CLAIMS

What is claimed is:

1. A data access control system, comprising:

a database storing information comprising a user identifier and a user key associated with a user, and a service provider identifier and a service provider key associated with a service provider;

a server configured for data communication with a client device associated with the service provider via a network;

a contactless card associated with the user, the contactless card comprising a communications interface, a processor, and a memory, the memory storing an applet, a user token, and personal user data associated with the user, wherein the personal user data is encrypted using the user key;

a client application comprising instructions for execution on the client device, the client application configured to:

in response to a tap action between the contactless card and the client device: receive the user token from the contactless card, and transmit to the server a service provider token, the user token, and a request for a data access key, wherein the service provider token is associated with the service provider;

receive from the server the data access key;

receive from the contactless card the encrypted personal user data; and

using the data access key, decrypt the encrypted personal user data; and,

~~a processor in data communication with the server and the database, the processor configured to:~~

~~receive from the client device the service provider token, the user token, and the request for the data access key;~~

~~identify the service provider based on the service provider token;~~

~~identify the user based on the user token;~~

~~verify that 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 from the user key; and~~

~~transmit to the client device the data access key.~~

~~2. The data access control system of claim 1, wherein the user token comprises the user key, and the processor is further configured to authenticate the user based on the user key.~~

~~3. The data access control system of claim 1, wherein the service provider token comprises the service provider key, and the processor is further configured to authenticate the service provider based on the service provider key.~~

~~4. The data access control system of claim 1, wherein:~~

~~the service provider token comprises the service provider key; and~~

~~the data access key is generated from the user key and the service provider key.~~

~~5. The data access control system of claim 1, wherein the client application is further configured to display the decrypted personal user data on the client device.~~

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

~~store the data access key on the client device; and~~

~~only display the decrypted personal user data on the client device if the data access key remains stored on the client device.~~

~~7. The data access control system of claim 1, wherein:~~

~~the memory of the contactless card further stores basic user data associated with the user, the basic user data encrypted with a basic service provider key; and~~

~~the client application is further configured to:~~

~~receive from the contactless card the encrypted basic user data; and~~

~~using the basic service provider key, decrypt the encrypted basic user data.~~

~~8. The data access control system of claim 7, wherein the client application is further configured to:~~

~~receive from the server the basic service provider key; and~~

~~store the basic service provider key in a memory of the client device.~~

~~9. The data access control system of claim 8, wherein:~~

~~the client application is further configured to transmit to the server a request for the basic service provider key, the request for the basic service provider key being independent of the tap action between the contactless card and the client device; and~~

~~the processor is further configured to:~~

~~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.~~

~~10. The data access control system of claim 9, wherein the basic service provider key is valid only for a predetermined period of time.~~

~~11. A method for controlling data access, comprising:~~

~~establishing a database storing information comprising a user identifier and a user key associated with a user, and a service provider identifier and a first service provider key associated with a service provider;~~

~~receiving from a first client device associated with the service provider, via a network, a service provider token and a request for a data access key to access personal user data stored on a contactless card associated with the user, the personal user data encrypted using the user key, the request generated in response to a tap action between the contactless card and the first client device, the request accompanied by a user token stored on the contactless card;~~

~~identifying the service provider based on the service provider token;~~

~~identifying the user based on the user token;~~

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

~~retrieving the user key from the database;~~

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

~~transmitting to the first client device the data access key.~~

~~12. The method of claim 11, wherein the user token includes the user key, the method further comprising authenticating the user based on the user key.~~

~~13. The method of claim 11, wherein the service provider token comprises the first service provider key, the method further comprising authenticating the service provider based on the first service provider key.~~

~~14. The method of claim 13, wherein the data access key is generated based on the user key and the first service provider key.~~

~~15. The method of claim 13, 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 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 of claim 11, wherein the database further stores updated personal user data associated with the user, the method further comprising:~~

~~encrypting the updated personal user data using the user key; and~~

~~transmitting to the first client device the encrypted updated personal user data.~~

~~18. A method for controlling data access, comprising:~~

~~establishing a database storing information comprising a user identifier and a user key associated with a user, and a service provider identifier and a service provider key associated with a service provider;~~

~~providing a contactless card comprising a communications interface, a processor, and a memory, the memory storing an applet and a user token, wherein the communications interface is configured to support at least one of near field communication, Bluetooth, or Wi-Fi, and wherein the contactless card is associated with the user;~~

~~providing a client application comprising instructions for execution on a client device associated with the service provider, the client application configured to:~~

~~in response to a tap action between the contactless card and the client device: receive the user token from the contactless card, and transmit via a network, to a server, a service provider token, the user token, and a request for a data access key, wherein the service provider token is associated with the service provider;~~

~~receive from the server the data access key and a link to a data repository storing encrypted personal user data associated with the user, wherein the data access key is generated based on the user key;~~

~~transmit to the data repository, via the link, a request for the encrypted personal user data;~~

~~receive from the data repository the encrypted personal user data; and~~

~~using the data access key, decrypt the encrypted personal user data;~~

~~receiving from the client device, via the network, a service provider token and the request for the data access key to access the personal user data associated with the user, the request accompanied by the user token;~~

~~identifying the service provider based on the service provider token;~~

~~identifying the user based on the user token;~~

~~verifying that the service provider is authorized to receive access to the personal user data associated with the user;~~

~~generating the link to the data repository storing the encrypted personal user data;~~

~~retrieving the user key from the database;~~

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

~~transmitting to the client device the data access key and the link to the data repository storing the encrypted personal user data.~~

~~19. The method of claim 18, wherein the data access key is generated based on the user key and the service provider key.~~

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.