

CLAIMS

What is claimed is:

1. A key management method, comprising:
 - sending, by a security chip of a computer device, a request for obtaining a service key to a key management service;
 - receiving, by the security chip, a service key ciphertext from the key management service, wherein the service key ciphertext is obtained by encrypting the service key by the key management service based on a migration key of the security chip;
 - decrypting, by the security chip, the service key ciphertext based on the migration key to obtain the service key;
 - storing, by the security chip, the service key in the security chip;
 - providing, by the security chip, the service key to an application program of the computer device when the application program needs to encrypt data based on the service key;
 - invalidating, by the security chip, the service key after a preset time period; and
 - resending, by the security chip, a request for obtaining a new service key to the key management service to obtain the new service key from the key management service.
2. The method according to claim 1, wherein before the sending, by the security chip, a request for obtaining a service key to the key management service, the method further comprises:
 - sending, by the security chip, a migration certificate to the key management service, wherein the migration certificate is stored in the security chip and is configured for identity authentication of the security chip; and
 - authenticating, by the key management service, the migration certificate.
3. The method according to claim 2, wherein the storing, by the security chip, the service key in the security chip comprises:
 - encrypting, by the security chip, the service key with a storage key to generate an encrypted service key, and storing the encrypted service key in the security chip, wherein storage keys corresponding to different security chips are different.
4. The method according to claim 2, wherein the storing, by the security chip, the service key in the security chip comprises:
 - storing, by the security chip, the service key in a secured space of the security chip.

5. The method according to claim 2, wherein the migration certificate comprises the migration key of the security chip, wherein the security chip provides the migration key to the key management service when the security chip sends the migration certificate to the key management service.

6. The method according to claim 1, wherein the providing, by the security chip, the service key to an application program of the computer device comprises:

receiving, by the security chip, service data sent by the application program; and

encrypting, by the security chip, the service data with the service key to generate encrypted service data, and sending the encrypted service data to the application program.

7. The method according to claim 1, wherein the providing, by the security chip, the service key to an application program of the computer device comprises:

sending, by the security chip, the service key to the application program for the application program to encrypt service data with the service key.

8. A security chip disposed in a computer device, wherein the security chip comprises one or more microprocessors and one or more memories configured with instructions that, when executed by the one or more microprocessors, cause the security chip to perform operations comprising:

sending a request for obtaining a service key to a key management service;

receiving a service key ciphertext from the key management service, wherein the service key ciphertext is obtained by encrypting the service key by the key management service based on a migration key of the security chip;

decrypting the service key ciphertext based on the migration key to obtain the service key;

storing the service key in the security chip;

providing the service key to an application program of the computer device when the application program needs to encrypt data based on the service key;

invalidating the service key after a preset time period; and

resending a request for obtaining a new service key to the key management service to obtain the new service key from the key management service.

9. The security chip according to claim 8, wherein the providing the service key to an application program of the computer device comprises:

receiving service data sent by the application program; and
encrypting the service data with the service key to generate encrypted service data, and
sending the encrypted service data to the application program.

10. The security chip according to claim 8, wherein the providing the service key to an application program of the computer device comprises:

sending the service key to the application program for the application program to encrypt service data with the service key.

11. A security chip disposed in a computer device, wherein the security chip comprises one or more microprocessors and one or more memories configured with instructions that, when executed by the one or more microprocessors, cause the security chip to perform operations comprising:

sending a request for obtaining a service key to a key management service;

receiving a service key ciphertext from the key management service, wherein the service key ciphertext is obtained by encrypting the service key by the key management service based on a migration key of the security chip;

decrypting the service key ciphertext based on the migration key to obtain the service key;

storing the service key in the security chip; and

providing the service key to an application program of the computer device when the application program needs to encrypt data based on the service key,

wherein before the sending a request for obtaining a service key to the key management service, the operations further comprise:

sending a migration certificate to the key management service, wherein the migration certificate is stored in the security chip and is configured for identity authentication of the security chip such that the key management service authenticates the migration certificate.

12. The security chip according to claim 11, wherein the storing the service key in the security chip comprises:

encrypting the service key with a storage key to generate an encrypted service key, and
storing the encrypted service key in the security chip, wherein storage keys corresponding to different security chips are different.

13. The security chip according to claim 11, wherein the storing the service key in the

security chip comprises:

storing the service key in a secured space of the security chip.

14. The security chip according to claim 11, wherein the migration certificate comprises the migration key of the security chip, wherein the security chip provides the migration key to the key management service when the security chip sends the migration certificate to the key management service.

15. A non-transitory computer-readable storage medium storing instructions executable by a security chip of a computer device to cause the security chip to perform operations comprising:

sending a request for obtaining a service key to a key management service;

receiving a service key ciphertext from the key management service, wherein the service key ciphertext is obtained by encrypting the service key by the key management service based on a migration key of the security chip;

decrypting the service key ciphertext based on the migration key to obtain the service key;

storing the service key in the security chip;

providing the service key to an application program of the computer device when the application program needs to encrypt data based on the service key;

invalidating the service key after a preset time period; and

resending a request for obtaining a new service key to the key management service to obtain the new service key from the key management service.

16. The non-transitory computer-readable storage medium according to claim 15, wherein before the sending a request for obtaining a service key to the key management service, the operations further comprise:

sending a migration certificate to the key management service, wherein the migration certificate is stored in the security chip and is configured for identity authentication of the security chip such that the key management service authenticates the migration certificate.

17. The non-transitory computer-readable storage medium according to claim 16, wherein the storing the service key in the security chip comprises:

encrypting the service key with a storage key to generate an encrypted service key, and storing the encrypted service key in the security chip, wherein storage keys corresponding to

different security chips are different; or
storing the service key in a secured space of the security chip.

18. The non-transitory computer-readable storage medium according to claim 16, wherein the migration certificate comprises the migration key of the security chip, wherein the security chip provides the migration key to the key management service when the security chip sends the migration certificate to the key management service.

19. The non-transitory computer-readable storage medium according to claim 15, wherein the providing the service key to an application program of the computer device comprises:
receiving service data sent by the application program; and
encrypting the service data with the service key to generate encrypted service data, and sending the encrypted service data to the application program.

20. The non-transitory computer-readable storage medium according to claim 15, wherein the providing the service key to an application program of the computer device comprises:
sending the service key to the application program for the application program to encrypt service data with the service key.