

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, by the first execution unit and through a service application, information to be verified, wherein the service application is running in the first security environment;

10 verifying, by the first execution unit, the information to be verified and obtaining a verification result of the information to be verified;

obtaining, by the first execution unit and through the service application, a dynamic parameter sent by the second execution unit, wherein the dynamic parameter is associated with a validity time;

15 signing, by the first execution unit, the verification result and the dynamic parameter by means of a signature verification private key to obtain signature information;

obtaining, by the second execution unit and through the service application, the signature information;

20 verifying, by the second execution unit, the signature information by means of a signature verification public key corresponding to the signature verification private key;

verifying, by the second execution unit, the dynamic parameter obtained by parsing the signature information, wherein verifying the dynamic parameter
25 comprises comparing, within the validity time, the dynamic parameter with a pre-stored copy of the dynamic parameter; and

performing, by the second execution unit, service authorization based on the verification result.

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

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 the dynamic parameter sent by the second execution unit comprises at least one of a random number or time information.

5 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:

10 obtaining, by the first execution unit and through a service application that runs in the first security environment, a dynamic parameter sent by the second execution unit, wherein the dynamic parameter is associated with a validity time;

15 signing, by the first execution unit and by means of a signature verification private key, a verification result and the dynamic parameter to obtain signature information, wherein the verification result is obtained after the first execution unit verifies information to be verified sent by the service application;

obtaining, by the second execution unit, the signature information sent by the first execution unit by using the service application;

verifying the signature information by means of a signature verification public key corresponding to the signature verification private key;

20 parsing the signature information to obtain the verification result from the signature information; and

performing service authorization based on the verification result obtained by parsing the signature information.

25 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.

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

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

8. The method according to claim 7, wherein verifying the signature information by means of the signature verification public key comprises:

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, wherein the public key certificate is obtained by the service application from the first execution unit, and wherein 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 wherein performing service authorization comprises:

performing service verification based on the verification result obtained by parsing the signature information.

9. The method according to claim 8, wherein parsing the signature information provides the dynamic parameter, and wherein the verifying the signature information by means of the signature verification public key comprises:

verifying the dynamic parameter.

10. A service authorization apparatus comprising a first security environment and a second security environment, wherein a first execution unit runs in the first security environment, and a second execution unit runs in the second security environment, and wherein the apparatus further comprises:

an acquisition module, configured to (i) obtain information to be verified, and send the information to be verified to the first execution unit for verification, (ii) obtain a dynamic parameter that is associated with a validity time sent by the second execution unit, wherein the dynamic parameter comprises at least one of a random number or time information, and (iii) send the dynamic parameter to the first execution unit, wherein the first execution unit is configured to obtain a verification result of the information to be verified and is configured to sign the verification result and the dynamic parameter by means of a signature verification private key;

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

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.

11. The apparatus according to claim 10, 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).

12. The apparatus according to claim 10 or 11, wherein the information to be
5 verified comprises biometric feature information to be verified.

13. A service authorization apparatus comprising at least a first security environment and a second security environment, wherein a first execution unit runs in the first security environment, and the service authorization apparatus runs in the second security environment, and wherein the service authorization apparatus further
10 comprises:

a sending module, configured to send a dynamic parameter that is associated with a validity time to a service application, wherein the dynamic parameter comprises at least one of a random number or time information, so that the first execution unit signs, by means of a signature verification private key, a verification
15 result and the dynamic parameter obtained from the service application to obtain signature information;

an acquisition module, configured to obtain the signature information sent by the first execution unit by using the service application, wherein the signature information is obtained after the first execution unit signs the verification result by means of the
20 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

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 service authorization based on the verification result obtained by
25 parsing the signature information.

14. The apparatus according to claim 13, 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.

15. The apparatus according to claim 13, wherein the acquisition module is
30 configured to obtain a certificate authority (CA) public key from a CA by using a second management server corresponding to the apparatus.

16. The apparatus according to claim 15, 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.

17. The apparatus according to claim 16, wherein parsing the signature information provides the dynamic parameter, and wherein the verification module is configured to verify the signature information by verifying the dynamic parameter.