HERBST 2013



KEYnote 26

DAS WIBU-MAGAZIN

Einfache Software- und Prozessintegration

Themen

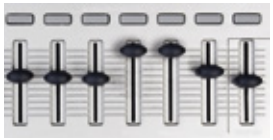
- Skalierbare Lizenzierung mit CodeMeter
- AxProtector – einfach sicher
- SmartShelter PDF: Dokumente schützen und monetarisieren

WIBU SYSTEMS

Inhalt

INFORMATION
Wibu-Systems global 3

KNOW-HOW
Skalierbare Lizenzierung mit CodeMeter 4



KNOW-HOW
Secure Boot 6

PRODUKT
AxProtector – einfach sicher 8



PRODUKT
SmartShelter PDF: Dokumente schützen und monetarisieren 10



PRODUKT
Customer Portal 12

HIGHLIGHTS
Aktuelles in Kürze 14

CASE STORY
Erfolgsgeschichte Propellerhead 15

INFORMATION
Wibu-Systems informiert 16

Sehr geehrte Kunden und Partner,



PRISM, Tempora, XKeyscore beherrschen seit Wochen die Medien. Es geht um private Daten der Bürger aber auch um Industriespionage. Für Unternehmen ist Know-how überlebenswichtig. Es steckt in Algorithmen und Verfahren in Software im PC-Bereich oder eingebaut in Geräten und Maschinen. Dazu kommen Fertigungsdaten, die wichtiges Know-how der zu produzierenden Produkte enthalten. Mit zunehmender Vernetzung bekommt „Security" in offenen Systemen höchste Priorität. Regierungen, sei es in Europa mit IEC62443, in den USA mit ISA99 oder in Asien, treiben die Sicherheitsforschung.

Die Anforderungen an Schutzlösungen nehmen zu: Im Bereich der klassischen IT wird Lizenzierung und Monitoring immer wichtiger, um Anwendern eine möglichst flexible Nutzung zu ermöglichen, aber diese dennoch abrechnen zu können. Im Industriebereich wird harte Sicherheit gegen Cyberangriffe und Manipulation wichtiger. Wir forschen und entwickeln mit CodeMeter in beide Richtungen. Die CmLicenseCentral bekommt Zusatzmodule wie Händlerfunktionalität, Benutzungsmessung und elektronische Softwareauslieferung, unsere Werkzeuge erleichtern und verbessern den Integritätsschutz und wir unterstützen zusätzliche Industrie-Umgebungen und Standards. Dies gibt Ihnen Zukunftssicherheit beim Einsatz unserer Lösungen, die Ihre heutigen Anforderungen genauso wie die kommenden erfüllen.

Lesen Sie in diesem KEYnote mit dem Leitthema „Einfache Integration in Software und Prozesse" über nützliche Neuheiten für Ihren Einsatz und sprechen Sie uns bei Fragen an.

Bis zum Jahresende sind wir auf vielen Konferenzen und Messen weltweit vertreten. Besuchen Sie uns – unsere Spezialisten und ich freuen uns auf ein persönliches Gespräch! Sollte kein Termin passen, wünsche ich Ihnen schon heute ein erfolgreiches Jahresendgeschäft und alles Gute für Sie und Ihre Familien.

Ihr Oliver Winzenried



Oliver Winzenried (Vorstand)

Wibu International Partner Summit 2013



Wibu-Systems global

Wibu-Systems, 1989 von Marcellus Buchheit und Oliver Winzenried gegründet, hat sich zu einem Global Player in seiner Branche entwickelt. Tochtergesellschaften in den USA und in China, Verkaufsbüros in Belgien, Frankreich, Großbritannien, Niederlande und Spanien sowie Distributoren in vielen weiteren Ländern bieten Ihnen und Ihren internationalen Teams technische Kompetenz und Belieferung vor Ort.

Finanziell unabhängig und inhabergeführt verfolgt Wibu-Systems mittel- und langfristige Visionen, um Ihnen, den Softwareanbietern und Geräteherstellern, weltweit Lösungen zur Softwarelizenzierung und zum Produktschutz anzubieten genauso wie Lösungen zum Schutz des Know-hows und vor Manipulation und Cyberangriffen. Die Forschung und Entwicklung befindet sich komplett am Hauptsitz in Karlsruhe, wobei Kooperationen mit Partnern und Forschungseinrichtungen in Asien, Europa und den USA bestehen. Das Produktmanagement ist global ausgerichtet, um die Anforderungen der teilweise unterschiedlichen Märkte bestmöglich erfüllen zu können. Internationale Patente unterstreichen die technologische Kompetenz und reduzieren das Risiko, Rechte Dritter zu verletzen. Die Zertifizierung des Unternehmens nach ISO 9001:2008 sowie internationale Produktprüfzeichen für Sicherheit wie Underwriters Laboratories (C-UL-US) in den USA und Kanada sowie VDE in Europa garantieren Ihnen den risikolosen Einsatz. Weiterhin erfüllen die Produkte viele lokale Standards wie CE in Europa, FCC in den USA und Kanada, KCC in Korea, RCM in Australien und Neuseeland und VCCI in Japan. Die sorgfältige Auswahl der Fertigungspartner und der verwendeten Komponenten sowie eine vertrauensvolle partnerschaftliche Zusammenarbeit gewährleisten die Einhaltung der zahlreichen neuen Anforderungen zur Vermeidung gefährlicher Substanzen wie RoHS und REACH, Joint Industry Guide (JIG) und die Beachtung der Herkunft der sogenannten Conflict Minerals. Last, but not least sind die Exportbestimmungen ein wichtiges Thema, bei dem Sie für die Anwendung der Wibu-Systems-Produkte zum Produkt- und Know-how-Schutz entsprechende Dokumente wie eine Auskunft zur Güterliste (AzG) in Deutschland oder eine Einstufung als EAR99 und NLR (No License Required) von der amerikanischen BIS erhalten.

Alle diese Punkte geben Ihnen Sicherheit beim Einsatz der Wibu-Systems-Lösungen und erfordern neben Erfahrung am Hauptsitz auch Kompetenz in vielen Ländern vor Ort. Regelmäßige Schulungen der Mitarbeiter in den Auslandsniederlassungen und bei Distributoren stellen sicher, dass Sie – oder Ihre Kollegen in den verschiedenen Ländern – optimale Beratung und Unterstützung in Landessprache bekommen. Sprechen Sie Ihren Vertriebsmitarbeiter gerne an, wenn Sie Wünsche und Anforderungen an eine lokale Belieferung in bestimmte Länder haben oder an einem globalen Support interessiert sind.





Skalierbare Lizenzierung mit CodeMeter

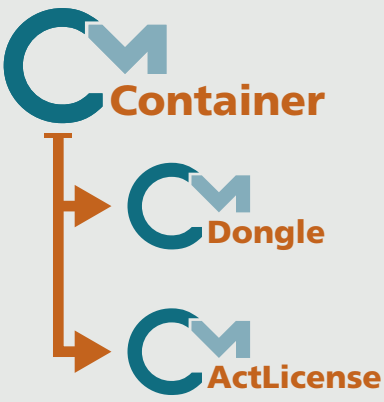
„Dongles braucht doch keiner mehr!" Diese schon vor einigen Jahren getätigte Aussage taucht in Zeiten von fortschreitender Virtualisierung immer wieder auf. Aber es ist gar nicht die Frage nach einer ganz bestimmten Technologie oder Bauform; der heutige Endkunde erwartet flexible und sichere Modelle für einen Lizenzzugriff unabhängig von den Randbedingungen, unter denen er Software einsetzt. Welche umfassenden Möglichkeiten CodeMeter dabei zur Verfügung stellt, das beschreibt der folgende Artikel.

Die Anforderungen an ein modernes Lizenzmanagement sind aus Sicht von Softwareanbietern (ISV = Independent Software Vendor) und deren Endkunden heute vielfältig. Auf der einen Seite muss es natürlich sicher sein und damit den neuesten Stand der Technologie repräsentieren, um illegales Kopieren, Reverse-Engineering und Manipulation der Software zu verhindern. Auf der anderen Seite soll es flexible Lizenzmodelle wie Netzwerklizenzen, Feature-On-Demand, Pay-Per-Use und zeitbasierte Modelle auf einfache Art und Weise abbilden können.

CodeMeter stellt Lizenzen in vielfältiger Art und Weise unter einem technischen Dach zur Verfügung und wird damit allen Anforderungen des Marktes gerecht. Hardwarebasiert (CmDongle) für ein Höchstmaß an Sicherheit und Flexibilität ebenso wie rein Software-basierte Aktivierungen (CmActLicenses) mit intelligenter Bindung an den Zielrechner. Beide Varianten arbeiten lokal und auch im Netzwerk. Daneben stehen auch ungebundene Lizenzen für Demoversionen (Trial Licenses) oder reine Softwareverschlüsselung (Protection Only) zur Verfügung. Die Lösung CmWAN ermöglicht die Nutzung von Lizenzen in der Cloud.

Der Endkunde selbst hat den Anspruch, die Lizenzmodelle des Softwareherstellers in seiner spezifischen Systemumgebung effektiv und effizient einsetzen zu können. Nur wenn das gewährleistet ist, kann der ISV mit seiner Software beim Endkunden auch erfolgreich sein. Dazu stellt CodeMeter verschiedene Möglichkeiten für den Zugriff auf Lizenzen zur Verfügung. Ein Höchstmaß an Sicherheit bietet dabei der CmDongle in unterschiedlichen Bauformen, auf den bis zu 6.000 Lizenzen auch von unterschiedlichen Herstellern gespeichert werden können. Zusätzlich lässt sich auf Wunsch auch noch zusätzlicher Flash-Speicher mitbestellen, auf dem die eigene Software auch direkt an den Kunden geliefert werden kann.

CmActLicenses dagegen kommen ohne Hardware aus, lassen sich aber beispielsweise durch die patentierte SmartBind®-Technologie sicher an den Rechner eines Endkunden binden, aber auch in virtuellen Umgebungen geschützt einsetzen.



Flexible Verwendung von Hardware- und Software-basierten Lizenzen

Dongle oder Software-Aktivierung?

Diese Frage stellt sich mit der CodeMeter-Technologie gar nicht erst. Die Integration eines Lizenzmanagements wird unabhängig von dieser Entscheidung in die Software des ISV durchgeführt. Die Entwicklung erfolgt gegen sogenannte CmContainer, die eine transparente Schicht über den später tatsächlich eingesetzten Lizenzspeicher (CmDongle oder CmActLicenses) darstellen.

Sobald die Software fertig ist, legt der ISV das gewünschte Einsatzzenario fest. Die Software kann dann mit CmDongles oder mit CmActLicenses oder sogar mit einer Kombination aus beidem ausgeliefert werden. Dies bedeutet für den ISV eine höchstmögliche Flexibilität bei der Distribution, weil letztlich erst beim Kunden festgelegt wird, mit welchem Lizenzspeicher dort tatsächlich gearbeitet werden soll. Dadurch lassen sich beispielsweise verschiedene geografische Anforderungen an ein Lizenzmanagement realisieren.

Aber auch im Bereich der Softwarewartung lässt sich ein solches Modell intelligent einsetzen. Die Software selbst ist dabei wirksam mit CmActLicenses geschützt, ein Servicetechniker erhält über einen an dem System angesteckten CmDongle aber noch weitere Wartungsroutinen freigeschaltet.

Lizenzen im lokalen Netzwerk (CmLAN)

Über lokale Lizenzen hinaus bieten Netzwerklizenzen dem Endkunden eine noch größere Flexibilität bei der Nutzung seiner Software. Dabei kommen Floating-Lizenzen (auch Concurrent-Lizenzen genannt) zum Einsatz. Der Endkunde erhält eine bestimmte Anzahl von Lizenzen vom ISV zur Verfügung gestellt, die er innerhalb seines lokalen Netzwerks verwenden kann.

Dabei kann sowohl ein CmDongle als auch eine CmActLicense für die Netzwerklizenzen genutzt werden. Der CmDongle wird einfach in den Server gesteckt und die CmActLicense ist auf dem Rechner zu aktivieren, der als Netzwerkserver dienen soll.

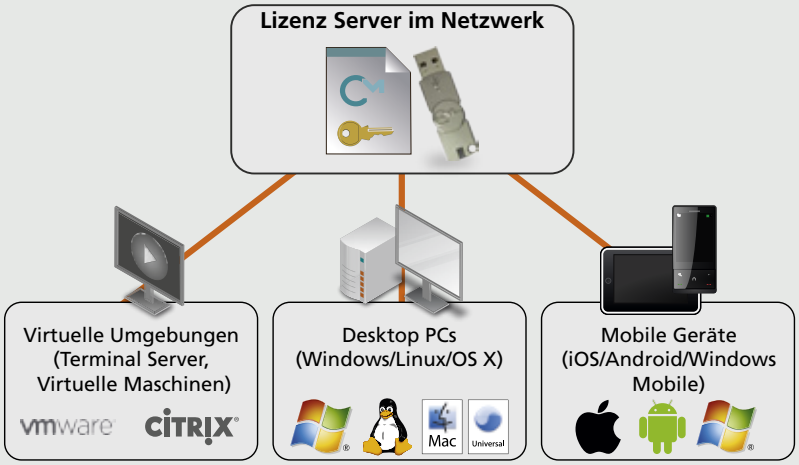
Auf dem Rechner, der im Netzwerk als Lizenzserver agiert, als auch auf allen Rechnern, die die Lizenzen verwenden möchten, wird die CodeMeter-Runtime installiert. Dann können so viele Lizenzen im Netzwerk gleichzeitig genutzt werden, wie vom ISV zur Verfügung gestellt wurden. Jeder weitere anfragende PC bekommt erst eine Lizenz zugeordnet, wenn aus dem bestehenden Lizenzpool wieder eine Lizenz freigegeben wurde.

Die Nutzung von Netzwerklizenzen bietet insbesondere in heterogenen Netzwerken große Vorteile, in denen Rechner mit unterschiedlichen Betriebssystemen auf einen gemeinsamen Lizenzpool zugreife.

Der Endkunde kann auch mehrere Lizenzserver in einem Netzwerk betreiben. Dann kann im Netzwerk die Summe aller zur Verfügung stehenden Lizenzen genutzt werden. Dadurch sind insbesondere auch Konzepte wie Lastverteilung oder Hochverfügbarkeit realisierbar.

Das bei CmWAN verwendete HTTPS-Protokoll erlaubt eine einfache Kommunikation auch durch Firewalls hindurch. Das notwendige hohe Sicherheitsniveau wird einerseits durch eine Authentisierung des Clients gegenüber dem Server gewährleistet. Zusätzlich wird eine verschlüsselte Direktverbindung zwischen Client und Server aufgebaut.

Aus Sicht eines Clients ist die Nutzung von Lizenzen in der Cloud sehr einfach. Man trägt einfach den HTTPS-Link auf den Lizenzserver in der Cloud in die Serversuchliste ein und kann in der Anwendung dann auch auf die dort bereitgestellten Lizenzen in der Cloud zugreifen.



Nutzung von Netzwerklizenzen in heterogenen Netzwerken

Lizenzen in der Cloud (CmWAN)

Eine konsequente Weiterentwicklung des Konzepts von CmLAN steht den Kunden von Wibu-Systems nun als neues Produkt CmWAN seit Einführung von CodeMeter 5.0 zur Verfügung. Mit dieser Technologie lassen sich Lizenzen nun nicht nur im lokalen Netzwerk verwenden, sondern sind jetzt auch direkt aus der Cloud heraus über ein Wide Area Network nutzbar.

Aber nicht nur lokale Software kann ab sofort mit Lizenzen in der Cloud arbeiten, auch Software, die selbst in der Cloud läuft, hat nun Zugriff auf Lizenzen, die ebenfalls in der Cloud verfügbar sind. Dabei steht auch hier wieder das ganze Repertoire der bewährten Lizenzierungsmodelle zur Verfügung, die man von der CodeMeter-Technologie kennt. Mit einer Standard-CodeMeter-Integration lassen sich sowohl lokale als auch Lizenzen aus der Cloud ohne Änderung der Software des ISV nutzen.

Die Lizenz ist immer da!

Es gibt viele verschiedene Möglichkeiten für einen ISV, Lizenzen für seine Endkunden zur Verfügung zu stellen. Ob Hardware- oder Software-basiert, ob lokal, im Netzwerk oder in der Cloud gilt: Wibu-Systems hat für jede Anforderung eine einheitliche, skalierbare Lösung. Und für Endkunden gilt ohne Kompromiss: Eine Lizenz muss zum richtigen Zeitpunkt an der richtigen Stelle verfügbar sein! Die Technologie von Wibu-Systems sorgt dafür.



Secure Boot

Mikrocontroller und elektronische Steuerungen bestimmen unser Leben. Von Atomkraftwerken über Industrieanlagen bis hin zu Zügen findet man sie überall. Vor weniger als 10 Jahren waren dies noch kleine Kästen mit proprietärer Hard- und Software: Inseln ohne Datenverbindung zur Außenwelt. Im Fehlerfall kam ein Servicetechniker zur Anlage. Zur Zeit- und Kostenreduktion werden immer mehr Steuerungen online verfügbar gemacht. Der Techniker kann so viele Incidents remote lösen. Dies eröffnet aber ein komplett neues Bedrohungsszenario: **Cyber-Physical-Attacks**.

Motivation für einen Angriff

Integrität: Warum sollte jemand eine Steuerung manipulieren? Denken Sie hier an Terrorismus oder Geheimdienste? Möglich, man denke an Stuxnet. Und Sabotage? Klingt zwar unwahrscheinlich aber was ist ein Hackerangriff auf eine unzureichend geschützte Steuerung anderes als Sabotage? Bei einer offline betriebenen Steuerung muss ein Saboteur vor Ort sein, um Schaden anzurichten. Er muss sich Zutritt verschaffen verbunden mit dem Entdeckungsrisiko. Bei einem online zugänglichen System und einer damit verbundenen Cyber-Attacke ist das Risiko für den Angreifer minimal. Der Angreifer kann sein Wissen bündeln und unerkannt mit vielen Gleichgesinnten zusammenarbeiten. Dabei spielt es keine Rolle, ob er dies aus politischen Gründen macht, jemanden erpressen will oder einfach nur beweisen will, dass er es kann.

Aber auch ein Betreiber kann ein Interesse haben, die Steuerung zu manipulieren, um seine Maschine oder Anlage zu „tunen". Doch der Betrieb außerhalb der vorgesehenen Parameter birgt Risiken, von denen erhöhter Verschleiß noch das Geringste ist. Aus Gewährleistungs- und Haftungsgründen möchte der Hersteller dieses Tuning unterbinden oder doch zumindest nachweisen können.

Vertraulichkeit: Industriespionage ist ein weiteres oft unterschätztes Bedrohungsszenario. Sowohl die Prozessparameter des Betreibers, als auch die Steuerlogik der Anlage sind für die jeweiligen Konkurrenten höchst interessant. Auch hier vereinfacht eine Remote Schnittstelle den Datendiebstahl. Während man in Action-Filmen immer sofort sieht, wer auf welche Dateien zugreift, wird in der Regel auf realen Systemen nur das Einloggen protokolliert. Oft können diese Protokolle leicht manipuliert werden. Der Datendiebstahl bleibt meist unerkannt und der Angreifer kann die Daten offline in aller Ruhe analysieren.

Wie muss ich mich schützen?

Viele Steuerungen setzen heute auf Standard-Hardware wie Industrie-PCs mit Standard-Betriebssystemen wie VxWorks, QNX, Windows oder Linux Embedded. Auch die Laufzeit-Umgebung der Steuerung ist oft ein gemeinsamer Standard (zum Beispiel CODESYS). Natürlich sollte der Zugang zum Remote-Netzwerk durch VPN- und Firewall-Lösungen geschützt sein. Dies ist aber kein ausreichender Schutz für die Steuerung selbst. Der Angreifer, der diese Hürde übersprungen hat, kann sich frei im internen Netz bewegen. Passwörter und Zugangsschlüssel für die VPNs unterschiedlicher Kunden liegen oft ungeschützt auf dem Rechner des Servicetechnikers. Da ein Gesamtsystem nur so stark sein kann wie sein schwächstes Glied reicht schon ein unachtsamer Techniker oder die Wahl eines unzureichenden Passwortes, um das komplette System zu korrumpieren.

Auf der anderen Seite können Firewall- und VPN-Lösungen Fehler und Hintertüren enthalten oder Schlüssel können zu kurz gewählt sein, speziell bei der Verwendung von RSA. Auch zeigen aktuelle Enthüllungen, dass die Sicherheit solcher Systeme nicht als ultimativ angesehen werden kann. Die Kehrseite der Veröffentlichungen ist das Risiko, dass sich mit diesen Informationen potenzielle Angreifer auf veröffentlichte Schwachstellen konzentrieren können.

Aber auch Insellösungen sind betroffen: Unterschiedliche Personen in einem Unternehmen haben physikalischen Zugang zu den Steuerungen. Servicetechniker verbinden diese mit ihren Notebooks wenn sie vor Ort sind. Backups der Steuersoftware und der Prozessparameter liegen an unterschiedlichen Stellen im Unternehmen.

Dies bedeutet, dass der Schutz schon auf dem Zielsystem, also der Steuerung selbst, anfangen muss. Auf der Steuerung darf nur Code laufen und es dürfen nur Konfigurationen sowie Prozessparameter verwendet werden, die von der autorisierten Stelle genehmigt wurden.

Die meisten Steuerungen sind im Feld aktualisierbar. Damit können neue Funktionen nachträglich ausgeliefert oder Fehler behoben werden. Diese Update-Fähigkeit ist gleichzeitig die Schwachstelle, da ein Angreifer auf diesem Weg eigenen, manipulierten Code auf die Steuerung bringen kann sowohl remote als auch lokal an der Steuerung. Um dies zu verhindern, muss die Steuerung in einer sicheren Umgebung booten und ablaufen. Alle Komponenten der Steuerung, beginnend mit dem Pre-Bootloader bis zur Applikation sollten kryptografisch authentifiziert und somit vertrauenswürdig sein. Man spricht hier von „Secure Boot".

Wie funktioniert Secure Boot?

Die einzelnen Bestandteile auf der Steuerung werden vom Hersteller oder Anlagenentwickler digital signiert. Doch wie funktioniert die Überprüfung? Auf der einen Seite überprüft die vorherige Stufe, ob die nächste Stufe gestartet werden kann. Also der Pre-Bootloader der Bootloarder. Der Bootloader das Betriebssystem. Und so weiter bis zur Application, wie in der Grafik dargestelt. Da es für die Sicherheit der ganzen Kette essenziell ist, dass der öffentliche Schlüssel bei den ersten Prüfung nicht ausgetauscht wurde, das heißt der Schlüssel muss authentisch sein. Die erste Stufe sollte nicht änderbar sein. Hier spricht man von einem sicheren Anker. Die höchste Sicherheit bietet hier ein Pre-Bootloader, der als System-On-Chip (SOC) fest eingebrannt ist. Ein zweiteiliger Bootloader, bei dem der erste Teil nicht aktualisiert werden kann, ist eine kostengünstige Alternative. Diese bietet zumindest ausreichenden Schutz gegen Remote-Angriffe.

Bin ich in einer sicheren Umgebung?

Es ist eine zusätzliche Anforderung, dass die nächste Stufe überprüft, ob die vorherige Stufe korrekt durchgelaufen ist. CodeMeter bietet beides: die Überprüfung vorwärts als auch rückwärts. Die Rückwärtsüberprüfung wird mittels einer State-Engine im CmDongle und einer mit dieser State-Engine verknüpften Verschlüsselung realisiert. Nur wenn eine Stufe ordnungsgemäß ausgeführt wurde und damit der richtige Zustand im CmDongle gesetzt ist, kann die nächste Stufe entschlüsselt werden. Dies verhindert, dass Teile der Software auf einer Simulation des Gerätes im Labor eines Angreifers laufen. Damit ist eine Analyse der Software in dieser Umgebung unmöglich. Dies verhindert Spionage, aber auch das Suchen nach Schwachstellen und Implementierungsfehlern mit dem Zweck eines späteren Angriffes und trägt somit zusätzlich zum Schutz des Gerätes bei.

Fazit

Secure Boot und Integritätsschutz durch Signatur und Verschlüsslung sind ein wesentlicher Anteil bei der Sicherung einer Steuerung. Sie erschweren physikalische Attacken nachhaltig und machen Cyber-Physical-Attacks nahezu unmöglich.

CodeMeter bietet eine Lösung, die bereits tief im Gerät eingreift und bei der sich alle Komponenten gegenseitig überprüfen. Berechtigungsstufen können fein granular definiert und an den entsprechenden Anwendungsfall angepasst werden. CodeMeter schützt gegen Spionage, Manipulation und Sabotage.

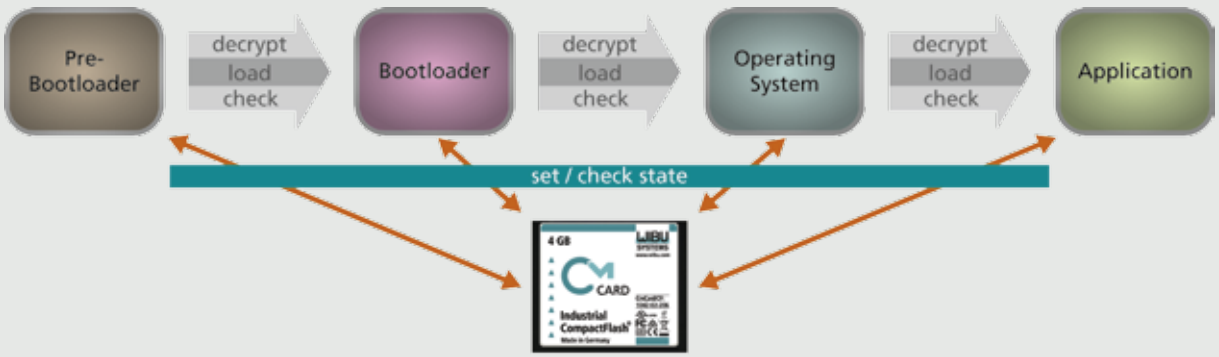
Warum so kompliziert? Reicht nicht auch ein Hash?

Bei asymmetrischer Kryptografie wie ECC wird immer ein Schlüsselpaar aus einem privaten Schlüssel und einem öffentlichen Schlüssel verwendet. Der Rückweg ist mathematisch unmöglich. Vom öffentlichen Schlüssel kann man nicht auf den privaten Schlüssel zurückrechnen.

Der private Schlüssel wird geheim verwahrt. Am sichersten kann er in einem CmDongle verwahrt werden. Der öffentliche Schlüssel ist, wie der Name bereits sagt, öffentlich für jeden verfügbar.

Und wozu sind jetzt die beiden Schlüssel? Mit dem privaten Schlüssel wird eine Signatur erzeugt, was nur die Person kann, welche diesen Schlüssel besitzt. Mit dem öffentlichen Schlüssel kann jeder die Gültigkeit der Signatur überprüfen. Aber niemand kann damit eine gültige Signatur erzeugen.

Im Gegensatz dazu hat man bei einer Hash-Funktion mit oder ohne Salt den gleichen Schlüssel zum Erzeugen des Hashwertes wie beim Überprüfen. Somit kann jeder, der diesen Hash überprüfen kann, auch einen gültigen Hash erzeugen. Eine Signatur sollte daher niemals durch einen Hash ersetzt werden. Die Sicherheit ist nur vorgegaukelt.





AxProtector – einfach sicher

Schutz von Software soll einfach und sicher sein – schließt sich das nicht aus? Dass es so nicht sein muss, zeigt Wibu-Systems mit dem AxProtector. Das Tool schützt vor Betrugsversuchen, lässt sich einfach in die Software einbauen und der Prozess des Schützens kann nahtlos in bestehende Prozesse integriert werden.

Der Schutz des geistigen Eigentums und das Sicherstellen ausschließlich lizenzierter Nutzung von Software ist nur eine der Herausforderungen, vor der ein Software-Hersteller steht. Die Auslieferung von Anwendungen erfolgt in unterschiedlichen Arten: als ausführbares Programm oder als Bibliothek. Egal ob es um Programme für die Windows-Welt, für Macs oder Linux-Systeme geht – die Lösung für diese Aufgabenstellungen hat einen Namen: AxProtector.

Hinter dem Kunstwort AxProtector (Automatic Executable Protection) verbergen sich Werkzeuge zum automatischen Schutz kompilierter Programme. Die zu schützenden Programme sind unterschiedlich: sie reichen von „richtigen" Binärdateien, zum Beispiel geschrieben in C/C++ oder Delphi bis zu vorkompiliertem Code, der in .NET für Windows oder plattformübergreifendem Java erstellt wurde. Diese verschiedenen Typen lassen sich mit AxProtector schützen, wobei unter der Haube unterschiedliche Ansätze zum Schutz verfolgt werden.

Einheitliche Oberfläche

Startet man den AxProtector, ist zunächst der Anwendungstyp auszuwählen. Danach startet die Oberfläche des Assistenten, die einen in wenigen Schritten vom ungeschützten zum verschlüsselten Programm führt. Man findet sich ohne Einarbeitung und Handbuch sofort zurecht. Der AxProtector unterstützt mehrere sogenannte Lizenzierungssysteme, sodass man ein und dasselbe Programm für die Verwendung mit verschiedenen Lizenzen verschlüsseln kann, zum Beispiel mit einer hardwarebasierten CmDongle-Lizenz oder mit einer aktvierungsbasierten CmActLicense. Oder man erlaubt beide Lizenzen; dann sucht das geschützte Programm beim Start selbständig eine passende Lizenz. Auf einfache Art kann man wählen, wie die durch die geschützte Software verwendete Lizenz gezählt werden soll, zum Beispiel pro Start der Anwendung oder nur einmal pro Rechner. Ob und wie oft die verwendete Lizenz geprüft werden soll, ist nur eine von vielen Einstellungsmöglichkeiten, die sinnvoll vorbelegt sind.

Schutz gegen Angriffe

Das geschützte Programm erkennt später selbständig Manipulationsversuche oder Angriffe von Hackern. Solche Ereignisse lösen die Sperre der verwendeten Lizenzen aus. Damit bleibt Ihr Wissen geschützt und weitere Angriffe sind unterbunden. Bei der verwendeten Verschlüsselung nutzt der AxProtector die Möglichkeiten von CodeMeter voll aus: Neben den in der Lizenz hinterlegten Schlüsseln gibt es einen softwareseitig variierbaren Schlüssel, sodass Verschlüsselungen nicht vorhersehbar sind. Auch prüft der AxProtector, ob die geschützte Software seit ihrer Verschlüsselung manipuliert wurde und verweigert in diesem Fall den Start.

Mehr Sicherheit – IxProtector

Die hohe Sicherheit der automatischen Verschlüsselung kann bei Bedarf durch die Verwendung von Funktionsverschlüsselung noch erhöht werden. Gezielt ausgewählte Funktionen werden zusätzlich verschlüsselt und nur bei Bedarf zu funktionsfähigem Code gewandelt. Dieser individuelle Schutz wird als IxProtector bezeichnet und lässt sich erfreulicherweise einfach in die

Software integrieren. Eine Markierung der Funktion, ein einfacher API-Aufruf zur Entschlüsselung bei Bedarf und die Angabe dieser Funktion in der Konfiguration – mehr bedarf es nicht.

Bei .NET und Java-Anwendungen wird aufgrund der anderen Formate grundsätzlich der Schutz über die Verschlüsselung auf Methoden- bzw. Klassenebene umgesetzt. Diese werden zur Laufzeit bei Bedarf automatisch entschlüsselt.

Modularer Schutz sowie das Auslesen oder die Verwendung von Lizenzdetails lassen sich ebenfalls mit wenigen Handgriffen umsetzen. In der Oberfläche lassen sich einfach weitere Lizenzen definieren, zum Beispiel für separat zu lizenzierende Module. Das Vorhandensein dieser zusätzlichen Lizenzen kann zur Laufzeit mit dem Wibu Universal Protection Interface (WUPI) geprüft werden. In der Kombination mit der vorgenannten Funktionsverschlüsselung können diese Module sicherheitstechnisch abgesichert werden.

AxProtector schützt folgende Programmtypen:

- Windows-Anwendungen (32-Bit, 64-Bit)
- Windows-Bibliotheken (32-Bit, 64-Bit)
- Mac OS X-Anwendungen (32-Bit, 64-Bit)
- Mac OS X-Bibliotheken (32-Bit, 64-Bit)
- Linux-Anwendungen (32-Bit, 64-Bit)
- Linux-Bibliotheken (32-Bit, 64-Bit)
- .NET Assembly
- Java-Anwendungen
- Java Servlet

Für Embedded Systeme schützt der AxProtector Anwendungen auf den folgenden Plattformen:

- Linux ARM
- Windows Embedded
- Android
- VxWorks

Komfortable Meldungsverwaltung

Sind Lizenzen nicht vorhanden, ob nun die Basis-Lizenz oder eine zusätzlich definierte, kommt eine flexible Fehlerbehandlung zum Einsatz. Das Verhalten im Fehlerfall sowie die Meldungen an den Anwender können durch Konfiguration des AxProtector und der sogenannten UserMessage-Bibliothek angepasst werden. Somit kann für eine Applikation eine individuell gestaltete Fehlermeldung angezeigt werden oder im Falle eines geschützten Dienstes die Ereignisse in eine Protokolldatei geschrieben werden.

Einfache Prozessintegration

Der Prozess des Schützens sollte fest in die standardisierten Abläufe eingebunden werden, sodass die geschützte Software schon in der Testphase verwendet wird. Im Build-Prozess kann die Verschlüsselung der Anwendungen und Bibliotheken dann einfach integriert werden. Die in der AxProtector-Oberfläche erstellten Parameter können per Knopfdruck in eine Konfigurationsdatei exportiert werden. Damit wird die Verschlüsselung mit einem Kommandozeilenaufruf automatisiert durchgeführt.

Investitionsschutz

Wibu-Systems veröffentlicht regelmäßig neue Versionen des AxProtectors, die dann neue und verbesserte Sicherheitsmechanismen an Bord haben. Durch diese kostenlosen Aktualisierungen steigt die Sicherheit Ihrer Anwendung ohne Ihr Zutun und hält somit auch in Zukunft genügend Sicherheitsabstand zu den Angreifern. Der Schutz mit AxProtector ist also nicht nur einfach, sondern wird mit der Zeit auch noch besser, damit der technologische Fortschritt nicht für unliebsame Überraschungen sorgt.

Einfach und sicher

Mit dem AxProtector können Sie also Ihre Anwendung oder Bibliothek in wenigen Schritten doppelt schützen: Die geschützte Software ist sowohl gegen Raubkopieren geschützt als auch gegen die Analyse des enthaltenen Codes. Sie sichern so Ihren Umsatz und schützen gleichzeitig das von Ihnen entwickelte Know-how.





SmartShelter PDF: Dokumente schützen und monetarisieren

Bei klassischer Software ist der Schutz gegen unberechtigtes Kopieren schon seit langer Zeit ein wichtiges Thema. Wie aber ist es um Schutz und Lizenzierung von Dokumenten bestellt? Wie lassen sich kontinuierliche Einkünfte durch den Verkauf von geschützten Inhalten erzielen oder sogar multiplizieren? Ist das Thema anders zu behandeln, weil im Detail schwieriger oder komplexer als bei Standardsoftware? Der Artikel zeigt die Gemeinsamkeiten der beiden Szenarien und geht auf die Besonderheiten des Dokumentenschutzes aus einer vertriebsorientierten Sicht ein.

Der Austausch von Informationen ist einer der grundlegenden Bestandteile unserer Kommunikationskultur. Nicht immer sollen diese Informationen unbegrenzt vervielfältigt werden dürfen oder kostenlos zugänglich sein. Das Wissen soll nur bestimmten Zielgruppen wie eigenen Servicetechnikern zur Verfügung stehen und vor Werksspionage geschützt werden. Im Zeitalter von digitalen Dokumenten in global vernetzten Systemen müssen die Verantwortlichen in anderen Kategorien denken und sind gefordert, wirksame Schutzmaßnahmen zu ergreifen. Wibu-Systems bietet dabei mit CodeMeter ein System, das unter dem Motto „One Technology Fits All" nicht nur den Anforderungen im Dokumentenbereich gerecht wird, sondern auch im klassischen PC-Bereich, bei industriellen Steuerungen und bei Cloud-basierten Lösungen optimal eingesetzt werden kann.

Dokumente einfach schützen

In den frühen neunziger Jahren hat das Unternehmen Adobe® mit PDF ein Austauschformat für digitale Inhalte auf den Markt gebracht, das heute einen weltweiten Standard darstellt. Im Funktionsumfang von Adobe Acrobat® findet sich ein Dokumentenschutzsystem, das auf der Vergabe von Passwörtern beruht. Doch die Problematik bei der Nutzung von Passwörtern ist die nicht-kontrollierbare Weitergabe und die Verwendung von viel zu kurzen Passwörtern, die ein schnelles Hacken ermöglichen.

Es ist gut, ein Passwort einzusetzen, aber der Sicherheitslevel ist in den meisten Fällen mehr als mangelhaft – lange und kryptische Passwörter erweisen sich dagegen als wenig praxistauglich. Was liegt näher, als die Erzeugung solcher Passwörter automatisch durchzuführen und sicher in einem Hardware-Dongle oder einer Softlizenz zu verwahren?

Plug-in steuert Verschlüsselung und Lizenzierung

SmartShelter PDF® klinkt sich nach der Installation als Plug-in in das Programm ein und stellt dem Benutzer Funktionen zur Erzeugung eines geschützten Dokuments zur Verfügung. Das Plug-in ist sowohl für Windows als auch für Apple Macintosh erhältlich. Das Sicherheitskonzept basiert auf einer Kombination aus einem für einen Benutzer weltweit eindeutigen Firm Code, der direkt von Wibu-Systems vergeben wird, und einem frei wählbaren Product Code. Die Kombination aus beidem bildet die Nutzungslizenz für ein Dokument. Einer der großen Vorteile der Lösung von Wibu-Systems ist, dass diese Lizenzen sowohl Hardware-basiert (CmDongle) als auch Software-basiert (CmActLicense) oder in Kombination eingesetzt werden können.

Um ein Dokument zu verschlüsseln, wird das SmartShelter PDF Plug-in aufgerufen. Der Herausgeber des Dokuments vergibt den

gewünschten Product Code. Das SmartShelter PDF Plug-in erzeugt nun ein Passwort mit sehr hoher Sicherheit und übernimmt die Verwaltung der Verschlüsselung des Dokuments und die sichere Speicherung des Passworts. Der Nutzer kommt mit dem Passwort gar nicht mehr in Berührung. Für den großflächigen Einsatz in automatisierten Umgebungen wird SmartShelter PDF als Kommandozeilenwerkzeug verwendet.



SmartShelter PDF Plug-in

Optionen zu Dokumentennutzung

Die Nutzung des Dokuments kann durch Einschränkung oder Freigabe von Rechten beim Drucken oder Ändern, aber auch auf ausschließliche Nutzung des Dokuments im Acrobat Reader® eingeschränkt werden. Zusätzlich lässt sich der Schutz weiter verschärfen: Bildschirmfotos lassen sich verhindern und die Aktivierung eines Debugger-Checks schließt bei Erkennung eines gestarteten Debuggers sofort das Dokument.

Auf Kundenseite wird einmalig ein SmartShelter PDF Plug-in für den frei verfügbaren Acrobat Reader installiert. Zum Öffnen des verschlüsselten Dokuments wird dann die korrekte Lizenz benötigt.

Flexible Lizenzmodelle ermöglichen Monetarisierung

Die CodeMeter-Technologie ermöglicht nicht nur den Schutz des Dokuments, sondern erlaubt auch vielfältige Lizenzmodelle für dessen Nutzung festzulegen. Angefangen von zeitlich begrenzten Lizenzen über Pay-per-Use bis hin zu Netzwerklizenzen stehen unterschiedliche Modelle zur Verfügung, die auch kombiniert werden können. Dadurch lassen sich neue Erlösmodelle für Dokumente definieren. Das Konzept lässt auch ein rollenbasiertes Rechtekonzept für zu schützende Dokumente zu.

Verteilung von Lizenzen leicht gemacht

Es gibt verschiedene Möglichkeiten, eine Lizenz zu verteilen. Im Falle eines Berechtigungssystems können CmDongles oder CmActLicenses mit den entsprechenden Berechtigungsstufen (Lizenzen) vorproduziert und direkt an Benutzer ausgegeben werden.

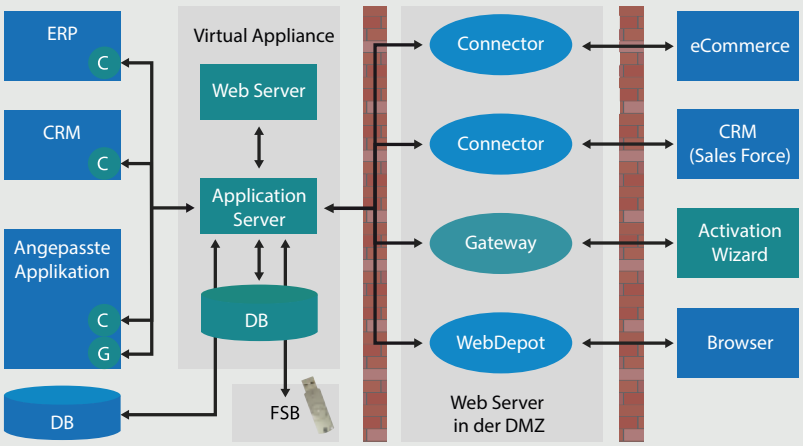
Eine höhere Flexibilität für Herausgeber und Nutzer bietet die Verwendung einer Online-Aktivierung, wie sie mit der CmLicenseCentral Internet realisierbar ist. In diesem Fall werden die Lizenzen nicht vorab erzeugt, sondern der Nutzer bezieht die Lizenzen online direkt über den Sever des Herausgebers. Damit können Lizenzen z.B. über einen Web-Shop weltweit rund um die Uhr verkauft und verteilt werden.

Der Herausgeber legt die zu verkaufenden Lizenzen in Form von Produkten in der CmLicenseCentral an. Erwirbt der Nutzer nun ein bestimmtes Produkt, so erhält er dafür vom Herausgeber der Lizenzen ein Ticket per E-Mail, das er über das Webportal des Herausgebers einmalig gegen seine Lizenzen einlösen kann. Diese werden dabei direkt auf seinen CmDongle übertragen oder als CmActLicense aktiviert.

Die CmLicenseCentral Internet kann auch in bestehende Prozesse des Herausgebers integriert werden. Dies lässt sich über die Verwendung von Web-Schnittstellen realisieren. Damit ist eine Verbindung zu existierenden internen oder externen ERP- oder CRM-Systemen möglich, um daraus direkt Bestellungen des Kunden anzustoßen und entsprechende Tickets zu erzeugen. Es kann aber auch eine direkte Integration in ein Shopsystem des Herausgebers erfolgen.

Fazit

Wer seine Dokumente nicht nur schützen sondern auch gleichzeitig mit Lizenzmodellen für seine Nutzer versehen möchte, der findet mit SmartShelter PDF eine ideale Lösung für die Erstellung geschützter Dokumente und die Erzeugung und Verteilung von Lizenzen. SmartShelter PDF ist auf der einen Seite die richtige Wahl für Herausgeber, die für jedes Exemplar auch Einkünfte erzielen möchten, und auf der anderen Seite für Unternehmen, die kostenpflichtige Inhalte auf den Markt bringen möchten oder Spezifikationen, Patentschriften und rechtliche Dokumente schützen wollen. Dabei sind sowohl die Anforderungen von Small Business-Lösungen als auch die von komplexen Systemen optimal abgedeckt.



Flexible Integration der CmLicenseCentral Internet in bestehende Prozesse



Customer Portal

Als unabhängiger Softwarehersteller (Independent Software Vendor – ISV) fragen Sie sich vielleicht: „Warum benötige ich ein Kunden-Portal?" Die Antwort ist: „Weil Sie zum Ersten **mehr verkaufen** und zum Zweiten dabei die **internen Prozesskosten reduzieren** wollen!" Ein System für Lizenzierung, Schutz und Sicherheit – wie CodeMeter – hilft Ihnen, diese Anforderungen zu erfüllen. Das Kunden-Portal ist dabei nur ein Baustein von mehreren, um diese Ziele zu erreichen. Dieser Artikel zeigt, wie ein Kunden-Portal Sie dabei unterstützt und welche Optionen es Ihnen bietet.

Was ist ein Kunden-Portal?

Ein Kunden-Portal ist eine Webanwendung, in welcher Ihr User seine gekauften Lizenzen sehen und verwalten kann. Ihr User meldet sich dazu im Kunden-Portal an. Meist erfolgt dies über einen Benutzernamen und ein Passwort. Alternativ kann dies aber auch über einen Lizenzschlüssel – das Ticket – erfolgen. Nach erfolgreichem Login kann der Kunde die von ihm gekauften Lizenzen und Software sehen. Er sieht, welche Lizenzen bereits aktiviert oder abgeholt wurden, kann die Aktivierung im Portal durchführen und sich die entsprechende Software herunterladen. Zusätzlich können De-Aktivierungen und Re-Aktivierungen als Option angeboten werden. Auch das Registrieren von Lizenzen, die über einen Händler verkauft wurden, kann hier durch den User erfolgen.

Kurzum, sowohl Sie als auch der User haben einen Gesamtblick über die gekauften Lizenzen eines einzelnen Kunden.

Wie kann ich damit mehr verkaufen?

Up-Selling und Cross-Selling an bestehende Kunden ist einfacher und kostengünstiger als das Gewinnen eines neuen Kunden. Um dies effizient durchführen zu können, ist es notwendig zu wissen, welche Lizenzen der User besitzt. Software und Lizenzen werden oft über Händler verkauft und als ISV kennen Sie Ihre eigenen User damit nur teilweise. Bieten Sie Ihrem Kunden einfach die Option, alle gekauften Lizenzen selber im Kunden-Portal zu registrieren. Durch ein Bonusprogramm, welches zum Beispiel Zusatzmodule vergünstigt oder den Zugriff auf exklusiven Online-Inhalt anbietet, kann der Kunde zum Registrieren motiviert werden.

Dies hat einen großen Mehrwert für Sie und für Ihre Kunden. Sie erhalten einen Überblick, welche Lizenzen der User bereits besitzt und können ihm gezielt Angebote schicken. Sie können das Kunden-Portal nutzen um, dem User diese Angebote anzuzeigen. Dies können Updates zu bestehenden Produkten sein, Upgrades auf einen neuen Funktionsumfang oder auch komplett andere ergänzende Produkte. Neben der Anzeige im Portal kann diese Auswertung auch für Ihren Newsletter verwendet werden.

Welche Vorteile hat der User?

Aber nicht nur Sie als ISV haben Mehrwerte von einer Registrierung im Kunden-Portal. Auch der User hat einen großen Vorteil: Seine Lizenzen gehen nicht verloren. Denn wer hat schon noch nach drei Jahren alle Lizenzschlüssel vorliegen, wenn er den alten Rechner neu installiert oder seine Software auf einen neuen Rechner umzieht? Kein User möchte hier auf die liebgewordene Software verzichten. Im Kunden-Portal findet der User alle seine Lizenzen wieder. Er benötigt dazu lediglich seine eigene E-mail-Adresse, um sich sein Passwort zurücksetzen zu

lassen, da er dies in den meisten Fällen nach dieser Zeit nicht mehr kennt.

Zusätzlich erhält er die Information, ob und welche Updates zu seinen gekauften Produkten verfügbar sind. Vor allem, wenn der neue Rechner ein neues Betriebssystem hat, ist oft ein Update der Software notwendig, um eine reibungslose Funktonalität zu gewährleisten.

Wie reduziere ich damit meine Kosten?

Typische User wechseln – je nach Zielgruppe – alle ein bis fünf Jahre den Rechner oder installieren diesen neu. Falls Sie die Lizenz in einem Dongle wie den CmDongle gespeichert haben, dann ist dieser Wechsel ohne eine erneute Aktivierung möglich. Dongle am alten Rechner abziehen, am neuen Rechner einstecken und weiterarbeiten. Im Falle einer Softwarelizenz wie einer CmActLicense ist dies anders. Der neue Rechner muss neu aktiviert werden. Nach geltendem Recht hat der Kunde ein Anrecht auf die Lizenz. Eine Bindung an einen Rechner und das Erlöschen der Lizenz mit dem End-Of-Life dieses Rechners ist in der Regel unzulässig. Das „muss neu aktiviert werden" gilt damit sowohl für Sie als den ISV, der verpflichtet ist, dies bereitzustellen und für den User, der es durchführen muss.

Und hier kommt das Kunden-Portal ins Spiel. Sie definieren ein Regelwerk für De-Aktivierungen und Re-Aktivierungen. Das konkrete Regelwerk ist stark von Produkt und Zielgruppe abhängig. So können Sie zum Beispiel festlegen, dass ein User die Lizenz jederzeit de-aktivieren und die so zurückerhaltene Lizenz auf einen neuen Rechner erneut aktivieren kann. Für den Fall, dass eine De-Aktivierung nicht möglich ist, definieren Sie eine Anzahl an initialen Re-Aktivierungen – zum Beispiel „keine weitere" – und einen Zeitrahmen, nach dem der Kunde weitere Re-Aktivierungen erhält – zum Beispiel „nach einem Jahr". Durch dieses Regelwerk erhält der User die Möglichkeit mit dem Kunden-Portal seine Lizenz selbständig in einem von Ihnen definierten Rahmen umzuziehen. Ein Supportfall ist erst notwendig, wenn Ihre Kunde diesen Rahmen sprengen. Damit behalten Sie auch weiterhin die Kontrolle über Ihre verkauften Lizenzen aber reduzieren den Supportaufwand immens.

Wer nutzt meine Software wie lange?

Als ISV möchten Sie gerne wissen, wie oft und wie lange eine spezielle Version Ihrer Software vom User eingesetzt wird. Auch hier kann Ihnen das Kunden-Portal helfen. Eine automatische Anmeldung am Kunden-Portal aus Ihrer Software heraus bietet detaillierte Nutzungsdaten. Als Motivation kann der Zugriff auf exklusive Online-Inhalte dienen. Bei dieser Gelegenheit kann die Gültigkeit der Lizenz geprüft werden.

Auch ohne eine automatische Anmeldung kann anhand der Anzahl und der Verteilung der Aktivierungen und Re-Aktivierungen eine Abschätzung der durchschnittlichen Lebensdauer eines PC in Ihrer Zielgruppe und der durchschnittlichen Lebensdauer Ihrer Software getroffen werden.



Wie hilft mir CmLicenseCentral dabei?

CmLicenseCentral unterstützt Sie bei der Implementierung eines Kunden-Portal. Mit dem Web Depot bietet Ihnen die CmLicenseCentral eine schlüsselfertige und kompakte Stand-Alone-Lösung. Sie passen lediglich das Erscheinungsbild an Ihr Corporate Design an und definieren die Regeln für De-Aktivierungen und Re-Aktivierungen. Schon ist Ihr Support entlastet. Folgende Funktionen sind im Web Depot verfügbar:

- Online-Lizenzaktivierung und De-Aktivierung
- Offline-Lizenzaktivierung und De-Aktivierung
- Automatische Re-Aktivierungen

Je nach bereits vorhandener Infrastruktur bei Ihnen kann das Web Depot modular zu einem kompletten Kunden-Portal erweitert und in die bestehenden Systeme integriert werden. Folgende Module sind dabei standardmäßig verfügbar:

- Kunden-Login (Stand Alone)
- Kunden-Login (Integriert als Single Sign On)
- Lizenzüberblick
- Kunden-Registrierung
- Lizenz-Registrierung / Ticket-Registrierung
- Anforderung und Erzeugung von Demo-Lizenzen
- Erzeugung von Notfall-Lizenzen

Mit diesen Modulen ist ein individuelles Zuschneiden des Kunden-Portals auf Ihre Anforderungen und eine Integration in Ihre bestehenden Systeme möglich. Die Funktionalitäten der CmLicenseCentral können auch per Web-Services (SOAP) direkt in ein bestehendes Portal integrieren. Die CmLicenseCentral bietet Ihnen volle Flexibilität und komplette Integration.

Aktuelles in Kürze

Weltpremiere: CmCard/CFast

Die CmCard/CFast integriert den CodeMeter Smart Card-Chip und hochzuverlässigen SLC-Flash-Speicher mit schneller SATA II Schnittstelle. S.M.A.R.T., Power-Fail-Schutz, kontrollierte BOM sind einige weitere Features der mit 2 bis 16 GB Speicher jetzt verfügbaren Karte.



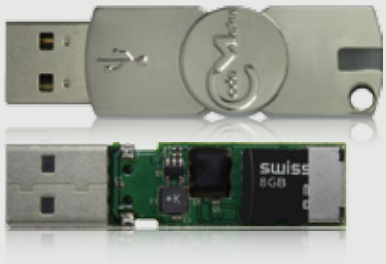
Interner CmStick/IV



Der CmStick/I zum Einbau in Geräte oder PCs erfreut sich immer größerer Beliebtheit. Der neue CmStick/IV, „Intern Vertikal", unterstützt auch kompakte Mainboards und rundet die Palette mit CmStick/I und CmStick/CI ab.

Neuer CmStick/M

CodeMeter-Funktionalität, Hardware AES-Verschlüsselung und höchste Flexibilität beim Speicher zeichnen den CmStick/M 1011-03 aus. Er wird mit industriellem SLC-Flash von 128 MB bis 16 GB bei erweitertem Temperaturbereich sowie MLC-Flash von 8 GB bis 128 GB in Q1/2014 verfügbar sein.



WHQL Zertifizierungen

Im Rahmen der regelmäßigen Kompatibilitätstests der Wibu-Systems Soft- und Hardware absolvierten im ersten Halbjahr 2013 die CmCard/SD 4GB und der CmStick für USB erfolgreich den Microsoft Windows Hardware Quality Labs Test. Dies garantiert problemlosen Einsatz beim Kunden.

Microsoft Partner
Gold OEM

Neues RCM Prüfzeichen

Wibu-Systems ist bereits heute bei den australischen Behörden registriert und hat das neue Radio Compliance Mark, RCM, für alle Produkte erhalten.

Oliver Winzenried in Verbandsgremien bestätigt

Die Mitarbeit von Wibu-Systems in Verbänden ist wichtig, um Anforderungen von Softwareanbietern und industriellen Anwendern zu verstehen. In diesem Jahr wurde Oliver Winzenried im Hauptvorstand des BITKOM bestätigt und als Vorsitzender des Vorstands der Arbeitsgemeinschaft Protect-ing im VDMA gewählt.

BITKOM

VDMA

protect-ing.de

Qualifizierung erweitert

Im Rahmen der Vorqualifizierung der CodeMeter-Hardware wurde das Prüffeld um einen Klimaschrank für Temperatur- und Feuchtetests erweitert.



Erfolgreiche Webinarserie

Ergänzend zu Workshops und Seminaren führen wir regelmäßig Webinare durch, die auf große Resonanz bei Kunden und Interessenten stoßen. Besonders Webinare gemeinsam mit Partnern wie Wind River, CODESYS oder Charismathics bieten einen Überblick aus verschiedenen Blickrichtungen. Melden Sie sich an, es lohnt sich.

CodeMeter SDK 5.10



Das neue Runtime 5.10 ermöglicht ein schnelles Einspielen von Remote-Updates in CmDongles, speziell bei vielen Product Items. Eine neue Schnittstelle ermöglicht eine Java-freie Nutzung aus dem Browser. Der AxProtector .NET 9.0 kann zusätzlich Methoden obfuskieren, Traps verwenden und ermöglicht das Konfigurieren des Cachings von unverschlüsselten Methoden. Viele weitere Änderungen lesen Sie in den Release-Notes.

Kundenzufriedenheitsumfrage

Zusammen mit TNS Custom Research haben wir erneut unsere Kunden befragt. Wir bedanken uns bei allen Kunden für die Hinweise. Neben individuellen Antworten ergab sich ein starker Wunsch nach höchster Sicherheit, auch wenn diese mit höheren Kosten verbunden ist. Unsere Kunden schätzen die plattformunabhängige Lösung mit Aktivierung, der CmActLicense, die Vielfalt an CmDongles sowie die anpassbare Backend-Integration in Vertriebsprozesse mit der CmLicenseCentral.

Gratulation an Jens Kopf, Produktmanager bei der Pilz GmbH & Co. KG: er hat bei der Verlosung unter den Teilnehmern an der Umfrage einen Gutschein für ein „Dinner for two" gewonnen hat.

Erfolgsgeschichte Propellerhead

propellerhead

Propellerhead Software ist ein 1994 gegründetes, im Privatbesitz befindliches Unternehmen mit Sitz in Stockholm, Schweden. Propellerhead ist bekannt für seine musikerfreundlichen Produkte und hat einige der weltweit innovativsten Softwareprodukte, Interface- und Technologie-Standards entwickelt und etabliert. Musiker, Produzenten und auch die Medien loben Reason, ReCycle und ReBirth als inspririerende, hervorragend klingende und qualitativ hochwertige Musiksoftware. Die Musik-App "Figure" hat 2012 die Auszeichnung "Apple's App of the Year" für seine Verfügbarkeit in verschiedenen Märkten erhalten. Technologien wie ReWire und das Dateiformat REX sind De-Facto-Industriestandards, die in vielen wichtigen Musikprogrammen implementiert sind. Aktuell werden Propellerhead-Produkte von hunderttausenden Profis und Enthusiasten für alle Aufgaben rund um das Musikmachen genutzt.



Die Herausforderung

Wir waren auf der Suche nach einer Lösung, die alle unsere Wünsche erfüllt. Sie sollte sicher und wirtschaftlich sein, genug Infrastruktur bieten, damit sie mit unseren Systemen zur Lizenzierung und Distribution funktioniert, aber gleichzeitig offen und für uns flexibel genug sein, damit wir langfristig das Wechselwirkungsschadenrisiko minimieren können.

Die Lösung

Der Einsatz von CodeMeter erlaubt uns, unseren Anwendern die gewünschten, sehr unterschiedlichen Lizenzoptionen anzubieten, was sie wirklich schätzen. Um ein Beispiel zu nennen: Wir können die gleiche Software für



den einzelnen Privatkunden mit einer Lizenz in beliebigen Schritten zu Firmenlizenzen für hunderte Mitarbeiter hoch setzen und CodeMeter arbeitet in allen Fällen gleich gut. Unsere Ingenieure setzen das API ein, um auf einfache Weise unsere Software zu schützen, sodass wir einen hochwertigen Sicherheitslevel erreichen.

Der Erfolg

Seit unserer Entscheidung für CodeMeter hat uns Wibu-Systems mit einer sehr zuverlässigen Lösung beliefert, sowohl hinsichtlich Technologie als auch Support. Der maßgefertigte CmStick, unser „Ignition Key", der CmStick/CI für den Embedded-Bereich und die aktivierungsbasierte Lösung CmActLicense geben uns ein Höchstmaß an Flexibilität und Nutzen.



Ernst Nathorst-Böös
Vorstand von Propellerhead:
„Durch den Einsatz der erstklassigen Softwareschutzlösung von Wibu-Systems konnte Propellerhead ein Lizenzierungssystem aufbauen, das besonders gut für die Anwender passt und gleichzeitig sowohl unsere Interessen als auch die unserer Partner schützt. Unsere Partner entwickeln Zusatz-Software zu unseren Produkten. Ich bezweifle, dass „Rack Extension" ohne diesen Schutz jemals einen solchen Erfolg erreicht hätte, den es jetzt hat."



Secure Code Webinare .NET

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 in 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 bis 16:00 Uhr (Dauer 1:30h, danach 30 Minuten für Fragen und Antworten)

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

Besuchen Sie uns auf folgenden Veranstaltungen:

Konferenzen:

ESWC 2013 VENICE

02. – 03. November 2013
NH Laguna Palace
Venedig, Italien

EKON 17

03. – 04. November 2013
Leonardo Royal Hotel,
Köln, Deutschland

XP 2013 DAYS GERMANY

14. – 16. November 2013
IHK Karlsruhe
Karlsruhe, Deutschland

WIND RIVER
Developer Conference China

5. November – Shenzhen, JW Marriott Hotel
6. November – Shanghai, Sheraton Pudong Hotel
8. November – Beijing, Marriott Northeast Hotel

Messen:

MEDICA®

MEDICA 2013
11-13 Uhr, TechForum Halle 12
22. November 2013
Düsseldorf Messegelände,
Düsseldorf, Deutschland

sps ipc drives 2013
Halle 7 | Stand 640
26. – 28. November 2013
Nürnberg Messe,
Nürnberg, Deutschland

Impressum
KEYnote
26 Ausgabe, Herbst 2013

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
Marco Blume
Rüdiger Kügler
Wolfgang Völker
Oliver Winzenried

Design
Markus Quintus

Druck
E&B engelhardt und bauer,
Karlsruhe, EMAS III & ISO 14001 zertifiziert

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.
Wibu®, CodeMeter®, SmartShelter® und SmartBind® sind Warenzeichen von Wibu-Systems. Alle anderen Firmen- und Produktnamen sind eingetragene Marken der jeweiligen Eigentümer.
Copyright ©2013 Wibu-Systems.
Alle Rechte vorbehalten.

Bildernachweis:
Titelbild KEYnote24:
©iStockphoto.com/alxpin
Artikel Seite 4:
©iStockphoto.com/LuisPortugal
Artikel Seite 6:
Chemiewerk: ©iStockphoto.com/CaraMaria
Agent: ©iStockphoto.com/swilmor
Artikel Seite 8:
©lassedesignen-Fotolia.com
Gepanzertes Fahrzeug: image by Krzysztof Szkurlatowski; 12frames.eu
Artikel Seite 10:
©iStockphoto.com/Cristian_Baitg
Artikel Seite 12:
©iStockphoto.com/Alina_Vincent_Photography
Alle nicht gekennzeichneten Bilder/Grafiken liegen bei dem jeweiligen Urheber

MEDIA ACCESS
PERFECTION IN SOFTWARE PROTECTION
DOCUMENT

WIBU SYSTEMS

5060-002-01/20131023 © Copyright 2013