

一种密钥管理方法、安全芯片、业务服务器及信息系统

技术领域

[01] 本说明书实施例涉及互联网技术领域，尤其涉及一种密钥管理方法、安全芯片、业务服务器及信息系统。

5 背景技术

[02] 信息系统大多使用密码技术来保障数据安全（例如：数据库加密、通信加密、身份认证等等）。为了保护密钥的安全，信息系统通常使用 HSM(Hardware Security Module, 硬件密码模块) 或 KMS (Key Management Service, 密钥管理中心) 来保护密钥。

[03] 而对于大型信息系统，其往往拥有数以万计的业务服务器，在进行密钥管理时，
10 存在的问题较多。例如，KMS 压力巨大，容易出现宕机，导致整个密钥管理瘫痪，或者，密钥容易被黑客盗取，严重影响到信息安全。

发明内容

[04] 本说明书实施例通过提供一种密钥管理方法、安全芯片、业务服务器及信息系统，解决了现有技术中的信息系统，存在 KMS 压力大或业务密钥容易被黑客盗取的技术问题，实现了不仅降低 KMS 的压力，而且可以有效防止业务密钥容易被黑客盗取的技术效果。
15

[05] 第一方面，本说明书通过本说明书的一实施例提供如下技术方案：

[06] 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：

[07] 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；
20

[08] 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；

[09] 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
25 钥；

- [10] 所述安全芯片将所述业务密钥存储在所述安全芯片内;
- [11] 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。
- [12] 优选地, 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:
- 5 [13] 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;
- [14] 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。
- [15] 优选地, 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:
- [16] 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
- 10 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
- [17] 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。
- [18] 优选地, 所述安全芯片向所述应用程序提供所述业务密钥, 包括:
- [19] 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;
- 15 [20] 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。
- [21] 优选地, 所述安全芯片向所述应用程序提供所述业务密钥, 包括:
- [22] 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。
- 20 [23] 优选地, 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:
- [24] 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;
- [25] 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。
- [26] 第二方面, 本说明书通过本说明书的一实施例提供如下技术方案:
- 25 [27] 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:

- [28] 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；
- [29] 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；
- 5 [30] 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；
- [31] 存储单元，用于将所述业务密钥存储在所述安全芯片内；
- [32] 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。
- 10 [33] 优选地，所述安全芯片，还包括：
- [34] 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；
- [35] 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。
- 15 [36] 优选地，所述存储单元，具体用于：
- [37] 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
- [38] 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。
- 20 [39] 优选地，所述提供单元，具体用于：
- [40] 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。
- [41] 优选地，所述提供单元，具体用于：
- [42] 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
- 25 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。
- [43] 优选地，所述安全芯片还包括：
- [44] 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；

[45] 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。

[46] 第三方面, 本说明书通过本说明书的一实施例提供如下技术方案:

[47] 一种业务服务器, 在所述业务服务器中设置有安全芯片。

5 [48] 第四方面, 本说明书通过本说明书的一实施例提供如下技术方案:

[49] 一种信息系统, 包括:

[50] 密钥管理中心;

[51] 多台业务服务器, 在所述多台业务服务器中的每台业务服务器中都设置有安全芯片。

10 [52] 第五方面, 本说明书通过本说明书的一实施例提供如下技术方案:

[53] 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上述第一方面任一实施方式。

[54] 本说明书实施例中提供的一个或多个技术方案, 至少具有如下技术效果或优点:

[55] 在本说明书实施例中, 公开了一种密钥管理方法, 应用于安全芯片中, 所述安全
15 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: 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
20 片将所述业务密钥存储在所述安全芯片中; 其中, 在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, 由所述安全芯片向所述应用程序提供所述业
务密钥。由于在每台业务服务器中都设置了安全芯片, 且密钥传输过程中采用密文传输,
在密钥存储时将密钥存储在安全芯片中, 这样可以有效地避免客户攻击内存盗取业务密
钥, 提高了密钥的安全性。同时, 在向密钥管理中心请求一次业务密钥后, 可以将业务
25 密钥临时存储在安全芯片内, 在这段时间内若需要使用业务密钥时, 无需再向密钥管理
中心发起请求, 直接从业务服务器内部的安全芯片获取即可, 降低了密钥管理中心的压
力, 避免密钥管理中心出现宕机, 提高了信息系统的可靠性。本说明书实施例致力于在
密钥安全性和密钥管理中心压力之间实现平衡, 实现了不仅降低密钥管理中心的压力,

而且避免业务密钥被黑客盗取的技术效果。

附图说明

[56] 为了更清楚地说明本说明书实施例中的技术方案，下面将对实施例描述中所需要使用的附图作一简单地介绍，显而易见地，下面描述中的附图是本说明书实施例的一些
5 实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[57] 图 1 为本说明书实施例中一种信息系统的架构图；

[58] 图 2 为本说明书实施例中一种密钥管理方法的流程图；

[59] 图 3 为本说明书实施例中一种安全芯片的结构示意图。

10 具体实施方式

[60] 在正式介绍本方法之前，先对现有技术中进行如下介绍。

[61] 在现有技术中，在对密钥进行管理时，主要有以下两种方法：

[62] 第一种方法是：业务密钥存储在 KMS（密钥管理中心），并且业务密钥始终在 KMS 的保护下使用。即业务服务器每次使用密钥时，都需要请求 KMS。这种方法对于小型
15 信息系统是没有问题的，但对于大型信息系统（其拥有大量的业务服务器）来说，所有密码运算都请求 KMS，会造成严重的单点依赖，可能导致 KMS 宕机，影响系统稳定性。特别是，数据库加密、通信加密等操作涉及的数据量非常大，而某些高安全的信息系统会采用全网加密的方式，数据更是巨大，所有的数据都发往 KMS 是不现实的。

[63] 第二种方法是：业务密钥存储在 KMS，业务服务器要使用密钥时将密钥取回，使
20 用密钥的后续操作都在业务服务器中进行。使用这种方法，仅在密钥获取时依赖 KMS，而涉及大量数据的密钥使用过程则不依赖 KMS，避免了第一种方法的稳定性和性能问题。但这种做法导致密钥出现在业务服务器中，如果业务服务器被黑客攻破（例如：业务服务器的内存被攻击），黑客就可以获取业务密钥，这种问题在第一种方式中是不存在的。因为第一种方式会影响系统的稳定性和性能，所以现在大部分大型信息系统都采
25 用的是第二种做法。

[64] 由此可见，现有技术中的密钥管理方法，普遍存在 KMS 压力大或业务密钥容易被黑客盗取的技术问题。

[65] 本说明书实施例通过提供一种密钥管理方法、安全芯片、业务服务器及信息系统，解决了现有技术中的信息系统存在 KMS 压力大或业务密钥容易被黑客盗取的技术问题，实现了不仅降低 KMS 的压力，而且可以有效防止业务密钥容易被黑客盗取的技术效果。

[66] 本说明书实施例的技术方案为解决上述技术问题，总体思路如下：

- 5 [67] 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：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；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。
- 10

[68] 为了更好的理解上述技术方案，下面将结合说明书附图以及具体的实施方式对上述技术方案进行详细的说明。

- 15 [69] 首先说明，本文中出现的术语“多个”，一般指“两个以上”，包含“两个”的情况。

实施例一

- [70] 本实施例提供了一种密钥管理方法，应用于信息系统中（尤其是指大型信息系统，其拥有大量的业务服务器，例如，有数以万计的业务服务器），如图 1 所示，所述信息
- 20 系统至少包括密钥管理中心和多台业务服务器（例如：业务服务器 1、业务服务器 2、业务服务器 3、……）。

- [71] 其中，密钥管理中心（KMS，Key Management Service）是指能够提供完善的密钥管理和密码计算的系统，通常由多个 HSM 组成，提供高可用性、密钥备份等功能。本文中的密钥管理中心用于向每台业务服务器提供业务密钥，该业务密钥用于业务服务器
- 25 对业务数据进行加密，从而保障数据安全。

[72] HSM（hardware security module，硬件密码模块），硬件密码模块通常是明确物理边界（坚固的外壳）的软硬件的集合，能够确保密钥全生命周期的安全，并对外提供密钥管理和密码计算功能。典型的硬件密码模块包括密码卡、密码机等。

[73] 本实施例与现有技术区别之处在于，在每台业务服务器中都设置有一个安全芯片

(例如: 在业务服务器 1 中设置有安全芯片 1, 在业务服务器 2 中设置有安全芯片 2, 在业务服务器 3 中设置有安全芯片 3, ...), 每个安全芯片用于对其所在的业务服务器进行业务密钥的管理。

5 [74] 本方法即应用于安全芯片中(即: 应用于信息系统内每台业务服务器内的安全芯片中), 如图 2 所示, 所述方法包括:

[75] 步骤 S101: 安全芯片向密钥管理中心发送请求, 该请求用于向密钥管理中心获取业务密钥。

[76] 作为一种可选的实施例, 在步骤 S101 之前, 还包括:

10 [77] 安全芯片将迁移证书发送给密钥管理中心, 以供密钥管理中心进行验证, 迁移证书存储在安全芯片内; 待迁移证书验证通过后, 再执行步骤 S101。其中所述迁移证书存储在安全芯片内, 用于证明安全芯片具有合法身份。

[78] 在具体实施过程中, 执行步骤 S101 之前, 安全芯片需要初始化。在初始化过程中, 安全芯片需要将其迁移证书发给密钥管理中心, 密钥管理中心会对迁移证书进行验证。其中, 在每个安全芯片内存储有一个迁移证书, 该迁移证书可以是在安全芯片出厂前, 15 由芯片厂商刷到安全芯片内部, 或者, 在信息系统对应的运营商向厂家购买到安全芯片后, 由该运营商刷到安全芯片内部。该迁移证书用于证明安全芯片的身份的合法性。

[79] 若对迁移证书验证通过, 密钥管理中心则向安全芯片反馈一验证通过的信息。进一步, 即可执行步骤 S101, 即: 安全芯片向密钥管理中心发送请求, 以获取业务密钥。

20 [80] 步骤 S102: 安全芯片接收密钥管理中心发来的业务密钥密文, 业务密钥密文是密钥管理中心基于迁移密钥对业务密钥进行加密后获得的。

[81] 在具体实施过程中, 在密钥管理中心接收到安全芯片发来的请求后, 则提取一个业务密钥(例如: 从业务密钥库中随机提取一个业务密钥, 或基于预设规则从业务密钥库中提取一个业务密钥, 或利用 HSM 生成一个业务密钥, 等等)。并且, 在安全芯片之前发来的迁移证书中存储有第一迁移密钥, 该第一迁移密钥可以是非对称加密方式中 25 的公钥, 进一步, 密钥管理中心可以基于第一迁移密钥对刚才提取到的业务密钥进行加密, 生成一业务密钥密文, 并将该业务密钥密文发送给安全芯片。对应地, 安全芯片则接收密钥管理中心发来的业务密钥密文。

[82] 步骤 S103: 安全芯片基于迁移密钥对业务密钥密文进行解密, 获得业务密钥。

- [83] 在具体实施过程中，在安全芯片中还存储有与第一迁移密钥对应的第二迁移密钥，第二迁移密钥是与公钥对应的私钥，安全芯片即可基于第二迁移密钥对业务密钥密文进行解密，从而获得业务密钥（即：业务密钥的明文）。
- [84] 在具体实施过程中，每个安全芯片对应的迁移密钥（即：第一迁移密钥和第二迁移密钥）各不相同，从而提高了业务密钥在传出过程中的安全性，避免加密后的业务密钥被其它安全芯片截获并解密。
- 5 [85] 步骤 S104：安全芯片将业务密钥存储在安全芯片内。
- [86] 作为一种可选的实施例，步骤 S104，包括以下两种实施方式：
- [87] 方式一：安全芯片基于存储密钥对业务密钥进行加密，并将加密后的业务密钥存储 10 在安全芯片本地，每个安全芯片上的存储密钥各不相同。其中，所述存储密钥与迁移密钥不同，其用于对业务密钥进行加密存储使用。
- [88] 在具体实施过程中，在安全芯片内部还存储有一存储密钥，安全芯片可以基于该存储密钥对业务密钥(的明文)进行加密，并将加密后的业务密钥存储到安全芯片本地。
- [89] 在具体实施过程中，每个安全芯片上的存储密钥各不相同，从而提高了数据存 15 储的安全性，避免加密后的业务密钥被其它安全芯片解密。
- [90] 方式二：将业务密钥存储在特定安全空间内，该特定安全空间位于安全芯片内。
- [91] 在具体实施过程中，还可以在安全芯片内部设置一个特定安全空间，该特定安全空间采用软件或硬件加密方式，使得其中存储的数据绝对安全。
- [92] 针对每个安全芯片，可以采用上述两种方式中的任意一种，来对业务密钥进行安 20 全存储。
- [93] 相较于现有技术，在本实施例 中，由于在每台业务服务器中都设置了安全芯片，且业务密钥传输过程中采用密文传输，在业务密钥存储时是将业务密钥存储在安全芯片中（不是存储在业务服务器的硬盘或内存中），这样可以有效地降低黑客攻击内存盗取业务密钥的风险，提高了密钥的安全性。
- 25 [94] 步骤 S105：当业务服务器上的应用程序需要基于业务密钥对业务数据进行加密时，安全芯片向应用程序提供业务密钥。
- [95] 在具体实施过程中，若安全芯片的性能比较强，则可以将业务数据的加密过程由安全芯片本地完成。

[96] 具体来讲，在应用程序需要使用业务密钥时，安全芯片可以接收应用程序发来的待加密的业务数据，该应用程序安装在与该安全芯片对应的业务服务器上（即：该应用程序与该安全芯片位于同一个业务服务器上，每个安全芯片只为其所在业务服务器上的应用程序提供服务）；安全芯片基于业务密钥对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应用程序。

[97] 举例来讲，在业务服务器 1 上的应用程序 1 需要使用业务密钥时，应用程序 1 可以将待加密的业务数据发送给安全芯片 1，由安全芯片 1 基于业务密钥对业务数据进行加密后，并返还给应用程序 1。

[98] 在具体实施过程中，若安全芯片的性能比较弱，则可以将业务数据的加密过程由应用程序自己完成。

[99] 具体来讲，在应用程序需要使用业务密钥时，安全芯片可以将业务密钥发送给应用程序，以使得应用程序基于业务密钥对待加密的业务数据进行加密，该应用程序安装在与该安全芯片对应的业务服务器上（即：该应用程序与该安全芯片位于同一个业务服务器上，每个安全芯片只为其所在业务服务器上的应用程序提供服务）。

[100] 举例来讲，在业务服务器 2 上的应用程序 2 需要使用业务密钥时，安全芯片 2 可以将业务密钥发送给应用程序 2，由应用程序 2 对待加密的业务数据进行加密。

[101] 其中，应用程序每次使用完业务密钥后就将其彻底删除，下次需要使用时再重新向安全芯片获取，目的是避免业务密钥长时间滞留在非安全环境下（即：安全芯片以外的环境下），降低了被黑客窃取的风险。

[102] 作为一种可选的实施例，在步骤 S104 之后，还包括：

[103] 在经过预设时间段后，安全芯片对业务密钥进行失效处理；安全芯片重新向密钥管理中心发送请求，以向密钥管理中心获取新的业务密钥。其中，所述预设时间段可以根据实际需要灵活设置（例如：10 分钟、或半小时、或 1 小时、或 12 小时、或 24 小时、等等），对于所述预设时间段具体是多久，本实施例不做具体限定。这个失效时间可以是芯片在生产或初始化时设置好，或者密钥管理中心远程设置的。

[104] 也就是说，安全芯片还具有定期失效的功能，用于定期对业务密钥进行失效处理。

[105] 在具体实施过程中，每个业务密钥在安全芯片内只是临时存储，针对业务密钥可以设置一个失效时间（即：预设时间段），在安全芯片可以内部实现定时功能，在该失效时间到达后，则将其存储的业务密钥进行失效（例如：删除）处理。

[106] 而传统的安全芯片是没有这个功能的，业务密钥只能长期存储在安全芯片中。虽然攻击者在攻陷上层软件（例如 OS）后，可能无法窃取到业务密钥，但是攻击者能够恶意调用安全芯片中的业务密钥去执行密码运算。

5 [107] 另外，如果没有定期失效这个功能，在云环境下，由于应用有可能会在不同服务器之间迁移，则每个服务器上的安全芯片都会留存这个应用的业务密钥，这使得这个应用的业务密钥被恶意调用的可能性增大。云环境实际上放大了业务密钥留存的范围。使得上面这个攻击隐患更严重了。通过设置失效时间，使得攻击时间窗口由长期变为一个失效周期（比如：10 分钟），安全隐患减少明显。

10 [108] 同时，通过失效时间的管理，使得密钥管理中心对业务密钥有非常强的控制能力，如果密钥管理中心不想让业务服务器拥有本地进行密码运算的能力（回归到传统的密钥管理中心模式），只需要不再支持密钥迁移操作，在一个失效周期（比如：10 分钟）后，所有安全芯片中的业务密钥就全部失效了。业务服务器只能按照传统的方式使用业务密钥。

15 [109] 此处需要说明：业务服务器上的应用是没有权限设置这个失效时间的，这个失效时间只能由安全芯片来设置，这是考虑到业务服务器上的应用所处的环境比较复杂，应用容易被病毒感染，存在不安全的因素。

[110] 相较于现有技术，在本实施例中，在向密钥管理中心请求一次业务密钥后，在业务密钥失效前，业务密钥可以临时存储在安全芯片内，在这段时间内若需要使用业务密钥时，无需再向密钥管理中心发起请求，直接从业务服务器内部的安全芯片获取即可，
20 降低了密钥管理中心的压力，避免密钥管理中心出现宕机，提高了信息系统的可靠性。

[111] 在具体实施过程中，安全芯片在对业务密钥进行失效处理，安全芯片可以重复上述步骤 S101~步骤 S104，从而向密钥管理中心获取新的业务密钥。这样，就可以是实现周期性地对业务密钥进行更新。

[112] 上述本说明书实施例中的技术方案，至少具有如下的技术效果或优点：

25 [113] 在本说明书实施例中，公开了一种密钥管理方法，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：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;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。由于在每台业务服务器中都设置了安全芯片,且密钥传输过程中采用密文传输,在密钥

5 存储时将密钥存储在安全芯片中,这样可以有效地避免客户攻击内存盗取业务密钥,提高了密钥的安全性。同时,在向密钥管理中心请求一次业务密钥后,可以将业务密钥临时存储在安全芯片内,在这段时间内若需要使用业务密钥时,无需再向密钥管理中心发起请求,直接从业务服务器内部的安全芯片获取即可,降低了密钥管理中心的压力,避免密钥管理中心出现宕机,提高了信息系统的可靠性。本说明书实施例致力于在密钥安

10 全性和密钥管理中心压力之间实现平衡,实现了不仅降低密钥管理中心的压力,而且避免业务密钥被黑客盗取的技术效果。

实施例二

[114] 基于同一发明构思,本实施例提供了一种安全芯片,用于在信息系统内的业务服务器中,所述信息系统包括还密钥管理中心,如图4所示,所述安全芯片包括:

15 [115] 第一发送单元201,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;

[116] 第一接收单元202,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;

[117] 解密单元203,用于基于迁移密钥对所述业务密钥密文进行解密,获得所述业务密

20 钥;

[118] 存储单元204,用于将所述业务密钥存储在所述安全芯片内;

[119] 提供单元205,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。

[120] 作为一种可选的实施例,所述安全芯片,还包括:

25 [121] 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,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;

[122] 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。

[123] 作为一种可选的实施例，存储单元 204，具体用于：

[124] 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

5 [125] 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。

[126] 作为一种可选的实施例，提供单元 205，具体用于：

[127] 接收应用程序发来的待加密的业务数据，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；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。

10 [128] 作为一种可选的实施例，提供单元 205，具体用于：

[129] 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。

[130] 作为一种可选的实施例，所述安全芯片还包括：

[131] 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；

15 [132] 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。

实施例三

[133] 基于同一发明构思，本实施例提供了一种业务服务器，在该业务服务器中设置有上述安全芯片（即：实施例二中的任一实施方式中的安全芯片）。

20 实施例四

[134] 基于同一发明构思，本实施例提供了一种信息系统，如图 1 所示，包括：

[135] 密钥管理中心；

[136] 多台业务服务器（例如：业务服务器 1、业务服务器 2、业务服务器 3、...），并且，在这些业务服务器中的每台业务服务器中都设置有一安全芯片（即：实施例二中的任一实施方式中的安全芯片）。

25

实施例五

[137] 基于同一发明构思，本实施例提供了一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时可以实现如下方法步骤：

[138] 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；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第一迁移密钥对所述业务密钥进行加密后获得的；基于第二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；对所述业务密钥进行安全存储；在经过预设时间段后，对所述业务密钥进行失效处理。

[139] 在具体实施过程中，该程序被处理器执行时可以实现上述实施例一中任一实施方式中的方法步骤。

[140] 本领域内的技术人员应明白，本说明书实施例的实施例可提供为方法、系统、或计算机程序产品。因此，本说明书实施例可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本说明书实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

[141] 本说明书实施例是参照根据本说明书实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[142] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[143] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方

框图一个方框或多个方框中指定的功能的步骤。

[144] 尽管已描述了本说明书实施例的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本说明书实施例范围的所有变更和修改。

- 5 [145] 显然，本领域的技术人员可以对本说明书实施例进行各种改动和变型而不脱离本说明书实施例的精神和范围。这样，倘若本说明书实施例的这些修改和变型属于本说明书实施例权利要求及其等同技术的范围之内，则本说明书实施例也意图包含这些改动和变型在内。