

What is claimed is:

1. A network authentication method to be implemented using a client device and a verification server that are connected to a communication network, the client device being associated with an end user and storing an authentication application, said network authentication method comprising the steps of:

a) storing, by the verification server, a certificate that is assigned to the end user, the certificate including a unique user identifier (UID) of the end user, and an asymmetric key pair of a public key and a private key;

b) ~~storing, by upon receipt of the client device,~~ private key of the asymmetric key pair and a certificate reference ~~that,~~ which is mapped uniquely to the certificate assigned to the end user, that are associated with an authentication registration request from a network server, storing, by the client device, the certificate reference and a reference private key that is obtained by encrypting the private key with a personal identification number (PIN) code that is determined by the end user;

c) generating an input code through an input operation by the client device, to decrypt the reference private key stored in step b) with the user input code to obtain a current key, after receipt of a signature request and transaction data ~~that,~~ from the authentication server

in response to an authentication request received from
the network server, wherein the transaction data is
 associated with an electronic transaction message
 between the client device and athe network server and
 5 that is to be confirmed by the end user, and in response
 to execution of the authentication application,
~~generating a user input code through an input operation,~~
~~decrypting the reference private key stored in step b)~~
~~with the user input code to obtain a current key, and~~
 10 generating a digital signature for the transaction data
 using the current key and the transaction data; and
 d) determining by the verification server, upon
 receipt ~~of a~~ a verification request including the digital
 signature and athe certificate reference ~~via the~~
 15 ~~communication network,~~ determining from the
authentication server, based on the public key of the
 certificate to which the certificate reference received
 thereby is uniquely mapped, whether or not the digital
 signature received thereby is signed with the private
 20 key, and obtaining from the digital signature received
 thereby the transaction data that has been determined
 to be associated with the end user and that has been
 confirmed by the end user when it is determined that
 the digital signature is signed with the private key.

25

2. The network authentication method as claimed in claim
 1, wherein, in step c), when the user input code is

identical to the PIN code, the current key is identical to the private key.

3. The network authentication method as claimed in claim 1, to be implemented further using the network server and an authentication server that are connected to the communication network, said network authentication method further comprising, between steps b) and c), the steps of:

10 e) upon receipt of a transaction message associated with the electronic transaction, sending, by the network server, an authentication request for the electronic transaction to the authentication server via the communication network, the authentication request including the UID of the end user and the transaction data to be confirmed by the end user; and

15 f) after receipt of the authentication request from the network server, sending, by the authentication server, a signature request for the transaction data to the client device via the communication network, the signature request including the transaction data; wherein, in step c), prior to generation of the user input code, the client device further displays the transaction data thereon.

25 4. The network authentication method as claimed in claim 3, further comprising, between steps c) and d), the steps

of:

g) by the client device, sending, in response to execution of the authentication application, the digital signature generated in step c) and the certificate reference stored in step b) to the authentication server via the communication network; and

h) upon receipt of a digital signature and a certificate reference via the communication network, sending, by the authentication server, a verification request for the digital signature to the verification server via the communication network, the verification request including the digital signature and the certificate reference received by the authentication server;

wherein step d) is performed by the verification server upon receipt of the verification request.

5. The network authentication method as claimed in claim 4, further comprising, subsequent to step d), the steps of:

i) when it is determined that the digital signature is signed with the private key, notifying, by the verification server, the authentication server of successful digital signature verification;

j) upon receipt of the notification of successful digital signature verification from the verification server,

notifying, by the authentication server, the client device of completion of digital signature verification;

k) upon receipt of the notification of completion of digital signature verification from the authentication server, sending, by the client device, the certificate reference stored in step b) to the network server via the communication network;

l) upon receipt of a certificate reference via the communication network, sending, by the network server, a verification request for the transaction data to the verification server via the communication network, the verification request including the transaction data and the certificate reference received by the network server; and

m) in response to receipt of the verification request from the network server, by the verification server, determining whether or not the transaction data included in the verification request matches the transaction data obtained thereby in step d) and confirmed by the end user, and notifying the network server of successful transaction data verification when it is determined that the transaction data included in the verification request matches the transaction data obtained thereby in step d);

n) upon receipt of the notification of successful transaction data verification from the verification server, notifying, by the network server, the

authentication server of successful transaction data verification;

o) upon receipt of the notification of successful transaction data verification, notifying, by the authentication server, the network server of successful authentication of the electronic transaction.

6. The network authentication method as claimed in claim 3, the client device including a plurality of hardware components, each of which has a unique identification code, the authentication server storing reference hardware identification data that is associated with the UID of the end user and that is used to verify the identity of the client device, said network authentication method further comprising, between steps e) and f), the steps of:

p) in response to receipt of the authentication request from the network server, by the authentication server, generating a one-time message identification (MID) that corresponds uniquely to the authentication request, and sending the MID to the network server via the communication network;

q) transmitting, by the network server, the MID from the authentication server to the client device via the communication network;

r) in response to receipt of the MID from the network server, by the client device, executing the authentication application to generate hardware

scanning data that is associated with the identification codes of the hardware components of the client device and to send the MID received thereby and the hardware scanning data generated thereby to the authentication server via the communication network; and

5 s) upon receipt of the MID and the hardware scanning data via the communication network, by the authentication server, determining whether or not the hardware scanning data received thereby matches the reference hardware identification data stored therein;

10 wherein step f) is performed when it is determined that the hardware scanning data received by the authentication server in step s) matches the reference hardware identification data stored in the authentication server.

15 7. The network authentication method as claimed in claim 1, further comprising, prior to step a), the step of: I) in response to receipt of a certificate request for the end user that includes the UID of the end user, by the verification server, assigning the certificate to

20 the end user, and generating the certificate reference that is mapped uniquely to the certificate and that is to be stored in the client device in step b).

8. The network authentication method as claimed in claim 7, to be implemented further using an authentication server connected to the communication network, said network authentication method further comprising,

25

between steps a) and b), the steps of:

II) receiving, by the authentication server, an authentication registration request for the end user, the authentication registration request including the
5 UID of the end user, the private key, and the certificate reference generated by the verification server in step I);

III) sending, by the authentication server, the private key and the certificate reference received thereby to
10 the client device via the communication network; and
IV) upon receipt of the private key and the certificate reference from the authentication server, by the client device, in response to execution of the authentication application, generating the PIN code through an input
15 operation by the end user, and encrypting the private key with the PIN code to generate the reference private key.

9. The network authentication method as claimed in claim 8, to be implemented further using the network server,
20 the network server being connected to the communication network, said network authentication method further comprising, prior to step I), the step of:

V) after successful login, sending, by the network server, the certificate request to the verification server via
25 the communication network.

10. The network authentication method as claimed in claim 9, further comprising, between steps a) and

II), the steps of:

VI) in response to receipt of the certificate request from the network server, sending, by the verification server, the private key and the certificate reference
5 to the network server via the communication network;
and

VII) upon receipt of the private key and the certificate reference from the verification server, sending, by the network server, the authentication registration
10 request to the authentication server via the communication network.

11. The network authentication method as claimed in claim 9, the client device including a plurality of hardware components, each of which has a unique
15 identification code, said network authentication method further comprising, between steps II) and III), the steps of:

VIII) in response to receipt of the authentication registration request, by the authentication server,
20 generating an authentication code, and sending the authentication code to the network server via the communication network;

IX) upon receipt of the authentication code from the authentication server, sending, by the network server,
25 the authentication code to the client device;

X) in response to receipt of the authentication code from the network server, by the client device, executing

the authentication application to generate hardware scanning data that is associated with the identification codes of the hardware components of the client device and to send the authentication code received thereby and the hardware scanning data generated thereby to the authentication server via the communication network; and

5 XI) upon receipt of hardware scanning data and authentication code via the communication network, by the authentication server, determining whether or not the authentication code received thereby matches the authentication code generated in step VIII), and storing, when it is determined that a match occurs, the hardware scanning data received thereby as reference hardware identification data that is associated with the UID of the end user and that is used to verify the identity of the client device;

15 wherein step III) is performed when the authentication code received by the authentication server in step X) is identical to the authentication code generated by the authentication server in step VIII).

What is claimed is:

1. A network authentication method to be implemented using a client device and a verification server that are connected to a communication network, the client
5 device being associated with an end user and storing an authentication application, said network authentication method comprising the steps of:
 - a) storing, by the verification server, a certificate that is assigned to the end user, the certificate
10 including a unique user identifier (UID) of the end user, and an asymmetric key pair of a public key and a private key;
 - b) upon receipt of the private key of the asymmetric
15 key pair and a certificate reference, which is mapped uniquely to the certificate assigned to the end user, that are associated with an authentication registration request from a network server, storing, by the client device, the certificate reference and a reference
20 private key that is obtained by encrypting the private key with a personal identification number (PIN) code that is determined by the end user;
 - c) generating an input code through an input operation
25 by the client device to decrypt the reference private key stored in step b) with the user input code to obtain a current key, after receipt of a signature request and transaction data, from the authentication server in response to an authentication request received from the

network server, wherein the transaction data is associated with an electronic transaction message between the client device and the network server and that is to be confirmed by the end user, and in response to execution of the authentication application, generating a digital signature for the transaction data using the current key and the transaction data; and

d) determining by the verification server, upon receipt a verification request including the digital signature and the certificate reference from the authentication server, based on the public key of the certificate to which the certificate reference received thereby is uniquely mapped, whether or not the digital signature received thereby is signed with the private key, and obtaining from the digital signature received thereby the transaction data that has been determined to be associated with the end user and that has been confirmed by the end user when it is determined that the digital signature is signed with the private key.

2. The network authentication method as claimed in claim 1, wherein, in step c), when the user input code is identical to the PIN code, the current key is identical to the private key.

3. The network authentication method as claimed in claim 1, to be implemented further using the network server

and an authentication server that are connected to the communication network, said network authentication method further comprising, between steps b) and c), the steps of:

5 e) upon receipt of a transaction message associated with the electronic transaction, sending, by the network server, an authentication request for the electronic transaction to the authentication server via the communication network, the authentication request
10 including the UID of the end user and the transaction data to be confirmed by the end user; and

 f) after receipt of the authentication request from the network server, sending, by the authentication server, a signature request for the transaction data
15 to the client device via the communication network, the signature request including the transaction data;
 wherein, in step c), prior to generation of the user input code, the client device further displays the transaction data thereon.

20

4. The network authentication method as claimed in claim 3, further comprising, between steps c) and d), the steps of:

 g) by the client device, sending, in response to
25 execution of the authentication application, the digital signature generated in step c) and the certificate reference stored in step b) to the

authentication server via the communication network;
and

h) upon receipt of a digital signature and a
certificate reference via the communication network,
5 sending, by the authentication server, a verification
request for the digital signature to the verification
server via the communication network, the verification
request including the digital signature and the
certificate reference received by the authentication
10 server;

wherein step d) is performed by the verification
server upon receipt of the verification request.

5. The network authentication method as claimed in claim
15 4, further comprising, subsequent to step d), the steps
of:

i) when it is determined that the digital signature is
signed with the private key, notifying, by the
verification server, the authentication server of
20 successful digital signature verification;

j) upon receipt of the notification of successful digital
signature verification from the verification server,
notifying, by the authentication server, the client
device of completion of digital signature verification;

25 k) upon receipt of the notification of completion of
digital signature verification from the authentication
server, sending, by the client device, the certificate

reference stored in step b) to the network server via the communication, network;

l) upon receipt of a certificate reference via the communication network, sending, by the network server,
5 a verification request for the transaction data to the verification server via the communication network, the verification request including the transaction data and the certificate reference received by the network server;
and

10 m) in response to receipt of the verification request from the network server, by the verification server, determining whether or not the transaction data included in the verification request matches the transaction data obtained thereby in step d) and confirmed by the end
15 user, and notifying the network server of successful transaction data verification when it is determined that the transaction data included in the verification request matches the transaction data obtained thereby in step d);

20 n) upon receipt of the notification of successful transaction data verification from the verification server, notifying, by the network server, the authentication server of successful transaction data verification;

25 o) upon receipt of the notification of successful transaction data verification, notifying, by the authentication server, the network server of successful

authentication of the electronic transaction.

6. The network authentication method as claimed in claim 3, the client device including a plurality of hardware components, each of which has a unique identification code, the authentication server storing reference hardware identification data that is associated with the UID of the end user and that is used to verify the identity of the client device, said network authentication method further comprising, between steps e) and f), the steps of:

p) in response to receipt of the authentication request from the network server, by the authentication server, generating a one-time message identification (MID) that corresponds uniquely to the authentication request, and sending the MID to the network server via the communication network;

q) transmitting, by the network server, the MID from the authentication server to the client device via the communication network;

r) in response to receipt of the MID from the network server, by the client device, executing the authentication application to generate hardware scanning data that is associated with the identification codes of the hardware components of the client device and to send the MID received thereby and the hardware scanning data generated thereby to the authentication server via the communication network; and

s) upon receipt of the MID and the hardware scanning data via the communication network, by the authentication server, determining whether or not the hardware scanning data received thereby matches the reference hardware identification data stored therein;
5 wherein step f) is performed when it is determined that the hardware scanning data received by the authentication server in step s) matches the reference hardware identification data stored in the authentication server.
10

7. The network authentication method as claimed in claim 1, further comprising, prior to step a), the step of:
I) in response to receipt of a certificate request for the end user that includes the UID of the end user, by
15 the verification server, assigning the certificate to the end user, and generating the certificate reference that is mapped uniquely to the certificate and that is to be stored in the client device in step b).

8. The network authentication method as claimed in claim
20 7, to be implemented further using an authentication server connected to the communication network, said network authentication method further comprising, between steps a) and b), the steps of:

II) receiving, by the authentication server, an
25 authentication registration request for the end user, the authentication registration request including the UID of the end user, the private key, and the certificate

reference generated by the verification server in step I);

III) sending, by the authentication server, the private key and the certificate reference received thereby to the client device via the communication network; and
5 IV) upon receipt of the private key and the certificate reference from the authentication server, by the client device, in response to execution of the authentication application, generating the PIN code through an input operation by the end user, and encrypting the private
10 key with the PIN code to generate the reference private key.

9. The network authentication method as claimed in claim 8, to be implemented further using the network server, the network server being connected to the communication
15 network, said network authentication method further comprising, prior to step I), the step of:
V) after successful login, sending, by the network server, the certificate request to the verification server via the communication network.
20

10. The network authentication method as claimed in claim 9, further comprising, between steps a) and II), the steps of:
VI) in response to receipt of the certificate request from the network server, sending, by the verification
25 server, the private key and the certificate reference to the network server via the communication network;

and

VII) upon receipt of the private key and the certificate reference from the verification server, sending, by the network server, the authentication registration request to the authentication server via the communication network.

11. The network authentication method as claimed in claim 9, the client device including a plurality of hardware components, each of which has a unique identification code, said network authentication method further comprising, between steps II) and III), the steps of:

VIII) in response to receipt of the authentication registration request, by the authentication server, generating an authentication code, and sending the authentication code to the network server via the communication network;

IX) upon receipt of the authentication code from the authentication server, sending, by the network server, the authentication code to the client device;

X) in response to receipt of the authentication code from the network server, by the client device, executing the authentication application to generate hardware scanning data that is associated with the identification codes of the hardware components of the client device and to send the authentication code received thereby and the hardware scanning data generated thereby to the

authentication server via the communication network;
and

XI) upon receipt of hardware scanning data and
authentication code via the communication network, by
5 the authentication server, determining whether or not
the authentication code received thereby matches the
authentication code generated in step VIII), and storing,
when it is determined that a match occurs, the hardware
scanning data received thereby as reference hardware
10 identification data that is associated with the UID of
the end user and that is used to verify the identity
of the client device;

wherein step III) is performed when the authentication
code received by the authentication server in step X)
15 is identical to the authentication code generated by
the authentication server in step VIII).