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 at least a device integrity status from a device; in response to the device registration request, providing, by the at least one processor, a device registration response to the device, based on validation of the device integrity status; receiving, by the at least one processor from the device via an application, a first payment transaction request and an enrolment 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 method of claim 1, wherein the device registration request and the device attestation response are received after: the device provides, to a second server, a device attestation request including at least a first token; and the device receives, from the second server, the device attestation response including at least the device integrity status based on the first token.

3. The 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 a 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.

4. The method of claim 1, wherein the enrolment request is received after: a first server receives, via the application and from the device, the enrolment request including at least one of a consent for registering the application to the first type of authentication technique, merchant information, a payment amount, and payment card information, wherein the at least one processor provides to the application at least one of a payment authentication request and an account identification value upon validation of the payment card information.

5. The 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 and a payment authorization request from a first server for completing a transaction associated between a user and a merchant using at least a payment card.

6. The 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.

7. The 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 and the application 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.

8. A computer-implemented method comprising: determining, by at least one processor, one

or more authentication techniques associated with at least one issuer; providing, by the at least one processor, one or more determined authentication techniques to an application in a device, wherein the one or more authentication techniques are displayed in the application for user selection; receiving, by the at least one processor, a second payment transaction request with one of the one or more authentication techniques selected by a user; providing, by the at least one processor, a result of processing the second payment transaction request to the device; and facilitating, by the at least one processor, the processing of the second payment transaction request, wherein facilitating the processing of the second payment transaction request when the one of the one or more authentication techniques selected by the user is a first type of authentication technique comprises: receiving, by the at least one processor, the second payment transaction request including at least a device attestation response, a payment amount, a second token, merchant information, payment card information, a payment authentication request, and a payment authorization request; and generating, by the at least one processor, a third token upon processing the payment authentication request and the payment authorization request, wherein the generated third token is provided to the device for authenticating a third payment transaction.

9. The method of claim 8, wherein determining the one or more authentication techniques comprises: receiving, by the at least one processor and from the at least one issuer, a consent or a dissent for authenticating the second payment transaction request using the one or more authentication techniques; and identifying, by the at least one processor, the one or more authentication techniques having the consent of the at least one issuer.

10. The method of claim 8, wherein the one or more authentication techniques comprise at least one of a first type of authentication technique and one or more issuer authentication techniques.

11. The method of claim 8, wherein providing the one or more authentication techniques to

the application comprises: computing, by the at least one processor, a risk value for each of the determined one or more authentication techniques based on at least one of merchant information, issuer information, and user information; and modifying a consent of the determined one or more authentication techniques to a dissent based on the computed risk value being unacceptable, wherein the determined one or more authentication techniques are provided to the application.

12. 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 at least a device integrity status from a device; in response to the device registration request, provide a device registration response to the device, based on validation of the device integrity status; receive, from the device via an application, a first payment transaction request and an enrolment 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.

13. The payment server of claim 12, wherein the at least one processor is configured to receive the device registration request and the device attestation response after: the device provides, to a second server, a device attestation request including at least a first token; and the device receives, from the second server, the device attestation response including at least the device integrity status based on the first token.

14. The payment server of claim 12, 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 a 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.

15. The payment server of claim 12, wherein the at least one processor is configured to receive the enrolment request after: a first server receives, via the application and from the device, the enrolment request including at least a consent for registering the application 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.

16. The payment server of claim 12, wherein receiving the first payment transaction request comprises: receiving at least one of a payment authentication request and a payment authorization request from a first server, for completing a transaction associated between a user and a merchant using at least a payment card.

17. The payment server of claim 12, 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.

18. The payment server of claim 12, 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 and the application 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.

19. The payment server of claim 12, 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 an application in a 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.