CLAIMS

What is claimed is:

1. A digital certificate application method, applied to a client device, wherein the client device integrates a secure element and is loaded with client software, the method comprising:

sending, by the client device, a digital certificate application request to a server, wherein the server generates application information based on the application request and returns the application information to the client device, and wherein the application information comprises an application identifier uniquely corresponding to the application request;

delivering, by the client device, the application information returned by the server to the secure element;

generating, by the secure element, a pair of public and private keys based on an asymmetric algorithm;

signing, by the secure element, the application identifier using the private key to obtain terminal signature data;

encapsulating, by the secure element, the terminal signature data and the public key into a specified format and sending the specified format data to the client device; and

sending, by the client device, the specified format data to the server, wherein the server sends the public key, the terminal signature data, login user information of the client, and certificate usage information to a certificate authority after determining, based on the public key, that the terminal signature data and the application identifier are verified.

2. The method according to claim 1, wherein:

the application information further comprises asymmetric algorithm information and signature algorithm information; and

generating, by the secure element, a pair of public and private keys based on an asymmetric algorithm and signing, by the secure element, the application identifier using the private key to obtain terminal signature data comprises:

generating, by the secure element, the pair of public and private keys based on the asymmetric algorithm information in the application information,

calculating a security key length and a digest of the application identifier using the signature algorithm information in the application information, and

signing the digest by using the private key to obtain the terminal signature data.

3. The method according to claim 1, wherein the specified format is a type length value format.

4. A digital certificate application method, applied to a server, wherein the server is configured to interact with client software loaded on a client device, wherein the client device further integrates a secure element, the method comprising:

after receiving a digital certificate application request sent by the client device, generating application information and sending the application information to the client device and a certificate authority, wherein the application information comprises an application identifier uniquely corresponding to the application request;

receiving specified format data sent by the client device, wherein the specified format data is obtained after the secure element generates a pair of public and private keys, signs the application identifier by using the private key to obtain terminal signature data, and encapsulates the terminal signature data and the public key;

parsing the specified format data and verifying the terminal signature data based on the public key to obtain the application identifier in the terminal signature data; and

sending the public key, the terminal signature data, login user information of the client, and certificate usage information to the certificate authority after the terminal signature data and the application identifier are verified, wherein the certificate authority generates a digital certificate after determining that the terminal signature data and the application identifier are verified.

5. The method according to claim 4, wherein the application information further comprises asymmetric algorithm information and signature algorithm information, wherein the asymmetric algorithm information and signature algorithm information are used by the secure element to generate the pair of public and private keys for signing.

6. The method according to claim 4, wherein the public key is encapsulated into a PKCS1 format by the server.

7. The method according to claim 4, further comprising:

sending server signature data to the certificate authority for verification when the

terminal signature data and the application identifier are verified; wherein

the server signature data is generated after the server uses a server private key to sign server information.

8. The method according to claim 4, wherein the application identifier is carried in an exchange process of the digital certificate application and is used to identify the current digital certificate application.

9. The method according to claim 4, wherein the method further comprises, after receiving the specified format data sent by the client device:

extracting, by the server, the security key length, the public key, and the terminal signature data from the specified format data;

verifying the terminal signature data using the public key;

obtaining a security key length in the terminal signature data;

verifying whether the obtained security key length is consistent with the security key length extracted from the specified format; and

if yes, determine that the security key length is verified.

10. The method according to claim 9, further comprising, in response to verifying the terminal signature data and determining that the security key length is verified, determining that the public key is secure and the specified format is not tampered with.

11. The method according to claim 10, further comprising determining whether the application identifier is verified, and in response to determining that the application identifier is verified, determining that the client device is verified.

12. The method according to claim 4 or claim 11, wherein in response to determining that the terminal signature data or the application identifier fails in verification, the method further comprises:

confirming that the digital certificate application has a security risk; and

retuning an application failure message to the client device.

13. A digital certificate application device, applied to a terminal device, wherein the terminal device further integrates a secure element, and the device comprises multiple units configured to perform the method according to any one of claims 1 to 3.

14. A digital certificate application device, applied to a server, wherein the device is configured to interact with client software loaded on a terminal device, the terminal device further integrates a secure element, and the device comprises multiple units configured to perform the method according to any one of claims 4 to 12.

15. A digital certificate application device, applied to a client device, wherein the device comprises:

a secure element;

a processor; and

a memory configured to store a machine executable instruction; wherein by reading and executing the machine executable instruction that is stored in the memory and corresponding to digital certificate application logic, the processor is enabled to:

send a digital certificate application request to a server, wherein the server generates application information based on the application request and returns the application information, and wherein the application information comprises an application identifier uniquely corresponding to the application request;

deliver the application information returned by the server to the secure element, wherein the secure element generates a pair of public and private key based on an asymmetric algorithm, uses the private key to sign the application identifier to obtain terminal signature data, and encapsulates the terminal signature data and the public key into a specified format and returns the specified format data; and

send the specified format data to the server, wherein the server sends the public key, the terminal signature data, login user information, and certificate usage information to a certificate authority after determining, based on the public key, that the terminal signature data and the application identifier are verified.

16. A digital certificate application device, applied to a server, wherein the device comprises:

a processor; and

a memory configured to store a machine executable instruction; wherein by reading and executing the machine executable instruction that is stored in the memory and corresponding to digital certificate application logic, the processor is enabled to:

generate and send application information to a client device and a certificate authority after receiving a digital certificate application request sent by the client device, wherein the application information comprises an application identifier uniquely corresponding to the application request;

receive specified format data sent by the client device, wherein the specified format data is obtained after a secure element generates a pair of public and private keys, signs the application identifier by using the private key to obtain terminal signature data, and encapsulates the terminal signature data and the public key;

parse the specified format data and verify the terminal signature data based on the public key to obtain the application identifier in the terminal signature data; and

send the public key, the terminal signature data, login user information of the client device, and certificate usage information to the certificate authority after the terminal signature data and the application identifier are verified, wherein the certificate authority generates a digital certificate after determining that the terminal signature data and the application identifier are verified.