What is claimed is:

~~1 A device, comprising:~~

~~a processor; and~~

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

~~receive, by a first application executing on the processor, an indication specifying to receive data from a second application;~~

~~generate, by the first application, a first URL directed to the 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;~~

~~validate, by the second application, authentication credentials for 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 local TCP/IP server using the port specified in the parameter of the second URL; and~~

~~receive, by the first application, the data from the second application via the connection with the local TCP/IP server.~~

~~2. The 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 of the second application, a request to establish the connection from 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.~~

3. The device of claim 2, wherein the request further comprises a certificate of the first application, the memory storing instructions which when executed by the processor cause the processor to:

validate, by the second application, the certificate of the first application, wherein the second application further determines to establish the connection based on validating the certificate of the first application, wherein the local TCP/IP server is accessible only to applications executing on the device.

4. The device of claim 1, the memory storing instructions which when executed by the processor cause the processor to, prior to the second application initiating the local TCP/IP server:

receive, by the second application subsequent to validating the authentication credentials, encrypted data from a contactless card;

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

receive, by the second application, an indication from the authentication server specifying the authentication server decrypted the encrypted data, wherein the second application initiates the local TCP/IP server based at least in part on the received indication from the authentication server.

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

determine, by the first application, that the data received from the second application comprises one or more attributes of the account; and

autofill, by the first application, the one or more attributes of the account to one or more form fields in the first application.

7. The 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 device cause the processor to:

receive, by a first application executing on the processor, an indication specifying to receive data from a second application;

generate, by the first application, a first URL directed to the 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;

validate, by the second application, authentication credentials for 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 local TCP/IP server using the port specified in the parameter of the second URL; and

receive, by the first application, the data from the second application via the connection the local TCP/IP server.

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 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 device.

10. The computer-readable storage medium of claim 9, comprising computer-readable program code which when executed by the processor cause the processor to, prior to the second application initiating the local TCP/IP server:

receive, by the second application subsequent to validating the authentication credentials, encrypted data from a contactless card;

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

receive, by the second application, an indication from the authentication server specifying the authentication server decrypted the encrypted data, wherein the second application initiates the local TCP/IP server based at least in part on the received indication from the authentication server.

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:

determine, by the first application, that the data received from the second application comprises one or more attributes of the account; and

autofill, by the first application, the one or more attributes of the account to one or more form fields in the first application.

13. The computer-readable storage medium of claim 8, comprising computer-readable program code 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 the background task in the background of the OS,

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.

14. A method, comprising:

receiving, by a first application executing on a processor of a device, an indication specifying to receive data from a second application;

generating, by the first application, a first URL directed to the 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;

validating, by the second application, authentication credentials for 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 local TCP/IP server using the port specified in the parameter of the second URL; and
receiving, by the first application, the data from the second application via the connection the local TCP/IP server.

15. 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; and
determining, by the second application, to establish the connection based on identifying the identifier of the first application in the request.

16. The method of claim 15, wherein the request further comprises a certificate of the first application, further comprising:
validating, by the second application, the certificate of the first application, wherein the second application further determines to establish the connection based on validating the certificate of the first application, wherein the local TCP/IP server is accessible only to applications executing on the device, wherein the OS rejects requests to access to the TCP/IP server received from remote devices.

17. The method of claim 14, further comprising prior to the second application initiating the local TCP/IP server:

receiving, by the second application subsequent to validating the authentication credentials, encrypted data from a contactless card;

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

~~receiving, by the second application, an indication from the authentication server specifying the authentication server decrypted the encrypted data, wherein the second application initiates the local TCP/IP server based at least in part on the received indication from the authentication server.~~

~~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:~~
~~determining, by the first application, that the data received from the second application comprises one or more attributes of the account; and~~
~~autofilling, by the first application, the one or more attributes of the account to one or more form fields in the first application.~~

~~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 computer-implemented 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 first URL to open the second application;

initiating, by the second application executing on the processor, 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 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 second URL; and

receiving, by the first application, data from the second application via the connection with the TCP/IP server.

2. The computer-implemented method of claim 1, further comprising:

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

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

3. The computer-implemented method of claim 1, wherein the identifier of the first application comprises a token, further comprising:

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

validating, by the TCP/IP server, the token.

4. The computer-implemented method of claim 1, wherein the first URL and the second URL comprise universal link URLs directed to the first and second applications, respectively.

5. The computer-implemented method of claim 1, 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 TCP/IP server as part of the background task in the background of the OS.

6. The computer-implemented method of claim 1, further comprising:

determining, by the first application, that the data received from the second application comprises one or more attributes of an account; and

autofilling, by the first application, the one or more attributes of the account to one or more form fields in the first application.

7. The computer-implemented method of claim 1, further comprising prior to the second application initiating the TCP/IP server:

receiving, by the second application, a cryptogram from a contactless card;

transmitting, by the second application, the cryptogram to a server; and

receiving, by the second application, an indication from the server specifying the server decrypted the cryptogram, wherein the second application initiates the TCP/IP server based at least in part on the indication received from the server.

8. An apparatus, comprising:

a processor; and

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

generate, by a first application, 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), the first URL to open the second application;

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 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 second URL; and

receive, by the first application, data from the second application via the connection with the TCP/IP server.

9. The apparatus of claim 8, 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 prior to the OS accessing the first URL, at least a portion of the first URL; and

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

10. The apparatus of claim 8, wherein the identifier of the first application comprises a token, the memory storing instructions which when executed by the processor cause the processor to, prior to the establishment of the connection:

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

validate, by the TCP/IP server, the token.

11. The apparatus of claim 8, wherein the first URL and the second URL comprise universal link URLs directed to the first and second applications, respectively.

12. The apparatus of claim 8, 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 TCP/IP server as part of the background task in the background of the OS.

13. The apparatus of claim 8, the memory storing instructions which when executed by the processor cause the processor to:

determine, by the first application, that the data received from the second application comprises one or more attributes of an account; and

autofill, by the first application, the one or more attributes of the account to one or more form fields in the first application.

14. The apparatus of claim 8, the memory storing instructions which when executed by the processor cause the processor to, prior to the second application initiating the TCP/IP server:

receive, by the second application, a cryptogram from a contactless card;

transmit, by the second application, the cryptogram to a server; and

receive, by the second application, an indication from the server specifying the server decrypted the cryptogram, wherein the second application initiates the TCP/IP server based at least in part on the indication received from the server.

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

generate, by a first application, 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), the first URL to open the second application;

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 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 second URL; and

receive, by the first application, data from the second application via the connection with the TCP/IP server.

16. The computer-readable storage medium of claim 15, 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 prior to the OS accessing the first URL, at least a portion of the first URL; and

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

17. The computer-readable storage medium of claim 15, wherein the identifier of the first application comprises a token, the medium comprising computer-readable program code which when executed by the processor cause the processor to, prior to the establishment of the connection:

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

validate, by the TCP/IP server, the token.

18. The computer-readable storage medium of claim 15, wherein the first URL and the second URL comprise universal link URLs directed to the first and second applications, respectively.

19. The computer-readable storage medium of claim 15, comprising computer-readable program code 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 TCP/IP server as part of the background task in the background of the OS.

20. The computer-readable storage medium of claim 15, comprising computer-readable program code which when executed by the processor cause the processor to:

determine, by the first application, that the data received from the second application comprises one or more attributes of an account; and

autofill, by the first application, the one or more attributes of the account to one or more form fields in the first application.