

## WIBU-SYSTEMS AG

# CodeMeter

## -Die Digital-Rights-Management Lösung der Zukunft

### Informationen und Fragen

WIBU-SYSTEMS AG, Version 1.1, 09.03.2003,

- Deutsch-

## Inhalte

1. CodeMeter Grundlagen	2
2. Die Anwendung von CodeMeter	4
3. Details für den Licensor	5
4. Details zum CM-Stick	6
5. Details zur Benutzung beim User	7
6. Details zur zertifizierten Zeit	7
7. CM-Talk Details	8
8. Details zu den Plattformen	10
9. Details zur Sicherheit	10
10. WIBU-SYSTEMS AG	12

---

# 1. CodeMeter Grundlagen

## 1. Was ist Code Meter?

CodeMeter ist eine hardwarebasierte Technologie zur Lizenzierung und Abrechnung der Nutzung von Software und anderem geistigem Eigentum.

## 2. Wie erfolgt der Einsatz von CodeMeter über das Internet?

CodeMeter benutzt das Internet nur zum Austausch von Lizenzierungsdaten zwischen dem **Licensor** (Softwarehersteller oder Content-Anbieter, der die Lizenzen zur Verfügung stellt) und dem **User** (Benutzer der Lizenz). Nach dem Austausch der Lizenzierungsdaten, kann die lizenzierte Software oder der digitale Inhalt auf einem lokalen Rechner ohne Internet-Verbindung genutzt werden.

## 3. Welche revolutionären, neuen Ideen stehen hinter CodeMeter?

- Die **CodeMeter-Hardware (CM-Stick)** verwaltet ein Digital-Rights-Management System das Tausende von Lizenzen (Produktrechte) von Hunderten verschiedener Herstellern zur Verfügung stellt.
- Der CM-Stick ist Eigentum des Users, nicht des Licensors.
- CodeMeter erlaubt das Vermieten oder Bezahlen nach Nutzung, optional auch eingeschränkte Nutzung verschiedener Eigenschaften einer Software oder digitalen Inhalts.
- Der CM-Stick bietet für den User zusätzliche Sicherheitsmerkmale für den Schutz digitalen Inhalts.
- Der CM-Stick verwendet neueste Sicherheitstechnologie und Entschlüsselungsalgorithmen.

## 4. Wie funktioniert die CodeMeter Technologie?

Ein Licensor schließt mit einem User einen Lizenzvertrag über die Nutzung eines bestimmten Softwarepakets ab. Der Vertrag ist in einem kleinen Hardware-Stift abgespeichert, dem so genannten **CM-Stick**. Der CM-Stick befindet sich beim User und enthält Optionen für allgemeine Lizenzierung, Softwarevermietung (beschränkt auf eine bestimmte Zeit), und Bezahlung nach Nutzung. Der Vertrag wird via Internet mit Hilfe eines bestimmten Kommunikations-Protokolls, des **CM-Talk**, ausgetauscht. Mit CM-Talk erfolgt auch die Zahlung zwischen User und Licensor, optional auch über verschiedene Anbieter. Danach kann der User die Software nutzen.

## 5. Wozu wird der CM-Stick benötigt, die CodeMeter-Hardware?

Der CM-Stick verkörpert den Vertrag mit dem Licensor beim User auf technisch abgesicherte Weise. Nachdem der Vertrag ausgehändigt wurde, wird die Software per CodeMeter ohne ständige Internet-Verbindung benutzt. Der CM-Stick verwaltet die Lizenz vollständig beim User, und erkennt auch, wenn die Lizenzierungsoptionen abgelaufen sind. Erst dann muss erneut via CM-Talk eine neue Verbindung über das Internet hergestellt werden, um die Lizenz im CM-Stick aufzuladen.

## 6. Wie funktioniert das Zusammenspiel zwischen CodeMeter und der lizenzierten Software?

Das Software-Produkt bzw. digitaler Inhalt, kann unabhängig von einem CM-Stick heruntergeladen, kopiert und installiert werden. Ausführen kann man die Software aber nur, wenn man den CM-Stick besitzt, der die vom Licensor programmierten Lizenzoptionen enthält. Die Programmierung kann dabei auf jene Eigenschaften der Software beschränkt sein, die bezahlt werden müssen – alle anderen Teile können ohne CM-Stick ausgeführt werden.

## 7. Welche Vertragspartner gibt es bei CodeMeter?

Die Software ist gestaltet und lizenziert vom **Licensor** und dieser vermietet oder verkauft sie an den User. Die Bezahlung kann von einer unabhängigen Instanz, dem **Collector (Zahlungsstelle)** durchgeführt und kontrolliert werden. Auf dem „Vertriebsweg“ vom Licensor zum User kann es wahlweise zum Zwischenhandel mit einem oder mehreren **Trader** (Händler) kommen.

### 8. Müssen alle für CodeMeter beteiligten Stellen stets vorhanden sind?

Nahezu alle Seiten können autonom betrachtet werden. So kann zum Beispiel ein Softwarehersteller (Licensor) seine eigene Zahlungsabwicklung vornehmen und die Zahlungsstelle auf seine eigene Seite stellen. Es ist sogar möglich, dass die Zahlstelle auf der Seite vom User installiert wird, zum Beispiel wenn eine große Firma für alle Abteilungen ihre Zahlung zentral abwickeln möchte.

### 9. Welches Unternehmen hat CodeMeter entworfen?

CodeMeter wurde von der deutschen WIBU-SYSTEMS AG in Karlsruhe vollständig entworfen und entwickelt. WIBU-SYSTEMS produziert und verkauft auch den CM-Stick und lizenziert die für den Gebrauch von CodeMeter erforderliche Software. Das Patent für die Architektur des CM-Sticks ist in Europa, USA und Japan angemeldet.

### 10. Ist CodeMeter schon auf dem Markt?

Hinter CodeMeter verbirgt sich eine völlig neue Technologie. Seit geraumer Zeit wird es von ausgewählten Partnern aus dem PAIDFAIR Projekt (das teilweise von der Europäischen Kommission finanziert wird) getestet und bewertet: Sechs europäische Unternehmen stellen verschiedene Demonstrationssysteme zum Schutz von Software und geistigem Eigentum vor, um den Herstellern weniger Verlust durch Raubkopien zu garantieren und um zusätzliche Geschäftsmöglichkeiten durch Pay-Per-Use zu eröffnen.

### 11. Wann wird CodeMeter erhältlich sein?

Für kommerzielle Produkte wird CodeMeter ab Mitte 2003 verfügbar sein. Ein Prototyp für Demonstrationszwecke wird Ende des ersten Quartals 2003 vorgestellt (CeBIT, Computermesse in Hannover, Deutschland).

### 12. Was bedeutet PAIDFAIR?

PAIDFAIR steht als Akronym für **Protecting Accumulated Intellectual Data for Accounting in Real-Time** und ist von der EU gefördert. Sechs europäische Firmen zeigen unterschiedliche Demonstrationssysteme zum Schutz geistigen Eigentums und Software, aber auch zur Verringerung der Schäden durch Raubkopien für die Hersteller, sowie zur Erschließung neuer Vertriebswege zur Pay-Per-Use-Nutzung. CodeMeter ist die Haupttechnologie dieses PAIDFAIR-Projekts.

### 13. Ist CodeMeter kompatibel zu WIBU-KEY?

Da CodeMeter eine so revolutionäre Technologie beinhaltet, hat sich WIBU-SYSTEMS dazu entschlossen, keine Abwärtskompatibilität zu WIBU-KEY vorzusehen. Aber nahezu alle Architekturkonzepte von WIBU-KEY sind auch in CodeMeter enthalten und das mit einem sichereren und leistungsfähigeren neuen Design. Eine Migration von WIBU-KEY zu CodeMeter ist also wirklich einfach.

### Zusätzliche Information

CodeMeter Portal: <http://www.codemeter.com>

WIBU-SYSTEMS: <http://www.wibu.de>

CodeMeter Technologie <http://www.wibu.de/cm>

WIBU-KEY Technologie: <http://www.wibu.de/wk>

PAIDFAIR: <http://www.paidfair.com>

## 2. Die Anwendung von CodeMeter

14. Welche Software-Lizenzierungsmodelle werden von CodeMeter unterstützt?

CodeMeter unterstützt Gesamt-Lizenzierung, Software-Vermietung, Nutzungsoptionen:

- **General Licensing (Gesamtlizenzierung):** Vor der ersten Nutzung wird das Softwarepaket bezahlt. Die uneingeschränkte Nutzungserlaubnis wird im CM-Stick als Vertrag gespeichert. Dieses Modell ist der heutigen Softwarelizenzierung sehr ähnlich. Neu ist aber der Schutz durch den CM-Stick. Der Vertrag kann auf eine bestimmte Software-Version limitiert werden; somit können Upgrades und neue Software-Versionen getrennt verkauft und lizenziert werden.
- **Software Leasing (Softwarevermietung):** Nachdem ein Softwarepaket bezahlt wurde, kann es nur in einem bestimmten Zeitraum genutzt werden. Die Verwaltung des Zeitraums erfolgt im CM-Stick durch die Optionen *Activation Time* (Aktivierungsdatum) und *Expiration Time* (Verfallsdatum). Diese werden vom Licensor übermittelt, nachdem die Miete bezahlt wurde. Der CM-Stick benutzt dazu eine spezielle Technologie – **Certified Time** – die vom User nicht manipuliert werden kann, im Gegensatz zur Systemzeit des PCs, auf dem die Software ausgeführt wird.
- **Feature Use (Nutzungsoptionen):** Jede einzelne Ausführung einer bestimmten Funktion einer Software wird vom User bezahlt. Zur besseren Umsetzung kann diese Eigenschaft ohne Internet-Verbindung genutzt werden. Dazu verfügt der CM-Stick über eine *Unit Counter* Option (Einheitenzähler), die bei Vorauszahlung vom Licensor aktiviert wird und dessen Wert bei jeder Ausführung reduziert wird, bis der Wert Null erreicht ist. Dieser Zähler funktioniert ähnlich wie eine elektronische Geldbörse.

15. Wie sicher sind die Lizenzierungsoptionen im CM-Stick?

Alle lizenzrelevanten Elemente, die für die Bezahlung einer Lizenz, einer Vermietung oder eine Nutzungsoptionen benötigt werden, werden vollständig in der Firmware des CM-Stick kontrolliert. Diese Elemente können nur vom Licensor verändert werden, der dafür einen eigenen Sicherheitsschlüssel besitzt. Die Veränderung beinhaltet das Setzen der Eigenschaften, des Aktivierungsdatum und des Verfallsdatums sowie der Einheitenzähler. Die ausgeführte Software reduziert nur dann die Einheitenzähler, wenn ein bestimmte Eigenschaft benutzt wird.

16. Ist es möglich, ein CM-Stick an mehreren PCs gleichzeitig zu benutzen?

Ja, dies ist eine wichtige Eigenschaft von CodeMeter und ein großer Vorteil gegenüber jener Technologie, welche direkt in die Hardware des Computers integriert ist oder rein softwarebasiert ist: Die Software, die geschützt werden soll, ist vielleicht auf mehreren Computern gleichzeitig installiert, kann aber nur auf dem einen Computer benutzt werden, an dem der CM-Stick angeschlossen ist. Der User kann den CM-Stick von einem PC (etwa im Büro) auf einen anderen PC (etwa bei sich zu Hause) einfach umstecken.

17. Kann der User Lizenzierungsoptionen eines bestimmten CM-Sticks auf einem anderen CM-Stick reproduzieren?

Nein, das ist nicht möglich und daher eine wichtige Produkteigenschaft von CodeMeter: Jeder CM-Stick ist einzigartig in seinen Serieneinstellungen. Alle Verschlüsselungen und die sicheren Datentransfers zu einem bestimmten CM-Stick basieren auf dieser Serieninformation und können mit einem anderen CM-Stick nicht genutzt werden.

18. Kann eine früher gesendete Lizenzierungsoption zu einem späteren Zeitpunkt in den gleichen CM-Stick gespeichert werden?

Nein, das ist nicht möglich und daher ein weitere wichtige Gestaltungseigenschaft von CodeMeter: Jeder CM-Stick hat einen Licensor-spezifischen Zähler, der automatisch erhöht wird, sobald der Licensor neue Lizenzierungsoptionen in den CM-Stick sendet. Alle Verschlüsselungen und sicheren Datentransfers basieren auf dieser Zählerinformation und können kein zweites Mal im gleichen CM-Stick benutzt werden.

19. Erhält jeder User unterschiedliche lizenzierte Software bzw. digitalen Inhalt in Bezug auf den CM-Stick?

Normalerweise ist die lizenzierte Software bzw. der digitale Inhalt für alle User identisch und kann als identische Information an alle User via Standard-formatiertem FTP, DVD oder CD-ROM geschickt werden. Aber wenn der Licensor es wünscht, kann Software oder Information auch user-spezifisch verschlüsselt und geschützt werden.

### 3. Details für den Licensor

*20. Worin liegen die Vorteile von CodeMeter für den Licensor im Gegensatz zu einem klassischen Dongle?*

Ein klassischer Dongle wie etwa WIBU-KEY erlaubt keine gemeinsame Benutzung durch viele unabhängige Licensor, so wie das die CodeMeter-Hardware (der CM-Stick) erlaubt. Keine der momentan existierenden Dongle-Technologien verfügt über eine solche moderne Sicherheitstechnologie wie CodeMeter, die auf Hardware basiert und mit Softwareleasing und Pay-Per-Use funktioniert. Auch der Lizenztransfer vom Licensor in die Sicherheitshardware mit Hilfe der CM-Talk Methode ist keineswegs üblich und wenn vorhanden, dann nur sehr eingeschränkt.

*21. Worin liegen die Licensor-Vorteile von CodeMeter im Gegensatz zu einer softwarebasierten Sicherheitsmethode?*

Softwarebasierte Methoden weisen bei der sicheren Speicherung von Lizenz-Informationen große Schwächen auf. Nur der PC an sich kann als Speicherort dafür benutzt werden, und der PC kann relativ einfach von erfahrenen Hackern analysiert und geknackt werden. Somit können die Werte vom sicherem Ablaufdatum gefälscht oder die Zählerwerte von Nutzungsoptionen auf höhere Werte zurückgesetzt werden, ohne dass der Licensor darauf Einfluss hätte. Sicheres Softwarevermietung und Bezahlung nach Nutzung (Pay-Per-Use) ist somit nicht mehr gegeben.

*22. Wer kann CodeMeter benutzen?*

Der typische CodeMeter-Kunde ist der Anbieter von Standardsoftware, der seine Software gegen Raubkopien schützen möchte und der ein einfaches Lizenz-Management-System (CM-Talk) mit optionalem Leasing und Feature-Use-Technologie sucht. Eine andere große Kunden-Gruppe sind Anbieter digitalen Inhalts, die elektronisches Eigentum in ähnlicher Weise schützen und lizenzieren möchten.

*23. Ist CodeMeter über den klassischen Softwareschutz hinaus auch geeignet zum Schutz von geistigen Eigentums?*

WIBU-SYSTEMS plant die Entwicklung spezieller Verschlüsselung- und Lesertechnologie für CodeMeter, die für mehrere Dokument- und Datenformate unterstützt. Ein Beispiel dazu ist SmartShelter, das heute schon für WIBU-KEY erhältlich ist und welches in Zukunft das Verwalten des sicherheits- und bezahlungsbasierten Zugangs zu HTML orientierten Dokumenten und Daten erlaubt.

*24. Wie teuer ist CodeMeter für den Lizenzgeber.*

Der Preis für den Lizenzgeber basiert auf einer kleinen Gebühr, welche sich an der Anzahl der übertragenen Lizenzen in dem CM-Stick orientiert und aus einer Provision, die vom Preis der Software abhängig ist. Diese Gebühr ist unabhängig vom Preis des CM-Stick. Dieser ist Eigentum des Users. So kann CodeMeter auch für preiswerte Software benutzt werden, beispielsweise für PC-Spiele oder für die Verteilung und Bezahlung digitaler Information, die auf Kleinstbeträgen beruht.

*25. Als Software-Hersteller möchten wir CodeMeter für spezielle Zwecke nutzen. Wie können wir kooperieren?*

CodeMeter ist ein extrem flexibles Produkt mit einer Infrastruktur für allgemeine Lizenzierung über das Internet und mit einer leistungsfähigen, sichern Hardware beim User. Viele APIs (Application Programming Interfaces) erlauben Softwareherstellern, CodeMeter in schon existierende oder in neue Anwendungen auf flexible Art und Weise zu integrieren. WIBU-SYSTEMS ist sehr an der Erweiterung der Funktionalitäten von CodeMeter interessiert im Rahmen von Kooperationen mit anderen Softwareherstellern. Für weitere Informationen wenden Sie sich bitte per E-Mail an [cm@wibu.com](mailto:cm@wibu.com).

#### **Zusätzliche Information**

WIBUconcepts: <http://www.wibuconcepts.de>

## 4. Details zum CM-Stick

### 26. Wie funktioniert der CM-Stick beim User?

Der CM-Stick ist ein kleiner Stick mit einem USB-Stecker. Er ist nicht viel größer als ein Standardstecker an einem USB-Kabel. Der Stick enthält die komplette CodeMeter Sicherheitshardware in einem Sicherheitsprozessor. Der User installiert das CodeMeter-Runtime Kit, welches die Software für die Internet-Kommunikation zwischen dem CM-Stick und dem Licensor enthält, der die mit CodeMeter lizenzierte Software anbietet. Das CodeMeter-Runtime Kit stellt auch die Software zur Verfügung, die zur Ansteuerung des CM-Sticks von der geschützten Software auf der User-Seite benötigt wird.

### 27. Wie teuer ist der CM-Stick für den User?

Der Preis für einen einzelnen CM-Stick fällt in die Kategorie typischen Computerzubehörs wie Mäuse, USB-Laufwerke, Headsets etc. Ein exakter Preis wurde bis jetzt noch nicht festgelegt, bzw. gibt es auf Anfrage unter [cm@wibu.com](mailto:cm@wibu.com)

### 28. Kann ein einzelner CM-Stick für verschiedene Software-Pakete benutzt werden?

Ja. Das ist eines der bedeutenden Entwicklungsdetails von CodeMeter:

- Ein einziger CM-Stick beim User kann von vielen hundert völlig unabhängigen Licensors benutzt werden.
- Jeder Licensor kann mehrere hundert Lizenz-, Leasing oder Nutzungsoptionen speichern, um damit verschiedene Softwarepakete oder spezielle Eigenschaften dieser Softwarepakete zu steuern.

Alles in allem kann ein einziger CM-Stick Tausende von Lizenz-, Leasing- oder Nutzungsoptionen für Softwarepakete von Hunderten von Softwareunternehmen verwalten.

### 29. Wie wird der korrekte Gebrauch einer lizenzierten Software garantiert?

Eine Standardsoftware wird vom Licensor dahingehend programmiert, dass sie ohne den CM-Stick mit den korrekten Lizenzierungsoptionen nicht ausgeführt werden kann. Für diese Programmierung gibt es Hilfsprogramme, die von WIBU-SYSTEMS zur Verfügung gestellt werden. Während der Ausführung überprüft die Software abhängig von den aufgerufenen Funktionen die Feature Flags für die allgemeine Lizenzierung, die Aktivierungs- oder Verfallszeiten oder reduziert die Einheitenzähler.

### 30. Kann CodeMeter-lizenzierte Software kostenlos auf verschiedenen Rechnern installiert oder davon ein Backup angelegt werden?

CodeMeter ist keine Kopierschutztechnologie. Im Gegensatz zu softwarebasierter Kopierschutztechnologie schränkt CodeMeter die Installation, das Kopieren oder Vertreiben von Software nicht ein, sondern deren Ausführung.

### 31. Kann man den CM-Stick innerhalb eines Netzwerkes auf mehreren Rechnern benutzen?

CodeMeter unterstützt beim User den gemeinsamen Zugriff auf einen CM-Stick im Netzwerk. Der Licensor entscheidet je nach Lizenzoptionen, wie viele Kopien gleichzeitig im Netzwerk ausgeführt werden dürfen.

### 32. Wie kann man ein Softwarepaket auf dem PC im Büro und auf dem Laptop nutzen?

Man kann den CM-Stick so einfach an der USB-Schnittstelle anschließen wie beispielsweise eine Maus oder eine Digitalkamera. Somit können alle Lizenzinformationen einschließlich der aktuellen Nutzungseinheiten von einem Computer zum anderen transferiert werden.

## 5. Details zur Benutzung beim User

33. Welche Nutzen zieht der User aus dem CM-Stick außer Digital-Rights-Management?

Der CM-Stick enthält verschiedene Sicherheitselemente, die zum Schutze persönlicher Daten benutzt werden können. Zum Beispiel kann der Onlinezugriff auf viel sicherere Weise kontrolliert werden als das heute mit Passwörtern oder Schlüsseldateien möglich ist. Dateien können verschlüsselt werden; der Zugriff auf den lokalen Computer kann kontrolliert werden oder der Zugriff auf eine Web-Site kann mit Passwörtern gesteuert werden. WIBU-SYSTEMS und seine Partner werden solche Software anbieten.

34. Beim Nutzungsoptionen-Lizenz-Modell werden spezifische Werte im CM-Stick gespeichert. Was passiert, wenn der Stick beschädigt oder gestohlen wird?

Der User kann ein zeitspezifisch signiertes Backup von dem Licensor-spezifischen Inhalten des CM-Sticks erzeugen. Geht der Stick verloren, kann dieses Backup dem Licensor zugeschickt werden und bestätigt somit die Inhalte/Informationen. Auf Verantwortung des Licensors erhält ein anderer CM-Stick diese Information als neue Optionen. Der „alte“ verlorengegangene Stick wird auf eine Liste gesetzt, um zu verhindern, dass er künftig neue Lizenzinformationen erhält.

35. Wie kann der User die im CM-Stick gespeicherten Werte vor illegaler Benutzung schützen?

Mit verschiedenen PINs (Persönliche Identifikationsnummer) kann der User Licensor- oder Eigenschafts-spezifische Elemente aktivieren oder deaktivieren. Dies kann ganz allgemein angewandt werden oder auf jene kostenspezifischen Nutzungsoptionen beschränkt werden, welche die Einheitenzähler reduzieren. Selbst wenn mehrere User sich einen Stick teilen, kann jeder User mit seiner eigenen geheimen PIN die Optionen unabhängig von den anderen aktivieren oder deaktivieren.

36. Gibt es Alternativen zur PIN-basierten Sicherheit

Der CM-Stick unterstützt in Zusammenarbeit mit einigen PAIDFAIR Partnern, auch die Benutzung einer Smartcard oder eines Fingerabdrucklesers anstatt der Eingabe einer PIN. Beide Möglichkeiten erfüllen die Standards für SmartCards und für biometrische Schnittstellen.

### Zusätzliche Information

PAIDFAIR:<http://www.paidfair.com>

## 6. Details zur zertifizierten Zeit

37. Softwareleasing verwendet Zeitoptionen im CM-Stick. Wie genau funktioniert das?

Der Licensor kann unabhängig voneinander die Optionen für die Aktivierungszeit und die Verfallszeit bestimmen. Beide Optionen geben einen Zeitwert zwischen dem 1. Januar 2000 und dem 31. Dezember 2099 mit Sekundenauflösung an. Vor der Aktivierungszeit und nach der Verfallszeit kann beispielsweise eine Softwarefunktion, die diese Optionen abfragt, nicht benutzt werden. Ist keine Aktivierungszeit angegeben, kann die Funktion sofort genutzt werden, ist keine Verfallszeit angegeben, kann die Funktion uneingeschränkt genutzt werden.

38. An welcher Stelle wird die aktuelle Zeit verwaltet? Enthält der CM-Stick eine Echtzeituhr?

Der CM-Stick enthält keine Echtzeituhr, ein wichtiges Entwicklungsmerkmal. Eine Echtzeituhr muss ständig mit Strom aus einer Batterie versorgt werden. Auf der einen Seite reduziert eine Batterie die Zuverlässigkeit bei der Benutzung des CM-Sticks drastisch und auf der anderen Seite könnten Manipulationen bei der Versorgungsspannung der Uhr dessen Ausführung verlangsamen oder beschleunigen. Das sind die Gründe, warum der CM-Stick keine Echtzeituhr enthält.

39. Demnach gibt der PC selbst die Uhrzeit aus? Wie funktioniert das?

Wird der CM-Stick an einen eingeschalteten PC gesteckt, erhält er die Systemzeit von diesem PC. Solange der CM-Stick mit Strom versorgt wird, wird die Zeit im CM-Stick erhöht. Jede Licensor-spezifische Aktivierungs- oder Verfallszeit wird im CM-Stick mit diesem Wert verglichen.

40. Kann ein Hacker nicht ganz einfach eine falsche Systemzeit eingeben, um den CM-Stick zu überlisten?

Der CM-Stick verfügt noch über eine andere Zeit, die **Certified Time (zertifizierte Zeit)**. Diese Zeit ist auf einen Echtzeit-Startwert eingestellt, der während der Produktion des CM-Stick in den EEPROM-Speicher abgelegt wird, und ständig sekundengenau erhöht wird solange CM-Stick unter Strom steht. Der CM-Stick akzeptiert keinen Zeitwert vom PC der älter als die zertifizierte Zeit ist.

41. Aber diese zertifizierte Zeit wird nicht erhöht, wenn der CM-Stick keinen Strom hat. Wird dann nicht ein anderer, späterer Wert ausgegeben?

Ja, das stimmt. Deshalb kann der Licensor auch erzwingen, dass dieser Wert beim User immer aktualisiert wird. Dies erfolgt über eine Onlineverbindung zu einem **zertifizierten Zeitserver** sobald ein Lizenzvertrag abgeschlossen oder aktualisiert wird. Zertifizierte Zeitserver sind spezielle Server, die ein CodeMeter-spezifisches, korrektes Zeitzertifikat sicher in den CM-Stick übermitteln. Dieser speichert dies als neue zertifizierte Zeit.

42. Wie ist gewährleistet, dass die zertifizierte Zeit aktualisiert wird, nachdem der Lizenzvertrag abgeschlossen worden ist?

Der Licensor kann festlegen, dass seine Software den CM-Stick sperrt, bis dieser eine neue zertifizierte Zeit vom zertifizierten Zeitserver erhalten hat. Der Licensor kann die Update-Intervalle frei wählen je nach Wichtigkeit der genauen Zeit für Leasingzwecke.

## 7. CM-Talk Details

43. Wie sieht ein typischer Softwarekauf aus?

Der User sucht sich eine Software auf einer Web-Site aus und kontaktiert den Licensor bzw. die Softwarefirma. Nachdem der User den Preis des Licensors akzeptiert und bezahlt hat, wird der Lizenzvertrag in den CM-Stick beim User transferiert. Unabhängig vom Lizenzvertrag kann der User die Software downloaden und installieren. Nachdem der Lizenzvertrag im Stick gespeichert wurde, kann die Software ausgeführt werden, kontrolliert durch den Lizenzvertrag im CM-Stick.

44. Wie erfolgt die Zahlung der Software?

Die Zahlung kann unabhängig vom Licensor in einem **Collector** erfolgen. Das ist eine Zahlstelle, die eine CodeMeter-unabhängige Zahlungsart (Kreditkarte, virtuelles Geld etc.) verwendet. Nach Erhalt und Überprüfung des Geldes bestätigt der Collector den Auftrag und der Licensor transferiert den Lizenzvertrag in den CM-Stick beim User. Von dem überwiesenen Geld wird die Collector-Gebühr abgezogen, der Rest wird sofort oder in bestimmten Abständen dem Licensor ausbezahlt.

45. Wie viele Personen sind für die Abwicklung von CM-Talk erforderlich?

CM-Talk funktioniert vollautomatisch, basierend auf standardisierten Web-Services, welche im Internet mit einander verbunden sind. Der Lizenzgeber definiert die Produkte, welche verkauft werden sollen in einem Dokument, genannt PAD (Product Activation Description). Alle Verkäufe und Zahlungsmodalitäten werden in diesem Dokument gesteuert. Alle CM-Talk Aktivitäten verlaufen sehr schnell und der User muss nur Sekunden warten, bis die Softwarebestellung bestätigt ist.

46. Kann zwischen User und Licensor ein Wiederverkäufer geschaltet werden?

Der Licensor kann einen oder mehrere Wiederverkäufer – im CM-Talk-Modell **Trader** genannt – zulassen. In diesem Falle bestellt der User die Software nicht von der Web-Site des Licensors, sondern von der seines nächsten Traders. Der Licensor legt einen Preisbereich fest, in dem der Trader seine Marge definieren kann. Der Trader kennt nur den Einkaufspreis des Licensor oder des Trader davor, fügt seine Marge hinzu und schickt diesen Preis dem User oder dem nächsten Trader.

47. *Wie werden die Trader bezahlt?*

Mit Bestellung der Software erhält der Collector die Erträge aller Trader und kann so den Endpreis, den der User zahlt, auf die Margen, seine eigenen Gebühren und auf das Honorar des Licensors verteilen. Der Ertrag wird entweder sofort gezahlt oder in bestimmten Zeitabständen.

48. *Kann der Licensor je nach Kunde flexible Preise vergeben?*

Ja, der Licensor kann verschiedene Preise festlegen, die sich nach Status des Users, nach der bereits benutzten Software oder nach der Softwarebestellung (gemeinsame Pakete, etc.) richten.

49. *Wie schwierig gestaltet sich für den Licensor eine Änderung des Softwarepreis-Modells?*

Der Licensor fasst alle Preiskalkulationen in einem Dokument – dem PAD (Product Activation Description) – zusammen. Verschiedene Preisvarianten können direkt in diesem Dokument gespeichert werden oder in einer Datenbank beim Licensor, die mit der CodeMeter Software des Licensors verbunden ist.

50. *Kann der Trader unabhängig vom Licensor flexible Preise festlegen?*

Jeder Trader kann über sein eigenes PAD (Product Activation Description) verfügen, in der die verschiedenen Preisvarianten gespeichert werden. Aber der Trader kann den vom Licensor festgelegten Mindest- bzw. den Höchstpreis nicht unter- bzw. überschreiten.

51. *Kann der Trader seinen Endverkaufspreis vor dem Licensor geheim halten?*

Ja, dies ist ein wichtiges Entwicklungsmerkmal von CM-Talk: Trader und Licensor können immer nur den Preis vom vorherigen bzw. vom nachfolgenden Trader einsehen. Eine Ausnahme ist allerdings der Collector. Er muss das Honorar des Licensor, den Endverkaufspreis und die Gewinne der Trader kennen, damit er den richtigen Betrag vom User einsammeln kann und auf die/den Trader und Licensor verteilen kann.

52. *Kann der Collector oder ein Trader unabhängig vom Licensor dem User einen Lizenzvertrag schicken?*

Nein, das ist nicht möglich. Der Licensor ist die einzige Instanz mit dem Recht Lizenzverträge im CM-Stick des Users zu generieren, zu verändern oder zu löschen. Trader und Collector können die Lizenzverträge nur unverändert weitertransportieren.

53. *Wie funktioniert die CM-Talk Übertragung?*

CM-Talk verwendet Web-Services, welche dem SOAP Standards für Datenaustausch entsprechen. Bei Licensor, Collector und Trader laufen diese Services, die von den anderen CM-Talk Kommunikationspartnern aufgerufen werden.

54. *Wie leicht lässt sich diese Service-Funktionalität erweitern?*

Die PAD (Product Activation Description) erlaubt das Einbetten von SQL-basierten Datenbankzugriffen oder die Integration von .NET-Standard-basierten Windows-Komponenten. Diese Erweiterungsmöglichkeiten können fast alle Probleme in der Praxis lösen. Falls dies nicht ausreichen sollte, kann WIBUconcepts, die Beratungsabteilung von WIBU-SYSTEMS, spezielle Erweiterungen an ungewöhnliche Web-Services anpassen.

### Zusatz-Informationen

W3C SOAP Standard: <http://www.w3c.org/2000/xp/Group/>

W3C Web Service Standard: <http://www.w3c.org/2002/ws/>

WIBUconcepts: <http://www.wibuconcepts.de>

## 8. Details zu den Plattformen

55. Welche Plattformen unterstützt CodeMeter?

Der CM-Stick – die CodeMeter Hardware – basiert auf der USB-Technologie; daher unterstützt CodeMeter prinzipiell alle Plattformen, die auch USB-Schnittstellen unterstützen. Die erste Version ist für Windows 98/Me/2000 und XP verfügbar. Wird der CM-Stick über das lokale Netzwerk von einem anderen PC angesprochen, wird auch Windows 95 und NT 4.0 unterstützt.

56. Wann wird CodeMeter Apple und Unix unterstützen?

Diese Variante von CodeMeter wird Ende 2003 erhältlich sein.

57. Welche Plattformen werden beim Licensor und anderen Web-Services unterstützt?

Die Software beim Licensor, beim Trader und beim Collector basiert auf SOAP Web-Services und unterstützt momentan Windows 2000 und Windows XP. Andere Server-Plattformen, vor allem Linux, werden in Zukunft ebenfalls unterstützt werden.

58. Warum werden Windows 95 und Windows NT4.0 nicht generell unterstützt?

Beide Betriebssysteme unterstützen nicht die USB-Schnittstelle.

## 9. Details zur Sicherheit

59. Welche Verschlüsselungs-Algorithmen benutzt CodeMeter?

CodeMeter benutzt die modernsten und sichersten Algorithmen, die momentan erhältlich sind. Überall wo Daten des Licensors oder des Users durch symmetrische Verschlüsselung mit Hilfe geheimer Schlüssel gesichert werden, wird AES (Advanced Encryption Standard) benutzt. Für die asymmetrische Verschlüsselung mit öffentlichen und privaten Schlüsseln wird ECC (Elliptic-Curve-Cryptography) benutzt.

60. Welche Schlüsselgröße wird verwendet?

Die symmetrische AES-Verschlüsselung verwendet einen 128 Bit-Schlüssel. Der ECC-Algorithmus verwendet einen 224-Bit-Schlüssel. Die CodeMeter Architektur erlaubt zukünftig die Vergrößerung der ECC-Schlüsselgröße auf 256 Bit.

61. Warum wird AES verwendet, aber nicht DES, Triple DES und IDEA?

AES ist gemäß US NIST (National Institute of Standards and Technology) der offizielle Nachfolger von DES und Triple-DES. Dazu wurde er in einem internationalen und öffentlichen zweijährigen Wettbewerb aus Sicherheits- und Performance-Gründen gewählt. Der Algorithmus wurde von den belgischen Kryptographie-Experten J. Daemen und V. Rijmen entwickelt, daher auch der ursprüngliche Name Rijndael. Im Gegensatz zu DES, Triple-DES und IDEA ist AES bei weitem sicherer und schneller in der Anwendung.

62. Welche Algorithmen werden für Hashing-Operationen verwendet?

In Übereinstimmung mit der 256-Bit-Sicherheit haben wir SHA-256 (128-Bit-Sicherheit gegen Brute Force) für alle Hashing-Operationen innerhalb des CM-Sticks ausgewählt, anstatt des bekannten Vorgängeralgorithmus SHA-1 (80-Bit-Sicherheit gegen Brute Force) oder MD-5 (64-Bit-Sicherheit gegen Brute Force).

63. Ist die verwendete Schlüsselgröße groß genug für die nächsten Jahre?

In den folgenden Jahren werden Computer schneller und können leichter über globale Netzwerke miteinander verbunden werden. Somit wird es einfacher, kurze Schlüssel auch von heute sicheren Algorithmen wie DES zu knacken, indem man alle Möglichkeiten (Brute Force Methode) durchspielt. Daher genügt ein 56-Bit-Schlüssel, der 1982 sicher genug war, nicht mehr den heutigen Ansprüchen und die Zukunft.

Geht man von den Voraussagen bezüglich der Geschwindigkeit künftiger Computersysteme aus und von dem 56-Bit-Sicherheitsstandard von 1982, kann man die Größe der verwendeten symmetrischen Verschlüsselung von 128-Bit mit einem Sicherheitsstandard im Jahre 2075 gleichsetzen, der sicher genug für die nächsten 130 Jahre sein wird. Der 224-Bit ECC-Schlüssel verfügt über die gleiche Brute Force Sicherheit wie die 112-Bit-Schlüssel der symmetrischen Verschlüsselung und ist vergleichbar mit einem Sicherheitsstandard aus dem Jahre 2055 – sicher genug für die nächsten 75 Jahre.

*64. Warum wird anstatt des bekannten RSA-Algorithmus der ECC-Algorithmus (Elliptic Curve Cryptography) verwendet?*

Im Gegensatz zu RSA ist ECC schneller bei der Ver- und Entschlüsselung und kommt mit viel kürzeren Schlüsseln für die gleiche Sicherheitsklasse aus. Der typische RSA-Schlüssel hat heute eine Länge von 1024 Bit. CodeMeter funktioniert mit ECC-Schlüsseln mit einer Länge von 224 Bit, die 2048 Bit RSA entsprechen. Die CodeMeter-Architektur unterstützt für zukünftige Verwendung sogar 256 Bit ECC-Schlüssel, was einem 4096-Bit RSA-Schlüssel entspricht. Ein einzelner CM-Stick kann über 1000 voneinander unabhängige Schlüssel speichern – dank ECC und seinen kurzen Schlüsseln.

*65. Welche ECC-Standards erfüllt der CM-Stick?*

Der CM-Stick benutzt das polynomiale 224-bit ECC-Kurven-Schema, das von FIPS-182-2 und ANSI 9.62-1998 empfohlen wird.

*66. Welche Verschlüsselungs-Algorithmen unterstützt der CM-Stick direkt?*

Der CM-Stick unterstützt Einzelblock-AES, ECDSA (Elliptic Curve DSA) und ECIES (Elliptic Curve Integrated Encryption Scheme).

*67. Wie sicher ist der CM-Stick, die CodeMeter Hardware?*

Der CM-Stick enthält nur einen einzigen Chip, der Speicher (RAM und EEPROM), einen RISC-Prozessor, einen speziellen Hochleistungskryptoprozessor und die USB-Kommunikation in sich vereinigt. Dieser Chip wurde von ATMEL entwickelt und benutzt die RISC-Architektur. Dieser Controller erfüllt die Anforderungen des ISO 15408 Standard und des EAL 4, besser bekannt unter dem Namen „Common Criteria“.

*68. Wie sicher ist der Datenaustausch zwischen Licensor und User?*

Die Kommunikation zwischen Licensor und User wird Punkt-zu-Punkt verschlüsselt - unabhängig von Internet-Sicherheitsstandards. Alle Sicherheitsinformationen werden beim Licensor erzeugt und verschlüsselt und werden dann per CM-Talk an den User übermittelt. Dort kann nur der CM-Stick die Daten entschlüsseln und in seinem EEPROM-Speicher dauerhaft ablegen.

*69. Können Licensor, die sich gemeinsam einen CM-Stick teilen, ihre Lizenzen gegenseitig manipulieren?*

Nein, das ist nicht möglich und ein weiteres wichtiges Entwicklungsdetail von CodeMeter. Der CM-Stick handhabt innerhalb seines Speichers jeden Licensor-spezifischen Eintrag separat von den Einträgen anderer Licensors. Gemeinsames Benutzen, Verändern oder Wiederbenutzen eines Eintrags ist unmöglich, weil jeder Eintrag seinen eigenen Licensor-spezifischen, geheimen Schlüssel hat.

*70. Kann WIBU-SYSTEMS Lizenzen für eigene, nicht autorisierte Zwecke simulieren?*

Nein, das ist nicht möglich und ein weiteres wichtiges Entwicklungsdetail von CodeMeter. Der Licensor schickt dem User mit PKI-Verschlüsselung, die auf ECC basiert, einen geheimen Schlüssel, der nur vom CM-Stick selbst entschlüsselt werden kann. Danach wird der Schlüssel im EEPROM-Speicher abgespeichert. Da durch die PKI-Verschlüsselung ein privater Schlüssel verwendet wird, der zufällig im CM-Stick erzeugt wird, kann niemand – nicht einmal WIBU-SYSTEMS – die Entschlüsselung des geheimen Schlüssels des Licensors außerhalb des CM-Sticks vornehmen.

### Zusatzinformation

NIST Computer Security Resource Center (CSRC): <http://csrc.nist.gov/>

NIST Federal Information Processing Standards (FIPS): <http://csrc.nist.gov/publications/fips>

AES (Advanced Encryption Standard): <http://www.nist.gov/aes>

ECC (Encryption Curve Cryptography): [http://www.certicom.com/resources/ecc\\_tutorial/ecc\\_tutorial.html](http://www.certicom.com/resources/ecc_tutorial/ecc_tutorial.html)

ECDSA Standard: <http://csrc.nist.gov/encryption/tkdigsigs.html>

SHA-256 Standard: <http://csrc.nist.gov/cryptval/shs.html>

Discussion about the key size of encryption algorithms: <http://www.vaf.sk/download/keysize.pdf>

Atmel AT90SC micro controllers: <http://www.atmel.com/atmel/products/prod21a.htm>

## 10.WIBU-SYSTEMS AG

WIBU-SYSTEMS wurde 1989 in Karlsruhe von Oliver Winzenried und Marcellus Buchheit gegründet. Ziel war es, ein einfach zu handhabendes aber wirksames Kopierschutzsystem zu entwickeln.

Das Unternehmen entwickelt und vertreibt auf Hard- und Software basierende Lösungen für [Softwareschutz](#), [Dokumentenschutz](#) und [Zugangsschutz](#), Lizenzmanagement, [Electronic Software Distribution](#) (ESD) und [Digital Rights Management](#).

Eine Niederlassung in Seattle, USA und Shanghai, China, sowie [Vertriebspartner](#) weltweit unterstützen parallel den Erfolg des Unternehmens bei seinen Aktivitäten.

### Zusatzinformation

WIBU-KEY Software Protection: <http://www.wibu.de/de/wibukey.php>

SmartShelter Document Protection: <http://www.wibu.de/de/smartshelter.php>

SecuriKey Access Control: <http://www.wibu.de/de/securikey.php>

Electronic Software Distribution: [http://www.wibu.de/de/wk\\_details\\_esd.php](http://www.wibu.de/de/wk_details_esd.php)

Digital Rights Management: <http://www.wibu.de/de/cm.php>

WIBU-SYSTEMS distributors: <http://www.wibu.de/de/distributorena.php>