

权利要求书

1、一种密钥管理方法，应用于安全芯片中，所述安全芯片设置在信息系统内的业务服务器中，所述信息系统还包括密钥管理中心，所述方法包括：

5 所述安全芯片向所述密钥管理中心发送请求，所述请求用于向所述密钥管理中心获取业务密钥；

所述安全芯片接收所述密钥管理中心发来的业务密钥密文，所述业务密钥密文是所述密钥管理中心基于迁移密钥对所述业务密钥进行加密后获得的；

所述安全芯片基于所述迁移密钥对所述业务密钥密文进行解密，获得所述业务密钥；

所述安全芯片将所述业务密钥存储在所述安全芯片内；

10 当所述业务服务器上的应用程序需要基于所述业务密钥对业务数据进行加密时，所述安全芯片向所述应用程序提供所述业务密钥。

2、如权利要求 1 所述的方法，在所述安全芯片向所述密钥管理中心发送请求之前，还包括：

15 所述安全芯片将迁移证书发送给所述密钥管理中心，以供所述密钥管理中心进行验证，其中，所述迁移证书存储在所述安全芯片内，用于对所述安全芯片进行身份验证；待所述迁移证书验证通过后，所述安全芯片向所述密钥管理中心发送请求。

3、如权利要求 2 所述的方法，所述安全芯片将所述业务密钥存储在所述安全芯片内，包括：

20 所述安全芯片基于存储密钥对所述业务密钥进行加密，并将加密后的业务密钥存储在所述安全芯片内，每个安全芯片对应的存储密钥各不相同；或

所述安全芯片将所述业务密钥存储在特定安全空间内，所述特定安全空间位于所述安全芯片内。

4、如权利要求 1 所述的方法，所述安全芯片向所述应用程序提供所述业务密钥，包括：

25 所述安全芯片接收所述应用程序发来的待加密的业务数据；

所述安全芯片基于所述业务密钥对所述待加密的业务数据进行加密，并将加密后的业务数据发送给所述应用程序。

5、如权利要求 1 所述的方法，所述安全芯片向所述应用程序提供所述业务密钥，包括：

30 所述安全芯片将所述业务密钥发送给所述应用程序，以使得所述应用程序基于所述业务密钥对待加密的业务数据进行加密。

6、如权利要求 1~5 任一所述的方法，在所述安全芯片对所述业务密钥进行安全存储之后，还包括：

在经过预设时间段后，所述安全芯片对所述业务密钥进行失效处理；

所述安全芯片重新向所述密钥管理中心发送请求，以向所述密钥管理中心获取新的业务密钥。

7、一种安全芯片，应用于在信息系统内的业务服务器中，所述信息系统还包括密钥管理中心，所述安全芯片包括：

第一发送单元，用于向所述密钥管理中心发送请求，所述请求用于向所述密钥管理中心获取业务密钥；

10 第一接收单元，用于接收所述密钥管理中心发来的业务密钥密文，所述业务密钥密文是所述密钥管理中心基于迁移密钥对所述业务密钥进行加密后获得的；

解密单元，用于基于所述迁移密钥对所述业务密钥密文进行解密，获得所述业务密钥，所述第二迁移密钥存储在所述安全芯片内，且与所述第一迁移密钥对应；

存储单元，用于将所述业务密钥存储在所述安全芯片内；

15 提供单元，用于当所述业务服务器上的应用程序需要基于所述业务密钥对业务数据进行加密时，向所述应用程序提供所述业务密钥。

8、如权利要求 7 所述的安全芯片，所述安全芯片，还包括：

第二发送单元，用于在所述向所述密钥管理中心发送请求之前，将迁移证书发送给所述密钥管理中心，以供所述密钥管理中心进行验证，其中，所述迁移证书存储在所述安全芯片内，用于对所述安全芯片进行身份验证；

待所述迁移证书验证通过后，通过所述第一发送单元向所述密钥管理中心发送请求。

9、如权利要求 7 所述的安全芯片，所述存储单元，具体用于：

基于存储密钥对所述业务密钥进行加密，并将加密后的业务密钥进行存储，每个安全芯片对应的存储密钥各不相同；或

25 将所述业务密钥存储在特定安全空间内，所述特定安全空间位于所述安全芯片内。

10、如权利要求 8 所述的安全芯片，所述提供单元，具体用于：

接收所述应用程序发来的待加密的业务数据；基于所述业务密钥对所述待加密的业务数据进行加密；将加密后的业务数据发送给所述应用程序。

11、如权利要求 8 所述的安全芯片，所述提供单元，具体用于：

30 将所述业务密钥发送给应用程序，以使得所述应用程序基于所述业务密钥对待加密的业务数据进行加密，所述应用程序安装在与所述安全芯片对应的业务服务器上。

12、如权利要求 7~11 任一所述的安全芯片，所述安全芯片还包括：

失效单元，用于在经过预设时间段后，对所述业务密钥进行失效处理；

更新单元，用于在所述对所述业务密钥进行失效处理之后，重新向密钥管理中心发送请求，以向所述密钥管理中心获取新的业务密钥。

5 13、一种业务服务器，在所述业务服务器中设置有如权利要求 7~12 任一权项所述的安全芯片。

14、一种信息系统，包括：

密钥管理中心；

10 业务服务器，在所述业务服务器中设置有如权利要求 7~12 任一权项所述的安全芯片。

15、一种计算机可读存储介质，其上存储有计算机程序，其特征在于，该程序被处理器执行时可以实现如权利要求 1~6 任一权项所述的方法步骤。