

WHAT IS CLAIMED IS:

- 1 1. A method comprising:
2 receiving, by a user device, a second biometric template of a user;
3 providing, by the user device, an authentication request message
4 comprising an electronic identity and a derivative of the second biometric template of
5 the user to a resource provider computer to conduct an interaction, the authentication
6 request being forwarded to a processing server computer by the resource provider
7 computer; and
8 receiving, by the user device, an authentication response message
9 comprising an authentication result from the processing server computer,
10 wherein the authentication result is determined by the processing server
11 computer based on a comparison of the derivative of the second biometric template to a
12 derivative of a first biometric template accessible to the processing server computer,
13 and wherein the authentication result is also based on a validity of the electronic
14 identity.
- 1 2. The method of claim 1, further comprising:
2 receiving, by the user device, the first biometric template of the user;
3 generating, by the user device, the derivative of the first biometric
4 template;
5 generating, by the user device, an identity request message for an
6 electronic identity for the user, the identity request message comprising the derivative of
7 the first biometric template and an account identifier of the user;
8 sending, by the user device, the identity request message to a verification
9 server, wherein the verification server verifies the account identifier and generates the
10 electronic identity, and wherein the electronic identity is linked to the derivative of the
11 first biometric template in a database by the processing server computer;
12 receiving, by the user device, an identity response message comprising
13 the electronic identity; and
14 storing, by the user device, the electronic identity in a memory of the user
15 device for later use in an interaction.

1 3. The method of claim 2, wherein the processing server computer
2 initiates the publishing of a record to a blockchain, the record comprising a record of the
3 electronic identity and the derivative of the first biometric template of the user being
4 linked.

1 4. The method of claim 3, wherein the validity of the electronic identity
2 is based at least upon the record published on the blockchain of the electronic identity
3 and the derivative of the first biometric template of the user being linked.

1 5. The method of claim 3, wherein the record of the electronic identity
2 and the derivative of the first biometric template being linked is signed by the verification
3 server and the processing server computer using a digital signature encryption scheme.

1 6. The method of claim 5, wherein the validity of the electronic identity
2 is based at least upon the validation of one or more digital signatures appended to the
3 record of the electronic identity and the derivative of the first biometric template being
4 linked.

1 7. The method of claim 2, wherein the derivative of the first biometric
2 template and the derivative of the second biometric template are derived from the first
3 biometric template and second biometric template of the user respectively by passing
4 the first and second biometric templates through an algorithm.

1 8. The method of claim 2, wherein the derivative of the first biometric
2 is stored and retrieved by the processing server computer by communicating with an
3 authentication server.

1 9. A server computer comprising:
2 a network interface;
3 a processor; and
4 a non-transitory computer-readable medium comprising code for
5 instructing the processor to implement a method, the method comprising:

6 receiving, by the server computer, an authentication request
7 message comprising an electronic identity and a derivative of a second biometric
8 template of a user of a user device;
9 determining, by the server computer, a derivative of a first biometric
10 template linked to the electronic identity;
11 retrieving, by the server computer, the derivative of the first
12 biometric template;
13 comparing, by the server computer, the derivative of the first
14 biometric template to the derivative of the second biometric template; and
15 determining, by the server computer, an authentication result based
16 at least upon the comparison of the derivative of the first biometric template to
17 the derivative of the second biometric template and at least upon the validity of
18 the electronic identity.

1 10. The server computer of claim 9, wherein the method further
2 comprises:
3 receiving, by the server computer, an identity request message comprising
4 the derivative of the first biometric template and the electronic identity, wherein the
5 electronic identity is received from a verification server after the verification server
6 verifies an account identifier of the user;
7 linking, by the server computer, the derivative of the first biometric
8 template and the electronic identity in a mapping table;
9 storing, by the server computer, the derivative of the first biometric
10 template in a database; and
11 generating, by the server computer, an identity response message
12 comprising the electronic identity, wherein the identity response message is received by
13 the user device, and wherein the user device stores the electronic identity in a memory
14 of the user device for later use in an interaction.

1 11. The server computer of claim 10, wherein the method further
2 comprises:

3 initiating, by the server computer, the publishing of a record to a
4 blockchain, the record comprising a record of the electronic identity and the derivative of
5 the first biometric template being linked.

6 12. The server computer of claim 11, wherein determining the
7 authentication result based at least upon the validity of the electronic identity comprises:
8 comparing, by the server computer, the electronic identity to a record on
9 the blockchain of the electronic identity and the derivative of the first biometric template
10 being linked; and
11 validating, by the server computer, the electronic identity if the electronic
12 identity matches the record published on the blockchain.

1 13. The server computer of claim 11, wherein the record on the
2 blockchain of the electronic identity and the derivative of the first biometric template
3 being linked is signed by the verification server and the server computer using a digital
4 signature encryption scheme.

1 14. The server computer of claim 13, wherein determining the
2 authentication result based at least upon the validity of the electronic identity comprises:
3 validating, by the server computer, the digital signatures appended to the
4 record published on the blockchain using the public keys of at least the verification
5 server.

1 15. The server computer of claim 10, wherein the derivative of the first
2 biometric template and derivative of the second biometric template are derived from the
3 first biometric template and second biometric template of the user respectively by
4 passing the first and second biometric template through an algorithm.

1 16. The server computer of claim 10, wherein storing the derivative of
2 the first biometric template in a database comprises:
3 sending, by the server computer, the derivative of the first biometric
4 template to an authentication server, wherein the authentication server stores the
5 derivative of the first biometric template in the database, and wherein retrieving the

6 derivative of the first biometric template comprises sending a request to the
7 authentication server.

1 17. A resource provider computer comprising:
2 a network interface;
3 a processor; and
4 a non-transitory computer-readable medium comprising code for
5 instructing the processor to implement a method, the method comprising:
6 receiving, by the resource provider computer, an authentication
7 request message from a user device of a user, the authentication request
8 message comprising an electronic identity and a derivative of a second biometric
9 template of the user;
10 sending, by the resource provider computer, the authentication
11 request message to a processing server computer, the processing server
12 computer determining an authentication result based at least upon the
13 comparison of the derivative of the second biometric template to a derivative of a
14 first biometric template and based at least upon the validity of the electronic
15 identity;
16 receiving, by the resource provider computer, from the processing
17 server computer, an authentication response message comprising the
18 authentication result;
19 sending, by the resource provider computer, the authentication
20 response message to the user device; and
21 authenticating, by the resource provider computer, the user if the
22 authentication result indicates that the derivative of the second biometric
23 template and the derivative of the first biometric template match, and if the
24 authentication result indicates that the electronic identity is valid, wherein the
25 electronic identity is generated by a verification server upon verification of an
26 account identifier of the user.

1 18. The resource provider computer of claim 17, wherein the validity of
2 the electronic identity is based at least upon a record published on a blockchain of the
3 electronic identity and the derivative of the first biometric template being linked.

1 19. The resource provider computer of claim 18, wherein the record
2 published on the blockchain is signed by the verification server and the processing
3 server computer.

1 20. The resource provider computer of claim 19, wherein the validity of
2 the electronic identity is based at least upon the validation of one or more digital
3 signatures appended to the record published on the blockchain.