(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 105960775 B
(45)授权公告日 2020.01.07

(21)申请号 201480074834.5

(22)申请日 2014.03.03

(65)同一申请的已公布的文献号
申请公布号 CN 105960775 A

(43)申请公布日 2016.09.21

(85)PCT国际申请进入国家阶段日
2016.08.03

(86)PCT国际申请的申请数据
PCT/US2014/019966 2014.03.03

(87)PCT国际申请的公布数据
WO2015/133990 EN 2015.09.11

(73)专利权人 英特尔公司
地址 美国加利福尼亚州

(72)发明人 N•M•史密斯 A•奈舒图特

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 姬利永

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/06(2006.01)

(56)对比文件
CN 101241527 A,2008.08.13,
CN 101241527 A,2008.08.13,
US 2013347064 A1,2013.12.26,
US 2012233466 A1,2012.09.13,
US 2012246463 A1,2012.09.27,
CN 102355351 A,2012.02.15,
CN 101345619 A,2009.01.14,

审查员 罗林

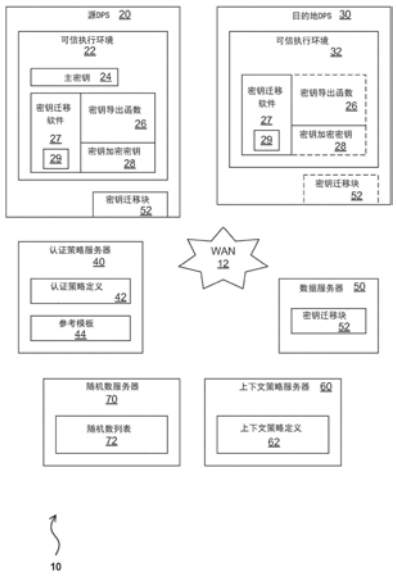
权利要求书4页 说明书18页 附图5页

(54)发明名称

用于迁移密钥的方法和装置

(57)摘要

一种目的数据处理系统(DPS)从源DPS接收密钥迁移块。该密钥迁移块包括主密钥的加密版本。该目的DPS接收标识(a)认证策略和(b)上下文策略的用户输入。该目的DPS基于该所标识的认证策略从该用户处收集认证数据。该目的DPS基于该所标识的上下文策略收集上下文数据。该目的DPS使用该认证数据和该上下文数据来解密该密钥迁移块。该认证数据可以包括多种类型的认证数据,可能包括生物特征数据。该用户还可以输入索引,并且该目的DPS可以使用该索引从随机数服务器检索数字。该目的DPS可以使用该数字来解密该密钥迁移块。对其他实施例进行了描述并要求保护。



CN 105960775 B

1.一种具有密钥迁移能力的数据处理系统,所述数据处理系统包括:

处理元件;

响应于所述处理元件的机器可访问介质;以及

在所述机器可访问介质中的数据,所述数据当由所述处理元件访问时使所述数据处理系统能够成为执行包括以下各项的操作的目的数据处理系统:

从源数据处理系统接收包括主密钥的加密版本的密钥迁移块,所述密钥迁移块至少部分地基于认证策略和上下文策略而生成;

接收标识所述认证策略的用户输入;

接收标识所述上下文策略的用户输入;

基于所述标识的认证策略从所述目的数据处理系统的用户处收集认证数据;

基于所述标识的上下文策略收集所述目的数据处理系统的上下文数据;以及

使用所述认证数据和所述上下文数据来解密所述密钥迁移块。

2.根据权利要求1所述的数据处理系统,其中:

所述机器可访问介质被配置成在所述目的数据处理系统中提供可信执行环境TEE;

在所述机器可访问介质中的所述数据包括被配置成在所述TEE中执行的密钥迁移软件;并且

所述密钥迁移软件被配置成使用所述认证数据和所述上下文数据来在所述目的数据处理系统的所述TEE中解密所述密钥迁移块。

3.根据权利要求1所述的数据处理系统,其中,收集认证数据的所述操作包括从所述目的数据处理系统的所述用户处收集生物特征数据。

4.根据权利要求1所述的数据处理系统,其中,基于所述标识的认证策略收集认证数据的所述操作包括:

基于所述标识的认证策略收集两种或更多种不同类型的认证数据。

5.根据权利要求1所述的数据处理系统,其中,所述操作进一步包括:

接收对被用于加密所述密钥迁移块中的所述主密钥的随机数进行标识的用户输入;以及

使用所述随机数来解密所述密钥迁移块。

6.根据权利要求5所述的数据处理系统,其中:

接收对被用于加密所述密钥迁移块中的所述主密钥的所述随机数进行标识的用户输入的所述操作包括接收大小小于16字节的索引;

所述随机数具有大于或等于16字节的大小;并且

所述操作进一步包括使用所述索引从远程随机数服务器检索所述随机数。

7.根据权利要求1所述的数据处理系统,其中,所述操作进一步包括:

基于标识所述上下文策略的所述用户输入从远程上下文策略服务器检索所述上下文策略。

8.一种用于迁移密钥的方法,所述方法包括:

在目的数据处理系统处,从源数据处理系统接收包括主密钥的加密版本的密钥迁移块,所述密钥迁移块至少部分地基于认证策略和上下文策略而生成;

在所述目的数据处理系统处,接收标识所述认证策略的用户输入;

在所述目的数据处理系统处，接收标识所述上下文策略的用户输入；

基于所述标识的认证策略从所述目的数据处理系统的用户处收集认证数据；

基于所述标识的上下文策略收集所述目的数据处理系统的上下文数据；以及

在所述目的数据处理系统处，使用所述认证数据和所述上下文数据来解密所述密钥迁移块。

9.根据权利要求8所述的方法，其中：

所述目的数据处理系统包括可信执行环境TEE；并且

由在所述目的数据处理系统的所述TEE中执行的密钥迁移软件来执行使用所述认证数据和所述上下文数据来解密所述密钥迁移块的操作。

10.根据权利要求8所述的方法，其中，收集认证数据的操作包括从所述目的数据处理系统的所述用户处收集生物特征数据。

11.根据权利要求8所述的方法，其中，基于所述标识的认证策略收集认证数据的操作包括：

基于所述标识的认证策略收集两种或更多种不同类型的认证数据。

12.根据权利要求8所述的方法，进一步包括：

在所述目的数据处理系统处，接收对被用于加密所述密钥迁移块的所述主密钥的随机数进行标识的用户输入；以及

使用所述随机数来解密所述密钥迁移块。

13.根据权利要求12所述的方法，其中：

接收对被用于加密所述密钥迁移块中的所述主密钥的所述随机数进行标识的用户输入的操作包括接收大小小于16字节的索引；

所述随机数具有大于或等于16字节的大小；并且

所述方法进一步包括使用所述索引从远程随机数服务器检索所述随机数。

14.根据权利要求8所述的方法，进一步包括：

基于标识所述上下文策略的所述用户输入从远程上下文策略服务器检索所述上下文策略。

15.根据权利要求8所述的方法，进一步包括：

基于标识所述认证策略的所述用户输入从远程认证策略服务器检索所述认证策略。

16.根据权利要求8所述的方法，其中，使用所述认证数据和所述上下文数据来解密所述密钥迁移块的操作包括：

在密钥导出函数KDF中使用所述认证数据和所述上下文数据；

使用所述KDF来生成密钥加密密钥KEK；以及

使用所述KEK来解密所述密钥迁移块。

17.根据权利要求8所述的方法，进一步包括：

在所述目的数据处理系统处接收所述密钥迁移块之前，在所述源数据处理系统处从所述主密钥的所有者处接收用户输入，其中，所述用户输入选择所述认证策略和所述上下文策略；以及

响应于接收到选择所述认证策略和所述上下文策略的所述用户输入，使用所述选择的认证策略和所述选择的上下文策略来创建包括所述主密钥的所述加密版本的所述密钥迁

移块。

18.根据权利要求17所述的方法,其中:

所述源数据处理系统包括可信执行环境TEE;

所述主密钥的明文版本驻留在所述源数据处理系统的所述TEE中;并且

在所述源数据处理系统的所述TEE中执行(a)接收选择所述认证策略和所述上下文策略的所述用户输入和(b)使用所述选择的认证策略和所述选择的上下文策略来创建所述密钥迁移块的操作。

19.根据权利要求17所述的方法,进一步包括:

在所述源数据处理系统处从远程随机数服务器接收随机数列表和相应的索引;

在从所述远程随机数服务器接收到所述随机数列表之后,接收从所述随机数列表中选择随机数的用户输入;以及

在接收到选择所述随机数的所述用户输入之后,使用所述选择的随机数来生成所述密钥迁移块。

20.存储有用于迁移密钥的计算机指令的至少一个机器可访问介质,其中,所述计算机指令响应于在数据处理系统上被执行而使所述数据处理系统能够执行根据权利要求8至19中任一项所述的方法。

21.一种具有密钥迁移能力的数据处理系统,所述数据处理系统包括:

处理元件;

响应于所述处理元件的至少一个机器可访问介质;以及

至少部分地存储在所述至少一个机器可访问介质中的计算机指令,其中,所述计算机指令响应于被执行而使所述数据处理系统能够执行根据权利要求8至19中任一项所述的方法。

22.一种具有密钥迁移能力的数据处理系统,所述数据处理系统包括:用于执行根据权利要求8至19中任一项所述的方法的装置。

23.一种用于促进密钥迁移的装置,所述装置包括:

非瞬态机器可访问介质;以及

在所述机器可访问介质中的数据,所述数据当由目的数据处理系统访问时使所述目的数据处理系统能够执行包括以下各项的操作:

从源数据处理系统接收包括主密钥的加密版本的密钥迁移块,所述密钥迁移块至少部分地基于认证策略和上下文策略而生成;

接收标识所述认证策略的用户输入;

接收标识所述上下文策略的用户输入;

基于所述标识的认证策略从所述目的数据处理系统的用户处收集认证数据;

基于所述标识的上下文策略收集所述目的数据处理系统的上下文数据;以及

使用所述认证数据和所述上下文数据来解密所述密钥迁移块。

24.根据权利要求23所述的装置,其中,所述操作进一步包括:

接收对被用于加密所述密钥迁移块中的所述主密钥的随机数进行标识的用户输入;以及

使用所述随机数来解密所述密钥迁移块。

25.根据权利要求24所述的装置,其中:

接收对被用于加密所述密钥迁移块中的所述主密钥的所述随机数进行标识的用户输入的所述操作包括接收大小小于16字节的索引;

所述随机数具有大于或等于16字节的大小;并且

所述操作进一步包括使用所述索引从远程随机数服务器检索所述随机数。

用于迁移密钥的方法和装置

技术领域

[0001] 在此所描述的实施例总体上涉及数据处理，并且具体地涉及用于迁移密钥的方法和装置。

背景技术

[0002] 数字密钥对于计算机安全性的许多不同的方面是至关重要的。例如，为了提供计算机之间的安全通信，密钥可以用于对通信进行加密。此外，为了提供对消息的认证，密钥可被用于在消息从发送者发送到接收者之前对消息进行数字签名。

[0003] 为了有效的安全性，必须保持一些类型的密钥是私密的。例如，公钥加密涉及一对密钥，其中这些密钥中的一个是公开的并且另一个是私密的。另外，有时需要将私钥从一个设备复制或迁移到另一个设备。例如，如果旧个人计算机(PC)的用户得到新的PC，则用户可能需要将一个或多个私钥从旧PC迁移到新PC。

[0004] 本公开描述了用于迁移密钥的方法和装置。

附图说明

[0005] 图1是具有用于迁移密钥的特征的示例性分布式数据处理系统的框图。

[0006] 图2是更详细地展示图1的源数据处理系统的框图。

[0007] 图3是用于在为密钥准备密钥迁移块之前认证该密钥的所有者的示例性过程的流程图。

[0008] 图4是用于准备密钥迁移块的示例性过程的流程图。

[0009] 图5呈现了用于迁移密钥的示例性过程的流程图。

具体实施方案

[0010] 为了本公开的目的，要迁移的密钥可以被称为主密钥。为了将主密钥从一个设备迁移到另一个设备，主密钥的所有者可以将主密钥保存在文件中，并且该文件随后可被从一个设备复制到另一个设备。为了本公开的目的，包含要迁移的主密钥的文件可以被称为档案文件或密钥迁移块。

[0011] 各种公钥加密标准(PKCS)包括关于密钥的某些教导。例如，被称为PKCS#12的标准描述了可被用来存储密钥的文件格式。根据PKCS#12，使用密钥加密密钥(KEK)对主密钥进行加密，并且然后将主密钥的该加密版本存储在档案文件中。档案文件也可以被称为PKCS#12块。

[0012] 根据PKCS#12，使用密钥导出函数(KDF)导出或生成KEK。具体地，根据PCKS#12，用户向KDF提供个人标识码(PIN)，并且KDF使用该PIN码生成KEK。用户应然后保持PIN为秘密的，只与期望的目标实体共享它。目标实体可以通过将PIN输入到PKCS#12算法来获得明文KEK。然后目标实体可以使用KEK从PKCS#12块解密主密钥。

[0013] 根据PKCS#12，知道或猜出PIN的任何人可以使用PIN与KDF来生成相同的KEK。因

此,PKCS#12标准受到蛮力攻击,包括对PIN的字典攻击。例如,攻击者可以进行离线字典攻击以破解PKCS#12。当PKCS#12块公开可用(例如,在可以被远程地访问的数据存储设备上)时,这种风险特别严重。为了本公开的目的,可以被远程地访问的数据存储设备可以被统称为“云”。目前提供如DROPBOX、GOOGLEDOCS、SKYDRIVE、ICLOUD和其他等名称或商标的云存储服务。云存储服务可以是传统的密钥托管和密钥迁移服务的有吸引力的替代方案。然而,典型的云存储服务缺乏实现稳健的密钥迁移所必要的安全性和访问控制语义。

[0014] 此外,如果PKCS#12块在云上公开可用,则攻击者可能会容易地获得块的副本来进行离线字典攻击。PKCS#12标准描述了一种将密钥封装成可传输的格式的方法,但该标准没有定义用于管理迁移或访问的可靠安全的方法。有关PKCS#12的更多信息可以在互联网上找到:en.wikipedia.org/wiki/PKCS_12。

[0015] 本公开描述了用于更安全地迁移密钥的方法和装置。如下面所解释的,为了说明的目的,本公开描述了一个或多个示例性实施例。然而,本教导不限于这些特定实施例。

[0016] 本公开描述了一种用于密钥迁移的方法,该方法是自我导向的,因为密钥的所有者具有指定和执行迁移过程的更大的能力。在至少一个实施例中,在没有迁移机构或任何其他可信或受过训练的第三方的帮助的情况下执行该方法。在另一个实施例中,通过一个或多个可信第三方和一个或多个受过训练的第三方而不是通过既可信又受过训练的第三方来执行该方法。例如,该方法可以使用数据服务器,该服务器被认为是受过训练的,因为它知道密钥迁移块的源和目的,但并不被认为是可信的,因为它不知道解开密钥迁移块以获得经加密密钥所需的秘密。并且该方法可以使用随机数服务器、认证策略服务器和上下文策略服务器,这些服务器被认为是可信的,因为每个服务器都知道获得经加密密钥所需的秘密中的某个秘密。然而,该方法可能需要随机数服务器、认证策略服务器、上下文策略服务器是分开的且不同的,这样,攻击者为了完成攻击将需要损害所有三个服务器。

[0017] 一个实施例针对密钥导出使用若干附加组件,同时分离这些方法用于包括或获得这些组件,从而应用被称为职责分离的安全性原则。例如,多个服务(其可以在用户控制下或外包给可信服务提供者)可以各自贡献密钥导出所需的材料的不同的部分。只有当正确地呈现所有的材料时密钥迁移才将成功。攻击者因此在能够击败安全性之前必须损害为密钥导出贡献输入的所有分级服务。此外,各个分级服务提供者发布他们的输入的端点可以使用可信执行环境(TEE)技术(如由英特尔公司(Intel Corporation)开发的软件防护扩展(SGX)和/或由英特尔公司开发的聚合安全性引擎(CSE))进行硬化。另外或替代地,端点可以使用通过安谋控股公司(ARM Holdings PLC)所提供的TRUSTZONE商标的安全性扩展、通过虚拟化技术和/或通过其他硬化技术保护的环境。CSE是嵌入在片上系统(SoC)中的硬件安全性引擎,该引擎从主CPU和存储器隔离执行。有关SGX的更多信息可以在互联网上找到:software.intel.com/en-us/blogs/2013/09/26/protecting-application-secrets-with-intel-sgx。

[0018] 如下面更详细描述的,本公开描述了一种用于用户导向的密钥迁移的方法,该方法涉及控制迁移的终止点上的访问的丰富的上下文敏感策略,其中可以使用云存储服务来促进迁移。

[0019] 在至少一个实施例中,该方法涉及迁移的源端点和目标端点两者上的TEE,并且该方法涉及结合认证、授权和上下文输入的使用的KDF。成功的迁移需要在目标端点上成功地

重新导出KEK,以便使被包裹的主密钥被解密并且因此可供使用。

[0020] 将密钥迁移块存储在云服务上可能会将块暴露给可能已经损害云服务的攻击者或具有维护云服务的授权并且因此可以访问订户内容的内部人员。云内容因此受到蛮力攻击,包括已知密文攻击、已知明文攻击、字典攻击和中间人攻击。然而,根据本公开,在至少一个实施例中,不同的KDF输入由不同的实体管理。因此,没有单个的实体保持重新导出KEK所必要的所有输入。因此,为了成功侵入在运输过程中的迁移块,攻击者将需要成功地损害提供输入的所有实体。

[0021] 图1是根据一个实施例的具有用于迁移密钥的特征的示例性分布式数据处理系统10的框图。在图1的实施例中,分布式数据处理系统10包括源数据处理系统(DPS)20和目的DPS 30。如图所示,源DPS 20和目的DPS 30被配置成用于提供相应的TEE 22和TEE 32。如下面更详细描述的,分布式数据处理系统10还包括认证策略服务器40、随机数服务器70、上下文策略服务器60以及数据服务器50。随机数服务器70提供随机数列表72。在图1的实施例中,分布式数据处理系统10内的各种处理系统可以经由广域网(WAN)12(如因特网)彼此通信。在一个实施例中,认证策略服务器40、上下文策略服务器60和随机数服务器70是可信的,而数据服务器50是不可信的。类似地,TEE 22和TEE 32是可信的,而源DPS 20和目的DPS 30还可以包括是不可信的主机软件。为了本公开的目的,如果项目具有或"知道"秘密信息,则其可以被认为是可信的,其中秘密信息是解密密钥迁移块所需的信息。相比之下,如果项目不能访问任何秘密信息,则其可以被认为是不可信的。

[0022] 如图1中所示,源DPS 20具有存储在TEE 22中的主密钥24。在一个实施例中,主密钥24是私钥。此外,如下面更详细描述的,源DPS 20在TEE 22内执行KDF 26以生成KEK 28,并且源DPS 20然后使用KEK 28生成主密钥24的密钥迁移块52。然后源DPS 20可以将密钥迁移块52复制到数据服务器50。如下面更详细描述的,用户然后可以使用目的DPS 30从数据服务器50检索密钥迁移块52;并且如果用户可以提供和/或获得所有的必要的输入,用户就可以从TEE 32内的密钥迁移块52提取主密钥24。

[0023] 图2是更详细地展示源DPS 20的框图。在图2的实施例中,源DPS 20包括与处理器80进行通信的随机存取存储器(RAM)86、硬盘驱动(HDD)88、网络端口82、可信平台模块(TPM)84、一个或多个生物特征传感器110以及一个或多个上下文传感器112。另外或替代地,源DPS 20可以包括其他类型的存储设备(例如,快闪存储器)、其他输入/输出(I/O)端口、多个处理器和/或其他组件。目的DPS 30的组成可以与源DPS 20相同或相似。认证策略服务器40、数据服务器50、上下文策略服务器60以及随机数服务器70还可以包括像那些在源DPS 20中的组件和/或任何其他合适的组件。

[0024] RAM 86中包含所有者认证策略100、密钥导出函数26、密钥加密密钥28,其中密钥导出函数26包括接收者认证因子92、不可预测性因子94、接收者上下文因子96。HDD 88中包含主密钥24、密钥迁移块52、公钥67。如虚线框所示,RAM 86中的存储的一部分和HDD 88中的存储的一部分在TEE 22内被保护。在TEE 32外执行的软件不能访问由TEE 22保护的任何存储区域。同样,TEE 32可以保护目的DPS 30中的RAM和HDD(和/或其他存储设备)中的存储区域的多个部分。并且如以下所示,不允许软件在TEE 22内执行,除非该软件已首先被验证是安全的。

[0025] 图3是用于在准备主密钥的密钥迁移块之前认证该主密钥的所有者的示例性过程

的流程图。为了讨论的目的，主密钥的所有者可以被称为爱丽丝(Alice)，并且目标(例如，爱丽丝想让其接收主密钥的人)可被称为鲍勃(Bob)。然而，在某些情况下(例如，如果爱丽丝已经获得新的PC来替换旧PC，并且她正在将密钥从旧PC迁移到新PC，则爱丽丝也可以充当鲍勃。

[0026] 综上所述，爱丽丝标识她希望迁移到鲍勃的设备的密钥。密钥在爱丽丝相信不被主机恶意软件损害的源TEE中被保护。爱丽丝使用她确定的适当强的多因素认证策略向源TEE进行认证。上下文传感器可以用于根据生物特征模板收集她的身份的生物特征数据。她的可信认证模板提供者(其可以是她已经预订的可信服务，)将她的身份的她的参考模板提供给TEE，从而允许TEE向TEE认证爱丽丝。

[0027] 具体地，图3的过程可以在源DPS 20中操作，在框110处开始，其中源DPS 20的用户(例如，爱丽丝)选择要迁移的私钥。例如，用户可以选择要迁移的主密钥24。如在图1和图2中所示，主密钥24由TEE 22在源DPS 20中保护。由于TEE 22的性质，主密钥24的所有者可以相信TEE 22不被主机恶意软件损害。

[0028] 例如，TEE 22(和TEE 32)可以提供其中代码在被从平台的其余部分隔离的CPU核心上执行并且数据被存储在被从平台的其余部分隔离的储存器中的TEE环境。该TEE环境也可以具有隔离的信令(例如，中断)和可信I/O(例如，使用除了通过TEE不能被访问的专用I/O设备)。此外，在至少一个实施例中，对要在TEE中执行的软件(包括固件)进行签名，并且被允许执行之前该签名被验证。另外，TEE环境也可以对代码和数据进行加密和解密。例如，在将数据存储在可以从该TEE外访问的设备上之前，该TEE可以对该数据进行加密。

[0029] 如图3的框112处所示，用户还可以针对源DPS 20选择所有者认证策略用来验证当前用户是主密钥的所有者。在一个实施例中，TEE 22从认证策略服务器40检索多种认证策略定义42，并且然后TEE 22显示具有这些认证策略的描述或概要的列表以及相应的索引。然后用户选择这些策略中的一个策略。在一个实施例中，策略中的每个策略需要多个认证因素被验证以将用户认证为所有者。例如，TEE 22可以呈现包括以下各项的策略列表：

[0030] • 需要指纹和声纹的认证的第一个策略；

[0031] • 需要指纹和视网膜图像的认证的第二个策略；以及

[0032] • 需要声纹和视网膜图像的认证的第三个策略。

[0033] 认证策略可以包括任何合适的类型的认证数据和因素，包括但不限于手指静脉、手掌静脉、虹膜扫描、心电图(ECG)读数、智能卡令牌、一次性密码令牌、电子围栏接近、用户存在感测等。

[0034] 为了本公开的目的，生物特征模板是针对特定人的特定类型的生物特征测量(例如，指纹)的一组生物特征数据。为了认证一个人是这个人所声称的那个人，执行新的生物特征测量以生成新的生物特征模板，并且然后将新的模板与一个或多个参考模板进行比较。

[0035] 如框114处所示，一旦用户已经选择认证策略，则TEE 22根据所选择的策略的需要从认证策略服务器40获得主密钥24的所有者的一个或多个参考生物特征模板。在一个实施例中，认证策略服务器40提供参考模板44以及认证策略定义42。因此，认证策略服务器40也可以被称为认证模板服务器。在其他实施例中，可以使用单独的认证策略服务器和认证模板服务器。在图1的实施例中，认证策略服务器40可以包括具有许多不同的人的生物特征认

证数据的参考模板，其中包括主密钥24的所有者的一个或多个参考模板44，如图1中所示。参考模板44可以包括主密钥24的所有者的指纹、声纹和视网膜图像的生物特征数据。在替代实施例中，一个人的每个不同类型的生物特征数据可以存储在不同的模板中。

[0036] 如框116处所示，TEE 22然后从当前用户获得生物特征数据。例如，TEE 22可以从当前用户扫描指纹、扫描视网膜和/或记录声纹。如框120处所示，TEE 22然后将来自当前用户的生物特征数据与参考模板44中的生物特征数据进行比较，以判定当前用户是否是所有者。

[0037] 因此，用户使用他或她确定的适当强的多因素认证策略向TEE 22认证。如果生物特征数据不匹配，则TEE 22可以显示错误消息，如框130处所示，并且然后过程可以结束。然而，如果生物特征数据相匹配，则TEE 22可以前进到准备密钥迁移块52，如框140处所示和下面更详细描述的。

[0038] 图4是用于准备密钥迁移块52的示例性过程的流程图。在一个实施例中，源DPS 20使用图4的过程来实现图3的框140。

[0039] 爱丽丝希望密钥迁移块24受到保护以免受蛮力密码攻击。因此，如框210处所示，图4的过程从爱丽丝使用TEE 22从随机数服务器70获得随机数列表来开始。替代地，爱丽丝可以使用TEE中的随机数发生器自己生成这样的列表，并且然后与随机数服务器70共享该列表。在两种情况下，她并没有告诉随机数服务器70她将在KDF中使用来自列表的哪个数。这是为了保证随机数服务器70处的员工或其他内部人员无法轻松地了解爱丽丝的选择。

[0040] 如框212处所示，TEE 22然后使用可信I/O技术(如所发布的名称或商标为利用受保护交易显示的INTEL IDENTITY PROTECTION TECHNOLOGY(英特尔身份保护技术)(INTEL IPT))的技术)向爱丽丝呈现列表。有关利用受保护交易显示的INTEL IPT的更多详细信息可以在互联网上找到：www.intel.com/content/www/us/en/architecture-and-technology/identity-protection/protected-transation-display.html。如框214处所示，爱丽丝然后可以使用随机PIN键盘显示器从列表中选择随机数中的一个随机数，其中该PIN对应于列表中的行数。例如，PIN值00001可以表示列表中的第一个条目，并且PIN值01234可以表示第1234个条目。标识所选择的随机数的PIN也可以被称为随机数PIN或RPIN。爱丽丝应该记住RPIN值(即，她选择的行数)，因为最终会需要这个数字从密钥迁移块52提取主密钥24。

[0041] 另外或替代地，爱丽丝可以将一个或多个位附加到RPIN(和/或其他PIN中的任何PIN)。密钥迁移软件可以使用这些位作为到KDF 26的直接输入，以进一步防止内部人员攻击。类似地，当鲍勃在目的DPS 30解开主密钥24时，鲍勃可能需要附加与爱丽丝所附加的相同的值，这样，目的DPS 30处的密钥迁移软件也可以使用这些位作为到KDF 26的直接输入。

[0042] 如框220处所示，爱丽丝然后输入或选择标识符以标识所期望的目标(即，应该能够从密钥迁移块52提取主密钥24的人或实体)。例如，爱丽丝可以将所期望的目标标识为“IdProvider/鲍勃”，其中“IdProvider”是标识特定域的字符串，并且“鲍勃”是该域内的目标的用户id。用于在不同的目标之间进行区分的任何值可用于该域，或如果无需用户id的消歧，则可以省略该域。

[0043] 如框222处所示，爱丽丝也可以从认证策略服务器40获得认证策略列表。该列表可以包括多种认证策略定义42连同每个认证策略的描述或概要以及相应的索引。在一个实施

例中，认证策略服务器40向TEE 22提供多因素认证(MFA)策略列表。该列表可以包括多个行，其中每个行具有(a)行数或索引(例如，“00001”)、(b)特定认证策略的文本描述或概要(例如，“认证英特尔芯片组版本1.0、指纹、人脸、英特尔3D相机v1”)以及(c)该策略的完整表达。例如，示例性认证策略和示例性上下文策略可以表达如下：

[0044]

```
"device": "ALICE-MOBL2",
"sp": " IT MFA Policy Server Pub Key",
"defaultMFAPolicies": [
    {
    “environment”: “Host”,
    "action": { "OS logon”: [
        {“level”: “1”,
        “actionResults”: [
            "UserCredentialsReleased " : "domain password",
        ] //actionResults
        }, //level
        {“level”: “2”,
        “actionResults”: [
            "UserCredentialsReleased " : "domain password",
                        "DeviceCredentialsReleased": “Asymmetric"
                        ] //actionResults
        }, //level
    ]}, //action
    “MfaSet”: [
        {“level”: “1”,
        “environment”: “SecurityEngine”,
        "factorSet": [
            {“environment”: “SecurityEngine”,
            “factors”:   [
                {"factorType": "NFC", “continuous”: false,
                “factorEnv": "SecurityEngine”,
```

[0045]

```
                    “factorEntailment”: “Intel chipset rel 1.0”}
                ]}//factors
            ] //factorSet
            },
            { “level”: “2”,
            “environment”: “SecurityEngine”,
            "factorSet": [
                {“environment”: “SecurityEngine”
                 “factors”: [
                    {"factorType": "fingerprint", “continuous”: false,
                    “factorEnv": ”SecureElement”,
                    “factorEntailment”: “Authentec v1”}
                ]},//factors
                // ---logical OR---
                {“environment”: “SecurityEngine”,
                “factors”:   [
                    {"factorType": ”PTD", “continuous”: false,
                    “factorEnv”: ”SecurityEngine”,
                    “factorEntailment”: “Intel DAL v9”} ,
                    {"factorType": ”3DFace", “continuous”: true,
                    “factorEnv”: ”Host”,
                    “factorEntailment”: “Intel 3D camera v1”}
                ]}//factors
            ] // factorSet
            }
        ] //MfaSet
        },
        {
        “environment”: “Host”,
        "action": { "VPN”: [ etc…]}
        }
    ]//defaultMfaPolicies
    "defaultContextPolicies": [
```

[0046]

```
{“contextSet”: [
    “environment”: “Host”,
    “context”: {“contextType”: “userPresence”,
        "trigger": "onNotPresent”,
        “notify”: [
            "OS Login",
            "VPN"
        ], //notify
        }, //trigger
        "factorSet": [
            {“environment”: “SecurityEngine”,
            “factor”: {"factorType": "irProximity", “continuous”: true,
                “factorEnv": "SecurityEngine”,
                “factorEntailment”: “Intel chipset rel 1.0”},
            “factor”: {"factorType": "KeyboardActivity", “continuous”: false,
                “factorEnv": ”OS”,
                “factorEntailment”: “Keyboard Vendor”}
            }] //factorSet
    }//context
    “context”: {“contextType”: “geoFence”, “fenceDef”: “OID_x”,
        "trigger": "onEnter”,
        “notify”: [
                    "OS Login",
            "VPN",
            “FDE”,
            “IdP”,
            // etc…
        ], //notify
        "trigger": "onExit”,
        “notify”: [
                    "OS Login",
            "VPN"
            “FDE”,
```

```
                    “IdP”,
                    // etc…
                ], //notify
                "factorSet": [
                    “environment”: “SecurityEngine”
[0047]              “factor”: {"factorType": "WiFiLocation", “continuous”: true,
                                “factorEnv": "SecurityEngine”,
                                “factorEntailment”: “Intel Sensor Hub 1.0”}
            }//context
        ]} //contextSet
    ] //defaultContextPolicies
```

[0048] 如框224和框226处所示，TEE 22可以使用可信输出技术呈现列表(或者仅仅来自列表的索引和文本概要)，并且然后爱丽丝可以从列表中选择所期望的策略来用于认证目标。例如，爱丽丝可以使用随机PIN键盘显示器从列表中选择所期望的认证策略，其中该PIN与列表中的索引或行号相匹配。标识所选择的认证策略的PIN也可以被称为认证策略PIN或APIN。替代地，对于针对目标的认证策略，TEE 22可以简单地使用TEE 22用于认证爱丽丝的相同的认证策略(和相应的APIN)。在这两种情况下，爱丽丝应该记住索引或APIN值，因为最终也会需要这个数字从密钥迁移块52提取主密钥24。

[0049] 如框228处所示，然后TEE 22可以使用针对目标的所选择的认证策略和所指定的标识符从认证策略服务器40获得目标的一个或多个参考模板。然后TEE 22可以对参考模板进行散列。为了尊重目标的隐私策略，TEE 22可以防止模板在TEE 22外暴露。另外，TEE 22可以对所选择的认证策略的文本概要和/或完整表达进行散列。

[0050] 如框230处所示，然后TEE 22可以从上下文策略服务器60获得多个上下文策略定义62。每个上下文策略定义62可以规定某些属性或元素作为在其内密钥迁移块52将被解密的上下文的必要部分。这些属性可以包括但不限于位置(例如，地理围栏坐标或边界)、一天中的时间、目标TEE软件的版本等。如框232和框234处所示，TEE 22可以向爱丽丝呈现上下文策略列表(例如，显示索引和每个上下文策略的文本描述或概要)，爱丽丝可以从列表中选择所期望的上下文策略。TEE 22可以使用如上面所描述的那些技术(例如，可信I/O技术)等技术来呈现列表和从爱丽丝接收输入(例如，用于标识所选择的行或索引的PIN)。标识所选择的上下文策略的PIN也可以被称为上下文策略PIN或CPIN。

[0051] 替代地，爱丽丝可以使用策略定义语言(如可扩展访问控制标记语言(XACML))手动设计指定这些必需的元素的上下文策略，并且然后她可以将该策略上传到上下文策略服务器60。

[0052] 除了指定哪些上下文元素将被考虑，爱丽丝还可以指定这些元素中的某些元素或所有元素的必要的值。例如，除了指定时间和位置是必需的上下文的一部分，爱丽丝还可以指定哪些特定时间是可接受的以及哪些特定位置。实际值(参考值)可以与策略一起包括，或者使用遵循策略的结构的单独的文件。

[0053] 然后TEE 22可以对所选择的上下文策略的文本概要和/或完整表达进行散列。

[0054] 如框240处所示，TEE 22然后建立KDF 26。在一个实施例中，TEE 22将KDF 26创建为包括以上元素参考中的许多或全部，如：

[0055] • 爱丽丝所选择的随机数(例如，“Rand1234”)；

[0056] • 相应的RPIN值；

[0057] • 所期望的目标的指定的标识符(例如，“IdProvider/鲍勃”)；

[0058] • APIN；

[0059] • 所选择的认证策略的文本描述的散列值(例如，“AuthPolicy”)

[0060] • 目标的每个参考模板的散列值(例如，“RefTplt_Bob”)；

[0061] • CPIN；以及

[0062] • 所选择的上下文策略的文本描述的散列值(例如，“ContextPolicy”)。

[0063] 如框242处所示，然后TEE 22可以使用KDF 26生成KEK 28。

[0064] 因此，在一个实施例中，KDF可以描述如下：

[0065] KEK＝KDF(Rand1234,RPIN,“IdProvider/Bob”,APIN,Hash(AuthPolicy),

[0066] Hash(RefTplt_Bob),CPIN,Hash(ContextPolicy))

[0067] 替代地，KDF可以描述如下：

[0068] rand＝Fetch_random_number_server(RPIN),

[0069] context＝[auth_value＝Fetch_authentication_template_server(APIN),

[0070] context_value＝Fetch_context_policy_server(CPIN)],

[0071] …

[0072] wrap_key＝KDF(rand,label,context,…)

[0073] 如框244处所示，然后爱丽丝可以使用KEK 28创建密钥迁移块52。换句话说，爱丽丝可以使用KEK 28来包裹主密钥24。例如，密钥迁移块52可以是PKCS#12块。如框250处所示，然后爱丽丝可以将密钥迁移块52复制到数据服务器50。数据服务器50可以提供云存储服务，并且密钥迁移块52可以驻留在数据服务器50上，直到爱丽丝完成到鲍勃的迁移需要的时间。一旦迁移已完成，数据服务器50可以删除密钥迁移块52。可替换地，除了复制/迁移服务，数据服务器50还可以封存密钥迁移块52一段时间，作为备份/恢复服务。

[0074] 如框252处所示，爱丽丝可以向鲍勃发送数据，以为鲍勃配备解开主密钥24将需要的信息。例如，爱丽丝可以向鲍勃提供RPIN、APIN和CPIN。其他这样的数据项目可以包括由爱丽丝用作鲍勃的标识符的字符串、所必需的认证因素的描述和任何所必需的上下文条件等。爱丽丝可以使用任何合适的技术或技术的组合将必要的信息发送给鲍勃。例如，爱丽丝可以亲自与鲍勃见面以告诉他信息的一个或多个项目(例如，RPIN)，和/或爱丽丝可以通过电子邮件、经由通用串行总线(USB)设备、在一张纸上书写等将信息的一个或多个项发送给鲍勃。

[0075] 准备迁移私钥24的过程然后可以结束。

[0076] 根据一个实施例，KDF 26的第一个参数是随机数。根据国家标准与技术研究院(NIST)特别出版物800-108 2009年10月Lily Chen的“使用伪随机函数的密钥导出的建议(Recommendation for Key Derivation Using Pseudorandom Functions)”(“SP800-108”)中所描述的惯例，此值也可以被认为是密钥导出密钥(KDK)。KDF 26的后续参数可以

连接在一起并且基本实现为SP800-108中所描述的伪随机函数(PRF)的“标签”参数的扩展。KDF 26也可以使用来自SP800-108的其他参数。如下面更详细描述的,目标可以使用RPIN、APIN和CPIN参数来查找实际值以包括在用来解开私钥24的KDF中。替代地,可以在根据SP800-108的PRF中使用所查找的值,其中KDF使用该PRF。这些RPIN、APIN和CPIN参数被包括在KDF定义中来显示什么值需要从爱丽丝被传送给鲍勃并且然后提供给构建实际PRF的函数。

[0077] 在上面所描述的操作中,TEE 22打开与随机数服务器70、认证策略服务器40以及上下文策略服务器60中的每一个的会话以获得通过RPIN、APIN和CPIN作为索引所标识的元素。然后这些元素被包括在KDF 26的输入参数中。PIN值也可以被包括在KDF中以确保鲍勃从爱丽丝获得关于迁移交易的信息并且鲍勃的TEE使用与爱丽丝相同的服务器。KDF 26可以包括鲍勃的身份的参考模板以断言仅可以使用特定模板匹配。换句话说,爱丽丝可以选择(例如)在2012年1月2日下午1:15收集的参考指纹。并且然后由目标提供的指纹必须与该特定参考指纹相匹配。KDF 26可以包括CPIN和上下文策略的散列以指定可以在其中解开主密钥24的上下文环境。

[0078] 因此,根据本公开,TEE可以通过使用PIN和用于从潜在KDK列表中选择KDK的算法或服务来选择用作PRF参数的KDK。这种方法的加密价值在于随机数服务器或随机数提供者(RNP)可以生成非常大的随机数(例如,512个字节或更多字节)列表。这可以确保KDK中的大量的熵。它也允许使用一次一密加密,其中随机数或KDK比消息更大。PIN是到列表中的索引值。因此列表的大小可以是小的(相对于KDK的大小),并且PIN可以更容易记住和在个人之间传输。在不涉及其他策略要求的实施例中,KDF参数(和相关联的操作)可以被限制到RPIN或RPIN和随机数本身,并且这样的实施例可以足以确保对密钥迁移动作的强有力的保护。

[0079] 图5呈现了用于迁移主密钥24的示例性过程的流程图。如下面更详细描述的,鲍勃的TEE通过(a)根据需要使用随机数服务器70、认证策略服务器40和上下文策略服务器60重新组装KDF输入、(b)应用KDF函数以重现KEK 28以及(c)使用KEK 28解开密钥迁移块52来完成迁移。

[0080] 图5的过程在爱丽丝已经将密钥迁移块52复制到数据服务器50之后开始。然后,如框310处所示,鲍勃从爱丽丝接收所需的迁移参数(例如,RPIN、APIN、CPIN、目标标识符等)。此外,如框312处所示,TEE 32从数据服务器50获得密钥迁移块52。

[0081] 如框314处所示,鲍勃然后使用可信输入通道将RPIN、APIN和CPIN值输入到TEE 32。例如,TEE 32可以使用可信I/O技术来提示鲍勃各种输入参数。如框316处所示,鲍勃也可以将被爱丽丝用于标识鲍勃的标识符输入到TEE 32中。

[0082] 如框320、框322和框324处所示,TEE 32然后使用RPIN、APIN和CPIN从随机数服务器70、认证策略服务器40和上下文策略服务器60检索正确的随机数、认证策略定义42和上下文策略定义62。换句话说,鲍勃打开与每个所需服务器的会话来接收查询结果(使用RPIN、APIN、CPIN作为相应的索引)。另外,如框326处所示,TEE 32可以从认证策略服务器40检索指定的认证策略所需要的任何认证模板。

[0083] 如框330处所示,TEE 32然后使用目的DPS 30的上下文传感器获得当前上下文的数据。如框332处所示,TEE 32然后使用目的DPS 30的生物特征传感器从当前用户获得生物特征数据。替代地,如果认证策略需要或允许,TEE 32可以使用较早收集并且然后本地存储

的参考模板将目的DPS 30认证为属于鲍勃。

[0084] 如框340处所示，TEE 32然后判定(a)来自当前用户的生物特征数据是否与从认证策略服务器40检索的认证模板相匹配和(b)当前上下文的数据是否满足从上下文策略服务器60检索的上下文策略定义62中所定义的上下文要求。如框342处所示，如果生物特征数据不匹配和/或如果当前上下文不满足上下文要求，则TEE 32生成错误消息，并且过程结束，TEE 32没有解开主密钥24。

[0085] 然而，如框360处所示，如果生物特征与上下文与要求相匹配，则TEE 32然后根据爱丽丝先前所选择的选项基于在目的DPS 30处要求的参数创建KDF。例如，TEE 32可以生成使用包括以下各项的参数的KDF：由鲍勃输入的RPIN、CPIN和APIN、来自随机数服务器70的相应的随机数、来自认证策略服务器40和上下文策略服务器60的相应的认证策略和上下文策略、目的DPS 30的当前上下文数据、特定认证参考模板以及来自目的DPS 30的当前用户的生物特征数据。因此，在一个实施例中或在一种情况下，TEE 32生成具有包括一个或多个上下文策略和一个或多个实际上下文值(例如要求迁移必须从相同的位置开始和结束的策略和标识设备的当前地理坐标的实际上下文值)的参数的KDF。所采样的传感器值可以被包括在内，因为它们在起点的时间和完成的时间两者是已知的。在图1的实施例中，TEE 32生成与TEE 22中的KDF 26相匹配的KDF 26。

[0086] 在不同的实施例中或在不同的情况下，TEE可以生成具有不同组参数的KDF。例如，所选择的上下文策略定义可能要求目的设备在午夜前完成迁移，并且当前上下文数据可能指示当前时间为晚上11:30。因此TEE可以断定当前上下文是可接受的。并且TEE然后可以从KDF参数列表中省略当前上下文数据。类似地，如果上下文策略要求目的设备位于德克萨斯州(Texas)，则TEE可以生成具有针对上下文策略(例如，“如果位置是德克萨斯州，则允许”)的参数的KDF，并且没有针对所采样的实际上下文值(例如，目的设备的当前地理坐标)的参数。策略设计者可以判定所收集的上下文值的粒度是否为使得假设可以对它们进行重复以完成迁移将是实际的。

[0087] 在TEE 32生成KDF之后，TEE 32然后使用KDF生成KEK，如框362处所示。如果TEE 32向KDF提供所有的正确的参数，则所生成的KEK 28将与源DPS 20的KEK 28相匹配。如框364处所示，TEE 32然后使用KEK 28来解密密钥迁移块52并且提取或解开主密钥24。如框366所示，然后目的DPS 30可以将主密钥24保存在TEE 32中。

[0088] 然而，再次参考框362，如果任何的KDF输入不正确，则所生成的KEK将不与KEK 28相匹配。因此，TEE 32将无法解密密钥迁移块52以访问主密钥24。因此，在图1中，KDF 26和KEK 28在TEE 32中使用虚线轮廓示出，以表示它们可能不与TEE 22中的KDF和KEK相匹配。

[0089] 本公开描述了用于管理被馈送到KDF中的输入的新颖的和有用的方式。一个实施例的优点是攻击者将需要损害每个支持服务以收集重构KDF所必要的所有的输入。使用服务来提供潜在元素列表以及使用PIN来从这些列表中标识所选择的元素也提供好处。例如，可以在列表中列举MFA策略，并且作为迁移动作的一部分可以方便地使用APIN从列表传送特定策略。类似地，可以使用列举包括各种选项和选项的组合的上下文策略陈述的服务来指定上下文策略(如一天中的时间限制和位置地理围栏限制)，作为KDF的一部分。

[0090] 在一个实施例中，如果目的TEE提供正确的数据，则随机数服务器向目的TEE提供与被提供到源TEE的相同的随机数，认证策略服务器向目的TEE提供与被提供到源TEE的相

同的认证策略，并且上下文策略服务器向目的TEE提供与被提供到源TEE的相同的上下文策略。然而，在周期的完成之后(例如，在密钥迁移已经完成之后)，服务器可以修改、重新组织或替换它们相应的列表，使得由爱丽丝和鲍勃使用的RPIN、APIN和CPIN将标识不同的随机数、认证策略和上下文策略。

[0091] 在一个实施例中，随机数服务器提供大列表。例如，该列表可以使用八个字符的PIN(使用阿拉伯数字)。因此，该列表可以包括1亿条目。替代地，该列表可以使用八个字符的PIN(使用所有美国信息交换标准代码(ASCII)打印字符)。因此，该列表可以包括超过6千万亿条目。不同的实施例可以使用扩展ASCII字符集或任何其他合适的字符编码方案来实现列表索引值，其中索引被转换成较大的数值。此外，不同的实施例可以针对PIN或索引使用不同的大小，包括但不限于PIN实现为四个、五个、六个、七个或八个ASCII编码的二进制字节。其他实施例可以使用小于16字节的大小的PIN。

[0092] 相比于PIN指向的随机数的大小，PIN的大小可以相对是小的。例如，不同的实施例可以使用大小为16、32或64字节(即，128、256或512位)或更多字节的随机数。因此，PIN可以被认为是小的，并且随机数可以被认为是大的或非常大的。因此，猜测被用于密钥迁移块的随机数将是不切实际的。攻击者将需要使用来自随机数服务器列表或数据库。但随机数服务器可以监控并拒绝可疑的查询。例如，随机数服务器可以拒绝与密码猜测攻击的签名相匹配的查询。

[0093] 在一个实施例中，爱丽丝从列表中手动随机选择RPIN。在另一个实施例中，源DPS中的TEE使用随机数发生器自动随机选择RPIN。换句话说，RPIN可以是系统生成的PIN。

[0094] 本公开指的是由源DPS和目的DPS中的TEE执行的各种操作。在一个实施例中，源TEE和目的TEE包括推动这个过程的一个或多个软件组件。例如，TEE可以包括密钥迁移软件27，并且密钥迁移软件27可以包括KDF发生器29。

[0095] 因此，在TEE 22和TEE 32中，密钥迁移软件27可以提示爱丽丝和鲍勃输入需要的用户输入数据(例如，RPIN、APIN、CPIN等)。密钥迁移软件27可以使用可信I/O通道获得用户输入，如上面所描述的。密钥迁移软件27还可以收集生物特征和上下文数据。密钥迁移软件27还可以使用KDF发生器29来基于用户输入生成KDF。然后密钥迁移软件27可以使用所得KDF生成KEK。并且然后密钥迁移软件27可以使用所得KEK来加密或解密密钥迁移块52。

[0096] 为了本公开的目的，如“随机数”和“随机数发生器”等术语应该被理解为包括伪随机数和伪随机数发生器。

[0097] 鉴于在此所描述和展示的原理和示例性实施例，将认识到可以在不背离这些原理的情况下在排列和细节上对所展示的实施例进行修改。此外，上述的讨论集中于特定的实施例，但设想其他配置。此外，尽管在此使用如“一个实施例(an embodiment)”、“一个实施例(one embodiment)”、“另一实施例(another embodiment)”等表达，但这些短语意在一般指实施例可能性，并且不旨在将本发明限制到特定实施例配置。如在此所使用的，这些短语可以指相同的实施例或不同的实施例，并且这些实施例可以组合到其他实施例中。

[0098] 任何合适的操作环境和编程语言(或操作环境和编程语言的组合)可以被用来实现在此所描述的组件。如上所述，本发明的教导可用于在许多不同类型的数据处理系统中获得益处。示例性数据处理系统包括但不限于分布式计算系统、超级计算机、高性能计算系统、计算集群、大型计算机、小型计算机、客户端-服务器系统、个人计算机(PC)、工作站、服

务器、便携式计算机、膝上型计算机、平板计算机、个人数字助理(PDA)、电话、手持式设备、娱乐设备(如音频设备、视频设备、音频/视频设备(例如,电视机和机顶盒))、车辆用处理系统以及用于处理或发送信息的其他设备。因此,除非另有明确说明或上下文需要,对任何特定类型的数据处理系统(例如,移动设备)的引用应该被理解为也包括其他类型的数据处理系统。此外,除非另有明确说明,被描述为耦合到彼此、彼此通信、响应于彼此等的元件不需要是彼此连续通信的并且不需要直接耦合到彼此。同样,当一个组件被描述为从另一个组件接收数据或向另一个组件发送数据时,该数据可通过一个或多个中间组件来发送或接收,除非另有明确说明。另外,可以将数据处理系统的一些组件实现为具有用于与总线进行通信的接口(例如,连接器)的适配卡。替代地,可以使用如可编程或不可编程逻辑设备或阵列、专用集成电路(ASIC)、嵌入式计算机、智能卡等组件将设备或组件实现为嵌入式控制器。为了本公开的目的,术语“总线”包括可以由两个以上的设备共享的路径以及点对点路径。

[0099] 本公开可以指指令、函数、过程、数据结构、应用程序、微代码、配置设置以及其他类型的数据。如上面所描述的,当数据被机器或设备访问时,机器或设备可以通过执行任务、定义抽象数据类型或低级硬件上下文和/或执行其他操作作出响应。例如,数据储存器、RAM和/或快闪存储器可以包括各种指令集,这些指令集当被执行时执行各种操作。这样的指令集可以一般地被称为软件。另外,术语“程序”可以一般用于覆盖范围广泛的软件构造,包括应用、例程、模块、驱动程序、子程序、过程以及其他类型的软件组件。此外,在上文被描述为在一个示例性实施例中驻留在特定设备上的应用和/或其他数据在其他实施例中可以驻留在一个或多个其他设备上。并且在上文被描述为在一个示例性实施例中在一个特定设备上执行的计算操作在其他实施例中可以由一个或多个其他设备执行。

[0100] 还应该理解,在此所描述的硬件和软件组件表示合理地自包含使得每个功能元件可以基本上独立于其他功能元件被设计、构造或更新的功能元件。在替代实施例中,组件中的许多组件可以实现为硬件、软件或硬件和软件的组合,用于提供在此所描述和展示的功能。例如,替代实施例包括用于执行本发明的操作的机器可访问媒体编码指令或控制逻辑。这样的实施例也可以被称为程序产品。这样的机器可访问介质可以包括但不限于有形存储介质(如磁盘、光盘、RAM、只读存储器(ROM)等)以及处理器、控制器和包括RAM、ROM和/或其他存储设备的其他组件。为了本公开的目的,术语“ROM”可以一般用于指非易失性存储器设备,如可擦除可编程ROM(EPROM)、电可擦除可编程ROM(EEPROM)、快闪ROM、快闪存储器等。在一些实施例中,用于实现所描述的操作的控制逻辑中的一些或全部可以以硬件逻辑来实现(例如,作为集成电路芯片的一部分、可编程门阵列(PGA)、ASIC等)。在至少一个实施例中,所有组件的指令可以存储在非瞬态机器可访问介质中。在至少一个其他实施例中,可以使用两个或更多个非瞬态机器可访问介质来存储组件的指令。例如,一个组件的指令可以存储在一个介质中,并且另一个组件的指令可以存储在另一个介质中。替代地,一个组件的指令的一部分可以存储在一个介质中,并且该组件的其他指令(以及其他组件的指令)可以存储在一个或多个其他介质中。指令还可以在分布式环境中使用,并且可以被本地和/或远程地存储以供单处理器或多处理器机器访问。

[0101] 此外,虽然已经关于以特定顺序执行的特定操作描述了一个或多个示例性过程,但是可以对这些过程应用许多修改以得到本发明的许多替代实施例。例如,替代实施例可

以包括使用比所有所公开的操作更少的操作的过程、使用附加操作的过程以及其中在此所公开的个别操作被组合、细分、重新排列或以其他方式改变的过程。

[0102] 鉴于从在此所描述的示例性实施例可以容易地得出的多种有用的排列，该详细描述旨在仅作为说明性的，并且不应被视为限制覆盖的范围。

[0103] 下面的示例涉及进一步的实施例。

[0104] 示例A1是一种具有密钥迁移能力的数据处理系统。所述数据处理系统包括处理元件、响应于所述处理元件的机器可访问介质以及在所述机器可访问介质中的数据。当所述数据由所述处理元件访问时，所述数据使所述数据处理系统能够成为执行包括以下各项的操作的目的数据处理系统：(a)从源数据处理系统接收包括主密钥的加密版本的密钥迁移块；(b)接收标识认证策略的用户输入；(c)接收标识上下文策略的用户输入；(d)基于所述标识的认证策略从所述目的数据处理系统的用户处收集认证数据；(e)基于所述标识的上下文策略收集所述目的数据处理系统的上下文数据；以及(f)使用所述认证数据和所述上下文数据来解密所述密钥迁移块。

[0105] 示例A2包括示例A1的特征，并且所述机器可访问介质被配置成在所述目的数据处理系统中提供可信执行环境(TEE)。此外，在所述机器可访问介质中的所述数据包括被配置成在所述TEE中执行的密钥迁移软件，并且所述密钥迁移软件被配置成使用所述认证数据和所述上下文数据来在所述目的数据处理系统的所述TEE中解密所述密钥迁移块。

[0106] 示例A3包括示例A1的特征，并且收集认证数据的所述操作包括从所述目的数据处理系统的所述用户处收集生物特征数据。示例A3还可以包括示例A2的特征。

[0107] 示例A4包括示例A1的特征，并且基于所述标识的认证策略收集认证数据的所述操作包括基于所述标识的认证策略收集两种或更多种不同类型的认证数据。示例A4还可以包括示例A2至A3中任何一项或多项的特征。

[0108] 示例A5包括示例A1的特征，并且所述操作进一步包括：(a)接收对被用于加密所述密钥迁移块中的所述主密钥的随机数进行标识的用户输入；以及(b)使用所述随机数来解密所述密钥迁移块。示例A5还可以包括示例A2至A4中任何一项或多项的特征。

[0109] 示例A6包括示例A5的特征，并且接收对被用于加密所述密钥迁移块中的所述主密钥的所述随机数进行标识的用户输入的所述操作包括接收大小小于16字节的索引。此外，所述随机数具有大于或等于16字节的大小；并且所述操作进一步包括使用所述索引从远程随机数服务器检索所述随机数。示例A5还可以包括示例A2至A4中任何一项或多项的特征。

[0110] 示例A7包括示例A1的特征，并且所述操作进一步包括基于标识所述上下文策略的所述用户输入从远程上下文策略服务器检索所述上下文策略。示例A7还可以包括示例A2至A6中任何一项或多项的特征。

[0111] 示例B1是一种用于迁移密钥的方法。所述方法包括：(a)在目的数据处理系统处，从源数据处理系统接收包括主密钥的加密版本的密钥迁移块；(b)在所述目的数据处理系统处，接收标识认证策略的用户输入；(c)在所述目的数据处理系统处，接收标识上下文策略的用户输入；(d)基于所述标识的认证策略从所述目的数据处理系统的用户处收集认证数据；(e)基于所述标识的上下文策略收集所述目的数据处理系统的上下文数据；以及(f)在所述目的数据处理系统处，使用所述认证数据和所述上下文数据来解密所述密钥迁移块。

[0112] 示例B2包括示例B1的特征。另外，所述目的数据处理系统包括可信执行环境(TEE)；并且由在所述目的数据处理系统的所述TEE中执行的密钥迁移软件来执行使用所述认证数据和所述上下文数据来解密所述密钥迁移块的所述操作。

[0113] 示例B3包括示例B1的特征。另外，收集认证数据的所述操作包括从所述目的数据处理系统的所述用户处收集生物特征数据。示例B3还可以包括示例B2的特征。

[0114] 示例B4包括示例B1的特征。另外，基于所述标识的认证策略收集认证数据的所述操作包括基于所述标识的认证策略收集两种或更多种不同类型的认证数据。示例B4还可以包括示例B2至B3中的任何一项或多项的特征。

[0115] 示例B5包括示例B1的特征。另外，所述方法包括：(a)在所述目的数据处理系统处，接收对被用于加密所述密钥迁移块的所述主密钥的随机数进行标识的用户输入；以及(b)使用所述随机数来解密所述密钥迁移块。示例B5还可以包括示例B2至B4中的任何一项或多项的特征。

[0116] 示例B6包括示例B5的特征。另外，接收对被用于加密所述密钥迁移块中的所述主密钥的所述随机数进行标识的用户输入的所述操作包括接收大小小于16字节的索引。此外，所述随机数具有大于或等于16字节的大小；并且所述方法进一步包括使用所述索引从远程随机数服务器检索所述随机数。示例B6还可以包括示例B2至B4中任何一项或多项的特征。

[0117] 示例B7包括示例B1的特征。另外，所述方法包括：基于标识所述上下文策略的所述用户输入从远程上下文策略服务器检索所述上下文策略。示例B7还可以包括示例B2至B6中任何一项或多项的特征。

[0118] 示例B8包括示例B1的特征。另外，所述方法包括：基于标识所述认证策略的所述用户输入从远程认证策略服务器检索所述认证策略。示例B8还可以包括示例B2至B7中任何一项或多项的特征。

[0119] 示例B9包括示例B1的特征。另外，使用所述认证数据和所述上下文数据来解密所述密钥迁移块的所述操作包括：(a)在密钥导出函数(KDF)中使用所述认证数据和所述上下文数据；(b)使用所述KDF来生成密钥加密密钥(KEK)；以及(c)使用所述KEK来解密所述密钥迁移块。示例B9还可以包括示例B2至B8中任何一项或多项的特征。

[0120] 示例B10包括示例B1的特征。另外，所述方法包括：(a)在所述目的数据处理系统处接收所述密钥迁移块之前，在所述源数据处理系统处从所述主密钥的所有者处接收用户输入，其中，所述用户输入选择所述认证策略和所述上下文策略；以及(b)响应于接收到选择所述认证策略和所述上下文策略的所述用户输入，使用所述选择的认证策略和所述选择的上下文策略来创建包括所述主密钥的所述加密版本的所述密钥迁移块。示例B10还可以包括示例B2至B9中任何一项或多项的特征。

[0121] 示例B11包括示例B10的特征。另外，所述源数据处理系统包括可信执行环境(TEE)，并且所述主密钥的明文版本驻留在所述源数据处理系统的所述TEE中。此外，在所述源数据处理系统的所述TEE中执行(a)接收选择所述认证策略和所述上下文策略的所述用户输入和(b)使用所述选择的认证策略和所述选择的上下文策略来创建所述密钥迁移块的所述操作。示例B11还可以包括示例B2至B9中任何一项或多项的特征。

[0122] 示例B12包括示例B10的特征。另外，所述方法包括：(a)在所述源数据处理系统处

从远程随机数服务器接收随机数列表和相应的索引；(b)在从所述远程随机数服务器接收到所述随机数列表之后，接收从所述随机数列表中选择随机数的用户输入；以及(c)在接收到选择所述随机数的所述用户输入之后，使用所述选择的随机数来生成所述密钥迁移块。示例B12也可以包括示例B2至B11中任何一项或多项的特征。

[0123] 示例C是包括用于迁移密钥的计算机指令的至少一个机器可访问介质。所述计算机指令响应于在数据处理系统上被执行而使所述数据处理系统能够执行根据示例B1至B12中任何一项或多项的方法。

[0124] 示例D是一种具有密钥迁移能力的数据处理系统。所述数据处理系统包括处理元件、响应于所述处理元件的至少一个机器可访问介质以及至少部分地存储在所述至少一个机器可访问介质中的计算机指令。另外，响应于被执行，所述计算机指令使所述数据处理系统能够执行根据示例B1至B12中任何一项或多项的方法。

[0125] 示例E是一种具有密钥迁移能力的数据处理系统。所述数据处理系统包括用于执行示例B1至B12中任何一项或多项的方法的装置。

[0126] 示例F1是一种用于促进密钥迁移的装置。所述装置包括非瞬态机器可访问介质和在所述机器可访问介质中的数据，所述数据当由目的数据处理系统访问时使所述目的数据处理系统能够执行包括以下各项的操作：(a)从源数据处理系统接收包括主密钥的加密版本的密钥迁移块；(b)接收标识认证策略的用户输入；(c)接收标识上下文策略的用户输入；(d)基于所述标识的认证策略从所述目的数据处理系统的用户处收集认证数据；(e)基于所述标识的上下文策略收集所述目的数据处理系统的上下文数据；以及(f)使用所述认证数据和所述上下文数据来解密所述密钥迁移块。

[0127] 示例F2包括示例F1的特征。此外，在所述机器可访问介质中的所述数据包括被配置成在所述目的数据处理系统的可信执行环境(TEE)中执行的密钥迁移软件。此外，所述密钥迁移软件被配置成使用所述认证数据和所述上下文数据来在所述目的数据处理系统的所述TEE中解密所述密钥迁移块。

[0128] 示例F3包括示例F1的特征。此外，收集认证数据的所述操作包括从所述目的数据处理系统的所述用户处收集生物特征数据。示例F3还可以包括示例F2的特征。

[0129] 示例F4包括示例F1的特征。此外，基于所述标识的认证策略收集认证数据的所述操作包括基于所述标识的认证策略收集两种或更多种不同类型的认证数据。示例F4还可以包括示例F2至F3中任何一项或多项的特征。

[0130] 示例F5包括示例F1的特征，并且所述操作进一步包括：(a)接收对被用于加密所述密钥迁移块中的所述主密钥的随机数进行标识的用户输入；以及(b)使用所述随机数来解密所述密钥迁移块。示例F5还可以包括示例F2至F4中任何一项或多项的特征。

[0131] 示例F6包括示例F5的特征。此外，接收对被用于加密所述密钥迁移块中的所述主密钥的所述随机数进行标识的用户输入的所述操作包括接收大小小于16字节的索引。此外，所述随机数具有大于或等于16字节的大小；并且所述操作进一步包括使用所述索引从远程随机数服务器检索所述随机数。示例F6还可以包括示例F2至F4中任何一项或多项的特征。

[0132] 示例F7包括示例F1的特征。此外，所述操作进一步包括基于标识所述上下文策略的所述用户输入从远程上下文策略服务器检索所述上下文策略。示例F7还可以包括示例F2

至F6中任何一项或多项的特征。

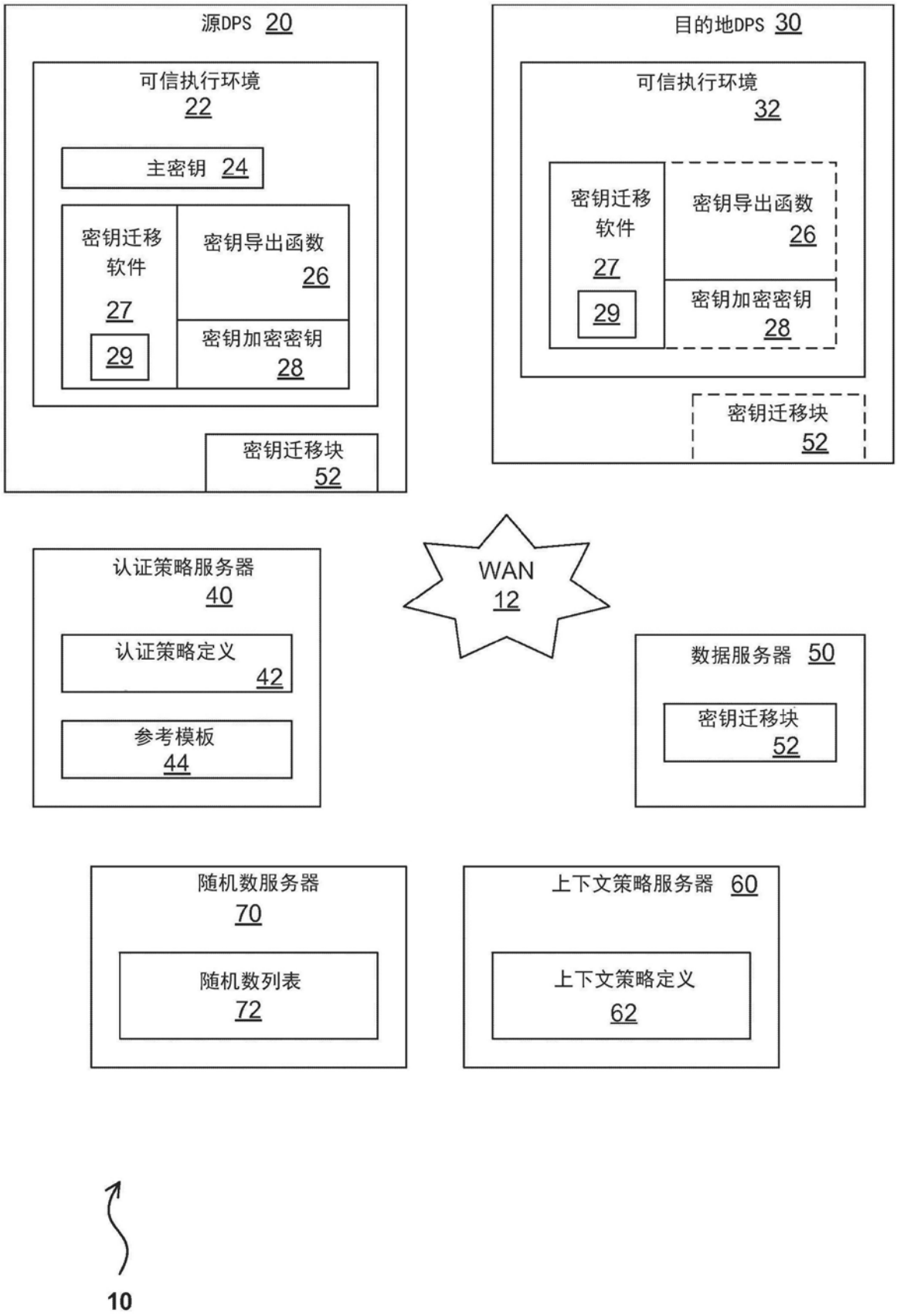

源DPS 20
可信执行环境
22
主密钥 24
密钥迁移软件
27
29
密钥导出函数
26
密钥加密密钥
28
密钥迁移块
52
目的地DPS 30
可信执行环境
32
密钥迁移软件
27
29
密钥导出函数
26
密钥加密密钥
28
密钥迁移块
52
认证策略服务器
40
认证策略定义
42
参考模板
44
WAN
12
数据服务器 50
密钥迁移块
52
随机数服务器
70
随机数列表
72
上下文策略服务器 60
上下文策略定义
62
10

图1

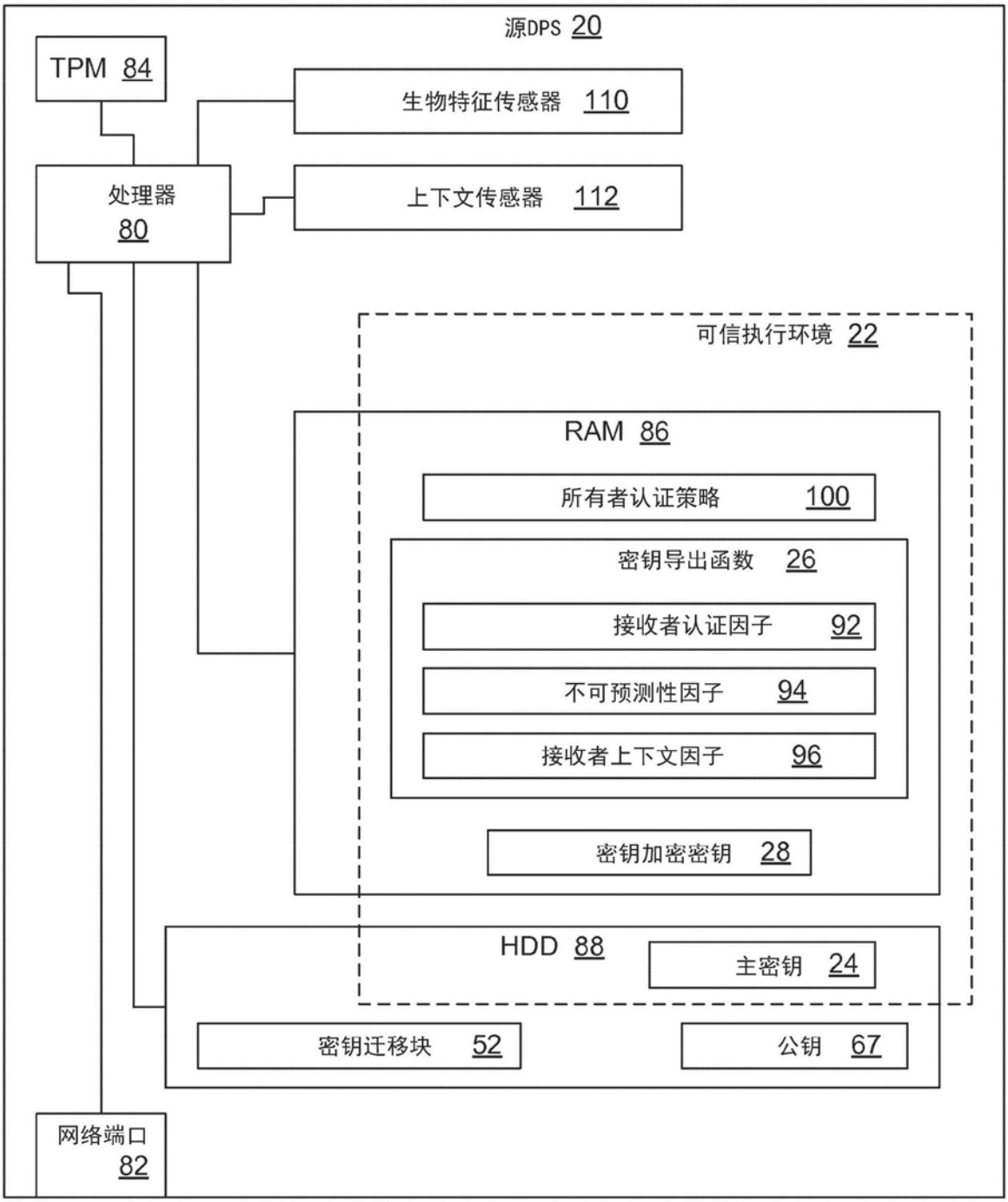

源DPS 20
TPM 84
生物特征传感器 110
处理器 80
上下文传感器 112
可信执行环境 22
RAM 86
所有者认证策略 100
密钥导出函数 26
接收者认证因子 92
不可预测性因子 94
接收者上下文因子 96
密钥加密密钥 28
HDD 88
主密钥 24
密钥迁移块 52
公钥 67
网络端口 82

图2

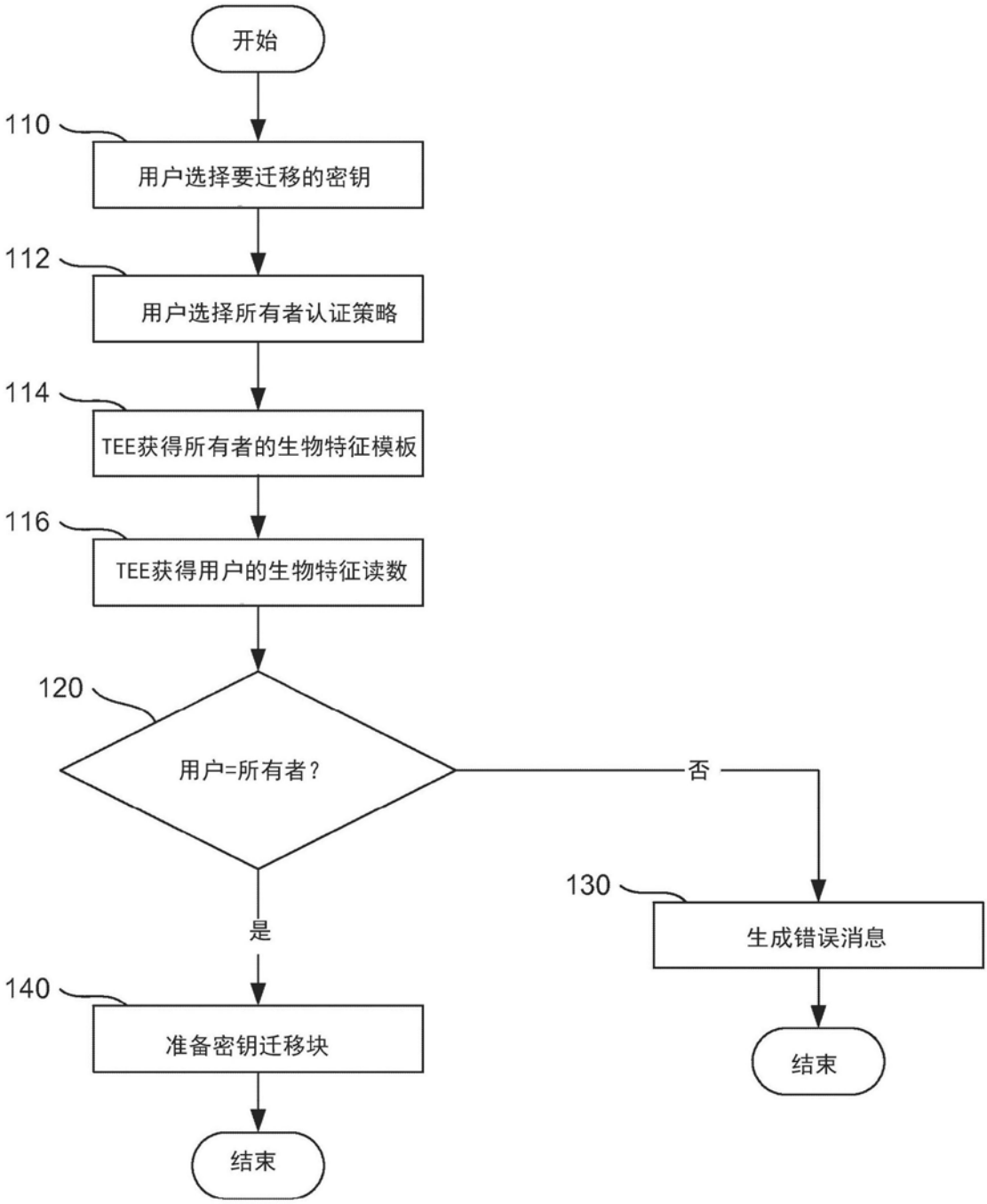

开始
110
用户选择要迁移的密钥
112
用户选择所有者认证策略
114
TEE获得所有者的生物特征模板
116
TEE获得用户的生物特征读数
120
用户=所有者？
否
是
130
生成错误消息
结束
140
准备密钥迁移块
结束

图3

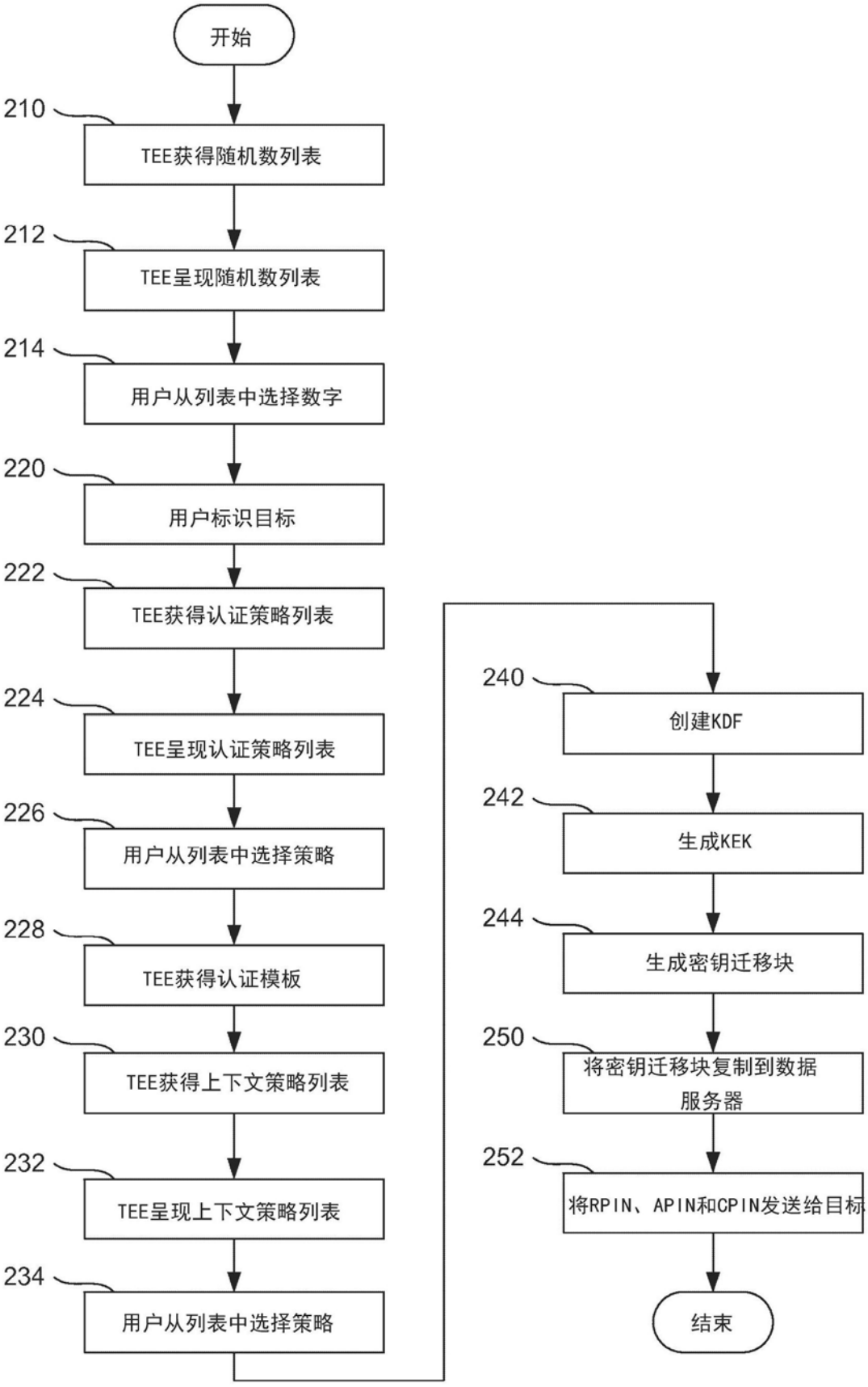

开始
210
TEE获得随机数列表
212
TEE呈现随机数列表
214
用户从列表中选择数字
220
用户标识目标
222
TEE获得认证策略列表
224
TEE呈现认证策略列表
226
用户从列表中选择策略
228
TEE获得认证模板
230
TEE获得上下文策略列表
232
TEE呈现上下文策略列表
234
用户从列表中选择策略
240
创建KDF
242
生成KEK
244
生成密钥迁移块
250
将密钥迁移块复制到数据服务器
252
将RPIN、APIN和CPIN发送给目标
结束

图4

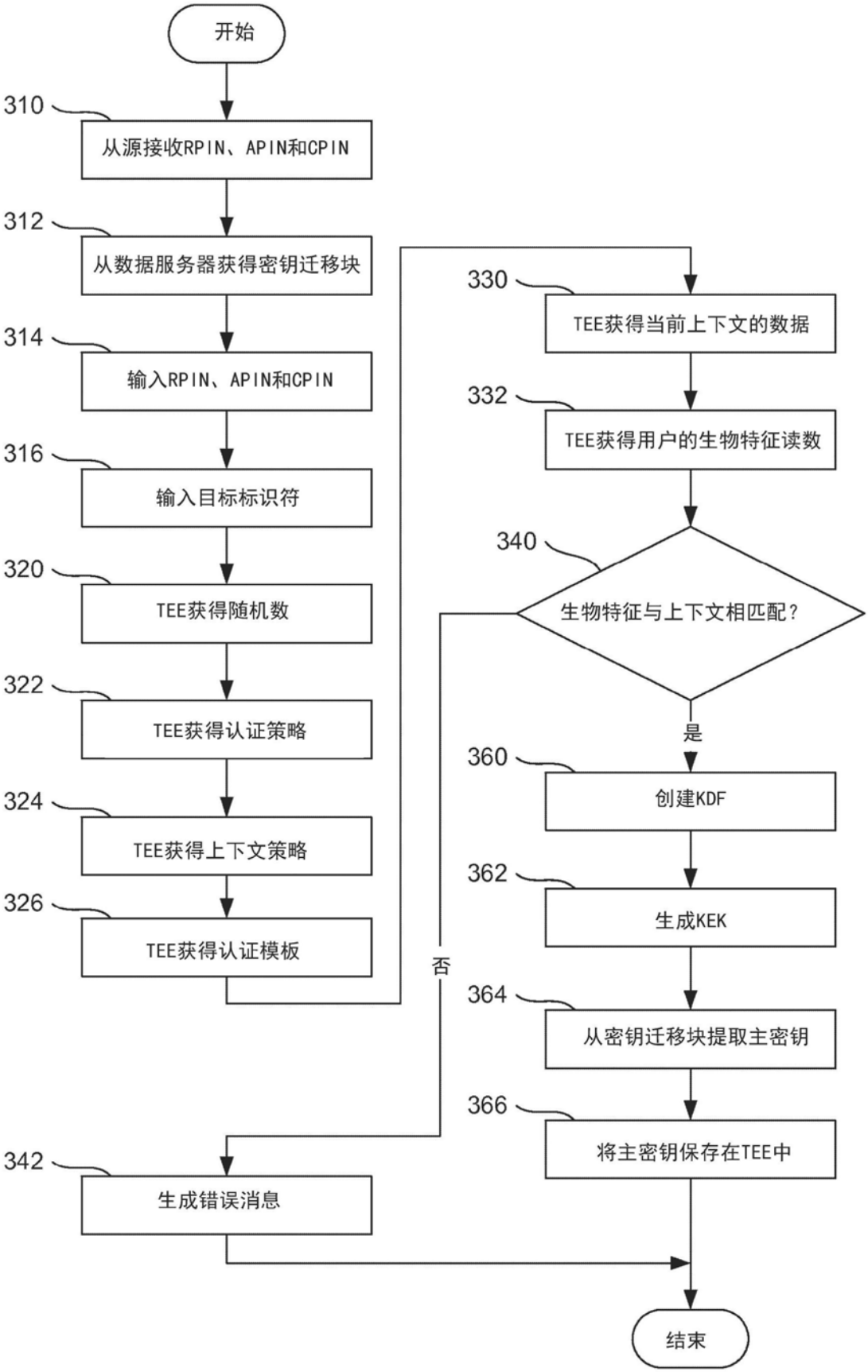

开始
310
从源接收RPIN、APIN和CPIN
312
从数据服务器获得密钥迁移块
314
输入RPIN、APIN和CPIN
316
输入目标标识符
320
TEE获得随机数
322
TEE获得认证策略
324
TEE获得上下文策略
326
TEE获得认证模板
330
TEE获得当前上下文的数据
332
TEE获得用户的生物特征读数
340
生物特征与上下文相匹配?
是
否
360
创建KDF
362
生成KEK
364
从密钥迁移块提取主密钥
366
将主密钥保存在TEE中
342
生成错误消息
结束

图5