CLAIMS

1. A cryptographic service platform, the cryptographic service platform being connected to a primary security module and at least one secondary security module, and each security module having a master key; the cryptographic service platform comprising:

a registration module, configured to: call the secondary security module to generate an asymmetric key pair comprising a target public key and a target private key, and obtain and then store the target public key returned by the secondary security module;

a working key creation module, configured to: receive a working key creation request of a business system, and with the target public key of the secondary security module as input, call the primary security module to generate a working key for the business system, and obtain the following returned by the primary security module: a working key ciphertext encrypted by a master key of the primary security module, and a working key ciphertext encrypted by the target public key of the secondary security module; with the working key ciphertext encrypted by the target public key of the secondary security module as input, call the secondary security module to obtain the following returned by the secondary security module: a working key ciphertext encrypted by its own master key after decrypting the input working key ciphertext with the target private key; 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; and with a working key ciphertext corresponding to the target security module and the data to be operated as input, call the target security module to obtain an operation result of the target security module, the operation result being obtained in a way that the target security module uses a stored master key to decrypt the working key ciphertext to obtain a working key, and then the data to be operated is encrypted with the working key obtained by decryption.

2. The cryptographic service platform according to claim 1, wherein the target private key stored

by the registration module is encrypted with the master key of the secondary security module.

3. The cryptographic service platform according to claim 1, wherein the registration module is further configured to: obtain target private key indication data encrypted by the master key of the secondary security module; and

when the secondary security module is called by the working key creation module, the target private key indication data is still taken as input, for the secondary security module to obtain the target private key by using the master key to decrypt and decrypt the input working key ciphertext.

4. The cryptographic service platform according to claim 3, wherein the target private key indication data encrypted by the master key of the secondary security module comprises: a target private key ciphertext generated by encrypting the target private key with the master key of the secondary security module, or a target private key identifier encrypted with the master key of the secondary security module.

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

with the target public key as input, call the primary security module for authenticating the target public key by the primary security module, and obtain a key check value obtained through performing, by the primary security module, message authentication code value calculation on the target public key; and

the key check value is taken as input by the working key creation module when calling the primary security module, for the primary security module to check the input target public key of the secondary 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 the security modules having master keys;

obtaining a working key ciphertext corresponding to the target security module, the working key ciphertext being obtained in the following way in advance: with a target public key generated by the secondary security module in advance as input, calling the primary security module to generate a working key for the business system, and obtain the following returned by the primary security module: a working key ciphertext encrypted by the master key of the primary security module, and a working key ciphertext encrypted by the target public key of the secondary security module; with the working key ciphertext encrypted by the target public key of the secondary security module as input, calling the secondary security module to obtain the following returned by the secondary security module: a working key ciphertext encrypted by its own master key after decrypting the input working key ciphertext with a target private key; and

with the working key ciphertext and the data to be operated as input, calling the target security module to obtain an operation result returned by the target security module and send the operation result to the business system, the operation result being obtained in a way that the target security module uses the stored master key to decrypt the working key ciphertext to obtain a working key, and then the data to be operated is encrypted with the working key obtained by decryption.

7. The method according to claim 6, wherein the target private key stored by the registration module is encrypted with the master key of the secondary security module.

8. The method according to claim 6, further comprising: obtaining target private key indication data encrypted by the master key of the secondary security module; and

when the secondary security module is called, still taking the target private key indication data as input, for the secondary security module to obtain a target private key by using the master key to decrypt and decrypt the input working key ciphertext.

9. The method according to claim 8, wherein the target private key indication data encrypted by the master key of the secondary security module comprises: a target private key ciphertext generated by encrypting the target private key with the master key of the secondary security module, or a target

private key identifier encrypted with the master key of the secondary security module.

10. The method according to claim 7, further comprising:

with the target public key as input, calling the primary security module, and obtaining a key check value obtained through performing, by the primary security module, message authentication code value calculation on the target public key; and

when the primary security module is called to generate a working key for the business system, still taking the key check value as input, for the primary security module to check the input target public key of the secondary security module.

11. A cryptographic service device, comprising a memory, a processor, and a computer program stored on the memory and executable on the processor, wherein the processor implements the following method when executing the program:

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 the security modules having master keys;

obtaining a working key ciphertext corresponding to the target security module, the working key ciphertext being obtained in the following way in advance: with a target public key generated by the secondary security module in advance as input, calling the primary security module to generate a working key for the business system, and obtaining the following returned by the primary security module: a working key ciphertext encrypted by the master key of the primary security module, and a working key ciphertext encrypted by the target public key of the secondary security module; with the working key ciphertext encrypted by the target public key of the secondary security module as input, calling the secondary security module to obtain the following returned by the secondary security module: a working key ciphertext encrypted by its own master key after decrypting the input working key ciphertext with a target private key; and

with the working key ciphertext and the data to be operated as input, calling the target security module to obtain an operation result returned by the target security module and send the operation result to the business system, the operation result being obtained in a way that the target security module uses the stored master key to decrypt the working key ciphertext to obtain a working key, and then the data to be operated is encrypted with the working key obtained by decryption.

12. A method for creating a working key, comprising:

receiving a working key creation request of a business system;

with a target public key of a secondary security module as input, calling a primary security module to generate a working key for the business system, and obtaining the following returned by the primary security module: a working key ciphertext encrypted by a master key of the primary security module, and a working key ciphertext encrypted by the target public key of the secondary security module; and

with the working key ciphertext encrypted by the target public key of the secondary security module as input, calling the secondary security module to obtain the following returned by the secondary security module: a working key ciphertext encrypted by its own master key after decrypting the input working key ciphertext with a target private key; wherein the target public key and the target private key are generated in advance by the secondary security module.

13. A cryptographic service device, comprising a memory, a processor, and a computer program stored on the memory and executable on the processor, wherein the processor implements the following method when executing the program:

receiving a working key creation request of a business system;

with a target public key of a secondary security module as input, calling a primary security module to generate a working key for the business system, and obtaining the following returned by the primary security module: a working key ciphertext encrypted by a master key of the primary security module, and a working key ciphertext encrypted by the target public key of the secondary security module; and

with the working key ciphertext encrypted by the target public key of the secondary security module as input, calling the secondary security module to obtain the following returned by secondary security module: a working key ciphertext encrypted by its own master key after decrypting the input working key ciphertext with a target private key; wherein the target public key and the target private key are generated in advance by the secondary security module.