WHAT IS CLAIMED IS:

1. A computer-implemented method, comprising:

performing an enrollment process using an authentication application executed on a mobile device of a user by:

initiating the enrollment process for enrolling the user in an authentication program;

capturing a biometric enrollment sample of the user using the mobile device;

generating a biometric enrollment template using the biometric enrollment sample of the user; and

storing the biometric enrollment template locally or at an authentication computer; and

receiving, by a resource provider application executing on the mobile device of the user, a selection for conducting a transaction that triggers an authentication process, wherein the resource provider application is a merchant application;

performing the authentication process using the resource provider application executing on the mobile device of the user by:

obtaining a biometric authentication sample captured by the mobile device;

generating a biometric authentication template of the user from the biometric authentication sample;

retrieving the biometric enrollment template from the authentication application or the authentication computer;

authenticating the user of the mobile device based on the biometric authentication template without retrieving the biometric enrollment sample of the user, authenticating including:

generating, by the resource provider application, a first cryptographic key and a public value from the biometric authentication template and a first function,

generating, by the resource provider application, a second cryptographic key from the biometric enrollment template, the public value, and a second function, and

using, by the resource provider application, the first and second cryptographic keys to authenticate the user by comparing the first cryptographic key representing the biometric authentication template to the second cryptographic key representing the biometric enrollment template; and

executing at least one operation in response to the user being authenticated.

2. The computer-implemented method of claim 1, further comprising:

confirming that the biometric enrollment template of the user is managed by the authentication computer; and

retrieving the biometric enrollment template from the authentication computer, wherein the biometric enrollment template is transmitted to the authentication computer after being previously generated at the mobile device, wherein the biometric enrollment template is stored in an encrypted format partially or entirely at the authentication computer.

3. The computer-implemented method of claim 1, comprising:

associating, by the authentication application, the biometric enrollment template of the user to at least one of: a user identifier or an identifier managed by the authentication computer; and

storing, by the authentication application, the biometric enrollment template.

4. The computer-implemented method of claim 1, further comprising:

sending, by the resource provider application, a user identifier to an authentication gateway computer; and

receiving, by the resource provider application, user enrollment information from the authentication gateway computer, the user enrollment information comprising an indication of enrollment and one or more identifiers managed by the authentication computer.

5. The computer-implemented method of claim 1, wherein the at least one operation comprises delivering access to a resource provided by a resource provider based on the user being authenticated.

6. A user device comprising:

one or more biometric capture devices;

one or more processors; and

one or more memories storing a resource provider application, an authentication application, and computer-executable instructions, wherein executing the computer-executable instructions by the one or more processors causes the user device to:

perform an enrollment process using the authentication application executed on the user device of a user by:

initiating the enrollment process for enrolling the user in an authentication program;

capturing a biometric enrollment sample of the user using the user device;

generating a biometric enrollment template using the biometric enrollment sample of the user; and

storing the biometric enrollment template locally or at an authentication computer; and

receiving, by the resource provider application executing on the user device of the user, a selection for conducting a transaction that triggers an authentication process, wherein the resource provider application is a merchant application;

perform the authentication process using the resource provider application executing on the user device of the user by:

obtaining a biometric authentication sample captured by the user device;

generating a biometric authentication template of the user from the biometric authentication sample;

retrieving the biometric enrollment template from the authentication application or the authentication computer;

authenticating the user of the user device based on the biometric authentication template without retrieving the biometric enrollment sample of the user, authenticating including:

generating a first cryptographic key and a public value from the biometric authentication template and a first function,

generating a second cryptographic key from the biometric enrollment template, the public value, and a second function, and

using the first and second cryptographic keys to authenticate the user by comparing the first cryptographic key representing the biometric authentication template to the second cryptographic key representing the biometric enrollment template; and

execute at least one operation in response to the user being authenticated.

7. The user device of claim 6, wherein executing the computer-executable instructions by the one or more processors further causes the user device to:

confirming that the biometric enrollment template of the user is managed by the authentication computer; and

retrieving the biometric enrollment template from the authentication computer, wherein the biometric enrollment template is transmitted to the authentication computer after being previously generated at the user device, wherein the biometric enrollment template is stored in an encrypted format partially or entirely at the authentication computer.

8. The user device of claim 6, wherein the one or more processors further cause the user device to:

associate, by the authentication application, the biometric enrollment template of the user to at least one of: a user identifier or an identifier managed by the authentication computer; and

store, by the authentication application, the biometric enrollment template.

9. The user device of claim 6, wherein the one or more processors further cause the user device to:

send, by the resource provider application, a user identifier to an authentication gateway computer; and

receive, by the resource provider application, user enrollment information from the authentication gateway computer, the user enrollment information comprising an indication of enrollment and one or more identifiers managed by the authentication computer.

10. The user device of claim 6, wherein the at least one operation comprises delivering access to a resource provided by a resource provider based on the user being authenticated.

11. A computer-implemented method, comprising:

performing an enrollment process using an authentication application executed on a mobile device of a user by:

initiating the enrollment process for enrolling the user in an authentication program;

capturing a biometric enrollment sample of the user using the mobile device;

generating a biometric enrollment template using the biometric enrollment sample of the user; and

storing the biometric enrollment template locally or at an authentication computer; and

performing an authentication process using a resource provider application executing on the mobile device of the user by:

obtaining a biometric authentication sample captured by the mobile device;

generating a biometric authentication template of the user from the biometric authentication sample;

authenticating the user of the mobile device based on the biometric authentication template without retrieving the biometric enrollment sample of the user, authenticating including:

receiving an obfuscated circuit and information about the obfuscated circuit;

generating an obfuscated authentication result using the biometric authentication template, the obfuscated circuit, and the information about the obfuscated circuit;

providing, by the resource provider application, the obfuscated authentication result to an obfuscated matching circuit, wherein the obfuscated matching circuit determines a match result between the

obfuscated authentication result and an obfuscated enrollment result generated using the obfuscating circuit and the biometric enrollment template, wherein the biometric enrollment template is previously generated at the mobile device using a previously obtained biometric enrollment sample of the user captured using the mobile device;

receiving a notification of the match result; and

executing at least one operation in response to the user being authenticated.

12. The method of claim 1, wherein the biometric enrollment template is stored locally, and the biometric enrollment template is retrieved from the authentication application.

13. The user device of claim 6, wherein the biometric enrollment template is stored locally, and the biometric enrollment template is retrieved from the authentication application.

14. The computer-implemented method of claim 1, wherein the authenticating further includes:

sending, by the resource provider application, to the authentication application or the authentication computer, an encrypted match result based on comparing the first cryptographic key to the second cryptographic key, wherein the authentication application or the authentication computer decrypts the encrypted match result; and

receiving, by the resource provider application, from the authentication application or the authentication computer, a notification of a decrypted match result.

15. The computer-implemented method of claim 14, wherein a digital signature is received along with the notification.

16. The computer-implemented method of claim 1, wherein executing the at least one operation in response to the user being authenticated includes accessing a resource.

17. The computer-implemented method of claim 1, wherein executing the at least one operation in response to the user being authenticated includes processing the transaction.

18. The computer-implemented method of claim 1, wherein executing the at least one operation in response to the user being authenticated includes receiving a credential from the authentication application, wherein the authentication application is a digital wallet application.

19. The computer-implemented method of claim 18, wherein executing the at least one operation in response to the user being authenticated includes transmitting the credential for the transaction.