signature data. The code scanning device sends the code scanning result to the CA. The CA obtains first digest data by performing a hash operation on the two-dimensional code generation data, identifies the public key corresponding to the private key by using the identifier of the SE, and verifies the signature data by using the public key to obtain second digest data. When the first digest data is the same as the second digest data, it indicates that the target two-dimensional code is generated by the electronic device corresponding to the identifier of the SE, and is not tampered with.

[0041] Optionally, when the predetermined signature algorithm is an encryption-based one-time signature algorithm, the obtaining signature data based on a predetermined signature algorithm stored in the secure element includes: obtaining a one-time encryption password based on a shared key stored in the secure element, where the one-time encryption password is the signature data.

[0042] In some embodiments of the present specification, when the predetermined signature algorithm is the encryption-based one-time signature algorithm, the signature algorithm can be an HOTP algorithm. The SE can store the shared key, and the key is shared by the SE and an authentication server. A one-time encryption password can be generated based on the shared key. In some embodiments, a counter is disposed in the electronic device, and the one-time encryption password is obtained by performing a hash-based message authentication code (HMAC) operation based on the shared key and a value of the counter. It should be understood that a different one-time encryption password is generated each time, and therefore security of each signature addition process can be ensured. In addition, on the authentication server, a password is also generated based on the shared key and the value of the counter. When the password is the same as the one-time encryption password generated by the SE, it indicates that data is not tampered with.

[0043] When the signature data is the one-time encryption password, the target two-dimensional code is generated based on the two-dimensional code generation data and the one-time encryption password.

[0044] Optionally, after the signature data is obtained by adding the digital signature to the to-be-signed data based on the private key, the method further includes: generating a one-time encryption password based on a shared key stored in the secure element; and the generating a target two-dimensional code based on the two-dimensional code generation data and the signature data includes: generating the

CLAIMS

1. A two-dimensional code generation method, applied to an electronic device, wherein a secure element is disposed in the electronic device, and the method comprises:
obtaining (S21), using the secure element, two-dimensional code generation data stored in the secure element when a two-dimensional code generation request is received, wherein the two-dimensional code generation data comprises account data of a user corresponding to the electronic device and timestamp data of the electronic device;
obtaining signature data (S22) based on a predetermined signature algorithm stored in the secure element; and
generating a target two-dimensional code (S23) based on the two-dimensional code generation data and the signature data.

2. The two-dimensional code generation method according to claim 1, wherein before the obtaining signature data (S22) based on a predetermined signature algorithm stored in the secure element, the method further comprises:
obtaining to-be-signed data; and
the obtaining signature data based on a predetermined signature algorithm stored in the secure element comprises: obtaining the signature data by adding a digital signature to the to-be-signed data based on the predetermined signature algorithm.

3. The two-dimensional code generation method according to claim 2, wherein when the predetermined signature algorithm is a public key infrastructure-based signature algorithm, the obtaining the signature data (S22) by adding a digital signature to the to-be-signed data based on the predetermined signature algorithm comprises:
obtaining a private key generated by the secure element; and
obtaining the signature data by adding the digital signature to the to-be-signed data based on the private key.

4. The two-dimensional code generation method according to claim 1, wherein when the predetermined signature algorithm is an encryption-based one-time signature algorithm, the obtaining signature data (S22) based on a predetermined signature algorithm stored in the secure element comprises:
obtaining a one-time encryption password based on a shared key stored in the secure element, wherein the one-time encryption password is the signature data and the target two-dimensional code is generated (S23) based on the two-dimensional code generation data and the one-time encryption password.

5. The two-dimensional code generation method according to claim 3, wherein after the obtaining the signature data by adding the digital signature to the to-be-signed data based on the private key, the method further comprises:
generating a one-time encryption password based on a shared key stored in the secure element; and
the generating a target two-dimensional code (S23) based on the two-dimensional code generation data and the signature data comprises:
generating the target two-dimensional code based on the two-dimensional code generation data, the signature data, and the one-time encryption password.

6. A data processing method, wherein the data processing method comprises:
receiving two-dimensional code scanning data (S31) obtained by scanning a target two-dimensional code through a target electronic device, wherein the target two-dimensional code is a two-dimensional code generated by using the method according to any one of claims 1 to 5, and the two-dimensional code scanning data comprises signature data and two-dimensional code generation data for generating the target two-dimensional code; and
verifying the signature data (S32) based on a signature method of the signature data to obtain a verification result.

7. The data processing method according to claim 6, wherein when the signature method is a public key infrastructure-based signature method, the verifying the signature data (S32) based on a signature method of the signature data to obtain a verification result comprises:

verifying the signature data based on a public key corresponding to the signature data to obtain the verification result.

8. The data processing method according to claim 6, wherein when the signature method is an encryption-based one-time signature method, the verifying the signature data (S32) based on a signature method of the signature data to obtain a verification result comprises:
obtaining a target one-time encryption password based on a shared key corresponding to the signature data; and
verifying the signature data based on the target one-time encryption password to obtain the verification result.

9. The data processing method according to claim 6, wherein after the receiving two-dimensional code scanning data (S31) obtained by scanning a target two-dimensional code through a target electronic device, the method further comprises:
obtaining target timestamp data for receiving the two-dimensional code scanning data;
obtaining initial timestamp data in the two-dimensional code generation data; and
determining whether the two-dimensional code is valid based on a target time difference between the target timestamp data and the initial timestamp data and a predetermined time difference, wherein it is determined that the target two-dimensional code is valid when the target time difference is less than or equal to the predetermined time difference, or it is determined that the target two-dimensional code is invalid when the target time difference is greater than the predetermined time difference.

10. The data processing method according to claim 9, wherein when the target two-dimensional code is a collection code, after the obtaining a verification result, the method further comprises:
obtaining account data in the two-dimensional code generation data when the verification result indicates a verification success; and

updating an amount in the account data based on a collection amount corresponding to the collection code.

11. A two-dimensional code generation apparatus, comprising a memory, a processor, and a computer program that is stored in the memory and can run on the processor, wherein when the processor executes the program, the steps of the method according to any one of claims 1 to 5 are implemented.

12. A system, comprising a server configured to perform a method according to any one of claims 6 to 10, and a two-dimensional code generation apparatus according to claim 11.

13. A computer-readable storage medium, wherein the computer-readable storage medium stores a computer program, and when the program is executed by a processor, the steps of the method according to any one of claims 1 to 10 are implemented.