(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 107682586 B
(45)授权公告日 2019.12.06

(21)申请号 201710651269.X

(22)申请日 2017.08.02

(65)同一申请的已公布的文献号
申请公布号 CN 107682586 A

(43)申请公布日 2018.02.09

(30)优先权数据
2016-152288 2016.08.02 JP

(73)专利权人 佳能株式会社
地址 日本东京都大田区下丸子3丁目30番2号

(72)发明人 角谷直哉

(74)专利代理机构 北京魏启学律师事务所 11398
代理人 魏启学

(51)Int.Cl.
H04N 1/44(2006.01)
H04N 1/00(2006.01)

(56)对比文件
CN 104657686 A,2015.05.27,
CN 102769525 A,2012.11.07,
CN 102355351 A,2012.02.15,
CN 103748827 A,2014.04.23,
US 2015358161 A1,2015.12.10,
CN 1702999 A,2005.11.30,

审查员 徐燕丽

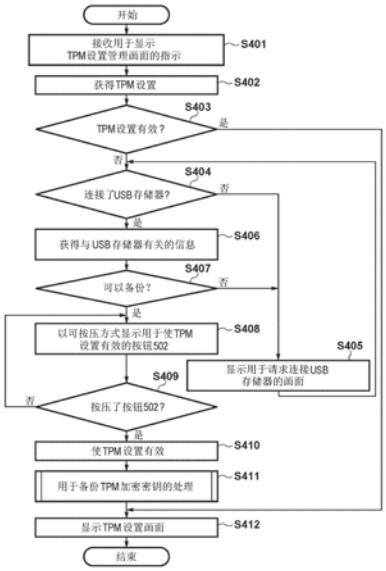
权利要求书2页 说明书12页 附图14页

(54)发明名称

信息处理设备及其控制方法和存储介质

(57)摘要

本发明涉及一种信息处理设备及其控制方法和存储介质。在具有硬件安全模块即HSM的信息处理设备中,在能够备份HSM的加密密钥的条件下,使得可以使用HSM的加密密钥来对数据进行加密和解密的HSM功能能够被设置成有效。



CN 107682586 B

1.一种信息处理设备,其具有硬件安全模块即HSM,所述信息处理设备包括:

判断单元,用于判断是否能够备份所述HSM的加密密钥;

控制单元,用于在所述判断单元判断为能够备份所述HSM的加密密钥的条件下,进行控制以使得能够接收用以使HSM功能有效的指示,其中所述HSM功能用于使用所述加密密钥进行数据的加密和解密;

设置单元,用于在接收到用以使所述HSM功能有效的指示的情况下,将所述HSM功能设置成有效;以及

备份单元,用于备份所述HSM的加密密钥。

2.根据权利要求1所述的信息处理设备,其中,

在所述设置单元将所述HSM功能设置成有效的情况下,所述备份单元备份所述HSM的加密密钥。

3.根据权利要求1所述的信息处理设备,其中,

所述判断单元基于是否连接了用于存储所述HSM的加密密钥的外部存储器、或者所述外部存储器是否具有能够存储所述HSM的加密密钥的空闲存储区域,来判断是否能够备份所述HSM的加密密钥。

4.根据权利要求1所述的信息处理设备,其中,还包括显示单元,所述显示单元用于显示用以给出使所述HSM功能有效的指示的指示部,

其中,在能够接收到用以使所述HSM功能有效的指示的情况下,所述显示单元将所述指示部显示成能够操作,并且在无法接收到用以使所述HSM功能有效的指示的情况下,所述显示单元将所述指示部显示成不能操作。

5.根据权利要求1所述的信息处理设备,其中,所述备份单元根据来自具有管理权限的用户的指示来备份所述HSM的加密密钥。

6.一种信息处理设备,其具有硬件安全模块即HSM,所述信息处理设备包括:

第一判断单元,用于判断是否能够备份所述HSM的加密密钥;

控制单元,用于在所述第一判断单元判断为能够备份所述HSM的加密密钥的条件下,进行控制以使得能够接收用以使HSM功能有效的指示,其中所述HSM功能用于使用所述加密密钥进行数据的加密和解密;

第二判断单元,用于判断所述HSM功能是否有效;

第三判断单元,用于判断是否备份了所述HSM的加密密钥;以及

备份单元,用于在所述第二判断单元判断为所述HSM功能有效、并且所述第三判断单元判断为没有备份所述HSM的加密密钥的情况下,备份所述HSM的加密密钥。

7.根据权利要求6所述的信息处理设备,其中,

所述备份单元显示用于提示用户备份所述HSM的加密密钥的画面。

8.根据权利要求6所述的信息处理设备,其中,所述第二判断单元判断在用户登录时所述HSM功能是否有效。

9.根据权利要求6所述的信息处理设备,其中,在所述第二判断单元判断为所述HSM功能无效、并且所述第三判断单元判断为没有备份所述HSM的加密密钥的情况下,所述备份单元显示用于接收用以备份所述HSM的加密密钥的指示的画面。

10.根据权利要求6所述的信息处理设备,其中,在所述第二判断单元判断为所述HSM功

能无效、并且所述第三判断单元判断为备份了所述HSM的加密密钥的情况下，所述备份单元显示用于接收用以使所述HSM功能有效的指示的画面。

11.一种信息处理设备的控制方法，所述信息处理设备具有硬件安全模块即HSM，所述控制方法包括以下步骤：

判断是否能够备份所述HSM的加密密钥；

在判断为能够备份所述HSM的加密密钥的条件下，进行控制以使得能够接收用以使HSM功能有效的指示，其中所述HSM功能用于使用所述加密密钥进行数据的加密和解密；

在接收到用以使所述HSM功能有效的指示的情况下，将所述HSM功能设置成有效；以及

备份所述HSM的加密密钥。

12.一种计算机可读存储介质，其存储用于使处理器执行信息处理设备的控制方法的程序，所述信息处理设备具有硬件安全模块即HSM，所述控制方法包括以下步骤：

判断是否能够备份所述HSM的加密密钥；

在判断为能够备份所述HSM的加密密钥的条件下，进行控制以使得能够接收用以使HSM功能有效的指示，其中所述HSM功能用于使用所述加密密钥进行数据的加密和解密；

在接收到用以使所述HSM功能有效的指示的情况下，将所述HSM功能设置成有效；以及

备份所述HSM的加密密钥。

13.一种信息处理设备的控制方法，所述信息处理设备具有硬件安全模块即HSM，所述控制方法包括：

判断是否能够备份所述HSM的加密密钥；

在判断为能够备份所述HSM的加密密钥的条件下，进行控制以使得能够接收用以使HSM功能有效的指示，其中所述HSM功能用于使用所述加密密钥进行数据的加密和解密；

判断所述HSM功能是否有效；

判断是否备份了所述HSM的加密密钥；以及

在判断为所述HSM功能有效、并且判断为没有备份所述HSM的加密密钥的情况下，备份所述HSM的加密密钥。

14.一种计算机可读存储介质，其存储用于使处理器执行信息处理设备的控制方法的程序，所述信息处理设备具有硬件安全模块即HSM，所述控制方法包括以下步骤：

判断是否能够备份所述HSM的加密密钥；

在判断为能够备份所述HSM的加密密钥的条件下，进行控制以使得能够接收用以使HSM功能有效的指示，其中所述HSM功能用于使用所述加密密钥进行数据的加密和解密；

判断所述HSM功能是否有效；

判断是否备份了所述HSM的加密密钥；以及

在判断为所述HSM功能有效、并且判断为没有备份所述HSM的加密密钥的情况下，备份所述HSM的加密密钥。

信息处理设备及其控制方法和存储介质

技术领域

[0001] 本发明涉及一种信息处理设备及其控制方法和存储介质。

背景技术

[0002] 通常,在诸如PC(个人计算机)和具有打印功能的MFP(多功能外围设备/数字多功能外围设备)等的信息处理设备中,以加密方式存储机密数据。

[0003] 近年来,一些信息处理设备在对这些信息处理设备中所包括的机密数据进行加密/解密的情况下,使用物理地连接至这些信息处理设备的外部的硬件安全模块(HSM,hardware security module)中所存储的加密密钥。例如,该HSM使用符合TCG(Trusted Computing Group,可信计算组织)标准的TPM(Trusted Platform Module,可信平台模块)。TPM是使得可以安全地管理加密密钥的具有防篡改性的安全芯片。

[0004] 通常,配备有TPM的装置通过对机密数据进行加密、并且在TPM内管理该加密所使用的密钥,来实现机密数据的安全管理。以下将使用信息处理设备的TPM的这种加密/解密称为“TPM功能”。在采用该TPM功能的情况下,例如,如果TPM故障或丢失,则在一些情况下更换TPM。

[0005] 现在,例如,如果由于故障因而利用新的TPM替换TPM,则该新的TPM芯片内的TPM加密密钥不同于故障之前的旧TPM内的TPM加密密钥。因此,使用旧TPM内的TPM加密密钥所加密的信息处理设备中的机密数据不能被新的TPM解密并使用。因此,需要备份TPM所管理的加密密钥(以下称为TPM加密密钥)。在大多情况下,通过使诸如USB存储器等的外部存储器连接至该设备、并且将TPM加密密钥存储至所连接的外部存储器,来进行TPM加密密钥的备份。例如,如果TPM发生故障,则利用新TPM替换该设备的TPM,使存储有原来的TPM加密密钥的外部存储器连接至该设备,并且使用该外部存储器中所存储的TPM加密密钥来将TPM加密密钥恢复到新TPM。

[0006] 在日本特开2015-122720中描述了与使用TPM功能的装置的TPM加密密钥的备份有关的技术。根据该技术,在使TPM功能有效之后生成TPM加密密钥,因而使用该装置的用户在使TPM功能有效之后,执行TPM加密密钥向诸如USB存储器等的外部存储器的备份。

[0007] 然而,存在用户在使装置的TPM功能有效之后忘记备份TPM加密密钥的情况。可以想到,这是因为例如在使TPM功能有效时没有准备备份所用的USB存储器、或者使TPM功能有效的用户与备份并管理TPM加密密钥的用户有所不同。还可想到,并不知晓存在备份功能的用户使TPM功能有效。如果这样在没有备份TPM加密密钥的情况下更换TPM,则存在如下问题:使用旧TPM的TPM加密密钥所加密的装置中的机密数据不能被解密并使用。

发明内容

[0008] 本发明的各方面是消除上述的传统技术的问题。

[0009] 本发明的特征是提供一种用于防止用户忘记备份HSM加密密钥的技术。

[0010] 根据本发明的第一方面,提供一种信息处理设备,其具有硬件安全模块即HSM,所

述信息处理设备包括:备份单元,用于备份所述HSM的加密密钥;设置单元,用于在接收到用以使HSM功能有效的指示的情况下,将所述HSM功能设置成有效,其中所述HSM功能使得能够使用所述HSM的加密密钥来进行数据的加密和解密;以及控制单元,用于在所述备份单元能够备份所述HSM的加密密钥的条件下,进行控制,以能够接收用以使所述HSM功能有效的指示。

[0011] 根据本发明的第二方面,提供一种信息处理设备,其具有硬件安全模块即HSM,所述信息处理设备包括:备份单元,用于备份所述HSM的加密密钥;第一判断单元,用于判断HSM功能是否有效,其中所述HSM功能使得能够使用所述HSM的加密密钥来进行数据的加密和解密;第二判断单元,用于判断是否备份了所述HSM的加密密钥;以及控制单元,用于在所述第一判断单元判断为所述HSM功能有效、并且所述第二判断单元判断为没有备份所述HSM的加密密钥的情况下,进行控制以备份所述HSM的加密密钥。

[0012] 根据本发明的第三方面,提供一种信息处理设备的控制方法,所述信息处理设备具有硬件安全模块即HSM,所述控制方法包括以下步骤:备份所述HSM的加密密钥;在接收到用以使HSM功能有效的指示的情况下,将所述HSM功能设置成有效,其中所述HSM功能使得能够使用所述HSM的加密密钥来进行数据的加密和解密;以及在能够备份所述HSM的加密密钥的条件下,进行控制,以能够接收用以使所述HSM功能有效的指示。

[0013] 根据本发明的第四方面,提供一种计算机可读存储介质,其存储用于使处理器执行信息处理设备的控制方法的程序,所述信息处理设备具有硬件安全模块即HSM,所述控制方法包括以下步骤:备份所述HSM的加密密钥;在接收到用以使HSM功能有效的指示的情况下,将所述HSM功能设置成有效,其中所述HSM功能使得能够使用所述HSM的加密密钥来进行数据的加密和解密;以及在能够备份所述HSM的加密密钥的条件下,进行控制,以能够接收用以使所述HSM功能有效的指示。

[0014] 根据本发明的第五方面,提供一种信息处理设备的控制方法,所述信息处理设备具有硬件安全模块即HSM,所述控制方法包括:备份所述HSM的加密密钥;判断HSM功能是否有效,其中所述HSM功能使得能够使用所述HSM的加密密钥来进行数据的加密和解密;判断是否备份了所述HSM的加密密钥;以及在判断为所述HSM功能有效、并且判断为没有备份所述HSM的加密密钥的情况下,进行控制以备份所述HSM的加密密钥。

[0015] 根据本发明的第六方面,提供一种计算机可读存储介质,其存储用于使处理器执行信息处理设备的控制方法的程序,所述信息处理设备具有硬件安全模块即HSM,所述控制方法包括以下步骤:备份所述HSM的加密密钥;判断HSM功能是否有效,其中所述HSM功能使得能够使用所述HSM的加密密钥来进行数据的加密和解密;判断是否备份了所述HSM的加密密钥;以及在判断为所述HSM功能有效、并且判断为没有备份所述HSM的加密密钥的情况下,进行控制以备份所述HSM的加密密钥。

[0016] 通过以下参考附图对典型实施例的说明,本发明的其它特征将变得明显。

附图说明

[0017] 包含在说明书中并构成说明书的一部分的附图示出了本发明的实施例,并且连同说明书一起用来解释本发明的原理。

[0018] 图1是用于说明根据本发明的第一实施例的多功能外围设备的示意硬件结构的框

图。

[0019] 图2是用于说明根据第一实施例的TPM和HDD所处理的加密密钥和机密数据的示意结构的框图。

[0020] 图3是用于说明根据第一实施例的用于启动多功能外围设备的处理的流程图。

[0021] 图4是用于说明根据第一实施例的用于使多功能外围设备中的TPM功能有效的处理的流程图。

[0022] 图5A～5C描述示出根据第一实施例的多功能外围设备的控制台单元上所显示的TPM设置管理画面的示例的图。

[0023] 图6是用于说明根据第一实施例的多功能外围设备所进行的、图4的步骤S411中的用于备份TPM加密密钥的处理的流程图。

[0024] 图7描述示出根据第一实施例的多功能外围设备的控制台单元上所显示的用于输入TPM加密密钥的备份所用的密码的画面的示例的图。

[0025] 图8是用于说明根据第二实施例的用于启动多功能外围设备的处理的流程图。

[0026] 图9描述示出根据第二实施例的多功能外围设备所提供的功能的主菜单画面的示例的图。

[0027] 图10是用于说明根据第二实施例的多功能外围设备所进行的用户认证处理的流程图。

[0028] 图11是用于说明根据本发明的第三实施例的多功能外围设备所进行的用于使HSM功能有效的处理和备份处理的流程图。

[0029] 图12A～12C描述示出根据第三实施例的多功能外围设备的控制台单元上所显示的HSM设置管理画面的示例的图。

具体实施方式

[0030] 以下参考附图来详细说明本发明的各实施例。应当理解，以下实施例并不意图限制本发明的权利要求书，并且并非根据以下实施例所述的各方面的所有组合对于用以解决根据本发明的问题的方式而言都是必需的。

[0031] 在这些实施例中，假定物理地连接至信息处理设备的外部的硬件安全模块(HSM)使用TPM(可信平台模块)。在本实施例中，将MFP(多功能外围设备/数字多功能外围设备)作为可以连接至/使用TPM并且具有用户认证功能的信息处理设备的示例来进行说明。然而，本发明不限于这种多功能外围设备，并且能够采用可以连接至/使用诸如TPM等的HSM并且具有用户认证功能的任何信息处理设备。

[0032] 第一实施例

[0033] 图1是用于说明根据本发明的第一实施例的多功能外围设备100的示意硬件结构的框图。

[0034] 控制单元101连接至作为图像输入装置的扫描器单元102和作为图像输出装置的打印机单元103，并且还通过连接至网络104或公共线路105来进行图像信息和装置信息的输入/输出。

[0035] CPU 106是用于进行多功能外围设备100的整体控制的处理器。RAM 107是提供CPU 106进行工作所用的系统工作存储器的存储器，并且还暂时存储图像数据、用户信息和密码

等。ROM 108是引导ROM，并且存储引导程序。HDD 109是硬盘驱动器，并且存储CPU 106所执行的程序、应用程序和图像数据等。此外，用于执行后面将说明的根据实施例的流程图的程序也存储在该HDD 109中。CPU 106通过将HDD 109中所存储的程序展开到RAM 107中并且执行该程序，来实现根据实施例的流程图的步骤。然而，除该CPU 106以外的处理器也可以执行这些流程图的步骤，或者CPU 106和其它处理器可以进行协作以执行这些流程图的处理。

[0036] 控制台单元接口110实现以下作用：控制与具有触摸面板的控制台单元111的接口；将要显示在控制台单元111上的图像数据输出至控制台单元111；并且将用户经由控制台单元111所输入的信息发送至CPU 106。网络接口112连接至网络104，并且经由网络104进行信息的输入/输出。调制解调器113连接至公共线路105，并且经由公共线路105进行相对于其它装置的信息的输入/输出。SRAM 114是可以高速进行工作的非易失性记录介质。RTC 115是实时时钟，并且进行用于即使在没有向控制单元101供给电力的状态下也对当前时刻进行连续计数的处理。上述装置配置在系统总线116上。

[0037] 图像总线I/F 117是使系统总线116和用于高速传送图像数据的图像总线118相连接并且对该数据结构进行转换的总线桥。图像总线118由PCI总线或IEEE 1394构成，并且以下所述的装置配置在该图像总线118上。RIP单元119是光栅图像处理器，并且将PDL代码展开成位图图像。装置I/F单元120使扫描器单元102、打印机单元103和控制单元101相连接，并且对图像数据进行同步和异步之间的转换。扫描器图像处理单元121对从扫描器单元102所输入的图像数据进行校正、处理和编辑。打印机图像处理单元122对要输出至打印机单元103的图像数据进行校正和分辨率转换等。TPM 123使得能够使用TPM加密密钥(TPM功能)。USB连接单元124连接至USB存储器125(外部存储器)，并且进行相对于USB存储器125的数据的输入/输出。

[0038] 图2是用于说明根据第一实施例的TPM 123和HDD 109所处理的加密密钥和机密数据的示意结构的框图。图2的上部示出TPM 123的示意结构，其中该TPM 123包括TPM根密钥201、TPM加密密钥202和TPM寄存器203。此外，图2的下部示出与TPM功能有关并且存储在HDD 109中的数据的示意结构，并且该数据包括装置加密密钥211、装置加密密钥块(device encryption Blob)212和加密数据213。

[0039] 在第一实施例中，使用装置加密密钥211对多功能外围设备100所处理的机密数据进行加密。该机密数据不仅包括诸如多功能外围设备100的图像数据和地址簿等的个人数据，并且还包括多功能外围设备100的应用程序软件所处理的各个加密密钥和证书、以及用户认证功能的密码等，但没有特别限制。

[0040] 使用TPM加密密钥202对装置加密密钥211进行加密。此外，使用TPM根密钥201对该TPM加密密钥202进行加密。假定该TPM根密钥201不能被来自外部的方法覆盖、删除或取出，并且仅可用于加密。该加密密钥链系列使得可以实现包括防篡改性的鲁棒安全。另外，在诸如工厂出货时等、TPM 123第一次连接至多功能外围设备100的情况下，在TPM 123中不存在TPM加密密钥202。在第一次启动多功能外围设备100时，CPU 106生成加密密钥，并且将该加密密钥作为TPM加密密钥输入至TPM 123。这样，在TPM 123内，使用TPM根密钥201对TPM加密密钥202进行加密，并且使TPM加密密钥202与TPM根密钥201相关联。在CPU 106将TPM加密密钥202输入至TPM 123的情况下，将信息存储在TPM寄存器203中，并且此外，TPM 123将加密密钥块输出至CPU 106。这些项用于验证TPM加密密钥202的有效性，并且将在后面要说明的

针对图3的处理的描述中进行说明。

[0041] 注意，第一实施例中的这些密钥的结构仅是示例，并且本发明不限于此。例如，可以采用在TPM中不存在TPM根密钥并且仅存储TPM加密密钥的结构，或者可以采用使用除TPM根密钥和TPM加密密钥以外的加密密钥来更加鲁棒地保护TPM内的加密密钥的结构。还可以采用使用TPM加密密钥、而不是使用利用TPM加密密钥所加密的装置加密密钥来对HDD 109中的机密数据进行直接加密的结构。

[0042] 接着，将参考图1～图3来说明在根据第一实施例的多功能外围设备100启动时所进行的用于验证TPM 123的加密密钥的有效性的控制。注意，本实施例的多功能外围设备100的处理由多功能外围设备100内的CPU 106来控制。

[0043] 图3是用于说明根据第一实施例的用于启动多功能外围设备100的处理的流程图。注意，例如，CPU 106通过将HDD 109中所存储的程序展开到RAM 107中并执行该程序，来实现该处理。

[0044] 首先，在步骤S301中，CPU 106从SRAM 114获得多功能外围设备100的TPM设置。该TPM设置是表示多功能外围设备100的TPM功能是有效还是无效的设置信息。接着，过程进入步骤S302，其中在该步骤S302中，CPU 106判断步骤S301中所获得的TPM设置是否有效。如果在步骤S302中CPU 106判断为TPM设置无效，则该处理结束。另一方面，如果在步骤S302中CPU 106判断为TPM设置有效，则过程进入步骤S303，其中在该步骤S303中，CPU 106验证加密密钥的有效性。

[0045] 在第一实施例中，将TPM 123的TPM加密密钥202以及装置加密密钥211设置为有效性验证对象。由于TPM加密密钥202是通过使用TPM根密钥201对HDD 109的装置加密密钥211进行加密所获得的密钥，因此有效性的验证是指确认装置加密密钥211是否是通过利用TPM根密钥201对TPM加密密钥202进行解密所获得的。如上所述，TPM 123的TPM加密密钥202是由CPU 106输入的，并且是利用TPM根密钥201进行加密的。此时，在CPU 106生成TPM加密密钥202并且将TPM加密密钥202存储至TPM 123时，CPU 106从TPM 123获得加密密钥块212并且将加密密钥块212存储至HDD 109。此时，还将使该加密密钥块212与TPM 123相关联的信息存储在TPM 123的TPM寄存器203中。因此，在步骤S303中，CPU 106将HDD 109中所存储的加密密钥块212输入至TPM 123。因此，TPM 123将所输入的加密密钥块212与TPM寄存器203中所存储的关联信息进行比较。如果这两者一致，则确认出TPM 123的TPM加密密钥202和HDD 109中所存储的装置加密密钥211彼此关联。

[0046] 注意，用于确认加密密钥的有效性的该处理仅是示例，并且不限于该处理。例如，可以将装置加密密钥的副本保持在TPM寄存器203中，并且CPU 106可以将装置加密密钥211输入至TPM 123，并且将装置加密密钥211与TPM寄存器203中所保持的装置加密密钥进行比较。这样可以确认HDD 109的装置加密密钥211和TPM 123的TPM加密密钥202是否彼此关联。

[0047] 在步骤S303的处理之后，过程进入步骤S304，其中在该步骤S304中，CPU 106通过验证加密密钥的有效性来判断是否可以正常使用CPU 106所处理的加密密钥。如果在步骤S304中CPU 106通过验证加密密钥的有效性判断为可以正常使用加密密钥，则该处理结束。另一方面，如果在步骤S304中CPU 106通过验证加密密钥的有效性判断为不能正常使用要处理的加密密钥，则过程进入步骤S305，其中在该步骤S305中，CPU 106将错误画面(这里未示出)显示在控制台单元111上，并且结束该处理。

[0048] 上述处理是用于在启动多功能外围设备100时验证TPM加密密钥的有效性的处理。此时，如步骤S305那样不能正常使用加密密钥的情况的示例是诸如以下等的情况：由于TPM芯片的故障、或者TPM芯片连接至或包括TPM芯片的主板的故障，因而更换芯片/主板，然后启动多功能外围设备100。

[0049] 接着，将参考图1、4和5来说明根据第一实施例的用于使TPM功能有效的控制。

[0050] 图4是用于说明根据第一实施例的用于使多功能外围设备100中的TPM功能有效的处理的流程图。注意，例如，CPU 106通过将HDD 109中所存储的程序展开到RAM 107中并执行该程序，来实现该处理。

[0051] 首先，在步骤S401中，CPU 106从控制台单元111接收用于显示TPM设置管理画面(图5A～5C)的指示。接着，过程进入步骤S402，并且CPU 106获得SRAM 114中所存储的TPM设置。接着，过程进入步骤S403，并且CPU 106判断所获得的TPM设置是否被设置成有效。如果判断为TPM设置有效，则过程进入步骤S412，否则过程进入步骤S404，其中在该步骤S404中，CPU 106判断USB存储器125是否连接至USB连接单元124。如果在步骤S404中CPU 106判断为USB存储器125没有连接至USB连接单元124，则过程进入步骤S405。在步骤S405中，CPU 106将用于请求用户使USB存储器125连接至USB连接单元124的消息显示在控制台单元111上，并且过程进入步骤S404。

[0052] 图5A描述示出根据第一实施例的多功能外围设备100的控制台单元111上所显示的TPM设置管理画面的示例的图。

[0053] 这里，例示如下示例：显示请求用户使可以备份TPM加密密钥的USB存储器125连接至USB连接单元124的消息，以使TMP设置有效。该画面包括当前TPM设置项501和用于使TPM设置有效的按钮502。在步骤S405的状态下的图5A中，没有连接USB存储器125，因而以灰化方式显示用于使TPM设置有效的按钮502，使得不能按压按钮502。

[0054] 如果在步骤S404中CPU 106判断为USB存储器125连接至USB连接单元124，则过程进入步骤S406，其中在该步骤S406中，CPU 106获得与USB存储器125有关的信息，并且过程进入步骤S407。在步骤S407中，CPU 106判断是否可以将TPM加密密钥备份在USB存储器125的存储区域中。如果在步骤S407中判断为不能备份TPM加密密钥，则过程进入步骤S405。这里，不能备份TPM加密密钥的状态是指如下情况：例如，在USB存储器125中不存在空闲存储区域、或者用户不具有能够向存储区域进行写入的权限的情况下，不能将TPM加密密钥写入USB存储器125。

[0055] 注意，在第一实施例中，假定TPM加密密钥的备份目的地是USB存储器，但备份目的地可以是除USB存储器以外的存储器，并且没有特别限制。例如，可以使用诸如USB-HDD和SD卡等的存储介质、经由网络的SMB或者云存储区域等。

[0056] 另一方面，如果在步骤S407中CPU 106判断为可以将TPM加密密钥备份在USB存储器125的存储区域中，则过程进入步骤S408，其中在该步骤S408中，CPU 106以可按压状态显示上述的用于使TPM设置管理画面的TPM设置有效的按钮502。图5B示出例示如下示例的图：在TPM设置管理画面上，用于使TPM设置有效的按钮502的灰化状态解除，并且以可按压的状态显示按钮502。

[0057] 接着，过程进入步骤S409，其中在该步骤S409中，CPU 106判断是否按压用于使TPM设置有效的按钮502。如果在步骤S409中CPU 106判断为按压了按钮502，则过程进入步骤

S410,其中在该步骤S410中,CPU 106使TPM设置有效。之后,在步骤S411中,CPU 106执行用于备份TPM加密密钥的处理。

[0058] 在第一实施例中,在TPM设置有效的情况下,CPU 106将用于生成TPM加密密钥的指示输出至TPM 123。因此,TPM 123生成TPM加密密钥,并且将加密密钥块212输出至CPU 106。表示TPM功能的设置有效的设置信息由CPU 106存储在SRAM 114中。

[0059] 在这些步骤S404～S411中用户使TPM功能有效的情况下,在可以预先备份TPM加密密钥的条件下执行用于生成TPM加密密钥的处理。这样具有防止用户忘记备份TPM加密密钥的效果。

[0060] 接着,将参考图1、6和7来说明步骤S411中的用于备份TPM加密密钥的处理。

[0061] 图6是用于说明根据第一实施例的多功能外围设备100所进行的图4的步骤S411的用于备份TPM加密密钥的处理的流程图。

[0062] 在步骤S601中,CPU 106将用于输入TPM加密密钥的备份所用的密码的画面显示在控制台单元111上,并且在备份TPM加密密钥时接收该密码的输入。

[0063] 图7描述示出根据第一实施例的多功能外围设备100的控制台单元111上所显示的用于输入TPM加密密钥的备份所用的密码的画面的示例的图。

[0064] 将从控制台单元111所输入的密码以利用“*”掩蔽的方式显示在密码输入框701中。这里,在用户按压OK(确定)按钮702时,CPU 106接收到TPM加密密钥的备份所用的密码和用以执行TPM加密密钥的备份的指示。在第一实施例中,该密码信息由CPU 106保持在SRAM 114中。另外,在第一实施例中,假定输入两次相同的密码以防止误设置。

[0065] 如果这样在步骤S602中CPU 106判断为密码的输入完成,则过程进入步骤S603,其中在该步骤S603中,CPU 106基于SRAM 114中所保持的密码来对TPM加密密钥进行加密,并且过程进入步骤S604。在第一实施例中,假定采用PKCS#12(公钥加密标准#12)格式来进行使用密码的加密。注意,在第一实施例中,利用基于用户所指定的密码信息的密码加密方法来进行TPM加密密钥的备份,但本发明不限于此。例如,可以利用多功能外围设备100中预先保持的固定密码、公共密钥、或者使用PKI机制的公开密钥或秘密密钥来保护TPM加密密钥。

[0066] 接着,过程进入步骤S604,其中在该步骤S604中,CPU 106使加密后的TPM加密密钥形成为输出文件格式并归档该文件以备份加密后的TPM加密密钥,并且过程进入步骤S605。在第一实施例中,在进行后面将说明的TPM加密密钥的恢复之前,通过向要输出的文件添加标识头部以将该文件标识为加密后的TPM加密密钥的文件来归档该文件。在第一实施例中,将该数据称为TPM加密密钥备份数据。

[0067] 在步骤S605中,CPU 106将归档后的TPM加密密钥备份数据写入USB存储器125。接着,过程进入步骤S606,其中在该步骤S606中,CPU 106判断TPM加密密钥备份数据是否可被正常写入USB存储器125,并且如果判断为向USB存储器125的写入失败,则过程进入步骤S607。在步骤S607中,CPU 106将写入错误显示在控制台单元111上,并且过程进入步骤S601,其中在该步骤S601中,重复备份处理。

[0068] 另一方面,如果在步骤S606中判断为向USB存储器125的备份成功,则过程进入步骤S608,其中在该步骤S608中,CPU 106将备份完成标志存储至SRAM 114,并且过程进入步骤S609。在步骤S609中,CPU 106将表示TPM加密密钥的备份完成的消息显示在控制台单元111上,并且结束用于备份TPM加密密钥的该处理。

[0069] 注意，在第一实施例中，假定在按压用于使TPM设置有效的按钮502时、画面自动切换为图7中的用于输入TPM加密密钥的备份所用的密码的画面。然而，在不存在画面自动转变的情况下，可以采用画面根据用户指示而转变并且进行备份的结构。

[0070] 接着，说明现在返回至图4。

[0071] 在这样TPM加密密钥的备份完成的情况下，过程进入图4的步骤S412，并且CPU 106将表示TPM设置有效的消息显示在控制台单元111上。

[0072] 图5C示出在TPM设置有效的情况下TPM设置画面上的示例的图。

[0073] 图5C示出如下示例：当前TPM设置项501改变为“ON(开启)”，并且以灰化方式显示用于使TPM设置有效的按钮502，使得该按钮502不可按压。

[0074] 注意，根据第一实施例，设想只有具有管理权限的用户可以使TPM设置有效并且备份TPM加密密钥。因此，仅在具有管理权限的用户登录的情况下，才显示图5A～5C所示的TPM设置管理画面。

[0075] 如上所述，根据第一实施例，在具有TPM功能的信息处理设备中，在可以备份TPM加密密钥的条件下，用户可以将TPM设置从无效状态改变为有效状态。这样可以防止用户在使TPM设置有效之后忘记备份TPM加密密钥。

[0076] 第二实施例

[0077] 接着，将说明本发明的第二实施例。在上述的第一实施例中，假定用户在使多功能外围设备100的TPM设置有效时、经由控制台单元111进行操作。然而，代替只有利用来自本地UI的这种设置才使TPM设置有效，还存在远程地使TPM设置有效的情况。一个示例是将包括多功能外围设备100的TPM设置的管理员设置作为数据经由网络导入的情况。在这种情况下，在假定远程地给出指示的情况下，以下是不现实的：除非如第一实施例那样连接了诸如USB存储器等的存储器，否则无法使TPM功能有效。另一方面，如果采用即使在没有连接存储器的情况下也可以远程地使TPM设置有效的结构，则存在发生没有备份TPM加密密钥的情形的可能性。

[0078] 有鉴于此，在第二实施例中，在经由网络从远程设备接收到用以使TPM设置有效的指示的情况下，即使没有连接存储器，也允许使TPM设置有效。在启动在没有备份TPM加密密钥的状态下使TPM设置有效的多功能外围设备100时、或者在这种状态下在多功能外围设备100中进行用户认证时，提示用户备份TPM加密密钥，由此防止用户忘记备份TPM加密密钥。注意，关于根据第二实施例的多功能外围设备100和TPM 123的结构以及TPM加密密钥备份处理等，在第二实施例中没有进行说明的部分与第一实施例中的这些部分相同。以下将说明在从远程设备接收到用以使TPM设置有效的指示时使TPM设置有效的情况下的处理。同样在第二实施例中，在用户尝试从多功能外围设备100的控制台单元111使TPM设置有效时，多功能外围设备100执行第一实施例的处理。

[0079] 图8是用于说明根据第二实施例的用于启动多功能外围设备100的处理的流程图。注意，例如，CPU 106通过将HDD 109中所存储的程序展开到RAM 107中并执行该程序，来实现该处理。图8的该处理与根据上述的第一实施例的图3的流程图的不同之处在于：添加了步骤S806和S807的处理。该添加的处理是用于在没有备份TPM加密密钥的情况下显示备份指示的处理，但后面将详细说明该处理。根据第二实施例的图8的流程图中的步骤S801～S805的处理与第一实施例的图3中的步骤S301～S305的处理相同，因而省略了针对这些步

骤的说明。

[0080] 如果在步骤S804中CPU 106通过验证加密密钥的有效性而判断为可以正常使用CPU 106所处理的加密密钥，则过程进入步骤S806。在步骤S806中，CPU 106参考SRAM 114中所存储的备份完成标志，并且判断是否备份了TPM加密密钥。该备份完成标志是在上述的第一实施例的步骤S608中CPU 106存储在SRAM 114中的信息。如果这样在步骤S806中CPU 106判断为备份了TPM加密密钥，则该处理结束。另一方面，如果在步骤S806中CPU 106判断为没有备份TPM加密密钥，则过程进入步骤S807，其中在该步骤S807中，CPU 106将用于指示TPM加密密钥的备份的画面显示在控制台单元111上，并且结束该处理。

[0081] 图9描述示出根据第二实施例的多功能外围设备100所提供的功能的主菜单画面的示例的图。在多功能外围设备100启动时，CPU 106将该画面显示在控制台单元111上。在第二实施例中，在该主菜单画面的状态行901的区域中显示备份指示消息902，并且显示用于提示用户备份TPM加密密钥的画面。

[0082] 因此，多功能外围设备100的用户通知没有备份TPM加密密钥，并且可以采取适当措施。

[0083] 接着，将说明在管理员针对多功能外围设备100进行用户认证的情况下的控制。

[0084] 图10是用于说明根据第二实施例的多功能外围设备100所进行的用户认证处理的流程图。注意，例如，CPU 106通过将HDD 109中所存储的程序展开到RAM 107中并执行该程序，来实现该处理。

[0085] 首先，在步骤S1001中，CPU 106使控制台单元111显示登录画面，并且过程进入步骤S1002。在步骤S1002中，CPU 106经由控制台单元111接收来自用户的用户信息和密码的输入。这样所输入的用户信息和密码被保持在RAM 107中。在第二实施例中，RAM 107用于暂时存储用户信息和密码，而且可以使用诸如HDD 109等的可以存储数据的其它设备，并且没有进行限制。后面所述的第三实施例同样也不限于这种方式。另外，在第二实施例中，CPU 106使用装置加密密钥211对与用户认证所用的用户信息相关联的密码进行加密，并且将该密码存储在HDD 109中。

[0086] 接着，过程进入步骤S1003，其中在该步骤S1003中，CPU 106从HDD 109获得与所输入的用户信息相关联地进行加密后的密码信息，对该密码信息进行解密，将该密码信息与已输入的密码进行比较，并验证该密码是否是正确密码，并且过程进入步骤S1004。在第二实施例中，使用装置加密密钥211来进行利用CPU 106针对加密后的密码的这种解密。另外，使用TPM 123的TPM加密密钥202对装置加密密钥211进行加密。CPU 106通过将加密后的装置加密密钥211输入至TPM 123，来获得并使用利用TPM加密密钥202进行解密后的装置加密密钥。此外，该TPM加密密钥202已利用TPM根密钥201进行了加密，并且在使用TPM加密密钥202时，使用TPM根密钥201对TPM加密密钥202进行解密。

[0087] 如果在步骤S1004中CPU 106通过使用步骤S1002中所输入的用户信息和密码来对用户进行认证、结果认证失败，则在控制台单元111上显示错误，并且过程进入步骤S1002。另一方面，如果在步骤S1004中CPU 106判断为所输入的用户信息和密码正确、并且用户认证成功，则过程进入步骤S1005，其中在该步骤S1005中，CPU 106允许用户登录多功能外围设备100。接着，过程进入步骤S1006，其中在该步骤S1006中，CPU 106使RAM 107保持已登录的用户的用户信息，并且使过程进入步骤S1007。在步骤S1007中，CPU 106从SRAM 114获得

TPM设置，并且过程进入步骤S1008。

[0088] 在步骤S1008中，CPU 106判断从SRAM 114获得的TPM设置是否被设置成有效。这里，如果CPU 106判断为TPM设置无效，则该处理结束。另一方面，如果在步骤S1008中CPU 106判断为TPM设置被设置成有效，则过程进入步骤S1009，其中在该步骤S1009中，CPU 106判断是否从SRAM 114备份了TPM加密密钥。此时，如第一实施例所述，根据SRAM 114中所存储的备份完成标志是否为开启来判断是否备份了TPM加密密钥。这里，如果判断为备份了TPM加密密钥，则该处理结束。另一方面，如果在步骤S1009中CPU 106判断为没有备份TPM加密密钥，则过程进入步骤S1010，其中在该步骤S1010中，CPU 106判断已登录的用户是否具有管理权限。这里，如果判断为该用户具有管理权限，则过程进入步骤S1011，其中在该步骤S1011中，CPU 106使得显示用于提示用户备份TPM加密密钥的画面。在第二实施例中，将上述的图7中的用于输入TPM加密密钥的备份所用的密码的画面显示在控制台单元111上。之后的用于备份TPM加密密钥的处理与上述的第一实施例的处理相同。在步骤S1012中，与上述的图6的流程图相同，CPU 106执行用于备份TPM加密密钥的处理，并且结束该处理。

[0089] 该处理使得可以在已登录的用户是管理员并且没有备份TPM加密密钥的情况下，通过提示用户备份TPM加密密钥来防止用户忘记备份TPM加密密钥。注意，在第二实施例中，紧挨在对用户进行认证之后在控制台单元111上显示用于提示备份的画面，但本发明不限于此。例如，可以采用如下结构：在用户改变多功能外围设备100的管理设置的情况下，在控制台单元111的显示转变为管理画面时显示这种画面。

[0090] 如果在步骤S1010中CPU 106判断为已登录的用户不具有管理权限，则该处理结束。在第二实施例中，这是因为，设想TPM加密密钥的备份仅由具有管理权限的用户来执行。

[0091] 注意，在第二实施例中，即使没有备份TPM加密密钥，也可以执行多功能外围设备100所提供的诸如复制功能等的其它功能。然而，可以采用以下规格：如果没有备份TPM加密密钥，则不能操作图9的主菜单画面中所设置的诸如复制按钮等的按钮，使得不允许执行预定功能，并且没有特别限制。

[0092] 如上所述，根据第二实施例，在启动在没有备份TPM加密密钥的状态下使TPM设置有效的多功能外围设备100、或者在这种状态下对用户进行认证的情况下，提示用户备份TPM加密密钥。不同于第一实施例，例如，这样使得可以在用户远程地使TPM设置有效的情况下、防止用户忘记备份TPM加密密钥。

[0093] 第三实施例

[0094] 接着，将说明本发明的第三实施例。在上述的第一实施例和第二实施例中，在具有TPM功能的多功能外围设备100中，在使TPM设置有效之后生成TPM加密密钥，因而还可以仅在使TPM设置有效之后才进行备份。然而，可能存在功能(以下称为HSM(Hardware Security Module，硬件安全模块)功能)有效之前生成加密密钥(以下称为HSM加密密钥)的一些其它HSM。有鉴于此，在第三实施例中，将说明在可以在HSM功能有效之前生成/备份HSM加密密钥的多功能外围设备100中用于防止用户忘记备份HSM加密密钥的控制。在第三实施例中，以下将说明与上述的第一实施例和第二实施例的不同之处。

[0095] 图11是用于说明根据本发明的第三实施例的多功能外围设备100所进行的用于使HSM功能有效的处理和备份处理的流程图。注意，例如，CPU 106通过将HDD 109中所存储的程序展开到RAM 107中并执行该程序，来实现该处理。

[0096] 首先，在步骤S1101中，CPU 106从控制台单元111接收用于显示HSM设置管理画面的指示。接着，过程进入步骤S1102，其中在该步骤S1102中，CPU 106从SRAM 114获得HSM设置。接着，在步骤S1103中，CPU 106判断从SRAM 114所获得的HSM设置是否有效。如果在步骤S1103中CPU 106判断为所获得的HSM设置无效，则过程进入步骤S1104，其中在该步骤S1104中，CPU 106将用于请求用户预先备份HSM加密密钥的消息显示在控制台单元111上，然后过程进入步骤S1105。

[0097] 在步骤S1105中，CPU 106判断是否备份了HSM加密密钥。同样在这种情况下，与上述的步骤S806相同，根据SRAM 114中所存储的备份完成标志是否为开启来判断是否备份了HSM加密密钥。这里，如果判断为没有备份HSM加密密钥，则过程进入步骤S1106，其中在该步骤S1106中，CPU 106接收HSM加密密钥的备份，并且过程进入步骤S1107。

[0098] 图12A描述示出在图11的步骤S1106中在多功能外围设备100的控制台单元111上所显示的HSM设置管理画面的示例的图。这里，显示用于请求用户预先备份HSM加密密钥的消息，并且当前HSM设置1203为关闭。这里，如图12A所示，以可操作方式显示用于指示HSM加密密钥的备份的执行的按钮1202，并且以灰化方式显示用于使HSM设置有效的按钮1201，使得该按钮1201不可操作。

[0099] 在步骤S1107中，CPU 106判断是否通过对按钮1202进行操作而指示了HSM加密密钥的备份的执行，并且如果判断为指示了HSM加密密钥的备份的执行，则过程进入步骤S1108，并且执行用于备份HSM加密密钥的处理。在用于备份HSM加密密钥的该处理中，TPM加密密钥的备份仅被HSM加密密钥的备份替换，并且该处理与上述的第一实施例的步骤S411基本相同。

[0100] 另一方面，如果在步骤S1105中CPU 106判断为备份了HSM加密密钥，则过程进入步骤S1109，其中在该步骤S1109中，CPU 106接收到用以使HSM设置有效的指示，并且过程进入步骤S1110。

[0101] 图12B描述示出在图11的步骤S1109中在多功能外围设备100的控制台单元111上所显示的HSM设置管理画面的示例的图。

[0102] 这里，HSM加密密钥已备份，因而解除用于使HSM设置有效的按钮1201的灰化状态，使得可以按压按钮1201。另外，在图12B中，以灰化状态显示用于指示HSM加密密钥的备份的执行的按钮1202，使得该按钮1202不可操作。

[0103] 在步骤S1110中，CPU 106判断是否通过按压用于使HSM设置有效的按钮1201作出了用以使HSM设置有效的指示。这里，如果判断为按压了用于使HSM设置有效的按钮1201，则CPU 106使过程进入步骤S1111以使HSM设置有效，并且使过程进入步骤S1112。通过采用由于这种处理、因而除非必定备份了HSM加密密钥否则不能使HSM设置有效的结构，可以防止用户忘记备份HSM加密密钥。

[0104] 接着，在步骤S1112中，CPU 106将HSM功能设置有效的状态显示在HSM设置管理画面上。

[0105] 图12C描述示出在图11的步骤S1112中在多功能外围设备100的控制台单元111上所显示的HSM设置管理画面的示例的图，并且这里示出表示HSM设置已有效的画面的示例。

[0106] 在图12C中，HSM设置有效，并且HSM加密密钥已备份，因而将当前HSM设置1202设置成ON，并且以灰化方式显示用于使HSM设置有效的按钮1201，使得该按钮1201不可操作。此

外,以灰化方式显示用于指示HSM加密密钥的备份的执行的按钮1202,使得该按钮1202不可操作。

[0107] 如上所述,根据第三实施例,可以采用如下结构:在可以在HSM设置有效之前备份HSM加密密钥的多功能外围设备中,除非必定备份了HSM加密密钥,否则不能使HSM设置有效。这样使得可以在HSM设置有效时防止用户忘记备份HSM加密密钥。

[0108] 其它实施例

[0109] 本发明的实施例还可以通过如下的方法来实现,即,通过网络或者各种存储介质将执行上述实施例的功能的软件(程序)提供给系统或装置,该系统或装置的计算机或是中央处理单元(CPU)、微处理单元(MPU)读出并执行程序的方法。

[0110] 尽管已经参考典型实施例说明了本发明,但是应该理解,本发明不限于所公开的典型实施例。所附权利要求书的范围符合最宽的解释,以包含所有这类修改、等同结构和功能。

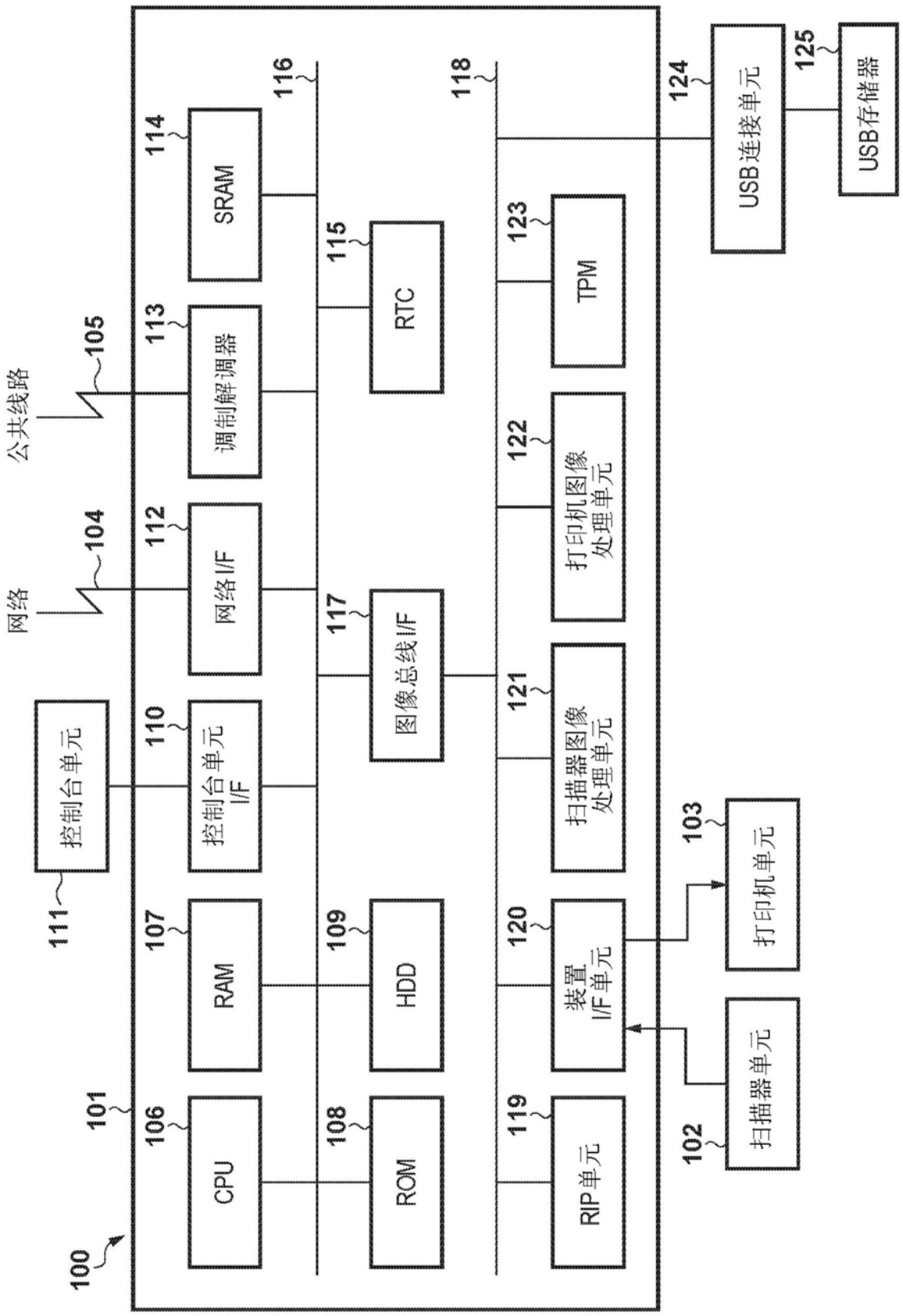

100
101
CPU
106
ROM
108
RIP单元
119
RAM
107
HDD
109
装置
I/F单元
120
控制台单元
111
控制台单元
I/F
110
网络I/F
112
调制解调器
113
SRAM
114
RTC
115
图像总线I/F
117
扫描器图像
处理单元
121
打印机图像
处理单元
122
TPM
123
USB连接单元
124
USB存储器
125
公共线路
105
网络
104
116
118
扫描器单元
102
打印机单元
103

图1

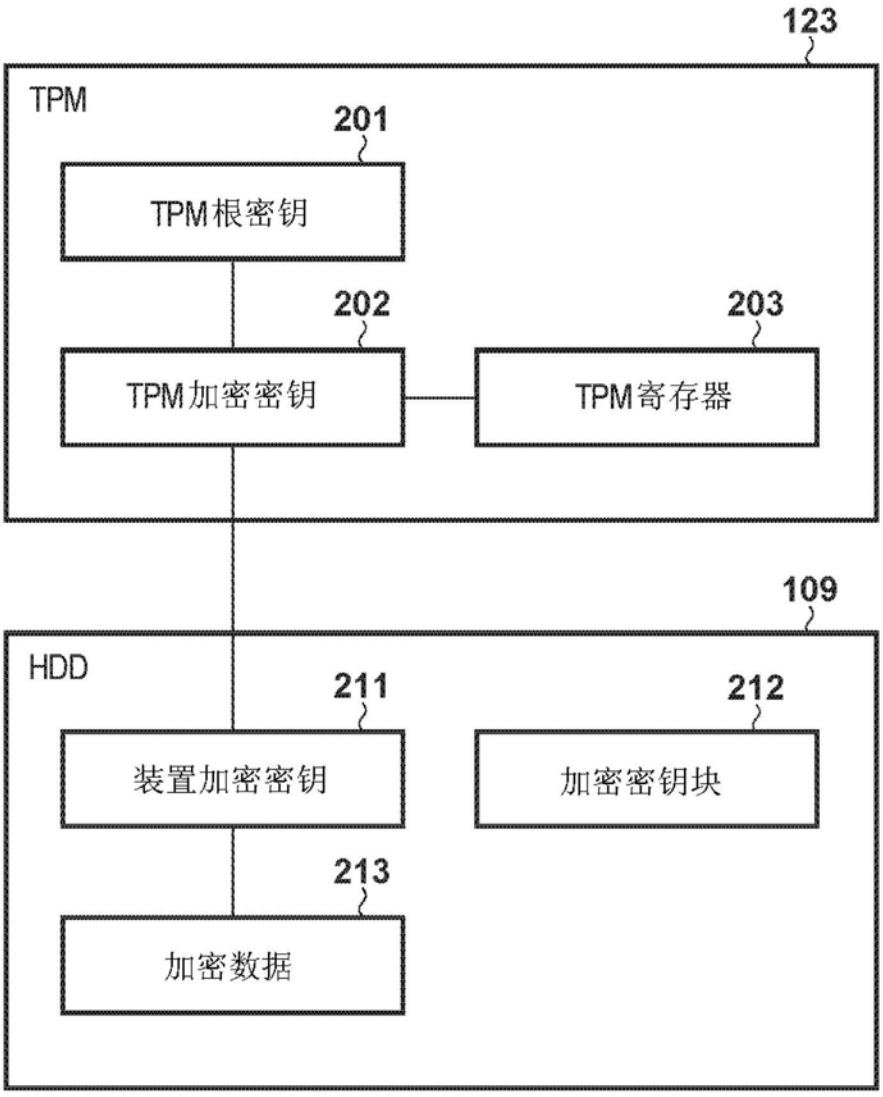

123
TPM
201
TPM根密钥
202
203
TPM加密密钥
TPM寄存器
109
HDD
211
212
装置加密密钥
加密密钥块
213
加密数据

图2

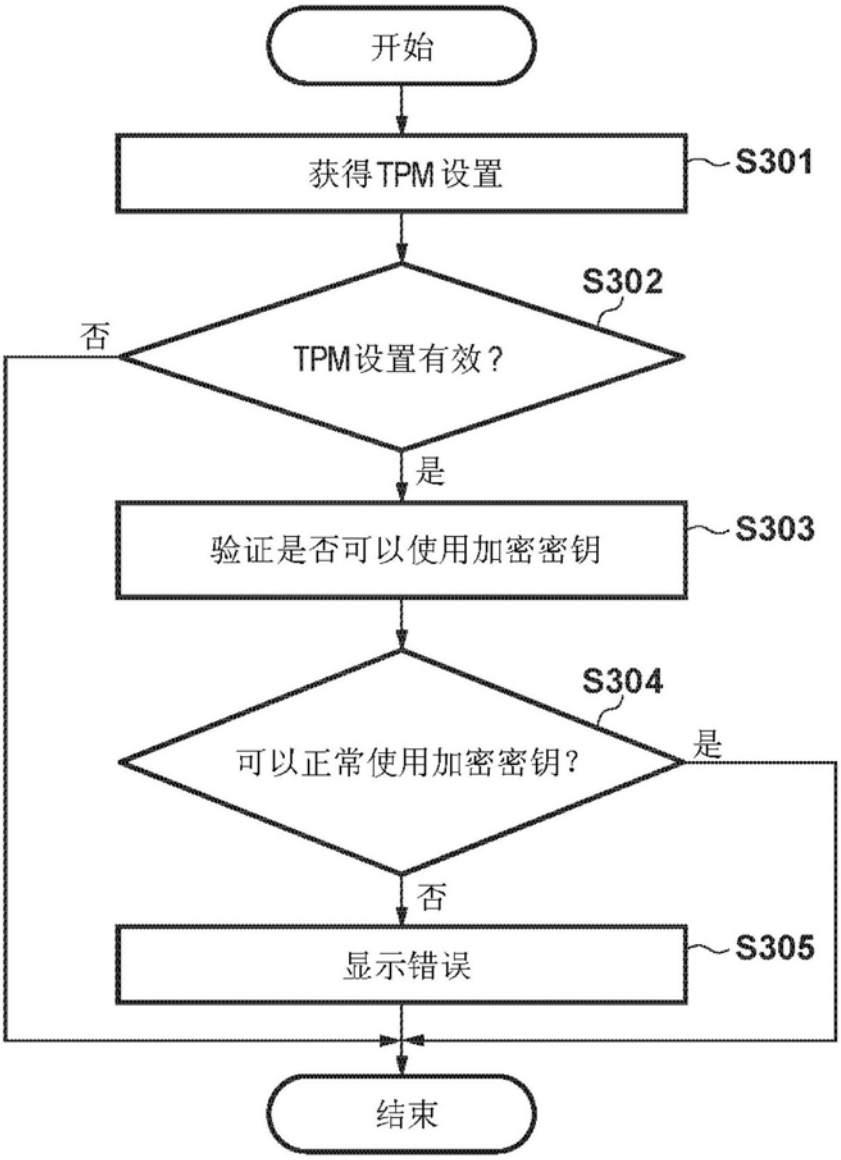

开始
获得TPM设置
S301
S302
TPM设置有效？
否
是
验证是否可以使用加密密钥
S303
S304
可以正常使用加密密钥？
是
否
显示错误
S305
结束

图3

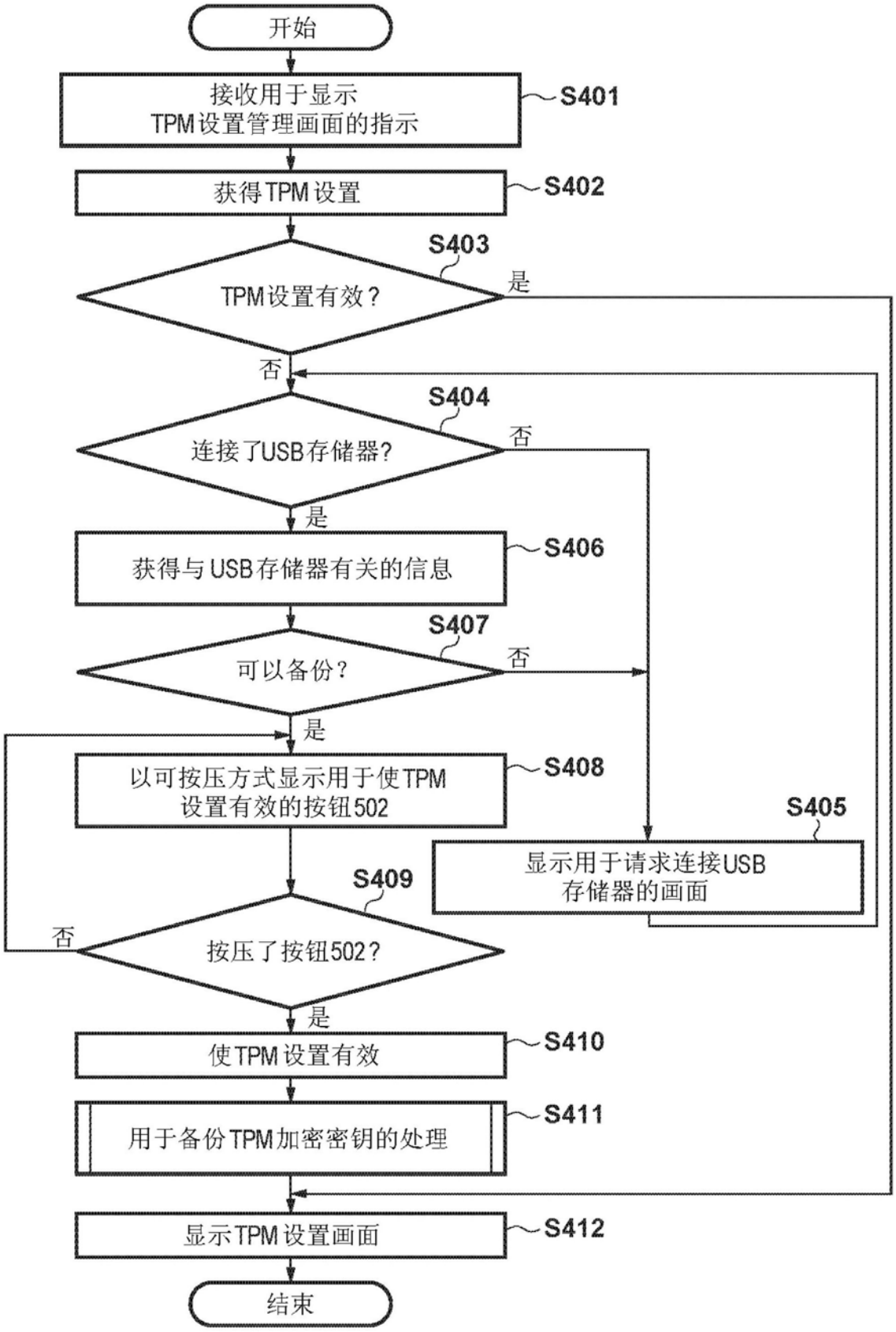

开始
接收用于显示TPM设置管理画面的指示
S401
获得TPM设置
S402
S403
TPM设置有效？
是
否
S404
连接了USB存储器？
否
是
获得与USB存储器有关的信息
S406
S407
可以备份？
否
是
以可按压方式显示用于使TPM设置有效的按钮502
S408
S405
显示用于请求连接USB存储器的画面
S409
否
按压了按钮502？
是
使TPM设置有效
S410
用于备份TPM加密密钥的处理
S411
显示TPM设置画面
S412
结束

图4

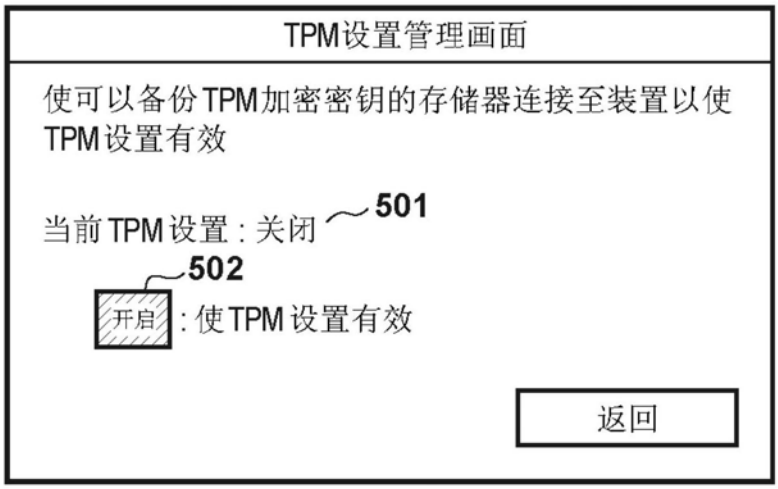

TPM设置管理画面
使可以备份TPM加密密钥的存储器连接至装置以使TPM设置有效
当前TPM设置：关闭
501
502
开启
：使TPM设置有效
返回

图5A

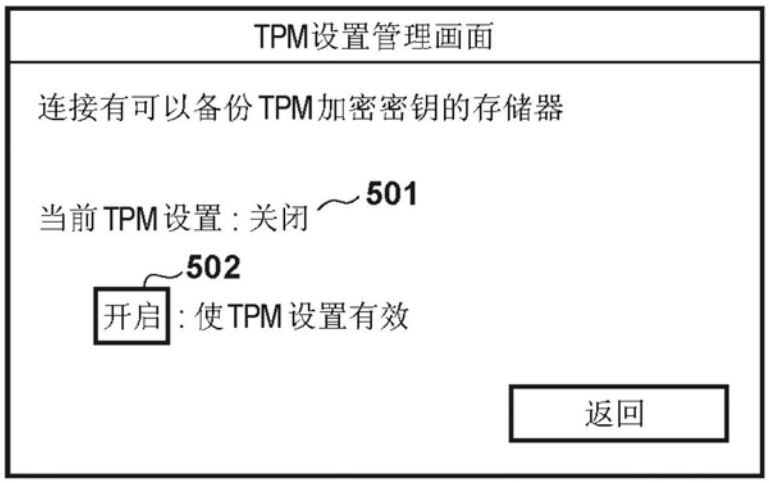

TPM设置管理画面
连接有可以备份TPM加密密钥的存储器
当前TPM设置：关闭
501
502
开启
：使TPM设置有效
返回

图5B

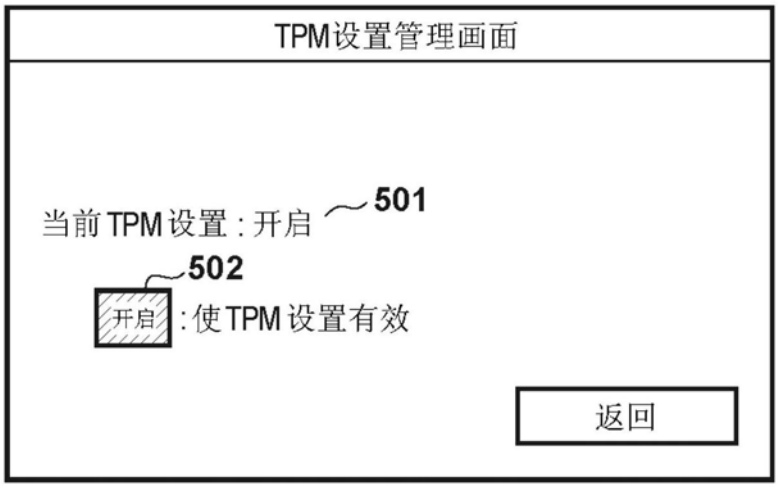


图5C

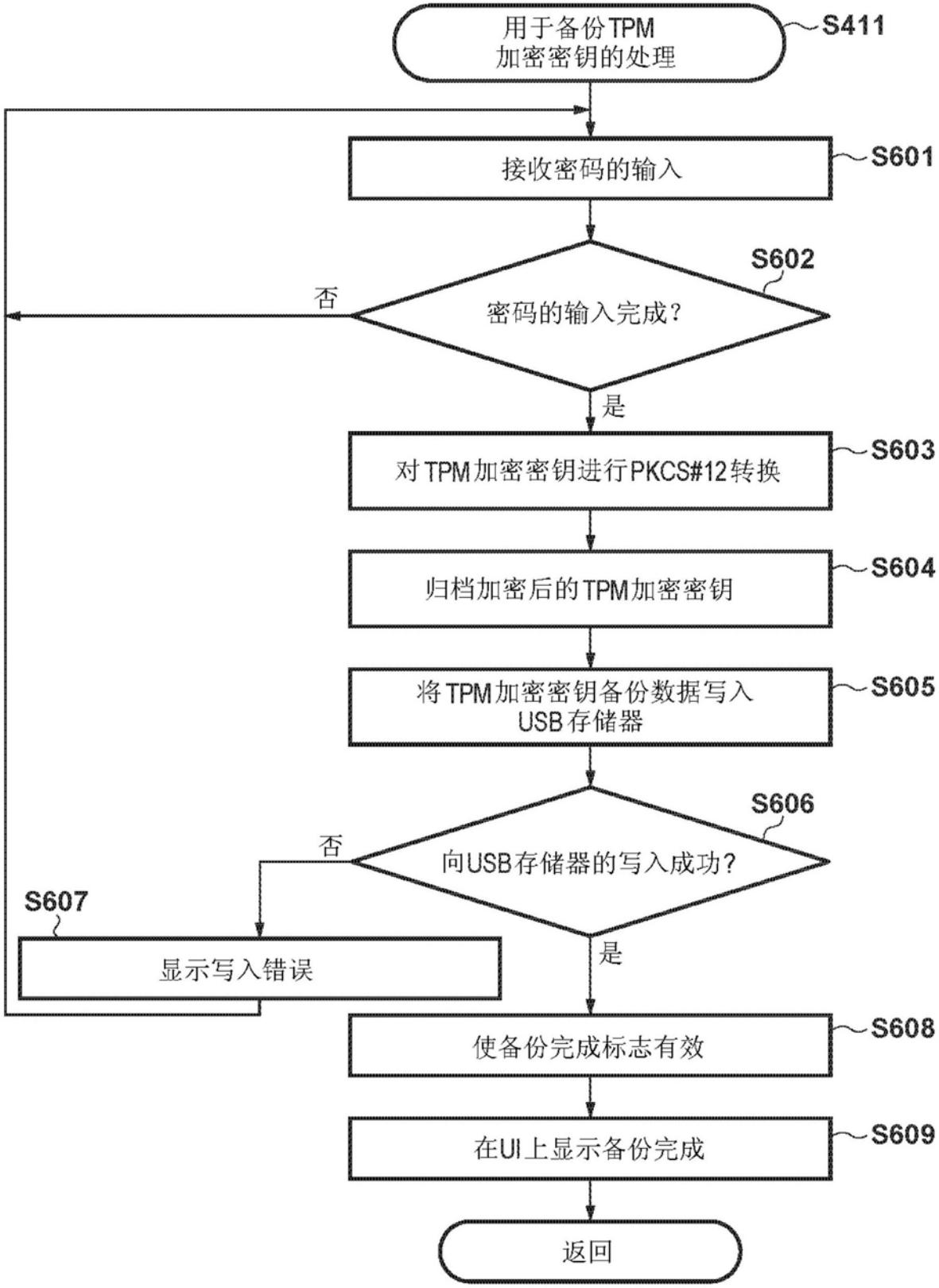

用于备份TPM
加密密钥的处理
S411
接收密码的输入
S601
S602
密码的输入完成?
否
是
对TPM加密密钥进行PKCS#12转换
S603
归档加密后的TPM加密密钥
S604
将TPM加密密钥备份数据写入
USB存储器
S605
S606
向USB存储器的写入成功?
否
S607
显示写入错误
是
使备份完成标志有效
S608
在UI上显示备份完成
S609
返回

图6

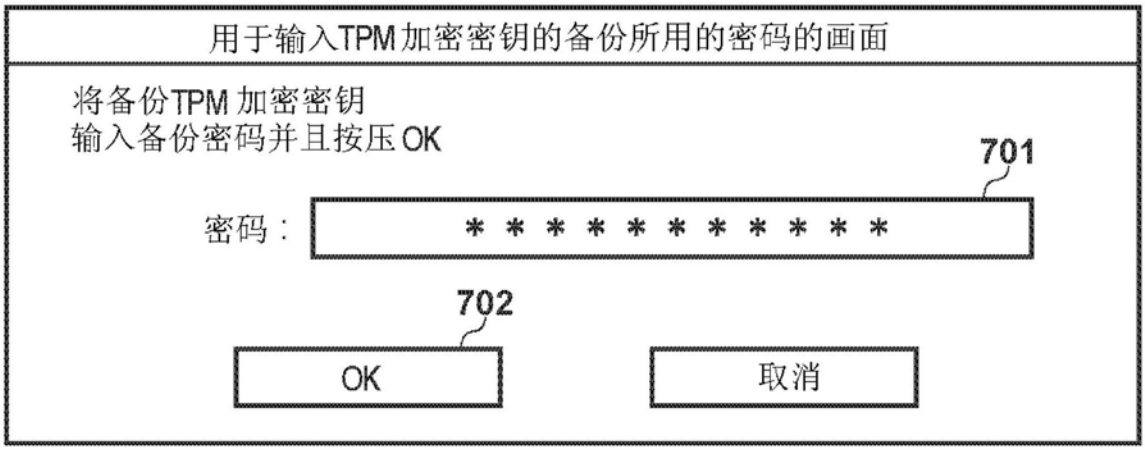

用于输入TPM加密密钥的备份所用的密码的画面
将备份TPM加密密钥
输入备份密码并且按压OK
701
密码：
* * * * * * * * * * * *
702
OK
取消

图7

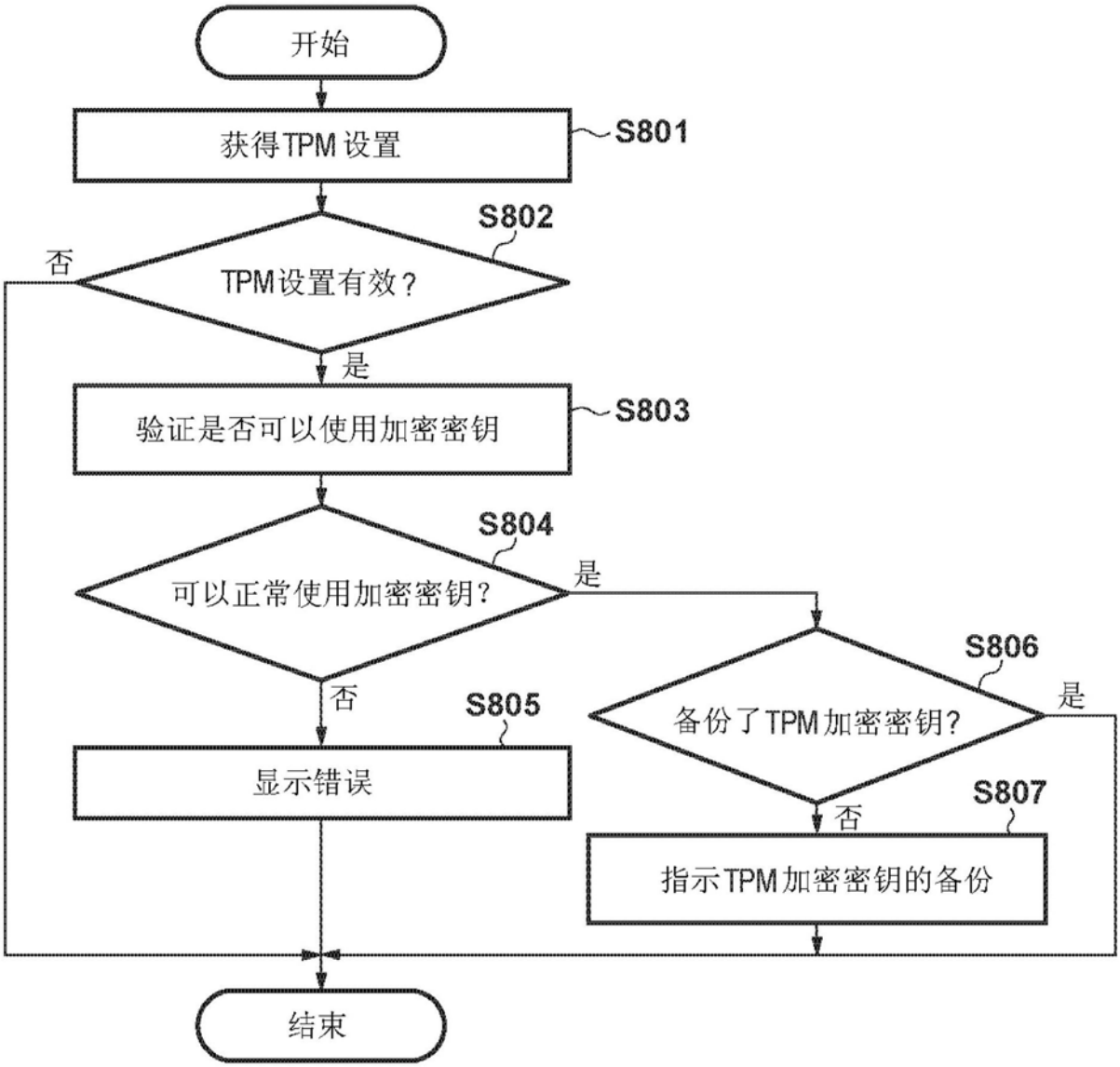

开始
获得TPM设置
S801
S802
TPM设置有效？
否
是
验证是否可以使用加密密钥
S803
S804
可以正常使用加密密钥？
是
否
S805
显示错误
S806
备份了TPM加密密钥？
是
否
S807
指示TPM加密密钥的备份
结束

图8

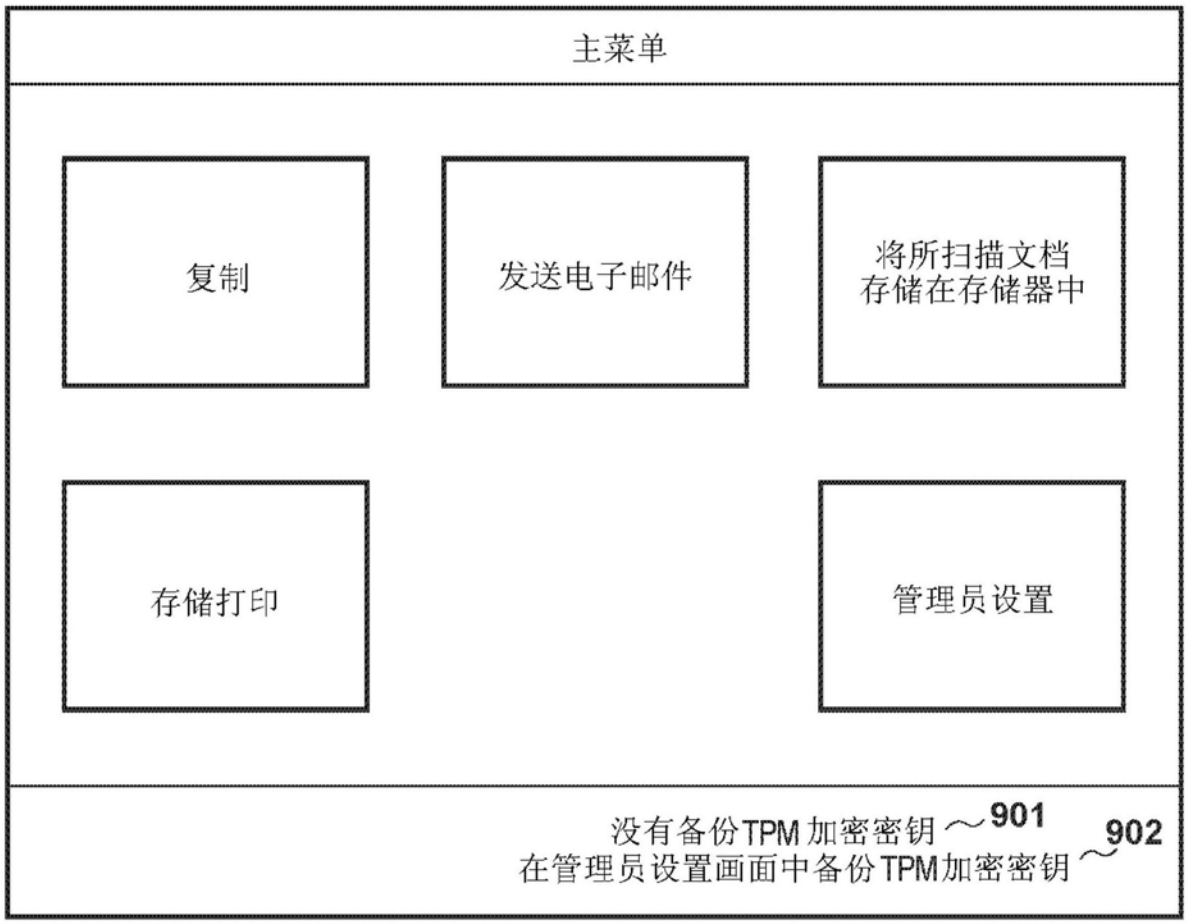

主菜单
复制
发送电子邮件
将所扫描文档
存储在存储器中
存储打印
管理员设置
没有备份TPM加密密钥
901
在管理员设置画面中备份TPM加密密钥
902

图9

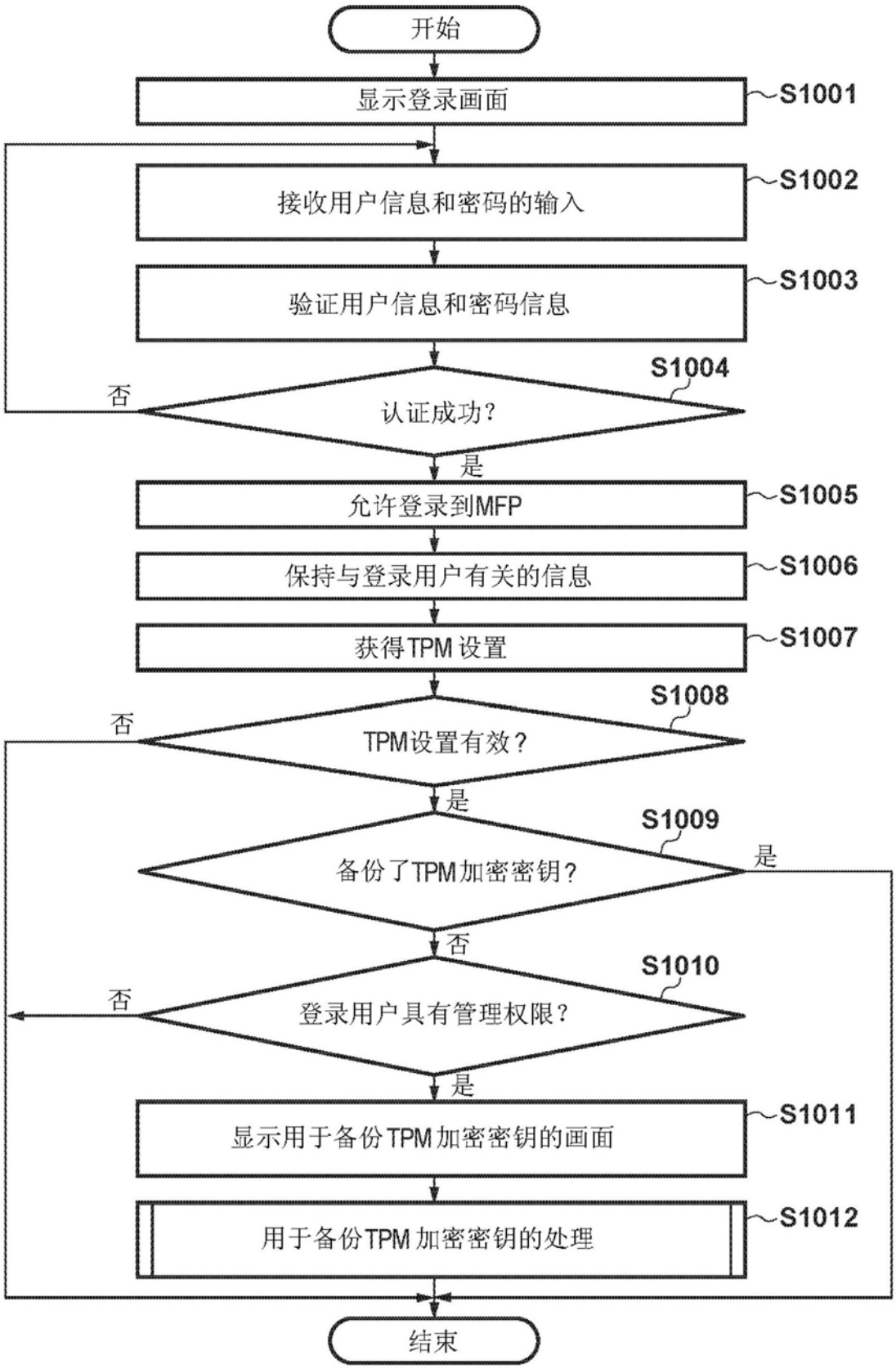

开始
显示登录画面
S1001
接收用户信息和密码的输入
S1002
验证用户信息和密码信息
S1003
S1004
否
认证成功?
是
允许登录到MFP
S1005
保持与登录用户有关的信息
S1006
获得TPM设置
S1007
S1008
否
TPM设置有效?
是
S1009
备份了TPM加密密钥?
是
否
S1010
否
登录用户具有管理权限?
是
显示用于备份TPM加密密钥的画面
S1011
用于备份TPM加密密钥的处理
S1012
结束

图10

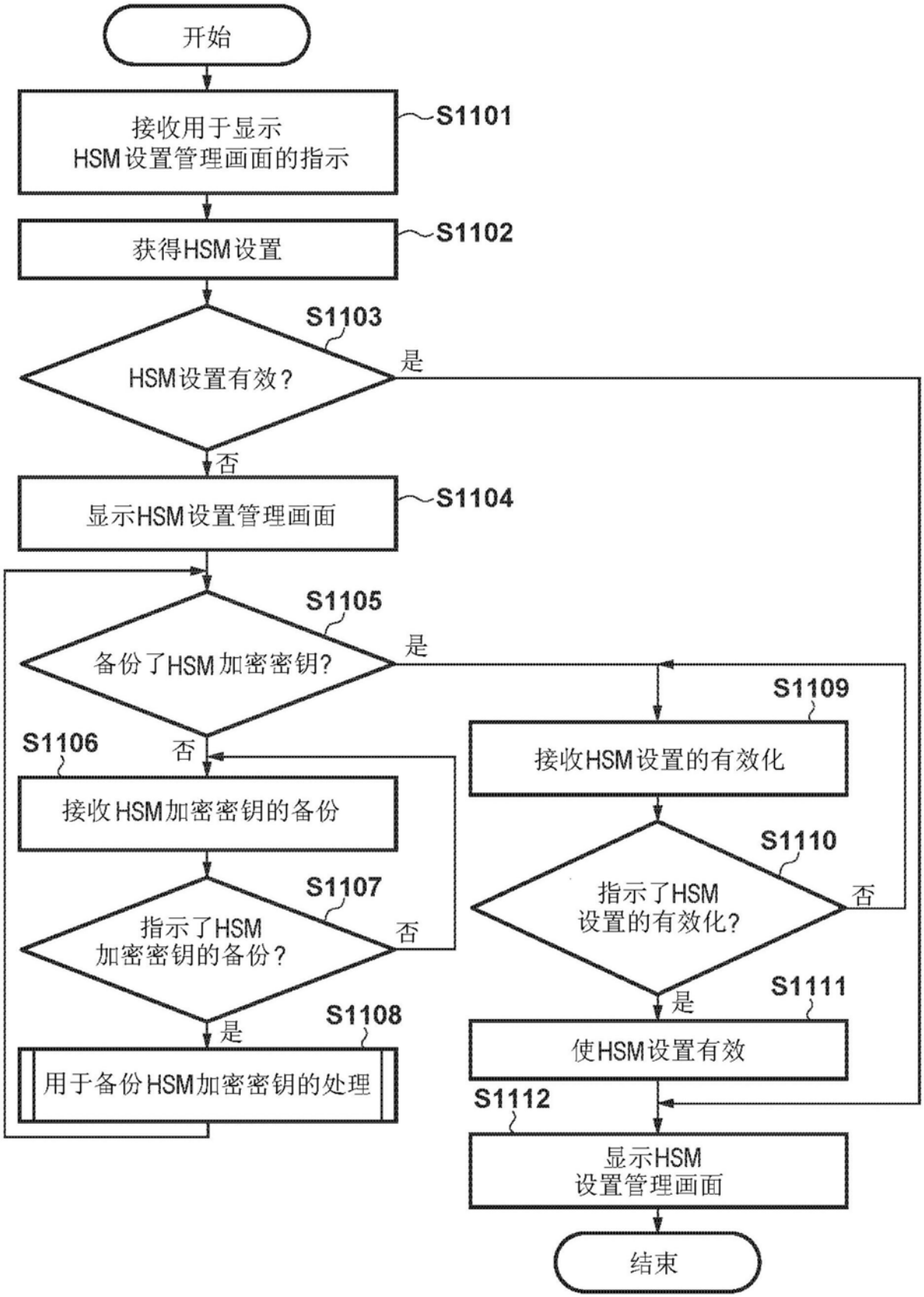

开始
接收用于显示HSM设置管理画面的指示
S1101
获得HSM设置
S1102
S1103
HSM设置有效？
是
否
显示HSM设置管理画面
S1104
S1105
备份了HSM加密密钥?
是
S1106
否
接收HSM加密密钥的备份
S1107
指示了HSM加密密钥的备份？
否
是
S1108
用于备份HSM加密密钥的处理
S1109
接收HSM设置的有效化
S1110
指示了HSM设置的有效化?
否
是
S1111
使HSM设置有效
S1112
显示HSM设置管理画面
结束

图11

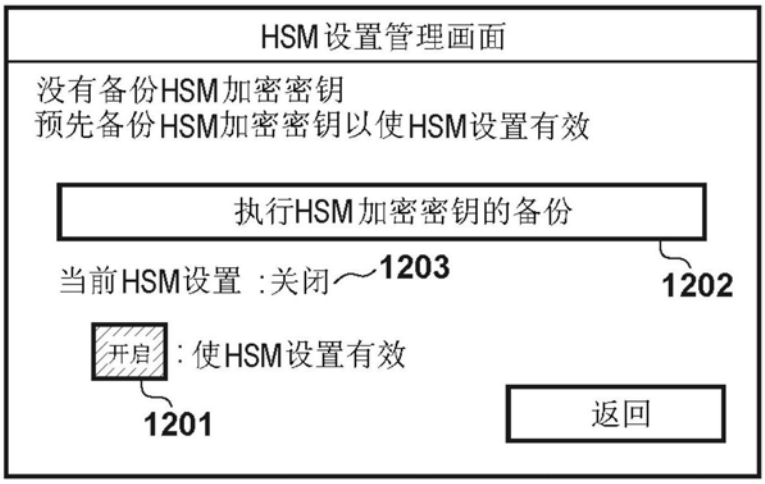

HSM设置管理画面
没有备份HSM加密密钥
预先备份HSM加密密钥以使HSM设置有效
执行HSM加密密钥的备份
1202
当前HSM设置 :关闭
1203
开启
:使HSM设置有效
1201
返回

图12A

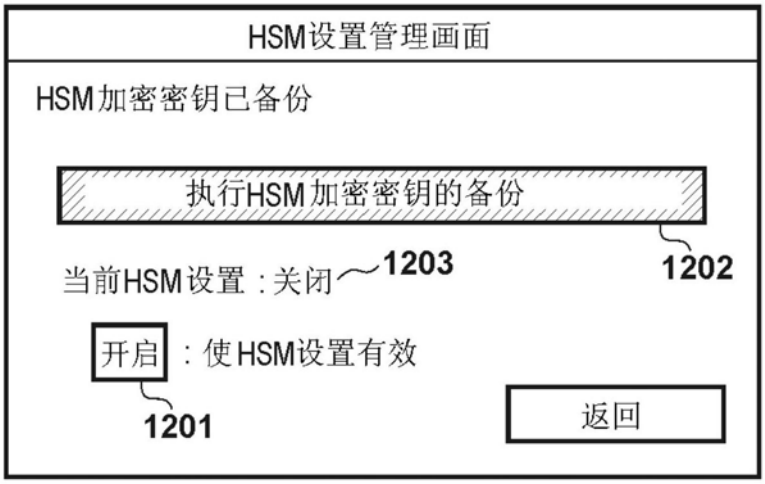

HSM设置管理画面
HSM加密密钥已备份
执行HSM加密密钥的备份
1202
当前HSM设置 :关闭
1203
开启
:使HSM设置有效
1201
返回

图12B

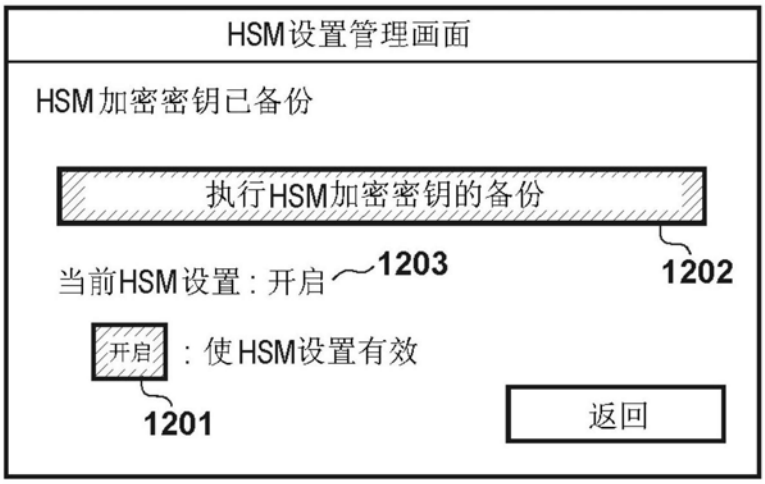

HSM设置管理画面
HSM加密密钥已备份
执行HSM加密密钥的备份
1202
当前HSM设置：开启
1203
开启
：使HSM设置有效
1201
返回

图12C