



# Authentication in Electronic Business

## Methods of Authentication

From an historical viewpoint, the authentication of persons has always been implemented through the presentation of authentic documents. Documents, on the other hand, are verified by hand written signature or through special manufacturing methods utilizing stamps, watermarks or similar methods.

In the modern world, authentication is primarily implemented by means of knowledge. Such knowledge is often coupled with possession, for example with smart cards, WibuKey or CodeMeter.

For authentication using knowledge, there are now different manifestations. It can take the form of a question, i.e. a common secret which is equally and symmetrically available to both sides, the verifier (user B) and the verified party (presenter, user A). Or, in the asymmetric case, the verifier can authenticate the genuineness of the secret of the verified party by means of mathematical criteria.

Both in the symmetric and asymmetric case, there is the option of disclosing either the secret or only the knowledge in order to verify the secret.

Although many methods employed today require disclosure of the secret, from the standpoint of security, such processes are very dubious, since the entire secret can be read on the transmission channel and, in the asymmetric case as well (e.g. credit card), the verifier can present himself as the verified party at a later point in time.

Authors:  
Rüdiger Kügler  
Wolfgang Völker  
Dr. Peer Wichmann

## Principle of Authentication

Authentication represents one of the oldest problems in public life. Authentication can be categorized into three different aspects:

- validation of persons,
- validation of subjects, such as, e.g., commercial products or money, and
- validation of information or documents

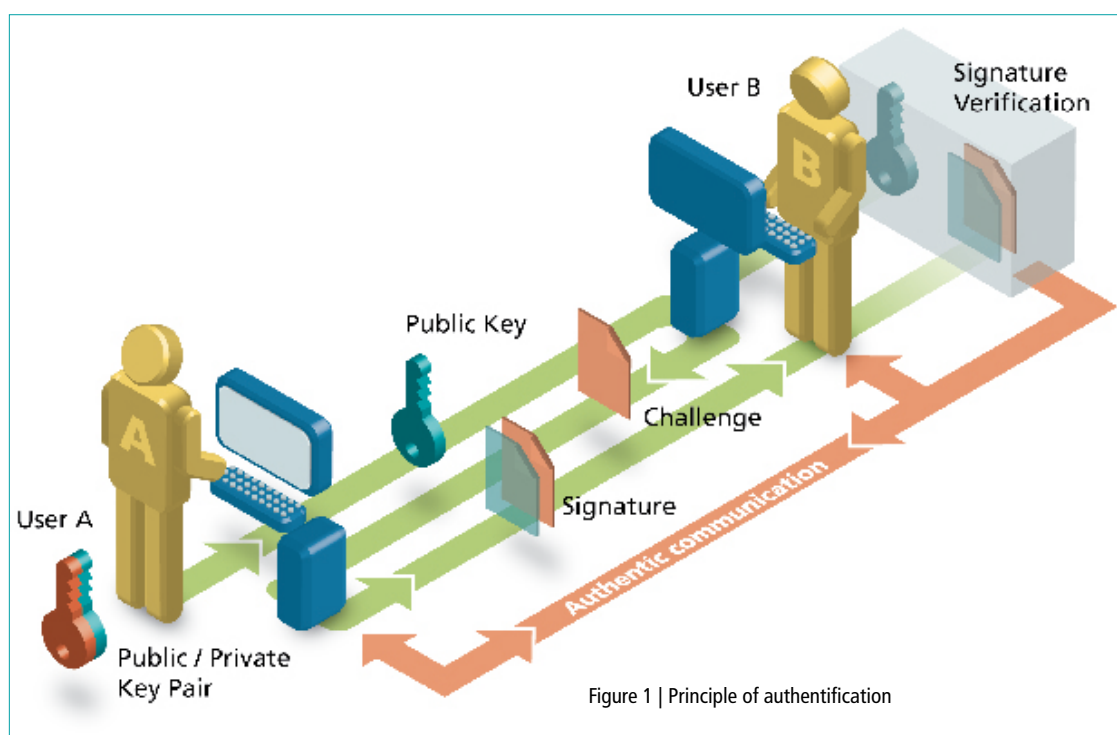


Figure 1 | Principle of authentication

Classically, authentication goes hand in hand with identification, since it is usually not meaningful to talk of verifying authenticity without having an identification.

In electronic business transactions, however, authenticity can also refer to a pseudonym. From the viewpoint of data protection, this is desirable for many reasons and in most cases, meets the requirements, since the pseudonym can be mapped as a real identity by means of a further process.

Authentication via electronic signature is practical and modern: a document is signed with an electronic signature.

The verifier confirms the genuineness of the presenter using the validity of the signature.

CodeMeter integrates several positive aspects of authentication:

- Security through the use of a standardized ECDSA signature.
- Secure storage of the cryptographic key in the CmStick.
- The user is not directly identifiable, since pseudonymity is achieved via the serial number of the CmStick. This is important for many modern day applications, since, e.g., authentication that is largely anonymous is also possible within the scope of age verification.
- Simply applied API.
- Authentication without a common secret and without disclosure of a secret.

The sequence of the authentication using a signature in the Cm Stick and the verification comprise the following individual steps:

1. Transmission of the public verification key to the verifier (one-time and not confidential)
2. Generation of an inquiry message (challenge) by the verifier and transmission to the presenter
3. Generation of the hash value and signature and transmission to the verifier
4. Verification of the signature

## CodeMeter Technology

### ■ Hardware

The core of CodeMeter is the CmStick, a USB hardware that allows the encryption and decryption of data. The required keys are generated in the CmStick and cannot be read out externally. In the CmStick, different keys for a wide variety of licenses can be stored in a tree network. The first level contains the Firm Item (FI). Every licensor has his own Firm Item. Only the licensor is able attach, modify or delete entries with his Firm Security Box (FSB) in his Firm Item.

The Product Items (PI) are found on the second level. Product Items identify a product and/or a license.

The Product Item Options are positioned below the Product Items. The license information, e.g. the pay-

per-use counter, is stored on this level.

The CmStick offers 128-bit AES (Advanced Encryption Standard) for symmetric encryption and 224-bit ECC (Elliptic Curve Cryptography) for asymmetric encryption.

It is protected against hardware-specific attacks, such as, e.g., readout with an electron microscope.

Over 1000 licenses from more than 100 different manufacturers can be stored on the CmStick. Accordingly, each individual license is provided with different options, such as, e.g., a limitation counter or expiry date.

### ■ Infrastructure

With the CmTalk infrastructure, CodeMeter enables the transmission of licenses to the user via the Internet to the CmStick.

For this purpose, the user goes into the online shop of the dealer (trader) and orders a license. The trader automatically transmits the inquiry to the software manufacturer (licensor).

In the next step, the user pays the paying agent (collector) for the license.

As soon as the collector has confirmed the payment, the license is generated by the software manufacturer (licensor) and transferred to the user.

In this case, all participants identify themselves through their own CmSticks. The licensor therefore has a Firm Security Box (FSB) in order to generate the licenses.

As shown in Figure 2, the flexibility of CodeMeter also offers the licensor the option of undertaking all three roles himself.



Figure 2 | CmTalk

## Asymmetric implementation with CodeMeter

### ■ Initial key exchange

For the signature, a Product Item is required in a CmStick. Using this Product Item and the secret data (private key) contained therein, an ECDSA signature is then calculated.

The public key matching this private key can be generated with this CmStick.

The public key of the presenter must now be sent once to the verifier. This can be done in two different ways:

- Programming the Product Item prior to the delivery and storing the public key in the database of the verifier.
- Programming the Product Item using CmTalk.

#### ■ Client side

On an authentication page, the authentication is performed via the CmStick using a Java-Applet or ActiveX-Control, depending on the computer platform and browser. In this case, the presenter prompts the verifier (server) for a challenge, which is signed by the presenter via the Product Item in the CmStick.

After successful authentication, the session on the server is identified as being verified and the client receives access to the protected side. The authentication process can be repeated again at any time, e.g. after a pre-determined period of time, upon request by the server.

The CodeMeter Runtime Kit must be installed on the client side.

#### ■ Server side

In addition to the existing session administration, the above-mentioned challenge must be generated and the signature produced by the presenter must also be verified on the server side.

Until verification of the signature, the challenge must be appropriately and securely stored by the server (session variable) or be provided with a cryptographic check criterion so that the authentication can be performed at a later point in time.

Upon receipt of the signature from the presenter, a check is executed on the server side to determine whether the challenge used and the signature are valid. To this end, the public key stored on the server is used to check the signature, which must match the serial number.

If the signature is valid (verified), the session is considered authentic. From here on, the previous session handling is used. A CmStick on the server is not required for verifying the signature. Here, the CodeMeter SDK only has to be installed on the server and the CmValidate Signature function called up.

The SDK is currently available for Windows, Macintosh and Linux. Other special platforms are available upon request.

#### ■ Examples

For asymmetric authentication with CodeMeter, sample implementations can be obtained for various technologies, such as, e.g., PHP or JSP with server components in Java or C. These can be requested from technical support at [support@wibu.de](mailto:support@wibu.de).

## Symmetrical implementation with CodeMeter

As an alternative to the implementation with asymmetric algorithms described above, authentication can also be carried out using with symmetric algorithms. The main difference is that both sides then possess the same secret. As a result, the symmetric variant does not fulfill the same high security requirements as the asymmetric variant.

The usual variant for symmetric authentication is verification using a password. However, the disadvantage of this is that during the authentication, the secret is made public within the scope of the transmission channel and can thus only be utilized to a limited extent for further authentication.

Significantly more appropriate is the utilization of a process which does not disclose the secret, but rather only unequivocally verifies its possession. The sequence is similar to the process flow described above. Unlike an electronic signature, however, symmetric encryption with AES is deployed here.

#### ■ Initial key exchange

The key required on both sides can be programmed either prior to delivery of the hardware to the customer or at a later point via CmTalk. The key can be stored as secret data in the Product Item and thus cannot be read out externally. The keys must be stored in a way that ensures confidentiality on the server side, to prevent compromising and thus eradicating the basis of the authentication.

#### ■ Client side

In the login HTML side a Java-Applet or ActiveX-Control is integrated as in the case of the asymmetric implementation (CmAuthMod). In this case, the CmAuthMod accepts the connection to the CmStick. The sequence is identical with the asymmetric protocol for the user.

#### ■ Server side

Here as well, the server side is identical with the asymmetric variant in regards to the sequence. However, the keys employed must be stored securely to ensure confidentiality. In the asymmetric case, only the keys must be authentic.

## Symmetrical implementation with WibuKey

In terms of the sequence and modules, implementation on the basis of WibuKey is basically identical to a symmetric CodeMeter implementation.

Some restrictions are imposed, however, since the cryptographic keys cannot be assigned here as freely as with CodeMeter. In this case, only the existence of individual code users can be verified.

A type of group authentication thus results, with which the affiliation to an authorized group is confirmed, but without verifying the individual user. The security level achieved through this mechanism not as high as compared to the symmetric CodeMeter variants.

## Security options

The CmStick possesses a password and the enabling function has three modes:

- Deactivated
- Activated until unplugged
- Fully activated

We recommend the setting „Activated until unplugged“, since only the password must be entered on the PC each time it is plugged in again. The signature cannot be generated without inputting the pertinent password. The secret data entries used for the encryption can be generated directly in the CmStick and never leave the CmStick.

If symmetric processes are deployed, AES is used for CodeMeter and Feal-32 for WibuKey. The utilization of CodeMeter offers the same options with respect to enabling as those provided with asymmetric protocols.

In the case of WibuKey, the authentication only refers to the possession of WibuKey. Additional knowledge within the scope of an enabling process is not possible.

From a security perspective, the advantages of asymmetric implementation with CodeMeter prevail.



**WIBU-SYSTEMS is  
DIN EN ISO 9001:2000  
certified and  
member of SIIA,  
BITKOM, PCMCIA,  
USB Implementers Forum,  
and others.**

**“To gain the confidence  
of our customers each  
day anew!”**

WIBU-SYSTEMS was founded in 1989 by Oliver Winzenried and Marcellus Buchheit. The company's focus is Digital Rights Management, as well as protection of software, documents, access and media. The philosophy of WIBU-SYSTEMS is an essential part of the daily work at the headquarters in Karlsruhe, Germany, as well as in the WIBU-SYSTEMS offices in Seattle, USA, and in Shanghai, China.

WIBU-SYSTEMS continuously expands its portfolio with important security solutions. CodeMeter is a revolutionary and patented Digital Rights Management solution to protect software and digital contents for many products of many vendors with one system in a very secure way - with advantages for both the vendor and the user. The WibuKey software protection system is definitely established in the international market and has been there for many years. In addition to the protection of software, WibuKey offers options for e.g. license management, modular software management and Electronic Software Distribution (ESD) to a very high level of security.

## Advantages

Authentication with hardware mechanisms such as CodeMeter or WibuKey yields the advantage of being enhanced with a further component. Conventional authentication via knowledge (password) is supplemented with authentication by means of possession. The two methods can both be combined to increase security.

Furthermore, with CodeMeter, the enabling allows a closer interconnection between the two variants. CodeMeter in conjunction with asymmetric authentication proves itself to be an ideal solution here:

- No secret keys with the verifier
- Higher performance, since hardware is not required on the server
- Signatures can also be used for other purposes, e.g. for transactions
- Simple implementation on various platforms on the server
- Simple integration on the client side as Applet or ActiveX
- Highest level of security
- Secure storage of the private key in the CmStick
- Optimal pseudonymization, e.g. for age verification

Additional products are SmartShelter for the protection of HTML and PDF documents and audio/video media data and the access control system SecuriKey. WIBU-SYSTEMS is supported by qualified partners worldwide.

In the SIIA Codie Awards competition, WIBU-SYSTEMS has been elected with CodeMeter as two finalists in the category Best Digital Rights Management Solution: Software and Best Security Software. The CmStick has been awarded the iF Product Design Award and has been nominated for the Designpreis der Bundesrepublik Deutschland 2006.



DESIGNPREIS  
2006  
NOMINEE

**WIBU  
SYSTEMS**

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