

being unique to the customer loyalty card-eBay combination. The eBay provider then has an identifier for the customer loyalty card-eBay pair without the need for further information from the customer loyalty card.

The same applies for Amazon, wherein the identifier computed for the customer loyalty card-Amazon pair is different from the identifier for the customer loyalty card-eBay pair. This prevents different providers, for example eBay and Amazon, from combining their data records regarding customer behavior, since they are not able to determine from the identifiers whether they are communicating with the same or different persons.

In one aspect, there is provided a method for blocking a cryptographic device, wherein an identifier corresponding to an embodiment of the invention is associated with the pair comprising the cryptographic device and a computer system, by means of which the pair is identifiable, having the following steps: Computation of the identifier by the blocking system, based on a first public key, the second secret key, and the third secret key, wherein the first public key is included in the first secret key of the cryptographic device, and together with same forms an asymmetrical cryptographic key pair, transmission of the identifier to the computer system, and storage of the identifier in a blocking list of the computer system.

Herein disclosed is~~In another aspect, the invention relates to a method for blocking a~~ cryptographic device, wherein an identifier corresponding to a method according to one of the preceding claims is associated with the pair comprising the cryptographic device and a computer system, by means of which the pair is identifiable, having the following steps: Computation of the identifier by the blocking device, based on the first public key, the second secret key, and the third secret key, transmission of the identifier to the computer system, and storage of the identifier in a blocking list of the computer system.

In another aspect, there is provided a computer program product, in particular a digital storage medium, having executable instructions for carrying out a method according to an embodiment of the invention.

Also disclosed is~~In another aspect, the invention relates to~~ a computer program product for executing an embodiment of a method according to the invention for generating an identifier, and/or an embodiment of a method according to the invention for blocking a cryptographic device.

In one aspect, there is provided a blocking system for blocking the use of a cryptographic device with regard to a set of computer systems, wherein the cryptographic device has a first secret key, wherein one blocking list and one second secret key are associated with each of the computer systems, having: means for generating a second public key for each of the second secret keys from the second secret key in question and a third public key, wherein the third public key is included in a third secret key to which the blocking system has access, wherein an identifier is determinable by each of the second public keys and the first secret key of the cryptographic device, and identifies the pair comprising the cryptographic device and the computer system which is associated with the second public key in question, means for receiving a blocking command, means for generating the identifier for each of the pairs from the first public key of the cryptographic device, the second secret keys, and the third secret key, wherein the first public key is included in the first secret key of the cryptographic device, and together with same forms an asymmetrical cryptographic key, and means for transmitting the identifiers to the computer systems in question for storage in the respective blocking lists thereof.

Herein disclosed is~~In another aspect, the invention relates to~~ a blocking system for blocking the use of a cryptographic device with regard to a set of computer systems, wherein the cryptographic device has a first secret key, wherein one second secret key is associated with each of the computer systems, having: means for generating a second public key for each of the second secret keys from the second secret key in question and a third public key, wherein the third public key is included in a third secret key to

Claims

1. Method for generating an identifier for identifying a pair, wherein the pair comprises a cryptographic device ~~(100)~~ and a computer system ~~(1, 2, ..., i, ...l)~~, 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.
2. Method according to Claim 1, wherein the identifier is transmitted from the cryptographic device to the computer system.
3. Method according to Claim 1 or 2, wherein the blocking system has first subsystems ~~(134)~~ and second subsystems ~~(136)~~, wherein only the first subsystem has access to the third secret key, and only the second subsystem has access to the second secret key, wherein the second subsystem is provided for generating the second public key from the second secret key and the third public key.
4. Method according to Claim 3, wherein the computer system is included in a set of

computer systems, and wherein the blocking system has a plurality of the second subsystems ~~(136.j)~~, wherein a subset of the computer systems is associated with each of the second subsystems, wherein one second secret key is associated with each of the computer systems, wherein each of the second subsystems is able to access the second secret keys which are associated with the subset of the computer systems of this second subsystem, wherein, for each pair which may be formed from the cryptographic device and one of the computer systems, an identifier is defined by the first secret key and the second public key of the computer system in question.

5. Method according to one of the preceding claims, wherein the first and second subsystems of the blocking system are linked to one another via a public network ~~(144)~~.
6. Method for blocking a cryptographic device, wherein an identifier corresponding to a method according to one of the preceding claims is associated with the pair comprising the cryptographic device and a computer system ~~(i)~~, by means of which the pair is identifiable, having the following steps:
 - Computation of the identifier by the blocking system ~~(120)~~, based on a first public key, the second secret key, and the third secret key, wherein the first public key is included in the first secret key of the cryptographic device, and together with same forms an asymmetrical cryptographic key pair,
 - Transmission of the identifier to the computer system, and
 - Storage of the identifier in a blocking list ~~(138.i)~~ of the computer system.
7. Method according to Claim 6, wherein for computing the identifier by the first

subsystem, a fourth public key is generated from the third secret key and the first public key, and the fourth public key is transmitted from the first subsystem to the second subsystem which is associated with the computer system in question, so that the second subsystem generates the identifier from the fourth public key and the second secret key which is associated with the computer system in question.

8. Method according to Claim 7, wherein as the result of a blocking command, the first subsystem generates the fourth public key and then transmits the fourth public key to all of the second subsystems, wherein the second subsystems then determine the identifier for each possible pair and transmit same to the computer systems, so that in each of the computer systems the identifier which identifies the pair containing the computer system in question and the cryptographic device is stored in the respective blocking list.
9. Method according to one of the preceding claims, wherein the cryptographic device is a value document or security document, in particular a chip card.
10. Computer program product, in particular a digital storage medium, having executable instructions for carrying out a method according to one of the preceding claims.
11. Blocking system for blocking the use of a cryptographic device ~~(100)~~ with regard to a set of computer systems ~~(1, 2, ..., i, ..., I)~~, wherein the cryptographic device has a first secret key ~~(102)~~, wherein one blocking list and one second secret key ~~(118.i)~~ are associated with each of the computer systems, having:
 - means ~~(130, 132)~~ for generating a second public key ~~(116.i)~~ for each of the second secret keys from the second secret key in question and a third public key ~~(128)~~, wherein the third public key is included in a third secret

key-(126) to which the blocking system has access, wherein an identifier is determinable by each of the second public keys and the first secret key of the cryptographic device, and identifies the pair comprising the cryptographic device and the computer system which is associated with the second public key in question,

- means-(130, 132) for receiving a blocking command,
- means-(130, 132) for generating the identifier for each of the pairs from the first public key of the cryptographic device, the second secret keys, and the third secret key, wherein the first public key is included in the first secret key of the cryptographic device, and together with same forms an asymmetrical cryptographic key, and
- means-(130, 132) for transmitting the identifiers to the computer systems in question for storage in the respective blocking lists-(138-i) thereof.

12. Blocking system according to Claim 11, wherein the blocking system has first subsystems-(134) and second subsystems-(136), wherein only the first subsystem has access to the third secret key, and only the second subsystem has access to the second secret key, wherein the second subsystem is provided for generating the second public key from the second secret key and the third public key.

13. Blocking system according to Claim 12, wherein the first subsystem contains the means-(130', 132') for receiving the blocking command, wherein the blocking command contains identification data for identifying the cryptographic device, and wherein the first subsystem is designed to access a database-(106) with the aid of the identification data in order to read the first public key of the identifier

from the database.

14. Computer system having

- means ~~(122.i, 124.i)~~ for receiving a second public key ~~(116.i)~~ from a blocking system ~~(120)~~ according to one of Claims 11 through 13,
- means ~~(122.i, 124.i)~~ for transmitting the second public key to a user computer system ~~(112)~~ which is linkable to the cryptographic device ~~(100)~~,
- means ~~(122.i, 124.i)~~ for receiving the identifier for the pair formed from the cryptographic device and the computer system, and
- means ~~(122.i, 124.i)~~ for comparing the identifier to a blocking list ~~(138.i)~~, wherein identifiers received from the blocking system as the result of the blocking command are stored in the blocking list.