

WE CLAIM:

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 any preceding claim 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 any preceding claim in which the reader is configured to read the user information stored on the storage device.
5. 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 boarding pass.
6. A decryption system according to any preceding claim 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 any preceding claim 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 any preceding claim 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 decryption system according to any preceding claim in which the reader is a wireless reading means.
10. A decryption system according to claim 9 wherein the wireless reading means comprises 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.
11. A decryption system according to any preceding claim in which the reader is configured to read the user identity document data from a predetermined region of the token.

12. A decryption system according preceding claim wherein the reader is a portable reader or scanner or a mobile telephone.

13. A decryption system according to any preceding claim 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.

14. 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.

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

16. A token generating system for generating a boarding pass comprising:

a server configured to collect user identity document data and user identification information from a user and to construct boarding pass a 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, an expiry date of the user identity document and 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.

17. 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 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.

Dated this 07th Day of November, 2014

Priyank Gupta
IN-PA-1454
Agent for the Applicant