WHAT IS CLAIMED IS:

1. A computer-implemented method, comprising:

receiving, by a user device, a selection of a payment card of a plurality of payment cards stored in a merchant application of the user device for a payment transaction between a user of the user device and a merchant associated with the merchant application;

in response to receiving the selection of the payment card, initiating, by the user device, the payment transaction between the user and the merchant via the merchant application;

in response to receiving the selection of the payment card, sending, by the merchant application, a request to the user device for verifying a phone number associated with a Subscriber Identification Module (SIM) card in the user device;

receiving, by the user device, the request for verifying the phone number associated with the SIM card in the user device from the merchant application installed in the user device; and

in response to receiving the request, obtaining, by the user device, the phone number from the SIM card and a key from at least one of a server associated with a manufacturer of the user device or a network server, wherein obtaining the key comprises:

sending a request for the key to the server associated with the manufacturer of the user device; and

one of:

(i) receiving a first key from the server associated with the manufacturer, wherein the server associated with the manufacturer generates the first key in real-time using one or more cryptographic techniques, wherein the key comprises the first key;

(ii) fetching a second key from a memory associated with the user device, wherein the second key was generated by the server associated with the manufacturer and stored in the memory associated with the user device during manufacturing of the user device, wherein the key comprises the second key; or

(iii) sending the request for the key to the network server from the server associated with the manufacturer of the user device and receiving a third key from the network server via the server associated with the manufacturer of the user device, wherein the network server generates the third key in real-time using the one or more cryptographic techniques, wherein the key comprise the third key;

generating, by the user device, a first cryptogram based on the phone number using the key;

sending, by the user device, the first cryptogram and a safety attestation certificate to the server associated with the manufacturer for verification, the safety attestation certificate indicating integrity of the user device; and

upon verification of the first cryptogram and the safety attestation certificate by the server associated with the manufacturer, receiving, by the user device, a second cryptogram from the server associated with the manufacturer, wherein the merchant application provides the second cryptogram and payment transaction details to an issuer server for authentication of the payment transaction.

2. The method of claim 1, wherein generating the first cryptogram is based on one or more encryption techniques using at least one of the phone number and a unique identification value associated with the user device and the first key.

3. The method of claim 1, wherein providing the first cryptogram to the server associated with the manufacturer triggers the server associated with the manufacturer to decrypt the first cryptogram using the first key and one or more decryption techniques corresponding to one or more encryption techniques used to generate the first cryptogram and to validate the phone number and a unique identification value associated with the user device based on user information stored in a database corresponding to the server associated with the manufacturer of the user device.

4. The method of claim 1, wherein the second cryptogram received by at least one processor from the server associated with the manufacturer is generated by the server associated with the manufacturer using the second key based on at least one of the phone number and a unique identification value associated with the user device, wherein the second key is obtained from the network server.

5. The method of claim 1, wherein providing the second cryptogram and the payment transaction details to the issuer server comprises sending the second cryptogram and the payment transaction details to the issuer server via at least one of the following: the network server, a direct integration with the issuer server, an Access Control Server (ACS), a Merchant Plug-In (MPI) provider, or any combination thereof.

6. The method of claim 1, further comprising:

receiving an authentication response from the issuer server after authentication of the payment transaction, wherein the authentication of the payment transaction comprises:

decrypting, by the issuer server, the second cryptogram using the second key, wherein the second key is obtained from the network server;

validating, by the issuer server, the phone number associated with the user device based on payer information stored in a database associated with the issuer server; and

providing, by the issuer server, the authentication response to the user device based on a result of the validation.

7. The method of claim 1, wherein a unique identification value comprises at least an International Mobile Equipment Identity (IMEI) number associated with the user device.

8. A user device for authenticating a payment transaction, comprising:

at least one processor; and

a memory communicatively coupled to the at least one processor, wherein the memory stores processor instructions, which, on execution, causes the at least one processor to:

receive a selection of a payment card of a plurality of payment cards stored in a merchant application of the user device for a payment transaction between a user of the user device and a merchant associated with the merchant application;

in response to receiving the selection of the payment card, initiate the payment transaction between the user and the merchant via the merchant application;

in response to receiving the selection of the payment card, receive a request for verifying a phone number associated with a Subscriber Identification Module (SIM) card in the user device from a merchant application installed in the user device;

in response to receiving the request, obtain the phone number from the SIM card and a key from at least one of a server associated with a manufacturer of the user device or a network server, wherein, when obtaining the key, the processor instructions further cause the at least one processor to:

send a request for the key to the server associated with the manufacturer of the user device; and

one of:

(i) receive a first key from the server associated with the manufacturer, wherein the server associated with the manufacturer generates the first key in real-time using one or more cryptographic techniques, wherein the key comprises the first key;

(ii) fetch a second key from a memory associated with the user device, wherein the second key was generated by the server associated with the manufacturer and stored in the memory associated with the user device during manufacturing of the user device, wherein the key comprises the second key; or

(iii) send the request for the key to the network server from the server associated with the manufacturer of the user device and receive a third key from the network server via the server associated with the manufacturer of the user device, wherein the network server generates the third key in real-time using the one or more cryptographic techniques, wherein the key comprises the third key;

generate a first cryptogram based on the phone number using the key;

send the first cryptogram and a safety attestation certificate to the server associated with the manufacturer for verification, the safety attestation certificate indicating integrity of the user device; and

upon verification of the first cryptogram and the safety attestation certificate by the server associated with the manufacturer, receive a second cryptogram from the server associated with the manufacturer, wherein the merchant application provides the second cryptogram and payment transaction details to an issuer server for authentication of the payment transaction.

9. The user device of claim 8, wherein the at least one processor is configured to generate the first cryptogram based on one or more encryption techniques using at least one of the phone number and a unique identification value associated with the user device and the first key.

10. The user device of claim 8, wherein the at least one processor is configured to provide the first cryptogram to the server associated with the manufacturer for triggering the server associated with the manufacturer to decrypt the first cryptogram using the first key and one or more decryption techniques corresponding to one or more encryption techniques used to generate the first cryptogram and to validate the phone number and a unique identification value associated with the user device based on user information stored in a database corresponding to the server associated with the manufacturer of the user device.

11. The user device of claim 8, wherein the at least one processor is configured to receive the second cryptogram generated by the server associated with the manufacturer using the second key based on at least one of the phone number and a unique identification value associated with the user device, wherein the second key is obtained from the network server.

12. The user device of claim 8, wherein the at least one processor is further configured to provide the second cryptogram and the payment transaction details to the issuer server comprises sending the second cryptogram and the payment transaction details to the issuer server via at least one of the following: the network server, a direct integration with the issuer server, Access Control Server (ACS), a Merchant Plug-In (MPI) provider, or any combination thereof.

13. The user device of claim 8, wherein the at least one processor is further configured to:

receive an authentication response from the issuer server after authentication of the payment transaction, wherein the authentication of the payment transaction comprises:

decrypting, by the issuer server, the second cryptogram using the second key, wherein the second key is obtained from the network server;

validating, by the issuer server, the phone number associated with the user device based on payer information stored in a database associated with the issuer server; and

providing, by the issuer server, the authentication response to the user device based on a result of the validation.