

In the claims:

1. A method of generating a digital signature, the method comprising:

generating a public and a private key on a secure device;
storing biometric information indicative of a user in the secure device;

receiving biometric information indicative of the user;
and

comparing the stored biometric information with the received biometric information on the secure device,
and

if the comparison is successful, generating a digital signature for a message.

2. The method of claim 1, wherein the secure device is portable.

3. The method of claim 1, wherein the secure device is a smart card.

4. The method of claim 1, additionally comprising generating a digital certificate that includes an identifier associated with the secure device.

5. A system for generating a digital signature, the system comprising:

means for generating a public and a private key on a secure device;

means for storing biometric information indicative of a user on the secure device;

means for receiving biometric information indicative of the user; and

means for comparing the stored biometric information with the received biometric information on the secure device, and if the comparison is successful, generating a digital signature for a message.

6. The system of claim 5, additionally comprising means for generating a digital certificate that includes an identifier associated with the secure device.

7. The system of claim 5, wherein the secure device is portable.

8. The system of claim 5, wherein the secure device is a smart card.

9. A method of generating a digital signature, the method comprising:

storing biometric information in a secure and portable device; and

generating, with the biometric information, a public key and a private key on the secure and portable device.

10. The method of claim 9, additionally comprising:

receiving a message; and

generating a digital signature for the message using, at least in part, the private key.

11. The method of claim 9, wherein the device includes a unique device identifier that is associated with the generated public and private keys.

12. A secure device for generating a digital signature, the secure device comprising:

a module configured to generate a public and a private key on a secure device;

a memory configured to store biometric information indicative of a user in the secure device; and

a biometric data analyzer configured to receive biometric information indicative of the user, and wherein the biometric data analyzer is configured to compare the stored biometric information with the received biometric information on the secure device, and if the comparison is successful, the biometric data analyzer generates a digital signature for a message.

13. The secure device of claim 12, wherein the secure device is portable.

14. The secure device of claim 12, wherein the secure device is a smart card.

15. A secure device, comprising:

a biometrics processor configured to process biometric data and configured to authenticate the identity of a user;

a biometrics interface for receiving biometric data and transmitting the biometric data to the biometrics processor;

a card reader interface for transmitting at least one message to an electronic device; and

a cryptoprocessor for generating a digital signature for the message;

wherein the secure device transmits the generated digital signature to the electronic device via the card reader interface subsequent to the biometric processor authenticating the identity of the user.

16. The secure device of claim 15, wherein the secure device is a smart card.

17. The secure device of claim 15, wherein the secure device is portable.

18. The secure device of claim 15, wherein the secure device transmits to the electronic device an electronic certificate that includes an identifier that is associated with the secure device.

19. A method of generating a digital signature on a smart card, comprising:

generating a public key on a portable smart card;

generating a private key on the portable smart card;

storing the private key in a tamperproof memory in the portable smart card;

storing biometric information indicative of a user in the portable smart card;

receiving biometric information indicative of the user at the portable smart card;

comparing the stored biometric information with the received biometric information on the portable smart card, and if the comparison is successful, generating a digital signature for a message, wherein the digital signature includes an encrypted message digest of the message, and wherein the digital signature is encrypted, at least in part, using the generated private key; and

transmitting the generated digital signature to a remote electronic device.

20. The method of claim 19, wherein the digital signature is transmitted with the message to a remote electronic device.