WHAT IS CLAIMED IS:

1. A method for establishing security infrastructure, comprising:

receiving, by an intermediate service organization, an organization secret key sent by a third-party service organization;

encrypting, by the intermediate service organization, the organization secret key by a first encryption means; wherein the first encryption means is to use a service private key of the intermediate service organization to sign the organization secret key and use a root public key of a terminal to encrypt the signed organization secret key;

sending, by the intermediate service organization, the encrypted organization secret key to a secure storage region of the terminal;

receiving, by the intermediate service organization, a first terminal public key encrypted by the terminal using a second encryption means, wherein the second encryption means is to use a root private key of the terminal to sign the first terminal public key and use a service public key of the intermediate service organization to encrypt the signed first terminal public key; and

sending, by the intermediate service organization, the first terminal public key obtained by decryption to the third-party service organization.

2. The method of claim 1, wherein before the receiving, by the intermediate service organization, the organization secret key sent by the third-party service organization, the method further comprises:

sending, by the intermediate service organization, the service public key to the secure storage region of the terminal;

receiving, by the intermediate service organization, the root public key encrypted by the terminal using a third encryption means, wherein the third encryption means is to use the root private key to sign the root public key and use the service public key to encrypt the signed root public key; and

decrypting, by the intermediate service organization, to obtain the root public key.

3. A method for establishing security infrastructure, comprising:

receiving, by a terminal, an organization secret key of a third-party service organization encrypted by an intermediate service organization using a first encryption means, wherein the first encryption means is to use a service private key of the intermediate service organization to sign the organization secret key and use a root public key of the terminal to encrypt the signed organization secret key;

decrypting, by the terminal, to obtain the organization secret key by using a root private key

of the terminal and a service public key of the intermediate service organization;

storing, by the terminal, the organization secret key in a secure storage region of the terminal;

encrypting, by the terminal, a first terminal public key by a second encryption means, wherein the second encryption means is to use the root private key of the terminal to sign the first terminal public key and use the service public key of the intermediate service organization to encrypt the signed first terminal public key; and

sending, by the terminal, the encrypted first terminal public key to the intermediate service organization.

4. The method of claim 3, wherein before the receiving, by the terminal, the organization secret key of the third-party service organization encrypted by the intermediate service organization using the first encryption means, the method further comprises:

receiving, by the terminal, the service public key sent by the intermediate service organization;

storing, by the terminal, the service public key in the secure storage region;

encrypting, by the terminal, the root public key by a third encryption means, wherein the third encryption means is to use the root private key to sign the root public key and use the service public key to encrypt the signed root public key; and

sending, by the terminal, the encrypted root public key to the intermediate service organization.

5. The method of claim 4, wherein after the sending, by the terminal, the encrypted first terminal public key to the intermediate service organization, the method further comprises:

receiving, by the terminal, an application secret key encrypted by the third-party service organization using a fourth encryption means, wherein the fourth encryption means is to use an organization private key to sign the application secret key and use the first terminal public key to encrypt the signed application secret key;

decrypting, by the terminal, to obtain the application secret key by using a first terminal private key and an organization public key; wherein the organization secret key comprises the organization public key;

storing, by the terminal, the application secret key in the secure storage region of the terminal; and

sending, by the terminal, a second terminal public key encrypted by a fifth encryption means to the third-party service organization, wherein the fifth encryption means is to use a second terminal private key to sign the second terminal public key and use the organization

public key to encrypt the signed second terminal public key.

6. The method of claim 5, further comprising:

generating, by the terminal, the root public key, the root private key, the first terminal public key, the first terminal private key, the second terminal public key, and the second terminal private key corresponding to the third-party service organization in an onboard manner.

7. The method of claim 5, further comprising:

receiving, by the terminal, an access request of a third-party application that is an application corresponding to the third-party service organization;

generating, by the terminal, check content;

sending, by the terminal, the check content to the third-party service organization;

receiving, by the terminal, a checking instruction sent by the third-party service organization, wherein the checking instruction is obtained by the third-party service organization using an application private key to sign the check content;

performing, by the terminal, signature verification on the checking instruction by using an application public key; wherein the application secret key comprises the application public key;

allowing, by the terminal, the third-party application to access a secure region of the terminal after the verification passes.

8. The method of any one of claims 3 to 7, wherein the secure storage region of the terminal is a Secure Element, SE, or Trusted Execution Environment, TEE.

9. A method for establishing security infrastructure, comprising:

encrypting, by a third-party service organization, an application public key by a fourth encryption means; wherein the fourth encryption means is to use an organization private key to sign the application public key and use a first terminal public key to encrypt the signed application public key;

sending, by the third-party service organization, the encrypted application public key to a terminal; and

receiving, by the third-party service organization, a second terminal public key encrypted by the terminal using a fifth encryption means, wherein the fifth encryption means is to use a second terminal private key to sign the second terminal public key and use an organization public key to encrypt the signed second terminal public key.

10. The method of claim 9, further comprising:

sending, by the third-party service organization, an access request to the terminal through a third-party application that is an application corresponding to the third-party service organization;

receiving, by the third-party service organization, check content sent by the terminal;

signing, by the third-party service organization, the check content by using an application private key to generate a checking instruction;

sending, by the third-party service organization, the checking instruction to the terminal, so that the terminal performs signature verification on the checking instruction by using the application public key; and

allowing the third-party application to access a secure region of the terminal after the verification passes.

11. An electronic device, comprising a processor, a memory, a transceiver and a bus interface, wherein the processor, the memory and the transceiver are connected through buses;

the transceiver is configured to receive an organization secret key sent by a third-party service organization; receive a first terminal public key encrypted by a terminal using a second encryption means, and send the first terminal public key obtained by decryption to the third-party service organization; wherein the second encryption means is to use a root private key of the terminal to sign the first terminal public key and use a service public key of the intermediate service organization to encrypt the signed first terminal public key;

the processor is configured to read a program in the memory to perform following operations: encrypting the organization secret key by a first encryption means, and sending the encrypted organization secret key to a secure storage region of a terminal, wherein the first encryption means is to use a service private key of the intermediate service organization to sign the organization secret key and use a root public key of the terminal to encrypt the signed organization secret key; and

the memory is configured to store one or more executable programs and store data used by the processor when performing the operations.

12. The electronic device of claim 11, wherein the transceiver is further configured to:

send the service public key to the secure storage region of the terminal; and receive the root public key encrypted by the terminal using a third encryption means, wherein the third encryption means is to use the root private key to sign the root public key and use the service public key to encrypt the signed root public key; and

the processor is further configured to decrypt to obtain the root public key.

13. An electronic device, comprising a processor, a memory, a transceiver and a bus interface, wherein the processor, the memory, the transceiver and the bus interface are connected through buses;

the transceiver is configured to receive an organization secret key of a third-party service

organization encrypted by an intermediate service organization using a first encryption means, and send an encrypted first terminal public key to the intermediate service organization; wherein the first encryption means is to use a service private key of the intermediate service organization to sign the organization secret key and use a root public key of the terminal to encrypt the signed organization secret key;

the processor is configured to decrypt to obtain the organization secret key by using a root private key of the terminal and a service public key of the intermediate service organization, and store the organization secret key in a secure storage region of the terminal; and encrypt a first terminal public key by a second encryption means, wherein the second encryption means is to use the root private key of the terminal to sign the first terminal public key and use the service public key of the intermediate service organization to encrypt the signed first terminal public key.

14. The electronic device of claim 13, wherein the transceiver is further configured to: receive the service public key sent by the intermediate service organization, and store the service public key in the secure storage region; and send an encrypted root public key to the intermediate service organization; and

the processor is further configured to encrypt the root public key by a third encryption means, wherein the third encryption means is to use the root private key to sign the root public key and use the service public key to encrypt the signed root public key.

15. The electronic device of claim 14, wherein the transceiver is further configured to: receive an application secret key encrypted by the third-party service organization using a fourth encryption means, and send a second terminal public key encrypted by a fifth encryption means to the third-party service organization; wherein the fourth encryption means is to use an organization private key to sign the application secret key and use the first terminal public key to encrypt the signed application secret key, and the fifth encryption means is to use a second terminal private key to sign the second terminal public key and use an organization public key to encrypt the signed second terminal public key; and

the processor is further configured to decrypt to obtain the application secret key by using a first terminal private key and the organization public key, and store the application secret key in the secure storage region of the terminal; wherein the organization secret key comprises the organization public key.

16. The electronic device of claim 15, wherein the processor is further configured to:

generate the root public key, the root private key, the first terminal public key, the first terminal private key, the second terminal public key, and the second terminal private key

corresponding to the third-party service organization in an onboard manner.

17. The electronic device of claim 15, wherein the transceiver is further configured to:

receive an access request of a third-party application that is an application corresponding to the third-party service organization; and receive a checking instruction sent by the third-party service organization, wherein the checking instruction is obtained by the third-party service organization using an application private key to sign the check content;

the processor is further configured to:

generate check content and send the check content to the third-party service organization; perform signature verification on the checking instruction by using an application public key; and allow the third-party application to access a secure region of the terminal after the verification passes; wherein the application secret key comprises the application public key.

18. The electronic device of any one of claims 13 to 17, wherein the secure storage region of the terminal is a Secure Element, SE, or Trusted Execution Environment, TEE.

19. An electronic device, comprising a processor, a memory, a transceiver and a bus interface, wherein the processor, the memory, the transceiver and the bus interface are connected through buses;

the processor is configured to encrypt an application public key by a fourth encryption means, and send the encrypted application public key to a terminal, wherein the fourth encryption means is to use an organization private key to sign the application public key and use a first terminal public key to encrypt the signed application public key; and

the transceiver is configured to receive a second terminal public key encrypted by the terminal using a fifth encryption means, wherein the fifth encryption means is to use a second terminal private key to sign the second terminal public key and use an organization public key to encrypt the signed second terminal public key.

20. The electronic device of claim 19, wherein the transceiver is further configured to:

send an access request to the terminal through a third-party application that is an application corresponding to the electronic device; receive check content sent by the terminal, and instruct the processor to sign the check content by using an application private key to generate a checking instruction; send the checking instruction to the terminal, so that the terminal performs signature verification on the checking instruction by using the application public key; and instruct the processor to allow the third-party application to access a secure region of the terminal after the verification passes.