WHAT IS CLAIMED IS:

1. A computer-implemented method comprising:

receiving, by at least one processor, a device registration request and a device attestation response including a first token from a device, wherein the first token is sent by a first server to a second server, and wherein, in response to receiving the first token from the first server, the second server sends device information to the first server;

in response to the device registration request, providing, by the at least one processor, a device registration response to the device, wherein the device registration response is stored on the device;

receiving, by the at least one processor from the device, a first payment transaction request and an enrollment request to authenticate a second payment transaction request using a first type of authentication technique; and

enrolling, by the at least one processor, the device to the first type of authentication technique and providing a second token to the device based on a result of the first payment transaction request, wherein the second token is used for authenticating the second payment transaction request.

2. The computer-implemented method of claim 1, wherein providing the device registration response comprises:

validating, by the at least one processor, the device attestation response by verifying an origin of the device attestation response using one or more cryptographic techniques based on the first token; and

in response to successful validation, sending, by the at least one processor, the device registration response including at least a device identification value to the device; and

in response to unsuccessful validation, sending, by the at least one processor, the device registration response including at least an error message to the device.

3. The computer-implemented method of claim 1, wherein the enrollment request is received after:

the first server receives, from the device, the enrollment request including at least one of a consent for registering the device to the first type of authentication technique, merchant information, a payment amount, or payment card information, wherein the at least one processor

provides to the device at least one of a payment authentication request or an account identification value upon validation of the payment card information.

4. The computer-implemented method of claim 1, wherein receiving the first payment transaction request comprises:

receiving, by the at least one processor, at least one of a payment authentication request or a payment authorization request from the first server for completing a transaction associated between a user and a merchant using at least a payment card.

5. The computer-implemented method of claim 1, wherein the result of the first payment transaction request is received by the at least one processor after:

facilitating, by the at least one processor, processing of at least one of a payment authentication request and a payment authorization request based on one or more issuer authentication techniques.

6. The computer-implemented method of claim 1, wherein the enrollment of the device comprises:

verifying, by the at least one processor, a first payment authentication response received from the device with a second payment authentication response obtained while facilitating a payment authentication request based on one or more issuer authentication techniques;

in response to successful verification, enrolling the device to the first type of authentication technique; and

generating the second token for authenticating the second payment transaction request using the first type of authentication technique, wherein the generated second token is provided to the device.

7. A payment server for authenticating digital transactions, comprising:

at least one processor; and

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

receive a device registration request and a device attestation response including a first token from a device, wherein the first token is sent by a first server to a

second server, and wherein, in response to receiving the first token from the first server, the second server sends device information to the first server;

in response to the device registration request, provide a device registration response to the device, wherein the device registration response is stored on the device;

receive, from the device, a first payment transaction request and an enrollment request to authenticate a second payment transaction request using a first type of authentication technique; and

enroll the device to the first type of authentication technique and provide a second token to the device based on a result of the first payment transaction request, wherein the second token is used for authenticating the second payment transaction request.

8. The payment server of claim 7, wherein providing the device registration response comprises:

validating the device attestation response by verifying an origin of the device attestation response using one or more cryptographic techniques based on the first token;

in response to successful validation, sending, by the payment server, the device registration response including at least a device identification value to the device; and

in response to unsuccessful validation, sending, by the payment server, the device registration response including at least an error message to the device.

9. The payment server of claim 7, wherein the at least one processor is configured to receive the enrollment request after:

the first server receives, from the device, the enrollment request including at least a consent for registering the device to the first type of authentication technique, merchant information, a payment amount, and payment card information, wherein the at least one processor is configured to provide, to the application, at least one of a payment authentication request and an account identification value upon validation of the payment card information.

10. The payment server of claim 7, wherein receiving the first payment transaction request comprises:

receiving at least one of a payment authentication request and a payment authorization request from the first server, for completing a transaction associated between a user and a merchant using at least a payment card.

11. The payment server of claim 7, wherein the at least one processor is configured to receive the result of the first payment transaction request after processing of at least one of a payment authentication request and a payment authorization request based on one or more issuer authentication techniques.

12. The payment server of claim 7, wherein enrolling the device comprises:

verifying a first payment authentication response received from the device with a second payment authentication response obtained while facilitating a payment authentication request based on one or more issuer authentication techniques;

in response to successful verification, enrolling the device to the first type of authentication technique; and

generating the second token for authenticating the second payment transaction request using the first type of authentication technique, wherein the generated second token is provided to the device.

13. The payment server of claim 7, wherein the at least one processor is further configured to:

determine one or more authentication techniques associated with at least one issuer;

provide one or more determined authentication techniques to the device registered with the payment server, wherein the one or more authentication techniques are displayed in the application for user selection;

receive a second payment transaction request with one of the one or more authentication techniques selected by a user; and

provide a result of processing the second payment transaction request to the device, wherein the payment server facilitates the processing of the second payment transaction request.