WHAT IS CLAIMED IS:

1. A method comprising:

receiving, by a public device, from a user, a request to perform an interaction with a resource provider;

collecting, by the public device, from the user, a first biometric template corresponding to the user;

unlocking, by the public device, a data vault using the first biometric template, wherein the data vault comprises access data locked using a second biometric template corresponding to the user;

transmitting, by the public device, the access data to the resource provider; and

performing, by the public device, the interaction with the resource provider,

wherein the access data comprises an interaction token or a master secret key, wherein the data vault comprises a plurality of random points and a plurality of biometric points, the plurality of biometric points corresponding to the second biometric template and an encoding function, wherein the encoding function is derived from the access data, and

wherein unlocking the data vault comprises:

determining, by the public device, a subset of the plurality of biometric points corresponding to the first biometric template;

determining, by the public device, the encoding function based on the subset of the plurality of biometric points; and

determining, by the public device, the access data based on the encoding function.

2. The method of claim 1, wherein the second biometric template is an enrollment template, and the first biometric template is an authentication template, and wherein the method further comprises:

receiving, by the public device, from a communication device associated with the user, a delegation request message;

transmitting, by the public device, to an authentication server computer, a validation request message; and

receiving, by the public device, from the communication device, the data vault.

3. The method of claim 2, further comprising:

receiving, by the public device, a subsequent data vault from the communication device, the subsequent data vault comprising subsequent access data locked using the second biometric template or a subsequent biometric template corresponding to the user; and

replacing, by the public device, the data vault with the subsequent data vault.

4. The method of claim 1, wherein:

the encoding function comprises a polynomial comprising one or more polynomial coefficients derived from the access data;

determining, by the public device, the encoding function based on the subset of the plurality of biometric points comprises interpolating the polynomial, by the public device, based on the subset of the plurality of biometric points; and

determining, by the public device, the access data based on the encoding function comprises determining, by the public device, the access data based on the one or more polynomial coefficients.

5. The method of claim 1, wherein the data vault was formed using a fuzzy vault scheme, and wherein the method further comprises:

storing, by the public device, the first biometric template;

storing, by the public device, the access data; and

after transmitting, by the public device, the access data to the resource provider, deleting, by the public device, the first biometric template and the access data.

6. The method of claim 1, wherein the method further comprises:

storing, by the public device, the data vault;

receiving, by the public device, a revocation message; and

in response to receiving the revocation message, deleting, by the public device, the data vault.

7. The method of claim 1, wherein the first biometric template and the second biometric template comprise data based on one or more of the following: a fingerprint scan, a face scan, an iris scan, a retina scan, a DNA sample, a hand-written signature, and/or a voice recording.

8. A public device comprising:

a processor; and

a non-transitory computer readable medium coupled to the processor, the non-transitory computer readable medium comprising code, when executed by the processor implements a method comprising:

receiving from a user, a request to perform an interaction with a resource provider;

collecting from the user, a first biometric template corresponding to the user;

unlocking a data vault using the first biometric template, wherein the data vault comprises access data locked using a second biometric template corresponding to the user;

transmitting the access data to the resource provider; and

performing the interaction with the resource provider,

wherein the data vault comprises a plurality of random points and a plurality of biometric points, the plurality of biometric points corresponding to the second biometric template and an encoding function, wherein the encoding function is derived from the access data, and

wherein unlocking the data vault comprises:

determining a subset of the plurality of biometric points corresponding to the first biometric template;

determining the encoding function based on the subset of the plurality of biometric points; and

determining the access data based on the encoding function.

9. The public device of claim 8, wherein the method further comprises:

receiving from a communication device associated with the user, a delegation request message;

transmitting to an authentication server computer, a validation request message; and

receiving from the communication device, the data vault.

10. The public device of claim 9, wherein the method further comprises:

receiving a subsequent data vault from the communication device, the subsequent data vault comprising subsequent access data locked using the second biometric template or a subsequent biometric template corresponding to the user; and

replacing the data vault with the subsequent data vault, and

wherein the data vault and the subsequent data vault were formed using a fuzzy vault scheme.

11. The public device of claim 8, wherein:

the encoding function comprises a polynomial comprising one or more polynomial coefficients derived from the access data;

determining the encoding function based on the subset of the plurality of biometric points comprises interpolating the polynomial based on the subset of the plurality of biometric points; and

determining the access data based on the encoding function comprises determining the access data based on the one or more polynomial coefficients.

12. The public device of claim 8, wherein the method further comprises:

storing the first biometric template;

storing the access data; and

after transmitting the access data to the resource provider, deleting the first biometric template and the access data.

13. The public device of claim 8, wherein the method further comprises:

storing the data vault;

receiving a revocation message; and

in response to receiving the revocation message, deleting the data vault.

14. The public device of claim 8, wherein the first biometric template and the second biometric template comprise data based on one or more of the following: a fingerprint scan, a face scan, an iris scan, a retina scan, a DNA sample, a hand-written signature, and/or a voice recording.

15. A method comprising:

receiving, by a communication device associated with a user, from an authentication server computer or a token server computer, access data;

generating, by the communication device, a data vault by locking the access data using a biometric template corresponding to the user; and

transmitting, by the communication device, the data vault to a public device, wherein the data vault comprises a plurality of biometric points and a plurality of random points, and wherein generating, by the communication device, the data vault by locking the access data using the biometric template corresponding to the user comprises:

generating, by the communication device, an encoding function corresponding to the access data;

generating, by the communication device, the plurality of biometric points by applying the biometric template as an input to the encoding function; and

generating, by the communication device, the plurality of random points.

16. The method of claim 15, further comprising:

generating, by the communication device associated with the user, a revocation message; and

transmitting, by the communication device, the revocation message to the public device, wherein the public device subsequently deletes the data vault.

17. The method of claim 15, wherein the method further comprises:

transmitting, by the communication device associated with the user, to the public device, a delegation request message;

receiving, by the communication device, from the authentication server computer, a delegation confirmation message; and

transmitting, by the communication device, to a biometric server computer, a delegation confirmation response.