

Method for generating an identifier

Abstract

The invention relates to a method for generating an identifier for identifying a pair, wherein the pair comprises a cryptographic device (100) and a computer system (1, 2,...,i,...I), wherein the cryptographic device has a first secret key (102), wherein a second secret key (118.i) is associated with the computer system, wherein a blocking system (120) for accessing the second secret key of the computer system is provided, wherein the blocking system has a third secret key (126), and wherein the following steps are carried out for generating the identifier:

- Generating a second public key (116.i) from the second secret key and a third public key (128) associated with the third secret key by means of the blocking system,
- Transmitting the second public key (116.i) to the computer system (i), and
- Generating the identifier from the first secret key and the second public key, using the cryptographic device.

(Figure 1)