WHAT IS CLAIMED IS:

1. A method comprising:

receiving, by a virtual terminal, virtual terminal configuration data from a virtual terminal configuration data source via a virtual terminal configurations API;

transmitting, by the virtual terminal, to a device reader, a value;

receiving, by the virtual terminal, encrypted access data from the device reader interacting with a user device,

wherein the virtual terminal is on a resource provider computer, which also comprises a software development kit, SDK, that decrypts the encrypted access data using a symmetric or asymmetric encryption key, and

wherein the SDK digitally signs the access data to form a digital signature and a browser plug-in in the virtual terminal validates the digital signature before further processing the access data;

the method further comprising:

transmitting, by the virtual terminal, a transaction request comprising at least the value and the access data to a transaction platform via a transaction API; and

receiving, by the virtual terminal, a transaction response from the transaction platform via the transaction API.

2. The method of claim 1, wherein the access data is an access token.

3. The method of claim 1, wherein the access data is a real credential.

4. The method of claim 1 further comprising:

responsive to receiving the access data from the user device via the device reader, transmitting a token request message comprising the access data to a token provider computer via a token service API; and

receiving a token response message comprising an access token from the token provider computer via the token service API.

5. The method of claim 1, wherein the virtual terminal configuration data source is a configurations application stored on the resource provider computer running the virtual terminal.

6. The method of claim 1, wherein the virtual terminal is operated by a resource provider.

7. The method of claim 1, wherein the user device is a card.

8. The method of claim 1, wherein the user device is a mobile phone.

9. A system comprising:

a resource provider computer comprising

one or more processors,

one or more non-transitory computer readable medium, the one or more non-transitory computer readable medium comprising instructions which can be executed by the one or processors to:

receive, by a virtual terminal, virtual terminal configuration data from a virtual terminal configuration data source via a virtual terminal configurations API;

transmit, by the virtual terminal, to a device reader, a value;

receive, by the virtual terminal, encrypted access data from the device reader interacting with a user device,

wherein the resource provider computer comprises a software development kit, SDK, that interfaces with the virtual terminal and that decrypts the encrypted access data using a symmetric or asymmetric encryption key, and

wherein the SDK digitally signs the access data to form a digital signature and a browser plug-in in the virtual terminal validates the digital signature before further processing the access data;

wherein the instructions can be further executed by the one or processors to:

transmit, by the virtual terminal, a transaction request comprising at least the value and the access data to a transaction platform via a transaction API; and

receive, by the virtual terminal, a transaction response from the transaction platform via the transaction API.

10. The system of claim 9, wherein the instructions further comprise:

transmitting a token request via a token request API to a token server computer.

11. The system of claim 10, wherein the instructions further comprise

receiving a token response via the token request API from the token server computer.

12. The system of claim 9, wherein the transaction platform comprises a transport computer.

13. The system of claim 9, wherein the SDK is programmed to perform encryption and decryption.