What is claimed is:

1. A mobile device, comprising:

a processor; and

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

generate, by a first application executing on the processor, a first URL directed to a second application, wherein a parameter of the first URL comprises an identifier of the first application;

access, by a mobile operating system (OS) executing on the processor, the first URL to open the second application;

receive, by the second application from a server, a virtual account number (VAN) associated with an account;

initiate, by the second application, a local transmission control protocol/internet protocol (TCP/IP) server on a port;

generate, by the second application, a second URL directed to the first application, wherein a parameter of the second URL comprises the port;

access, by the OS, the second URL to open the first application;

establish, by the first application, a connection with the TCP/IP server using the port specified in the parameter of the second URL;

receive, by the first application, the VAN from the second application via the connection with the local TCP/IP server; and

autofill, by the first application, the VAN to a form field of a payment form in the first application.

2. The mobile device of claim 1, the memory storing instructions which when executed by the processor cause the processor to, prior to the second application receiving the VAN:

receive, by the second application, encrypted data from a contactless card assigned to the account;

transmit, by the second application, the encrypted data to the server; and

receive, by the second application, an indication from the server specifying the server decrypted the encrypted data, wherein the second application receives the VAN based at least in part on the received indication from the server.

3. The mobile device of claim 1, the memory storing instructions which when executed by the processor cause the processor to:

receive, by the local TCP/IP server, a request to establish the connection from the first application, wherein the request comprises a certificate of the first application;

validate, by the second application, the certificate of the first application; and

determine, by the second application, to establish the connection based on identifying the identifier of the first application in the request and the validation of the certificate of the first application, wherein the local TCP/IP server is accessible only to applications executing on the mobile device.

4. The mobile device of claim 1, the memory storing instructions which when executed by the processor cause the processor to, prior to the second application receiving the VAN:

determine, by the second application, that the account has not been accessed using the second application within a time threshold;

output, by the second application, an indication specifying to provide authentication credentials for the account;

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

validate, by the second application, the received authentication credentials for the account.

5. The mobile device of claim 1, the memory storing instructions which when executed by the processor cause the processor to:

validate, by the first application using an application programming interface (API) of the OS, at least a portion of the first URL; and

validate, by the second application using the API of the OS, at least a portion of the second URL.

6. The mobile device of claim 1, the memory storing instructions which when executed by the processor cause the processor to:

receive, by the second application from the server, a plurality of attributes comprising a name associated with the account, an expiration date of the VAN, and a card verification value (CVV) of the VAN;

receive, by the first application, the plurality of attributes from the second application via the connection with the local TCP/IP server;

autofill, by the first application, each attribute to a respective field of the payment form in the first application; and

process, by the first application, payment for a purchase using the VAN and the received attributes.

7. The mobile device of claim 1, wherein the first and second URLs comprise universal link URLs, wherein the OS restricts communication between the first and second applications

without using the local TCP/IP server based on the first and second applications being registered with different developers, the memory storing instructions which when executed by the processor cause the processor to:

register, by the second application using an application programming interface of the OS, the second application as a background task to execute in a background of the OS; and

execute, by the OS, the local TCP/IP server as part of the background task in the background of the OS.

8. A non-transitory computer-readable storage medium comprising computer-readable program code which when executed by a processor of a mobile device cause the processor to:

generate, by a first application executing on the processor, a first URL directed to a second application, wherein a parameter of the first URL comprises an identifier of the first application;

access, by a mobile operating system (OS) executing on the processor, the first URL to open the second application;

receive, by the second application from a server, a virtual account number (VAN) associated with an account;

initiate, by the second application, a local transmission control protocol/internet protocol (TCP/IP) server on a port;

generate, by the second application, a second URL directed to the first application, wherein a parameter of the second URL comprises the port;

access, by the OS, the second URL to open the first application;

establish, by the first application, a connection with the TCP/IP server using the port specified in the parameter of the second URL;

receive, by the first application, the VAN from the second application via the connection with the local TCP/IP server; and

autofill, by the first application, the VAN to a form field of a payment form in the first application.

9. The computer-readable storage medium of claim 8, comprising computer-readable program code which when executed by the processor cause the processor to:

receive, by the second application, encrypted data from a contactless card assigned to the account;

transmit, by the second application, the encrypted data to the server; and

receive, by the second application, an indication from the server specifying the server decrypted the encrypted data, wherein the second application receives the VAN based at least in part on the received indication from the server.

10. The computer-readable storage medium of claim 8, comprising computer-readable program code which when executed by the processor cause the processor to:

receive, by the local TCP/IP server of the second application, a request to establish the connection from the first application, wherein the request comprises a certificate of the first application;

validate, by the second application, the certificate of the first application; and

determine, by the second application, to establish the connection based on identifying the identifier of the first application in the request and the validation of the certificate of the first application, wherein the local TCP/IP server is accessible only to applications executing on the mobile device.

11. The computer-readable storage medium of claim 8, comprising computer-readable program code which when executed by the processor cause the processor to:

validate, by the first application using an application programming interface (API) of the OS, at least a portion of the first URL; and

validate, by the second application using the API of the OS, at least a portion of the second URL.

12. The computer-readable storage medium of claim 8, comprising computer-readable program code which when executed by the processor cause the processor to:

receive, by the first application, an updated value for an attribute of the account;

transmit, by the first application, the updated value for the attribute of the account to the second application via the connection with the local TCP/IP server; and

output, by the second application, an indication specifying to store the updated value for the attribute in the account.

13. The computer-readable storage medium of claim 8, comprising computer-readable program code which when executed by the processor cause the processor to:

receive, by the second application from the server, a plurality of attributes comprising a name associated with the account, an expiration date of the VAN, and a card verification value (CVV) of the VAN;

receive, by the first application, the plurality of attributes from the second application via the connection with the local TCP/IP server;

autofill, by the first application, each attribute to a respective field of the payment form in the first application; and

process, by the first application, payment for a purchase using the VAN and the received attributes.

14. A method, comprising:

generating, by a first application executing on a processor of a mobile device, a first URL directed to a second application, wherein a parameter of the first URL comprises an identifier of the first application;

accessing, by a mobile operating system (OS) executing on the processor, the first URL to open the second application;

receiving, by the second application from a server, a virtual account number (VAN) associated with an account;

initiating, by the second application, a local transmission control protocol/internet protocol (TCP/IP) server on a port;

generating, by the second application, a second URL directed to the first application, wherein a parameter of the second URL comprises the port;

accessing, by the OS, the second URL to open the first application;

establishing, by the first application, a connection with the TCP/IP server using the port specified in the parameter of the second URL;

receiving, by the first application, the VAN from the second application via the connection with the local TCP/IP server; and

autofilling, by the first application, the VAN to a form field of a payment form in the first application.

15. The method of claim 14, further comprising, prior to the second application receiving the VAN:

receiving, by the second application, encrypted data from a contactless card assigned to the account;

transmitting, by the second application, the encrypted data to the server; and

receiving, by the second application, an indication from the server specifying the server decrypted the encrypted data, wherein the second application receives the VAN based at least in part on the received indication from the server.

16. The method of claim 14, further comprising:

receiving, by the local TCP/IP server of the second application, a request to establish the connection from the first application, wherein the request comprises a certificate of the first application;

validating, by the second application, the certificate of the first application; and

determining, by the second application, to establish the connection based on identifying the identifier of the first application in the request and the validation of the certificate of the first application, wherein the local TCP/IP server is accessible only to applications executing on the mobile device.

17. The method of claim 14, further comprising:

determining, by the second application, that the account has not been accessed using the second application within a time threshold;

outputting, by the second application, an indication specifying to provide authentication credentials for the account;

receiving, by the second application, authentication credentials for the account; and

validating, by the second application, the received authentication credentials for the account.

18. The method of claim 14, further comprising:

validating, by the first application using an application programming interface (API) of the OS, at least a portion of the first URL; and

validating, by the second application using the API of the OS, at least a portion of the second URL.

19. The method of claim 14, further comprising:

receiving, by the second application from the server, a plurality of attributes comprising a name associated with the account, an expiration date of the VAN, and a card verification value (CVV) of the VAN;

receiving, by the first application, the plurality of attributes from the second application via the connection with the local TCP/IP server;

autofilling, by the first application, each attribute to a respective field of the payment form in the first application; and

processing, by the first application, payment for a purchase using the VAN and the received attributes.

20. The method of claim 14, wherein the first and second URLs comprise universal link URLs, wherein the OS restricts communication between the first and second applications without using the local TCP/IP server based on the first and second applications being registered with different developers, the method further comprising:

registering, by the second application using an application programming interface of the OS, the second application as a background task to execute in a background of the OS; and

executing, by the OS, the local TCP/IP server as part of the background task in the background of the OS.

1. A method, comprising:

generating, by a first application executing on a processor, a first URL directed to a second application, wherein a parameter of the first URL comprises an identifier of the first application;

accessing, by a mobile operating system (OS) executing on the processor, the second application based on the first URL;

receiving, by the second application from a server, data associated with an account;

initiating, by the second application, a transmission control protocol/internet protocol (TCP/IP) server on a port;

generating, by the second application, a second URL directed to the first application, wherein a parameter of the second URL comprises the port;

accessing, by the OS, the first application based on the second URL;

receiving, by the first application, the data via a connection with the TCP/IP server using the port specified in the second URL; and

autofilling, by the first application, the data to a form field in the first application.

2. The method of claim 1, further comprising:

establishing, by the first application, the connection with the TCP/IP server using the port specified in the second URL.

3. The method of claim 1, wherein the data comprises one or more of an account number associated with the account, an expiration date of the account number, a card verification value (CVV) of the account number, or a billing address of the account.

4. The method of claim 1, further comprising prior to the second application receiving the data:

receiving, by the second application, encrypted data from a contactless card;

transmitting, by the second application, the encrypted data to the server; and

receiving, by the second application, an indication from the server specifying the server decrypted the encrypted data, wherein the second application receives the data based at least in part on the received indication from the server.

5. The method of claim 1, further comprising:

selecting, by the second application, a port number from a plurality of port numbers as the port.

6. The method of claim 1, further comprising:

receiving, by the TCP/IP server, a request to establish the connection from the first application, wherein the request comprises a certificate of the first application;

validating, by the second application, the certificate of the first application; and

determining, by the second application, to establish the connection based on identifying the identifier of the first application in the request and the validation of the certificate of the first application, wherein the TCP/IP server is accessible only to applications executing on the processor.

7. The method of claim 1, further comprising:

validating, by the first application using an application programming interface (API) of the OS, at least a portion of the first URL; and

validating, by the second application using the API of the OS, at least a portion of the second URL.

8. A computing apparatus comprising:

a processor; and

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

generate, by a first application executing on a processor, a first URL directed to a second application, wherein a parameter of the first URL comprises an identifier of the first application;

access, by a mobile operating system (OS) executing on the processor, the second application based on the first URL;

receive, by the second application from a server, data associated with an account;

initiate, by the second application, a transmission control protocol/internet protocol (TCP/IP) server on a port;

generate, by the second application, a second URL directed to the first application, wherein a parameter of the second URL comprises the port;

access, by the OS, the first application based on the second URL;

receive, by the first application, the data via a connection with the TCP/IP server using the port specified in the second URL; and

autofill, by the first application, the data to a form field in the first application.

9. The computing apparatus of claim 8, wherein the instructions further cause the processor to:

establish, by the first application, the connection with the TCP/IP server using the port specified in the second URL.

10. The computing apparatus of claim 8, wherein the data comprises one or more of an account number associated with the account, an expiration date of the account number, a card verification value (CVV) of the account number, or a billing address of the account.

11. The computing apparatus of claim 8, wherein the instructions further cause the processor to, prior to the second application receiving the data:

receive, by the second application, encrypted data from a contactless card;

transmit, by the second application, the encrypted data to the server; and

receive, by the second application, an indication from the server specify the server decrypted the encrypted data, wherein the second application receives the data based at least in part on the received indication from the server.

12. The computing apparatus of claim 8, wherein the instructions further cause the processor to:

select, by the second application, a port number from a plurality of port numbers as the port.

13. The computing apparatus of claim 8, wherein the instructions further cause the processor to:

receive, by the TCP/IP server, a request to establish the connection from the first application, wherein the request comprises a certificate of the first application;

validate, by the second application, the certificate of the first application; and

determine, by the second application, to establish the connection based on identifying the identifier of the first application in the request and the validation of the certificate of the first application, wherein the TCP/IP server is accessible only to applications executing on the processor.

14. The computing apparatus of claim 8, wherein the instructions further cause the processor to:

validate, by the first application using an application programming interface (API) of the OS, at least a portion of the first URL; and

validate, by the second application using the API of the OS, at least a portion of the second URL.

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

generate, by a first application executing on a processor, a first URL directed to a second application, wherein a parameter of the first URL comprises an identifier of the first application;

access, by a mobile operating system (OS) executing on the processor, the second application based on the first URL;

receive, by the second application from a server, data associated with an account;

initiate, by the second application, a transmission control protocol/internet protocol (TCP/IP) server on a port;

generate, by the second application, a second URL directed to the first application, wherein a parameter of the second URL comprises the port;

access, by the OS, the first application based on the second URL;

receive, by the first application, the data via a connection with the TCP/IP server using the port specified in the second URL; and

autofill, by the first application, the data to a form field in the first application.

16. The computer-readable storage medium of claim 15, wherein the instructions further cause the processor to:

establish, by the first application, the connection with the TCP/IP server using the port specified in the second URL.

17. The computer-readable storage medium of claim 15, wherein the data comprises one or more of an account number associated with the account, an expiration date of the account number, a card verification value (CVV) of the account number, or a billing address of the account.

18. The computer-readable storage medium of claim 15, wherein the instructions further cause the processor to, prior to the second application receiving the data:

receive, by the second application, encrypted data from a contactless card;

transmit, by the second application, the encrypted data to the server; and

receive, by the second application, an indication from the server specify the server decrypted the encrypted data, wherein the second application receives the data based at least in part on the received indication from the server.

19. The computer-readable storage medium of claim 15, wherein the instructions further cause the processor to:

select, by the second application, a port number from a plurality of port numbers as the port.

20. The computer-readable storage medium of claim 15, wherein the instructions further cause the processor to:

receive, by the TCP/IP server, a request to establish the connection from the first application, wherein the request comprises a certificate of the first application;

validate, by the second application, the certificate of the first application; and

determine, by the second application, to establish the connection based on identifying the identifier of the first application in the request and the validation of the certificate of the first application, wherein the TCP/IP server is accessible only to applications executing on the processor.