may rely on log-in credentials (e.g., username and password) to confirm a cardholder's identity. However, if the log-in credentials are compromised, another person could have access to the user's account.

[0006] Despite concerns over security, the widespread use of log-in credentials passwords to safeguard account access and critical information continues. A potential solution to this problem is proposed by the FIDO Alliance in the form of the FIDO2 project to create a FIDO authentication standard. The FIDO2 project incorporates W3C's Web Authentication specification and the FIDO Client-Authentication Protocol to permit the use of common devices to authenticate online services and control account access. The FIDO2 project provides for the authentication of a device by initiating a cryptographic challenge that is answered by an authenticator device using a private key. However, security issues remain, including difficulties in proving an authorized user is present at the outset of the device authentication process.

[0007] These and other deficiencies exist. Accordingly, there is a need to provide users with an appropriate solution that overcomes these deficiencies to provide data security, authentication, and verification for contactless cards. Further, there is a need for both an improved method of activating a card and an improved authentication for account access.

SUMMARY

[0008] Aspects of the disclosed technology include systems and methods for cryptographic authentication of contactless cards. Various embodiments describe systems and methods for implementing and managing cryptographic authentication of contactless cards.

[0008a] An aspect of the present disclosure provides a non-transitory memory storing a client application and a diversified key. The client application comprises instructions

for execution on a client device comprising a processor, a memory, and a communication interface and the client application is configured to receive a challenge from a first server, transmit a in response to the challenge, an authentication request signal to a contactless card, transmit authentication data received from the contactless card to a second server, wherein the authentication data is encrypted with the diversified key, receive, from the second server, a verification of the authentication data, wherein the verification permits the use of a Fast Identity Online (FIDO) private key, sign the challenge using the FIDO private key, and transmit the signed challenge to the first server.

[0008b] Another aspect of the present disclosure provides a method comprising receiving, by a client application comprising instructions for execution on a client device, a challenge from a first server, wherein the client device comprises a processor, a memory storing a Fast Identity Online (FIDO) private key and a FIDO public key, and a communication interface, transmitting, by the client application, an authentication request to a contactless card, transmitting, by the client application, authentication data received from the contactless card, to a second server, receiving, by the client application, a verification of the authentication data, wherein the verification permits the use of the FIDO private key, signing, by the client application, the challenge using the FIDO private key, and transmitting, by the client application, the signed challenge to the first server.

[0008c] Another aspect of the present disclosure provides a contactless card comprising a memory containing a counter, a diversified key, a Fast Identity Online (FIDO) public key, and a FIDO private key, a communication interface, and a processor in communication with the memory and communication interface. The processor is configured to update the counter when the communication interface is within a range of a communication field associated with a client device, receive, via the communication interface, a transaction verification request from the client device, create a cryptogram using the diversified key and the counter, wherein the cryptogram stores the FIDO private key, and transmit a transaction verification response to the client device, the transaction verification response including the cryptogram, wherein the transaction verification response provides the FIDO private key, in an encrypted form, to the client device in connection with a challenge.

[0009] There is also disclosed provide a client device comprising: a processor; a memory containing a FIDO public key, a FIDO private key, and account information; and a

CLAIMS

1. A non-transitory memory storing a client application and a diversified key, wherein:

the client application comprises instructions for execution on a client device comprising a processor, a memory, and a communication interface, and

the client application is configured to:

receive a challenge from a first server,

transmit, in response to the challenge, an authentication request signal to a contactless card,

transmit authentication data received from the contactless card to a second server, wherein the authentication data is encrypted with the diversified key,

receive, from the second server, a verification of the authentication data, wherein the verification permits the use of a Fast Identity Online (FIDO) private key,

sign the challenge using the FIDO private key, and

transmit the signed challenge to the first server.

2. The non-transitory memory of claim 1, wherein the client application is configured to transmit a FIDO public key to the first server.

3. The non-transitory memory of claim 1, wherein the client application stores the FIDO private key in the memory of the client device.

4. The non-transitory memory of claim 1, wherein the client application is configured to, prior to receiving the challenge from the first server, transmit a request for the challenge to the first server.

5. The non-transitory memory of claim 1, wherein the authentication data is received from the contactless card via a near field communication field generated by the communication interface.

6. The non-transitory memory of claim 1, wherein the client application is configured to receive a verification input prior to signing the challenge using the FIDO private key.

7. The non-transitory memory of claim 1, wherein:

the non-transitory memory further stores identification information and a master key, and

the application is configured to generate the diversified key using the identification information with the master key.

8. The non-transitory memory of claim 7, wherein the identification information comprises a site identifier for a website.

9. The non-transitory memory of claim 8, wherein the first server is associated with the website.

10. The non-transitory memory of claim 1, wherein:

the non-transitory memory stores a master key,

the application is configured to receive a counter from the first server, and

the application is configured to generate the diversified key using the master key and the counter.

11. The non-transitory memory of claim 1, wherein the FIDO private key is stored on the contactless card, encrypted using the diversified key and transmitted to the client application via a read of the contactless card.

12. The non-transitory memory of claim 1, wherein the challenge comprises one of a random number or a string of random characters.

13. The non-transitory memory of claim 1, wherein the client application is configured to generate, using the diversified key, the FIDO private key and a FIDO public key.

14. A method, comprising:

receiving, by a client application comprising instructions for execution on a client device, a challenge from a first server, wherein the client device comprises a processor, a memory storing a Fast Identity Online (FIDO) private key and a FIDO public key, and a communication interface;

transmitting, by the client application, an authentication request to a contactless card;

transmitting, by the client application, authentication data received from the contactless card, to a second server;

receiving, by the client application, a verification of the authentication data, wherein the verification permits the use of the FIDO private key;

signing, by the client application, the challenge using the FIDO private key; and

transmitting, by the client application, the signed challenge to the first server.

15. The method of claim 14, comprising transmitting, by the client application, a FIDO public key to the first server.

16. The method of claim 14, wherein the client application stores the FIDO private key in the memory of the client device.

17. The method of claim 14, comprising receiving, by the client application, a verification input prior to signing the challenge using the FIDO private key.

18. A contactless card, comprising:

a memory containing a counter, a diversified key, a Fast Identity Online (FIDO) public key, and a FIDO private key;

a communication interface; and

a processor in communication with the memory and communication interface, the processor configured to:

update the counter when the communication interface is within a range of a communication field associated with a client device;

receive, via the communication interface, a transaction verification request from the client device;

create a cryptogram using the diversified key and the counter, wherein the cryptogram stores the FIDO private key; and

transmit a transaction verification response to the client device, the transaction verification response including the cryptogram, wherein the transaction verification response provides the FIDO private key, in an encrypted form, to the client device in connection with a challenge.

19. The contactless card of claim 18, wherein the processor is configured to transmit the cryptogram, via the communication interface, to an application executing on the client device.

20. The contactless card of claim 18, wherein the cryptogram in the transaction verification response further includes the FIDO public key being transmitted, by the client device, to a server.