Security

Digital electronic signatures and encryption of files can be used to increase security in the area of data drives.

To be able to use these, a digital user certificate is required. During the creation process, a digital key pair is generated which is confirmed by a certification authority. This key pair consists of 2 parts, the private and the public key:

- Private key: This is password protected and always remains in the possession of the user.
- Public key: This is required by the communication partner and must be made known to him in some way.

Sign

Principle: You sign your files with the help of your private key. The communication partner can then use your public key to check whether / that the files are unchanged.

Encrypt

Principle: You encrypt your files with the help of the communication partner's public key. The communication partner can then decrypt the files with the help of his private key. You must therefore first have the communication partner's public key for encryption.

Prerequisites

A basic prerequisite for use is the correct integration of the certification authorities in your operating system and a valid digital user certificate. Then configure the appropriate application software:

Seiten in diesem Namensraum:

C

- Cleopatra