CryptWatch

CryptWatch provides highly secure mobile processing of sensitive data outside secure environments through a set of pre-defined requirements and for multiple usage scenarios.

All known attack patterns, such as USB Dumper on insecure computers of third parties, are prevented by a high-security hardware device. This results in greater advantages both the enterprise and the mobile environments can enjoy. Global players benefit from this solution, just like public clients, SMEs and private users. The management functions allow to elevate the added values and the cost optimization asset in all areas.

CryptWatch consists of an encapsulated piece of hardware in the form factor of a smart card-based CodeMeter USB stick, called CmStick, that features the following specifications:

1 Proprietary protection technology and self-defending crypto-infrastructure

- Memory drive
- Implementation of the encryption algorithms directly in the hardware

2 Integrity protected application memory

3 Cryptographically protected data storage, which ensures the following:

- Data can only be read with the keys and the encryption algorithms from point 1
- Data can only be decrypted with the applications in the application memory from point 2. The decryption takes place in the hardware.

Three usage scenarios under the radar for CmStick hardware unit with in-built automatic encryption technology:

Mobility

The stick contains integrity protection applications that come from the „Secure Application Store", all key algorithms and data are split in three different hardware areas.

- No unauthorized access through the host system possible from outside
- Decryption exclusively through the secure application PDWatch available from the Secure Application Store
- Operation independently of itWatch Enterprise Security Suite and with no installation required on any platform – but integrated with many enterprise environments for greater value
- Encryption application against tampering attempts
- Protection against unauthorized data disclosure, as the encryption occurs in the encrypted CmStick alone
- Encryption and Decryption exclusively on the hardware device CmStick
- No installation required

CryptWatch

Enterprise

The use is bound to the CmStick personalized for the user and the data can be decrypted only on this stick after successful authentication of the user with his/her CmStick; this means that the transfer of data is tied to the specific hardware.

Strong Two- and More-Factor Authentication

The principle *I know* and *I have* is translated into practice in several ways

- Knowledge:
  - Standard login at the workplace
  - Optional PIN / password for memory drive
  - Top security
- Possession:
  - Customized CmStick with CryptWatch memory drive

As a prerequisite, it-WESS should be installed.

PKI, additional server or hardware are not necessary.

Customized memory drive CmStick for maximum security upon transferring data inside and outside companies

Encryption is performed inside the hardware. The company should select between:

- Keys for disclosure to third parties
- and Company Keys, which ensure that the information remains in a predefined infrastructure (no theft, no data loss)

Company Key encryption is bound to the CmStick AND to the existing itWESS installation.

Encryption in the cloud regardless of the workplace (home workstations, partner communication, ...)

itWatch GmbH

Aschauer Str. 30 ✦ 81549 Munich
Tel: +49 (0)89 / 620 30 100
Fax: +49 (0)89 / 620 30 10 69
www.itWatch.de ✦ info@itWatch.de