

用于安全性信息交互的数据存储系统及方法

技术领域

本发明涉及数据存储系统及方法，更具体地，涉及用于安全性信息交互的
5 数据存储系统及方法。

背景技术

目前，随着网络技术的日益发展以及不同领域的业务种类的日益丰富（例如基于互联网的金融交易领域），对用于安全性信息交互的数据存储系统及方法的需求日益增长，因此，安全性数据存储系统及方法变得越来越重要。
10

通常，现有的安全性数据存储系统（例如，在采用基于公钥密码系统的数字证书、动态密码等相关认证技术的应用中，通常使用 USBKey 来存储相关的数字证书和密钥对）包括如下两种实现方式：（1）在安全性数据存储系统（包括安全性数据存储装置）中使用用户口令和解锁口令两者，所述用户口令用于
15 认证安全性数据存储装置的使用者的身份，而所述解锁口令用于对安全性数据存储装置进行解锁（当用户口令连续输入错误次数达到预定次数时，所述安全性数据存储装置被自动锁定），从而使所述用户口令恢复到初始状态，其中，所述安全性数据存储装置的用户口令由制造商初始化并可以被用户重置，而解锁口令则均相同（例如，同一批次的 USBKey 具有相同的解锁口令）；（2）在
20 安全性数据存储系统中不支持用户口令（例如不支持 PIN 码）的初始化和重置，即一旦安全性数据存储装置被锁定之后，用户必须使用新的安全性数据存储装置（例如 USBKey）并重新下载新的安全性信息数据（例如数字证书）。

然而，上述第一种实现方式存在如下问题：由于解锁口令则均相同，故一旦该解锁口令泄密，则可以对任意的安全性数据存储装置进行解锁，因而存在
25 巨大的潜在安全风险。

上述第二种实现方式存在如下问题：用户使用成本增加（例如一旦安全性数据存储装置被锁定，则需要使用新的安全性数据存储装置），并显著加大了使用的复杂性（例如重新下载新的安全性信息数据）。

因此，存在如下需求：提供一种具有高的安全度并且方便易用的用于安全

性信息交互的数据存储系统及方法。

发明内容

为了解决上述现有技术方案中所存在的问题，本发明提出了一种用于安全性信息交互的数据存储系统及方法。

本发明的目的是通过以下技术方案实现的：

一种用于安全性信息交互的数据存储系统，所述用于安全性信息交互的数据存储系统包括：

安全性信息存储装置，所述安全性信息存储装置用于存储和提供与安全性信息交互相关的数据信息；

解锁口令生成装置，所述解锁口令生成装置用于基于从所述安全性信息存储装置提取的原始参数而生成对应于所述安全性信息存储装置的解锁口令，并将所述解锁口令写入所述安全性信息存储装置中；

解锁服务器，所述解锁服务器用于当所述安全性信息存储装置被锁定时基于从所述安全性信息存储装置获取的原始参数而生成与所述安全性信息存储装置对应的解锁口令，并用所述解锁口令解锁所述已被锁定的安全性信息存储装置。

在上面所公开的方案中，优选地，所述原始参数是能够唯一标识所述安全性信息存储装置的至少一个要素。

在上面所公开的方案中，优选地，所述原始参数是所述安全性信息存储装置的标识符。

在上面所公开的方案中，优选地，所述与安全性信息交互相关的数据信息包括解锁口令、用户口令以及业务认证数据。

在上面所公开的方案中，优选地，所述安全性信息存储装置进一步包括：数据通信接口，所述数据通信接口用于完成与外部设备的数据通信；

解锁口令初始化模块，所述解锁口令初始化模块用于响应来自所述解锁口令生成装置的原始参数提取请求消息而提供与所述安全性信息存储装置对应的原始参数，并将来自所述解锁口令生成装置的已生成的解锁口令存储在所述数据存储模块中；

解锁模块,所述解锁模块用于根据来自所述解锁服务器的原始参数提取请求消息而提供与所述安全性信息存储装置对应的原始参数,并基于来自所述解锁服务器的解锁请求消息中的解锁口令而解锁所述安全性信息存储装置;

5 加锁模块,所述加锁模块用于当满足预定条件时加锁所述安全性信息存储装置;

数据存储模块,所述数据存储模块用于存储所述与安全性信息交互相关的数据信息。

10 在上面所公开的方案中,优选地,所述安全性信息存储装置进一步包括信息重置模块。所述信息重置模块用于当所述安全性信息存储装置被解锁时将所述与安全性信息交互相关的数据信息中的预定项初始化。

在上面所公开的方案中,优选地,所述数据通信接口是USB接口。

在上面所公开的方案中,优选地,所述解锁口令生成装置进一步包括:

15 原始参数提取模块,所述原始参数提取模块用于向所述安全性信息存储装置发送所述原始参数提取请求消息,并将从所述安全性信息存储装置获取的原始参数传送到口令生成模块;

口令生成模块,所述口令生成模块用于基于所述原始参数并通过调用第一动态链接库而生成对应于所述安全性信息存储装置的解锁口令,以及将所述生成的解锁口令传送到所述安全性信息存储装置。

20 在上面所公开的方案中,优选地,所述第一动态链接库由服务提供商或相关第三方设定。

在上面所公开的方案中,优选地,所述解锁服务器进一步包括:

原始参数获取模块,所述原始参数获取模块用于向所述安全性信息存储装置发送原始参数提取请求消息,并将从所述安全性信息存储装置获取的原始参数传送到解锁口令生成模块;

25 解锁口令生成模块,所述解锁口令生成模块用于基于所述原始参数并通过调用第二动态链接库而生成对应于所述安全性信息存储装置的解锁口令,以及将所述生成的解锁口令传送到解锁启动模块;

解锁启动模块,所述解锁启动模块用于基于所述生成的解锁口令构造解锁请求消息,并将所述解锁请求消息传送到所述安全性信息存储装置。

在上面所公开的方案中，优选地，所述第二动态链接库由所述安全性信息存储装置的制造商设定。

在上面所公开的方案中，优选地，所述安全性信息存储装置是 USBKey。

本发明的目的还通过以下技术方案实现：

- 5 一种用于安全性信息交互的数据存储方法，所述用于安全性信息交互的数据存储方法包括如下步骤：

(A1) 解锁口令生成装置基于从安全性信息存储装置提取的原始参数而生成对应于所述安全性信息存储装置的解锁口令，并将其写入所述安全性信息存储装置中；

- 10 (A2) 当所述安全性信息存储装置被锁定时，解锁服务器基于从所述安全性信息存储装置获取的原始参数而生成与所述安全性信息存储装置对应的解锁口令，并用所述解锁口令解锁所述已被锁定的安全性信息存储装置；

- (A3) 当所述安全性信息存储装置处于非锁定状态下时，所述安全性信息存储装置经数据通信接口而与用户终端进行通信，从而完成安全性信息的交互。
15 互。

在上面所公开的方案中，优选地，所述原始参数是能够唯一标识所述安全性信息存储装置的至少一个要素。

在上面所公开的方案中，优选地，所述原始参数是所述安全性信息存储装置的标识符。

- 20 在上面所公开的方案中，优选地，所述安全性信息是业务认证数据。

在上面所公开的方案中，优选地，所述用于安全性信息交互的数据存储方法进一步包括：

(A4) 当满足预定条件时，所述安全性信息存储装置被加锁。

- 25 在上面所公开的方案中，优选地，所述步骤 (A2) 进一步包括：当所述安全性信息存储装置被解锁时将预定项初始化。

在上面所公开的方案中，优选地，所述数据通信接口是 USB 接口。

在上面所公开的方案中，优选地，所述步骤 (A1) 进一步包括：

(B1) 向所述安全性信息存储装置发送原始参数提取请求消息，从而从所述安全性信息存储装置获取原始参数；

(B2) 基于所述原始参数并通过调用第一动态链接库而生成对应于所述安全性信息存储装置的解锁口令, 以及将所述生成的解锁口令传送到所述安全性信息存储装置。

在上面所公开的方案中, 优选地, 所述第一动态链接库由服务提供商或相关第三方设定。

在上面所公开的方案中, 优选地, 所述步骤(A2)进一步包括:

(C1) 向所述安全性信息存储装置发送原始参数提取请求消息, 从而从所述安全性信息存储装置获取原始参数:

(C2) 基于所述原始参数并通过调用第二动态链接库而生成对应于所述安全性信息存储装置的解锁口令:

(C3) 基于所述生成的解锁口令构造解锁请求消息, 并将所述解锁请求消息传送到所述安全性信息存储装置。

在上面所公开的方案中, 优选地, 所述第二动态链接库由所述安全性信息存储装置的制造商设定。

在上面所公开的方案中, 优选地, 所述安全性信息存储装置是 USBKey。

本发明所公开的用于安全性信息交互的数据存储系统及方法具有如下优点: (1) 由于不同的安全性信息存储装置具有不同的解锁口令, 故降低了由于解锁口令泄密而导致的潜在的安全性风险; (2) 降低了解锁过程的复杂度, 并同时降低了用户对安全性信息存储装置的持有成本; (3) 由于所述第一动态链接库和所述第二动态链接库是由不同的提供方设定的, 故解锁口令的生成和写入细节(例如采用何种密钥算法)对于外部而言是不可见的, 从而在整体上进一步降低了解锁口令在生成和写入过程中存在的潜在安全风险。

附图说明

结合附图, 本发明的技术特征以及优点将会被本领域技术人员更好地理解, 其中:

图1为根据本发明的实施例的用于安全性信息交互的数据存储系统的示意性结构图;

图2为根据本发明的实施例的用于安全性信息交互的数据存储方法的流程

图。

具体实施方式

图1是根据本发明的实施例的用于安全性信息交互的数据存储系统的示意性结构图。如图1所示，本发明所公开的用于安全性信息交互的数据存储系统包括安全性信息存储装置1、解锁口令生成装置2和解锁服务器3。其中，所述安全性信息存储装置1用于存储和提供与安全性信息交互相关的数据信息。所述解锁口令生成装置2用于基于从所述安全性信息存储装置1提取的原始参数而生成对应于所述安全性信息存储装置1的解锁口令，并将其写入所述安全性信息存储装置1中。所述解锁服务器3用于当所述安全性信息存储装置1被锁定时基于从所述安全性信息存储装置1获取的原始参数而生成与所述安全性信息存储装置1对应的解锁口令，并用所述解锁口令解锁所述已被锁定的安全性信息存储装置1。

示例性地，所述原始参数是能够唯一标识所述安全性信息存储装置1的至少一个要素。

示例性地，所述原始参数是所述安全性信息存储装置1的标识符（即 ID）。

示例性地，所述与安全性信息交互相关的数据信息包括解锁口令、用户口令以及业务认证数据（例如数字证书，动态密码等）。

如图1所示，优选地，在本发明所公开的用于安全性信息交互的数据存储系统中，所述安全性信息存储装置1进一步包括数据通信接口5、解锁口令初始化模块6、解锁模块7、加锁模块8和数据存储模块9。其中，所述数据通信接口5用于完成与外部设备的数据通信。所述解锁口令初始化模块6用于响应来自所述解锁口令生成装置2的原始参数提取请求消息而提供所述安全性信息存储装置1对应的原始参数，并将来自所述解锁口令生成装置2的已生成的解锁口令存储在该数据存储模块9中。所述解锁模块7用于根据来自所述解锁服务器3的原始参数提取请求消息而提供所述安全性信息存储装置1对应的原始参数，并基于来自所述解锁服务器3的解锁请求消息中的解锁口令而解锁所述安全性信息存储装置1。所述加锁模块8用于当满足预定条件时加锁所述安全性信息存储装置1（示例性地，所述预定条件是用户口令连续输入错误次数达到预定次数）。

所述数据存储模块9用于存储所述与安全性信息交互相关的数据信息。

可选地，在本发明所公开的用于安全性信息交互的数据存储系统中，所述安全性信息存储装置1进一步包括信息重置模块15。所述信息重置模块15用于当所述安全性信息存储装置1被解锁时将所述与安全性信息交互相关的数据信息中的预定项初始化（示例性地，所述预定项是用户口令）。

优选地，在本发明所公开的用于安全性信息交互的数据存储系统中，所述数据通信接口5是 USB 接口。

如图1所示，优选地，在本发明所公开的用于安全性信息交互的数据存储系统中，所述解锁口令生成装置2进一步包括原始参数提取模块10和口令生成模块11。其中，所述原始参数提取模块10用于向所述安全性信息存储装置1发送所述原始参数提取请求消息，并将从所述安全性信息存储装置1获取的原始参数传送到所述口令生成模块11。所述口令生成模块11用于基于所述原始参数并通过调用第一动态链接库（密钥算法动态链接库 DLL1）而生成对应于所述安全性信息存储装置1的解锁口令，以及将所述生成的解锁口令传送到所述安全性信息存储装置1。

优选地，在本发明所公开的用于安全性信息交互的数据存储系统中，所述第一动态链接库由服务提供商（例如银行）或相关第三方设定（即所述第一动态链接库由服务提供商或相关第三方提供）。

如图1所示，优选地，在本发明所公开的用于安全性信息交互的数据存储系统中，所述解锁服务器3进一步包括原始参数获取模块12、解锁口令生成模块13和解锁启动模块14。其中，所述原始参数获取模块12用于向所述安全性信息存储装置1发送原始参数提取请求消息，并将从所述安全性信息存储装置1获取的原始参数传送到所述解锁口令生成模块13。所述解锁口令生成模块13用于基于所述原始参数并通过调用第二动态链接库（解锁动态链接库 DLL2）而生成对应于所述安全性信息存储装置1的解锁口令，以及将所述生成的解锁口令传送到所述解锁启动模块14。所述解锁启动模块14用于基于所述生成的解锁口令构造解锁请求消息，并将所述解锁请求消息传送到所述安全性信息存储装置1。

优选地，在本发明所公开的用于安全性信息交互的数据存储系统中，所述

第二动态链接库由所述安全性信息存储装置1的制造商设定（即所述第二动态链接库由所述安全性信息存储装置1的制造商提供）。

如图1所示，示例性地，在本发明所公开的用于安全性信息交互的数据存储系统中，所述外部设备包括用户终端4，解锁口令生成装置2和解锁服务器3。

5 示例性地，在本发明所公开的用于安全性信息交互的数据存储系统中，所述安全性信息存储装置1是 USBKey。

如图1所示，本发明所公开的用于安全性信息交互的数据存储系统的基本工作原理如下：所述安全性信息存储装置1的制造商通过使用解锁口令生成装置2基于从所述安全性信息存储装置1提取的原始参数而调用所述第一动态链接库，从而生成对应于所述安全性信息存储装置1的解锁口令，并将其写入所述安全性信息存储装置1中；当所述安全性信息存储装置1被锁定时（例如用户口令连续输入错误次数达到预定次数），所述解锁服务器3基于从所述安全性信息存储装置1获取的原始参数而调用所述第二动态链接库，从而生成所述安全性信息存储装置1对应的解锁口令，并用所述解锁口令解锁所述已被锁定的安全性信息存储装置1；当所述安全性信息存储装置1处于非锁定状态下时，所述安全性信息存储装置1可以经所述数据通信接口5而与所述用户终端4进行通信，从而完成与业务相关的安全性信息的交互（例如金融交易中的安全性数据的认证）。

图2是根据本发明的实施例的用于安全性信息交互的数据存储方法的流程图。如图2所示，本发明所公开的用于安全性信息交互的数据存储方法包括如下步骤：（A1）解锁口令生成装置基于从安全性信息存储装置提取的原始参数而生成对应于所述安全性信息存储装置的解锁口令，并将其写入所述安全性信息存储装置中；（A2）当所述安全性信息存储装置被锁定时，解锁服务器基于从所述安全性信息存储装置获取的原始参数而生成与所述安全性信息存储装置对应的解锁口令，并用所述解锁口令解锁所述已被锁定的安全性信息存储装置；（A3）当所述安全性信息存储装置处于非锁定状态下时，所述安全性信息存储装置经数据通信接口而与用户终端进行通信，从而完成安全性信息的交互（例如金融交易中的安全性数据的认证）。

示例性地，在本发明所公开的用于安全性信息交互的数据存储方法中，所

述原始参数是能够唯一标识所述安全性信息存储装置的至少一个要素。

示例性地，在本发明所公开的用于安全性信息交互的数据存储方法中，所述原始参数是所述安全性信息存储装置的标识符（即 ID）。

示例性地，所述安全性信息是业务认证数据（例如数字证书，动态密码等）。

5 如图2所示，优选地，本发明所公开的用于安全性信息交互的数据存储方法进一步包括：（A4）当满足预定条件时，所述安全性信息存储装置被加锁（示例性地，所述预定条件是用户口令连续输入错误次数达到预定次数）。

如图2所示，优选地，在本发明所公开的用于安全性信息交互的数据存储方法中，所述步骤（A2）进一步包括：当所述安全性信息存储装置被解锁时
10 将预定项初始化（示例性地，所述预定项是用户口令）。

优选地，在本发明所公开的用于安全性信息交互的数据存储方法中，所述数据通信接口是 USB 接口。

如图2所示，优选地，在本发明所公开的用于安全性信息交互的数据存储方法中，所述步骤（A1）进一步包括：（B1）向所述安全性信息存储装置发送
15 原始参数提取请求消息，从而从所述安全性信息存储装置获取原始参数；（B2）基于所述原始参数并通过调用第一动态链接库（密钥算法动态链接库 DLL1）而生成对应于所述安全性信息存储装置的解锁口令，以及将所述生成的解锁口令传送到所述安全性信息存储装置。

优选地，在本发明所公开的用于安全性信息交互的数据存储方法中，所述
20 第一动态链接库由服务提供商（例如银行）或相关第三方设定（即所述第一动态链接库由服务提供商或相关第三方提供）。

如图2所示，优选地，在本发明所公开的用于安全性信息交互的数据存储方法中，所述步骤（A2）进一步包括：（C1）向所述安全性信息存储装置发送原始参数提取请求消息，从而从所述安全性信息存储装置获取原始参数；（C2）
25 基于所述原始参数并通过调用第二动态链接库（解锁动态链接库 DLL2）而生成对应于所述安全性信息存储装置的解锁口令；（C3）基于所述生成的解锁口令构造解锁请求消息，并将所述解锁请求消息传送到所述安全性信息存储装置。

优选地，在本发明所公开的用于安全性信息交互的数据存储方法中，所述

第二动态链接库由所述安全性信息存储装置的制造商设定(即所述第二动态链接库由所述安全性信息存储装置的制造商提供)。

示例性地,在本发明所公开的用于安全性信息交互的数据存储方法中,所述安全性信息存储装置是 USBKey。

- 5 尽管本发明是通过上述的优选实施方式进行描述的,但是其实现形式并不局限于上述的实施方式。应该认识到:在不脱离本发明主旨和范围的情况下,本领域技术人员可以对本发明做出不同的变化和修改。

10

15

20

25

权利要求

1. 一种用于安全性信息交互的数据存储系统，所述用于安全性信息交互的数据存储系统包括：

- 5 安全性信息存储装置，所述安全性信息存储装置用于存储和提供与安全性信息交互相关的数据信息；

 解锁口令生成装置，所述解锁口令生成装置用于基于从所述安全性信息存储装置提取的原始参数而生成对应于所述安全性信息存储装置的解锁口令，并将所述解锁口令写入所述安全性信息存储装置中；

- 10 解锁服务器，所述解锁服务器用于当所述安全性信息存储装置被锁定时基于从所述安全性信息存储装置获取的原始参数而生成与所述安全性信息存储装置对应的解锁口令，并用所述解锁口令解锁所述已被锁定的安全性信息存储装置。

2. 根据权利要求1所述的用于安全性信息交互的数据存储系统，其特征在于，
15 所述原始参数是能够唯一标识所述安全性信息存储装置的至少一个要素。

3. 根据权利要求2所述的用于安全性信息交互的数据存储系统，其特征在于，所述原始参数是所述安全性信息存储装置的标识符。

4. 根据权利要求3所述的用于安全性信息交互的数据存储系统，其特征在于，所述与安全性信息交互相关的数据信息包括解锁口令、用户口令以及业务
20 认证数据。

5. 根据权利要求4所述的用于安全性信息交互的数据存储系统，其特征在于，所述安全性信息存储装置进一步包括：

 数据通信接口，所述数据通信接口用于完成与外部设备的数据通信；

- 解锁口令初始化模块，所述解锁口令初始化模块用于响应来自所述解锁口
25 令生成装置的原始参数提取请求消息而提供与所述安全性信息存储装置对应的原始参数，并将来自所述解锁口令生成装置的已生成的解锁口令存储在所述数据存储模块中；

 解锁模块，所述解锁模块用于根据来自所述解锁服务器的原始参数提取请求消息而提供与所述安全性信息存储装置对应的原始参数，并基于来自所述解

锁服务器的解锁请求消息中的解锁口令而解锁所述安全性信息存储装置；

加锁模块，所述加锁模块用于当满足预定条件时加锁所述安全性信息存储装置；

数据存储模块，所述数据存储模块用于存储所述与安全性信息交互相关的
5 数据信息。

6. 根据权利要求5所述的用于安全性信息交互的数据存储系统，其特征在于，所述安全性信息存储装置进一步包括信息重置模块。所述信息重置模块用于当所述安全性信息存储装置被解锁时将所述与安全性信息交互相关的数据信息中的预定项初始化。

10 7. 根据权利要求6所述的用于安全性信息交互的数据存储系统，其特征在于，所述数据通信接口是USB接口。

8. 根据权利要求7所述的用于安全性信息交互的数据存储系统，其特征在于，所述解锁口令生成装置进一步包括：

原始参数提取模块，所述原始参数提取模块用于向所述安全性信息存储装
15 置发送所述原始参数提取请求消息，并将从所述安全性信息存储装置获取的原始参数传送到口令生成模块；

口令生成模块，所述口令生成模块用于基于所述原始参数并通过调用第一动态链接库而生成对应于所述安全性信息存储装置的解锁口令，以及将所述生成的解锁口令传送到所述安全性信息存储装置。

20 9. 根据权利要求8所述的用于安全性信息交互的数据存储系统，其特征在于，所述第一动态链接库由服务提供商或相关第三方设定。

10. 根据权利要求9所述的用于安全性信息交互的数据存储系统，其特征在于，所述解锁服务器进一步包括：

原始参数获取模块，所述原始参数获取模块用于向所述安全性信息存储装
25 置发送原始参数提取请求消息，并将从所述安全性信息存储装置获取的原始参数传送到解锁口令生成模块；

解锁口令生成模块，所述解锁口令生成模块用于基于所述原始参数并通过调用第二动态链接库而生成对应于所述安全性信息存储装置的解锁口令，以及将所述生成的解锁口令传送到解锁启动模块；

解锁启动模块,所述解锁启动模块用于基于所述生成的解锁口令构造解锁请求消息,并将所述解锁请求消息传送到所述安全性信息存储装置。

11. 根据权利要求10所述的用于安全性信息交互的数据存储系统,其特征在于,所述第二动态链接库由所述安全性信息存储装置的制造商设定。

5 12. 根据权利要求11所述的用于安全性信息交互的数据存储系统,其特征在于,所述安全性信息存储装置是 USBKey。

13. 一种用于安全性信息交互的数据存储方法,所述用于安全性信息交互的数据存储方法包括如下步骤:

(A1) 解锁口令生成装置基于从安全性信息存储装置提取的原始参数而生成对应于所述安全性信息存储装置的解锁口令,并将其写入所述安全性信息存储装置中;

(A2) 当所述安全性信息存储装置被锁定时,解锁服务器基于从所述安全性信息存储装置获取的原始参数而生成与所述安全性信息存储装置对应的解锁口令,并用所述解锁口令解锁所述已被锁定的安全性信息存储装置;

15 (A3) 当所述安全性信息存储装置处于非锁定状态下时,所述安全性信息存储装置经数据通信接口而与用户终端进行通信,从而完成安全性信息的交互。

14. 根据权利要求13所述的用于安全性信息交互的数据存储方法,其特征在于,所述原始参数是能够唯一标识所述安全性信息存储装置的至少一个要素。

15. 根据权利要求14所述的用于安全性信息交互的数据存储方法,其特征在于,所述原始参数是所述安全性信息存储装置的标识符。

16. 根据权利要求15所述的用于安全性信息交互的数据存储方法,其特征在于,所述安全性信息是业务认证数据。

25 17. 根据权利要求16所述的用于安全性信息交互的数据存储方法,其特征在于,所述用于安全性信息交互的数据存储方法进一步包括:

(A4) 当满足预定条件时,所述安全性信息存储装置被加锁。

18. 根据权利要求17所述的用于安全性信息交互的数据存储方法,其特征在于,所述步骤(A2)进一步包括:当所述安全性信息存储装置被解锁时将

预定项初始化。

19. 根据权利要求18所述的用于安全性信息交互的数据存储方法，其特征在于，所述数据通信接口是USB接口。

20. 根据权利要求19所述的用于安全性信息交互的数据存储方法，其特征在于，所述步骤（A1）进一步包括：

（B1）向所述安全性信息存储装置发送原始参数提取请求消息，从而从所述安全性信息存储装置获取原始参数；

（B2）基于所述原始参数并通过调用第一动态链接库而生成对应于所述安全性信息存储装置的解锁口令，以及将所述生成的解锁口令传送到所述安全性信息存储装置。

21. 根据权利要求20所述的用于安全性信息交互的数据存储方法，其特征在于，所述第一动态链接库由服务提供商或相关第三方设定。

22. 根据权利要求21所述的用于安全性信息交互的数据存储方法，其特征在于，所述步骤（A2）进一步包括：

（C1）向所述安全性信息存储装置发送原始参数提取请求消息，从而从所述安全性信息存储装置获取原始参数；

（C2）基于所述原始参数并通过调用第二动态链接库而生成对应于所述安全性信息存储装置的解锁口令；

（C3）基于所述生成的解锁口令构造解锁请求消息，并将所述解锁请求消息传送到所述安全性信息存储装置。

23. 根据权利要求22所述的用于安全性信息交互的数据存储方法，其特征在于，所述第二动态链接库由所述安全性信息存储装置的制造商设定。

24. 根据权利要求23所述的用于安全性信息交互的数据存储方法，其特征在于，所述安全性信息存储装置是USBKey。