Claims

1. A physical security item comprising a security certificate comprising first data that has been encrypted using a private encryption key, the encrypted first data being operable to be decrypted using a public decryption key associated with the private encryption key in order to authenticate the security certificate, characterised in that the security certificate further comprises second data that has been encrypted using a public encryption key, the encrypted second data being operable to be decrypted using a private decryption key associated with the public encryption key, wherein each of the encrypted first and second data is applied on the security item in the form of a visual image or in digital form on a microprocessor chip or a magnetic stripe, and wherein the private encryption key and the public encryption key are centrally stored in separate securely accessible key directories.
2. The security item of claim 1, wherein the visual image comprises a QR code, a barcode or a greyscale image.
3. The security item of claim 1 or claim 2, wherein the security certificate forms part of a travel visa.
4. A system for authenticating a security certificate of a physical security item, the security certificate comprising first data that has been encrypted using a private encryption key, the encrypted first data being

operable to be decrypted using a public decryption key associated with the private encryption key in order to authenticate the security certificate, wherein the security certificate further comprises second data that has been encrypted using a public encryption key, the encrypted second data being operable to be decrypted using a private decryption key associated with the public encryption key, wherein each of the encrypted first and second data is applied on the security item in the form of a visual image or in digital form on a microprocessor chip or a magnetic stripe, and wherein the private encryption key and the public encryption key are centrally stored in separate securely accessible key directories, the system comprising:

a public decryption key directory configured to allow an authorised user to access the public decryption key associated with the private encryption key; and

an authentication unit configured to decrypt the encrypted first data using the accessed public decryption key associated with the private encryption key,

a confidential data decryption unit configured to receive, from an authorised user, the encrypted second data and to decrypt the received data using the private decryption key associated with the public encryption key, the private decryption key being stored on a private decryption key directory configured to allow the authorised user to access the private encryption key associated with the public encryption key.

5. The system of claim 4, wherein the authentication unit is configured to determine whether or not the encrypted first data has been successfully decrypted using the accessed public decryption key.

6. The system of claim 5, wherein the authentication unit is configured to indicate that the security certificate is authentic if the encrypted first data is successfully decrypted and/or is configured to indicate that the security certificate is not authentic if the security certificate is not successfully decrypted.

7. The system of any one of claims 4 to 6, wherein the public decryption key directory comprises a database containing at least one public decryption key.

8. A method of authenticating a security certificate of a physical security item, the security certificate comprising first data that has been encrypted using a private encryption key, the encrypted first data being operable to be decrypted using a public decryption key associated with the private encryption key in order to authenticate the security certificate, wherein the security certificate further comprises second data that has been encrypted using a public encryption key, the encrypted second data being operable to be decrypted using a private decryption key associated with the public encryption key, wherein each of the encrypted first and second data is applied on the security item in the form of a visual image or in digital form on a microprocessor chip or a magnetic stripe, and wherein the private encryption key and the public encryption key are centrally stored in separate securely accessible key directories, the method comprising:

collecting the encrypted first and second data stored on the security certificate;

transmitting the encrypted first and second data to an authentication unit for attempted decryption of the encrypted first and second data using the public decryption key associated with the private encryption key and the private decryption key associated with the public encryption key respectively; and

determining the success or failure of the attempted decryption of the encrypted first and second data, wherein a successful decryption of the encrypted first and second data authenticates the security certificate.

9. The method of claim 8, wherein the method comprises:

retrieving the public decryption key associated with the private encryption key from a public decryption key directory and the private decryption key associated with the public encryption key from a private decryption key directory.

10. The method of claim 8 or claim 9, wherein the visual image comprises a QR code, a barcode or a greyscale image.

11. The method of any of claims 8 to 10, wherein the security certificate forms part of a travel visa.