

ABSTRACT

CRYPTOGRAPHIC OPERATION METHOD, METHOD FOR CREATING WORKING KEY, CRYPTOGRAPHIC SERVICE PLATFORM, AND CRYPTOGRAPHIC SERVICE DEVICE

5 This specification provides a cryptographic operation method, a method for creating a working key, a cryptographic service platform, and a cryptographic service device. Among security modules connected to the cryptographic service platform, the key management function is provided by a primary security module. The primary security module is configured to generate a key. Both the primary security module and a secondary security module can provide the cryptographic operation
10 function required by the cryptographic service platform. Each security module independently generates its own master key, a working key of a business system is generated by the primary security module, and the cryptographic service platform stores a working key ciphertext encrypted by the master key of the primary security module and a working key ciphertext encrypted separately by the master key of each secondary security module. Plaintexts of the master keys and the working key as
15 sensitive security parameters will not exceed the boundaries of the security modules, so the security of the key will not be lost, and the security requirements of the key are met. The cryptographic service platform can call any security module to respond to a cryptographic operation request of the business system, and the cryptographic service platform is compatible with multiple types of security modules.

20 [FIGURE 4]