Claims

1. A self-authentication device ~~(14)~~ for the user or owner of an electronic security device ~~(12)~~, wherein the self-authentication device ~~(14)~~ is separate from the security device ~~(12)~~ and is configured for connecting to a computing device ~~(300, 400, 500, 600)~~ via a first communication link for self-authentication processing, and wherein the self-authentication device ~~(14)~~ is configured for enabling resetting a user password stored in the security device ~~(12)~~ upon successful self-authentication without requiring user-input of an authorization password.

2. The self-authentication device ~~(14)~~ as claimed in claim 1, wherein the self-authentication processing comprises matching a first key and/or a first unique identifier stored in the self-authentication device ~~(14)~~ with a second key and/or a second unique identifier stored in the security device ~~(12)~~.

3. The self-authentication device ~~(14)~~ as claimed in any one of claims 1 to 2, wherein the self-authentication device ~~(14)~~ is configured for generating a third key and/or a third unique identifier for configuring another security device ~~(15)~~ as associated with the self-authentication device ~~(14)~~.

4. The self-authentication device ~~(14)~~ as claimed in any one of claims 1 to 3, wherein the self-authentication device ~~(14)~~ is further configured for connecting to a host computer ~~(300, 400, 500, 600)~~ via a second communication link, for reading data stored for example in a virtual secured disk on the host computer ~~(300, 400, 500, 600)~~.

5. The self-authentication device ~~(14)~~ as claimed in claim 4, wherein the self-authentication device ~~(14)~~ is further configured for connecting to the host computer ~~(300, 400, 500, 600)~~ via the second communication link, for reading data stored for example in the virtual secured disk on the host computer ~~(300, 400, 500, 600)~~ without requiring a password.

6. The self-authentication device ~~(14)~~ as claimed in any one of claims 1 to 5 wherein the self-authentication device ~~(14)~~ is configured for decrypting data stored for example in a virtual secured disk on a host computer ~~(300, 400, 500, 600)~~, generating a fourth key, and encrypting the data using the fourth key.

7. The self-authentication device ~~(14)~~ as claimed in any one of claims 1 to 6, wherein the security device ~~(12)~~ is a data encryption token.

8. A self-authentication method for the user or owner of an electronic security device ~~(12)~~, the method comprising connecting an self-authentication device ~~(14)~~ separate from the security device ~~(12)~~ to a computing device ~~(300, 400, 500, 600)~~ via a first communication link for self-authentication processing, and resetting a user password stored in the security device ~~(12)~~ upon successful authentication of the association between the self-authentication device ~~(14)~~ and the security device ~~(12)~~ without requiring user-input of an authorization password.

9. The method as claimed in claim 8, wherein the self-authentication processing comprises authenticating an association between the security device ~~(12)~~ and the self-authentication device ~~(14)~~.

10. The method as claimed in claim 9, wherein the self-authentication processing comprises matching a first key and/or a first unique identifier stored in the self-authentication device ~~(14)~~ with a second key and/or a second unique identifier stored in the security device ~~(12)~~.

11. The method as claimed in any one of claims 8 to 10, wherein the self-authentication processing comprises obtaining a third key and/or a third unique identifier from the self-authentication device ~~(14)~~ for configuring an un-associated security device ~~(15)~~ as associated with the self-authentication device ~~(14)~~.

12. The method as claimed in any one of claims 8 to 11, further comprising connecting the self-authentication device ~~(14)~~ to a host computer ~~(300, 400, 500, 600)~~ via a third communication link for reading data stored for example in a virtual secured disk on the host computer ~~(300, 400, 500, 600)~~.

13. The method as claimed in claim 12, wherein the reading of the data stored for example in the virtual secured disk on the host computer ~~(300, 400, 500, 600)~~ is without requiring a password.

14. The method as claimed in any one of claims 8 to 13, further comprising:

decrypting data stored for example in a virtual secured disk of a host computer ~~(300, 400, 500, 600)~~;

encrypting the decrypted data using a new key; and

storing the new key in the security device ~~(12)~~ and a matching authentication key in the self-authentication device ~~(14)~~.

15. The method as claimed in any one of claims 8 to 14, wherein the security device ~~(12)~~ is a data encryption token.

Claims

1. A self-authentication device for the user or owner of an electronic security device, wherein the self-authentication device is separate from the security device and is configured for connecting to a computing device via a first communication link for self-authentication processing, and wherein the self-authentication device is configured for enabling resetting a user password stored in the security device upon successful self-authentication without requiring user-input of an authorization password.

2. The self-authentication device as claimed in claim 1, wherein the self-authentication processing comprises matching a first key and/or a first unique identifier stored in the self-authentication device with a second key and/or a second unique identifier stored in the security device.

3. The self-authentication device as claimed in any one of claims 1 to 2, wherein the self-authentication device is configured for generating a third key and/or a third unique identifier for configuring another security device as associated with the self-authentication device.

4. The self-authentication device as claimed in any one of claims 1 to 3, wherein the self-authentication device is further configured for connecting to a host computer via a second communication link, for reading data stored for example in a virtual secured disk on the host computer.

5. The self-authentication device as claimed in claim 4, wherein the self-authentication device is further configured for connecting to the host computer via the second communication link, for reading data stored for example in the virtual secured disk on the host computer without requiring a password.

6. The self-authentication device as claimed in any one of claims 1 to 5 wherein the self-authentication device is configured for decrypting data stored for example in a virtual secured disk on a host computer, generating a fourth key, and encrypting the data using the fourth key.

7. The self-authentication device as claimed in any one of claims 1 to 6, wherein the security device is a data encryption token.

8. A self-authentication method for the user or owner of an electronic security device, the method comprising connecting an self-authentication device separate from the security device to a computing device via a first communication link for self-authentication processing, and resetting a user password stored in the security device upon successful authentication of the association between the self-authentication device and the security device without requiring user-input of an authorization password.

9. The method as claimed in claim 8, wherein the self-authentication processing comprises authenticating an association between the security device and the self-authentication device.

10. The method as claimed in claim 9, wherein the self-authentication processing comprises matching a first key and/or a first unique identifier stored in the self-authentication device with a second key and/or a second unique identifier stored in the security device.

11. The method as claimed in any one of claims 8 to 10, wherein the self-authentication processing comprises obtaining a third key and/or a third unique identifier from the self-authentication device for configuring an un-associated security device as associated with the self-authentication device.

12. The method as claimed in any one of claims 8 to 11, further comprising connecting the self-authentication device to a host computer via a third communication link for reading data stored for example in a virtual secured disk on the host computer.

13. The method as claimed in claim 12, wherein the reading of the data stored for example in the virtual secured disk on the host computer is without requiring a password.

14. The method as claimed in any one of claims 8 to 13, further comprising:

decrypting data stored for example in a virtual secured disk of a host computer;

encrypting the decrypted data using a new key; and

storing the new key in the security device and a matching authentication key in the self-authentication device.

15. The method as claimed in any one of claims 8 to 14, wherein the security device is a data encryption token.