kommunikation mit externen Devices, wenn ein fester Schlüssel verwendet werden soll.

Das Kern-API ist für die folgenden Programmiersprachen verfügbar. Für das C-API stehen eine Vielzahl an Interfaces für weitere Programmiersprachen (Delphi, Fortran, Visual Basic, …) zur Verfügung.

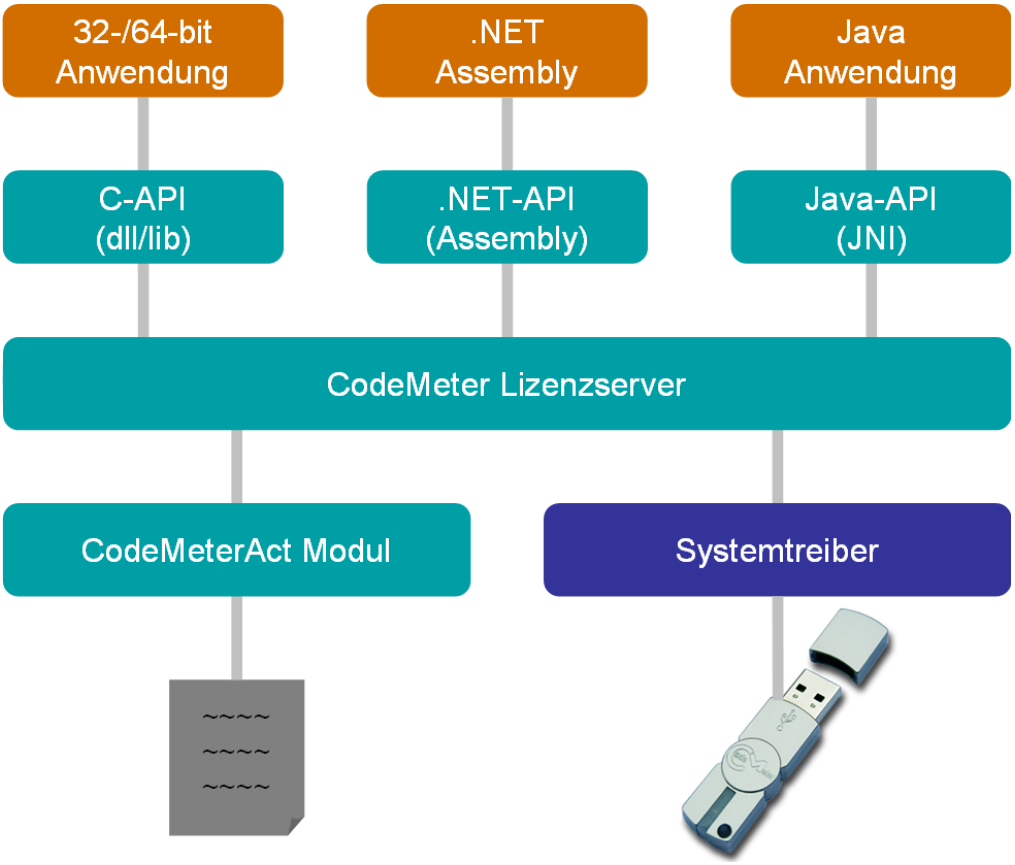


Abbildung 15: Verfügbare CodeMeter APIs

Die Grundfunktionalität ist durch CmAccess (Lizenz belegen), CmCrypt (Daten ver- oder entschlüsseln) und CmRelease (Lizenz freigeben) gegeben.

Wenn Sie CodeMeter und CodeMeterAct gleichzeitig verwenden möchten, dann können Sie die gleichen Funktionsaufrufe und Konzepte verwenden, denn CodeMeter und CodeMeterAct unterscheiden sich nur durch den Firm Code.

8 Lizenzverwaltung - Backoffice Integration

8.1 Das Prinzip – Ticketsystem

Die Integration des Softwareschutzes in die Software ist ein wichtiger Punkt, der vor allem die Sicherheit des Systems stark beeinflusst. Demgegenüber entscheidet eine effiziente Integration in Vertriebs-, Produktions- und Supportprozesse über die Bedienbarkeit eines Systems und damit über die Akzeptanz bei Kunden und eigenen Mitarbeitern. Diese Einbindung fassen wir unter Backoffice Integration (BOI) zusammen.

Im Mittelpunkt dieser „Backoffice Integration" steht CodeMeter License Central. CodeMeter License Central ist ein einheitliches Ticketsystem für CodeMeter und CodeMeterAct.

Wenn Sie einen CmStick oder eine CodeMeterAct-Lizenzdatei für ein bestimmtes Produkt programmieren möchten, schicken Sie eine entsprechende Anfrage mit der Artikelnummer an CodeMeter License Central. Sie erhalten ein eindeutiges Ticket zurück. Dies geschieht meist im Rahmen eines Verkaufs dieses Artikels, daher nennen wird diese Schnittstelle Sales-Interface. Das Ticket stellt die Berechtigung dar, die „gekauften" Produkte in einen CmStick oder eine CodeMeterAct-Lizenzdatei zu programmieren.

Sie entscheiden, ob Sie die Programmierung der Lizenz gleich selbst vornehmen, später erledigen, oder das Ticket an Ihren Kunden weitergeben. Ihr Kunde kann sich dann die gekauften Lizenzen zu einem beliebigen Zeitpunkt in einen beliebigen CmStick bzw. in eine beliebige CodeMeterAct-Lizenzdatei abholen. Das Interface zum Abholen von Lizenzen nennen wir Depot-Interface.

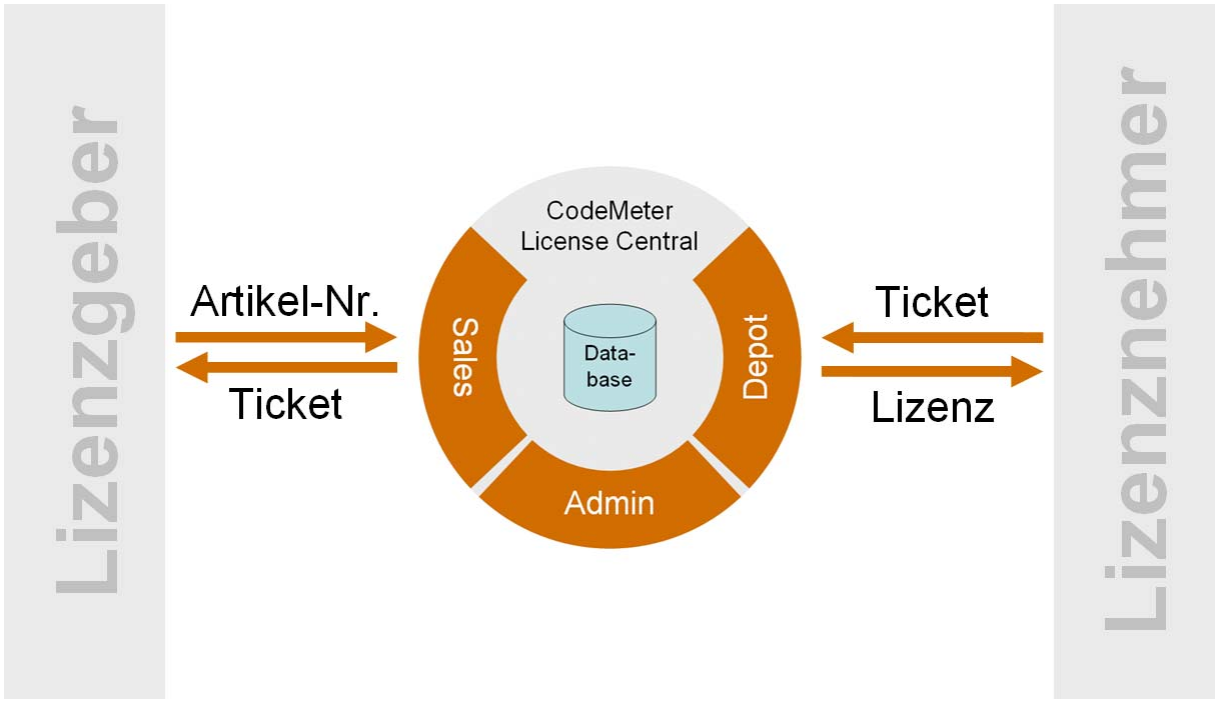


Abbildung 16: Abholung einer Lizenz durch den Lizenznehmer

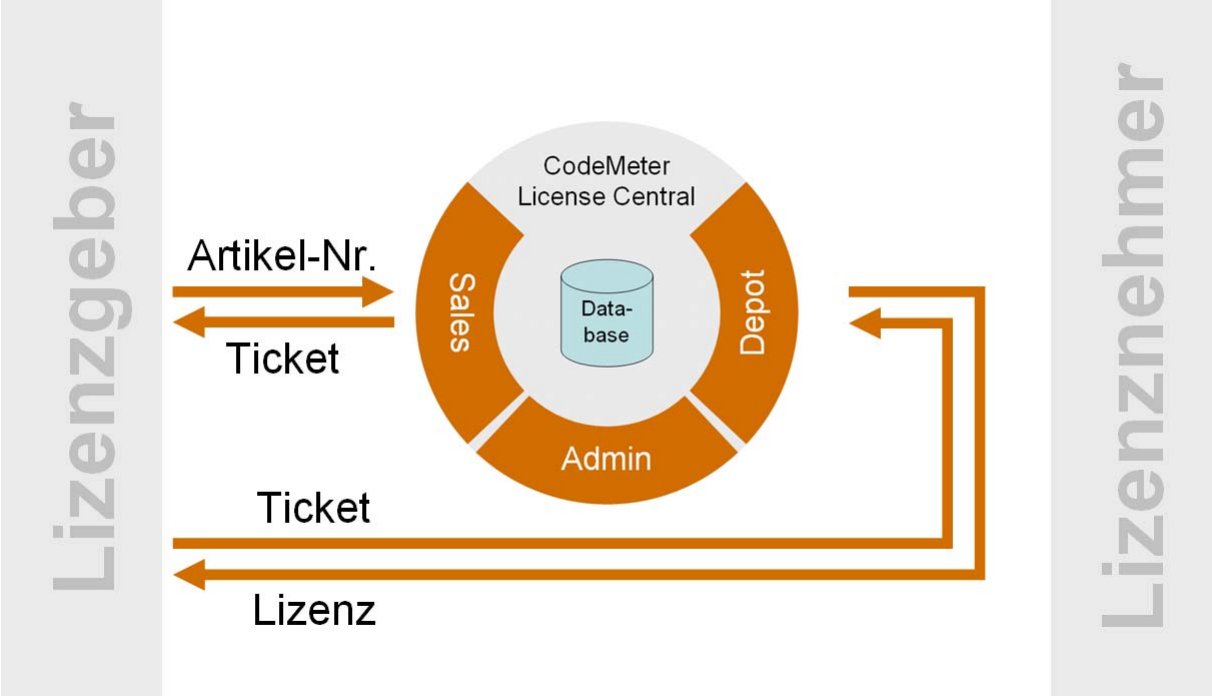


Abbildung 17: Abholung einer Lizenz durch den Lizenzgeber

Neben dem Depot-Interface und dem Sales-Interface besitzt die CodeMeter License Central ein Admin-Interface. Das Admin-Interface bietet Ihnen Funktionen für die Definition von Lizenzeigenschaften (z.B. Ablaufdatum, Lizenzanzahl), die Verwaltung der Zugriffsrechte, die Erzeugung von Statistiken und Berichten sowie die Durchführung von Support-Tätigkeiten.

8.2 CodeMeter License Central – Der Kern

8.2.1 Architektur

Der Kern von CodeMeter License Central besteht aus einer Datenbank und Webservices für das Sales-Interface, das Depot-Interface und das Admin-Interface.

Die Webservices sind plattformunabhängig in Java verfügbar. Voraussetzung ist ein Tomcat Application Server.

Die Webservices stellen eine SOAP basierte Schnittstelle zur CodeMeter License Central zur Verfügung. Die komplette Kommunikation mit der CodeMeter License Central erfolgt über diese Webservices. Die Webservices haben eine interne Schnittstelle zur Datenbank.

Als Datenbank werden MySQL (Windows / Linux) und MSSQL (Windows) unterstützt. Weitere Datenbanken können auf Anfrage integriert werden.

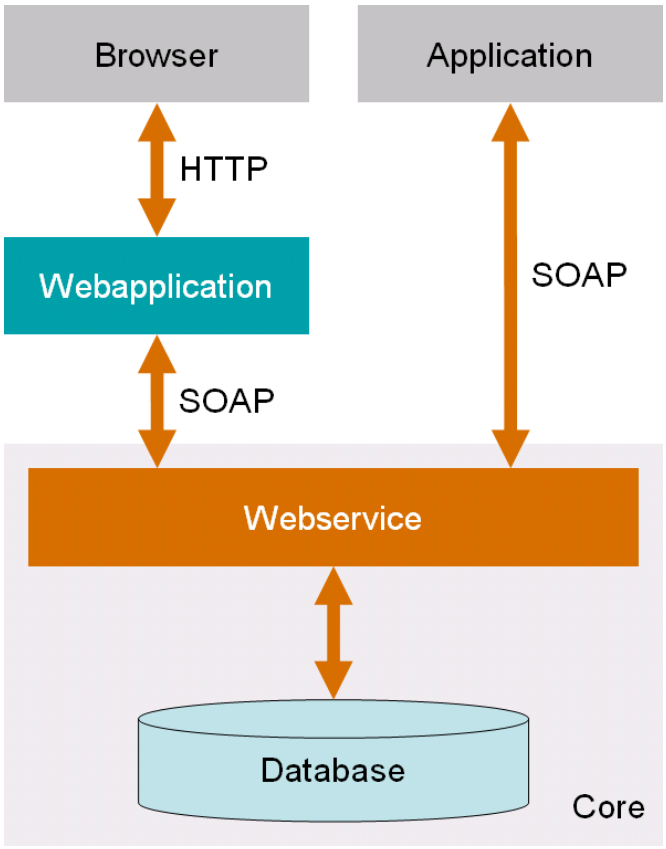


Abbildung 18: SOAP-Zugriffe auf die CodeMeter License Central

Die SOAP-Zugriffe bietet Ihnen eine maximale Flexibilität. Es ist möglich von einer Anwendung heraus direkt auf CodeMeter License Central zuzugreifen. Neben dem direkten Zugriff ist auch der Zugriff über eine Webanwendung mittels eines Webbrowsers möglich.

Diese beiden Möglichkeiten gelten für alle drei Interfaces. Auch eine Aufteilung ist möglich. Sie können zum Beispiel das Depot-Interface direkt aus Ihrer ausgelieferten Software heraus aufrufen, während die internen Schnittstellen, das Admin- und das Sales-Interface über Webseiten angesprochen werden.

Die SOAP-Funktionen stehen Ihnen als dokumentiertes CodeMeter License Central API (CmLC-API) für die Integration in eigene Anwendungen zur Verfügung.

8.2.2 Grundfunktionen

Sales-Interface

Das Sales-Interface nimmt Vorgänge entgegen. Sie schicken die Artikelnummer des Produktes, das ausgeliefert werden soll, sowie optional eine Kundenummer und eine Auftragsnummer an das Sales-Interface. Das Sales Modul liefert Ihnen dann das passende Ticket zurück.

Bei wiederkehrenden Vorgängen (z.B. CheckPoints, Verlängerung von Lizenzen) kann auch die originale Auftragsnummer mitgegeben werden. In diesem Fall wird das bestehende Ticket um einen Abholvorgang erweitert. D.h. der Lizenznehmer kann die Lizenz mit seinem bereits bekannten Ticket erweitern. Dies spart Ihnen den Verwaltungsaufwand neuer Tickets und erleichtert dem Lizenznehmer das Arbeiten. Sie können dann sogar mit dem vorhandenen Ticket - direkt per SOAP aus Ihrer Anwendung heraus - die Lizenz automatisch erweitern oder verlängern.

Ja nach Artikelkonfiguration können bei einem Vorgang auch Parameter dynamisch übergeben werden. Damit können Sie zum Beispiel die Anzahl der Netzwerklizenzen übergeben, oder den Namen des Lizenznehmers, wenn dieser in Customer Owned License Information geschrieben werden soll.

Depot-Interface

Mit Hilfe des Depot-Interface können Lizenzen abgeholt werden. Das Abholen erfolgt durch das Hochladen einer Kontext Datei und das Herunterladen einer Update Datei. Nach dem Einspielen der Update Datei kann optional eine neue Kontext Datei hochgeladen werden, um das Einspielen der Lizenz zu quittieren. Dieser Prozess kann natürlich in einem Schritt durchgeführt werden, so dass der Lizenznehmer nur „die Lizenz abholt".

Das Depot-Interface bietet Ihnen zwei Möglichkeiten um Lizenzen abzuholen:

- **Direkt** (Der PC mit dem zu programmierenden CmStick verfügt über eine Internetverbindung.)
- **Indirekt** (Über Dateiaustausch werden die Freischaltdaten auf einen anderen PC übertragen.)

Neben dem Abholen von Lizenzen bietet das Depot-Interface auch Methoden zum Zurückgeben von Lizenzen.

Derzeit ist das Zurückgeben von Lizenzen noch nicht implementiert.

Nach dem Zurückgeben einer Lizenz bekommt der Lizenznehmer ein neues Ticket. Dies erhält er erst nach dem Hochladen der Quittung. Mittels des neuen Tickets kann der Lizenznehmer die Lizenz dann auf einen anderen PC übertragen, bzw. kann er diese Lizenz auch Weiterverkaufen und dem Käufer das Ticket geben. Wenn Sie Weiterverkaufen erlauben möchten, dann schalten Sie das Zurückgeben von Lizenzen einfach ein. Standardmäßig ist das Zurückgeben von Lizenzen - damit auch das Weiterverkaufen - abgeschaltet. Wenn der Anwender Lizenzen zurückgeben möchte, dann sollten Sie den Kaufpreis erst nach dem Hochladen der Quittung erstatten

Im Depot-Interface ist es zusätzlich möglich Informationen über die gekauften und aktivierten Lizenzen abzurufen.

Je nach Produktkonfiguration könne Sie dem Lizenznehmer das Kopierschutzsystem (CodeMeter / CodeMeterAct) vorgeben oder ihm die Wahl - ob Hardware oder Aktivierung – selbst überlassen.

Admin-Interface

Das Admin-Interface besteht aus den Teilen Lizenzkonfiguration, Auswertungen, Support, und Benutzerverwaltung.

In der Lizenzkonfiguration verwalten Sie die Lizenzeigenschaften und die dazugehörigen Artikelnummern. Hier legen Sie für jede Lizenz individuell fest, welche Parameter fest programmiert werden und welche im Sales-Interface übergeben werden können.

Im Statistik-Modul können Sie die Daten aus CodeMeter License Central auswerten, zum Beispiel: „Welcher Kunde hat welche Lizenzen in welchen CmSticks?"

Für das Abschließen von offenen Vorgängen (z.B. Quittung nicht hochgeladen), die Freigabe von weiteren Aktivierungen und das Bearbeiten von Blacklist-Einträgen steht Ihnen das Support-Modul zur Verfügung.

Die Benutzerverwaltung bietet Ihnen die Möglichkeit, die Zugriffsrechte auf CodeMeter License Central zu konfigurieren. Die Authentifizierung kann über Benutzername und Passwort, IP-Adresse oder CmStick erfolgen. So können Sie zum Beispiel festlegen, dass ein Vertriebspartner mit wechselnden IP Adressen sich mit CmStick authentifizieren muss, während sich ein automatischer Sales-Connector über IP Adresse anmeldet.

8.3 CodeMeter License Central Desktop

Mit CodeMeter License Central Desktop stellen wir Ihnen ein Komplettpaket für den internen Einsatz zur Verfügung, das neben dem Kern fertige Webanwendungen beinhaltet, mit denen Sie auf die Funktionen von CodeMeter License Central zugreifen.

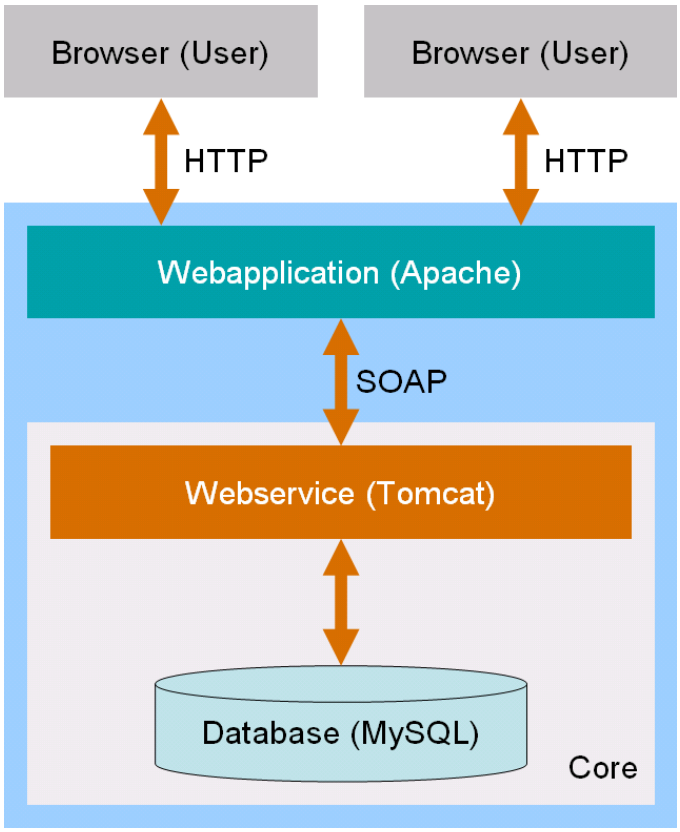


Abbildung 19: Architektur von CodeMeter License Central Desktop

CodeMeter License Central Desktop ist als fertiges Paket für ein von WIBU-SYSTEMS bereitgestelltes Linux VmWare Image verfügbar. Das Paket beinhaltet eine MySQL Datenbank, eine Tomcat Applicationserver und einen Apache Webserver.

Die Zugriffe auf CodeMeter License Central Desktop erfolgen über Webanwendungen, die in dem gleichen VmWare Image auf dem Apache Webserver laufen. Mehrere Benutzer können gleichzeitig über die Webanwendungen zugreifen, sie benötigen lediglich eine TCP/IP Verbindung zum VmWare Image mit CodeMeter License Central Desktop.

CodeMeter License Central Desktop beinhaltet die folgenden Module:

- **Sales – Manual** (Manuelles Erfassen von Vorgängen)
- **Depot – Get** (Lizenzen abholen)
- **Depot – Return** (Lizenzen zurückgeben)
- **Admin – Statistics** (Auswertungen)

- **Admin – Support** (Supporttätigkeiten)
- **Admin – Products** (Administration der CodeMeter Eigenschaften der Artikel)
- **Admin – User** (Verwaltung der Benutzer, die CodeMeter License Central Desktop verwenden dürfen)

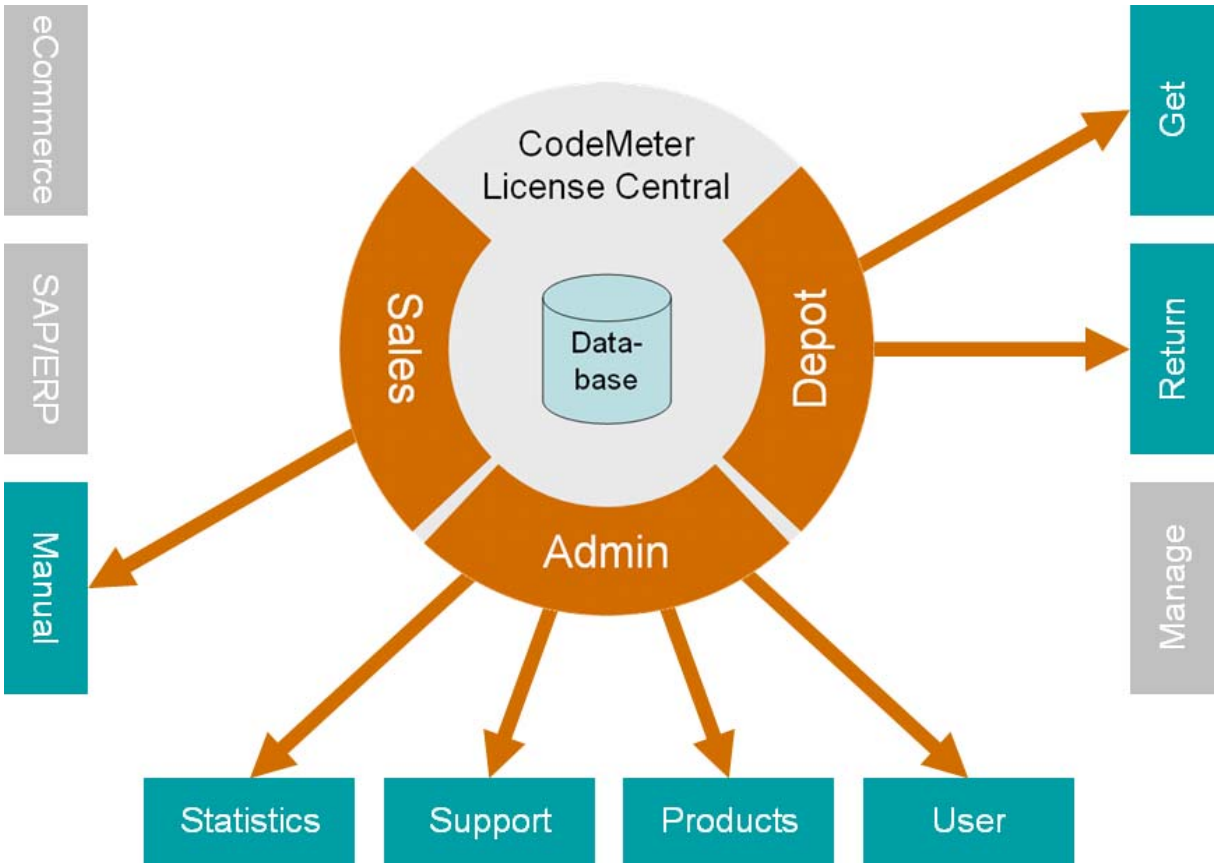


Abbildung 20: Module von CodeMeter License Central Desktop

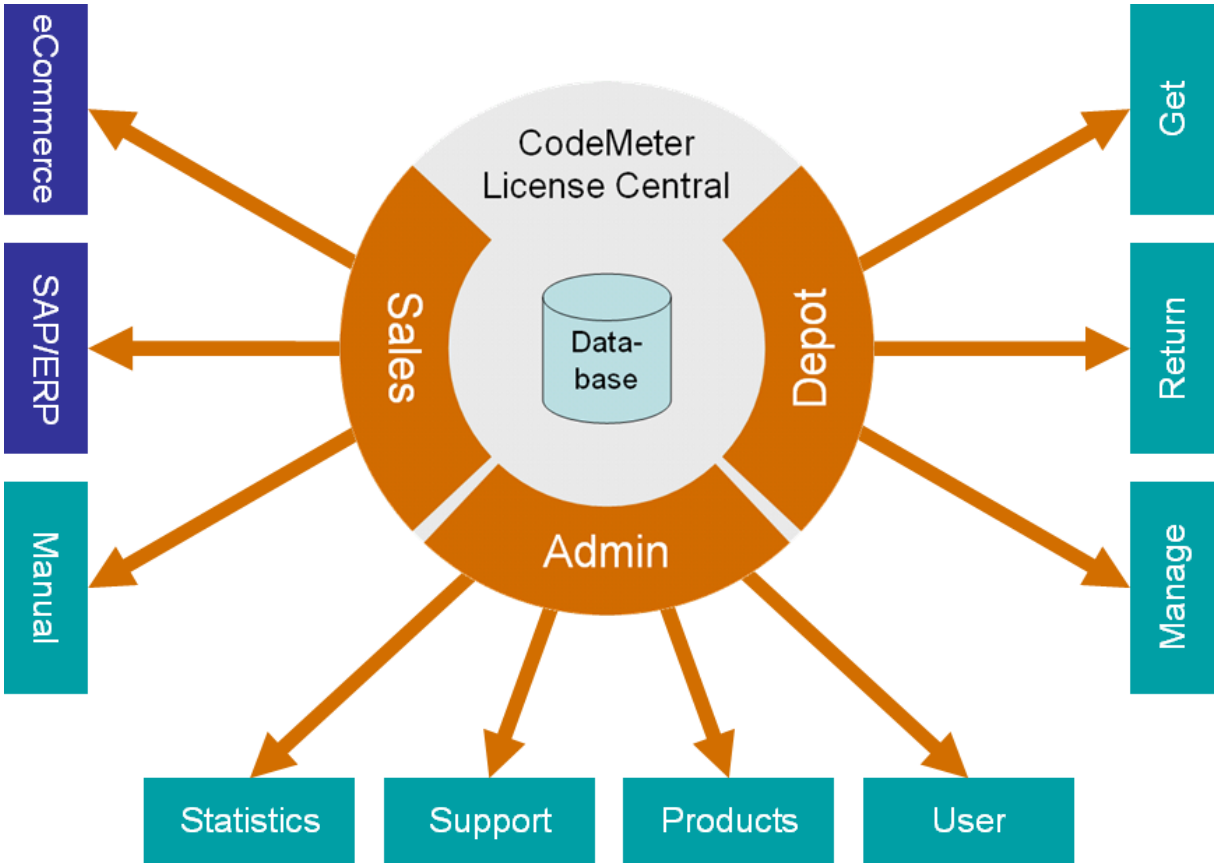


Abbildung 21: Module von CodeMeter License Central Enterprise

8.4 CodeMeter License Central Enterprise

8.4.1 Unterschiede zur Desktop Version

Im Gegensatz zu CodeMeter License Central Desktop, bei der Sie ein Komplettpaket erhalten, kann CodeMeter License Central Enterprise an Ihre Anforderungen angepasst werden.

CodeMeter License Central Enterprise bietet weitere Module, die eine automatische Integration in die Verkaufsprozesse durch Connectoren ermöglichen. Die Erzeugung der Tickets kann in CodeMeter License Central Enterprise durch ein eigenes Modul mit einem eigenen Regelwerk ersetzt werden. Auch eine verteilte Installation (Webservices, Webanwendungen und Datenbank) auf mehreren Rechnern ist möglich.

In der folgenden Tabelle finden Sie einen Vergleich des Funktionsumfangs zwischen CodeMeter License Central Enterprise und CodeMeter License Central Desktop:

Eigenschaft	Desktop	Enterprise
Core - Datenbank	MySQL	MySQL, MSSQL, weitere auf Anfrage
Core - Java Webservices	X	X
Core - Anpassbare Ticketerzeugung		X
Core - verteilte Installation		X
Sales - Manuelle Verkaufserfassung per Webseite	X	X
Sales - ERP-Connector		X
Sales - eCommerce Connector		X
Admin - Statistik per Webseite	X	X

Admin - Support Webseiten	X	X
Admin - Produktpflege Webseiten	X	X
Admin - Benutzerverwaltung (Zugriffe des Lizenzgebers) Webseiten	X	X
Depot - Lizenzen Abholen Webseite	X	X
Depot - Lizenzen Zurückgeben Webseite	X	X
Depot - Lizenzen Verwalten Webseite		X
Depot - Userverwaltung (Zugriffe des Lizenznehmers)		X

Tabelle 10: Funktionsumfang der CodeMeter License Central

8.4.2 Sales Connectoren

Um eine automatische Integration in den Verkaufsprozess zu ermöglichen muss das ERP-System oder der Online Shop nach dem erfolgreichen Verkaufsvorgang einen Prozess anstoßen.

eCommerce Connector

Viele Online Shops (Cleverbridge, ShareIt, Digital River, Element5, …) bieten standardmäßig den Aufruf eines Lizenzgenerators über SOAP nach dem Verkauf an. Da jeder Online Shop einen anderen Dialekt spricht, benötigen Sie einen eCommerce Connector, der die Daten vom Online Shop System so umwandelt, dass die CodeMeter License Central diese versteht. Der eCommerce Connector schickt dann diese Daten an das Sales-Interface und erhält das Ticket zurück. Je nach Online Shop muss das Ticket noch aufbereitet und als Lizenz-String oder Abhol-Link zurückgegeben werden. Diese Transformation übernimmt ebenfalls der eCommerce Connector.

Die Anzeige des Tickets, zum Beispiel als URL-kodierter Abhol-Link auf der Bestellbestätigungsseite, kann in den meisten Online Shops konfiguriert werden. Häufig wird das Ticket zusätzlich in die Bestellbestätigungsmail integriert.

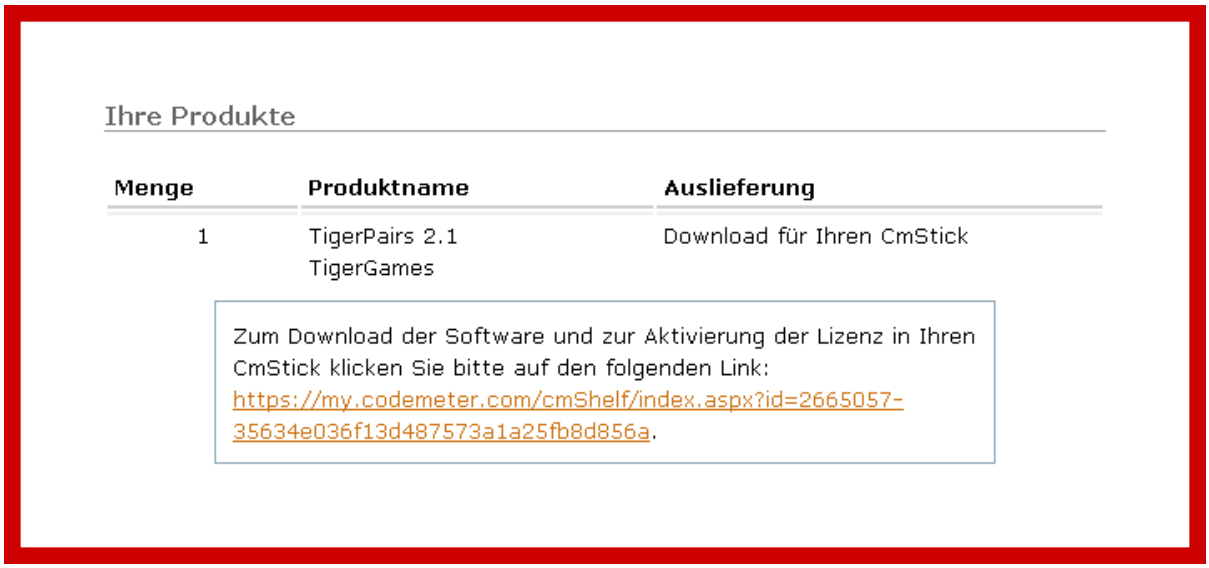


Abbildung 22: Anzeige des Tickets als Abhollink in einen Online Shop von Cleverbridge

Der eCommerce Connector authentifiziert sich gegenüber CodeMeter License Central. Auf der anderen Seite muss der eCommerce Connector daher selbst sicherstellen, dass die Anfrage vom richtigen Online Shop kam. Dies kann über IP-Range Überprüfung oder über ein individuelles Login erfolgen.

Der eCommerce Connector muss für jeden Online Shop angepasst werden.

ERP Connector

Durch einen ERP Connector erfolgt die Integration in ein ERP System, zum Beispiel SAP.

Die Anpassungen am ERP System sind dabei marginal:

1) Nach der Auftragserfassung wird der ERP Connector angesprochen. Dieser kann zum Beispiel als Dynamische Link Library realisiert sein, die direkt aus dem ERP heraus aufgerufen wird. Der Connector schickt die Auftragsdaten an CodeMeter License Central und erhält das Ticket zurück. Das Ticket gibt der Connector weiter an das ERP-System.

2) Das Ticket sollte im ERP System gespeichert und auf dem Auftrag ausgedruckt werden. Viele ERP Systeme bieten dafür benutzerdefinierte Felder.

Sollte diese Erweiterung des ERP-Systems nicht möglich sein, dann können Sie mit einer Schattendatenbank arbeiten. D.h. die Auftragsdaten werden aus dem ERP-System in diese Schattendatenbank exportiert und von dort wird dann der ERP Connector angesprochen und das Ticket weiterverarbeitet.

8.4.3 Abholung durch den Lizenznehmer

Falls der Lizenznehmer die Lizenzen direkt abholen soll, dann benötigt er einen Zugriff auf die CodeMeter License Central. Je nach geplantem Zugriff, direkt per SOAP aus der Anwendung heraus oder über einen Webseite, stellen Sie dazu den Webserver oder Webserver und Application Server in die DMZ (Demilitarisierte Zone).

In diesem Fall ist es aus Sicherheitsgründen ratsam, die Installation auf mehrere Rechner zu verteilen und die restlichen Module (Datenbank und evtl. den Application Server) hinter der inneren Firewall zu positionieren.

Die Webseiten, die der Kunde zum Abholen der Lizenz angezeigt bekommt, können an Ihr Corporate Design angepasst werden.

In der CodeMeter License Central Enterprise Edition können Sie eine Nutzerverwaltung für den Lizenznehmer aktivieren, z.B. wenn er eine größere Firma ist und mehrere Mitarbeiter Lizenzen abholen sollen. Dann kann der Lizenznehmer selbst einsehen, welche Lizenzen von welchen Mitarbeitern abgeholt wurden. In diesem Fall identifiziert sich der Nutzer nicht mit der Ticketnummer, sondern mit seinem Account.

8.5 Zusatzmodule

Über Zusatzmodule kann die Funktionalität von CodeMeter License Central erweitert und Schnittstellen zu weiteren Systemen implementiert werden.

8.5.1 One2One Marketing Modul (OZOMM)

Das One2One Marketing Modul kann bei zeitlich befristeten Lizenzen eingesetzt werden. Es ist als Zusatzmodul zu CodeMeter License Central Enterprise verfügbar und stellt eine Schnittstelle zu weiteren CRM Systemen des Lizenzgebers zur Verfügung.

Beim Versuch eine Lizenz zu verlängern, wird der SOAP Request nicht ans Depot-Interface, sondern an OZOMM geschickt.

- OZOMM überprüft anhand der Tickernummer, ob der Kunde eine Verlängerung bekommen darf
- OZOMM verlängert die Lizenz über das Sales-Interface
- OZOMM holt die Lizenz über das Depot-Interface ab
- OZOMM schickt zusätzliche Marketinginformationen an den Kunden (Angebote über Upgrades)

Für die Angebote besitzt OZOMM eine Schnittstelle zum CRM System des Lizenzgebers. Die Überprüfung, ob der Kunde die Lizenz verlängern darf, erfolgt über eine Schnittstelle zum CRM oder ERP System des Lizenzgebers.

Die Connectoren zum ERP System bzw. CRM System des Lizenzgebers werden individuell für die entsprechenden Systeme entwickelt. Diese Connectoren können die Daten online aus den entsprechenden Systemen holen bzw. diese in regelmäßigen Abständen in eine eigene Datenbank importieren.

9 Kontakt

Hauptsitz | WIBU-SYSTEMS AG
Rueppurrer Strasse 52-54 | 76137 Karlsruhe, Germany
Tel.: +49-721-93172-0 | Fax: +49-721-93172-22
E-Mail: info@wibu.de | Web: www.wibu.de

WIBU-SYSTEMS USA Inc.
110 W Dayton Street, Suite 204 | Edmonds, WA 98020-7245, USA
Tel: +1.425.775.6900 / Tel: +1-800-6-GO-WIBU (+1-800-646-9428) | Fax: +1-206-237-2644
E-Mail: info@wibu.us | Web: www.wibu.us

WIBU-SYSTEMS (Shanghai) Co. Ltd.
Room 1602, KIC66 Jin Chuang Road, Yang Pu District | 20 200433 Shanghai, VR China
Tel: +86-21-55661790 | Fax: +86-21-55661780
E-Mail: info@wibu.com.cn | Web: www.wibu.com.cn

WIBU-SYSTEMS BV
Adam Smithstraat 33 | 7559 SW Hengelo, The Netherlands
Tel :+31 (0)74 75 01 495| Fax: +31 (0)74 75 01 496
E-Mail: sales@wibu-systems.nl | Web: www.wibu-systems.nl

WIBU-SYSTEMS LTD
The Mansion, Bletchley Park, Bletchley
Milton Keynes MK3 6DS, United Kingdom
Tel: +44 (0)20 314 747 27| Fax: +44 (0)20 314 747 28
E-Mail: info@wibu.co.uk | Web: www.wibu.co.uk

WIBU-SYSTEMS NV
Drie Eikenstraat 661 | B-2650 Edegem (Antwerpen), Belgium
Tel.: +32 (0)3 400 03 14| Fax: +32 (0)3 400 28 40
E-Mail: sales@wibu.be | Web: www.wibu.be

WIBU-SYSTEMS Iberia
C. Josep M. Gironella, 1-3 | 17003 GIRONA, Spain
Tel: +34 (0) 91 414 8768 | Fax: +34 (0) 91 414 8769
E-Mail: info@wibu.es | Web: www.wibu.es