AIRPORT SECURITY CHECK SYSTEM AND METHOD THEREFOR

FIELD OF THE INVENTION

This invention relates in general to a security system. More particularly, this invention relates to a security system for passengers who are required to have a passport, official travel document or other identity document certifying the passenger's identity in order to travel to their destination. More specifically, this invention relates to a security system for streamlining or expediting passenger processing through security at an airport as well as to a system for decrypting user information stored on a storage device.

BACKGROUND OF THE INVENTION

Many passports are now embedded with a radio frequency identification (RFID) chip which allows biometric and other data to be stored on the passport using the chip. Data may be wirelessly read from the chip using electromagnetic fields generated by a reader. The chip responds by transmitting data via an electromagnetic field coil associated with the chip.

Biometric passports are equipped with protection mechanisms to avoid and/or detect attacks. Biometric passports and chip characteristics are documented in the International Civil Aviation Civil Organization's (ICAO) Doc 9303. Most biometric passports at a minimum support Basic Access Control (BAC), which is mandatory in Europe. BAC protects the communication channel between the chip on or within the passport and the reader by encrypting transmitted information. Usually, data is stored on the passport in an encrypted or secured form which is accessible using a key. This prevents unauthorised users from skimming i.e. unauthorised reading of the data stored in the chip. Furthermore, an eavesdropper cannot eavesdrop information being transferred without knowing the correct key if the passport supports BAC.

Typically, at some point prior to a passenger's departure on a flight, a security check is performed to verify that a passenger's name on a boarding pass matches the name on their passport. The information stored on the chip, such as biometric information, may be used to authenticate the identity of a traveller. A boarding pass is usually a paper document with the passenger's name, flight details, gate and seat number printed on it. Usually, the security check is a visual check performed by a security officer who checks that the passenger name on the boarding pass matches the passenger name on the passenger's

passport. The security officer will usually check that the photograph shown on the passport is of the passenger using the passport. As this is a visual check, it is prone to human error.

In some cases, the security check will include reading the biometric data stored on the RFID chip embedded in the passport. However, as the data stored on the chip is encrypted, before data can be read from the passport, the reader needs to provide a key, which may be derived from a Machine Readable Zone (MRZ) located within the passport.

In order to read the data from the MRZ, the passport must be opened and placed on an optical reader, which performs Optical Character Recognition (OCR) on the MRZ. Optical Character Recognition is the mechanical or electronic translation of scanned images of printed text into machine-encoded text.

The reader then derives the key from the data read from the Machine Readable Zone data of the passport. A second RFID scan is then performed which uses the key derived from the OCR to retrieve the biometric data from the passport. This is a two-step process and is prone to error particularly during the OCR part. This is because the OCR part is sensitive to where the passport is placed on the scanner and also may also give an incorrect reading due to dirt on the scanner glass. If an error occurs during the OCR part, then the RFID scan will fail. To recover, the MRZ data has to be manually entered in order to read the biometric data. Because the interpretation of the MRZ is currently done using OCR, only accuracy rates of 80% to 90% can be achieved.

SUMMARY OF THE INVENTION

The invention is defined in the appended claims to which reference should now be made. Embodiments of the invention seek to address the above problems by providing an improved decryption system which eliminates the need for an OCR scan of the Machine Readable Zone. Thus, passport reading is more streamlined and will result in faster throughput of passengers through security. Embodiments of the invention may reduce the time to read a passport by approximately 4 seconds. Embodiments of the invention avoid the need to use optical character recognition software, which typically only has accuracy rates of 80% to 90% on the characters in the Machine Readable Zone. An inaccurate OCR of the MRZ will result in a failure in reading the biometrics from the passport. By having the passenger enter the APIS key data prior to or during check-in and making it available to be electronically read with the boarding pass information, the dependency on OCR is

removed. Embodiments of the invention are also less expensive to implement since according to embodiments of the invention, expensive dual OCR/RFID readers may be replaced with lower cost RFID readers.

BRIEF DESCRIPTION OF THE DRAWINGS

An embodiment of the invention will now be described, by way of example only, and with reference to the accompanying drawings, in which:

Figure 1 shows the front page of a passport including a Machine Readable Zone;

Figure 2 shows schematic diagram of the main functional components of an embodiment of the invention;

Figure 3a shows a passenger check-in screen;

Figure 3b shows a screen where the passenger enters supplementary passport details;

Figure 4 shows a screen of the data contained within the boarding pass after being read from the mobile communication device;

Figure 5 shows the identification data read from the mobile communication device;

Figure 6 is a schematic diagram showing a further embodiment which compares a biometric facial image read from a passport to an image of the passenger captured with a camera; and

Figure 7 shows the main steps performed by the embodiment of figure 6.

The following description is of a system for use in the aviation industry, but this is exemplary and other applications of the invention will also be discussed. For example, the security system may be used in any environment where security procedures require a user's identification document and a token for providing a service to the user to be authenticated as belonging to the user before a product or service is provided to the user. Thus, embodiments of the invention have particular application in the travel industry (for example rail, air, coach and the like), but also in the ticketing industry, such as ticketing for theatre, cinema, and the like.

Figure 1 of the accompanying drawings shows a data page of a passport which is divided into a number of zones. A Visual Inspection Zone, is located in the upper half of the page and contains data not specifically intended to be read by machine. A MRZ of the passport is located in the bottom half of the data page and contains data which is both human readable and machine readable.

The MRZ data may comprise: the document number, the date of expiry, and optionally, the date of birth of the user. Below is an example of the data contained in the MRZ of the passport, although some personal details have been blanked out with an X to protect the owner's identity:

```
P<IRLSMITH<<<<JOHN<<<<XXXX<<<<<<<<<<<<<<<<<<<
PC12345670IRL7903130M1711157<<<<<<<<<<<<<<<4
```

The data within the MRZ may be structured as 2 lines of alphanumeric characters. The data on each line may be separated by one or more filler characters which may be represented by <. Each line of data may be 44 characters in length.

Referring now to figure 2, this shows the main functional components of a system 201 embodying the invention. The components shown within the dashed line 203 of figure 2 may be located at an airport, although the server 205 does not necessarily need to be located at an airport. The system may comprise a remote check-in server 205 provided by an airline or third party. The remote check-in server 205 is configured to allow a passenger to check-in to a flight for which the passenger has purchased a ticket to travel.

Typically, the passenger remotely accesses the server 205 via a computer or a mobile communication device such as a portable laptop or mobile telephone. However, the user may perform check-in in person at the airport 203 using a check-in desk.

Regardless of how the user performs check-in, associated with each user is a token storage medium such as a portable or mobile device 207 which is capable of storing a boarding pass such as an electronic boarding pass or e-boarding pass. The boarding pass may be thought of as a token which is issued by a service provider to a user which allows the user receive the service in return for payment.

Usually, the server 205 is wirelessly coupled to the user's mobile device 207, for example, using a wireless communications network, but in principle, any communications means, such as a wired network may be used provided the e-boarding pass can be transferred to, and stored on the user's mobile device 207.

Usually, the mobile device 207 comprises a Near Field Communication (NFC) tag or chip communicatively couple to the mobile device. Typically, the NFC enabled integrated circuit

or chip is hard wired to the mobile device, but this is in fact optional. However, the mobile device comprises a communication means which allows data to be transferred from the mobile device 207 to a key construction unit 209. The mobile device 207 may be coupled to a wired communication means using for example a Universal Serial Bus (USB) port.

In the embodiment shown in figure 2, the key construction unit 209 and the security passport reader 211 are integrally provided on a single unit 212. However, the key construction unit 209 may be provided as a separate component to the security passport reader 211. In either case, the key construction unit 209 is communicatively coupled to a passport or identity card reader 211. The key construction unit 209 may be wirelessly coupled to the reader 211, for example by using WiFi or other wireless radio communication means or via a wired connection.

Operation of the security system 201 will now be described referring to figures 2 to 5 of the drawings. Figures 3a and 3b show the process of checking in a passenger and illustrate the typical details which may be collected from a passenger at check-in.

The passenger usually enters their name and optionally a mobile telephone number and email address. This data is usually referred to as Advanced Passenger Information System data (APIS). The passenger usually performs this step at a remote location from the airport 203.

In addition to the information described above which is entered during check-in or collected from the passenger profile at check-in, embodiments of the invention may prompt a user to enter additional passport details that are collected from the passenger. Figure 3b below illustrates the additional passport details or information that may be collected from a passenger at check-in.

The additional information entered at check-in may comprise one or more of the passport number, date of birth and date of expiry of their passport. The server then incorporates this information into a boarding pass or e-boarding pass, which is delivered to their mobile telephone using wired or wireless communication means known to the skilled person. Usually, the data is encoded as alphanumeric data, but other encoding schemes may be used.

The boarding pass may be represented as a 2D bar code or as an NFC boarding pass. The additional APIS data may be stored in a field for individual airline use which is then encoded as a 2D bar code or as NFC data.

The alphanumeric data in this field may have the following format:

A 9 character Alphanumeric Passport Number. If the passport number is less than 9 characters, then the remaining characters may be padded with the character "<", for example: "ABC123XY<".

A 6 character numeric date of birth in YYMMDD format, for example "720823".

A 6 character numeric date of expiry in YYDDMM format, for example, "210922".

The data is then rendered into a bar coded boarding pass. An NFC boarding pass may have the information in alphanumeric format.

The additional information may be Advanced Passenger Information System (APIS) data. This additional information may comprise one or more of passport or identity card number, date of birth and expiry date of the passport. When entering the information, the passenger may also be invited to tick a check box to indicate that the details entered correspond to those shown in the passport.

Once the passenger has entered these details, the server 205 transmits this information together with the boarding pass, to the mobile telephone or device 207 associated with the passenger. Usually, the additional information entered by the passenger is encoded onto a specific region of the boarding pass as text data or as barcode data or other data. Thus, security passport readers embodying the invention may be configured to read the additional information from the boarding pass by reading data from that specific region. Legacy passport readers, which are not configured to read data from this region of the boarding pass, ignore the additional data.

The mobile telephone or device 207 then stores the additional information and boarding pass as an NFC boarding pass. The boarding pass is stored in a memory such a flash memory or on an integrated circuit memory chip.

In one example, the boarding pass has additional user identity document data or information associated with it which provides further user identity document data or information in addition to the passenger name on the boarding pass.

When the passenger subsequently arrives at the airport, and when a security check is performed on the passenger, the NFC boarding pass together with this passport information is read from their mobile telephone or device 207. In order to read the NFC boarding pass from the mobile device, the passenger swipes their mobile device in close proximity to an NFC reader associated with the key construction unit 209. Usually, the NFC boarding pass is read from the mobile telephone or device 207 using the NFC chip which is communicatively coupled to the mobile telephone or device 207. Thus, the chip may also be communicatively coupled to the storage means associated with the mobile device. Other wired or wireless communication means may be used to transfer the NFC boarding pass from the mobile device 207 to the key construction unit, instead of using near field communications. Figure 4 of the drawings shows the contents of the boarding pass after being read from the mobile device. The picture shown in figure 4 may be displayed on a terminal associated with the reader 211. The data read from the device may comprise one or more of a passenger name, airline, flight number, departure date, departure city, arrival city, seat number, class, frequent flyer number, e-ticket number, boarding time, document number, date of birth, and date of expiry. Although in the picture shown in figure 4 all of this data is displayed, this is not essential and one or more of the data fields read from the mobile device may be displayed on the terminal. A security officer may then approve or deny the user's boarding pass by pressing the appropriate field on the terminal marked approve or deny.

The key construction unit 209 then extracts the additional data from the NFC boarding pass by reading the data contained within the specific region of the boarding pass. The data is data encoded on or within the boarding pass.

The key construction unit 209 then reconstructs the key using the additional data. The key construction unit 209 may construct the key using a key derivation mechanism which will be known to the skilled person. The key construction unit 209 then sends or passes the key to the passport security reader 211.

The passenger or security officer then subsequently scans or swipes the passport 213 in close proximity to the reader 211.Thus, the RFID chip or integrated circuit 214 embedded within the passport starts communicating with the reader. These initial communications between the reader and RFID chip may include an authentication step where the reader may be authenticated as being a genuine reader, rather than an unauthorised user

attempting to read or skim the data stored on the chip. The reader may authenticate itself using the key constructed by the key construction unit.

If the reader has been authenticated as being genuine, data requested by the reader may then be sent from the chip 214 to the reader 211. Usually, the data is sent to the reader in an encrypted form. This may prevent an eavesdropper intercepting data sent from the chip 214 to the reader 211.

The reader 211 then receives the encrypted data sent from the chip 214 and decrypts the data using the key constructed from the additional data. Other contactless integrated circuits 214 may also be embedded within the passport 213 or other official travel document without departing from the scope of the invention.

Usually, the passport is scanned immediately after the user has swiped their mobile device past the NFC reader associated with the key construction unit. Thus, the key construction unit 209 may only construct the key in response to receiving the additional data from the mobile device 207. In this way, when the security passport reader 211 receives a key from the key construction unit 209, the reader 211 is thus primed with a key which allows data to be decrypted on a subsequently scanned RFID chip 213 associated with the passport 213.The reader 211 may construct different keys for authentication and encryption or decryption.

The encrypted data stored on the RFID chip 211 may be biometric data such as iris recognition data, facial recognition data, and fingerprint recognition data, however in principle, any data may be stored on the chip or other wireless storage means or device associated with the passport. Thus, any data may be decrypted and read from the chip. However in a preferred embodiment, the reader 211 reads a user's surname and name from the chip.

The reader 211 may then compare the information read from the encrypted data on the RFID chip 214 with the data on the boarding pass. If the decrypted information read from the chip 214 matches corresponding information read from the user's boarding pass, then the user may be deemed to have passed the security check. Thus, this avoids the need for a second scan of the passport 213. This is beneficial since an extra scan of the passport 213 can be avoided, thereby reducing OCR reading errors and speeding up passenger processing through security.

Figure 5 shows a picture displayed on a terminal associated with the reader 211 which displays the details read from the passport 213 such as the user identification information. As shown in figure 5, the information may comprise one or more of the user's surname, name, document number, personal number, nationality, passport issuing state, date of birth, date of passport expiry, and gender may be read from the RFID chip. Data associated with a passenger's picture may also be read from the chip. The data contained within the machine readable zone may also be displayed on the terminal.

Also shown in figure 5 is a visual indication of the results of the comparison of the data read from the chip and the data encoded onto the boarding pass, such as the name on the boarding pass and the name read from the passport. In figure 5, the surname and given name have a check mark next to each of them. This indicates that both the surname and name on the passport 213 match the name on the boarding pass. This avoids the need for a human visual check of the boarding pass and passport 213, thereby improving accuracy and speeding up check in time.

As outlined above, with the introduction of NFC boarding passes, a boarding pass may be sent directly to a passenger's mobile telephone and may be read using an NFC/RFID scanner. New supplementary (APIS) passenger passport data, such as passport number, date of birth and date of expiry may be requested from the passenger at the time of check-in. This supplementary information may then be passed with the NFC boarding pass to the passenger's mobile telephone. When the NFC boarding pass is read at security, the supplementary passport information is then used to derive the key for access to the passport biometric data. Having this supplementary passport information eliminates the need to do an OCR scan of the passport details. Simply placing the passport close to the RFID scanner even when the passport is closed will result in the biometric information being read from the passport.

Although the present invention has been described with reference to a mobile device 207 such as a portable telephone which stores the e-boarding pass, the mobile device 207 is in fact optional. In some embodiments, after the user has performed remote check-in with server 205, a paper boarding pass may also be printed by the user or at another location alternatively or in addition to the generation and storage of the NFC boarding pass. Thus, embodiments of the invention may also be configured such that the server 205 generates a boarding pass including the additional information which is physically printed on the

boarding pass to encode the additional information on the paper boarding pass. The user may print the boarding pass using a standard printer, which has the additional information encoded on it within a specific region of the boarding pass. Thus, it is not essential in all embodiments for the electronic boarding pass to be sent to a user's electronic device provided a token storage medium is provided.

Further, some offices issuing official travel documents also require that the travel document is provided with a Faraday cage protecting a RFID chip within the cage from electro-magnetic waves. To access the chip protected within the cage, the official travel document must be opened prior to reading and thus, this provides an extra layer of security to prevent unauthorised reading of data from the RFID chip.

Preferably, the reading or NFC/RFID scanning is performed by a mobile telephone or other mobile or portable reader or scanner.

In some embodiments, the passport may be pre-stored on the mobile telephone. The passport may be stored in a secured or unsecured manner in the mobile telephone or other portable communication device. Thus, in some embodiments, the passport information is provided by a mobile telephone. Further, the security check matching may occur when the travel document such as the boarding pass is sent, or when checking-in.

In a further example, in addition to the security check which is performed to verify that a passenger name on a boarding pass matches the name on their passport, the photo in the passport may be checked against the passenger for a match. Embodiments of the invention may fully automate this check by comparing the passport facial biometric image also known as the reference image with the actual image of the passenger trying to board the flight. This may involve taking a photo of the passenger and automatically executing a facial recognition algorithm to compare it to the passport reference image.

In this example, embodiments of the invention may perform the following steps:

1. When a passenger checks in to a flight the minimum BAC information is collected i.e. passport number, date of birth and date of expiry. The boarding pass information together with the BAC information is transmitted and stored on the passengers' mobile telephone as an NFC boarding pass. The may be performed by placing the telephone on the passport. The telephone may then read the BAC information from the current boarding pass stored on the telephone, at step 701.

2. Typically a security check is done to authenticate the identity of the traveller. An NFC enabled telephone e.g. Samsung S3 or desktop reader may be used to read the NFC boarding pass stored on the passengers phone. As previously described, using the BAC details from the NFC boarding pass, the passengers' passport may also be read by an NFC enabled telephone or desktop reader at security. BAC provides access to the passengers' passport details and more importantly to the facial biometric image of the passenger. This may be performed by reading passport biometric facial image using the BAC information, at step 703, preferably saving the image on the phone. The passport details may then be automatically compared with the details in the NFC boarding pass e.g. first name and last name. In addition to this, the passenger or security officer may take the passenger picture using a front facing camera on using a telephone or other camera. The passenger may pose for a snapshot using a front facing camera on a phone, at step 705. After the picture is taken, a facial recognition algorithm may be used to automatically compare the picture to the passport facial biometric image. The algorithm compares the passport biometric facial image with the snapshot, at step 707.

The following numbered clauses are hereby included to give further description of the invention:

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

a server configured to collect user identity document data from the or a user and to construct a token comprising the user identity document data;

a key construction unit communicatively coupled to a reader configured to read the data from the token;

wherein the key construction unit uses the user identity document data read from the token to construct a key which enables the or a reader to decrypt the user information stored on the storage device.

2. A decryption system according to clause 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 preferably a user's date of birth.

3. A decryption system according to clause 1 wherein the or a 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 clause 1 in which the reader is configured to read the user information stored on the storage device.

5. A decryption system according to clause 1 in which 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.

6. A decryption system according to clause 7 further comprising a comparator 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.

7. A decryption system according to clause 7 further comprising a comparator 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.

8. A decryption system according to clause 1 further comprising a mobile device associated with a user for storing the token.

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

10. A decryption system according to clause 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 such as an airport check-in security desk.

11. A decryption system according to clause 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.

12. A decryption system according to clause 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.

13. A decryption system according to clause 1 in which the reader 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.

14. A boarding pass for use with the decryption system of clause 1, 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 predetermined region of the token 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.

15. 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 comprises a user identity document number and an expiry date of the user identity document and preferably the user's date of birth.

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

a reader configured to read data from a token such as a boarding pass and the like, the token including user identity document data encoded in a machine readable form, the reader configured to read the data encoded on the storage device; and

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

17. A decryption system according to clause 0 in which the reader is configured to read the user identity document data from a predetermined region of the token.

18. A decryption method for decrypting user information encrypted on a storage device associated with a user identity document, comprising the steps of:

collecting, using a server, user identity document data from the or a user;

constructing a token including the user identity document data encoded in a machine readable form;

reading, using a reader, the data from the token;

constructing, using a key construction unit, a key with the user identity document data read from the token, wherein the key enables the identity document reader to decrypt the user information stored on the storage device; and

preferably reading, using the reader, the information from the storage device.

19. A decryption method according to clause 18 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 preferably a user's date of birth.

20. A decryption method according to clause 18 wherein the or a user manually enters the user identity document data prior to reading the data encoded on the token.

21. A decryption method according to clause 18 further comprising the step of reading the user information stored on the storage device.

22. A decryption method according to clause 18 in which the token further comprises user identification information and in particular comprising the step of reading the user identification information from the token.

23. A decryption method according to clause 18 in which the token further comprises user identification information and in particular comprising the step of reading the user identification information from the token and further comprising the step of comparing the user identification information read from the token and the user information decrypted from the storage device associated with the user identity document.

24. A decryption method according to clause 18 in which the token further comprises user identification information and in particular comprising the step of reading the user identification information from the token and further comprising the step of 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 authenticating the user depending upon the result of the comparison.

25. A decryption method according to clause 18 further comprising a mobile device associated with a user for storing the token.

26. A decryption method according to clause 18 in which the token is a boarding pass further comprising the step of encoding the user identity document data in a predetermined region of the boarding pass.

27. A decryption method according to clause 18 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 such as an airport check-in security desk.

28. A decryption method according to clause 18 further comprising the step of constructing the key in response to reading the user identity document data encoded in machine readable form on or within the token.

29. A decryption method according to clause 18 in which the identity document reader is primed to decrypt the user information encrypted on the storage device in response to reading the user identity document data from the token.

30. A decryption method according to clause 18 in which the reader 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, further comprising the step of communicating with the storage device.

31. A token generating method for generating a boarding pass and the like comprising the steps of:

collecting, using a server, user identity document data from a user;

constructing, using a key construction unit, a token such as a boarding pass including the user identity document data encoded in a machine readable form; and

generating, using the or a server, the token having the data encoded on or within a predetermined region wherein 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.

32. A decryption method for decrypting user information encrypted on a storage device associated with a user identity document, the method comprising the steps of:

reading, using a reader, data from a token such as a boarding pass and the like, the token including user identity document data encoded in a machine readable form;

deriving, using a key construction unit, a key from the user identity document data encoded on or within the token; and

decrypting the user information stored on the storage device using the derived key.

33. A decryption method according to clause 18 or 32 in further comprising the step of reading the user identity document data from a predetermined region of the token and preferably in which the reader reads the data encoded on the storage device.

34. A computer program product which when executed undertakes the method of clause 18 or 32.

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

a server configured to collect user identity document data from the or a user and to construct a token comprising the user identity document data;

a reader configured to read the data from the token wherein the reader uses the user identity document data read from the token to decrypt the user information stored on the storage device.

36. A decryption system according to clause 35 wherein the reader is a portable reader or scanner such as a mobile telephone.

37. A decryption system according to clause 35 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.

38. The decryption system according to any one of clauses 1 to 17 further comprising the step of reading a user identity document biometric facial image using the key

39. The decryption system according to any one of clauses 1 to 17 or 38 further comprising the step of capturing an image of the user with a camera and preferably comparing the captured image with the passport biometric facial image read from the user identity document.

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;

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 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 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 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 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 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 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 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 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 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 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.

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.

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, 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.

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.

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.

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. 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.

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.

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.

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.

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.

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.

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.

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.

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 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 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.

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.

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.

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.

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.

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.

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.

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.

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 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.