

WHAT IS CLAIMED IS:

- 1 1. A method comprising:
2 receiving, by an authentication node, a plurality of encrypted match
3 values, wherein the plurality of encrypted match values were formed by a plurality of
4 worker nodes that compare a plurality of encrypted second biometric template parts
5 derived from a second biometric template to a plurality of encrypted first biometric
6 template parts derived from a first biometric template;
7 decrypting, by the authentication node, the plurality of encrypted match
8 values resulting in a plurality of decrypted match values; and
9 determining, by the authentication node, if a first biometric template
10 matches the second biometric template using the plurality of decrypted match values.
- 1 2. The method of claim 1 further comprising:
2 dividing, by the authentication node, the second biometric template
3 resulting in second biometric template parts;
4 encrypting, by the authentication node, the second biometric template
5 parts resulting in encrypted second biometric template parts; and
6 transmitting, by the authentication node, the encrypted second biometric
7 template parts to the plurality of worker nodes.
- 1 3. The method of claim 1 further comprising:
2 encrypting, by the authentication node, the second biometric template
3 resulting in an encrypted second biometric template; and
4 transmitting, by the authentication node, the encrypted second biometric
5 template to the plurality of worker nodes, wherein the plurality of worker nodes derive
6 the encrypted second biometric template parts.
- 1 4. The method of claim 1, wherein determining, by the authentication
2 node, if the first biometric template matches the second biometric template using the
3 plurality of decrypted match values, further comprises:

4 determining, by the authentication node, a weight associated with each
5 decrypted match value of the plurality of decrypted match values;
6 determining, by the authentication node, an overall authentication
7 threshold;
8 comparing, by the authentication node, a number of worker nodes that
9 responded to a number of needed responses; and
10 determining, by the authentication node, if an overall decision based on
11 the weights and the decrypted match values is greater than or equal to the overall
12 authentication threshold.

1 5. The method of claim 1 further comprising:
2 transmitting, by the authentication node, if the first biometric template
3 matches the second biometric template, an authorization request message to an
4 authorizing entity computer; and
5 receiving, by the authentication node, an authorization response message
6 from the authorizing entity computer.

1 6. An authentication node comprising:
2 a processor;
3 a memory device; and
4 a computer-readable medium coupled to the processor, the computer-
5 readable medium comprising code executable by the processor for implementing a
6 method comprising:
7 receiving a plurality of encrypted match values, wherein the plurality of
8 encrypted match values were formed by a plurality of worker nodes that compare a
9 plurality of encrypted second biometric template parts derived from a second biometric
10 template to a plurality of encrypted first biometric template parts derived from a first
11 biometric template;
12 decrypting the plurality of encrypted match values resulting in a plurality of
13 decrypted match values; and

14 determining if a first biometric template matches the second biometric
15 template using the plurality of decrypted match values.

1 7. The authentication node of claim 6, wherein the method further
2 comprises:
3 dividing the second biometric template resulting in second biometric
4 template parts;
5 encrypting the second biometric template parts resulting in encrypted
6 second biometric template parts; and
7 transmitting the encrypted second biometric template parts to the plurality
8 of worker nodes.

1 8. The authentication node of claim 6, wherein the method further
2 comprises:
3 encrypting the second biometric template resulting in an encrypted second
4 biometric template; and
5 transmitting the encrypted second biometric template to the plurality of
6 worker nodes, wherein the plurality of worker nodes derive the encrypted second
7 biometric template parts.

1 9. The authentication node of claim 6, wherein the step of
2 determining, if the first biometric template matches the second biometric template the
3 plurality of decrypted match values, further comprises:
4 determining a weight associated with each decrypted match value of the
5 plurality of decrypted match values;
6 determining an overall authentication threshold;
7 comparing a number of worker nodes that responded to a number of
8 needed responses; and
9 determining if an overall decision based on the weights and the decrypted
10 match values is greater than or equal to the overall authentication threshold.

1 10. The authentication node of claim 6, wherein the method further
2 comprises:
3 transmitting if the first biometric template matches the second biometric
4 template, an authorization request message to an authorizing entity computer; and
5 receiving an authorization response message from the authorizing entity
6 computer.

1 11. A method comprising:
2 storing, by a worker node, an encrypted first biometric template part;
3 comparing, by the worker node, the encrypted first biometric template part
4 and an encrypted second biometric template part resulting in an encrypted match value;
5 and
6 transmitting, by the worker node, the encrypted match value to an
7 authentication node.

1 12. The method of claim 11 further comprising:
2 receiving, by the worker node, an encrypted first biometric template,
3 wherein an enrollment node encrypts a first biometric template resulting in the
4 encrypted first biometric template; and
5 deriving, by the worker node, from the encrypted first biometric template
6 the encrypted first biometric template part.

1 13. The method of claim 11 further comprising:
2 receiving, by the worker node, the encrypted first biometric template part
3 from an enrollment node, wherein the enrollment node divides a first biometric template
4 resulting in first biometric template parts, and wherein the enrollment node encrypts the
5 first biometric template parts.

6 14. The method of claim 11 further comprising:

7 receiving, by the worker node, an encrypted second biometric template,
8 wherein an authentication node encrypts a second biometric template resulting in the
9 encrypted second biometric template; and
10 deriving, by the worker node, from the encrypted second biometric
11 template the encrypted second biometric template part.

1 15. The method of claim 11 further comprising:
2 receiving, by the worker node, the encrypted second biometric template
3 part from an authentication node, wherein the authentication node divides a second
4 biometric template resulting in second biometric template parts, and wherein the
5 authentication node encrypts the second biometric template parts.

1 16. A worker node comprising:
2 a processor;
3 a memory device; and
4 a computer-readable medium coupled to the processor, the computer-
5 readable medium comprising code executable by the processor for implementing a
6 method comprising:
7 storing an encrypted first biometric template part;
8 comparing the encrypted first biometric template part and an encrypted
9 second biometric template part resulting in an encrypted match value; and
10 transmitting the encrypted match value to an authentication node.

11 17. The worker node of claim 16, wherein the method further
12 comprises:
13 receiving an encrypted first biometric template, wherein an enrollment
14 node encrypts a first biometric template resulting in the encrypted first biometric
15 template; and
16 deriving from the encrypted first biometric template the encrypted first
17 biometric template part.

1 18. The worker node of claim 16, wherein the method further
2 comprises:
3 receiving the encrypted first biometric template part from an enrollment
4 node, wherein the enrollment node divides a first biometric template resulting in first
5 biometric template parts, and wherein the enrollment node encrypts the first biometric
6 template parts.

1 19. The worker node of claim 16, wherein the method further
2 comprises:
3 receiving an encrypted second biometric template, wherein an
4 authentication node encrypts a second biometric template resulting in the encrypted
5 second biometric template; and
6 deriving from the encrypted second biometric template the encrypted
7 second biometric template part.

1 20. The worker node of claim 16, wherein the method further
2 comprises:
3 receiving the encrypted second biometric template part from an
4 authentication node, wherein the authentication node divides a second biometric
5 template resulting in second biometric template parts, and wherein the authentication
6 node encrypts the second biometric template parts.