

CLAIMS

What is claimed is:

1. A service authorization method, wherein a system of a device comprises at least a first security environment and a second security environment, a first execution
5 unit runs in the first security environment, a second execution unit runs in the second security environment, and the method comprises:

obtaining information to be verified, and sending the information to be verified to the first execution unit for verification;

receiving signature information that is returned by the first execution unit and
10 obtained by signing a verification result by means of a signature verification private key; and

sending the signature information to the second execution unit, so that the second execution unit verifies the signature information by means of a signature verification public key corresponding to the signature verification private key, and performs
15 service authorization based on the verification result after it is determined that the verification on the signature information succeeds.

2. The method according to claim 1, wherein the first security environment comprises a trusted execution environment (TEE), and the second security environment comprises an execution environment provided by a secure element (SE).

20 3. The method according to claim 1 or 2, wherein the information to be verified comprises biometric feature information to be verified.

4. The method according to claim 1 or 2, wherein before the receiving signature information that is returned by the first execution unit and obtained by signing a verification result by means of a signature verification private key, the method further
25 comprises:

obtaining a dynamic parameter sent by the second execution unit, wherein the dynamic parameter comprises at least one of a random number or time information; and

sending the dynamic parameter to the first execution unit, so that the first
30 execution unit signs the verification result and the dynamic parameter by means of the signature verification private key.

5. A service authorization method, wherein a system of a device comprises at least a first security environment and a second security environment, a first execution unit runs in the first security environment, a second execution unit runs in the second security environment, and the method comprises:

5 obtaining, by the second execution unit, signature information sent by the first execution unit by using a service application, wherein the signature information is obtained after the first execution unit signs a verification result by means of a signature verification private key, and the verification result is obtained after the first execution unit verifies information to be verified sent by the service application; and

10 verifying the signature information by means of a signature verification public key corresponding to the signature verification private key, and performing, after it is determined that the verification on the signature information succeeds, service authorization based on the verification result obtained by parsing the signature information.

15 6. The method according to claim 5, wherein the signature verification public key is obtained by the second execution unit from a first management server corresponding to the first execution unit by using a second management server corresponding to the second execution unit.

20 7. The method according to claim 5, wherein before the verifying the signature information by means of a signature verification public key corresponding to the signature verification private key, the method further comprises:

obtaining a CA public key from a certificate authority (CA) by using a second management server corresponding to the second execution unit.

25 8. The method according to claim 7, wherein the verifying the signature information by means of a signature verification public key corresponding to the signature verification private key, and performing, after it is determined that the verification on the signature information succeeds, service authorization based on the verification result obtained by parsing the signature information comprises:

30 verifying, by means of the CA public key, a public key certificate sent from the service application, wherein the public key certificate is obtained after the CA verifies the signature verification public key based on a CA private key corresponding to the CA public key, the public key certificate is obtained by the service application from the first execution unit, and the public key certificate is obtained by the first execution unit from the CA by using a first management server corresponding to the

first execution unit; and

verifying, after it is determined that the verification on the public key certificate succeeds, the signature information by means of the signature verification public key obtained by parsing the public key certificate, and performing, after it is
5 determined that the verification on the signature information succeeds, service verification based on the verification result obtained by parsing the signature information.

9. The method according to claim 8, wherein before the obtaining signature information sent by the first execution unit by using a service application, the method
10 further comprises:

sending a dynamic parameter to the service application, so that the first execution unit signs, by means of the signature verification private key, the verification result and the dynamic parameter obtained from the service application to obtain the signature information.

10. The method according to claim 9, wherein the verifying the signature information by means of a signature verification public key corresponding to the signature verification private key, and performing, after it is determined that the verification on the signature information succeeds, service authorization based on the verification result obtained by parsing the signature information comprises:
15

20 verifying the public key certificate by means of the CA public key;

verifying, after it is determined that the verification on the public key certificate succeeds, the signature information by means of the signature verification public key obtained by parsing the public key certificate; and

25 verifying, after it is determined that the verification on the signature information succeeds, the dynamic parameter obtained by parsing the signature information, and performing, after it is determined that the verification on the dynamic parameter succeeds, service authorization based on the verification result obtained by parsing the signature information.

11. A service authorization apparatus, wherein a system of a device that
30 comprises the apparatus comprises at least a first security environment and a second security environment, a first execution unit runs in the first security environment, a second execution unit runs in the second security environment, and the apparatus comprises:

an acquisition module, configured to obtain information to be verified, and send

the information to be verified to the first execution unit for verification;

a receiving module, configured to receive signature information that is returned by the first execution unit and obtained by signing a verification result by means of a signature verification private key; and

5 a sending module, configured to send the signature information to the second execution unit, so that the second execution unit verifies the signature information by means of a signature verification public key corresponding to the signature verification private key, and performs service authorization based on the verification result after it is determined that the verification on the signature information succeeds.

10 12. The apparatus according to claim 11, wherein the first security environment comprises a trusted execution environment (TEE), and the second security environment comprises an execution environment provided by a secure element (SE).

13. The apparatus according to claim 11 or 12, wherein the information to be verified comprises biometric feature information to be verified.

15 14. The apparatus according to claim 11 or 12, wherein the acquisition module is configured to obtain a dynamic parameter sent by the second execution unit, wherein the dynamic parameter comprises at least one of a random number or time information; and send the dynamic parameter to the first execution unit, so that the first execution unit signs the verification result and the dynamic parameter by means
20 of the signature verification private key.

15. A service authorization apparatus, wherein a system of a device comprises at least a first security environment and a second security environment, a first execution unit runs in the first security environment, the apparatus runs in the second security environment, and the apparatus comprises:

25 an acquisition module, configured to obtain signature information sent by the first execution unit by using a service application, wherein the signature information is obtained after the first execution unit signs a verification result by means of a signature verification private key, and the verification result is obtained after the first execution unit verifies information to be verified sent by the service application; and

30 a verification module, configured to verify the signature information by means of a signature verification public key corresponding to the signature verification private key, and perform, after it is determined that the verification on the signature information succeeds, service authorization based on the verification result obtained by parsing the signature information.

16. The apparatus according to claim 15, wherein the signature verification public key is obtained by the apparatus from a first management server corresponding to the first execution unit by using a second management server corresponding to the apparatus.

5 17. The apparatus according to claim 15, wherein the acquisition module is configured to obtain a CA public key from a certificate authority (CA) by using a second management server corresponding to the apparatus.

10 18. The apparatus according to claim 17, wherein the verification module is configured to verify, by means of the CA public key, a public key certificate sent from the service application, wherein the public key certificate is obtained after the CA verifies the signature verification public key based on a CA private key corresponding to the CA public key, the public key certificate is obtained by the service application from the first execution unit, and the public key certificate is obtained by the first execution unit from the CA by using a first management server corresponding to the first execution unit; and verify, after it is determined that the verification on the public key certificate succeeds, the signature information by means of the signature verification public key obtained by parsing the public key certificate, and perform, after it is determined that the verification on the signature information succeeds, service authorization based on the verification result obtained by parsing the signature information.

15 20 information.

19. The apparatus according to claim 18, wherein the apparatus further comprises:

25 a sending module, configured to send a dynamic parameter to the service application, so that the first execution unit signs, by means of the signature verification private key, the verification result and the dynamic parameter obtained from the service application to obtain the signature information.

30 20. The apparatus according to claim 19, wherein the verification module is configured to verify the public key certificate by means of the CA public key; verify, after it is determined that the verification on the public key certificate succeeds, the signature information by means of the signature verification public key obtained by parsing the public key certificate; and verify, after it is determined that the verification on the signature information succeeds, the dynamic parameter obtained by parsing the signature information, and perform, after it is determined that the verification on the dynamic parameter succeeds, service authorization based on the verification result

obtained by parsing the signature information.