

WHAT IS CLAIMED IS:

1 1. A method comprising:
2 receiving, by a public device, from a user, a request to perform an
3 interaction with a resource provider;
4 collecting, by the public device, from the user, a first biometric template
5 corresponding to the user;
6 unlocking, by the public device, a data vault using the first biometric
7 template, wherein the data vault comprises access data locked using a second
8 biometric template corresponding to the user;
9 transmitting, by the public device, the access data to the resource
10 provider; and
11 performing, by the public device, the interaction with the resource
12 provider.

1 2. The method of claim 1, wherein the second biometric template is
2 an enrollment template, and the first biometric template is an authentication
3 template, and wherein the method further comprises:
4 receiving, by the public device, from a communication device
5 associated with the user, a delegation request message;
6 transmitting, by the public device, to an authentication server computer,
7 a validation request message; and
8 receiving, by the public device, from the communication device, the
9 data vault.

1 3. The method of claim 2, further comprising:
2 receiving, by the public device, a subsequent data vault from the
3 communication device, the subsequent data vault comprising subsequent access
4 data locked using the second biometric template or a subsequent biometric template
5 corresponding to the user; and
6 replacing, by the public device, the data vault with the subsequent data
7 vault.

1 4. The method of claim 1, wherein the access data comprises an
2 interaction token or a master secret key, wherein the data vault comprises a plurality

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

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

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

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

1 5. The method of claim 4, wherein:

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

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

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

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

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

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

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

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

2 storing, by the public device, the data vault;

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

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

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

1 9. A public device comprising:
2 a processor; and
3 a non-transitory computer readable medium coupled to the processor,
4 the non-transitory computer readable medium comprising code, executable by the
5 processor for implementing a method comprising:
6 receiving from a user, a request to perform an interaction with a
7 resource provider;
8 collecting from the user, a first biometric template corresponding to the
9 user;
10 unlocking a data vault using the first biometric template, wherein the
11 data vault comprises access data locked using a second biometric template
12 corresponding to the user;
13 transmitting the access data to the resource provider; and
14 performing the interaction with the resource provider.

1 10. The public device of claim 9, wherein the method further
2 comprises:
3 receiving from a communication device associated with the user, a
4 delegation request message;
5 transmitting to an authentication server computer, a validation request
6 message; and
7 receiving from the communication device, the data vault.

1 11. The public device of claim 10, wherein the method further
2 comprises:
3 receiving a subsequent data vault from the communication device, the
4 subsequent data vault comprising subsequent access data locked using the second
5 biometric template or a subsequent biometric template corresponding to the user;
6 and

7 replacing the data vault with the subsequent data vault, and
8 wherein the data vault and the subsequent data vault were formed
9 using a fuzzy vault scheme.

1 12. The public device of claim 9, wherein the data vault comprises a
2 plurality of random points and a plurality of biometric points, the plurality of biometric
3 points corresponding to the second biometric template and an encoding function,
4 wherein the encoding function is derived from the access data, and wherein
5 unlocking the data vault comprises:
6 determining a subset of the plurality of biometric points corresponding
7 to the first biometric template;
8 determining the encoding function based on the subset of the plurality
9 of biometric points; and
10 determining the access data based on the encoding function.

1 13. The public device of claim 12, wherein:
2 the encoding function comprises a polynomial comprising one or more
3 polynomial coefficients derived from the access data;
4 determining the encoding function based on the subset of the plurality
5 of biometric points comprises interpolating the polynomial based on the subset of the
6 plurality of biometric points; and
7 determining the access data based on the encoding function comprises
8 determining the access data based on the one or more polynomial coefficients.

1 14. The public device of claim 9, wherein the method further
2 comprises:
3 storing the first biometric template;
4 storing the access data; and
5 after transmitting the access data to the resource provider, deleting the
6 first biometric template and the access data.

1 15. The public device of claim 9, wherein the method further
2 comprises:
3 storing the data vault;
4 receiving a revocation message; and

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

1 16. The public device of claim 9, wherein the first biometric template
2 and the second biometric template comprise data based on one or more of the
3 following: a fingerprint scan, a face scan, an iris scan, a retina scan, a DNA sample,
4 a hand-written signature, and/or a voice recording.

1 17. A method comprising:
2 receiving, by a communication device associated with a user, from an
3 authentication server computer or a token server computer, access data;
4 generating, by the communication device, a data vault by locking the
5 access data using a biometric template corresponding to the user; and
6 transmitting, by the communication device, the data vault to a public
7 device.

1 18. The method of claim 17, further comprising:
2 generating, by the communication device associated with the user, a
3 revocation message; and
4 transmitting, by the communication device, the revocation message to
5 the public device, wherein the public device subsequently deletes the data vault.

1 19. The method of claim 17, wherein the data vault comprises a
2 plurality of biometric points and a plurality of random points, and wherein generating,
3 by the communication device, the data vault by locking the access data using the
4 biometric template corresponding to the user comprises:
5 generating, by the communication device, an encoding function
6 corresponding to the access data;
7 generating, by the communication device, the plurality of biometric
8 points by applying the biometric template as an input to the encoding function; and
9 generating, by the communication device, the plurality of random
10 points.

1 20. The method of claim 19, wherein the method further comprises:

- 2 transmitting, by the communication device associated with the user, to
- 3 the public device, a delegation request message;
- 4 receiving, by the communication device, from the authentication server
- 5 computer, a delegation confirmation message; and
- 6 transmitting, by the communication device, to a biometric server
- 7 computer, a delegation confirmation response.