

# WIBU-SYSTEMS CodeMeter™ – a Revolutionary Digital Rights Management System

## White Paper and FAQ

Marcellus Buchheit, VP Research & Development, WIBU-SYSTEMS AG

Version 1.0 of 2003-Feb-05

## Contents

1	CodeMeter Basics .....	1
2	Application of CodeMeter .....	3
3	Licensor Issues .....	4
4	CM-Stick Details .....	5
5	User's Site Issues .....	5
6	Certified Time Details .....	6
7	CM-Talk Details .....	7
8	Platform Issues .....	8
9	Security Issues .....	9
10	WIBU-SYSTEMS AG .....	10

## 1 CodeMeter Basics

*What is CodeMeter?*

CodeMeter is a hardware-based technology to license and to measure the use of personal-computer-based software and other digital content.

*Does CodeMeter use the Internet?*

CodeMeter uses the Internet to exchange license data. This exchange is between the **Licensor** and the **User** of the license. The licensor is the provider of the license (software developer, digital content creator etc.). After this exchange, the licensed software or digital content can be used on a local computer without requiring any Internet connection.

*What are the revolutionary new ideas behind CodeMeter?*

- CodeMeter's hardware provides Digital Rights Management for thousands of licenses, distributed from hundreds of providers.
- This hardware is owned by the User, not the Licensor.
- CodeMeter permits leasing or pay-per-use, optionally restricted to specific features of a software or content product.
- The hardware provides additional security features for the user.
- The hardware utilizes the newest security technology and encryption algorithms.

The user makes a license agreement via CodeMeter with the licensor for a desired software package. The agreement is stored in a hardware device called **CM-Stick**. It reflects the user's options for general licensing, limited to a time frame (software leasing), and execution of specific features (pay-per-use). The agreement is exchanged over the Internet by a specific CodeMeter protocol, called **CM-Talk**, which manages also the payment between User and Licensor, optionally via additional providers. After this exchange, the software is now ready to use.

*Why is a CodeMeter CM-Stick required?*

The CM-Stick represents the agreement with the Licensor at User's Site in a secure way. CodeMeter does *not* require a permanent Internet connection after the license agreement is exchanged to execute the licensed software. The CM-Stick completely manages this license on User's Site, offline from the Licensor (or provider). This hardware detects also when the licensing options are expired. Only then another CM-Talk connection must be established via the Internet to refresh the licensing in the CM-Stick.

*How does CodeMeter work with the licensed software?*

The software product or digital content can be downloaded, copied and installed independent of a CM-Stick-stored license option. But the software product or the content reader is prepared by the Licensor that it can be executed only if the suitable licensor options are available in the CM-Stick at User's Site. This preparation can be limited to these parts of the software which have to be paid – the other parts may be executed without the CM-Stick.

*Which sites are defined in the CodeMeter business model?*

The software is designed and licensed by the **Licensor** and is leased or sold to the **User**. The payment can be controlled and handled by a third party, named as **Collector**. The "sales channel" between the Licensor and User optionally supports the intermediate trade by one or more **Traders**.

*Is it needed that all these sites exist for CodeMeter?*

Nearly all sites can be shared at one location. So a Licensor who wants to install an own payment management, installs the Collector on the own site. It is even possible that the Collector is installed on User's Site, for example when a large company wants to implement a centralized buying channel for all its divisions.

*Where was CodeMeter designed?*

CodeMeter was completely designed by WIBU-SYSTEMS AG, located in Karlsruhe, Germany. WIBU-SYSTEMS is also manufacturing and selling the CM-Stick, the CodeMeter hardware, and is licensing all required software to use CodeMeter to Users, Licensors, Collectors and Traders. The architecture of CM-Stick is patented, pending in USA, Europe and Japan.

*Is CodeMeter already on the market?*

CodeMeter is totally new designed technology, until now it is not used to manage commercial products. It is evaluated since a while by distinguished partners within the PAIDFAIR project and was optimized in this time to fulfill the requirements of the market and to cooperate with other technologies.

*When will CodeMeter be available on the market?*

CodeMeter will be available to manage commercial products in second half of 2003. A demonstration feature-complete prerelease is presented at end of first quarter 2003 (CeBIT computer fair in Hannover/Germany).

*What does PAIDFAIR means?*

PAIDFAIR is the abbreviation of "Protecting Accumulated Intellectual Data for Accounting in Real-Time" and is partially funded by the European Commission: Six European companies show different demonstration systems to protect intellectual property contents and software, to guarantee less piracy losses for vendors and to open additional business opportunities using pay-per-use solutions. CodeMeter is one the basic technology of PAIDFAIR.

*Is CodeMeter compatible with WIBU-KEY?*

Because CodeMeter is a so revolutionary technology, WIBU-SYSTEMS had decided that CodeMeter is not backwards binary-compatible to WIBU-KEY. But nearly all architecture concepts of WIBU-KEY are available again in CodeMeter in a much more secure and powerful new design. So a migration from WIBU-KEY to CodeMeter is really easy.

## Additional information

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

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

CodeMeter technology <http://www.wibu.com/cm>

WIBU-KEY technology: <http://www.wibu.com/wk>

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

## 2 Application of CodeMeter

*Which software licensing models are supported by CodeMeter?*

CodeMeter supports general licensing, software leasing and feature use:

- **General Licensing** means that a software package is paid once before first use and the unlimited usage permission is stored as agreement into the CM-Stick. This is very similar to software licensing today, but it is protected by the CM-Stick hardware. The agreement may be limited to a specific software version, so upgrades and new versions of software may be separately sold and licensed.
- **Software Leasing** means that a software package may be used in a certain time interval which is paid once before. The interval limits are managed by the CM-Stick by Activation Time and Expiration Time options which are transferred by the Licensor after the lease is paid. The CM-Stick uses a special technology, named **Certified Time**, which cannot be manipulated by the user in contrast to the system time of the computer where the software is executed.
- **Feature Use** means that each single execution of a specific function in the software by the user is paid. To support that the feature can be used without having an Internet connection between User and Licensor, the CM-Stick provides Unit Counters, which may be set by the Licensor by prepaying and which value is reduced during each execution of the feature until 0 is reached. Such a counter is similar like an electronic wallet.

*How safely stored are the licensing options in a CM-Stick?*

All licensing-relevant items, which reflects paying of a license, of a lease or of feature use, are fully controlled by the firmware of the CM-Stick. These items can be manipulated only by the Licensor, having its own secret key. This manipulation includes setting of feature, activation and expiration time or unit counters. Only the reduction of unit counters is done by the executed software when a specific feature is used.

*Is it possible that a single CM-Stick is used at several computers?*

Yes, this is an important design issue of CodeMeter and a big advantage against technology, which are integrated directly into the computer hardware or depends as software-base solution on computer-specific parameters: The software to be protected may be installed on several computers at same time, but can be used only at this computer, where the CM-Stick is connected. The user can remove the CM-Stick from one computer (for example in the office) and plug it again at another computer (for example at home).

*Is it possible that the user can reproduce licensing options from one CM-Stick to another CM-Stick?*

No, this is not possible and an important design feature of CodeMeter: Each CM-Stick is unique by its serial settings. All encryptions and secure data transfers to a specific CM-Stick depends on this serial information and cannot be used by any other CM-Stick.

*Is it possible that an earlier sent licensing option is later stored into the same CM-Stick a second time?*

No, this is not possible and another important design feature of CodeMeter: Each CM-Stick has a Licensor-specific counter which is automatically increased whenever a Licensor sends new licensing options to the CM-Stick. All encryptions and secure data transfers to a specific CM-Stick depends on this counter information and cannot be used a second time in the same CM-Stick.

*Is the licensed software or the digital content different for each user in dependence of the CM-Stick?*

Typically, the licensed software or digital content is identical for all users and can be distributed as identical information to all users via standard-formatted FTP, DVD or CD-ROM. But for very unique and user-specific information, this is an option, also completely supported by CodeMeter technology.

### 3 Licensor Issues

*Where are the advantages for a Licensor using CodeMeter in contrast to a classic dongle?*

A classic dongle, like WIBU-KEY, does not permit a general sharing between many independent licensors like the CodeMeter hardware (CM-Stick) does. Furthermore nearly none of the currently existing dongle technologies are providing such a safe software leasing and pay-per-use hardware security technology like CodeMeter does. The over-all number of licenses which could be stored within a CM-Stick is much higher than the capacity of classic dongles. Also the automatic transfer of licenses from a licensor into the protection hardware via a method like CM-Talk is typically not available or much more limited. Complete business transaction from pricing, buying, license generating and transfer is fully automated.

*Where are the advantages for a Licensor using CodeMeter instead of software-based protection methods?*

Software-based methods have a lot of weaknesses in saving licensing information in a secure way: Only the hardware of the personal computer itself can be used as location for this; this hardware can always be analyzed and cracked by experienced hackers. So expiration time values can be faked or feature-use counter values set back to higher values without influence of the licensor – which results in canceling of safe software leasing or pay-per-use.

mobility?

*Which Licensor can use CodeMeter?*

The typical Licensor of CodeMeter is a provider of standard software which should be protected against piracy and who wants to use an easy and full-automatic licensing management (CM-Talk) and optional leasing and feature-use technology. Another large group of Licensors are content provider who wants to protect and to license electronic properties in a similar way.

*Is CodeMeter also suitable to manage Intellectual Property content beyond of the classic software protection?*

WIBU-SYSTEMS plans to design special encryption and reader technology for several document and data formats which are managed by CodeMeter. One example is SmartShelter, which is available today for WIBU-KEY, and which can be used in future to management the secure- or payment-based access of HTML-orientated documents and data.

*How expensive is CodeMeter for a Licensor which is using it?*

The price for the Licensor to use CodeMeter technology is based on a small fee, which is calculated from the number of licenses transferred into the CM-Stick and from a commission of the price of sold software. This fee is independent of the price of the CM-Stick, which is owned and paid by the user and not by Licensor. So CodeMeter may also be used for cheap software, for example computer games, or for distributing and paying micro-payment-based digital information.

*As software developer we want to use CodeMeter for special purposes. How can we cooperate?*

CodeMeter is a very flexible product which provides a general licensing infrastructure via Internet and a powerful, safe hardware on user's site. Many application programming interfaces (API) permit software developers to integrate CodeMeter in a similar flexible way into existing or new application. WIBU-SYSTEMS is very interested to expand the general functionality of CodeMeter by a cooperation with other software developers. Please contact WIBUconcepts for more information.

**Additional information**

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

## 4 CM-Stick Details

*How is a CM-Stick working at User's Site?*

The CM-Stick is a small stick with a USB connector; it is not much longer than a standard connector at a USB cable. It contains the complete CodeMeter protection hardware in a security processor. The User installs the CodeMeter Runtime Kit which contains all software to establish the communication via Internet between the local CM-Stick and the Licensor, providing software, which is licensed by CodeMeter. The CodeMeter Runtime Kit handles also the connection between the executed licensed software and the CM-Stick on User's Site.

*How much is the CM-Stick for the User?*

The price for a single CM-Stick will be in the typical range of "personal computer accessories" like mice, USB drives, headsets etc. The exact price of a single CM-Stick for the user has not finally decided until now.

*May a single CM-Stick be used for several software packages?*

Yes, this is one of the major design issues of CodeMeter:

- A single CM-Stick at User's Site can be shared by many hundreds of totally independent Licensors.
- Each Licensor may store many hundred licensing, leasing or using options to control different software packages or specific features of such packages.

Altogether a single CM-Stick may handle thousands of licensing, leasing or using options for software packages of hundreds of Software companies.

*How is guaranteed that a licensed software is properly used?*

A standard software package is modified by the Licensor that it needs always a CM-Stick, containing the suitable licensing options, to be executed. This modification is done by tools, provided by WIBU-SYSTEMS. During the execution, the software checks Feature Flags for general licensing, checks Activation or Expiration Times for leasing or reduces Unit Counters during use, depending on the executed feature in the software.

*Can CodeMeter-licensed software be freely installed on several machines or be saved as backup?*

CodeMeter is not a copy-protection technology. In contrast to software-based copy protection technology, CodeMeter does not restrict installing, copying or distributing of software, but restricts their execution.

*Is it possible to share a CM-Stick between several computers in a network?*

CodeMeter supports on User's Site the shared use of a single CM-Stick in a local network. In dependence of the licensing details, the Licensor decides how many copies may be executed at same time within such a network.

*What happens if two computers are not connected by a network, for example sharing a software package between office and laptop?*

The CM-Stick can be easily plugged and unplugged at USB like a mouse or a digital camera. So all licensing information, including current usage units may be transferred from one computer to another and CodeMeter supplies for the user a high mobility of the licensing information.

## 5 User's Site Issues

*Are there any benefits of the owner of the CM-Stick at User's Site beyond the use for Digital Rights Management?*

The CM-Stick contains several security elements which can be used also to protected personal data at User's Site or control online access in a much more personal secure way than password or a key file can do this today. For examples, files could be encrypted, the access to the local computer can be controlled or passwords to access a

Website. The User can also store personal passwords, pin numbers and other secure information within the CM-Stick, protected against unauthorized access. Such software is shipped by WIBU-SYSTEMS and by its partners.

mobility of licenses

*At least in the Feature Use license model, a CM-Stick stores a specific value. What happens if the CM-Stick is damaged or stolen?*

The User can create a time-specific signed backup of the Licensor-specific contents of the CM-Stick. If the CM-Stick is lost, this backup information may be sent to the Licensor, who validates the information and transfers this (by Licensor's responsibility) as new options into another CM-Stick. The old CM-Stick can be set on a locking list to avoid that it is receiving future licensing information again.

*How can the user protect the stored values in the CM-Stick against unauthorized use?*

The user can enable or disable licensor-specific or feature-specific items within the CM-Stick by one or more PIN (Personal Identification Numbers). This restriction may be general or limited to the cost-intensive Feature Use by reducing Unit Counter options. Even if several users share a single CM-Stick for software use, everybody may use an own secret PIN to handle the enabling and disabling independently.

*Are there alternatives for the PIN-based security?*

The CM-Stick supports also, in cooperation with several PAIDFAIR partners, the use of a Smartcard or of a fingerprint reader instead of entering a PIN number. Both alternatives fulfill the standards concerning Smartcards and biometric interfaces.

### Additional information

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

## 6 Certified Time Details

*Software Leasing uses time options in the CM-Stick. How does this work?*

A Licensor may specify an Activation Time option and an Expiration Time option independently. Both specify a time value in second resolution between 1<sup>st</sup> January 2000 and 31<sup>st</sup> December 2099. A software feature which checks these options cannot be used before the Activation Time and after the Expiration Time. If no Activation Time is specified, the feature can be used immediately; if no Expiration Time is specified, the feature can be used unlimited into the future.

*Which instance manages the current time? Is there a real-time clock in the CM-Stick?*

It was an important design issue for the CM-Stick that it does not contain a real-time clock. Such a clock requires permanent power, coming from a battery. On the first hand, such a battery reduces the reliability of the CM-Stick dramatically; on the other hand, manipulations in the power or clock management would permit to slow or to speed up the real-time clock. That's why a CM-Stick does not use a real-time clock.

*So the personal computer itself dispenses the current time? How is this handled?*

When the CM-Stick is plugged at a switched-on personal computer, it receives the system time from this computer. During the CM-Stick has power, this time is increased in the CM-Stick itself. All comparisons with a Licensor-specific Activation Time or Expiration Time are done in the CM-Stick against this value.

*Isn't it easy for a cheating user to set a wrong system time to outwit the CM-Stick?*

The CM-Stick contains another time, named as **Certified Time**. It is set to a real-time start value during the production of the CM-Stick into the EEPROM memory and increased in this memory each time the CM-Stick has power. The CM-Stick does not accept a time value from the personal computer which is older than this Certified Time.

*But this Certified Time is not increased when the CM-Stick does not have power? So this value may be late-behind?*

Yes, this is right. That's why a Licensor can force that this value is updated at User's Site by an Internet connection to a **Certified Time Server** when a licensing agreement is established or updated. These are special servers which send a CodeMeter-specific correct time certificate in a secure form to the CM-Stick, which stores this as new Certified Time.

*How is guaranteed that the Certified Time is updated after the licensing agreement is established?*

The Licensor can define that its software is locking the CM-Stick time by time until a new Certified Time is received from a Certified Time Server. The length of this update-force interval may be chosen freely by the licensor, depending on the importance of a very precise time for leasing purposes.

## 7 CM-Talk Details

*How a typical license sale is done, for example for a software product?*

The User chooses a software product at a website and establishes a contact to the Licensor, the software company behind the product. The Licensor resends the price for the product and after accepting and paying the amount, the Licensor sends a License agreement into the CM-Stick of the User. Independent of this agreement, the User can download the software and install it. After storing the agreement into the CM-Stick, the software product may be executed, controlled by the license agreement in the CM-Stick.

*How the payment of the license sale is organized?*

The payment management may be independent of the Licensor and is handled in a **Collector**. This is a clearing location using payment technology independent of CodeMeter (credit card, cyber money etc.). After receiving and verifying the payment, the Collector confirms the order to the Licensor and that is sending the License agreement into the CM-Stick of the User. The received money is reduced by the Collector's fee; the remains are sent immediately or added-up in specific intervals to the Licensor.

*How many persons are required for such a CM-Talk sale?*

CM-Talk runs fully automatically, based on standardized Web Services which are loosely connected via the Internet. The Licensor defines the products to sale in a document, named PAD (Payment Activation Description) and all sales and payment management is controlled by this document. All CM-Talk operations are running in a very short time, so the user typically must wait only seconds until a software order is confirmed.

*Is it possible to integrate Resellers between User and Licensor?*

The Licensor may permit one or more resellers, named as **Trader** in the CM-Talk model. Then the User is not ordering the software at the website of the Licensor but on that of the nearest Trader. The Licensor defines a price interval within a trader may set a margin. The Trader sees only the received price from the Licensor or the Trader before, adds its margin and sends the price to the User or the next Trader.

*How such Traders are paid?*

During the order of the software package the Collector receives the margin values of all traders and automatically splits the User's retail price into these margins, the own fee and the royalty of the Licensor. Then the margin values are sent immediately or added-up in specific intervals to the legitimated traders. Also this money transfer can be done in an automatic way.

*Is it possible for the Licensor to make flexible prices, depending on a specific customer?*

Yes, a Licensor may define different prices depending on the status of a user, on the software which is already used there, or on the software order (shared packages etc.). CM-Talk selects then the best available price for a user by its automatic process.

*How difficult is the change of a software price model for the Licensor?*

All price calculations are done by the Licensor in the PAD document (Payment Activation Description). Several price variants may be stored directly in this document or in a Licensor-site database which is connected with the Licensor's Site CodeMeter software. So modifying a price model is typical an operation of few minutes.

*Is it possible for the Trader to make flexible prices independently from the Licensor?*

Even each Trader may have an own PAD (Payment Activation Description) where several price variants are stored. CM-Talk selects again automatically the best available price of a user. But a trader cannot exceed the minimum or maximum price which may optionally be defined by the Licensor.

*Can a Trader keep its retail price secret against a Licensor?*

Yes, this is an important design issue of CM-Talk: Each Trader and the Licensor can see only the price of the direct successor or predecessor. An exception is the Collector: This site must see the royalty, the User's retail price and all Trader margins to collect the correct amount from the User and to distribute the margins and royalty to the Traders and the Licensor.

*May a Collector or Trader send a license agreement independently from the Licensor to the User?*

No, this is not possible. The Licensor is the single instance which has the rights to create, modify or delete license agreements in a CM-Stick at User's Site. Trader and Collector may only transfer such agreements.

*How the CM-Talk transfer is realized?*

CM-Talk is using Web Services which fulfill the SOAP standard for exchanging data. Licensor, Collector and Trader are running such services which are called from the CM-Talk communication partner.

*How easily can this service functionality be extended?*

The PAD (Payment Activation Description) permits the embedding of SQL-based database access points or the integration of components, for Windows based on the .NET standard. This extensibility can solve nearly all extension problems in the practice. If this is not enough, WIBUconcepts, the consulting division of WIBU-SYSTEMS, can adapt special extension to the out-of-box web services.

### **Additional information**

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

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

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

## **8 Platform Issues**

*Which platforms are supported by CodeMeter?*

Because the CM-Stick – the CodeMeter hardware – is based on USB, CodeMeter principally supports all platforms where the USB interface is supported. The first release will be available for Windows 98, Windows Me, Windows 2000 and Windows XP. Windows 95 and Windows NT 4.0 are supported when the CM-Stick is addressed via the local network at another computer.

*When Apple Macintosh and Unix are supported by CodeMeter?*

Variants of CodeMeter on User's Site for Apple Macintosh MacOS X and Linux will be available until end of 2003.

*Which platforms are supported at the Licensor's Site and other CM-Talk Web Services?*

The software at Licensor's Site, CM-Talk Trader's Site and Collector's Site is based on SOAP Web Services and supports Windows 2000 and Windows XP at the moment; other server platforms, primarily Linux will follow in the future.

*Why Windows 95 and Windows NT 4 are not generally supported?*

Both operating systems are not supporting the USB interface.

## 9 Security Issues

*Which encryption algorithms are used in CodeMeter?*

CodeMeter uses the most modern and most secure algorithms which are available in the moment. For all purposes where Licensor's data or User's data are protected by symmetric encryption, using secret keys, AES (Advanced Encryption Standard) is used; for asymmetric encryption, using public and private keys, ECC (Elliptic Curve Cryptography) is used.

*Which key size is used?*

All symmetric AES encryption uses 128-bit for keys, the used ECC algorithm is based on 224-bit keys, the CodeMeter architecture permits to expand the ECC key size to 256-bit in future.

*Why AES is used and not DES, Triple DES or IDEA?*

AES is the official successor for DES and Triple DES, defined by the US NIST (National Institute of Standards and Technology). It was elected in an international and public competition during more than two years by security and performance reason. The algorithm is designed by the Belgium cryptography experts J. Daemen and V. Rijmen, originally named as Rijndael. In contrast to DES, Triple DES and IDEA, AES is much more secure and faster in execution.

*Which algorithms are used for data hashing?*

In accordance with the 256-bit security, the SHA-256 (128-bit security against brute-force) is selected for all hashing operations inside of the CM-Stick instead of the well-known predecessor algorithms SHA-1 (80-bit brute-force security) or MD-5 (64-bit brute force security).

*Is the used key size large enough for the next years?*

Computers become faster and can be connected easier via global networks in the following years. So it is easier to crack shorter keys even for secure algorithms like DES by checking all possibilities (Brute Force method). So a 56-bit key which was safe enough in 1982 was becoming weak in the last 20 years. Using the prediction of the speed of future computer systems, the used symmetric-encryption size of 128 bit reflects the security standard of 2075 like 56-bit in 1982 and is safe enough for the next 130 years. The 224-bit ECC key has the same Brute-Force-security like 112-bit symmetric encryption keys and reflects the security standard of 2055 – good enough for the next 75 years.

*Why ECC (Elliptic Curve Cryptography) is used and not the well-known RSA algorithm?*

In contrast to RSA, ECC is faster in encryption and decryption and needs much shorter keys for the same security class. Typical RSA keys of today have a length of 1024 bit. CodeMeter uses ECC keys with a length of 224-bit which corresponds with 2048-bit RSA. The CodeMeter architecture supports even 256-bit ECC keys for future use, which corresponds with 4096-bit RSA. Selecting ECC and its short keys, a single CM-Stick as CodeMeter hardware can store more than 1000 independent keys.

*Which ECC standards are fulfilled by the CM-Stick?*

The CM-Stick uses the polynomial 224-bit ECC curve and scheme, which is recommended by FIPS-182-2 and ANSI 9.62-1998

*Which encryption algorithms are directly supported by the CM-Stick?*

The CM-Stick supports single-block AES, ECDSA (Elliptic Curve DSA) and ECIES (Elliptic Curve Integrated Encryption Scheme).

*How safe is the CM-Stick, the CodeMeter hardware?*

The CM-Stick uses only one chip including all memory (RAM and EEPROM), a RISC processor, a special high-performance crypto processor and the USB communication. This chip is designed by Atmel, an US-based semiconductor company, and uses the AVR RISC Architecture. The design of this controller orientated to fulfill the ISO 15408 standard and the EAL3 certification level, better known as Common Criteria. The controller performs a lot of other standards, for example the internal random number generator fulfills the FIPS 140-1 standard.

*What is about security in the data transfer between licensor and user?*

The communication between licensor and user is encrypted and as point-to-point implementation independent on any Internet security standards: All security information is created and encrypted on Licensor's Site and then transferred via CM-Talk to the user, only the CM-Stick hardware itself can decrypt the data and store the created data into its EEPROM memory.

*Is it possible that shared licensors of a single CM-Stick manipulate their licenses vice-versa?*

No, this is not possible and an important design issue of CodeMeter: The CM-Stick handles each Licensor-specific item separately from all other Licensor-specific items within its memory, any sharing, modification or reuse of another item is impossible because each item has its own unique Licensor-specific secret key.

*Is it possible for WIBU-SYSTEMS to simulate a license of a Licensor for own unauthorized use?*

No, this is not possible and another important design issue by CodeMeter: The Licensor transfers a secret key by public-key encryption, based on ECC, to the user, which can be decrypted only by the CM-Stick itself to store the key into its EEPROM memory. Because the public-key encryption addresses a private key, which is randomly created in the CM-Stick, nobody can perform this decryption outside of the CM-Stick, even not WIBU-SYSTEMS.

### **Additional information**

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/keysizes.pdf>

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

## **10 WIBU-SYSTEMS AG**

WIBU-SYSTEMS was founded in 1989 in Karlsruhe/Germany by Oliver Winzenried and Marcellus Buchheit, with the focus to develop an easy to use and effective Software copy protection system.

The company develops and distributes solutions, based on hardware and software, for copy protection, document protection and access control, license management, Electronic Software Distribution (ESD) and also Digital Rights Management.

The headquarters of WIBU-SYSTEMS is located in the middle of the technological heart of Germany: Karlsruhe. WIBU-SYSTEMS, as a prosperity-orientated firm, sees the satisfaction of their customers and using newest technology in their products as highest priority in their company philosophy.

Offices in Seattle/USA and Shanghai/China, as well as our distributors around the world guarantee continuing relationships with customers and lasting success as a company.

**Additional information**

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

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

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

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

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

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