CLAIMS

What is claimed is:

1. A method, comprising:

receiving, by an operating system (OS) executing on a processor of a device, a uniform resource locator (URL) and a cryptogram from a contactless card associated with an account;

transmitting, by ~~launching, by the operating system responsive to receiving the URL,~~ an application associated with the URL~~contactless card;~~

~~transmitting, by the application~~, the cryptogram to an authentication server;

receiving, by the application, a decryption result from the authentication server indicating the authentication server decrypted the cryptogram;

transmitting, by the application based on the decryption result, a request for a one-time passcode (OTP) comprising an identifier to an OTP generator~~the URL~~;

receiving, by the device, the OTP from the~~an~~ OTP generator ~~at the URL~~;

receiving, by the application, an input value;

~~comparing, by the application, the input value to a copy of the OTP received from the OTP generator;~~

~~determining, by the application, that the comparison results in a match;~~ and

permitting~~displaying~~, by the application based on a~~the~~ determination that the input value matches a copy of the OTP received from the OTP generator, performance of a requested operation associated with the account~~comparison results in the match, one or more attributes of the account~~ on the device.

2. The method of claim 1, further comprising:

launching, by the OS, the application responsive to receiving the URL.

~~determining, by the application, the identifier in an account database on the device, wherein the identifier comprises one of an identifier of the contactless card or an identifier of the account.~~

3. The method of claim 1 or claim 2, wherein~~further comprising:~~

~~receiving, by~~ the requested operation comprises~~device, the OTP via at least~~ one or more of: (i) viewing one or more attributes of the account~~an email address associated with the identifier~~, (ii) transferring funds from the account,~~a short message service (SMS)~~

~~message at a phone number associated with the identifier, and~~ (iii) ~~a push notification received by the application based on a device identifier of the device associated with the identifier.~~

~~4. The method of claim 1, further comprising prior to transmitting the cryptogram to the authentication server:~~

receiving funds, or (iv) processing a purchase using funds from~~, by the application, authentication credentials for~~ the account. ~~; and~~

4.~~verifying, by the application, the received authentication credentials for the account.~~

~~5.~~ The method of claim 34, further comprising ~~subsequent to verifying the authentication credentials for the account~~:

receiving, by the application, a request to perform the~~an~~ operation. ~~associated with the account;~~

~~outputting, by the application, an indication specifying to tap the contactless card to the device to authorize the operation; and~~

~~authorizing, by the application, the requested operation based on the decryption result indicating the authentication server decrypted the cryptogram and the determination that the comparison results in the match.~~

~~6. The method of claim 1, wherein the OS receives the URL and the cryptogram from the contactless card based on near field communication (NFC), the method further comprising:~~

~~providing, by the OS, the received OTP to an autofill service of the OS; and~~

~~autofilling, by the autofill service, the OTP into a form field of the application.~~

5.~~7.~~ The method of any one of claims 1 to 4, wherein the URL is registered to launch the application in the OS, wherein the URL is directed to an application programming interface (API) endpoint for the OTP generator.

6. The method of any one of claims 1 to 5, further comprising:

comparing, by the application, the input value to the copy of the OTP received from the OTP generator.

7. The method of any one of claims 1 to 6, further comprising:

~~8. A system, comprising:~~

providing, by the OS, the received OTP to an autofill service of the OS; and

autofilling, by the autofill service, the OTP into a form field of the application.

8. A non-transitory computer-readable storage medium, the computer-readable storage medium including instructions that when executed by a processor, cause the processor to:

receive, by an operating system (OS), a uniform resource locator (URL) and a cryptogram from a contactless card associated with an account;

transmit, by an application associated with the URL, the cryptogram to an authentication server;

receive, by the application, a decryption result from the authentication server indicating the authentication server decrypted the cryptogram;

transmit, by the application based on the decryption result, a request for a one-time passcode (OTP) comprising an identifier to an OTP generator;

receive the OTP from the OTP generator;

receive, by the application, an input value; and

permit, by the application based on a determination that the input value matches a copy of the OTP received from the OTP generator, performance of a requested operation associated with the account.

9. The computer-readable storage medium of claim 8, wherein the instructions further cause the processor to:

launch, by the OS, the application responsive to receiving the URL.

10. The computer-readable storage medium of claim 8 or claim 9, wherein the requested operation comprises one or more of: (i) view one or more attributes of the account, (ii) transferring funds from the account, (iii) receiving funds, or (iv) processing a purchase using funds from the account.

11. The computer-readable storage medium of claim 10, wherein the instructions further cause the processor to:

receive, by the application, a request to perform the operation.

12. The computer-readable storage medium of any one of claims 8 to 11, wherein the URL is registered to launch the application in the OS, wherein the URL is directed to an application program interface (API) endpoint for the OTP generator.

13. The computer-readable storage medium of any one of claims 8 to 12, wherein the instructions further cause the processor to:

compare, by the application, the input value to the copy of the OTP received from the OTP generator.

14. The computer-readable storage medium of any one of claims 8 to 13, wherein the instructions further cause the processor to:

provide, by the OS, the received OTP to an autofill service of the OS; and

autofilling, by the autofill service, the OTP into a form field of the application.

15. A computing apparatus comprising:

a processor; and

a memory storing instructions that, when executed by the processor, cause the processor to:

receive, by an operating system (OS), ~~executing on the processor,~~ a uniform resource locator (URL) and a cryptogram from a contactless card associated with an account;

transmit, by ~~launch, by the operating system responsive to receiving the URL,~~ an application associated with the URL ~~contactless card;~~

~~transmit, by the application~~, the cryptogram to an authentication server;

receive, by the application, a decryption result from the authentication server indicating the authentication server decrypted the cryptogram;

transmit, by the application based on the decryption result, a request for a one-time passcode (OTP) comprising an identifier to an OTP generator; ~~the URL; and~~

receive~~, by the processor,~~ the OTP from the ~~an~~ OTP generator ~~at the URL~~;

receive, by the application, an input value; and

permit ~~compare~~, by the application based on a determination that~~,~~ the input value matches ~~to~~ a copy of the OTP received from the OTP generator, performance of a requested operation associated with the account.~~;~~

16. ~~determine, by the application, that the comparison results in a match; and~~

~~display, by the application based on the determination that the comparison results in the match, one or more attributes of the account.~~

~~9.~~ The computing apparatus ~~system~~ of claim 15, wherein ~~8,~~ the ~~memory storing~~ instructions further ~~that when executed by the processor~~ cause the processor ~~to~~:

launch~~determine~~, by the OS, the application responsive to receiving~~, the identifier in an account database stored in~~ the URL.

17. The computing apparatus of claim 15 or claim 16~~memory~~, wherein the requested operation~~identifier~~ comprises one ~~of an identifier of the contactless card~~ or more of: (i) view one or more attributes~~an identifier~~ of the account, (ii) transferring funds from the account, (iii) receiving funds, or (iv) processing a purchase using funds from the account.~~.~~

18.~~10.~~ The computing apparatus~~system~~ of claim 17, wherein~~8,~~ the ~~memory storing~~ instructions further ~~that when executed by the processor~~ cause the processor to:

~~receive, by the processor, the OTP via at least one of: (i) an email address associated with the identifier, (ii) a short message service (SMS) message at a phone number associated with the identifier, and (iii) a push notification received by the application based on a device identifier of the device associated with the identifier.~~

~~11. The system of claim 8, the memory storing instructions that when executed by the processor cause the processor to, prior to transmitting the cryptogram to the authentication server:~~

~~receive, by the application, authentication credentials for the account; and~~

~~verify, by the application, the received authentication credentials for the account.~~

~~12. The system of claim 11, the memory storing instructions that when executed by the processor cause the processor to, subsequent to verifying the authentication credentials for the account:~~

receive, by the application, a request to perform the~~an~~ operation~~. associated with the account;~~

~~output, by the application, an indication specifying to tap the contactless card to the system to authorize the operation; and~~

~~authorize, by the application, the requested operation based on the decryption result indicating the authentication server decrypted the cryptogram and the determination that the comparison results in the match.~~

~~13. The system of claim 8, wherein the OS receives the URL and the cryptogram from the contactless card based on near field communication (NFC), the memory storing instructions that when executed by the processor cause the processor to:~~

~~provide, by the OS, the received OTP to an autofill service of the OS; and~~

19. The computing apparatus of any one of claims 15 to 18,~~autofill, by the autofill service, the OTP into a form field of the application.~~

~~14. The system of claim 8, wherein the URL is registered to launch the application in the OS, wherein the URL is directed to an application programming interface (API) endpoint for the OTP generator.~~

~~15. A non-transitory computer-readable storage medium storing computer-readable instructions that when executed by a processor cause the processor to:~~

~~receive, by an operating system executing on the processor, a uniform resource locator (URL) and a cryptogram from a contactless card associated with an account;~~

~~launch, by the operating system responsive to receiving the URL, an application associated with the contactless card;~~

~~transmit, by the application, the cryptogram to an authentication server;~~

~~receive, by the application, a decryption result from the authentication server indicating the authentication server decrypted the cryptogram;~~

~~transmit, by the application based on the decryption result, a request for a one-time passcode (OTP) comprising an identifier to the URL; and~~

~~receive the OTP from an OTP generator at the URL;~~

~~receive, by the application, an input value;~~

~~compare, by the application, the input value to a copy of the OTP received from the OTP generator;~~

~~determine, by the application, that the comparison results in a match; and~~

~~display, by the application based on the determination that the comparison results in the match, one or more attributes of the account on a display.~~

~~16. The non-transitory computer-readable storage medium of claim 15, further comprising instructions that when executed by the processor cause the processor to:~~

~~determine, by the application, the identifier in an account database stored in the medium, wherein the identifier comprises one of an identifier of the contactless card or an identifier of the account.~~

~~17. The non-transitory computer-readable storage medium of claim 15, further comprising instructions that when executed by the processor cause the processor to:~~

~~receive the OTP via at least one of: (i) an email address associated with the identifier, (ii) a short message service (SMS) message at a phone number associated with the identifier, and (iii) a push notification received by the application based on a device identifier of the device associated with the identifier.~~

~~18. The non-transitory computer-readable storage medium of claim 15, further comprising instructions that when executed by the processor cause the processor to, prior to transmitting the cryptogram to the authentication server:~~

~~receive, by the application, authentication credentials for the account; and~~

~~verify, by the application, the received authentication credentials for the account.~~

~~19. The non-transitory computer-readable storage medium of claim 18, further comprising instructions that when executed by the processor cause the processor to, subsequent to verifying the authentication credentials for the account:~~

~~receive, by the application, a request to perform an operation associated with the account;~~

~~output, by the application, an indication specifying to tap the contactless card to a device comprising the processor to authorize the operation; and~~

~~authorize, by the application, the requested operation based on the decryption result indicating the authentication server decrypted the cryptogram and the determination that the comparison results in the match.~~

~~20. The non-transitory computer-readable storage medium of claim 15, wherein the OS receives the URL and the cryptogram from the contactless card based on near field communication (NFC),~~ wherein the URL is registered to launch the application in the OS, wherein the URL is directed to an application program~~programming~~ interface (API) endpoint for the OTP generator., ~~the medium further comprising instructions that when executed by the processor cause the processor to:~~

20. The computing apparatus of any one of claims 15 to 19, wherein the instructions further cause the processor to:

provide, by the OS, the received OTP to an autofill service of the OS; and

autofilling~~autofill~~, by the autofill service, the OTP into a form field of the application.