

CLAIMS

1. A method for authenticating a user of at least a first user electronic device and a second user electronic device using a network node, the method comprising:

(a) receiving, at the network node, from the first user electronic device, at a first moment in time, communication protocol information comprising:

(i) a restricted enrollment input ~~corresponding to an unrestricted enrollment input that has been restricted by,~~ wherein the restricted enrollment input has been produced by restricting an unrestricted enrollment input with an enrollment biometric template indicative of user enrollment biometrics of the user captured at an enrollment moment in time that is prior to the first moment in time;

(ii) an unrestricted authentication input that has been encrypted; and

(iii) a transformed matching function that is operative to output a success key in response to successfully evaluating the transformed matching function using two inputs;

(b) receiving, at the network node, from the second user electronic device, at a second moment in time after the first moment in time, a restricted authentication input ~~corresponding to the unrestricted authentication input that has been restricted by,~~ wherein the restricted authentication input has been produced by restricting the unrestricted authentication input with an authentication biometric sample indicative of user authentication biometrics captured at an authentication moment in time that is after the first moment in time but that is prior to the second moment in time;

(c) after the receiving the restricted authentication input, evaluating, at the network node, the transformed matching function using the restricted enrollment input and the restricted authentication input; and

(d) when the evaluating is successful, using, at the network node, the success key output by the transformed matching function to enable a secure operation, wherein:

(i) the enrollment biometric template is not accessible to the network node;

(ii) the authentication biometric sample is not accessible to the network node;

(iii) the user enrollment biometrics are not accessible to the network node; and

(iv) the user authentication biometrics are not accessible to the network node.

2. The method of claim 1, wherein the second user electronic device is the first user electronic device.

~~3. The method of claim 1, wherein the enrollment biometric template is not accessible to the network node.~~

~~4. The method of claim 1, wherein the authentication biometric sample is not accessible to the network node.~~

~~5. The method of claim 4, wherein the enrollment biometric template is not accessible to the network node.~~

~~63. A The method of claim 1, wherein:~~

~~for authenticating a user of at least a first user electronic device and a second user electronic device using a network node, the method comprising:~~

~~—— receiving, at the network node, from the first user electronic device, at a first moment in time, communication protocol information comprising:~~

~~—— a restricted enrollment input corresponding to an unrestricted enrollment input that has been restricted by an enrollment biometric template indicative of user enrollment biometrics captured at an enrollment moment in time that is prior to the first moment in time;~~

~~—— an unrestricted authentication input; and~~

~~—— a transformed matching function that is operative to output a success key in response to successfully evaluating the transformed matching function using two inputs;~~

~~—— receiving, at the network node, from the second user electronic device, at a second moment in time after the first moment in time, a restricted authentication input corresponding to the unrestricted authentication input that has been restricted by an authentication biometric sample indicative of user authentication biometrics captured at an authentication moment in time that is after the first moment in time but that is prior to the second moment in time;~~

~~—— after the receiving the restricted authentication input, evaluating, at the network node, the transformed matching function using the restricted enrollment input and the restricted authentication input; and~~

~~—— when the evaluating is successful, using, at the network node, the success key output by the transformed matching function to enable a secure operation, wherein:~~

(a) the communication protocol information further comprises doubly encrypted seed data comprising seed information that has been encrypted with an inner key and then encrypted with the success key; and

(b) the using the success key comprises:

(i) decrypting, at the network node, using the success key output by the transformed matching function, the doubly encrypted seed data to reveal singly encrypted seed data comprising the seed information that has been encrypted with the inner key; and

(ii) after the decrypting, sending, from the network node, to a remote entity, the singly encrypted seed data for further enabling the secure operation.

74. The method of claim 63, wherein the remote entity is the first user electronic device.

85. The method of claim 63, wherein the remote entity is the second user electronic device.

96. The method of claim 63, wherein the communication protocol information further comprises encrypted inner key data comprising the inner key that has been encrypted with a public encryption key of the first user electronic device.

107. The method of claim 96, wherein:

the second user electronic device is the first user electronic device;

the unrestricted authentication input of the communication protocol information ~~is~~ has been encrypted with the inner key; and

the method further comprises, after the receiving the communication protocol information, but before the receiving the restricted authentication input, sending, from the network node, to the first user electronic device, the encrypted inner key data and the unrestricted authentication input encrypted with the inner key.

118. The method of claim 63, wherein the seed information comprises at least a portion of a secret seed generated by the first user electronic device.

129. The method of claim 118, wherein the secret seed is not stored on the first user electronic device at the second moment in time.

~~13~~10. The method of claim ~~6~~3, wherein:

- (a) the communication protocol information further comprises doubly encrypted enrollment biometric template data comprising enrollment biometric template information that has been encrypted with the inner key and then encrypted with the success key; and
- (b) the using the success key further comprises:
 - (i) decrypting, at the network node, using the success key output by the transformed matching function, the doubly encrypted enrollment biometric template data to reveal singly encrypted enrollment biometric template data comprising the enrollment biometric template information that has been encrypted with the inner key; and
 - (ii) after the decrypting, sending, from the network node, to the remote entity, the singly encrypted enrollment biometric template data.

~~14~~11. The method of claim ~~6~~3, wherein the remote entity is configured to use the seed information to authenticate a challenge from a third party subsystem.

~~15.~~—A method for authenticating a user of a user electronic device using a network node, the method comprising:

- obtaining, at the user electronic device, a seed;
- generating, at the user electronic device, an enrollment biometric template indicative of user enrollment biometric identifier information;
- identifying, at the user electronic device, a transformed matching function that is operative to output a success key in response to successfully evaluating the transformed matching function using a first input and a second input;
- generating, at the user electronic device, a restricted enrollment input by restricting the first input using the enrollment biometric template;
- encrypting, at the user electronic device, with the success key, seed information that comprises at least a portion of the seed;
- after the encrypting, deleting the seed from the user electronic device; and
- sending, from the user electronic device, to the network node, enrollment data comprising the encrypted seed information and the transformed matching function and the restricted enrollment input.

~~16.~~—The method claim ~~15~~, wherein:

~~the method further comprises generating, at the user electronic device, an inner key;~~
~~and~~
~~the seed information comprises the at least a portion of the seed encrypted with the inner key.~~

~~17. The method of claim 15, further comprising:~~

~~after the sending, receiving, at the user electronic device, from the network node, the seed information;~~
~~recovering, at the user electronic device, the seed using the received seed information;~~
~~and~~
~~using, at the electronic device, the recovered seed to enable a secure operation.~~

~~18. The method of claim 15, further comprising:~~

~~after the sending, generating, at the user electronic device, an authentication biometric sample indicative of user authentication biometric identifier information;~~
~~generating, at the user electronic device, a restricted authentication input by restricting the second input using the authentication biometric sample; and~~
~~transmitting, from the user electronic device, to the network node, the restricted authentication input.~~

~~19. The method of claim 15, further comprising:~~

~~encrypting, at the user electronic device, with the success key, enrollment biometric template information that comprises at least a portion of the enrollment biometric template;~~
~~and~~
~~after both of the encrypting the enrollment biometric template information and the generating the restricted enrollment input, deleting the enrollment biometric template from the user electronic device, wherein the enrollment data further comprises the encrypted enrollment biometric template information.~~

~~20~~12. A non-transitory computer-readable storage medium storing at least one program, the at least one program comprising instructions, which, when executed by at least one processor of an electronic subsystem, cause the at least one processor to execute the method of any one of the previous claims.

—— receive, from a user electronic device, a restricted enrollment input corresponding to an unrestricted enrollment input that has been restricted by an enrollment biometric template indicative of user enrollment biometrics captured at an enrollment moment in time;

—— receive, from the user electronic device, a restricted authentication input corresponding to an unrestricted authentication input that has been restricted by an authentication biometric sample indicative of user authentication biometrics captured at an authentication moment in time after the enrollment moment in time;

—— receive, from the user electronic device, a transformed matching function that is operative to output a success key in response to successfully evaluating the transformed matching function using two inputs;

—— evaluate the received transformed matching function using the received restricted enrollment input and the received restricted authentication input; and

—— when the evaluation is successful, use the success key output by the transformed matching function to enable a secure operation.