CLAIMS

1. A cryptographic service platform, the cryptographic service platform being connected to a primary security module, wherein the cryptographic service platform comprises:

a registration module, configured to call the primary security module to generate a master key for a newly added secondary security module;

a working key creation module, configured to receive a working key creation request of a business system, call the primary security module to generate a working key for the business system, and acquire a working key ciphertext encrypted by a master key of the primary security module and a working key ciphertext encrypted by a master key of each connected secondary security module, returned by the primary security module; and

a cryptographic operation calling module, configured to receive a cryptographic operation request of the business system, the cryptographic operation request carrying data to be operated; determine a target security module responding to the cryptographic operation request, the target security module being one of the primary security module or at least one secondary security module; call the target security module using a working key ciphertext corresponding to the target security module and the data to be operated as input, and obtain an operation result of the target security module, the operation result being obtained by the target security module by decrypting the working key ciphertext to obtain the working key using the stored master key, and then encrypting the data to be operated using the decrypted working key.

2. The cryptographic service platform according to claim 1, wherein the registration module is further configured to configure the master key of the secondary security module by:

acquiring a target public key generated by the secondary security module;

calling the primary security module using the target public key as input, generating, by the primary security module, the master key of the secondary security module, and encrypting the generated master key using the target public key so as to obtain a master key ciphertext; and

sending the master key ciphertext to the secondary security module, and decrypting, by the secondary security module, the master key ciphertext using a target private key corresponding to the target public key so as to obtain the master key.

3. The cryptographic service platform according to claim 2, wherein the registration module is further configured to:

acquire a public key check value obtained when the primary security module performs message authentication code calculation on the target public key; and

call the primary security module using the target public key and the public key check value as input, and generate the master key of the secondary security module after the primary security module verifies the validity of the input target public key based on the public key check value.

4. The cryptographic service platform according to claim 1, wherein the registration module is further configured to configure the master key of the secondary security module by:

calling the primary security module, and acquiring two or more key components of the master key of the secondary security module after the primary security module generates the master key; and

outputting the two or more key components to key management entities, respectively, and transmitting, by the key management entities, the key components to the secondary security module so as to allow the secondary security module to generate the master key according to each key component.

5. The cryptographic service platform according to claim 1, wherein the registration module is further configured to:

receive and store the master key ciphertext of the secondary security module returned by the primary security module, the master key ciphertext being encrypted by the master key of the primary security module.

6. A cryptographic operation method, comprising:

receiving a cryptographic operation request initiated by a business system, the cryptographic operation request carrying data to be operated;

determining a target security module responding to the cryptographic operation request, the target security module being one of a primary security module or at least one secondary security module, and a master key of the secondary security module being generated by the primary security module;

acquiring a working key ciphertext corresponding to the target security module, the working key ciphertext being a ciphertext that is obtained when the primary security module encrypts the working key using the master key of the target security module, the working key being created by the primary security module for the business system; and

calling the target security module using the working key ciphertext and the data to be operated as input, acquiring an operation result returned by the target security module and sending the operation result to the business system, the operation result being obtained by the target security module by decrypting the working key ciphertext to obtain the working key using the stored master key, and then encrypting the data to be operated using the decrypted working key.

7. The method according to claim 6, wherein the master key of the secondary security module is obtained by:

acquiring a target public key generated by the secondary security module;

calling the primary security module using the target public key as input, generating, by the primary security module, the master key of the secondary security module, and encrypting the generated master key using the target public key so as to obtain a master key ciphertext; and

sending the master key ciphertext to the secondary security module, and decrypting, by the secondary security module, the master key ciphertext using a target private key corresponding to the target public key so as to obtain the master key.

8. The method according to claim 7, wherein calling the primary security module using the target public key as input, and generating, by the primary security module, the master key of the secondary security module comprises:

acquiring a public key check value obtained when the primary security module performs message authentication code calculation on the target public key; and

calling the primary security module using the target public key and the public key check value as input, and generating the master key of the secondary security module after the primary security module checks the validity of the input target public key based on the public key check value.

9. The method according to claim 6, wherein the master key of the secondary security module is obtained by:

calling the primary security module, and acquiring two or more key components of the master key of the secondary security module after the primary security module generates the master key; and

transmitting the two or more key components to key management entities, respectively, and transmitting, by the key management entities, the key components to the secondary security module respectively so as to allow the secondary security module to generate the master key according to each key component.

10. The method according to claim 6, further comprising:

receiving and storing the master key ciphertext of the secondary security module returned by the primary security module, the master key ciphertext being encrypted by the master key of the primary security module.

11. A cryptographic service device, comprising a memory, a processor, and a computer program stored on the memory and capable of running on the processor, wherein the processor executes the program so as to:

receive a cryptographic operation request initiated by a business system, the cryptographic operation request carrying data to be operated;

determine a target security module responding to the cryptographic operation request, the target security module being one of a primary security module or at least one secondary security module, and a master key of the secondary security module being generated by the primary security module;

acquire a working key ciphertext corresponding to the target security module, the working key ciphertext being a ciphertext that is obtained when the primary security module encrypts the working key using the master key of the target security module, the working key being created by the primary security module for the business system; and

call the target security module using the working key ciphertext and the data to be operated as input, acquire an operation result returned by the target security module, and send the operation result to the business system, the operation result being obtained by the target security module by decrypting the working key ciphertext to obtain the working key using the stored master key, and then encrypting the data to be operated using the decrypted working key.

12. A working key creation method, comprising:

receiving a working key creation request of a business system;

calling a primary security module to generate a working key for the business system, and acquiring a working key ciphertext encrypted by a master key of the primary security module and a working key ciphertext encrypted by a master key of each connected secondary security module, returned by the primary security module, the master key of the secondary security module being generated by the primary security module for the secondary security module by calling the primary security module.

13. A cryptographic service device, comprising a memory, a processor, and a computer program stored on the memory and capable of running on the processor, wherein the processor executes the program so as to:

receive a working key creation request of a business system;

call a primary security module to generate a working key for the business system, and acquire a working key ciphertext encrypted by a master key of the primary security module and a working key ciphertext encrypted by a master key of each connected secondary security module, returned by the primary security module, the master key of the secondary security module being generated by the primary security module for the secondary security module by calling the primary security module.