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, a master key, 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 server, transmit a verification request to a contactless card, receive a verification from the contactless card, wherein the verification permits the use of a Fast Identity Online (FIDO) private key, generate, using the master key and the diversified key, a FIDO key pair including the FIDO private key and a FIDO public key, sign the challenge using the FIDO private key, and transmit the signed challenge to the server.

[0008b] An 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 server, wherein the client device comprises a processor, a memory, and a communication interface, transmitting, by the client application, a verification request to a contactless card, receiving, by the client application, a verification from the contactless card, wherein the verification permits the use of a Fast Identity Online (FIDO) private key, generating, by the client application using a master key and a diversified key, a FIDO key pair including the FIDO private key and a FIDO public key, signing, by the client application, the challenge using the FIDO private key, andtransmitting, by the client application, the signed challenge to the server.

[0008c] An 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, receive, via the communication interface, a transaction verification request, create a cryptogram using the diversified key and the counter, wherein the cryptogram stores the FIDO public key, and create

a transaction verification response, the transaction verification response including the cryptogram, wherein the transaction verification permits use of the private key 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

communication interface in data communication with a contactless card and a server, the communication interface having a communication field; wherein, upon receipt of an instruction to initiate a transaction, the processor is configured to: transmit a transaction request to a first server, the transaction request including account information and transaction information relating to the transaction; receive a challenge from a second server; request a transaction verification from the contactless card; receive, via the communication interface, a transaction verification from the contactless card upon entry of the contactless card into the communication field, wherein the transaction verification permits use of the FIDO private key in connection with the challenge; sign the challenge using the private key; and transmit the signed challenge to the second server.

[0010] There is also disclosed a authorization method comprising: initiating, by a client application comprising instructions for execution on a client device, a transaction with a first server; transmitting, by the client application, transaction information to the first server; receiving, by the client application, a challenge sent by a second server; requesting, by the client application, a transaction verification; receiving, by the client application, a transaction verification, wherein the transaction verification authorizes the client application to utilize a FIDO private key stored in a memory of the client device to sign the challenge; signing, by the client application, the challenge using the FIDO private key; transmitting, by the client application, the signed challenge to the server; and receiving, by the client application, an indication from the server that the transaction has been approved.

[0011] There is also disclosed a contactless card comprising: a substrate, including: a memory containing an applet, a counter value, a master key, a diversified key, a FIDO public key, and a FIDO private key; a communication interface; and a

CLAIMS

What is claimed is:

1. A non-transitory memory storing a client application, a master key, 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 server,

transmit a verification request to a contactless card,

receive a verification from the contactless card, wherein the verification permits the use of a Fast Identity Online (FIDO) private key,

generate, using the master key and the diversified key, a FIDO key pair including the FIDO private key and a FIDO public key,

sign the challenge using the FIDO private key, and

transmit the signed challenge to the server.

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

3. The non-transitory memory of claim 1, wherein the 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 server, transmit a request for the challenge to the server.

5. The non-transitory memory of claim 1, wherein the verification 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

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

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

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

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

the non-transitory memory stores a counter, and

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

11. The non-transitory memory of claim 11, wherein the client application is configured to receive the counter from the server.

12. The non-transitory memory of claim 1, wherein the application is configured to randomly generate the FIDO key pair.

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

14. A method, comprising:

receiving, by a client application comprising instructions for execution on a client device, a challenge from a server, wherein the client device comprises a processor, a memory, and a communication interface;

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

receiving, by the client application, a verification from the contactless card, wherein the verification permits the use of a Fast Identity Online (FIDO) private key;

generating, by the client application using a master key and a diversified key, a FIDO key pair including the FIDO private key and a FIDO public key;

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

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

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

16. The method of claim 14, wherein the 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;

receive, via the communication interface, a transaction verification request;

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

create a transaction verification response, the transaction verification response including the cryptogram, wherein the transaction verification permits use of the private key 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 a client device.

20. The contactless card of claim 18, wherein the challenge comprises one of a random number or a string of random characters.