

CLAIMS

- 5 1. A security certificate comprising data that has been encrypted using a private encryption key, the data being operable to be decrypted using a public decryption key associated with the private encryption key in order to authenticate the security certificate.
2. The security certificate of claim 1, wherein the encrypted data is stored in the form of a visual image, optionally wherein the visual image comprises a QR code, a barcode or a greyscale image.
- 10 3. The security certificate of claim 1, wherein the encrypted data is stored in digital form, optionally wherein the encrypted data is stored on a microprocessor chip or a magnetic stripe.
4. The security certificate of any preceding claim, wherein the security certificate further comprises data that has been encrypted using a public encryption key, the data being operable to be decrypted using a private decryption key associated with the public encryption key.
- 15 5. The security certificate of any preceding claim, wherein the security certificate forms part of a travel visa.
6. A system for authenticating security certificates comprising:
 - 20 a security certificate generator configured to encrypt data using a private encryption key and then generate a security certificate comprising the encrypted data;
 - a public decryption key directory configured to allow an authorised user to access a public decryption key associated with the private encryption key; and
 - an authentication unit configured to decrypt the encrypted data using the accessed public decryption key associated with the private encryption key.
- 25 7. The system of claim 6, wherein the authentication unit is configured to determine whether or not the encrypted data has been successfully decrypted using the accessed public decryption key.
8. The system of claim 7, wherein the authentication unit is configured to indicate that the security certificate is authentic if the encrypted 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.
- 30 9. The system of any one of claims 6 to 8, wherein the public decryption key directory comprises a database containing at least one public decryption key.
10. The system of any one of claims 6 to 9, wherein the security certificate generator is configured to use a public encryption key to encrypt data when generating the security certificate.
- 35 11. The system of claim 10, wherein the system further comprises a confidential data decryption unit configured to receive, from an authorised user, data encrypted with the public encryption

key; the confidential data decryption unit being configured to decrypt the received data using a 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 12. A method of authenticating a security certificate comprising:
- collecting encrypted data stored on the security certificate, the data having been encrypted with a private encryption key;
- transmitting the encrypted data to an authentication unit for attempted decryption of the encrypted data using a public decryption key associated with the private encryption key; and
- 10 determining the success or failure of the attempted decryption of the encrypted data, wherein a successful decryption of the encrypted data authenticates the security certificate.
13. A method of authenticating a security certificate comprising:
- collecting encrypted data stored on the security certificate, the data having been encrypted with a private encryption key;
- 15 retrieving a public decryption key associated with the private encryption key from a public decryption key directory;
- attempting to decrypt the encrypted data using the public decryption key associated with the private encryption key; and
- 20 determining the success or failure of the attempted decryption of the encrypted data, wherein a successful decryption of the encrypted data authenticates the security certificate.
14. The method of claim 12 or claim 13, wherein the encrypted data is stored in the form of a visual image, optionally wherein the visual image comprises a QR code, a barcode or a greyscale image.
- 25 15. The method of any of claims 12 to 14, wherein the security certificate forms part of a travel visa.