(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 109983732 B
(45)授权公告日 2022.04.08

(21)申请号 201780072591.5
(22)申请日 2017.12.01
(65)同一申请的已公布的文献号
申请公布号 CN 109983732 A
(43)申请公布日 2019.07.05
(30)优先权数据
1620553.6 2016.12.02 GB
(85)PCT国际申请进入国家阶段日
2019.05.23
(86)PCT国际申请的申请数据
PCT/EP2017/025349 2017.12.01
(87)PCT国际申请的公布数据
WO2018/099606 EN 2018.06.07

(73)专利权人 古鲁洛吉克微系统公司
地址 芬兰图尔库
(72)发明人 托马斯·卡开宁 奥西·卡雷沃 米科·萨尔博姆
(74)专利代理机构 北京英赛嘉华知识产权代理有限责任公司 11204
代理人 王达佐 熊苹

(51)Int.Cl.
H04L 9/08(2006.01)
H04W 12/04(2021.01)
G06F 21/62(2013.01)
H04W 12/30(2021.01)
G06F 21/45(2013.01)
H04L 9/30(2006.01)

审查员 徐千慧

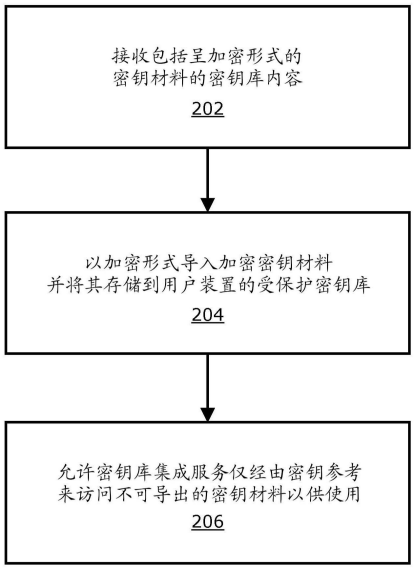
权利要求书3页 说明书14页 附图4页

(54)发明名称

保护密钥库内容的使用

(57)摘要

提供了一种保护最终用户的给定用户装置处的密钥库内容的使用的方法。在给定用户装置处接收密钥库内容。密钥库内容包括使用与给定用户装置兼容的加密凭证进行加密的密钥材料。密钥库内容呈与给定用户装置兼容的格式。密钥库内容的经加密的密钥材料导入到给定用户装置的受保护密钥库,其中密钥库内容的所有密钥材料被一次性导入。密钥材料以加密形式存储在受保护密钥库处,并且不能从密钥库中导出。在受保护密钥库内部,允许给定用户装置的一个或多个密钥库集成服务仅经由密钥引用来访问不可导出的密钥材料以供使用。



CN 109983732 B

1.一种保护最终用户的给定用户装置处的密钥库内容的使用的方法,其特征在于,所述方法包括以下步骤:

步骤(i) 在所述给定用户装置处接收所述密钥库内容,所述密钥库内容包括使用与所述给定用户装置兼容的加密凭证进行加密的密钥材料,所述密钥库内容由密钥服务提供商以与所述给定用户装置兼容的格式创建并从所述密钥服务提供商接收;

步骤(ii) 将所述密钥库内容的经加密的密钥材料导入到所述给定用户装置的受保护密钥库,并且将所述密钥材料以加密形式存储在所述受保护密钥库处,其中所述密钥库内容的所有被加密的密钥材料被一次性导入,并且其中所述密钥库内容以所述密钥材料不能从所述密钥库导出的方式存储在所述密钥库处,以及其中使用以下项通过所述被加密的密钥材料生成密钥:

-密钥偏移量,

-位偏移量,和/或

-字节偏移量;以及

步骤(iii) 在所述给定用户装置的所述受保护密钥库内部,允许所述给定用户装置的一个或多个密钥库集成服务仅经由密钥引用来访问不可导出的密钥材料以供使用。

2.根据权利要求1所述的方法,其特征在于,所述方法包括在所述给定用户装置的所述受保护密钥库内部,对待由所述给定用户装置的所述一个或多个密钥库集成服务使用的一个或多个所述密钥材料进行解密。

3.根据权利要求1或2所述的方法,其特征在于,在所述步骤(ii)处,所述密钥库内容被导入为单个数据文件。

4.根据权利要求1所述的方法,其特征在于,所述方法包括在所述密钥库内容内,接收待用于经由所述密钥引用来引用所述密钥材料的索引。

5.根据权利要求1所述的方法,其特征在于,所述方法包括在所述给定用户装置处,生成待用于经由所述密钥引用来引用所述密钥材料的索引。

6.根据权利要求1所述的方法,其特征在于,借助于偏移量来实施所述密钥引用,其中所述密钥材料基于所述偏移量来识别。

7.根据权利要求1所述的方法,其特征在于,所述密钥库是基于硬件的,并且在所述步骤(ii)处进行的导入步骤包括将存储在基于硬件的密钥库处的所述密钥材料绑定到所述给定用户装置的处理硬件的安全区域。

8.根据权利要求1所述的方法,其特征在于,所述方法包括将被授权为使用所述给定用户装置的所述密钥库的、在所述给定用户装置处托管的一个或多个可信软件应用程序或生态系统进程与所述密钥库集成。

9.根据权利要求8所述的方法,其特征在于,所述方法包括从可信软件服务提供商导入用于提供密钥库集成服务的所述一个或多个可信软件应用程序,其中当在所述给定用户装置处执行时,所述一个或多个可信软件应用程序能够操作以提供一个或多个密钥库集成服务并且被提供来自所述给定用户装置的内核的保护。

10.根据权利要求1所述的方法,其特征在于,所述方法包括在所述密钥服务提供商处,使用由所述给定用户装置或由所述密钥服务提供商提供的加密密钥数据来对所述密钥库内容进行加密。

11.根据权利要求1所述的方法,其特征在于,所述方法包括在所述给定用户装置处,使用所述最终用户的生物凭证的令牌来保护所述密钥库。

12.根据权利要求11所述的方法,其特征在于,所述最终用户的生物凭证包括以下中的至少一者:所述最终用户的指纹、所述最终用户的面部特征、所述最终用户的DNA图谱、所述最终用户的虹膜辨识、所述最终用户的行走方式、所述最终用户的书写方式、所述最终用户的心跳模式。

13.根据权利要求1所述的方法,其特征在于,在所述步骤(i)处在所述给定用户装置处以对称加密形式来接收所述密钥材料。

14.根据权利要求13所述的方法,其特征在于,所述方法包括在所述密钥服务提供商处,通过采用对称高级加密标准(AES)加密来对所述密钥材料进行加密。

15.根据权利要求1所述的方法,其特征在于,在所述步骤(i)处经由不安全的传输来接收所述密钥库内容。

16.根据权利要求1所述的方法,其特征在于,所述密钥材料包括以下中的至少一者:

(a)用于对称数据加密的秘密密钥,

(b)用于公钥基础设施(PKI)等效用法的私有密钥和公开密钥,

(c)待用于密码学、签名、完整性、验证、认证、授权的证书,

(d)用于生成密钥的一个或多个密钥生成器。

17.一种其上存储有计算机可读指令的非暂态计算机可读存储介质,所述计算机可读指令能够被处理器执行以执行根据权利要求1至16中任一项所述的方法。

18.一种用于保护最终用户的给定用户装置处的密钥库内容的使用的系统,包括处理器和其上存储有计算机程序的存储器,其特征在于,所述计算机程序能够被所述处理器执行以:

(i) 在所述给定用户装置处接收所述密钥库内容,所述密钥库内容包括使用与所述给定用户装置兼容的加密凭证进行加密的密钥材料,所述密钥库内容由密钥服务提供商以与所述给定用户装置兼容的格式创建并从所述密钥服务提供商接收;

(ii) 将所述密钥库内容的经加密的密钥材料导入到所述给定用户装置的受保护密钥库,并且将所述密钥材料以加密形式存储在所述受保护密钥库处,其中所述密钥库内容的所有被加密的密钥材料被一次性导入,并且其中所述密钥库内容以所述密钥材料不能从所述密钥库导出的方式存储在所述密钥库处,以及其中使用以下项通过所述被加密的密钥材料生成密钥:

-密钥偏移量,

-位偏移量,和/或

-字节偏移量;以及

(iii) 在所述给定用户装置的所述受保护密钥库内部,允许所述给定用户装置的一个或多个密钥库集成服务仅经由密钥引用来访问不可导出的密钥材料以供使用。

19.根据权利要求18所述的系统,其特征在于,所述计算机程序能够被执行以在所述给定用户装置的所述受保护密钥库内部,对待由所述给定用户装置的所述一个或多个密钥库集成服务使用的一个或多个所述密钥材料进行解密。

20.根据权利要求18或19所述的系统,其特征在于,当在(ii)处进行导入时,所述计算

机程序能够被执行以将所述密钥库内容导入为单个数据文件。

21.根据权利要求18所述的系统,其特征在于,所述计算机程序能够被执行以在所述密钥库内容内接收待用于经由所述密钥引用来引用所述密钥材料的索引。

22.根据权利要求18所述的系统,其特征在于,所述计算机程序能够被执行以在所述给定用户装置处生成待用于经由所述密钥引用来引用所述密钥材料的索引。

23.根据权利要求18所述的系统,其特征在于,所述密钥引用是借助于偏移量来实施的,其中所述密钥材料基于所述偏移量来识别。

24.根据权利要求18所述的系统,其特征在于,所述密钥库是基于硬件的,并且当在(ii)处进行导入时,所述计算机程序能够被执行以将存储在所述基于硬件的密钥库处的所述密钥材料绑定到所述给定用户装置的处理硬件的安全区域。

25.根据权利要求18所述的系统,其特征在于,所述计算机程序能够被执行以:将被授权为使用所述给定用户装置的所述密钥库的、在所述给定用户装置处托管的一个或多个可信软件应用程序或生态系统进程与所述密钥库集成。

26.根据权利要求25所述的系统,其特征在于,所述计算机程序能够被执行以从可信软件服务提供商导入用于提供密钥库集成服务的所述一个或多个可信软件应用程序,其中当在所述给定用户装置处执行时,所述一个或多个可信软件应用程序能够操作以提供一个或多个密钥库集成服务并且被提供来自所述给定用户装置的内核的保护。

27.根据权利要求18所述的系统,其特征在于,所述密钥服务提供商能够操作为使用由所述给定用户装置或由所述密钥服务提供商提供的加密密钥数据来对所述密钥库内容进行加密。

28.根据权利要求18所述的系统,其特征在于,在所述给定用户装置处使用所述最终用户的生物凭证的令牌来保护所述密钥库。

29.根据权利要求28所述的系统,其特征在于,所述最终用户的生物凭证包括以下中的至少一者:所述最终用户的指纹、所述最终用户的面部特征、所述最终用户的DNA图谱、所述最终用户的虹膜辨识、所述最终用户的行走方式、所述最终用户的书写方式、所述最终用户的心跳模式。

30.根据权利要求18所述的系统,其特征在于,在(i)处在所述给定用户装置处以对称加密形式接收所述密钥材料。

31.根据权利要求30所述的系统,其特征在于,所述密钥服务提供商能够操作以通过采用对称高级加密标准(AES)加密来对所述密钥材料进行加密。

32.根据权利要求18所述的系统,其特征在于,当在(i)处接收时,所述系统能够操作以经由不安全的传输来接收所述密钥库内容。

33.根据权利要求18所述的系统,其特征在于,所述密钥材料包括以下中的至少一者:

(a)用于对称数据加密的秘密密钥,

(b)用于公钥基础设施(PKI)等效用法的私有密钥和公开密钥,

(c)待用于密码学、签名、完整性、验证、认证、授权的证书,

(d)用于生成密钥的一个或多个密钥生成器。

保护密钥库内容的使用

技术领域

[0001] 本公开涉及用于保护最终用户的用户装置处的密钥库内容的使用的系统，例如，涉及依赖于使用密钥材料来实现数据安全的数据安全系统。此外，本公开还涉及保护最终用户的用户装置处的密钥库内容的使用的方法。此外，本公开还涉及包括其上存储有计算机可读指令的非暂态计算机可读存储介质的计算机程序产品，所述计算机可读指令能够由包括处理硬件的计算机化装置执行以执行上述方法。

背景技术

[0002] 对在用户装置上存储用户敏感数据的需求经常出现，因为目前存在的各种服务和功能被设计为在用户装置上作为软件应用程序运行，例如用于进行支付的软件应用程序。作为第一示例，目前存在用于银行和支付服务的多个应用程序，其中所述多个应用程序需要安全布置以用于在使用银行和支付服务时对客户维持强有力的保护，以便旨在避免恶意第三方侵入此类服务来窃取金钱。作为第二示例，用户可能需要存储秘密或私有密钥来访问受保护的电子邮件。出于这些和许多其它原因，非常希望提供一种用于处理与密钥材料有关的密钥库的稳健解决方案。

[0003] 存在许多安全服务提供商能够经由多个“生态系统”平台来访问，所述平台的密钥库是基于软件的。例如，Android™生态系统平台目前备受公众关注，因为全球有大量使用Android™生态系统平台的移动装置，例如平板状计算装置。参考谷歌文档，Android™密钥库系统将密码密钥存储在容器中以使得从给定安卓兼容装置提取更加困难。Android™密钥库系统在当前可用的密钥库系统当中在安全问题上是最先进的，但仍然遗憾的是，缺乏在市场上大量销售的当代装置中提供高效安全解决方案所需要的非常重要的功能性。Android™密钥库提供了一套基本完整的安全算法，诸如密码、密钥生成器、密钥工厂、密钥对生成器、mac和签名。所有这些服务均在由密钥库系统支持的硬件内部运行以使得使用高效且方便，但是没有考虑到真实世界的密码要求。

[0004] 此外，仅在几年时间里，移动电话的使用量就有了巨大增长，而且多家厂商拥有不同的装置型号，由不同的生态系统提供动力，诸如Google® Android™、Apple® iOS™、Microsoft® Windows®等等。从安全角度来看出现的问题是，每个生态系统具有其自己的安全解决方案以保护基于硬件或基于软件的密钥库中的用户敏感数据。这使得应用程序开发者即使在理论上也很难理解安全相关实施，尽管这是在基本层面上理解。几乎每个生态系统都具有其自己的密钥库解决方案，但从当前迫切需要来看，希望把重点放在移动平台上，因为几乎每个人都将很快拥有某种智能电话和大量不同应用程序，这些应用程序需要恰当实施的密钥库来将用户敏感密钥材料保存在其中。理论上，密钥库几乎满足任何已知安全问题，但实际上，其软件实施并不能满足片上系统(SoC)硬件设计的可靠解决方案。

[0005] 首先，Android™密钥库的设计不是为了导入数千或数百万个秘密密钥(即，密钥材料)，而是设计为仅维持几个秘密密钥。Android™密钥库是针对相同密钥被一次又一次地用

于加密目的的场景来设计的。其次，Android™密钥库支持一次仅导入一个纯原始密钥，这可能会暴露给恶意方。这是因为Android™密钥库的安全是基于不对称加密，这是非常缓慢的计算过程。

[0006] 此外，还有一些常规上已知的基于软件的密钥库解决方案，其中“充气城堡”(别名“BC”)是最知名的提供商。与基于硬件的Android™密钥库相比，BC支持用于呈抽象语法标记一(ASN.1)格式的受保护密钥材料的密钥库导入功能性，其可以一次将一个以上的密钥安全地导入到密钥库中。BC的主要问题是，密钥材料没有完全防止提取，因为密钥材料是从密钥库外部请求的并且被提供给另一个接着使用密钥材料的软件应用程序。这使得恶意第三方有可能从密钥库中检索与经过认证的请求相关的密钥材料。明确地说，在给定BC密钥库中没有对密钥材料加索引，这可能会迫使向恶意方泄露敏感的密钥材料。

发明内容

[0007] 本公开旨在旨在提供一种用于保护最终用户的给定用户装置处的密钥库内容的使用的改进系统。

[0008] 此外，本公开旨在提供一种保护最终用户的给定用户装置处的密钥库内容的使用的改进方法。

[0009] 本公开的另一个目的是至少部分克服如上所讨论的现有技术的至少一些问题。

[0010] 在第一方面，本公开的实施方式提供一种保护最终用户的给定用户装置处的密钥库内容的使用的方法，其特征在于，该方法包括以下步骤：

[0011] (i)在给定用户装置处接收密钥库内容，所述密钥库内容包括使用与给定用户装置兼容的加密凭证进行加密的密钥材料，密钥库内容由密钥服务提供商以与给定用户装置兼容的格式创建并从密钥服务提供商接收；

[0012] (ii)将密钥库内容的经加密的密钥材料导入到给定用户装置的受保护密钥库，并且将密钥材料以加密形式存储在受保护密钥库处，其中密钥库内容的所有密钥材料被一次性导入，并且其中密钥库内容以密钥材料不能从密钥库导出的方式存储在密钥库处；以及

[0013] (iii)在给定用户装置的受保护密钥库内部，允许给定用户装置的一个或多个密钥库集成服务仅经由密钥引用来访问不可导出的密钥材料以供使用。

[0014] 本公开的实施方式的优势在于，通过采用从密钥服务提供商到最终用户的给定用户装置的完整端到端过程，来促进密钥库内容抵御未授权访问的完整保护，其中密钥库内容的密钥材料在该过程的任何步骤处都不会被暴露或不安全地处理，一旦存储在给定用户装置的受保护密钥库处就不可导出，并且能够仅经由密钥引用而被与受保护密钥库集成的服务访问以供使用。

[0015] 在第二方面，本公开的实施方式提供一种计算机程序产品，包括其上存储有计算机可读指令的非暂态计算机可读存储介质，计算机可读指令能够由包括处理硬件的计算机化装置执行以执行根据前述第一方面的方法。

[0016] 在第三方面，本公开的实施方式提供一种用于保护最终用户的给定用户装置处的密钥库内容的使用的系统，其特征在于，系统能够操作以：

[0017] (i)在给定用户装置处接收密钥库内容，密钥库内容包括使用与给定用户装置兼容的加密凭证进行加密的密钥材料，密钥库内容由密钥服务提供商以与给定用户装置兼容

的格式创建并从密钥服务提供商接收；

[0018] (ii)将密钥库内容的经加密的密钥材料导入到给定用户装置的受保护密钥库，并且将密钥材料以加密形式存储在受保护密钥库处，其中密钥库内容的所有密钥材料被一次性导入，并且其中密钥库内容以密钥材料不能从密钥库导出的方式存储在密钥库处；以及

[0019] (iii)在给定用户装置的受保护密钥库内部，允许给定用户装置的一个或多个密钥库集成服务仅经由密钥引用来访问不可导出的密钥材料以供使用。

[0020] 从附图以及结合所附权利要求书解释的说明性实施方式的详细描述中，本公开的其它方面、优点、特征和目的将变得显而易见。

[0021] 应领会，在不脱离由所附权利要求书所限定的本公开的范围的情况下，本公开的特征易于以各种组合进行组合。

附图说明

[0022] 当结合附图阅读时更好地理解以上发明内容以及下面对说明性实施方式的详细描述。为了说明本公开，在附图中示出了本公开的示例性构造。然而，本公开不限于本文所公开的特定方法和设备。此外，本领域的技术人员将理解附图不是按比例绘制的。在任何可能之处，相同的元件已经由相同的标号指示。

[0023] 现在将参考以下各图仅以举例方式描述本公开的实施方式，其中：

[0024] 图1A是根据本公开的实施方式的用于保护最终用户的给定用户装置处的密钥库内容的使用的系统的示意图；

[0025] 图1B是根据本公开的实施方式的保护给定用户装置处的密钥库内容的使用的完整端到端过程流程的示意图；

[0026] 图1C是根据本公开的实施方式的如何将密钥库内容导入并加载到给定用户装置的受保护密钥库的示意图；以及

[0027] 图2是描绘根据本公开的实施方式的保护最终用户的给定用户装置处的密钥库内容的使用的方法的步骤的流程图。

[0028] 在附图中，带下划线数字用于表示带下划线数字上方的项目或带下划线数字邻近的项目。当数字不带下划线而是附有相关联箭头时，所述不带下划线数字用于标识箭头所指向的总体项目。

具体实施方式

[0029] 以下详细描述说明了本公开的实施方式及其可实施的方案。虽然已经公开了实行本公开的一些模式，但是本领域的技术人员将认识到，用于实现或实践本公开的其它实施例也是可能的。

[0030] 在第一方面，本公开的实施方式提供保护最终用户的给定用户装置处的密钥库内容的使用的方法，其特征在于，该方法包括以下步骤：

[0031] (i)在给定用户装置处接收密钥库内容，所述密钥库内容包括使用与给定用户装置兼容的加密凭证进行加密的密钥材料，密钥库内容由密钥服务提供商以与给定用户装置兼容的格式创建并从密钥服务提供商接收；

[0032] (ii)将密钥库内容的经加密的密钥材料导入到给定用户装置的受保护密钥库，并

且将密钥材料以加密形式存储在受保护密钥库处，其中密钥库内容的所有密钥材料被一次性导入，并且其中密钥库内容以密钥材料不能从密钥库导出的方式存储在密钥库处；以及

[0033] (iii)在给定用户装置的受保护密钥库内部，允许给定用户装置的一个或多个密钥库集成服务仅经由密钥引用来访问不可导出的密钥材料以供使用。

[0034] 任选地，除了密钥材料之外，受保护密钥库还包括关于被授权以使用存储在受保护密钥库处的密钥材料的最终用户和/或最终用户群组的信息。额外地或替代地，任选地，受保护密钥库包括与密钥材料的使用相关的其它信息。

[0035] 贯穿本公开，术语“最终用户”涵盖人类用户以及机器。作为示例，最终用户可以是注册的中继机器。这对于使用上述方法来辨识并验证执行机器到机器通信的服务器的情况特别有利。

[0036] 将了解，保护密钥库以仅供最终用户使用，即防止除了经授权的最终用户之外的任何人进行未授权使用，并且此类对密钥库的保护与被导入的密钥材料的加密无关。换句话说，使用一个或多个不同秘密密钥(诸如一个或多个预共享密钥)对密钥材料进行加密。

[0037] 任选地，在步骤(i)处以对称加密形式接收密钥材料。任选地，在这点上，使用对称密钥对密钥材料进行加密。

[0038] 任选地，所述方法包括在给定用户装置的受保护密钥库内部，对一个或多个密钥材料进行解密以由给定用户装置的一个或多个密钥库集成服务使用。

[0039] 贯穿本公开，术语“密钥引用”大体上指的是指代并识别存储在受保护密钥库处的给定密钥材料的给定引用。换句话说，通过给定密钥引用，知道将使用哪个密钥材料(例如，密钥或证书)，并且任选地，待使用的密钥材料位于受保护密钥库的哪个位置。根据本公开的实施例，决不从密钥库提取密钥材料本身。

[0040] 根据实施方式，借助于密钥材料的索引来实施密钥引用。任选地，索引是按出现次序排列的密钥材料的序数。任选地，该方法包括在密钥库内容内接收待用于经由密钥引用来引用密钥材料的索引。替代地，任选地，该方法包括在给定用户装置处生成待用于经由密钥引用来引用密钥材料的索引。作为示例，索引可以以与在密钥库内容中包括密钥材料的次序对应的连续方式来生成。例如，可以在给定用户装置向密钥服务提供商进行初始注册时或者在对密钥材料进行解密期间生成索引。

[0041] 根据另一实施例，通过偏移量来实施密钥引用，将基于该偏移量来识别密钥材料。将了解，给定偏移量指代并识别存储在受保护密钥库处的给定密钥材料。出于说明目的，稍后提供偏移量的一些示例。

[0042] 根据本公开的实施例，通过采用从密钥服务提供商到最终用户的给定用户装置的完整端到端过程来促进对密钥库内容的完整保护以抵御未授权访问，其中密钥库内容的密钥材料在该过程的任何步骤处都不会被暴露或不安全地处理。以加密形式创建密钥库内容并将其传递到给定用户装置。这有可能防止第三方窃听。在给定用户装置处，密钥库内容被一次性导入到给定用户装置的密钥库。

[0043] 任选地，作为包含所有密钥材料的单个列表(仅出于方便起见，下文称为“密钥代码列表”)来接收密钥库内容。替代地，任选地，作为多个密钥代码列表来接收密钥库内容。将了解，可以同时导入多个密钥代码列表。不管对不同密钥代码列表(即，密钥材料)进行加密的形式如何，所有密钥材料都是被一次性导入。

[0044] 任选地，在步骤(ii)处，作为单个数据文件将密钥库内容导入到给定用户装置。将了解，密钥库内容中所包括的密钥材料的数目可以多达数千，有可能数百万。在此类情况下，与常规密钥库技术相比，作为单个数据文件导入密钥库内容具有若干优点。

[0045] 仅出于说明目的，现在将考虑上述系统的示例实施，其采用Gurulogic Microsystem Oy的专有产品“*Starwindow*®”。在此类实施中，一旦在给定用户装置处接收到密钥库内容，则使用由“*Starwindow*®”产品的密钥库提供的“加载”功能来将所有密钥材料一次性导入到密钥库。任选地，“加载”功能还在密钥库内安全地对密钥材料进行解密以实现其快速使用。将了解，“加载”功能可以用于一次性导入所有密钥材料，即使在密钥库内容中包括有数百万个密钥材料时。

[0046] 上述同时导入大量密钥材料是通过不同实施方案来实现的，诸如以下选项：

[0047] 选项A：

[0048] 密钥代码列表包括八个不同128位密钥；这个密钥代码列表消耗128字节的存储空间。因为最小单位大小是一个字节，其代表八个位，所以128位密钥消耗16字节的存储空间。将了解，密钥通常表示最大可能的熵，从而加强了由此获得的保护，并且因此这些密钥不能用传统压缩技术来压缩。

[0049] 可以如下表示示例的密钥代码列表：

[0050] KeyCodeListA:UInt8的数组[0..15]中的数组[0..7]＝

[0051] (0x4B,0xDA,0x72,0x44,0xB3,0x12,0x07,0x43,0x6F,0x65,0x83,0x8C,0xF5,0x3F,0xF1,0x08,//密钥1

[0052] 0xCA,0x1E,0x7F,0xDF,0x5C,0x7F,0x78,0x0C,0x55,0x88,0x96,0x0B,0xA9,0xD9,0x22,0x6F,//密钥2

[0053] 0xB6,0x43,0x73,0x84,0x57,0x86,0x66,0xF8,0x79,0xB0,0xCC,0xA0,0x16,0x13,0x42,0xDF,//密钥3

[0054] 0xF0,0x6B,0x2B,0xF8,0x68,0x5A,0x31,0xCF,0x9A,0x65,0xF1,0xC7,0x94,0x62,0xDD,0x9B,//密钥4

[0055] 0xB1,0x28,0x68,0xEE,0x1B,0x4D,0x43,0x07,0xE4,0x97,0xFF,0x00,0x01,0xFF,0x00,0xE0,//密钥5

[0056] 0xEE,0x1F,0xFD,0xA9,0x69,0xE5,0xFF,0x00,0xDF,0x67,0x67,0xF70xB0,0xB9,0xAA,0x77,//密钥6

[0057] 0x9E,0x55,0xAC,0xE3,0xFE,0x16,0x27,0xD9,0xED,0xE1,0x2B,0xFF0x00,0x13,0xFF,0x00,//密钥7

[0058] 0xB5,0xE2,0x28,0x56,0x2D,0xBF,0xE9,0x39,0x1F,0xF0,0x74,0x9F,0x95,0x19,0x05,0x07,//密钥8)；

[0059] 其中16个字节的连续序列各自代表密钥。在这个示例中，密钥是基于密钥偏移量来生成的，即通过将偏移量增加密钥的大小(在这个示例中为16个字节)来生成。

[0060] 任选地，一次性导入是通过“压缩”待传递的密钥来完成的。存在至少两种不同方式(即，选项1)“B”和“C”，以及2)“D”)来实施这一点：

[0061] 选项B：

[0062] 仅出于说明目的，现在将相对于同一示例密钥代码列表来描述选项“B”。任选地，

通过基于字节偏移量而不是密钥偏移量来选择密钥，从同一密钥代码列表生成128个密钥(＝8×16)。作为示例，前三个密钥可以如下生成：

[0063] KeyCodeListB:UInt8的数组[0..127]＝

[0064] (0x4B,0xDA,0x72,0x44,0xB3,0x12,0x07,0x43,0x6F,0x65,0x83,0x8C,0xF5,0x3F,0xF1,0x08,//来自字节偏移量“0”的密钥1

[0065] (0xDA,0x72,0x44,0xB3,0x12,0x07,0x43,0x6F,0x65,0x83,0x8C,0xF5,0x3F,0xF1,0x08,0xCA//来自字节偏移量“1”的密钥2

[0066] (0x72,0x44,0xB3,0x12,0x07,0x43,0x6F,0x65,0x83,0x8C,0xF5,0x3F,0xF1,0x08,0xCA,0x1E,//来自字节偏移量“2”的密钥3

[0067] 将了解，可以通过以任何预定义次序选择偏移量来生成密钥，并且不一定总是通过将偏移量增加1来生成密钥，如在选项“A”中提供的示例密钥代码列表的上述示例中所说明。

[0068] 选项C：

[0069] 使用同一密钥代码列表，有可能通过基于位偏移量而不是密钥和字节偏移量选择密钥来生成1024个密钥(＝8×16×8个密钥)而不是上述八(8)个和128个密钥。例如，前三个16字节密钥(在选项“B”中生成)可以如下转换为位：

[0070] 0100 1011 1101 1010 0111 0010 0100 0100 1011 0011 0001 0010 0000 0111 0100 0011

[0071] 0110 1111 0110 0101 1000 0011 1000 1100 1111 0101 0011 1111 1111 0001 0000 1000

[0072] 1101 1010 0111 0010 0100 0100 1011 0011 0001 0010 0000 0111 0100 0011 0110 1111

[0073] 0110 0101 1000 0011 1000 1100 1111 0101 0011 1111 1111 0001 0000 1000 1100 1010

[0074] 0111 0010 0100 0100 1011 0011 0001 0010 0000 0111 0100 0011 0110 1111 0110 0101

[0075] 1000 0011 1000 1100 1111 0101 0011 1111 1111 0001 0000 1000 1100 1010 0001 1110

[0076] 因此，来自位偏移量“0”的第一128位密钥是：

[0077] 0100 1011 1101 1010 0111 0010 0100 0100 1011 0011 0001 0010 0000 0111 0100 0011

[0078] 0110 1111 0110 0101 1000 0011 1000 1100 1111 0101 0011 1111 1111 0001 0000 1000

[0079] 并且来自位偏移量“1”的第二128位密钥是：

[0080] 1001 0111 1011 0100 1110 0100 1000 1001 0110 0110 0010 0100 0000 1110 1000 0110

[0081] 1101 1110 1100 1011 0000 0111 0001 1001 1110 1010 0111 1111 1110 0010 0001 0001

[0082] 并且来自位偏移量“2”的第三128位密钥是：

[0083] 0010 1111 0110 1001 1100 1001 0001 0010 1100 1100 0100 1000 0001 1101 0000 1101

[0084] 1011 1101 1001 0110 0000 1110 0011 0011 1101 0100 1111 1111 1100 0100 0010 0011

[0085] 换句话说,与原始密钥相比,这种技术能够使用相同数量的密钥材料生成128倍密钥。

[0086] 将了解,代替使用前述密钥偏移量、前述字节偏移量或前述位偏移量,还可以使用其它类型的偏移量,诸如字偏移量,取决于是增大处理速度还是生成更大量密钥更重要。

[0087] 选项D:

[0088] 根据实施例,在给定用户装置的装置存储器中扩展65535个密钥,例如如下:

[0089] (a)将128位密钥扩展为(例如)352位密钥;

[0090] (b)将192位密钥扩展为(例如)432位密钥;以及

[0091] (c)将256位密钥扩展为(例如)512位密钥。

[0092] 接着可以相对于密钥库集成服务使用这些密钥,例如,使用诸如AES、Salsa20和ChaCha20等算法,但不限于此。

[0093] 密钥材料可以用于各种目的,诸如密码学、数据保护(例如,加密和解密)、签名、完整性、验证、认证、授权等。有利的是,使得密钥材料能够在受保护密钥库内部被密钥库集成服务访问以供使用,所述密钥库集成服务仅经由密钥引用来访问密钥材料以供使用。换句话说,软件应用程序或生态系统进程不能从密钥库外部访问密钥材料。

[0094] 如果恶意方试图使用密钥引用来访问、评估或调试其对应密钥材料,则任选地引起异常。作为示例,如果密钥库是在Android™上实施的并且技术接口是使用Java构建的,其中在SunMicrosystem®的Java与GoogleAndroid™的Java之间混合安全解决方案的技术实施,则密钥库应当支持Google Android™开发者参考文献中所定义的完全所需接口,使得可以使用已经存在的Java应用编程接口(API)来进行技术实施。然而,密钥库的技术实施不允许访问、评估或调试给定密钥引用所引用的密钥材料。

[0095] 在本公开的实施例中,密钥库内容由密钥服务提供商以前述格式创建,即以与给定用户装置兼容的格式创建,以便符合给定用户装置的密钥库的导入功能。这显著加快了给定用户装置处的步骤(ii)的导入过程。任选地,密钥库内容由密钥服务提供商以符合广泛用户装置的密钥库导入功能的格式创建;例如,用户装置采用以硬件实施的各种类型的专有安全密钥库,诸如前述TEE,并且采用软件支持的接口来向由密钥服务提供商发送的所接收的加密密钥库内容文件提供由安全密钥库呈现的标准化功能性的入口。任选地,在这点上,在密钥服务提供商处,密钥库内容被单独定制以与各种不同类型的用户装置兼容。

[0096] 此类用户装置的示例包括但不限于移动电话、智能电话、移动互联网装置(MID)、平板计算机、超移动个人计算机(UMPC)、平板手机计算机、个人数字助理(PDA)、连网板、个人计算机(PC)、手持式PC、膝上型计算机、台式计算机和交互式娱乐装置,诸如游戏机、电视(TV)机和机顶盒(STB)。

[0097] 此外,将了解,给定用户装置的密钥库可以是基于硬件的或基于软件的,例如如在TEE(“可信执行环境”)中使用硬件来实施,其防止在将密钥库内容初始导入并加载到给定用户装置的受保护密钥库之后从其导出数据。

[0098] 根据本公开的实施方式，密钥库是基于硬件的。任选地，在此类情况下，步骤(ii)处的导入包括将存储在基于硬件的密钥库处的密钥材料绑定到给定用户装置的处理硬件的安全区域。随后，在使用中，存储在密钥库中的密钥材料经由使用其引用来访问以供使用，但是不能从密钥库导出。任选地，指针用于传送密钥材料的密钥引用以由密钥库集成服务使用。

[0099] 一个或多个可信软件应用程序(例如，需要使用密钥库中的密钥材料的加密算法和/或解密算法)在操作中受到给定用户装置的内核层的保护。例如，给定用户装置的内核层以硬件与软件的混合来实施，并且通常是给定用户装置专有的，例如是给定用户装置的制造商专有的。可信软件应用程序介接到给定用户装置上的、在操作中支持的其它软件层中所支持的其它软件应用程序。有利的是，一个或多个可信软件应用程序以加密形式从可信软件服务提供商下载。任选地，密钥服务提供商和可信软件服务提供商是同一方。替代地，任选地，密钥服务提供商和可信软件服务提供商是相互不同的两方。

[0100] 因此，将了解，在包括硬件实施的密钥库的给定用户装置中，还存在托管于所述装置中的内核层和一个或多个软件层。可以导入软件应用程序并且接着在一个或多个软件层中执行。此外，由可信软件服务提供商提供的其它可信软件应用程序可以在内核层中执行，在该情况下可信软件应用程序受到内核层的安全防范的保护，所述安全防范通常比一个或多个软件层更安全；出于本公开的目的，受内核层的安全防范保护的软件应用程序被称为“密钥库集成服务”。在操作中，在一个或多个软件层中所支持的应用程序与内核层中所托管的“密钥库集成服务”之间发生各种数据交换。

[0101] 任选地，处理硬件的安全区域借助于专用硬件来实施，所述专用硬件被配置为不允许外部加载的软件应用程序或程序(即，在上述一个或多个软件层中)在专用硬件上进行操作。将了解，此类外部加载的软件应用程序或程序可能由敌对第三方恶意加载。更任选地，处理硬件的安全区域借助于可信执行环境(TEE；参见参考文献[1])来实施，例如如上所述。

[0102] 以这种方式，方法促进给定用户装置的软件与安全硬件之间的坚实且牢固的集成。

[0103] 根据本公开的实施例，“密钥材料”包括以下至少一者：

[0104] (a)用于对称数据加密的秘密密钥，

[0105] (b)用于公钥基础设施(PKI)等效用法的私有密钥和公开密钥，

[0106] (c)待用于密码学、签名、完整性、验证、认证、授权等的证书，

[0107] (d)用于生成密钥的一个或多个密钥生成器。

[0108] 任选地，在这点上，一个或多个密钥生成器用于可再现地生成密钥。换句话说，在每次使用相同输入时，给定密钥生成器都生成相同密钥。

[0109] 任选地，使用额外加密来单独保护一个或多个密钥材料。这对于某些安全应用特别有利。

[0110] 将了解，即使PKI本身使用不对称加密，密钥材料仍然可以使用对称加密来导入。

[0111] 此外，任选地，密钥材料包括一次性密钥，所述一次性密钥将仅使用一次并且将在使用之后丢弃。例如，此类一次性密钥可以用于登录到给定服务。额外地或替代地，任选地，至少一些密钥是可重复使用的加密密钥。

[0112] 此外,任选地,密钥库能够充当密钥生成器,并且能够可再现地生成新密钥。

[0113] 此外,根据本公开的实施方式,方法包括将被授权以使用给定用户装置的密钥库的托管在给定用户装置处的一个或多个可信软件应用程序或生态系统进程与密钥库集成。如上所述,贯穿本公开,此类集成软件应用程序或生态系统进程被称为“密钥库集成服务”。密钥库集成服务的示例包括但不限于数据传递服务、内容传递服务、银行服务和金融交易服务;此类服务通常涉及使用一个或多个密钥对数据进行加密和/或解密。

[0114] 任选地,在这点上,方法包括从可信软件服务提供商导入用于提供密钥库集成服务的一个或多个可信软件应用程序,其中当在给定用户装置处执行时,所述一个或多个可信软件应用程序可操作以提供一个或多个密钥库集成服务,并且被提供来自给定用户装置的内核的保护。

[0115] 此外,任选地,当密钥库是基于硬件时,使用符合基于硬件的密钥库的对称加密来对密钥材料进行加密。任选地,在这点上,方法包括在密钥服务提供商处通过采用对称高级加密标准(AES;参见参考文献[2])加密来对密钥材料进行加密,例如,使用128位密钥或256位密钥。

[0116] 替代地,任选地,当密钥库是基于软件时,使用符合基于软件的密钥库的不对称加密来对密钥库内容进行加密。

[0117] 此处将了解,为了使给定用户装置能够对加密密钥库内容进行解密,给定用户装置必须知道在加密期间所使用的加密凭证。将了解,在本公开的实施例中,使用哪种加密算法或哪种加密凭证来对密钥库内容进行加密是不相关的,因为不同装置供应商和生态系统提供商可以实施多个不同安全解决方案,所述安全解决方案接着可以由多个不同安全服务提供商在具有其自己的基于硬件或基于软件的密钥库的不同平台上实施。

[0118] 此外,如先前提到,用于对密钥材料进行加密的加密凭证与给定用户装置兼容。此类兼容的加密凭证可以由给定用户装置或密钥服务提供商提供。任选地,在这点上,方法包括在密钥服务提供商处使用由给定用户装置或密钥服务提供商提供的加密密钥数据来对密钥库内容进行加密。

[0119] 根据本公开的实施方式,方法包括在给定用户装置处使用最终用户的生物凭证的令牌(token)来保护密钥库。任选地,在这点上,最终用户的生物凭证包括以下中的至少一者:最终用户的指纹、最终用户的面部特征、最终用户的DNA图谱、最终用户的虹膜辨识、最终用户的行走方式、最终用户的书写方式、最终用户的心跳模式。将了解,用于保护密钥库的最终用户的生物凭证是借助于最终用户装置的基于硬件的功能性来提供的。这些基于硬件的功能性例如可以借助于TEE来实施。作为示例,可以使用最终用户装置的相机捕获最终用户的面部特征,并且使用图像相关性或使用神经网络算法对照参考模板进行验证。将了解,最终用户的生物凭证可以替代地对应于将来可行的任何其它类型的生物统计验证。

[0120] 根据本公开的另一实施方式,方法包括在给定用户装置处使用与最终用户相关联的个人识别码(PIN)来保护密钥库。将了解,PIN是借助于最终用户装置的基于硬件的功能性来提供的。

[0121] 根据本公开的又一实施方式,方法包括在给定用户装置处使用应用特定标识(ID)来保护密钥库。任选地,应用特定ID是借助于最终用户装置的基于硬件的功能性来提供的。替代地,任选地,应用特定ID是借助于基于平台的功能性来提供的。任选地,在此类情况下,

应用特定ID是示例标识符(即,示例ID)。

[0122] 此外,根据本公开的一个实施方式,在步骤(i)处经由不安全的传输来接收密钥库内容。作为示例,可以经由不安全的公共因特网连接来传送加密密钥库内容,因为当受到适当保护时,经加密的密钥库内容不会泄露任何用户敏感数据。这是可能的,因为使用加密来保护密钥材料,并且因此,不必保护密钥材料的传输。

[0123] 在第二方面,本公开的实施方式提供一种计算机程序产品,其包括其上存储有计算机可读指令的非暂态计算机可读存储介质,该计算机可读指令能够由包括处理硬件的计算机化装置执行以执行根据前述第一方面的方法。

[0124] 任选地,计算机可读指令能够从软件应用程序商店(例如,从“应用商店”)下载到计算机化装置。

[0125] 在第三方面,本公开的实施方式提供一种用于保护最终用户的给定用户装置处的密钥库内容的使用的系统,其特征在于,该系统可操作以:

[0126] (i)在给定用户装置处接收密钥库内容,所述密钥库内容包括使用与给定用户装置兼容的加密凭证进行加密的密钥材料,密钥库内容由密钥服务提供商以与给定用户装置兼容的格式创建并从其接收;

[0127] (ii)将密钥库内容的加密密钥材料导入到给定用户装置的受保护密钥库并且将密钥材料以加密形式存储在受保护密钥库处,其中密钥库内容的所有密钥材料被一次性导入,并且其中密钥库内容以密钥材料不能从密钥库导出的方式存储在密钥库处;以及

[0128] (iii)在给定用户装置的受保护密钥库内部,允许给定用户装置的一个或多个密钥库集成服务仅经由密钥引用来访问不可导出的密钥材料以供使用。

[0129] 任选地,除了密钥材料之外,受保护密钥库还包括关于被授权以使用存储在受保护密钥库处的密钥材料的最终用户和/或最终用户群组的信息。额外地或替代地,任选地,受保护密钥库包括与密钥材料的使用相关的其它信息。

[0130] 任选地,在(i)处以对称加密形式接收密钥材料。

[0131] 任选地,该系统可操作以在给定用户装置的受保护密钥库内部,对待由给定用户装置的一个或多个密钥库集成服务使用的一个或多个密钥材料进行解密。

[0132] 根据一个实施方式,借助于密钥材料的索引来实施密钥引用。任选地,所述系统可操作为在密钥库内容内接收待用于经由密钥引用来引用密钥材料的索引。替代地,任选地,所述系统可操作为在给定用户装置处,生成待用于经由密钥引用来引用密钥材料的索引。作为示例,可以以与在密钥库内容中包括密钥材料的次序对应的连续方式生成索引。例如,可以在给定用户装置向密钥服务提供商进行初始注册时或者在对密钥材料进行解密期间生成索引。

[0133] 根据另一个实施方式,借助于偏移量来实施密钥引用,将基于偏移量来识别密钥材料。

[0134] 任选地,当在(ii)处导入时,系统可操作为作为单个数据文件将密钥库内容导入到给定用户装置。

[0135] 此处将了解,本公开的实施例适合于各种不同类型的用户装置。此类用户装置的示例包括但不限于移动电话、智能电话、MID、平板计算机、UMPC、平板手机计算机、PDA、连网板、PC、手持式PC、膝上型计算机、台式计算机和交互式娱乐装置,诸如游戏机、电视机和

STB。

[0136] 根据本公开的一个实施方式，密钥库是基于硬件的。任选地，在此类情况下，当在(ii)处导入时，系统可操作为将存储在基于硬件的密钥库处的密钥材料绑定到给定用户装置的处理硬件的安全区域。

[0137] 任选地，借助于专用硬件来实施处理硬件的安全区域，所述专用硬件被配置为不允许外部加载的软件应用程序或程序在专用硬件上进行操作；例如，外部加载的软件应用程序可操作为经由受最终用户装置的内核层保护的、由可信软件应用程序提供的密钥库集成服务来介接，其中密钥库集成服务使密钥库免受外部加载的软件应用程序直接访问。将了解，此类外部加载的软件应用程序或程序可能由敌对第三方恶意加载。然而，将了解，如上所述，密钥库集成服务是使用从可信软件服务提供商提供的可信软件应用程序来实施的。更任选地，借助于TEE(参见参考文献[1])来实施处理硬件的安全区域。

[0138] 根据本公开的一个实施方式，“密钥材料”包括以下中的至少一者：

[0139] (a)用于对称数据加密的秘密密钥，

[0140] (b)用于PKI等效使用的私有密钥和公开密钥，

[0141] (c)待用于密码学、签名、完整性、验证、认证、授权等的证书，

[0142] (d)用于生成密钥的一个或多个密钥生成器。

[0143] 此外，根据本公开的一个实施方式，所述系统可操作为将被授权以使用给定用户装置的密钥库的、在给定用户装置处被托管的一个或多个可信软件应用程序或生态系统进程与密钥库集成。此类密钥库集成服务的示例包括但不限于数据传递服务、内容传递服务、银行服务和金融交易服务。

[0144] 任选地，在这点上，所述系统可操作为从可信软件服务提供商导入用于提供密钥库集成服务的一个或多个可信软件应用程序，其中当在给定用户装置处执行时，所述一个或多个可信软件应用程序能够操作为提供一个或多个密钥库集成服务并且被提供来自给定用户装置的内核的保护。

[0145] 此外，根据本公开的一个实施方式，密钥服务提供商能够操作为使用由给定用户装置或密钥服务提供商提供的加密密钥数据，来对密钥库内容进行加密。

[0146] 根据本公开的一个实施方式，在给定用户装置处使用最终用户的生物凭证的令牌来保护密钥库。任选地，在这点上，最终用户的生物凭证包括以下中的至少一者：最终用户的指纹、最终用户的面部特征、最终用户的DNA图谱、最终用户的虹膜辨识、最终用户的行走方式、最终用户的书写方式、最终用户的心跳模式。将了解，最终用户的生物凭证可以替代地对应于将来可行的任何其它类型的生物统计验证。

[0147] 根据本公开的另一实施方式，在给定用户装置处使用与最终用户相关联的PIN来保护密钥库。

[0148] 根据本公开的又一实施方式，在给定用户装置处使用应用特定ID来保护密钥库。

[0149] 任选地，密钥服务提供商能够操作为通过采用对称AES加密(参见参考文献[2])来对密钥材料进行加密，例如，使用128位密钥或256位密钥。

[0150] 此外，根据本公开的一个实施方式，当在(i)处接收时，所述系统能够操作为经由不安全的传输来接收密钥库内容。

[0151] 接下来，将参考附图描述本公开的实施方式。

[0152] 参考图1A,提供了根据本公开的一个实施方式的用于保护密钥库内容102的使用的系统100的示意图。系统100包括密钥服务提供商104和最终用户的给定用户装置106,其中密钥服务提供商104和给定用户装置106经由数据通信布置通信地耦合。

[0153] 密钥服务提供商104以与给定用户装置106兼容的格式创建密钥库内容102,对密钥库内容102中所包括的密钥材料进行加密,并且将密钥库内容102发送到给定用户装置106。任选地,密钥库内容102能够作为单个数据文件导入到给定用户装置106的受保护密钥库108。

[0154] 在给定用户装置106处,密钥库内容102(即,所有密钥材料)一次性导入到给定用户装置106的受保护密钥库108,其中密钥材料以加密形式存储并以密钥材料不能从受保护密钥库108导出的方式来存储,并且能够由密钥库集成服务仅经由密钥引用来访问以供使用。

[0155] 如前所述,可以借助于索引或偏移量来实施密钥引用。任选地,在密钥库内容102中接收索引;替代地,任选地,在给定用户装置106处生成索引,例如以与密钥库内容102中包括密钥材料的次序对应的连续方式生成索引。

[0156] 可信软件服务提供商120提供以加密形式导入到给定用户装置106的受保护密钥库108的一个或多个可信软件应用程序122,其中一个或多个可信软件应用程序122能够在给定用户装置106上以受给定用户装置106的内核124(例如,内核层)保护的方式执行。一个或多个可信软件应用程序122能够操作为使用密钥引用来访问密钥库108的密钥材料以用于各种目的,例如加密、解密、验证、认证,但是被防止将密钥材料泄露给给定用户装置106的一个或多个软件层中所支持的其它软件应用程序。由于以加密形式存储密钥材料,因此在使用之前需要对密钥材料进行解密。任选地,当将密钥材料加载到密钥库108时,在密钥库108内安全地对经加密的密钥材料进行解密。

[0157] 任选地,可信软件服务提供商120是与密钥服务提供商104相同的一方。替代地,任选地,可信软件服务提供商120是与密钥服务提供商104相互不同的一方。

[0158] 在图1B中,提供了根据本公开的一个实施方式的保护给定用户装置106处的密钥库内容102的使用的完整端到端过程流程的示意图。

[0159] 步骤1:密钥服务提供商104以与给定用户装置106兼容的格式创建密钥库内容102。

[0160] 步骤2:密钥服务提供商104对密钥库内容102中所包括的密钥材料进行加密。

[0161] 步骤3:给定用户装置106从密钥服务提供商104接收密钥库内容102。

[0162] 步骤4:将经加密的密钥材料导入到给定用户装置106的受保护密钥库108。任选地,使用来自最终用户的加密凭证来保护密钥库108。

[0163] 步骤5:将密钥材料加载到密钥库,其中在密钥库中安全地对密钥材料进行解密,以便能够容易并且快速地使用。

[0164] 步骤6:密钥库集成服务122在受保护密钥库内部仅经由密钥引用来访问密钥材料。

[0165] 禁止步骤7:密钥材料是不可导出的,并且无法从密钥库108导出。

[0166] 此外,在图1C中,提供了根据本公开的一个实施方式的如何将密钥库内容102导入并加载到受保护密钥库108的示意图。

[0167] 在从密钥服务提供商104接收到密钥库内容102后，即刻将其中所包括的、经加密的密钥材料一次性导入到用户装置106的受保护密钥库108。

[0168] 值得注意的是，密钥材料可以被提供为单个密钥代码列表或作为多个不同密钥代码列表。将了解，可以同时导入不同密钥代码列表。不管不同密钥代码列表(即，密钥材料)以哪种形式加密，都会一次性导入所有密钥材料。

[0169] 当在密钥库108处加载密钥材料时，接着在密钥库108内安全地对经加密的密钥材料进行解密。

[0170] 图1A、图1B和图1C仅仅是示例，其不应过度限制本文的权利要求书的范围。应当理解，系统100的特定命名是作为示例来提供的，并且不应被解释为将系统100限制于服务提供商和用户装置的特定数目、类型或布置；具体地说，仅仅为了简单起见，示出了单个用户装置。本领域的技术人员将认识到本公开的实施方式的许多变化、替代和修改。

[0171] 将了解，即使图1B和图1C示出了密钥材料的索引，密钥引用也不一定总是借助于此类索引来实施。值得注意的是，在替代实施方式中，密钥引用可以使用偏移量来实施，如前所述。

[0172] 接下来参考图2，提供了描绘根据本公开的实施方式的保护最终用户的给定用户装置处的密钥库内容的使用的方法的步骤的流程图。所述方法被描绘为逻辑流程图中的步骤集合，所述逻辑流程图表示能够以硬件、软件或其组合实施的步骤序列，例如如上所述。

[0173] 在步骤202处，在给定用户装置处接收密钥库内容。根据步骤202，密钥库内容包括使用与给定用户装置兼容的加密凭证进行加密的密钥材料。密钥库内容由密钥服务提供商以与给定用户装置兼容的格式创建并从其接收。

[0174] 在步骤204处，将密钥库内容的经加密的密钥材料一次性导入到给定用户装置的受保护密钥库，并且将密钥材料以加密形式存储在受保护密钥库处。根据步骤204，将密钥库内容以密钥材料不能从密钥库导出的方式存储在受保护密钥库处。

[0175] 在步骤206处，在给定用户装置的受保护密钥库内部，允许给定用户装置的一个或多个密钥库集成服务仅经由密钥引用来访问不可导出的密钥材料以供使用。如上所述，此类集成服务由在给定用户装置的内核层(例如，内核结构)的保护下运行的可执行软件提供。任选地，内核结构包括硬件，用于实现增强的安全度。

[0176] 步骤202至206仅是说明性的，并且还可以提供其它替代方案，其中在不脱离本文权利要求书的范围的情况下添加一个或多个步骤。

[0177] 在不脱离由所附权利要求书限定的本公开的范围的情况下可以对前文中所描述的本公开的实施方式做出修改。诸如“包括”、“包含”、“并入”、“由……组成”、“具有”、“是”等用于描述和要求保护本发明的表达旨在以非排他性方式解释，即允许没有明确描述的项目、部件或元件也存在。对单数的引用还应被理解为与复数相关；作为一个示例，“至少一个”在一个示例中指示“一个”，并且在另一个示例中指示“多个”；此外，“两个”和类似的“一个或多个”将以类似方式解释。所附权利要求书中的包括在括号内的数字旨在帮助理解权利要求，而不应以任何方式解释为限制这些权利要求所要求保护的主题。

[0178] 短语“在一个实施方式中”、“根据一个实施方式”等通常意味着跟随所述短语之后的特定特征、结构或特性包括在本公开的至少一个实施方式中，并且可以包括在本公开的一个以上实施方式中。重要的是，此类短语不一定指的是同一实施方式。

[0179] 参考文献

[0180] [1]Trusted execution environment-维基百科,免费的百科全书(2016年11月28日访问);URL:https://en.wikipedia.org/wiki/Trusted_execution_environment

[0181] [2]Advanced Encryption Standard-维基百科,免费的百科全书(2016年11月28日访问);URL:https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

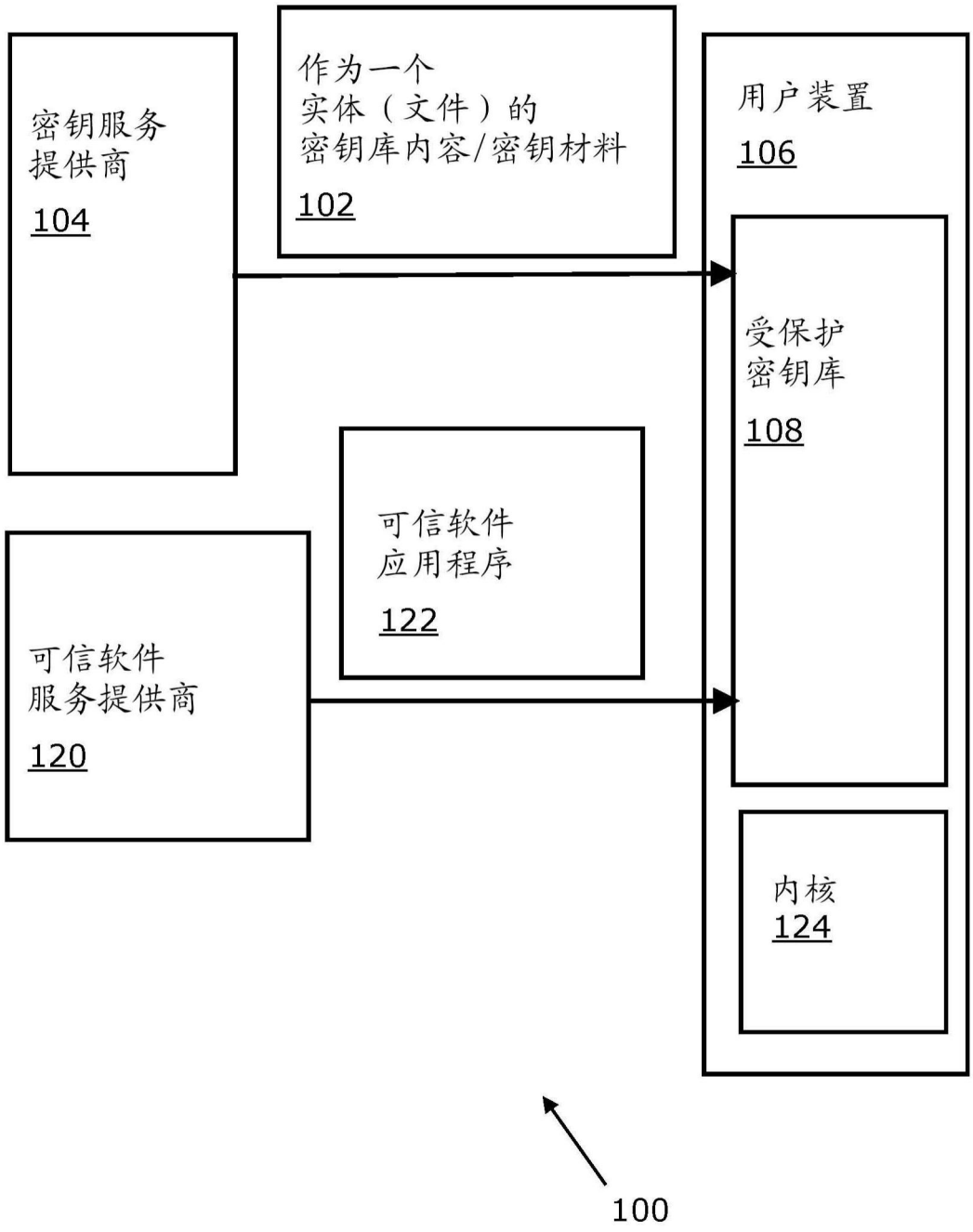

密钥服务
提供商
104
作为一个
实体（文件）的
密钥库内容/密钥材料
102
用户装置
106
受保护
密钥库
108
可信软件
应用程序
122
可信软件
服务提供商
120
内核
124
100

图1A

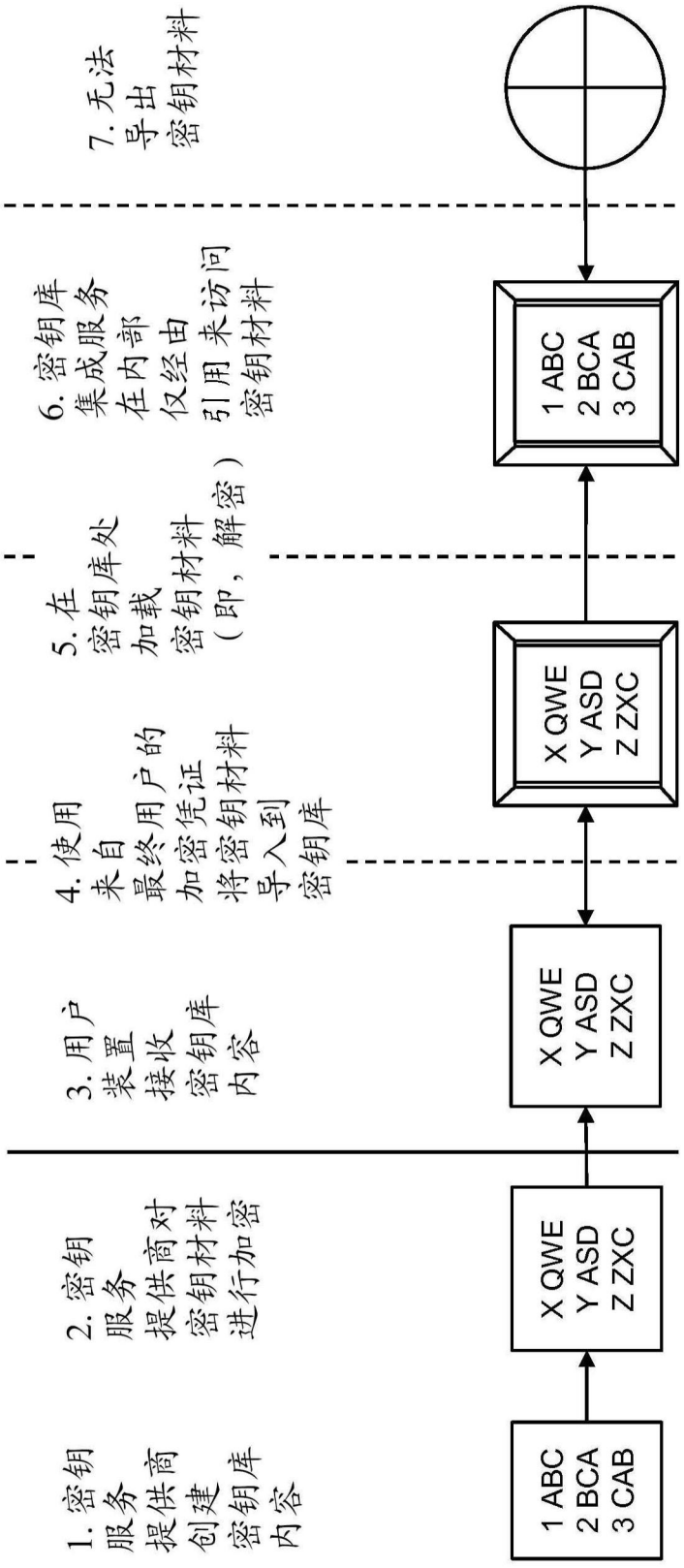

1. 密钥
服务
提供商
创建
密钥库
内容
2. 密钥
服务
提供商对
密钥材料
进行加密
3. 用户
装置
接收
密钥库
内容
4. 使用
来自
最终用户的
加密凭证
将密钥材料
导入到
密钥库
5. 在
密钥库处
加载
密钥材料
（即，解密）
6. 密钥库
集成服务
在内部
仅经由
引用来访问
密钥材料
7. 无法
导出
密钥材料
1 ABC
2 BCA
3 CAB
X QWE
Y ASD
Z ZXC
X QWE
Y ASD
Z ZXC
1 ABC
2 BCA
3 CAB

图1B

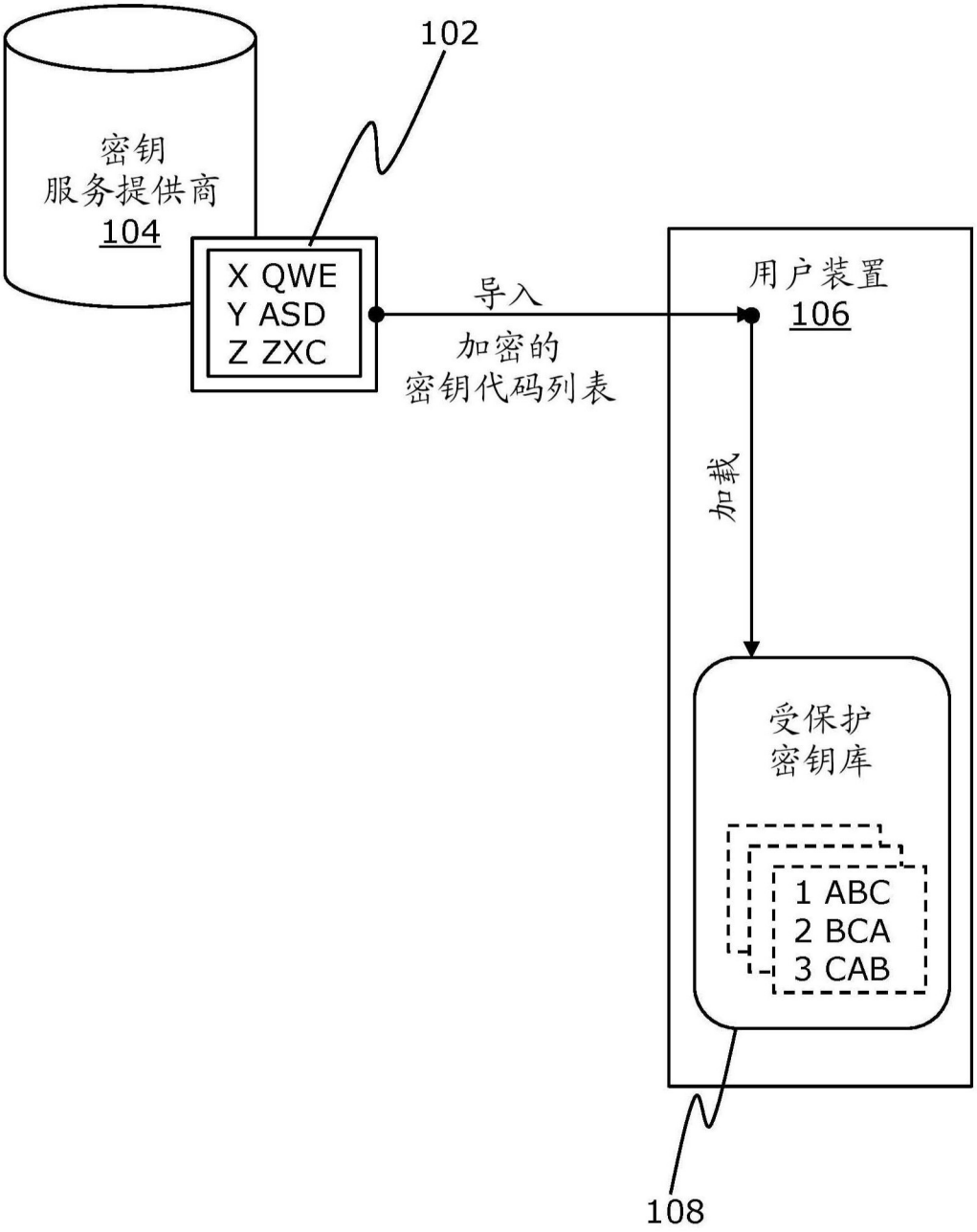

102
密钥
服务提供商
104
X QWE
Y ASD
Z ZXC
导入
加密的
密钥代码列表
用户装置
106
加载
受保护
密钥库
1 ABC
2 BCA
3 CAB
108

图1C

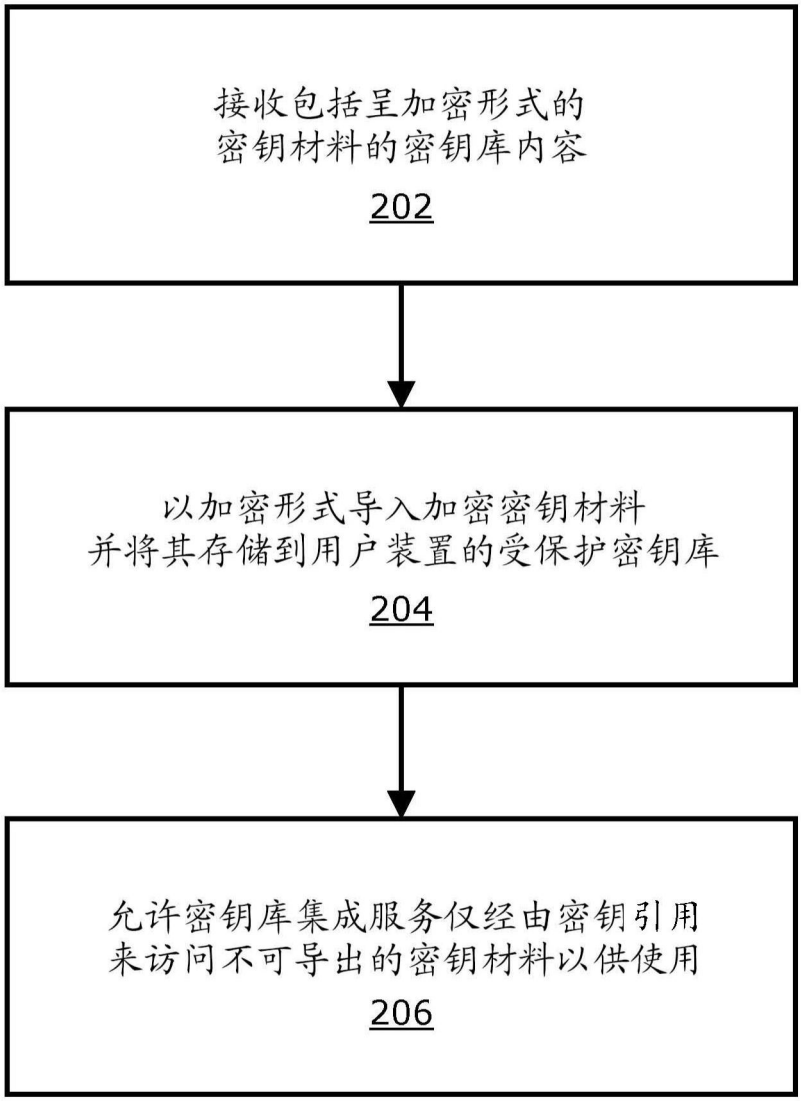

接收包括呈加密形式的
密钥材料的密钥库内容
202
以加密形式导入加密密钥材料
并将其存储到用户装置的受保护密钥库
204
允许密钥库集成服务仅经由密钥引用
来访问不可导出的密钥材料以供使用
206

图2