

WHAT IS CLAIMED IS:

- 1 1. A method comprising:
2 receiving, by a first server computer, authentication data for a user from a
3 user device;
4 determining, by the first server computer, a biometric identifier to be
5 associated with the authentication data;
6 transmitting, by the first server computer, the biometric identifier to a
7 second server computer along with a first encrypted biometric template associated with
8 the user, wherein the second server computer subsequently receives a second
9 encrypted biometric template and the biometric identifier from the user device, and
10 generates an encrypted match value data file by comparing the first encrypted biometric
11 template and the second encrypted biometric template;
12 receiving, by the first server computer, the encrypted match value data
13 file;
14 decrypting, by the first server computer, the encrypted match value data
15 file to determine an decrypted match value data file; and
16 determining, from the decrypted match value data file, a match likelihood
17 value.
- 1 2. The method of claim 1, wherein the first server computer is an
2 enrollment server computer and the second server computer is a match server
3 computer.
- 1 3. The method of claim 1, wherein the second encrypted biometric
2 template is received by the second server in relation to a transaction to be completed by
3 the user.
- 1 4. The method of claim 1, wherein the match likelihood value
2 represents a likelihood that the first encrypted biometric template and the second
3 encrypted biometric template are generated from the same user.
- 1 5. The method of claim 1, wherein the match likelihood value is
2 represented as a numeric value.

1 6. The method of claim 1, further comprising comparing the match
2 likelihood value to an acceptable risk threshold value to determine whether the user is
3 authenticated.

1 7. The method of claim 1, wherein each of the first encrypted
2 biometric template and the second encrypted biometric template are encrypted using a
3 public key associated with the first server computer.

1 8. The method of claim 7, wherein the match value data file is
2 decrypted using a private key associated with the first server computer.

1 9. The method of claim 1, further comprising transmitting, by the first
2 server computer, the biometric identifier to the user device.

1 10. The method of claim 1, further comprising providing an indication to
2 the second server computer as to whether or not the first encrypted biometric template
3 and the second encrypted biometric template based on the match likelihood value.

1 11. A server computer comprising:
2 a processor; and
3 a non-transitory computer-readable storage medium having code
4 embodied thereon, the code being configured to cause the processor to:
5 receive authentication data for a user from a user device;
6 determine a biometric identifier to be associated with the
7 authentication data;
8 transmit the biometric identifier to a second server computer along
9 with a first encrypted biometric template associated with the user, wherein the
10 second server computer subsequently receives a second encrypted biometric
11 template and the biometric identifier from the user device, and generates an
12 encrypted match value data file by comparing the first encrypted biometric
13 template and the second encrypted biometric template;
14 receive the encrypted match value data file;
15 decrypt the encrypted match value data file to determine an
16 decrypted match value data file; and
17 determine, from the decrypted match value data file, a match
18 likelihood value.

1 12. The method of claim 1, wherein the second server computer is
2 prevented from accessing plaintext data within the first encrypted biometric template.

1 13. The method of claim 1, wherein the first encrypted biometric
2 template and the second encrypted biometric template are both encrypted using a
3 public key associate with the server computer and using the same encryption technique.

1 14. The method of claim 13, wherein the encryption technique
2 comprises a homomorphic encryption technique.

1 15. The method of claim 1, wherein the encrypted match value data file
2 comprises an indication of a similarity between the first encrypted biometric template
3 and the second encrypted biometric template.

1 16. The method of claim 15, wherein the decrypted match value data
2 file comprises an indication of a similarity between a first decrypted biometric template
3 and a second decrypted biometric template.

1 17. The method of claim 16, wherein the match likelihood value is
2 determined based on the indicated similarity.

1 18. The method of claim 1, wherein the biometric identifier is
2 transmitted to the second server computer via a secure channel.

1 19. A method comprising:
2 receiving, at a match server from a service provider computer, a number
3 of encrypted biometric templates;
4 receiving, by the match server from an access device, an encrypted
5 authentication biometric template associated with a transaction;
6 generating, by the match server, a number of encrypted match result data
7 files by comparing the encrypted authentication biometric template to each of the
8 number of encrypted biometric templates;
9 identifying, from the number of encrypted match result data files, a closest
10 match; and
11 initiating the transaction using account information associated with the
12 closest match.

13 20. A computing device comprising:
14 a processor; and
15 a non-transitory computer-readable storage medium having code
16 embodied thereon, the code being configured to cause the processor to:
17 receive, from a service provider computer, a number of encrypted
18 biometric templates;
19 receive, from an access device, an encrypted authentication
20 biometric template associated with a transaction;
21 generate a number of encrypted match result data files by
22 comparing the encrypted authentication biometric template to each of the number
23 of encrypted biometric templates;
24 identify, from the number of encrypted match result data files, a
25 closest match; and
26 initiate the transaction using account information associated with
27 the closest match.