CLAIMS

1. A data access control system, comprising:

a server comprising a processor and a memory,

wherein the server is in data communication with a database and a client device, and

wherein the server is configured to:

receive, from the client device, a user token, a service provider token, and a request for a data access key to decrypt encrypted personal user data,

identify a user based on the user token,

identify a service provider based on the service provider token,

verify the service provider is authorized to receive access to the personal user data,

retrieve the user key from the database,

generate the data access key based on the user key, and

transmit the data access key to the client device.

2. The data control access system of claim 1, further comprising:

a contactless card associated with the user, the contactless card comprising a processor, a memory, and a communications interface,

wherein the memory of the contactless card stores the user token and the encrypted personal user data associated with the user.

3. The data access control system of claim 2, wherein the request for the data access key is generated in response to a tap action between the contactless card and the client device.

4. The data control access system of claim 2, wherein the memory of the contactless card stores basic user data associated with the user, the basic user data encrypted with a basic service provider key.

5. The data control access system of claim 4, wherein the server is further configured to generate the basic service provider key based on the identity of the service provider.

6. The data access control system of claim 5, wherein the server is further configured to:

receive a request for the basic service provider key,

verify that the service provider is authorized to receive the basic service provider key, and

transmit, to the client device, the basic service provider key.

7. The data access control system of claim 6, wherein the basic service provider key is valid only for a predetermined period of time.

8. The data access control system of claim 7, wherein the server receives the request for the basic service provider key after expiration of the predetermined period of time.

9. The data access control system of claim 7, wherein the request for the basic service provider key is independent of a tap action between the contactless card on the client device.

10. The data access control system of claim 6, wherein, after a verification that the service provider is not authorized to receive the basic service provider key, the server is further configured to transmit a denial notification to the client device.

11. A method for controlling data access, comprising:

receiving, from a first client device, a user token, a service provider token, and a request for a data access key to decrypt encrypted personal user data stored on a contactless card associated with a user;

identifying the user based on the user token;

identifying a service provider based on the service provider token;

verifying that the service provider is authorized to receive access to the personal user data stored on the contactless card;

retrieving a user key associated with the user from a database;

generating the data access key based on the user key; and

transmitting the data access key to the first client device.

12. The method for controlling data access of claim 11, further comprising authenticating the user based on the user key.

13. The method for controlling data access of claim 11, wherein the request for the data access key is generated in response to a tap action between the contactless card and the first client device.

14. The method for controlling data access of claim 11, further comprising:

retrieving a first service provider key associated with the service provider from the database,

wherein the data access key is generated based on the user key and the first service provider key.

15. The method for controlling data access of claim 14, further comprising:

receiving, from a second client device, a second service provider key,

wherein the data access key is generated based on the user key, the first service provider key, and the second service provider key.

16. The method for controlling data access of claim 15, wherein the second service provider key is transmitted by the second client device in response to a tap action between the contactless card and the second client device.

17. The method for controlling data access of claim 11, wherein:

the service provider token comprises a first service provider key, and

the method further comprises authenticating the service provider based on the first service provider key.

18. A server, comprising:

a processor; and

a memory,

wherein the server is in data communication with a database and a client device, and wherein the server is configured to:

receive, from the client device, a user token, a service provider token, and a request for a data access key to decrypt encrypted personal user data,

identify a user based on the user token,

identify a service provider based on the service provider token,

verify the service provider is authorized to receive access to the personal user data,

retrieve the user key from the database,

generate the data access key based on the user key, and

transmit the data access key to the client device.

19. The server of claim 18, wherein the server is further configured to:

generate a basic service provider key based on the identity of the service provider,

receive a request for the basic service provider key,

verify that the service provider is authorized to receive the basic service provider key, and

transmit, to the client device, the basic service provider key.

20. The server of claim 19, wherein the server is further configured to log each transmission of the basic service provider key.