CLAIMS

1. A method for distributively installing a dynamic virtual card platform including a plurality of function modules using a plurality of devices capable of mutual communication, the method comprising:

a platform updating step of updating, by a first device, a first function module and a second function module associated with the first function module, the first function module and the second function module constituting a dynamic virtual card platform that operates valid; and

a platform distribution and installation step of storing, by the first device, the updated first function module only in the first device and providing the updated second function module to a remote security module.

2. The method of claim 1, wherein the first function module comprises an ISD module and the second function module comprises an APSD module.

3. The method of claim 1, further comprising before the platform updating step, receiving, by the first device, a request for financial payment preparation from a third device,

wherein the platform updating step is performed each time the request is received, and

the third device and the security module are capable of communicating with each other.

4. The method of claim 3, wherein the first device is a server and

the security module is a security device capable of communicating with the third device or a module implemented by software in the third device,

wherein in the platform distribution and installation step, the second function module is provided to the security module using wire communication or wireless communication between the first device and the third device.

5. A virtual card creation method for dynamically creating a virtual card using a plurality of devices capable of mutual communication, the method comprising:

a platform updating step of updating, by a first device, a first function module and a

second function module associated with the first function module, the first function module and the second function module constituting a dynamic virtual card platform that operates valid;

a platform distribution and installation step of storing, by the first device, the updated first function module only in the first device and providing the updated second function module to a remote security module.

a payment application updating step of updating, by the first device, a value storage module constituting a dynamic virtual payment application that operates in the dynamic virtual card platform and a relay module associated with the value storage module; and

a payment application distribution and installation step of storing, by the first device, the updated value storage module only in the first device and providing the updated relay module to the security module,

wherein the relay module is configured to perform a function of relaying a payment transaction using a financial value stored in the value storage module by a third device communicating with the security module.

6. The method of claim 5, wherein when the payment transaction is performed, in order to invalidate the updated dynamic virtual card platform and the virtual card defined by the updated payment application,

when the payment transaction is performed, the updated dynamic virtual card platform is configured to be invalidated.

7. The method of claim 5, further comprising receiving, by the first device, a request for financial payment preparation from the third device before the platform updating step and the payment application updating step,

wherein the platform updating step and the payment application updating step are performed each time the request is received.

8. The method of claim 5, wherein the payment application updating step comprises:

dividing the updated relay module into a plurality of segments;

creating a digital signature value from the plurality of segments;

encrypting the plurality of segments using one or more keys; and

scrambling the plurality of encrypted segments,

wherein the payment application distribution and installation step comprises providing the scrambled information to the security module, and

the one or more keys and the digital signature value are provided to the security module.

9. The method of claim 8, wherein the security module is configured to perform:

descrambling the scrambled information;

decrypting the descrambled information using the one or more keys;

verifying the decrypted information using the digital signature value; and

installing the relay module in the security module using the verified decrypted information.