

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; and
20 apply a third level security mechanism by authenticating the user message
using a secure application-specific key.

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.

25

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.

30 4. The communications device as claimed in claim 1, 2 or 3 configured:

for the third level security mechanism to be an encryption mechanism;
for the secure application-specific key to be an encryption key; and
to encrypt the user message with the encryption key, wherein the encryption
key is obfuscated in memory associated with the instructions in the communications
5 device.

5. 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
10 configured for the user message to further comprise one or more of: a nonce and a
timestamp.

6. 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
15 hash value, and encrypting the hash value with the private signature key to generate
the digital signature.

7. The communications device as claimed in any preceding claim, wherein the
communications device is further configured for generating an enrolment message
20 comprising an assertion for verification by the remote device, wherein the
communications device is configured, under control of the processor, to execute
instructions stored in the memory to:

receive payload data for the enrolment message, in response to
authentication of the user by the remote device;
25 perform biometric authentication of the user;
in response to successful biometric authentication of the user, generate an
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.

8. The communications device as claimed in claim 7, wherein the
5 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.

9. The communications device as claimed in claim 7 or claim 8, wherein the
10 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 indicating successful enrolment by the remote device, and

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

10. A communications device for verifying an assertion in a user message 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
20 application-specific key, 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:

validate the secure application-specific key used by the remote device to authenticate the received user message;

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
30 device has been biometrically authenticated at the remote device.

11. A communications device as claimed in claim 10, the communications device being further configured, under control of the processor, to execute instructions stored in the memory to:
- 5 identify a key reference in the payload of the received user message, and
 look up the public signature key corresponding to the key reference stored in memory of the communications device.
12. A communications device as claimed in claim 10 or claim 11, the
10 communications device being further configured, under control of the processor, to execute instructions stored in the memory to perform one or more of:
- decrypt the payload of the user message using a service decryption key,
 wherein the secure application-specific key used by the remote device to
 authenticate the received user message is an encryption key corresponding to the
15 service decryption key such that successful decryption validates the secure
 application-specific key;
 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,
20 and/or client application data in the payload of the received user message.
13. A communications device as claimed in claim 10, 11 or 12, wherein the
communications device is further configured for verifying an assertion in an
enrolment message received from a remote device, the communications device
25 being further configured, under control of the processor, to execute instructions
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;
30 identify a public signature key in the message payload;

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.

- 5 14. A communications device for generating a user message comprising an 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:
- 10 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
- 15 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 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
- 20 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; and
- apply a third level security mechanism by authenticating the user message using a secure application-specific key.
- 25
15. A method, performed in a client communications device, for generating a user message comprising an assertion for verification by a remote server device, the 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 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 mechanism by authenticating the user message using a secure application-specific key.

16. The method as claimed in claim 15, 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.

17. The method as claimed in claim 15 or claim 16, wherein the third level security mechanism is an encryption mechanism and the secure application-specific key is an encryption key, the method further comprising:
encrypting the user message with the encryption key, wherein the encryption key is obfuscated in memory in the client communications device.

30

18. A computer program or computer program product comprising instructions for implementing the method of any one of claims 15 to 17.

19. A method, performed in a server communications device, for verifying an
5 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 key, 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
10 authenticate the received user message;

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

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

20. A computer program or computer program product comprising instructions for implementing the method of claim 19.

20