CLAIMS

What is claimed is:

1. A computer-implemented method for generating two-dimensional codes, comprising:

receiving, by a secure element chip, security data sent by a server, wherein the security data is obtained by the server based on an account associated with a two-dimensional code display device;

storing, by the secure element chip, the security data;

receiving, by the secure element chip, a code refresh notification sent by the server in response to the server identifying a code scanning event trigger;

in response to receiving the code refresh notification, transmitting, by the secure element chip, the security data to at least one processor comprised in the two-dimensional code display device for generating code information based on the security data;

receiving, by the secure element chip, the code information comprising an account identifier of the account associated with the two-dimensional code display device;

in response to obtaining a digital certificate for a private key stored in the secure element chip, signing, by the security element chip, the code information by using the private key to generate signed code information; and

providing, the signed code information to the two-dimensional code display device for the two-dimensional code display device to generate and display a two-dimensional code based on the code information, wherein the two-dimensional code comprises information associated with the account identifier and changes dynamically over time.

2. The computer-implemented method according to claim 1, wherein the security data is transmitted to the at least one processor at predetermined intervals.

3. The computer-implemented method according to claim 1, further comprising:

before receiving the security data, generating, by the secure element chip, a public-private key pair;

uploading, by the secure element chip, a public key to the server for the server to send the public key to a certificate authority for authentication of the public key; and

receiving, by the secure element chip from the server, a digital certificate indicating that the public key is authenticated.

4. The computer-implemented method according to claim 1, wherein the two-dimensional code changes dynamically according to changes of the code information generated by the at least one processor.

5. The computer-implemented method according to claim 1, wherein the two-dimensional code changes dynamically according to changes of the code information incurred by at least one of mixing one or more random numbers with the code information or mixing one or more timestamps with the code information.

6. A non-transitory, computer-readable medium storing one or more instructions executable by a computer system to perform operations comprising:

receiving, by a secure element chip, security data sent by a server, wherein the security data is obtained by the server based on an account associated with a two-dimensional code display device;

storing, by the secure element chip, the security data;

receiving, by the secure element chip, a code refresh notification sent by the server in response to the server identifying a code scanning event trigger;

in response to receiving the code refresh notification, transmitting, by the secure element chip, the security data to at least one processor comprised in the two-dimensional code display device for generating code information based on the security data;

receiving, by the secure element chip, the code information comprising an account identifier of the account associated with the two-dimensional code display device;

in response to obtaining a digital certificate for a private key stored in the secure element chip, signing, by the security element chip, the code information by using the private key to generate signed code information; and

providing, the signed code information to the two-dimensional code display device for the two-dimensional code display device to generate and display a two-dimensional code based on the code information, wherein the two-dimensional code comprises information associated with the account identifier and changes dynamically

over time.

7. The non-transitory, computer readable medium according to claim 6, wherein the security data is transmitted to the at least one processor at predetermined intervals.

8. The non-transitory, computer-readable medium according to claim 6, the operations further comprising:

before receiving the security data, generating, by the secure element chip, a public-private key pair;

uploading, by the secure element chip, a public key to the server for the server to send the public key to a certificate authority for authentication of the public key; and

receiving, by the secure element chip from the server, a digital certificate indicating that the public key is authenticated.

9. The non-transitory, computer-readable medium according to claim 6, wherein the two-dimensional code changes dynamically according to changes of the code information generated by the at least one processor.

10. The non-transitory, computer-readable medium according to claim 6, wherein the two-dimensional code changes dynamically according to changes of the code information incurred by at least one of mixing one or more random numbers with the code information or mixing one or more timestamps with the code information.

11. A computer-implemented system, comprising:

one or more computers; and

one or more computer memory devices interoperably coupled with the one or more computers and having tangible, non-transitory, machine-readable media storing one or more instructions that, when executed by the one or more computers, perform one or more operations comprising:

receiving, by a secure element chip, security data sent by a server, wherein the security data is obtained by the server based on an account associated with a two-dimensional code display device;

storing, by the secure element chip, the security data;

receiving, by the secure element chip, a code refresh notification sent by the

server in response to the server identifying a code scanning event trigger;

in response to receiving the code refresh notification, transmitting, by the secure element chip, the security data to at least one processor comprised in the two-dimensional code display device for generating code information based on the security data;

receiving, by the secure element chip, the code information comprising an account identifier of the account associated with the two-dimensional code display device;

in response to obtaining a digital certificate for a private key stored in the secure element chip, signing, by the security element chip, the code information by using the private key to generate signed code information; and

providing, the signed code information to the two-dimensional code display device for the two-dimensional code display device to generate and display a two-dimensional code based on the code information, wherein the two-dimensional code comprises information associated with the account identifier and changes dynamically over time.

12. The computer-implemented system according to claim 11, wherein the security data is transmitted to the at least one processor at predetermined intervals.

13. The computer-implemented system according to claim 11, the operations further comprising:

before receiving the security data, generating, by the secure element chip, a public-private key pair;

uploading, by the secure element chip, a public key to the server for the server to send the public key to a certificate authority for authentication of the public key; and

receiving, by the secure element chip from the server, a digital certificate indicating that the public key is authenticated.

14. The computer-implemented system according to claim 11, wherein the two-dimensional code changes dynamically according to changes of the code information generated by the at least one processor.

15. The computer-implemented system according to claim 11, wherein the two-

dimensional code changes dynamically according to changes of the code information incurred by at least one of mixing one or more random numbers with the code information or mixing one or more timestamps with the code information.