

CLAIMS

1. A decryption system for decrypting user information encrypted on a storage device associated with a user identity document, the system comprising:

means for reading user identity document data from a token;

5 key construction means for constructing a key for decrypting the user information stored on the storage device based on the user identity document data read from the token.

2. A decryption system according to claim 1 wherein the key construction means
10 derives the key based on one or more of a user identity document number, an expiry date of the user identity document and preferably a user's date of birth.

3. A decryption system according to any preceding claim wherein the token is a
15 boarding pass and the like, and preferably wherein the user identity document data is encoded in a machine readable form.

4. A decryption system according to any preceding claim further comprising means for
collecting user identity document data from the or a user and to construct the or a token
20 comprising the user identity document data.

5. A decryption system according to any preceding claim wherein the or a user enters
the user identity document data prior to the reading means reading the data encoded on
the token.

6. A decryption system according to any preceding claim in which the reading means
25 is configured to read the user information stored on the storage device.

7. A decryption system according to any preceding claim in which the token further
comprises user identification information and in particular in which the reading means is
30 further configured to read the user identification information from the token.

8. A decryption system according to any preceding claim further comprising
comparison means for comparing the user identification information read from the token
and the user information decrypted from the storage device associated with the user
35 identity document or for comparing the user identity document data read from the token

and the user information decrypted from the storage device associated with the user identity document.

9. A decryption system according to any preceding claim further comprising
5 comparison means for comparing the user identification information read from the token and the user information decrypted from the storage device associated with the user identity document and further comprising authentication means for authenticating the user depending upon the result of the comparison.

10. A decryption system according to any preceding claim further comprising a mobile
10 device associated with a user for storing the token.

11. A decryption system according to any preceding claim in which the token is a
boarding pass having the user identity document data encoded in a specific region of the
15 boarding pass.

12. A decryption system according to any preceding claim further comprising a mobile
device associated with a user for storing the token, wherein the mobile device comprises a
near field communication, NFC, chip communicatively coupled with the mobile device for
20 transmitting the token to the reading means such as an airport check-in security desk.

13. A decryption system according to any preceding claim in which the key construction
means is configured to construct the key in response to the reading means reading the
user identity document data encoded in machine readable form on or within the token.
25

14. A decryption system according to any preceding claim in which the identity
document reading means is primed to decrypt the user identification information encrypted
on or within the storage device in response to reading the user identity document data from
the token.
30

15. A decryption system according to any preceding claim in which the reading means
is a wireless reading means preferably comprising a near field communication, NFC,
reading means configured to communicate with a mobile device for storing the token
storage device and further preferably comprising a radio frequency identification, RFID,
35 reading means configured to communicate with the storage device.

16. A decryption system according to any one of claims 1 to 15 in which the reading means is configured to read the user identity document data from a predetermined region of the token.

5

17. A decryption system according to any one of claims 1 to 16 wherein the reading means is a portable reader or scanner such as a mobile telephone.

10

18. A decryption system according to any one of claims 1 to 17 in which the user identity document is a passport and preferably in which the user identity document or passport is pre-stored on a mobile communication device, preferably in a secured manner.

15

19. The decryption system according to any preceding claim further comprising means for reading a user identity document biometric facial image, from the storage device, using the user identity document data read from the token.

20

20. The decryption system according to any preceding claim further comprising means for capturing an image of the user with a camera and preferably comprising comparison means for comparing the captured image with the passport biometric facial image read from the user identity document.

25

21. A decryption method, preferably for execution by a processor, for decrypting user information encrypted on a storage device associated with a user identity document, the method comprising:

reading user identity document data from a token;
constructing a key for decrypting the user information stored on the storage device based on the user identity document data read from the token.

30

22. A decryption method according to claim 21 wherein the key construction means derives the key based on one or more of a user identity document number, an expiry date of the user identity document and preferably a user's date of birth.

35

23. A decryption method according to any one of claims 21 or 22 wherein the token is a boarding pass and the like, and preferably wherein the user identity document data is encoded in a machine readable form.

24. A decryption method according to claim 21 further comprising collecting user identity document data from the or a user and constructing the or a token comprising the user identity document data.

5 25. A decryption method according to claim 21 wherein the or a user enters the user identity document data prior to the reading means reading the data encoded on the token.

26. A decryption method according to claim 21 in which the reading means is configured to read the user information stored on the storage device.

10

27. A decryption method according to any preceding claim in which the token further comprises user identification information and in particular in which the reading means is further configured to read the user identification information from the token.

15 28. A decryption method according to claim 21 further comprising comparing the user identification information read from the token and the user information decrypted from the storage device associated with the user identity document or comparing the user identity document data read from the token and the user information decrypted from the storage device associated with the user identity document.

20

29. A decryption method according to claim 27 further comprising comparing the user identification information read from the token and the user information decrypted from the storage device associated with the user identity document and further comprising authenticating the user depending upon the result of the comparison.

25

30. A decryption method according to claim 21 further comprising a mobile device associated with a user for storing the token.

31. A decryption method according to claim 21 in which the token is a boarding pass
30 having the user identity document data encoded in a specific region of the boarding pass.

32. A decryption method according to claim 21 further comprising storing the token on a mobile device associated with a user, wherein the mobile device comprises a near field communication, NFC, chip communicatively coupled with the mobile device for transmitting
35 the token to the reading means such as an airport check-in security desk.

33. A decryption method according to claim 21 in which the key construction constructs the key in response to the reading means reading the user identity document data encoded in machine readable form on or within the token.

5 34. A decryption method according to claim 21 in which the identity document reading means is primed to decrypt the user identification information encrypted on or within the storage device in response to reading the user identity document data from the token.

10 35. A decryption method according to claim 21 in which the reading means is a wireless reading means preferably comprising a near field communication, NFC, reading means configured to communicate with a mobile device for storing the token storage device and further preferably comprising a radio frequency identification, RFID, reading means configured to communicate with the storage device.

15 36. A decryption method according to any one of claims 21 to 35 in which the reading means is configured to read the user identity document data from a predetermined region of the token.

20 37. A decryption method according to any one of claims 21 to 36 wherein the reading means is a portable reader or scanner such as a mobile telephone.

25 38. A decryption method according to any one of claims 21 to 37 in which the user identity document is a passport and preferably in which the user identity document or passport is pre-stored on a mobile communication device, preferably in a secured manner.

39. The decryption method according to claim 21 further comprising means for reading a user identity document biometric facial image using the user identity document data read from the token.

30 40. The decryption method according to claim 21 further comprising capturing an image of the user with a camera and preferably the step of comparing the captured image with the passport biometric facial image read from the user identity document.

35 41. A token generating system for generating a boarding pass and the like comprising:
a server configured to collect user identity document data from a user and to construct a token such as a boarding pass including the user identity document data

encoded in a machine readable form wherein the server is configured to generate the token having the data encoded on or within a predetermined region and the data preferably comprises a user identity document number and an expiry date of the user identity document and preferably the user's date of birth.

5

42. A boarding pass for use with the decryption system of any preceding claim the pass comprising:

user identity document data associated with a user identity document, the data encoded in a machine readable form wherein the data is encoded on or within a

10

predetermined region of the token and the data preferably comprises a user identity document number and an expiry date of the user identity document and preferably the user's date of birth.

CLAIMS

1. A decryption system for decrypting user information encrypted on a storage device associated with an identity document of a user, the system comprising:

a server configured to collect user identity document data from the user and to construct a token comprising the user identity document data, wherein the server is further configured to send the token to a mobile device associated with the user for storing the token at the mobile device and wherein the mobile device is physically separate from said storage device;

a key construction unit communicatively coupled to a machine reader configured to read the data from the token by radio frequency identification communication with the mobile device,

wherein the token further comprises user identification information and in particular in which the reader is further configured to read the user identification information from the token and wherein the key construction unit uses the user identity document data read from the token, stored on the mobile device, to construct a key for decrypting the user information stored on said storage device;

a comparator for comparing the user identification information read from the token stored on the mobile device and the user information decrypted from said storage device associated with the user identity document; and

authentication means for authenticating the user depending upon the result of the comparison.

2. A decryption system according to claim 1 wherein the key construction unit derives the key based on one or more of a user identity document number, an expiry date of the user identity document and a user's date of birth.

3. A decryption system according to claim 1 wherein the user manually enters the user identity document data prior to the reader reading the data encoded on the token.

4. A decryption system according to claim 1 in which the reader is configured to read the user information stored on the storage device.

5. A decryption system according to claim 1 in which the token is a boarding pass having the user identity document data encoded in a specific region of the boarding pass.

6. A decryption system according to claim 1 further comprising a mobile device associated with a user for storing the token, wherein the mobile device comprises a near

field communication, NFC, chip communicatively coupled with the mobile device for transmitting the token to the reader.

7. A decryption system according to claim 1 in which the key construction unit is configured to construct the key in response to the reader reading the user identity document data encoded in machine readable form on or within the token.

8. A decryption system according to claim 1 in which the identity document reader is primed to decrypt the user identification information encrypted on or within the storage device in response to the reader reading the user identity document data from the token.

9. A boarding pass for use with the decryption system of claim 1, the pass comprising:
user identity document data associated with a user identity document and user identification information, the data encoded in a machine readable form wherein the data is encoded on or within a predetermined region of the token and the data comprises a user identity document number and an expiry date of the user identity document and the user's date of birth.

10. A decryption system according to claim 1 in which the reader is a wireless reading means.

11. A decryption system according to claim 10 in which the reader is a wireless reading means comprising a near field communication, NFC, reading means configured to communicate with a mobile device for storing the token storage device and further comprising a radio frequency identification, RFID, reading means configured to communicate with the storage device.

12. A token generating system for generating a boarding pass and comprising:
a server configured to collect user identity document data and user identification information from a user and to construct a boarding pass token including the user identity document data and user identification information encoded in a machine readable form wherein the server is configured to generate the token having the data encoded on or within a predetermined region and the data comprises a user identity document number and an expiry date of the user identity document and preferably the user's date of birth, wherein the system is further configured to send the token to a mobile device associated with a user for storing the token on the mobile device; and

wherein:

a storage device, separate from the mobile device, configured to store encrypted user information associated with the user identity document;

a key construction unit communicatively coupled to a machine reader configured to read data from the token stored on the mobile device associated with the user by radio frequency identification communication with the mobile device and wherein the key construction unit further uses the user identity document data read from the token to construct a key for decrypting the user information encrypted on said storage device;

a comparator for comparing the user identification information read from the token stored on the mobile device and the user information decrypted from said storage device associated with the user identity document; and

authentication means for authenticating the user depending upon the result of the comparison.

13. A decryption system for decrypting user information encrypted on a storage device associated with an identity document of a user, the system comprising:

a machine reader configured to read data from a token stored on a mobile device associated with the user by radio frequency identification communication with the mobile device, the token including user identity document data encoded in a machine readable form, and the reader configured to read the data encoded on the storage device, wherein the mobile device is physically separate from said storage device and wherein a server is first configured to collect the user identity document data and user identification information from the user and to construct the token comprising the user identity document data and subsequently send the token to the mobile device for storing the token on the mobile device;

a key construction unit configured to derive a key from the user identity document data encoded on or within the token, stored on the mobile device, which enables the reader to decrypt the user information stored on the storage device;

a comparator for comparing the data read from the token stored on the mobile device and the user information decrypted from said storage device associated with the user identity document; and

authentication means for authenticating the user depending upon the result of the comparison.

14. A decryption system according to claim 13 in which the reader is configured to read the user identity document data from a predetermined region of the token.

15. A decryption system for decrypting user information encrypted on a storage device associated with an identity document of a user, the system comprising:

a server configured to collect user identity document data and user identification information from the user and to construct a token comprising the user identity document data, wherein the server is further configured to send the token to a mobile device associated with the user for storing the token at the mobile device and wherein the mobile device is physically separate from said storage device;

a machine reader configured to read the data from the token by radio frequency identification communication with the mobile device, wherein the reader uses the user identity document data read from the token, stored on the mobile device, to decrypt the user information stored on said storage device;

a comparator for comparing the data read from the token stored on the mobile device and the user information decrypted from said storage device associated with the user identity document; and

authentication means for authenticating the user depending upon the result of the comparison.

16. A decryption system according to claim 15 wherein the reader is a portable reader or scanner or a mobile telephone.

17. A decryption system according to claim 15 in which the user identity document is a passport and in which the user identity document or passport is pre-stored on a mobile communication device, in a secured manner.

18. The decryption system according to claim 15 further comprising the step of reading a user identity document biometric facial image using the user identity document data.

19. The decryption system according to claim 15 further comprising the step of capturing an image of the user with a camera and preferably the step of comparing the captured image with the passport biometric facial image read from the user identity document.