CLAIMS

1. A method for generating a two-dimensional code, the method being executed by a second server and comprising:

receiving a two-dimensional code generation request from a first server, the request comprising information for generating a two-dimensional code;

digitally signing the information for generating the two-dimensional code; and

sending the digitally signed information to the first server.

2. The method of claim 1, wherein before the step of receiving a two-dimensional code generation request from a first server, the method further comprises receiving a registration request from the first server, the registration request comprising information related to the current registration.

3. The method of claim 2, wherein after the step of receiving a registration request from the first server, the method further comprises:

completing registration of the first server according to the registration request after successfully verifying the information related to the current registration.

4. The method of claim 3, further comprising storing the registration information.

5. The method of claim 3 or 4, wherein before the step of digitally signing the information for generating the two-dimensional code, the method further comprises:

determining whether the first server is registered at the second server, wherein:

if yes, digitally signing the information for generating the two-dimensional code according to the received two-dimensional code generation request; and

if no, not digitally signing the information for generating the two-dimensional code, and sending a registration invitation to the first server.

6. The method of any one of claims 1 to 5, wherein the step of digitally signing the information for generating the two-dimensional code comprises digitally signing, on the basis of an asymmetric encryption algorithm and by using a private key, the information for generating the two-dimensional code.

7. The method of claim 6, wherein the asymmetric encryption algorithm comprises a RSA algorithm.

8. The method of claim 6, wherein according to different information for generating the two-dimensional code, different respective private keys are used in the step of digitally signing the information for generating the two-dimensional code.

9. The method of any one of claims 1 to 8, further comprising:

starting an application corresponding to the second server;

scanning the two-dimensional code using a scanning unit in the application;

verifying the scanned two-dimensional code using a public key; and

recognizing information corresponding to the scanned two-dimensional code if the verification succeeds.

10. The method of claim 9, further comprising determining that the two-dimensional code has been tampered if the verification is unsuccessful.

11. The method of claim 9, wherein the public key is obtained from the second server or a remote storage device.

12. The method of claim 9, further comprising storing information related to the verification step.

13. A method for generating a two-dimensional code, the method being executed by a first server and comprising:

sending a two-dimensional code generation request to a second server, the request comprising information for generating a two-dimensional code;

receiving, from the second server, two-dimensional code information comprising a digital signature generated by the second server; and

generating a two-dimensional code by using the two-dimensional code information.

14. The method of claim 13, wherein before the step of sending a two-dimensional code generation request to a second server, the method further comprises sending a registration request to the second server, the registration request comprising information related to current registration.

15. An electronic device, comprising:

a first server comprising multiple units configured to perform the method of claim 13 or 14; and

a second server comprising multiple units configured to perform the method of any one of claims 1 to 12.