HERBST 2012

KEYnote 24

DAS WIBU-MAGAZIN

Software-Schutz als Prozess

Themen

- Der Mythos Signatur
- Projektschutz durch Verschlüsselung
- CodeMeter® in virtuellen Umgebungen

WIBU SYSTEMS

Inhalt

INFORMATION
Quo Vadis CodeMeter? 3

KNOW-HOW
Der Mythos Signatur 4

PRODUKT
Angepasstes WebDepot 6

KNOW-HOW
Softwareschutz als Prozessbestandteil 8

KNOW-HOW
Projektschutz durch Verschlüsselung 10

PRODUKT
CodeMeter und Virtualisierung 12

HIGHLIGHTS
Aktuelles in Kürze 14

CASE STORY
Erfolgsgeschichte Sirona 15

INFORMATION
Wibu-Systems informiert 16

Sehr geehrte Kunden und Partner,

integrieren Sie Lizenzierung und Schutz Ihrer Software optimal in Ihre Prozesse! Das Titelthema dieses KEYnote-Magazins zeigt Ihnen, wie Sie dies mit geringem Aufwand erreichen.

Wir haben unsere Investitionen in Forschung und Entwicklung erhöht, um Sie mit leistungsfähigen Tools zu unterstützen. Wir haben Entwicklung, Innovationsmanagement, Support und Consulting personell aufgestockt und stehen Ihnen auch vor Ort zur Verfügung, um maßgeschneiderte Konzepte mit Ihnen zu entwickeln und Ihre Umsetzung zu begleiten. Einige neue Mitarbeiter stellen wir Ihnen auf der Seite 14 vor; wie wir Innovation mit Kontinuität verbinden, lesen Sie in „Quo Vadis CodeMeter?".

In „Der Mythos Signatur" lesen Sie, was asymmetrische Kryptographie mit Softwarelizenzierung zu tun hat und wie diese vorteilhaft mit CodeMeter eingesetzt wird. Weiteres Thema ist der Schutz der Daten Ihrer Anwendung und wie dieser mit CodeMeter realisiert werden kann. Setzen Sie oder Ihre Kunden bereits auf Virtualisierung? Mit CodeMeter sind Sie bestens dafür gerüstet, egal ob mit CmActLicense aktivierungsbasiert oder mit CmDongles, die Sie auch in virtuellen Umgebungen einfach nutzen können, beispielsweise mit Dongleservern von SEH. In einem weiteren Beitrag lesen Sie über die Anpassung des Webdepots der CodeMeter License Central. Dies ist die Weboberfläche, die Ihre Kunden oder Mitarbeiter zu sehen bekommen, wenn Sie über das Internet oder Intranet Lizenzen abrufen. Am Ende des Magazins lesen Sie über unsere neuen Webinare, die Ihnen mit minimalem Aufwand ohne Reisen wertvolles Know-how zu CodeMeter vermitteln. Der Einsatz von CodeMeter in Cerec-Geräten von Sirona zeigt Ihnen eine tolle Kundenanwendung im Bereich der Zahnmedizin.

In den Beiträgen führen wir in die Themen ein. Sprechen Sie uns mit Ihren Anforderungen an. Ich wünsche Ihnen ein gutes Jahresendgeschäft 2012 und viele neue Anregungen beim Lesen dieses KEYnote Magazins. Bis bald auf einer unserer Veranstaltungen, Messen oder Webinare.

Herzliche Grüße aus Karlsruhe,

Oliver Winzenried (Vorstand)

Quo Vadis CodeMeter?

Viele Trends sind gekommen. Einige davon haben sich durchgesetzt, andere haben ihre Nische gefunden und wieder andere sind komplett verschwunden. Für die Existenz einer Firma kann das Verpassen eines Trends genauso bedrohlich sein wie die Verwendung von wertvollen Ressourcen auf Trends, die sich nicht durchsetzen. Wie stellt sich Wibu-Systems dieser Herausforderung?

Kontinuität und Innovation

Unser oberstes Ziel ist es, Ihnen ein langfristiger und stabiler Partner zu sein und Ihnen qualitativ hochwertige Lösungen und Produkte stetig in kompatibler Form zu liefern. Auf der anderen Seite unterstützen wir neue Technologien frühzeitig für Sie, wie die Vergangenheit gezeigt hat. Einen Dongle in der Bauform USB und die Unterstützung von .NET sollen nur stellvertretend zwei Punkte sein, bei denen Wibu-Systems eine Vorreiterrolle gespielt hat.

Vielleicht fragen Sie sich: Wie schafft Wibu-Systems diese Schere zwischen Kontinuität und Innovation?

Bei Wibu-Systems konzentrieren wir uns auf unsere Kernkompetenzen, den Schutz und die Lizenzierung von digitalem geistigem Eigentum.

Unser Innovationsteam prüft neue Trends sorgfältig, teilweise in Kooperation mit dem Karlsruher Institut für Technologie (KIT), dem Forschungszentrum Informatik (FZI) und weiteren Einrichtungen. Durch die Teilnahme an vielen Partner- und Early-Adopter-Programmen sind wir in der Lage, neue Trends frühzeitig im Detail zu evaluieren.

Unser Architekturteam sorgt dafür, dass sich neue Lösungen nahtlos in die bestehenden Lösungen und Produkte integrieren, um so Synergie-Effekte nutzen zu können.

Unsere Lösungen für Sie

Für die Zukunft hat sich Wibu-Systems vier Hauptziele gesteckt:

- **Schutz und Lizenzierung von Software.** Als Hersteller von klassischer Software konnten Sie in der Vergangenheit auf die Kontinuität von Wibu-Systems bauen. Dies können Sie auch in der Zukunft.
- **Schutz und Lizenzierung von Dokumenten.** Hidden Champions im Bereich Straßenfräsen und Holzverarbeitung setzen bereits auf Wibu-Systems beim Schutz von Serviceunterlagen. Dabei basiert der Dokumentenschutz auf derselben bewährten Technologie wie der Softwareschutz. Lizenzerstellung, Lizenzauslieferung, Lizenzverwaltung und Lizenzmodelle sind komplett identisch. Lediglich die Integration in Adobe Acrobat® ist ein extra Modul.
- **Schutz und Lizenzierung für Embedded Devices.** Durch starke Partnerschaften im Automatisierungsumfeld sind unsere Lösungen auch in diesem Bereich bereits weit verbreitet. Die Lösungen umfassen den Schutz der Projektdaten des Maschinenbauers, den Schutz der Software auf der Steuerung gegen Raubkopien und Reverse-Engineering, Integritätsschutz und Autorisierung der Software auf der Steuerung und Lizenzierung von Features on Demand. Auch hier setzen wir auf unsere bewährte Technologie CodeMeter. Ein zusätzliches Embedded-Team kümmert sich um die Anpassung für die speziellen Anforderungen von Steuerungen.
- **Schutz, Lizenzierung und Authentifizierung in der Cloud.** In der Cloud setzen wir auf unsere bewährte Technologie CodeMeter und wenden uns an Softwarehersteller, die ihre Software schützen und lizenzieren möchten. In einigen Fällen ist Schutz mit Authentifizierung verbunden. Hier spielt CodeMeter besonders seine Stärke aus, da in der Basistechnologie bereits beides vorhanden ist: Asymmetrische Verfahren für die Authentifizierung und symmetrische Verfahren für den Schutz. Und natürlich gilt auch hier, dass unser Cloud-Team die Synergien aus der Grundlagenentwicklung verwendet und nicht die Kern-Ressourcen von Wibu-Systems beansprucht.

Wibu-Systems ist über die letzten Jahre stetig und kontinuierlich aus eigenen Mitteln gewachsen. Neue Geschäftsfelder werden zusätzlich und nicht zu Lasten der bestehenden Produkte und Lösungen erschlossen. Als Kunde und Partner können Sie auf unsere Kontinuität bauen. Damit sind wir der optimale Partner für eine langfristige und erfolgreiche Geschäftsbeziehung.

Der Mythos Signatur

„Ich setze Standard-Zertifikate ein, ich bin sicher". Das Einzige, was man mit Sicherheit über diese Aussage sagen kann, ist dass man nicht mit Sicherheit sagen kann, ob diese Aussage stimmt. Denn dazu muss man nämlich die Bedrohungsszenarien betrachten „Sicher für wen" und „Sicher gegen was". Im Fall von gesicherter E-Mail, wenn der Prüfende vertrauenswürdig ist, sind Standard-Signaturen und Standard-Zertifikate eine gute Lösung. Im Fall von Softwareschutz vermitteln Signaturen und Zertifikate oft ein falsches Gefühl von Sicherheit. Hier schafft CodeMeter Abhilfe. CodeMeter setzt zwar die gleichen Mechanismen ein, aber verwendet zusätzlich Verschleierung und Tarnung, da die Überprüfung hier im unsicheren Umfeld geschieht.

Grundlagen von Signaturen

Signieren bedeutet etwas zu unterschreiben. Diese Unterschrift wird mit entsprechenden Methoden durch eine andere Person überprüft. Zur Realisierung von Signaturen verwendet die IT asymmetrische Kryptographie.

Asymmetrische Kryptographie besteht aus einem Schlüsselpaar. Dieses besteht aus dem privaten und dem öffentlichen Schlüssel. Wie der Name schon sagt, ist der private Schlüssel geheim zu halten, während der öffentliche Schlüssel frei für jeden zugänglich ist.

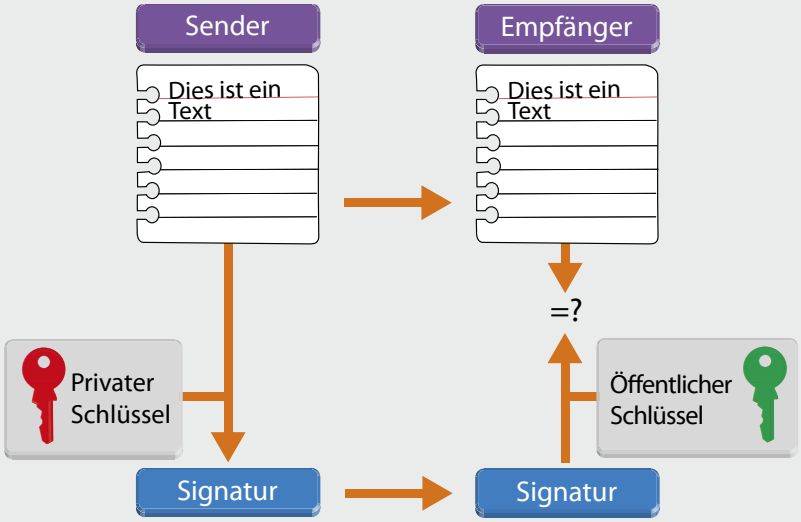
Betrachten wir das sichere Verschicken von E-Mails. Sowohl Sender als auch Empfänger haben jeweils ein Schlüsselpaar. Beide kennen den öffentlichen Schlüssel des jeweils anderen. Möchte ich nun, dass niemand die Nachricht lesen kann, dann verschlüssele ich diese mit dem öffentlichen Schlüssel des Empfängers. Nur der richtige Empfänger kann die Nachricht mit seinem privaten Schlüssel entschlüsseln. Möchte ich sicherstellen, dass der Empfänger sicher sein kann, dass die Nachricht wirklich von mir kommt und nicht verändert wurde, dann unterschreibe (signiere) ich diese mit meinem privaten Schlüssel. Jeder beliebige Empfänger kann mit meinem öffentlichen Schlüssel überprüfen, dass die Nachricht wirklich von mir kam.

Eine Kombination von beidem ist natürlich auch möglich. D.h. Nachrichten können unterschrieben und verschlüsselt werden. Diese Darstellung ist stark vereinfacht, da beim Unterschreiben zuerst ein Hash-Wert gebildet und danach bei der Verschlüsselung ein Hybridverfahren aus symmetrischer und asymmetrischer Verschlüsselung verwendet wird.

Eine Frage des Vertrauens

Wie wir gerade gelernt haben, ist der öffentliche Schlüssel nicht geheim. Jeder darf ihn kennen und jeder darf ihn benutzen. Entweder, um mir etwas Geheimes zu schicken oder um eine Signatur von mir zu überprüfen. Aber woher weiß mein E-Mail-Partner, dass mein öffentlicher Schlüssel wirklich mein öffentlicher Schlüssel ist und nicht der öffentliche Schlüssel einer anderen Person?

Dies ist die Kernfrage der asymmetrischen Kryptographie. Und nun kommen wir zu Zertifikaten. Jemand, der mich kennt, oder dem ich meine Identität nachweise, erstellt mir ein Zertifikat. Dieses beinhaltet meinen Namen, meinen öffentlichen Schlüssel und eine Gültigkeitsdauer. Damit kann mein E-Mail-Partner nun meinen öffentlichen Schlüssel überprüfen. Aber halt! Wie überprüft er denn die Richtigkeit des Zertifikats? Dazu nimmt er den öffentlichen Schlüssel desjenigen, der



Die Signatur wird mit dem privaten Schlüssel erzeugt und mit dem öffentlichen auf Richtigkeit überprüft.

mir das Zertifikat erstellt hat. Hier beißt sich die Katze in den Schwanz, oder mit anderen Worten: „Wer zertifiziert das Zertifikat?".

Egal wie lang die Kette der Zertifikate ist, irgendeinem Wurzelzertifikat (Root Certificate) muss ich vertrauen. In der Regel bringt das Betriebssystem bereits eines oder mehrere solcher Wurzelzertifikate von Zertifizierungsstellen (Certificate Authority) mit. Im Falle eines geschlossenen Systems wie iPhone oder Spielekonsolen ist dies das Zertifikat des Herstellers des Gerätes.

Wer überprüft die Signatur?

Das reine Vorhandensein einer Signatur und eines Zertifikates reicht noch nicht aus, damit etwas geschieht. Wenn Sie jetzt der Meinung sind, dass Sie sich hier auf das Betriebssystem (Windows, Mac OS) verlassen können, dann sind Sie im wahrsten Sinne des Wortes verlassen. Die Signatur und Zertifikatsprüfung im Betriebssystem ist so designed, dass Anwender vor unerwünschter Software wie Viren und Würmern geschützt werden. Eine Software ohne oder mit ungültiger Signatur läuft dennoch, wenn der Anwender die entsprechenden Warnmitteilungen ignoriert. Damit schützt eine vorhandene Signatur Ihre Software nicht vor Veränderung und vor Raubkopien.

Windows bietet Ihnen die Möglichkeit, die Signatur einer Anwendung (exe oder dll) per API selbst zu überprüfen. Dann überprüfen Sie, ob eine Signatur existiert, diese gültig ist und von Ihnen erstellt wurde. Dies klingt auf den ersten Blick recht gut, hat aber zwei Haken. Zum Ersten führt die Überprüfung der Signatur auf eine Ja/Nein-Entscheidung in Ihrer Software hinaus, die ein Hacker patchen kann. Und zum Zweiten fragen Sie das Betriebssystem nach der Signatur. Aber genau jenes Betriebssystem ist bereits unter der Kontrolle des Hackers und kann Ihnen beliebige Antworten vorspiegeln. Und dies mit einem generischen Hack des Signatur-API. Die Überprüfung einer Standard-Signatur und eines Zertifikates mit Bordmitteln des Betriebssystems ist zwar eine kleine Einstiegs-Hürde, bietet aber keinen wirksamen Schutz gegen Veränderung und gegen Raubkopien.

CodeMeter bietet die Lösung

Auch CodeMeter arbeitet mit Signaturen ganz nach Lehrbuch. Als Hersteller haben Sie einen privaten Schlüssel, der in Ihrer FSB (Firm Security Box, d.h. Master Dongle) sicher gespeichert ist. Beim Schutz Ihrer Software mit dem AxProtector wird Ihre Software mit Ihrem Schlüssel automatisch signiert. Die Überprüfungsroutinen und Ihr öffentlicher Schlüssel werden in Ihrer Software an verschiedenen Stellen versteckt hinterlegt.

Beim Starten Ihrer Anwendung wird die Signatur überprüft. Diese Überprüfung erfolgt innerhalb von Ihrer Software und an mehreren Stellen. Somit sind weder eine Simulation von außen noch das Patchen eines einzelnen Bytes möglich. Durch die Integration der Signaturüberprüfung in das generelle Kopierschutzsystem von CodeMeter bekommen Sie einen kompletten Rundum-Schutz für Ihre Software.

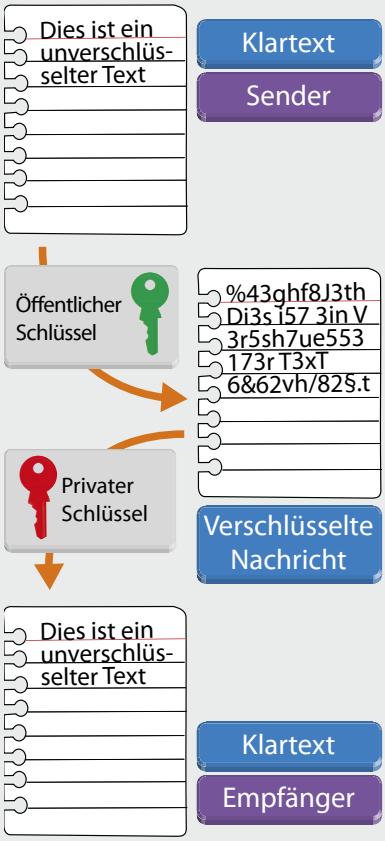
Fazit

Ein anerkanntes Standardverfahren ist sicherheitstechnisch immer besser als eine eigene proprietäre Lösung. Diese Aussage hat auch weiterhin ihre volle Gültigkeit, wenn das Standardverfahren im Rahmen seiner definierten Parameter verwendet wird. Genau dies ist aber die Herausforderung bei Signaturen im Softwareschutz, da die Vertrauenswürdigkeit des Überprüfenden einer der grundlegenden Parameter ist, der auf einem Desktop PC nicht erfüllt ist.

CodeMeter setzt daher auf eine gesunde Mischung aus Standardverfahren und proprietären Technologien und schützt Ihre Software sicher gegen alle Bedrohungsszenarien, die sich aus den Themen Integritätsschutz und Schutz gegen Raubkopien ergeben, auch in einem unsicheren Umfeld wie den PC des Kunden.

CodeMeter und VxWorks

Bei VxWorks ist der CodeMeter-Mechanismus bereits sicher in das Betriebssystem integriert. Das komplette Betriebssystem kann mittels CodeMeter so versiegelt werden, dass nur vom Hersteller des Gerätes autorisierte Partner Software aufspielen können.



Public-Key-Verschlüsselung: Die Entschlüsselung erfolgt mit dem geheimen privaten Schlüssel des Empfängers.

Angepasstes WebDepot

Aktivierungsbasierte Lösungen wie CmActLicense sind sehr modern. Donglebasierte Lösungen wie CmDongle wurden schon mehrmals totgesagt, erfahren aber regelmäßig eine Renaissance und sind aus vielen Branchen- und Industrielösungen nicht mehr wegzudenken.

Vergleich Dongle und Aktivierung

Generell spricht für einen Dongle die für den Kunden transparente Lizenzierung. Der Kunde weiß genau, wo sich seine Lizenz befindet: in seinem Dongle. Im Fall eines Austauschs des Rechners kann der Kunde die Lizenz in seinem Dongle einfach mitnehmen. Für eine Aktivierungsbasierte Lösung spricht, dass Lizenzen online schnell freigeschaltet werden können. CodeMeter verbindet die besten Punkte aus beiden Welten und bietet mit CmDongle und CmActLicense ein einzigartiges System, bei dem Softwarelizenzen transparent und verschiebbar sind und Dongles flexibel und schnell online programmiert werden können. Ein entscheidender Punkt hierbei ist das individuell an Ihre Anforderungen anpassbare License Central WebDepot.

Was ist das WebDepot?

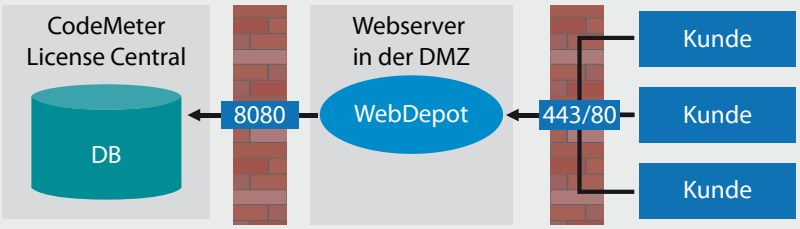
Das WebDepot ist eine webbasierte Anwendung, die Sie als Schnittstelle für Ihre Anwender zur CodeMeter License Central im Internet zur Verfügung stellen. Das WebDepot gibt es als PHP-Version für einen Apache Webserver. Eine .Net Version für den Internet Information Server (ISS) wird Ende 2012 ebenfalls zur Verfügung stehen.

Im WebDepot kann der Anwender über einen Browser selbständig Lizenzen sowohl in eine CmActLicense als auch in einen CmDongle übertragen. Es steht eine direkte Übertragung entweder auf den lokalen Rechner oder in einen lokal angeschlossenen CmDongle zur Verfügung. Optional kann der Kunde durch das Herunterladen einer Lizenzdatei die Lizenz offline auf einen anderen Rechner oder in einen anderen CmDongle übertragen. Als Zusatzoptionen sind die Berechnung eines Aktivierungscodes für die codebasierte (telefonische) Freischaltung und die Rückgabe von Lizenzen ins WebDepot integrierbar. Diese beiden Optionen sind nicht im Standardumfang enthalten.

Als Browser kann der Kunde die jeweils aktuellen Versionen vom Microsoft Internet Explorer, vom Mozilla Firefox, vom Google Chrome und auf OS X vom Safari verwenden. Für die direkte Übertragung benötigt er JavaScript und entweder Java oder ActiveX. Das WebDepot ist aber so implementiert, dass die dateibasierte Aktivierung auch verwendet werden kann, wenn JavaScript, Java und ActiveX deaktiviert sind. Somit ist auch bei höchsten Sicherheitseinstellungen eine eigenständige Aktivierung durch den Anwender möglich.

Warum ein WebDepot?

Warum benötigen Sie überhaupt ein WebDepot und warum stellen Sie die CodeMeter License Central nicht einfach komplett ins Internet? Zwei Gründe sprechen für ein extra WebDepot:
1) Sicherheit
2) Anpassbarkeit



Warum erhöht das WebDepot die Sicherheit?

Aus Sicherheitsgründen verwendet die CodeMeter License Central Diversität. Dies bedeutet den Einsatz von unterschiedlichen Technologien. Dieses Konzept wird zum Beispiel in Steuerungen von Schiffen oder in Atomkraftwerken verwendet. Fällt eine Technologie aus, weil ein systematischer Fehler (der also in einem zweiten baugleichen Teil genauso auftritt) vorliegt, übernimmt die zweite Technologie und der Betrieb geht sicher weiter. In Fall der CodeMeter License Central sichert Sie dieses Konzept gegen Einbruch, Datendiebstahl und nicht autorisierte Lizenzerstellung.

Ein Apache Webserver oder ein IIS stehen in der DMZ und hosten das WebDepot. Hinter der inneren Firewall steht ein Tomcat und nimmt die Abfragen vom WebDepot entgegen. Sollte ein Angreifer aufgrund eines systematischen Fehlers den Webserver mit dem WebDepot hacken (Exploit), ist er nur dort und nicht in der Datenbank oder an Ihrer Firm Security Box. Durch die innere Firewall ist sichergestellt, dass der Rechner mit dem WebDepot nur mit dem Tomcat per WebService kommunizieren kann. Der Angreifer würde also einen zweiten Exploit für den Tomcat benötigen, um weiter nach innen vorzudringen.

Damit ergeben sich beim Hosten einer License Central Internet automatisch folgende Grundregeln:

- Kein direkter Zugriff auf CodeMeter License Central aus dem Internet heraus
- Regelmäßiges Einspielen von Sicherheitspatches, vor allem auf dem Webserver in der DMZ. Nachgelagert auf dem Tomcat in der CodeMeter License Central
- WebDepot und CodeMeter License Central auf zwei verschiedenen Rechnern
- Kein Tomcat für das WebDepot

In unserem Hosting Paket, bereitgestellt durch Wibu Operating Services, läuft die CodeMeter License Central Internet für Sie in der Wibu Cloud und unser eingespieltes Team kümmert sich um die Einhaltung dieser Regeln.

Wie kann ich das WebDepot anpassen?

Die Oberfläche der CodeMeter License Central wurde für Sie als Softwarehersteller designt und sieht keine Anpassung an Ihr Corporate Design vor. Eine webbasierte Anwendung, die Sie Ihrem Kunden zur Verfügung stellen, sollte aber Ihr „Look and Feel" haben. Und genau dies ist mit dem WebDepot auf einfache Art und Weise möglich.
Sie definieren Ihre eigenen Styles in einer CSS-Datei und tauschen die vorhandenen neutralen Bilder durch Ihre eigenen Bilder aus. Schon hat das WebDepot Ihre Farben und Schriften. Durch den Austausch des Seiten-Headers und des Footers können Sie das WebDepot noch weiter an Ihr Design anpassen.

Lediglich die eigentliche Funktionalität ist immer gleich:

- Eine Tabelle der verfügbaren Lizenzen
- Eine Fläche für Hilfe und Fehlertexte
- Der Aktionsbereich mit Online- und Offline-Aktivierung

Auch die Texte können individuell angepasst werden. Alle Texte liegen in einer extra Sprach-Datei, um die Anpassung für Sie so einfach wie möglich zu gestalten.

Das WebDepot bietet prinzipiell die Unterstützung beliebiger Sprachen und wird in der Standardversion mit Englisch und Deutsch ausgeliefert. Über einen Eintrag in der Konfiguration fügen Sie einfach eine weitere Sprache hinzu. Sie übersetzen dann lediglich die Sprach-Datei in die von Ihnen gewünschte Sprache. Das WebDepot unterstützt UTF8, d.h. Sie können jede beliebige Sprache integrieren.

Wie kann ich das WebDepot integrieren und erweitern?

In vielen Fällen besitzt der Softwarehersteller bereits ein Kundenportal. In diesem Fall ist es natürlich möglich, das WebDepot in das bestehende Kundenportal zu integrieren. Sie können das WebDepot als Beispiel nehmen und die Webservices des Tomcat direkt aus Ihrem bestehenden Portal aufrufen oder sogar große Teile des Codes des WebDepots in Ihr Projekt übernehmen.

Alternativ können Sie aber auch das WebDepot übernehmen und im Kundenportal die Tickets des Kunden verwalten. Anstelle der Eingabe eines Tickets, loggt sich der Kunde im Kundenportal ein. Dort kann er dann auf ein Ticket klicken und wird ins WebDepot zum Abholen der entsprechenden Lizenzen weitergeleitet.

Softwareschutz als Prozessbestandteil

Die Erstellung von Software ist für einen Hersteller ein aufwändiger und kostenintensiver Prozess. Oft enthält die entwickelte Software auch umfangreiches, schützenswertes Spezialwissen. Durch Raubkopien, Reverse-Engineering und Manipulation entstehen der Branche jedes Jahr hohe monetäre Schäden. Gleich zwei Fliegen mit einer Klappe kann schlagen, wer Softwareschutz und Lizenzmanagement frühzeitig in den bestehenden Softwareentwicklungsprozess integriert.

Softwareschutz ist existenziell

Im Bereich der professionellen Softwareentwicklung wird heute ein wohldefinierter Prozess zugrunde gelegt, der auf der einen Seite vorab die Definition aller erforderlichen Ein- und Ausgabe-Parameter und der dazugehörigen Funktionen in Form von Spezifikationen vorschreibt, auf der anderen Seite aber auch die Transparenz über Kosten und zeitlichen Verlauf der Entwicklungsarbeiten ermöglicht. Ob man dabei nun auf ein klassisches Wasserfallmodell setzt oder die Entwicklung mit agilen Methoden wie SCRUM durchführt: die frühzeitige Einbindung von Softwareschutzmaßnahmen in den Prozessablauf zahlt sich grundsätzlich aus.

Unabhängig davon, ob es sich bei der Entwicklung einer Applikation für den Massenmarkt, um Individualsoftware, um eine spezielle Branchenlösung in einem Nischenmarkt, um Softwarelösungen in der Cloud oder um eine Steuerungssoftware im industriellen Bereich handelt, neben dem reinen Entwicklungsaufwand steckt in der Software auch ein hoher Anteil geistigen Eigentums eines Unternehmens. Gerät dieses Wissen durch Raubkopien oder Reverse-Engineering in falsche Hände, steht nicht selten auch gleich die Existenz auf dem Spiel. Raubkopien verursachen in der Softwarebranche hohe Umsatzausfälle. Nach einer aktuellen Studie der Software Alliance (BSA) aus dem Jahr 2012 liegt der Anteil der unlizenzierten Software bereits bei 42% aller installierten Software.

Einbindung in den Entwicklungsprozess

Die Integration von Softwareschutz und Lizenzmanagement in den bestehenden Softwareentwicklungsprozess stellt sich grundsätzlich als entwicklungsübergreifende Lösung dar. Aus diesem Grund ist es ratsam, die grundlegenden Weichenstellungen bereits frühzeitig am besten direkt zu Beginn des Projektes festzulegen. Zu diesem Zeitpunkt ist die Flexibilität bei der Einbindung am größten und alle Projektbeteiligten sind für diese Themen entsprechend sensibilisiert.

Wibu-Systems bietet aber auch einfache und schnelle Lösungen, die in späteren Projektphasen oder sogar nach Fertigstellung von Softwareprojekten zum Einsatz kommen. Mit dem AxProtector lässt sich mit wenigen Mausklicks ein hoher Schutzlevel erreichen, ohne in den Quellcode der zu schützenden Software eingreifen zu müssen. Die Anwendung wird komplett verschlüsselt und enthält anschließend Schutzmethoden wie Anti-Debugging, wechselnde Schlüssel, Intrusion Detection und geheime Sperrcodes, die im Falle eines Angriffs die Lizenz sperren. Die Möglichkeit, die Anwendung mit einem geeigneten Lizenzmodell zu versehen, ist zusammen mit dem Softwareschutz automatisch gleich mitimplementiert. Über die Verwendung des IxProtectors von Wibu-Systems lassen sich die Module der Anwendung bestimmten Lizenzen zuordnen, wodurch eine modulare Lizenzierung möglich ist.

Dem Softwarehersteller stehen eine Vielzahl unterschiedlicher Arten der Lizenzierung seiner Anwendung zur Verfügung. Angefangen von Einzelplatzlizenzen, über Netzwerklizenzen, zeitlich basierte Modelle, Feature-on-Demand bis hin zu Pay-per-Use Lizenzen existieren unterschied-

liche Modelle, die sich auch geeignet miteinander kombinieren lassen. Nutzen Sie dafür Hardwaredongles (CmStick/CmCard) und reine Softlizenzen (CmActLicense) als Lizenzcontainer. Es steht auch die Möglichkeit, die gleiche Software sowohl mit der einen als auch der anderen Lösung oder sogar mit einer Kombination von beiden auszuliefern, um den Anforderungen bestimmter lokaler Märkte Rechnung tragen zu können. Hier baut Wibu-Systems ganz auf das Prinzip: „One solution fits all".

Der große Vorteil der Lösungen von Wibu-Systems im Entwicklungsprozess ist, dass die Art der später eingesetzten Lizenzmodelle und die Form des Lizenzmediums (Dongle oder Softlizenz) zum Zeitpunkt der Entwicklung der Software noch nicht festgelegt werden müssen. Nach Fertigstellung der Software kann beispielsweise das Produktmanagement über Art und Umfang der Lizenz entscheiden und diese jederzeit ändern, ohne dass die Software selbst nochmal dafür angepasst werden muss. Das führt zu einer großen Flexibilität und einer Vereinfachung des Entwicklungsprozesses und ermöglicht eine strikte Trennung von Entwicklung, Softwareschutz und Lizenzierung bei gleichzeitiger Reduzierung der Entwicklungskosten.

Der Gesamtprozess der Verschlüsselung einer Software und der Festlegung der Lizenzierungsmodelle teilt sich in vier Schritte auf, die in der folgenden Grafik dargestellt sind. Dabei wird mit den Lösungen von Wibu-Systems aus einer ungeschützten und unlizenzierten Software eine gegen Raubkopien und Reverse-Engineering geschützte und mit Lizenzmodellen versehene Anwendung erstellt.

Unterstützung des Prozesses

Für jeden der vier Schritte stehen Ihnen bewährte Werkzeuge von Wibu-Systems zur Verfügung, die nicht nur mit den jeweiligen grafischen Oberflächen eingesetzt werden können, sondern auch mit umfangreichen Programmierschnittstellen ausgestattet sind, um die Werkzeuge auch während der Entwicklung optimal in die verwendeten Prozessumgebungen integrieren zu können. Dabei kann es sich beispielsweise um einen Buildserver handeln, der im Rahmen eines festgelegten Entwicklungsprozesses über Nacht automatisch die neuentwickelten Modelle übersetzt und mit dem Tool verschlüsselt. Darauf lassen sich dann auf Basis vordefinierter Ablaufszenarien automatische Tests durchführen.

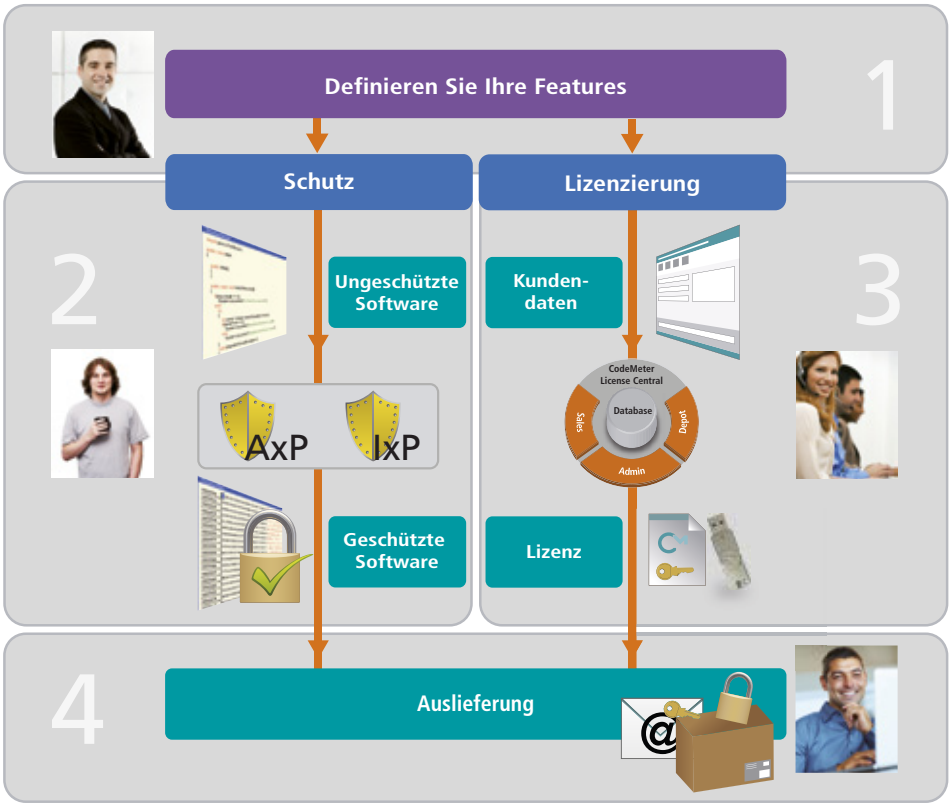
Fazit

Eine kostenoptimierte und transparente Softwareentwicklung ist nur durch die konsequente Nutzung von Softwareentwicklungsprozessen möglich. Dabei spielt es heute keine Rolle, ob man dazu klassische oder agile Methoden einsetzt. Die Einbeziehung von Softwareschutz und Lizenzmanagement ist unabhängig von dem gewählten Prozessmodell ein extrem wichtiger Aspekt, den optimalerweise zu Beginn der Prozessplanung oder bei der Aufstellung des initialen Backlogs im Rahmen agiler Methoden berücksichtigt wird.

Am Ende eines gut aufgestellten und gut gelebten Prozesses steht mit skalierbaren und flexiblen Lösungen von Wibu-Systems eine perfekt geschützte Software mit flexiblen Lizenzmodellen, die Ihren Gewinn erhöht und gleichzeitig die Entwicklungskosten reduziert.

Dann gilt auch für Sie zukünftig: „Planung ist das Ersetzen von Zufall durch Wissen."

In nur vier Schritten zur geschützten Software



1) **Definieren Sie die Features Ihrer Anwendung:** Legen Sie fest, welche Module Ihrer Software Sie separat lizensieren möchten.

2) **Schützen Sie Ihre Software:** Mit dem einfachen Werkzeug AxProtector von Wibu-Systems verschlüsseln Sie Ihre komplette Software ohne Eingriff in den Quellcode. Mit dem IxProtector schützen Sie einzelne Module und fügen eine weitere individuelle Schutzschicht hinzu. Legen Sie hier den Grundstein für den Einsatz individueller Lizenzierung.

3) **Erstellen Sie Ihre Lizenzen:** Mit der CodeMeter License Central bilden Sie Ihre ausgewählten Lizenzmodelle flexibel und einfach ab. Verkauf und Distribution von Lizenzen können damit direkt online oder offline abgebildet und in bestehende Back-Office-Prozesse eines Unternehmens integriert werden.

4) **Liefern Sie aus:** CodeMeter bietet Ihnen vielfältige Auslieferungsoptionen: Mit hardwarebasiertem CmDongle, mit rechnergebundener CmActLicense, vorprogrammiert oder als Lizenzcode.

Projektschutz durch Verschlüsselung

Nahezu jede Software verarbeitet in irgendeiner Form Daten. Je nach Anwendungsfall kann in diesen Daten viel Know-how und geistiges Eigentum des Softwareherstellers oder des Anwenders liegen. Dieser Artikel zeigt, wie Sie als Hersteller diese Daten schützen können, sowohl im eigenen Interesse, als auch als Mehrwert für Ihren Kunden.

Automatismus mit AxProtector

Der AxProtector bietet Ihnen mit der Dateiverschlüsselung eine schnell nutzbare Möglichkeit, wie Sie einfache Anforderungen abbilden können. Beim Schützen Ihrer Anwendung schalten Sie die Dateiverschlüsselung ein. Der AxProtector liegt sich dann wie ein Wächter zwischen die geschützte Anwendung und die zu lesende Datei. Falls die zu schützende Datendatei nun ebenfalls mit dem AxProtector verschlüsselt wurde, überprüft Ihre geschützte Anwendung nun ganz automatisch, ob die passende Lizenz auch für die Datendatei vorhanden ist. Falls ja, wird diese automatisch entschlüsselt.

Falls die passende Lizenz für die Datendatei nicht vorhanden ist, verweigert die geschützte Anwendung das Laden der Datendatei. Und hier sind wir bei der ersten Einschränkung der automatischen Dateiverschlüsselung: Das Fehlerhandling. Der Fehler wird von Ihrer originalen Anwendung verarbeitet und muss daher unter Umständen geringfügig angepasst werden.
Das Schreiben von Datendateien ist die zweite Herausforderung der geschützten Anwendung. Über ein Regelwerk können Sie das Schreiben sehr fein bis hin zur Dateierweiterung definieren.

Manuelle Verschlüsselung

Wenn Ihnen die einfachen Automatismen nicht ausreichen oder Sie selber gerne die volle Kontrolle behalten wollen, dann bietet Ihnen das CodeMeter Core API mächtige Funktionen für eine manuelle Integration von Ver- und Entschlüsselung in Ihre Anwendung.

Jede Kombination aus Firm Code und Product Code besitzt einen eigenen Schlüssel, den Sie verwenden können. Mit CmAccess2 öffnen Sie ein Handle auf den Lizenzeintrag. Mit CmCrypt2 verschlüsseln Sie Ihre Daten und mit CmRelase geben Sie das Handle wieder frei.

Neben Firm Code und Product Code geht in die Berechnung des verwendeten Schlüssels der Encryption Code ein. Diesen können Sie selber frei wählen. Wählen Sie einen beliebigen, aber festen Encryption Code und speichern Sie diesen im Source Ihrer Software ab. Dann ist das Geheimnis verteilt. Der eigentliche Schlüssel steckt in der CodeMeter Lizenz, aber mittels des Geheimnisses in der Software legen Sie fest, welcher der vielen möglichen Schlüssel verwendet werden soll. Damit kann nur Ihre Software die Daten entschlüsseln.

Beim Verschlüsseln setzen Sie die Option „CRC erzeugen". Diese Checksumme speichern Sie mit Firm Code und Product Code in Ihrer Datendatei ab. Beim Entschlüsseln setzen Sie Option „CRC überprüfen" und stellen somit sicher, dass die Datendatei korrekt entschlüsselt wurde. Als Verschlüsselungsmethode verwenden Sie AES im CBC-Modus. Damit können beliebig lange Daten (mindestens 16 Byte) in einem Block verschlüsselt werden. Bei CodeMeter werden dabei nur die ersten 16 Byte an den CmDongle geschickt, der Rest erfolgt ohne Einschränkung der Sicherheit im Hauptspeicher des Computers. Damit bietet Ihnen diese Methode eine hohe Performance auch bei großen Daten.

Rechteverwaltung

Falls Sie die Verschlüsselung von Datendateien als Mehrwert für Ihre Kunden anbieten, stellt sich die Frage, wie man die Zugriffsrechte auf die Daten verwaltet. Prinzipiell sind hier zwei Verfahren üblich:

- Rechteverwaltung mittels Lizenzen (bestehend aus Firm Code, Product Code und weiteren Optionen)
- Rechteverwaltung mittels Identitäten (in Form eines privaten Schlüssels)

Lizenzbasiert

Da jede Kombination aus Firm Code und Product Code einen anderen Schlüssel bietet, stellt jede Kombination ein einzelnes Recht dar. Die technische Realisierung erfolgt mittels manueller Verschlüsselung. Zusätzlich bieten Sie in der Software die Möglichkeit an, Firm Code und Product Code für die Verschlüsselung zu wählen.

Falls Ihr Kunde, der Anwender, die Rechte selber verteilen möchte, dann benötigt er einen eigenen Firm Code und die Infrastruktur für die Erstellung von Lizenzen (CodeMeter License Central). Damit stellt diese Lösung einen höheren einmaligen Aufwand beim Anwender dar. Dafür erhält er die volle Flexibilität bei der Vergabe von Berechtigungen, inklusive zeitlich beschränkter Rechte und einer Online-Übertragung der Lizenzen.

Identitätsbasiert

In vielen Anwendungsfällen erfolgt die Vergabe von Berechtigungen identitätsbasiert. Jede Person erhält eine eigene Identität. Datendateien werden speziell für eine oder mehrere Identitäten verschlüsselt. D.h. nur die definierten Empfänger sind in der Lage, die entsprechende Datendatei zu verwenden. Das System arbeitet analog zu verschlüsselter Kommunikation bei E-Mails. Auch dort wird eine E-Mail für die entsprechenden Empfänger verschlüsselt. Zusätzlich kann die verschlüsselnde Person die Datendatei signieren und somit Authentizität und Integrität sicherstellen.

Die Vorteile dieses Verfahrens sind der geringe Aufwand für den Anwender sowie Integrität und Authentizität. Jeder CmDongle besitzt bereits eine eindeutige Identität, bzw. kann sehr einfach eine weitere Identität erhalten. Der Anwender benötigt keine extra Infrastruktur, um die Lizenzen und Rechte zu erstellen und zu verwalten.

Die Implementierung erfolgt mittels asymmetrischer Kryptographie. Dabei besitzt jede Identität einen privaten und einen dazu passenden öffentlichen Schlüssel. Mit dem privaten Schlüssel wird signiert und Daten entschlüsselt. Mit dem öffentlichen Schlüssel werden Signaturen geprüft und Daten verschlüsselt. Bei der Implementierung stehen Sie vor zwei Herausforderungen. Zum Einen sollen Daten für mehrere Empfänger lesbar sein. Da Sie zum Verschlüsseln den öffentlichen Schlüssel des Empfängers verwenden, wären die Daten damit für jeden Empfänger anders. Außerdem ist asymmetrische Kryptographie nicht geeignet für die Verschlüsselung von größeren Daten.

Beide Herausforderungen lösen Sie mit einer Hybridverschlüsselung. Dazu wählen Sie einen zufälligen AES Schlüssel. Mit diesem verschlüsseln Sie die gewünschten Daten. Nun nehmen Sie die öffentlichen Schlüssel aller Empfänger und verschlüsseln den zufälligen AES Schlüssel mit jedem von diesen öffentlichen Schlüsseln und hängen diese zusammen mit einer Kennung des Empfängers an die Daten an. Zusätzlich können Sie die Daten wahlweise vor dem Verschlüsseln oder die gesamte verschlüsselte Nachricht noch zusätzlich mit dem privaten Schlüssel des Senders signieren. In den meisten Fällen wird zuerst signiert. Dann ist die Authentizität der Daten gewährleistet. Signieren Sie nach dem Verschlüsseln, ist die Authentizität der ganzen Nachricht gewährleistet.

Optional können Sie dieses Hybridverfahren mit Ihren eigenen Passwortverfahren verbinden und so eine Abwärtskompatibilität zu Ihrer bisherigen Lösung herstellen.

Die geschützten Daten enthalten dann die verschlüsselten Daten, für jeden Empfänger den individuell für ihn verschlüsselten Schlüssel und seine Kennung, sowie die Signatur zur Prüfung von Authentizität und Integrität.

Beim Entschlüsseln verwenden Sie den privaten Schlüssel des Empfängers, um die Daten zu entschlüsseln und den öffentlichen Schlüssel des Senders um die Authentizität und damit auch die Integrität zu überprüfen.

Das ganze Verfahren setzt voraus, dass jeder Teilnehmer sicher (authentisch) den öffentlichen Schlüssel des jeweilig anderen Teilnehmers kennt. Ist Ihr öffentlicher Schlüssel zum Beispiel fest in Ihrer Software im Quellcode hinterlegt, dann können Sie bei Datendateien überprüfen, ob diese von Ihnen erstellt wurden und andere Daten ablehnen. Hat der Sender eine Datenbank aller öffentlichen Schlüssel der Empfänger, dann kann er ihnen eine Datendatei erzeugen, ohne die passenden CmDongles selbst zu besitzen.

Best of Both Worlds

Über Gruppenschlüssel kann die identitätsbasierte Verschlüsselung um die Funktionalität der lizenzbasierten Verschlüsselung erweitert werden. Zusätzlich zur persönlichen Identität können gruppen- oder datenspezifische Schlüssel vergeben werden und in Form eines Lizenzeintrags in einem CmDongle gespeichert werden. Dann sind alle Lizenzoptionen möglich, die Verschlüsselung basiert aber auf dem als Hidden Data oder Secret Data gespeicherten privaten Schlüssel.

Dann können Berechtigungen auch mittels CodeMeter License Central erstellt und verteilt werden, sowohl permanent als auch temporär. Diese Flexibilität bietet Ihnen nur CodeMeter, da nur CodeMeter asymmetrische und symmetrische Verfahren in einem CmDongle vereint. Neben CmDongles bieten rechnergebundene CmActLicenses exakt die gleiche Funktionalität. Dann liegen die Schlüssel verschlüsselt in einer Lizenzdatei auf dem Rechner.

CodeMeter das Schlüsselmonster

Vielleicht haben Sie im Zusammenhang mit der asymmetrischen Kryptographie den Begriff RSA gehört oder gelesen. RSA ist ein in die Jahre gekommenes Verfahren, welches lange Schlüssellängen für ausreichende Sicherheit benötigt und bei dem öffentlicher und privater Schlüssel aufwendig berechnet werden müssen. Diese Berechnung war in der Vergangenheit oft der Angriffspunkt, wenn RSA gebrochen wurde.

Daher setzt CodeMeter bewusst auf den neuen Standard ECC. Mit einem ECC-Schlüssel von 224 Bit erreichen Sie die gleiche Sicherheit wie mit einem RSA-Schlüssel von 2048 Bit. Somit sind in einem CmDongle mehr als 2.000 verschiedene Schlüssel / Identitäten speicherbar.

ECC hat gegenüber RSA einen weiteren Vorteil. Der private Schlüssel ist eine reine Zufallszahl, aus dem der öffentliche Schlüssel berechnet werden kann. Somit ist das Erzeugen eines Schlüsselpaars einfacher und robuster.

Fazit

Unabhängig davon, ob Sie Ihre Daten lizenzbasiert, identitätsbasiert oder mit einer Mischung aus beiden schützen wollen: CodeMeter ist in jedem Fall die einfache und sichere Lösung für Ihren Anwendungsfall.

Glossar	
AES	Advanced Encryption Standard (Symmetrisches Verschlüsselungsverfahren)
CBC	Cipher Block Chaining Mode (Verkettung von Blöcken bei Verschlüsselung größerer Datenmengen)
RSA	Rivest, Shamir und Adleman (Asymmetrisches kryptographisches Verfahren)
ECC	Elliptic Curve Cryptography (Asymmetrisches kryptographisches Verfahren)
CRC	Cyclic Redundancy Check (Prüfsumme)
Hash	Kryptographische Prüfsumme

CodeMeter und Virtualisierung

Virtuelle Umgebungen sind aus der heutigen IT-Welt nicht mehr wegzudenken. Ihren Siegeszug begann die Virtualisierung bereits in den 90er- Jahren. Bessere Ressourcenausnutzung, weniger Investitionskosten und Plattformunabhängigkeit sind die zentralen Vorteile. Der folgende Artikel zeigt, wie Wibu-Systems mit seinen Lösungen diese Themen auch im virtuellen Raum perfekt beherrscht.

Die Einsatzgebiete

Unter Virtualität versteht man die Eigenschaft einer Sache, nicht in der Form zu existieren, in der sie zu existieren scheint, aber in ihrem Wesen oder ihrer Wirkung einer in dieser Form existierenden Sache zu gleichen. Auf den Bereich der IT übertragen heißt das, auf einem real existierenden Rechner eine weitere Umgebung (Virtuelle Maschine) zur Verfügung zu haben, in der virtuell ein zusätzlicher Rechner mit eigenem Betriebssystem existiert, der autark läuft, sich die real zur Verfügung stehenden Ressourcen aber mit diesem Rechner und anderen dort installierten, virtuellen Umgebungen teilt. Es besteht auch die Möglichkeit, im Rahmen der Virtualisierung einen physikalisch existierenden Rechner im Netzwerk freizugeben, auf den sich dann mehrere Personen einloggen und die dort vorhandenen Anwendungen und Ressourcen teilen (Terminal Server). Zielsetzung ist immer, die vorhandenen Ressourcen so effizient wie möglich auszunutzen. Genau das ist der entscheidende Punkt bei der Nutzung von Software in virtuellen Umgebungen, denn durch die Mehrfachnutzung der Ressourcen (und damit auch der lizenzierten Software) wird oft gegen Lizenzbedingungen verstoßen. Die Herausforderung für Softwarehersteller ist nun, einfache aber nachhaltige Lösungen dafür zu finden.

Die Herausforderungen

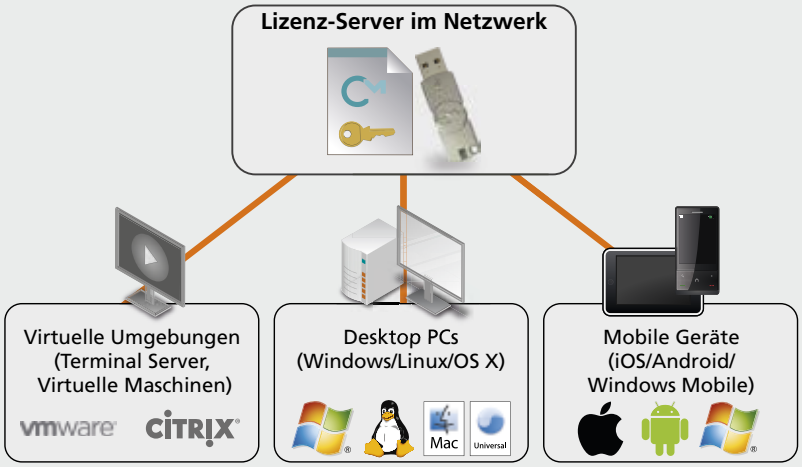
Möchte ein Softwarehersteller sicherstellen, dass die vorgesehenen Lizenzmodelle auch in virtuellen Umgebungen nicht umgangen werden können, so stehen mit den CodeMeter Softwareschutz und Lizenzierungslösungen von Wibu-Systems die richtigen Werkzeuge zur Verfügung.

CodeMeter unterstützt in virtuellen Umgebungen sowohl den Einsatz von Hardware basierten Schutzlösungen (CmDongle/CmCard) als auch von reinen Software-basierten Lizenzen (CmActLicense). Die Zielsetzung: die Lizenz nur dort sichtbar zu machen, wo sie auch tatsächlich verwendet werden darf. Hier besteht zwischen Hardware- und Softwarelösungen ein gravierender Unterschied. Während ein CmDongle selbst Träger einer Lizenz ist und diese entsprechend geschützt und einmalig ist, ist die Softlizenz direkt auf dem System selbst vorhanden und wird damit bei der Erstellung oder beim Klonen einer virtuellen Maschine mitkopiert. Um dies zu verhindern, muss die Bindung einer Softlizenz an die virtuelle Maschine auf intelligente Art und Weise durchgeführt werden.

Dazu steht mit SmartBind® ein auf der langjährigen Erfahrung von Wibu-Systems aufbauendes Bindungssystem zur Verfügung, das zum Patent angemeldet wurde. Dadurch wird eine Softlizenz nicht nur an verschiedene Hardwaremerkmale eines Rechners, sondern speziell im virtualisierten Umfeld an geeignete und verlässliche Eigenschaften gebunden. Das Klonen wird somit in 98 % aller Fälle sicher erkannt und die mitkopierten oder verschobenen Lizenzen entwertet.

Die effiziente Nutzung

Ein großer Vorteil in Bezug auf Effizienz und Auslastung ist die Nutzung einer virtuellen Maschine als Lizenzserver im Netzwerk, der die zur Verfügung stehenden Lizenzen im Netzwerk zur Verfügung stellt und überwacht. Dies eignet sich für den Aufbau eines Lizenzservers in hete-



rogenen Netzwerken, in denen real existierende Maschinen mit unterschiedlichen Betriebssystemen gemeinsam mit virtuellen Umgebungen und Terminalservern eingesetzt werden.

Dabei spielt es keine Rolle, ob die zur Verfügung stehenden Lizenzen auf einem angeschlossenen CmDongle oder als CmActLicense gebunden an den Lizenzserver bereitgestellt werden. Ein CmDongle bietet den Vorteil einer höheren Mobilität, da er von einem Server in einen anderen Server umgesteckt werden kann und die Lizenzen dann dort zur Verfügung stehen.

Die Bereitstellung von Lizenzen in einer virtuellen Umgebung kann auf vielfältige Weise erfolgen. Wird ein CmDongle mit lokalen Lizenzen beispielsweise einem bestimmten Gastsystem eines Hostsystems zugeordnet, so sind die Lizenzen auch nur dort sichtbar. Handelt es sich bei den Lizenzen aber um Netzwerklizenzen, so sind diese auch im Hostsystem selbst und in allen auf diesem Hostsystem installierten Gastsystemen verfügbar.

Voraussetzung für die Nutzung der Lizenzen auf den Systemen ist die Installation des CodeMeter-Dienstes sowohl auf dem Host als auch auf den entsprechenden Gastsystemen. Darüber erfolgt die gesicherte Kommunikation der einzelnen Komponenten und die korrekte Zählung der jeweils verwendeten Lizenzen.

Durch die flexible Technologie ist es auch möglich, verschiedene virtuelle Systeme miteinander zu verknüpfen. Somit stehen Netzwerklizenzen, die über einen Dongle am Hostsystem bereitgestellt wurden, auch anderen Host- und Gastsystemen zur Verfügung, die sich im gleichen Netzwerk befinden. Lokale Lizenzen bleiben aber begrenzt auf das jeweilige lokale System.

Bei der Nutzung eines Terminalservers teilen sich viele Nutzer einen Hostrechner und damit die dort vorhandenen Ressourcen und Programme. Auch hier spielt die effiziente Ressourcenauslastung eine entscheidende Rolle, da die Hardware des Hostrechners von allen gleichzeitig genutzt wird. Der Nutzer verwendet seinen eigenen Rechner lediglich als Ein-/Ausgabeterminal und loggt sich auf dem Terminalserver ein. Dort erhält er eine eigene Arbeitsumgebung (Session), die von den anderen Benutzern des Terminalservers abgeschottet ist. Auch hier sorgt der CodeMeter-Dienst von Wibu-Systems für die korrekte Bereitstellung und Überprüfung der auf dem Terminalserver zur Verfügung stehenden Lizenzen über verschiedene Sessions hinweg.

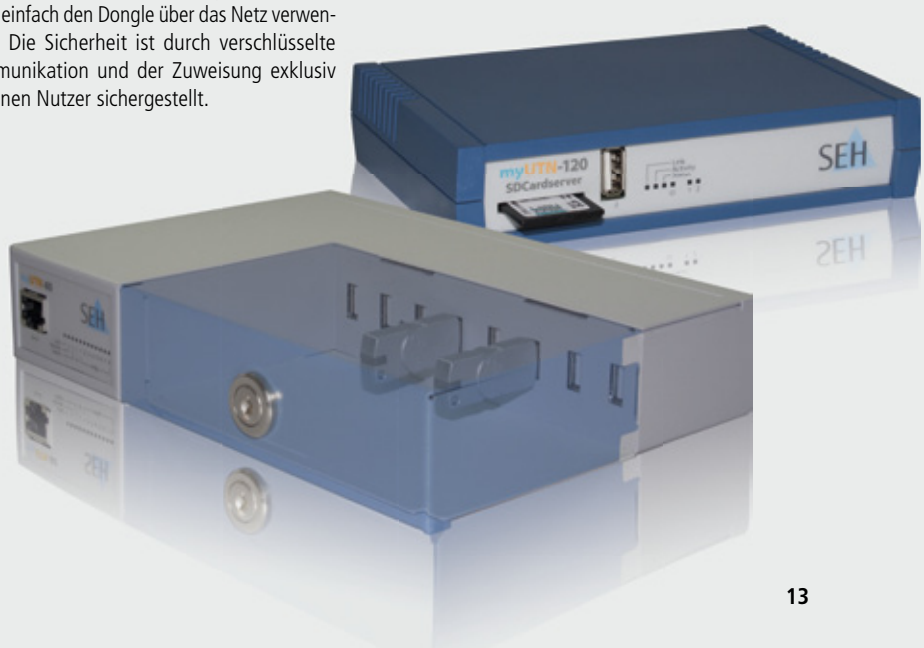
Nutzung von Dongleservern

Ein anderer Weg zur Bereitstellung von Lizenzen in Netzwerken ist der Einsatz von Dongleservern. Nicht immer kann der Dongle beispielsweise bei Lösungen in der Cloud in den Rechner eingesteckt werden, in dem er benötigt wird. Warum nicht einfach den Dongle über das Netz verwenden? Die Sicherheit ist durch verschlüsselte Kommunikation und der Zuweisung exklusiv für einen Nutzer sichergestellt.

Mit dem myUTN-80 USB Dongleserver oder dem myUTN-120 SDCardserver der SEH Computertechnik GmbH aus Bielefeld nutzen Sie wie gewohnt Ihre Software, ohne die Kopierschutzhardware direkt lokal an Ihren PC stecken zu müssen. Bis zu acht Dongles bzw. eine SD-Karte stehen damit sicher und zentral in vollem Funktionsumfang zur Verfügung. Wie bei einem lokal angeschlossenen Device kann nur jeweils ein Anwender über eine Punkt-zu-Punkt-Verbindung den jeweiligen Dongle nutzen. Die Lizenzbestimmungen der Software-Hersteller werden somit zu keiner Zeit umgangen.

Der Einsatz eines Dongleservers löst viele Fragestellungen im Alltags:

- Wissen Sie immer, wo Ihr Dongle gerade steckt? Liegt er irgendwo ungenutzt herum oder hat ein Kollege ihn gerade in Gebrauch? Die zentrale Aufbewahrung von Dongles macht Schluss damit!
- Wollen Sie Dongles für bestimmte Benutzer über das Netz bereitstellen oder exklusive Zugriffsrechte einrichten? Mit einem Dongleserver geht das schnell und einfach! Der Dongleserver ermöglicht, Dongles bestimmten Nutzern exklusiv zuzuweisen und die entsprechenden Schnittstellen zu verschlüsseln!
- Wurde der Dongle gestohlen oder ging verloren, gerade wenn Sie ihn brauchen? Mit einem abschließbaren Gehäuse verwahrt der Dongleserver die eingesteckten Dongles sicher.
- Verwenden Sie einen PC ohne USB-Schnittstelle? Oder alle USB-Schnittstellen sind besetzt? Oder nutzen Sie einen virtuellen Rechner? In diesem Fall ist der Dongleserver genau die richtige Alternative für Ihre Anwendungen.



Aktuelles in Kürze

CodeMeter Firmware 2.0

Alle CmStick, 1001-02 und CmStick/M, 1011-02 können auf die neue Version aktualisiert werden, wenn Sie das CodeMeter Runtime 4.50 oder neuer installiert haben. Es enthält folgende neuen Funktionen und Verbesserungen:

- Offline Field Update: Dies ermöglicht, Aktualisierungen der Firmware ohne Internetverbindung aus Ihrer Software heraus in CmDongles zu übertragen.
- 2048 Bit RSA-Schlüssel
- Verbesserungen der Hardwarezuverlässigkeit und Erhöhung der Lebensdauer durch neue Fehlerkorrekturverfahren.

Aktuelle Software-Versionen:

- CodeMeter SDK 4.50a/b, 2012-09-19
- CodeMeter License Central 1.51a, 2012-10-04
- CmIdentity 4.40, 2011-12-20
- WibuKey SDK 6.10, 2012-10-25
- AxProtector 8.20a, 2012-09-12
- SmartShelter PDF 6.01, 2012-06-19

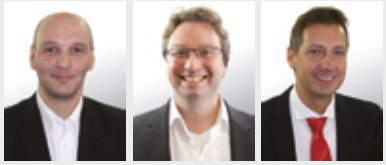
Aktuelle Firmware:

- CmStick, CmStick/M mit Artikelnummer 1001-02 und 1011-02: 2.0
- CmCard/µSD, /SD, /CF: 2.0

Mit der neuesten Software profitieren Sie von letzten Verbesserungen; die neueste Firmware bietet höchste Stabilität und neue Funktionalität. Bitte stets aktualisieren.

Wibu-Team bekommt Verstärkung

Vertrieb, Support & Consulting sowie Entwicklung ist vergrößert; hier die drei neuen Teammitglieder, die Sie kontaktieren können:



(v.l.n.r.) Dr. Ralf Trunko, zuständig für Innovationsmanagement, F&E-Projekte mit Partnern und Patente. Jens Schneider und Wolfgang Greiner unterstützen Sie im Consulting bei der Umsetzung Ihrer Softwarelizenzierungsstrategien.

Online Tutorials – Learning by doing mit dem CodeMeter SDK

Ihre ersten Schritte mit dem CodeMeter SDK werden kinderleicht mit den Video-Tutorials auf unserer Webseite oder auf Youtube.

http://www.youtube.wibu.com

Immer aktuell informiert

Mit KEYFlash, unserem Newsletter, sind Sie stets auf dem Laufenden, melden Sie sich gleich an:

http://www.wibu.com/de/newsletter.html

Abbonieren Sie auch unsere Social Media Kanäle: Auf Facebook und Google+ erfahren Sie alles über Neuigkeiten, Software, Presse, Messen, Veranstaltungen und Interviews. Über unseren Twitter-Kanal erhalten Sie gezielte Informationen zu neuen Software-Releases und Programmiertipps.

www.facebook.wibu.com
www.twitter.wibu.com
www.google.wibu.com

Business Whitepaper von Frost & Sullivan

FROST & SULLIVAN

Sicheres Lizenzmanagement für effektive Software-Monetarisierung ist der Titel des brandneuen Papiers, das wichtige Kriterien für die Entscheidung für ein Lizenzierungssystem liefert. Lassen Sie sich dieses hochinteressante, komprimierte Dokument nicht entgehen.

Microsoft Gold Partner OEM Hardware Rezertifizierung 2012

Microsoft Partner
Gold OEM

Wibu-Systems hat die Rezertifizierung zum Microsoft Gold Partner erfolgreich bestanden, zum fünften Mal in Folge seit 2008. Für Sie bedeutet dies, dass wir mit direktem Draht zu Microsoft frühzeitig neue Betriebssysteme erhalten und unterstützen sowie unsere Produkte den entsprechenden Microsoft Compliancetests wie „Windows Logo Tests" und „Windows Hardware Quality Labs", WHQL, unterziehen.

Weiterhin prüfen unabhängige anerkannte Prüflabors wie VDE und Underwriter Laboratories (UL) unsere Produkte auf Sicherheit und EMV. Dies garantiert Ihnen einen problemlosen weltweiten Einsatz.

Newsflash

+++ Firefox 16 PasswordManager PlugIn verfügbar +++ License Central 2.0 mit ausgefeiltem Reporting kurz vor Fertigstellung +++ CodeMeter Compact Runtime erweitert +++ WindRiver VxWorks Referenzsysteme mit CodeMeter im November 2012 +++ Whitepaper zu Integritätsschutz mit CodeMeter +++ Unterstützung von Windows 8 und Mac OS X Mountain Lion +++

Erfolgsgeschichte Sirona

sirona
The Dental Company

Mein Name ist CEREC und das, was ich mache, ist in aller Munde.

Früher mussten Sie zweimal zum Zahnarzt für eine Krone. Erst werden Abdruck und provisorische Füllung erstellt, dann eine Woche später wurde das im Labor hergestellte Inlay eingesetzt. Mit dem von Sirona entwickelten CEREC- Verfahren verkürzt sich die Behandlung auf eine einzige Sitzung. Der Zahn wird per Kamera ausgemessen, das Inlay per CEREC-Software vom Zahnarzt optimiert und dann aus einem farblich passenden kleinen Keramikblock ausgefräst. Dieses Inlay wird sofort in den Zahn eingesetzt: Kostengünstig und angenehm für den Patienten.

Sirona setzt mit Release 4.0 auf den hochminiaturisierten CmStick/C von CodeMeter, der seit 2011 in den Geräten für Zahnärzte steckt. Seit 2012 schützt CodeMeter auch die Software inLab für Zahntechniker und Labore, die jetzt individuell und mit günstigen Einstiegspreisen ihre Lösung aus Softwarebausteinen und Lizenzen zusammenstellen können.

Die Integration in die .NET-basierte CEREC-Software war dank leistungsfähiger CodeMeter-Tools AxProtector und IxProtector einfach. Durch individuelle Attribute im Quellcode konnte festgelegt werden, was wie geschützt werden soll. Selbst wenn die komplette Software geschützt wird, ist die Geschwindigkeit der Anwendung ausgezeichnet.

Die Übertragung von Lizenzen in die Geräte, auch nachträglich, ist optimal in den Sirona-Vertriebsprozess integriert. Der Anwender kauft eine Lizenz; die bei Sirona ausgelöste Bestellung wird automatisch in die CodeMeter License Central übertragen und generiert eine Ticketnummer, die der Anwender in einem Lizenzbrief erhält. Er gibt diese in die CEREC-Software ein und die Lizenz wird sicher über das Internet freigeschaltet.

CEREC-Geräte sind ein zugelassenes Medizinprodukt nach Medizinproduktegesetz MPG. CodeMeter stellt durch Codesignaturen sicher, dass die getestete und freigegebene Software nicht verändert werden kann. Daneben ist der CmStick/C extrem klein, als OEM-Produkt in Sirona-Farbe und besitzt weltweit alle wesentlichen Prüfzeichen bezüglich Sicherheit und EMV, wie beispielsweise VDE, UL, CE, FCC, VCCI und KCC.

Fazit: Sicherheit vor Nachbau und Know-how-Schutz für Sirona sowie Vorteile für die Anwender.

Ulrich Orth
Leiter der CAD/CAM Softwareentwicklung bei Sirona:
„Sirona ist globaler Markt- und Technologieführer in der Dentalindustrie. Unser Know-how zu schützen und den Nachbau zu verhindern ist extrem wichtig, genauso wie ein sicherer Betrieb unserer Medizingeräte nach MPG. Mit CodeMeter erfüllen wir alle Anforderungen vorbildlich und unsere Kunden erhalten Flexibilität und Preisvorteile".

Themen KEYnote 25:

- Erweitertes License Central Reporting
- Verbesserte Sicherheit durch Fallen
- Schutz von Serviceunterlagen und Dokumenten
- Hosting und Support

Vorschau:

Lesen Sie in der nächsten Ausgabe der KEYnote über unser „Erweitertes License Central Reporting". Das erweiterte Reporting umfasst umfangreiche Exportmöglichkeiten, komfortable Suche und detaillierte Übersichtsseiten.

Passend dazu erfahren Sie unter „Hosting und Support", wie wir Ihre CodeMeter License Central sicher und preiswert in der Wibu-Cloud für Sie hosten und welche Support-Level Sie dafür wählen können.

Lesen Sie außerdem, wie Sie ihre Programme durch absichtlich gelegte Fallen stärker schützen können in unserem Artikel „Verbesserte Sicherheit durch Fallen".

Wie Sie Ihre wichtigsten digitalen Dokumente zuverlässig vor Augen Dritter schützen, erfahren Sie in unserem Artikel „Schutz von Serviceunterlagen und Dokumenten".

Secure Code Webinare .NET

Secure Code Webinar

Sicherer Schutz von .NET-Assemblies gegen Raubkopieren und Reverse-Engineering, inklusive Lizenzmanagement.

Unser erfolgreiches Secure Code Seminar wird jetzt als Webinar angeboten. Erfahren Sie online, wie Sie Ihre .NET-Anwendungen innerhalb von wenigen Minuten sicher gegen Raubkopieren und Reverse-Engineering schützen.

Das Secure Code Webinar .NET richtet sich sowohl an den Produktmanager, der erfahren möchte, wie seine Lizenzmodelle mit CodeMeter realisiert werden, als auch an den Entwickler, der erfahren möchte, wie CodeMeter in .NET-Assemblies integriert wird.

Unser Webinar ist in einen Vormittags- und einen Nachmittags-Block unterteilt.

Teil 1, 9:30 Uhr bis 11:30 Uhr (Dauer 1:30h, danach 30 Minuten für Fragen und Antworten)

- Einführung in die Basistechnologie von CodeMeter
- Sichere Integration in Ihre Software durch intelligente Werkzeuge
- Fragen und Antworten

Teil 2, 14:00 Uhr - 16:00 Uhr (Dauer 1:30h, danach 30 Minuten für Fragen und Antworten)

- Einführung in die Lizenzverwaltung von CodeMeter
- Lizenzverwaltung mit der CodeMeter License Central
- Integration der License Central in Ihre Prozesse
- Fragen und Antworten

Impressum
KEYnote
24 Ausgabe, Herbst 2012

Herausgeber:
WIBU-SYSTEMS AG
Rüppurrer Straße 52-54
76137 Karlsruhe
Tel. +49 721 93172-0
Fax +49 721 93172-22
info@wibu.com
www.wibu.com

Verantwortlich für den Inhalt:
Oliver Winzenried

Redaktion:
Stefan Bamberg
Rüdiger Kügler
Oliver Winzenried

Design
Markus Quintus

Druck
E&B engelhardt und bauer,
Karlsruhe

Zuschriften sind jederzeit willkommen. Schreiben Sie uns an: global-marketing@wibu.com.
Sie sind durch das Redaktionsgeheimnis geschützt. Namentlich gekennzeichnete Artikel geben nicht unbedingt die Meinung der Redaktion wieder.

Bildernachweis:
Titelbild KEYnote24 (Leitartikel):
©iStockphoto.com/ Grady Reese
Artikel Seite 3:
©sxc.hu/timobalkr
Artikel Seite 6, Maler:
©iStockphoto.com/ DNY59
Seite 10, Glühbirne:
©sxc.hu/aldoaldoz
Seite 15, Laser und Steuergerät
©Sirona
Alle nicht gekennzeichneten Bilder/
Grafiken bei dem jeweiligen Urheber

5060-002-01/20121115