WHAT IS CLAIMED IS:

1. A method comprising:

receiving, by a first server computer, authentication data for a user from a user device;

determining, by the first server computer, a biometric identifier to be associated with the authentication data;

transmitting, by the first server computer, the biometric identifier to a second server computer along with a first encrypted biometric template associated with the user, wherein the second server computer subsequently receives a second encrypted biometric template and the biometric identifier from the user device, and generates an encrypted match value data file by comparing the first encrypted biometric template and the second encrypted biometric template;

receiving, by the first server computer, the encrypted match value data file;

decrypting, by the first server computer, the encrypted match value data file to determine a decrypted match value data file; and

determining, from the decrypted match value data file, a match likelihood value.

2. The method of claim 1, wherein the first server computer is an enrollment server computer and the second server computer is a match server computer.

3. The method of claim 1, wherein the second encrypted biometric template is received by the second server computer in relation to a transaction to be completed by the user.

4. The method of claim 1, wherein the match likelihood value represents a likelihood that the first encrypted biometric template and the second encrypted biometric template are generated from the same user.

5. The method of claim 1, wherein the match likelihood value is represented as a numeric value.

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

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

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

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

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

11. A server computer comprising:

a processor; and

a non-transitory computer-readable storage medium having code embodied thereon, the code being configured to cause the processor to:

receive authentication data for a user from a user device;

determine a biometric identifier to be associated with the authentication data;

transmit the biometric identifier to a second server computer along with a first encrypted biometric template associated with the user, wherein the second server computer subsequently receives a second encrypted biometric template and the biometric identifier from the user device, and generates an encrypted match value data file by comparing the first encrypted biometric template and the second encrypted biometric template;

receive the encrypted match value data file;

decrypt the encrypted match value data file to determine a decrypted match value data file; and

determine, from the decrypted match value data file, a match likelihood value.

12. The server computer of claim 11, wherein the second server computer is prevented from accessing plaintext data within the first encrypted biometric template.

13. The server computer of claim 11, wherein the first encrypted biometric template and the second encrypted biometric template are both encrypted using a public key associate with the server computer and using the same encryption technique.

14. The server computer of claim 13, wherein the same encryption technique comprises a homomorphic encryption technique.

15. The server computer of claim 11, wherein the encrypted match value data file comprises an indication of a similarity between the first encrypted biometric template and the second encrypted biometric template.

16. The server computer of claim 15, wherein the decrypted match value data file comprises the indication of a similarity between a first decrypted biometric template and a second decrypted biometric template.

17. The server computer of claim 16, wherein the match likelihood value is determined based on the indicated similarity.

18. The server computer of claim 11, wherein the biometric identifier is transmitted to the second server computer via a secure channel.

19. A method comprising:

receiving, at a match server from a service provider computer, a plurality of encrypted enrollment biometric templates;

receiving, by the match server from an access device, an encrypted authentication biometric template and a biometric identifier in a transaction;

determining, using the biometric identifier, an encrypted enrollment biometric template from the plurality of encrypted enrollment biometric templates;

generating, by the match server, an encrypted match result data file by comparing the encrypted authentication biometric template to the encrypted biometric enrollment template;

decrypting the encrypted match result data file to determine a match result;

determining if the match result exceeds a threshold; and

initiating the transaction using account information associated with the biometric identifier.

20. A computing device comprising:

a processor; and

a non-transitory computer-readable storage medium having code embodied thereon, the code being configured to cause the processor to:

receive, from a service provider computer, a plurality of encrypted enrollment biometric templates;

receive, from an access device, an encrypted authentication biometric template and a biometric identifier in a transaction;

determine, using the biometric identifier, an encrypted enrollment biometric template from the plurality of encrypted enrollment biometric templates;

generate an encrypted match result data file by comparing the encrypted authentication biometric template to the encrypted biometric enrollment template;

decrypt the encrypted match result data file to determine a match result;

determine if the match result exceeds a threshold; and

initiate the transaction using account information associated with the biometric identifier.