CLAIMS

What is claimed is:

1. A data access control system, comprising:

a server configured for data communication with a client device associated with a user;

a contactless card associated with the user, the contactless card comprising a communications interface, a processor, and a memory, the memory storing an applet and a user token, wherein the user token comprises a 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 the user token and a request for a data storage key;

receive from the server the data storage key, wherein the data storage key is generated from the user key;

create a secure memory block in a memory of the client device; and

encrypt the secure memory block using the data storage key; and

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

receive from the client device the user token and the request for the data storage key;

identify the user based on the user token;

verify that the user is authorized to create the secure memory block in the client device; and

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

~~2. The data access control system of claim 1, wherein 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 client application is further configured to store personal user data in the secure memory block.~~

~~4. The data access control system of claim 3, wherein:~~

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

~~in response a tap action between the contactless card and the client device, transmit to the server the user token and a request for a data access key;~~

~~receive from the server the data access key; and~~

~~decrypt the secure memory block using the data access key; and~~

~~the processor is further configured to:~~

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

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

~~verify that the user is authorized to access the secure memory block in the client device; and~~

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

~~5. The data access control system of claim 4, wherein the user token comprises a user key, and the data access key is generated from the user key.~~

~~6. The data access control system of claim 5, wherein the processor is further configured to authenticate the user based on the user key.~~

~~7. The data access control system of claim 4, wherein the client application is further configured to display the personal user data on the client device.~~

~~8. The data access control system of claim 4, wherein the client application is further configured to permit a second application on the client device to access the personal user data.~~

~~9. The data access control system of claim 3, wherein the user token comprises a user key, and wherein the client application is further configured to:~~

~~in response to a tap action between the contactless card and the client device, receive the user token from the contactless card;~~

~~verify that the user is authorized to access the secure memory block in the client device;~~

~~generate a data access key based on the user key; and~~

~~decrypt the secure memory block using the data access key.~~

~~10. The data access control system of claim 9, wherein the client application is further configured to display the personal user data on the client device.~~

~~11. The data access control system of claim 9, wherein the client application is further configured to permit a second application on the client device to access the personal user data.~~

~~12. A method for controlling data access, comprising:~~

~~providing a contactless card comprising a communications interface, a processor, and a memory, the memory storing an applet and a user token, the user token comprising a user key, 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 a~~

~~user;~~

~~providing a client application comprising instructions for execution on a client device associated with the user, the client device having an encrypted secure memory block storing personal user data, 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 the user token and a request for a data access key;~~

~~receive from the server the data access key, wherein the data access key is generated based on the user key; and~~

~~decrypt the secure memory block using the data access key;~~

~~receiving from the client device the user token and the request for the data access key;~~

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

~~verifying that the user is authorized to access the secure memory block in the client device; and~~

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

~~13. The method of claim 12, further comprising authenticating the user based on the user key.~~

~~14. The method of claim 12, wherein the client application is further configured to display the personal user data on the client device.~~

~~15. The method of claim 12, wherein the client application is further configured to permit a second application on the client device to access the personal user data.~~

16. The method of claim 12, wherein decrypt the secure memory block using the data access key comprises combining the data access key with data received from the contactless card to generate a new key used for performing the decryption.

17. A non-transitory machine-readable medium having stored thereon an application comprising program code for execution on a client device, the client device associated with a user, the client device configured to communicate over a short-range communication field with a contactless card associated with the user, the contactless card comprising memory storing a user token comprising a user key, the application configured to, when executed, perform procedures comprising:

in response to a tap action between the contactless card and the client device, receiving the user token from the contactless card, and transmitting to a server the user token and a request for a data storage key;

receiving from the server the data storage key, wherein the data storage key is generated from the user key;

creating a secure memory block in a memory of the client device;

storing personal user data in the secure memory block; and

encrypting the secure memory block using the data storage key.

18. The non-transitory machine-readable medium of claim 17, wherein the user token comprises a user key, and wherein the application is further configured to, when executed, perform procedures comprising:

in response to a tap action between the contactless card and the client device, receiving the user token from the contactless card;

~~verifying that the user is authorized to access the secure memory block in the client device;~~

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

~~decrypting the secure memory block using the data access key; and~~

~~providing the personal user data for display on the client device.~~

~~19. The data access control system of claim 1, wherein the communication interface is configured to support near field communication.~~

~~20. The method of claim 12, wherein the user token further comprises a user identifier.~~

1. A method for controlling data access performed by a client application comprising instructions for execution on a client device, the client device having a secure memory block storing personal user data, the method comprising:

receiving, from a contactless card, a user token;

storing personal user data in the secure memory block; and

encrypting the secure memory block using a data storage key.

2. The method for controlling data access of claim 1, further comprising:

transmitting, to a server, the user token and a request for the data storage key; and

receiving, from a server, the data storage key.

3. The method for controlling data access of claim 1, further comprising receiving, from the contactless card, the data storage key.

4. The method of claim 1, wherein:

the user token comprises a user key, and

the method further comprises generating the data storage key by encrypting a counter value using the user key.

5. The method for controlling data access of claim 1, further comprising permitting a second application on the client device to access the personal user data.

6. The method for controlling data access of claim 1, further comprising:

prior to encrypting the secure memory block, generating a new data storage key based on the data storage key and the user token; and

encrypting the secure memory block using the new data storage key.

7. The method for controlling data access of claim 1, further comprising:

receiving, from the server, a data access key; and

decrypting the secure memory block using the data access key.

8. The method for controlling data access of claim 7, further comprising re-encrypting the secure memory block after a predetermined time period.

9. The method for controlling data access of claim 7, further comprising receiving biometric information prior to decrypting the secure memory block.

10. The method for controlling data access of claim 1, wherein the user token is received from the contactless card via a tap action.

11. A system for controlling data access, comprising:

a contactless card comprising a communications interface, a processor, and a memory, the memory storing a user token; and

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

receive, from the contactless card, the user token,

transmit, to a server, the user token and a request for a data storage key,

receive, from the server, the data storage key,

create a secure memory block in a memory of the client device,

store personal user data in the secure memory block, and

encrypt the secure memory block using the data storage key.

12. The system for controlling data access of claim 11, further comprising:

the server,

wherein the server is configured to generate the data storage key from the user token.

13. The system for controlling data access of claim 12, wherein the server is further configured to verify that a user associated with the user token is authorized to access the secure memory block.

14. The system for controlling data access of claim 12, wherein:

the user token comprises a user key, and

the server is further configured to authenticate the user based on the user key.

15. The system for controlling data access of claim 12, wherein:

the server is further configured to:

encrypt a counter value with the user key to generate a data access key,

transmit the data access key to the client application, and

the client application is further configured to decrypt the secure memory block using the data access key.

16. The system for controlling data access of claim 15, wherein, the client application is further configured to:

prior to decrypting the secure memory block, generate a new data access key based on the data access key and the user token, and

decrypt the secure memory block using the new data access key.

17. The system for controlling data access of claim 16, wherein the client application is further configured to:

receive a user command, and

responsive to the user command, re-encrypt the secure memory block.

18. A non-transitory machine-readable medium having stored thereon a client application comprising program code for execution on a client device, the client device having a secure memory block storing personal user data, the client application configured to, when executed, perform procedures comprising:

receiving, from a contactless card, a user token;

receiving, from a server, a data storage key;

storing personal user data in the secure memory block; and

encrypting the secure memory block using the data storage key.

19. The non-transitory machine-readable medium of claim 18, the procedures further comprising:

receiving, from the server, a data access key;

decrypting the secure memory block using the data access key; and

re-encrypting the secure memory block after a predetermined time period.

20. The non-transitory machine-readable medium of claim 19, the procedures further comprising:

prior to decrypting the secure memory block, generating a new data access key based on the data access key and the user token, and

decrypting the secure memory block using the new data access key.