



## CodeMeter as Token

### Mobile Private Keys and Certificates: Safely Stored for Digital Authentication

CodeMeter® from WIBU-SYSTEMS is well known for protecting software application, digital content, and providing effective license management options. Now this award winning technology will provide data protection and data security for digital communication by using the different CodeMeter hardware form factors as authentication tokens. CodeMeter tokens can be used to safely store private keys and digital certificates.

For Windows, Mac, or Linux applications supporting Microsoft's CSP or the platform independent PKCS#11 authentication standard, a wide range of authentication options become available when CodeMeter is used in combination with CSSI, a popular middleware from charismathics, a well known and respected company in the security field.

With optional flash memory that allows for installation of mobile applications, the different CodeMeter form factors are unique as "all-in-one" devices: token, dongle, and memory device rolled into one.

#### Confidential, Authenticated, and Non-Revocable Communication

CodeMeter meets the security requirements for authentication solutions by using cryptographic asymmetric key pairs within cryptography. Each key pair consists of a private and a public key. The private key is known only to the user and is safely stored inside the CodeMeter token in an encrypted state.

#### PKI token applications:

- Encryption and secure signing of e-mail
- Encryption of data on remote access
- Access control (strong two-factor authentication)
- Certificate-based Windows login
- Web-based applications (Software as a Service, SaaS)
- Company-wide single-sign-on (Windows)
- Virtual private networks (VPN)

#### The All-In-One: Token, Dongle, and Memory Device

- Complete implementation of Microsoft CSP and PKCS#11
- Activation by PIN
- Storage of private keys (16 X.509 certificates applicable for several applications)
- Asymmetric encryption (RSA 1024)
- Creation of signatures
- Software protection for many operating systems (Windows, Windows Embedded, Windows CE, Mac OS X, Linux, Sun Solaris) and programming languages (.NET, Java)
- Many form factors: USB, PC-Card, ExpressCard, CF-Card, SD-Card, µSD-Card
- Optional flash memory

## CodeMeter as Token

### Asymmetric encryption

Confidentiality of the data communication is safeguarded since the data encrypted with the private key can only be decrypted with the matching public key, and vice versa. All encryption and decryption processes take place securely inside the CodeMeter token.

### Digital signatures

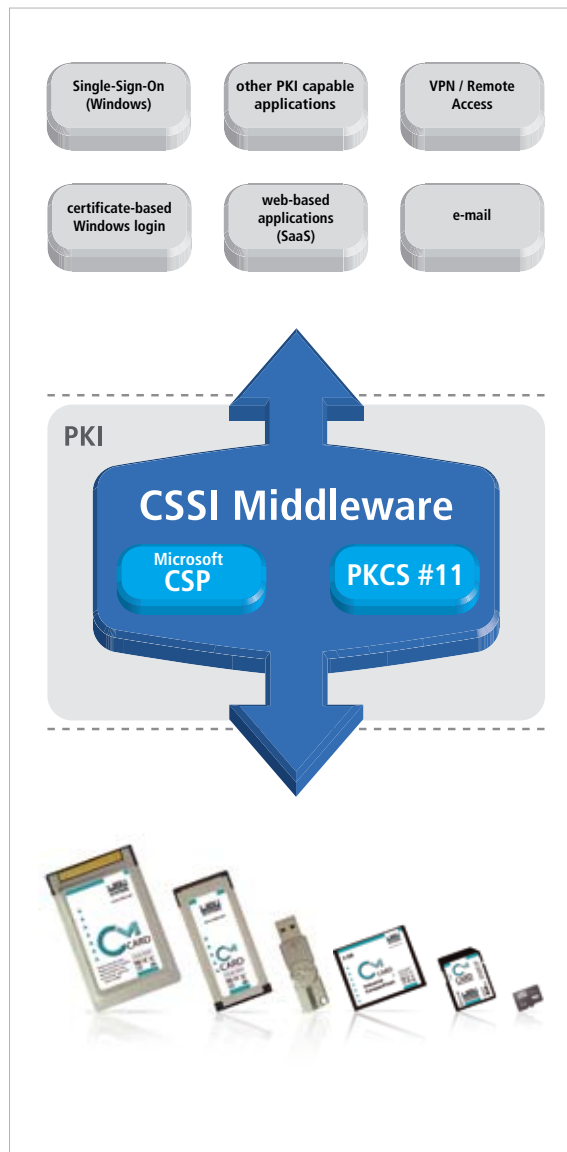
For verifying the sender and for providing for the non-repudiation of the data, CodeMeter uses "digital signatures". The signature represents an encrypted "finger print" (Hash value) of the data created with the private key inside the CodeMeter token. When verifying the signature within CSSI middleware, the public key is used to decrypt the encrypted finger print, and to compare it with the initial value.

### Digital certificates

In order to prevent the creation of digital signatures using false identities, a public key must be mapped to a unique and authenticated user. This authentication is accomplished by using "digital certificates" holding, among other things, the respective public keys, validity periods, and subject information. The certificates are issued by an certificate authority (CA) as part of a common public key infrastructure (PKI). Certificates serve as an "electronic ID", and are securely saved in X.509 format inside the CodeMeter token.

### CSSI middleware

CSSI, middle of the software producer charismathics, provides all services for access, identification, and authentication, and communicates function calls between the CodeMeter token and applications using the Windows proprietary CSP and the generic PKCS#11 interfaces. Using CSSI, the management of public keys together with other components can be organized within a common public key infrastructure (PKI).



**WIBU-SYSTEMS is**  
**DIN EN ISO 9001:2000**  
**certified and member**  
**of BITKOM e.V., VDMA**  
**PCMCIA, SD Card**  
**Association, USB**  
**Implementers Forum,**  
**SIIA and others, and**  
**Microsoft Gold Certified**  
**and Embedded Partner.**

When companies like SONY, Kodak, Motorola and Siemens think of software security and DRM (Digital Rights Management) for documents and media, they think of WIBU-SYSTEMS. These companies demand reliable and distinctive security solutions and recognize that a company, focused on DRM technologies since 1989, a company that consistently wins industry awards, and a company that is looking to the next threat instead of patching for the last one; is a company to do business with.

WIBU-SYSTEMS wants to provide "Perfection in Protection" for all our DRM products; elevate the level of customer service and increase the level of respect we show our own suppliers. And finally, help prepare the next generation of business leaders by investing in education and directly supporting youth activities.

Awards:



WIBU-SYSTEMS AG  
 Rueppurrer Strasse 52-54  
 D-76137 Karlsruhe  
 Phone: +49-721-93172-0  
 Fax: +49-721-93172-22  
 info@wibu.com | www.wibu.com

© 2009 WIBU, SmartShelter und CodeMeter are registered trademarks of WIBU-SYSTEMS AG. All other company names, labels or service names are trademarks or service names of the respective owners.

**WIBU**  
**SYSTEMS**

**MEDIA**  
**ACCESS**  
**PERFECTION IN SOFTWARE PROTECTION**  
**DOCUMENT**