

Claims

1. A communications device for generating a user message comprising an assertion for verification by a remote device, the communications device comprising
5 a processor and a memory, the communications device being configured, under control of the processor, to execute instructions stored in the memory to:
- receive payload data for the user message, the payload data having been generated by a secure application resident on the communications device;
 - apply a first level security mechanism of biometric authentication of the user,
10 the biometric authentication comprising receiving input biometric information from the user and validating the input biometric information against biometric information for the user previously stored in the memory;
 - in response to successful biometric authentication of the user, apply a second level security mechanism to generate a digital signature based on the message
15 payload, wherein the digital signature is generated using a private signature key stored in a secure element of the communications device, wherein the private key is accessible only when the biometric authentication of the user is successful;
 - generate the user message for sending to the remote device, the user message comprising the message payload and the digital signature;
 - 20 apply a third level security encryption mechanism by authenticating the user message using a secure application-specific encryption key; and
 - encrypt the user message with the encryption key, wherein the encryption key is obfuscated in memory associated with the instructions in the communications device.
- 25
2. The communications device as claimed in claim 1, configured for the digital signature to be generated in a secure environment of the communications device.

3. The communications device as claimed in claim 2, configured for access to the private signature key to be limited solely to the secure environment of the communications device.
- 5 4. The communications device as claimed in any preceding claim, configured for the message payload to comprise one or more of: a key reference; user authentication data; client device identity data, and client application data, and/or configured for the user message to further comprise one or more of: a nonce and a timestamp.
- 10 5. The communications device as claimed in any preceding claim, configured for the digital signature to be generated by hashing the message payload to create a hash value, and encrypting the hash value with the private signature key to generate the digital signature.
- 15 6. The communications device as claimed in any preceding claim, wherein the communications device is further configured for generating an enrolment message comprising an assertion for verification by the remote device, wherein the communications device is configured, under control of the processor, to execute
- 20 instructions stored in the memory to:
- receive payload data for the enrolment message, in response to authentication of the user by the remote device;
 - perform biometric authentication of the user;
 - in response to successful biometric authentication of the user, generate an
- 25 asymmetric signature key pair comprising the private signature key for generating the digital signature and a corresponding public signature key;
- store the private signature key in the secure element, and
 - generate the enrolment message for sending to the remote device, the enrolment message comprising the payload data and the public signature key.
- 30

7. The communications device as claimed in claim 6, wherein the communications device is further configured, under control of the processor, to execute instructions stored in the memory to:

encrypt the enrolment message with the encryption key.

5

8. The communications device as claimed in claim 6 or claim 7, wherein the communications device is further configured, under control of the processor, to execute instructions stored in the memory to:

receive a response message from the remote device, the response message

10 indicating successful enrolment by the remote device, and

store a key reference associated with the asymmetric signature key pair contained in the payload of the response message.

9. A communications device for verifying an assertion in a user message
15 received from a remote device, the user message having been generated by a secure application resident on the remote device and authenticated using a secure application-specific encryption key obfuscated in memory associated with the secure application, the communications device comprising a processor and a memory, the communications device being configured, under control of the processor, to execute
20 instructions stored in the memory to:

validate the secure application-specific key used by the remote device to authenticate the received user message by successfully decrypting the payload of the user message using a service decryption key;

25 if the secure application-specific key is validated, determine that the received user message originated from a genuine secure application;

validate a digital signature in the payload of the received user message, using a public signature key and the message payload, and

if the digital signature is validated, determine that the user of the remote device has been biometrically authenticated at the remote device.

30

10. A communications device as claimed in claim 9, the communications device being further configured, under control of the processor, to execute instructions stored in the memory to:
- identify a key reference in the payload of the received user message, and
 - 5 look up the public signature key corresponding to the key reference stored in memory of the communications device.
11. A communications device as claimed in claim 9 or claim 10, the communications device being further configured, under control of the processor, to
- 10 execute instructions stored in the memory to perform one or more of:
- determine the validity of a nonce or timestamp in the received user message, and
 - determine the validity of user authentication data; client device identity data, and/or client application data in the payload of the received user message.
- 15
12. A communications device as claimed in claim 9, 10 or 11, wherein the communications device is further configured for verifying an assertion in an enrolment message received from a remote device, the communications device being further configured, under control of the processor, to execute instructions
- 20 stored in the memory to:
- receive the enrolment message from the remote device;
 - validate data in the message payload, the validated data identifying the user of the remote device that sent the enrolment message;
 - identify a public signature key in the message payload;
 - 25 store the public signature key in memory of the communications device, and
 - generate a key reference for the public signature key for sending in a response message to the remote device.
13. A communications device for generating a user message comprising an
- 30 assertion for verification by a remote device in a financial transaction, the

communications device comprising a processor and a memory, the communications device being configured, under control of the processor, to execute instructions stored in the memory to:

- 5 receive payload data for the user message, the payload data having been generated by a secure application resident on the communications device;
- apply a first level security mechanism of biometric authentication of the user, the biometric authentication comprising receiving input biometric information from the user and validating the input biometric information against biometric information for the user previously stored in the memory;
- 10 in response to successful biometric authentication of the user, apply a second level security mechanism to generate a digital signature based on the message payload, wherein the digital signature is generated using a private signature key stored in a secure element of the communications device, wherein the private key is accessible only when the biometric authentication of the user is successful;
- 15 generate the user message for sending to the remote device, the user message comprising the message payload and the digital signature; and
- apply a third level security encryption mechanism by authenticating the user message using a secure application-specific encryption key; and
- to encrypt the user message with the encryption key, wherein the encryption
- 20 key is obfuscated in memory associated with the instructions in the communications device.

14. A method, performed in a client communications device, for generating a user message comprising an assertion for verification by a remote server device, the
- 25 method comprising, under control of a processor of the client communications device:

- receiving payload data for the user message, the payload data having been generated by a secure application resident on the communications device;
- applying a first level security mechanism of biometric authentication of the
- 30 user, the biometric authentication comprising receiving input biometric information

from the user and validating the input biometric information against biometric information for the user previously stored in the memory;

in response to successful biometric authentication of the user, applying a second level security mechanism by generating a digital signature based on the message payload, wherein the digital signature is generated using a private signature key stored in a secure element of the client communications device, wherein the private key is accessible only when the biometric authentication of the user is successful;

generating the user message for sending to the remote server device, the user message comprising the message payload and the digital signature; and

applying a third level security encryption mechanism by authenticating the user message using a secure application-specific encryption key; and

encrypting the user message with the encryption key, wherein the encryption key is obfuscated in memory associated with the instructions in the client communications device.

15. The method as claimed in claim 14, comprising:

generating the digital signature in a secure environment of the client communications device, and/or

limiting access to the private signature key solely to the secure environment of the client communications device.

16. A computer program or computer program product comprising instructions for implementing the method of any one of claims 13 to 15.

17. A method, performed in a server communications device, for verifying an assertion in a user message received from a remote client device, the user message having been generated by a secure application resident on the remote client device and authenticated with a secure application-specific encryption key obfuscated in

memory associated with the secure application, the method comprising, under control of a processor of the client communications device:

validating the secure application-specific key used by the remote device to authenticate the received user message by successfully decrypting the payload of

5 the user message using a service decryption key;

if the secure application-specific key is validated, determining that the received user message originated from a genuine secure application;

validating a digital signature in the payload of the received user message, using a public signature key and the message payload, and

10 if the digital signature is validated, determining that the user of the client device has been biometrically authenticated at the remote client device.

18. A computer program or computer program product comprising instructions for implementing the method of claim 17.

15