(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 101258505 B
(45)授权公告日 2011.12.14

(21)申请号 200680032530.8

(22)申请日 2006.07.26

(30)优先权数据
11/190,735 2005.07.26 US

(85)PCT申请进入国家阶段日
2008.03.05

(86)PCT申请的申请数据
PCT/US2006/029355 2006.07.26

(87)PCT申请的公布数据
WO2007/014314 EN 2007.02.01

(73)专利权人 苹果公司
地址 美国加利福尼亚

(72)发明人 C·R·温索基 A·沃德

(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 李玲

(51)Int.Cl.
G06F 21/00(2006.01)

(56)对比文件
EP 1460514 A2,2004.09.22, 说明书第[0013],[0018],[0022],[0025]-[0026],[0036],[0043]段.
说明书第[0013],[0018],[0022],[0025]-[0026],[0036],[0043]段.
CN 1512369 A,2004.07.14, 全文.
US 5974454 A,1999.10.26, 说明书第2栏第11-17行.
EP 1091285 A2,2001.04.11, 说明书第[0006],[0007],[0060]段.
EP 0778512 A2,1997.06.11, 说明书第2栏第30-42行,第6栏第22-26行,第9栏第29-35行、附图1.

审查员 崔哲

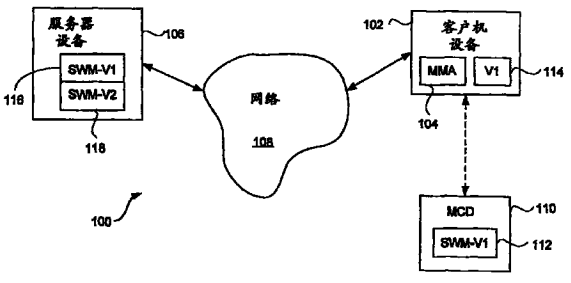
权利要求书 5 页 说明书 10 页 附图 10 页

(54)发明名称

安全的软件更新

(57)摘要

本发明涉及安全的软件更新。公开了用于更新电子设备内已在使用的软件的改进技术。在一个实施例中,软件能够使用密码术以安全和受控的方式被更新。更新软件的真伪及其对于特定电子设备的适当性能够在更新之前被确认。软件能够逐个模块地更新。在一个实施例中,服务器容纳用于不同电子设备的软件更新,并且将合适的软件更新通过数据网络提供给电子设备。



CN 101258505 B

1. 一种用于对至少部分地根据软件运行的电子设备上的软件进行升级的方法，所述方法包括以下步骤：

(a) 将设备信息发送到主机设备，其中所述设备信息包括版本指示符、密钥、以及下列各项中的一个或更多个：制造商信息、型号信息、和硬件平台信息；

(b) 在电子设备处接收加密的软件模块，其中所述加密的软件模块源自在主机设备处基于设备描述信息和当前版本指示符获得的软件模块，并且所述加密的软件模块先前在主机设备处已经利用所述电子设备提供的所述密钥被加密，专门供该电子设备使用；

(c) 在电子设备处对加密的软件模块进行解密；以及

(d) 此后将软件模块安装在电子设备上。

2. 根据权利要求 1 所述的方法，

其中所述密钥是与电子设备相关联的公钥，并且

其中所接收的加密的软件模块已经直接或间接利用所述公钥被加密。

3. 根据权利要求 2 所述的方法，其中所述解密步骤 (c) 是直接或间接利用存储在电子设备内的私有密钥进行的。

4. 根据权利要求 1 所述的方法，其中所述密钥是与电子设备相关联的公钥，并且

其中所接收的加密的软件模块已经利用随机生成的密钥被加密，并且该随机生成的密钥利用所述公钥被加密。

5. 根据权利要求 4 所述的方法，其中所述解密步骤 (c) 最初利用存储在电子设备内的私有密钥对加密的随机生成的密钥进行解密，然后利用该随机生成的密钥对加密的软件模块进行解密。

6. 根据权利要求 1 所述的方法，其中所述主机设备是服务器计算机或客户机计算机，并且

其中所述电子设备是移动电话、个人数字助理或媒体播放器。

7. 根据权利要求 1 所述的方法，其中所述方法是在没有请求软件升级的用户交互的情况下自动执行的。

8. 一种用于对便携式电子设备上的软件进行升级的方法，所述方法包括以下步骤：

发送步骤，将设备信息发送到主机设备，所述设备信息包括设备描述信息、公共密钥和当前版本指示符；

接收步骤，在便携式电子设备处接收加密的软件模块，所述加密的软件模块是由下述获得的：基于设备描述信息和当前版本指示符选择对于主机设备可用的软件模块，然后利用由便携式电子设备提供的公共密钥对其进行加密；

解密步骤，利用便携式电子设备所知的私有密钥在便携式电子设备处对加密的软件模块进行解密；

认证步骤，对解密的软件模块进行认证；以及

安装步骤，在所述解密步骤和所述认证步骤已经成功完成之后，将软件模块安装在便携式电子设备上。

9. 根据权利要求 8 所述的方法，其中所述发送步骤和所述接收步骤是在便携式电子设备可操作地连接到主机设备的时候执行的。

10. 根据权利要求 9 所述的方法，其中所述解密步骤、所述认证步骤和所述安装步骤是

在便携式电子设备已从主机设备断开连接之后执行的。

11. 根据权利要求 8 所述的方法，所述方法还包括：

识别步骤，识别便携式电子设备已从主机设备断开连接；并且

仅在所述识别步骤识别出便携式电子设备已从主机设备断开连接之后，才执行所述解密步骤。

12. 根据权利要求 8 所述的方法，其中所述方法还包括：

在所述安装步骤之后，更新当前版本指示符。

13. 根据权利要求 8 所述的方法，其中所述私有密钥对于便携式电子设备是唯一的。

14. 根据权利要求 8 所述的方法，其中对解密的软件模块进行的所述认证使用了数字签名。

15. 一种用于对便携式电子设备上的软件模块进行升级的方法，所述方法包括以下步骤：

接收步骤，在基于网络的服务器设备处接收设备信息，所述设备信息与便携式电子设备相关并且包括设备描述信息、公共密钥和便携式电子设备上的软件模块的当前版本指示符；

确定步骤，确定是否可从服务器设备得到软件模块的更新版本，所述确定步骤基于与便携式电子设备相关的设备描述信息；

加密步骤，当所述确定步骤确定出可从服务器设备得到软件模块的更新版本时，对软件模块的更新版本进行加密，所述加密步骤利用了由便携式电子设备提供的公共密钥；以及

传送步骤，将加密的软件模块传送到便携式电子设备。

16. 根据权利要求 15 所述的方法，其中所述方法还包括：

在便携式电子设备处接收加密的软件模块；

访问驻留在便携式电子设备上的私有密钥；以及

利用所述私有密钥在便携式电子设备处对加密的软件模块进行解密。

17. 根据权利要求 16 所述的方法，其中所述方法还包括：

在所述解密已经成功完成之后，将软件模块安装在电子设备上。

18. 根据权利要求 16 所述的方法，其中所述方法还包括：

对解密的软件模块进行认证；以及

在所述解密和所述认证已经成功完成之后，将软件模块安装在电子设备上。

19. 根据权利要求 15 所述的方法，

其中所述加密步骤包括：(i) 利用随机密钥对软件模块的更新版本进行加密；和 (ii) 利用公共密钥对该随机密钥进行加密，

其中所述传送步骤用来传送加密的软件模块和加密的随机密钥。

20. 根据权利要求 19 所述的方法，其中所述方法还包括：

在便携式电子设备处接收加密的软件模块和加密的随机密钥；

访问驻留在便携式电子设备上的私有密钥；

利用私有密钥对加密的随机密钥进行解密以提供所获取的随机密钥；以及

利用所获取的随机密钥在便携式电子设备处对加密的软件模块进行解密。

21. 根据权利要求 20 所述的方法，其中所述方法还包括：

在所述解密已经成功完成之后，将软件模块安装在电子设备上。

22. 一种基于网络的软件更新系统，包括：

多个移动客户机设备，每个移动客户机设备根据驻留在相应移动客户机设备上的至少一个软件模块运行；

能够访问多个软件模块的服务器设备，每个软件模块供所述多个移动客户机设备中的特定一个或多个使用；和

能够与服务器设备和移动客户机设备操作地连接的至少一个客户机设备，所述客户机设备运行用于数字媒体资源的媒体管理应用，

其中所述数字媒体资源由具有至少一个软件模块的数字权限管理库进行保护，并且

其中客户机设备在第一数据链路上与服务器设备进行交互以检索用于待被更新的移动客户机设备的更新软件模块，该更新软件模块属于数字权限管理库，所述用于待被更新的移动客户机设备的更新软件模块源自从服务器设备处基于设备描述信息和当前版本指示符获得的软件模块，并且其中此后客户机设备与移动客户机设备在第二数据链路上进行交互以将该更新软件模块提供给待被更新的移动客户机设备。

23. 根据权利要求 22 所述的基于网络的软件更新系统，

其中移动客户机设备随后用更新软件模块来替换现有的软件。

24. 一种用于对至少部分地根据软件运行的电子设备上的软件进行升级的装置，所述装置包括：

(a) 用于将设备信息发送到主机设备的器件，其中所述设备信息包括版本指示符、密钥、以及下列各项中的一个或更多个：制造商信息、型号信息、和硬件平台信息；

(b) 用于在电子设备处接收加密的软件模块的器件，其中所述加密的软件模块源自在主机设备处基于设备描述信息和当前版本指示符获得的软件模块，并且所述加密的软件模块先前在主机设备处已经利用所述电子设备提供的所述密钥被加密，专门供该电子设备使用；

(c) 用于在电子设备处对加密的软件模块进行解密的器件；以及

(d) 用于此后将软件模块安装在电子设备上的器件。

25. 根据权利要求 24 所述的装置，

其中所述密钥是与电子设备相关联的公钥，并且

其中所接收的加密的软件模块已经直接或间接利用所述公钥被加密。

26. 根据权利要求 25 所述的装置，其中所述解密是直接或间接利用存储在电子设备内的私有密钥进行的。

27. 根据权利要求 24 所述的装置，其中所述密钥是与电子设备相关联的公钥，并且

其中所接收的加密的软件模块已经利用随机生成的密钥被加密，并且该随机生成的密钥利用所述公钥被加密。

28. 根据权利要求 27 所述的装置，其中所述用于解密的器件 (c) 最初利用存储在电子设备内的私有密钥对加密的随机生成的密钥进行解密，然后利用该随机生成的密钥对加密的软件模块进行解密。

29. 根据权利要求 24 所述的装置，其中所述主机设备是服务器计算机或客户机计算

机，并且

其中所述电子设备是移动电话、个人数字助理或媒体播放器。

30. 根据权利要求 24 所述的装置，其中所述装置是在没有请求软件升级的用户交互的情况下自动执行的。

31. 一种用于对便携式电子设备上的软件进行升级的装置，所述装置包括：

发送器件，用于将设备信息发送到主机设备，所述设备信息包括设备描述信息、公共密钥和当前版本指示符；

接收器件，用于在便携式电子设备处接收加密的软件模块，所述加密的软件模块是由下述获得的：基于设备描述信息和当前版本指示符选择对于主机设备可用的软件模块，然后利用由便携式电子设备提供的公共密钥对其进行加密；

解密器件，用于利用便携式电子设备所知的私有密钥在便携式电子设备处对加密的软件模块进行解密；

认证器件，用于对解密的软件模块进行认证；以及

安装器件，用于在所述解密和所述认证已经成功完成之后，将软件模块安装在便携式电子设备上。

32. 根据权利要求 31 所述的装置，其中所述发送和所述接收是在便携式电子设备可操作地连接到主机设备的时候执行的。

33. 根据权利要求 32 所述的装置，其中所述解密、所述认证和所述安装是在便携式电子设备已从主机设备断开连接之后执行的。

34. 根据权利要求 31 所述的装置，还包括：

识别器件，用于识别便携式电子设备已从主机设备断开连接；并且

用于仅在所述识别器件识别出便携式电子设备已从主机设备断开连接之后，才执行所述解密的器件。

35. 根据权利要求 31 所述的装置，还包括：

用于在所述安装之后，更新当前版本指示符的器件。

36. 根据权利要求 31 所述的装置，其中所述私有密钥对于便携式电子设备是唯一的。

37. 根据权利要求 31 所述的装置，其中对解密的软件模块进行的所述认证使用了数字签名。

38. 一种用于对便携式电子设备上的软件模块进行升级的装置，所述装置包括：

接收器件，用于在基于网络的服务器设备处接收设备信息的器件，所述设备信息与便携式电子设备相关并且包括设备描述信息、公共密钥和便携式电子设备上的软件模块的当前版本指示符；

确定器件，用于确定是否可从服务器设备得到软件模块的更新版本，所述确定基于与便携式电子设备相关的设备描述信息；

加密器件，用于当所述确定器件确定出可从服务器设备得到软件模块的更新版本时，对软件模块的更新版本进行加密，所述加密利用了由便携式电子设备提供的公共密钥；以及

传送器件，用于将加密的软件模块传送到便携式电子设备。

39. 根据权利要求 38 所述的装置，还包括：

用于在便携式电子设备处接收加密的软件模块的器件；

用于访问驻留在便携式电子设备上的私有密钥的器件；以及

用于利用所述私有密钥在便携式电子设备处对加密的软件模块进行解密的器件。

40. 根据权利要求 39 所述的装置，还包括：

用于在所述解密已经成功完成之后，将软件模块安装在电子设备上的器件。

41. 根据权利要求 39 所述的装置，还包括：

用于对解密的软件模块进行认证的器件；以及

用于在所述解密和所述认证已经成功完成之后，将软件模块安装在电子设备上的器件。

42. 根据权利要求 38 所述的装置，

其中所述加密器件包括：(i) 用于利用随机密钥对软件模块的更新版本进行加密的器件；和 (ii) 用于利用公共密钥对该随机密钥进行加密的器件，

其中所述传送器件用来传送加密的软件模块和加密的随机密钥。

43. 根据权利要求 42 所述的装置，还包括：

用于在便携式电子设备处接收加密的软件模块和加密的随机密钥的器件；

用于访问驻留在便携式电子设备上的私有密钥的器件；

用于利用私有密钥对加密的随机密钥进行解密以提供所获取的随机密钥的器件；以及

用于利用所获取的随机密钥在便携式电子设备处对加密的软件模块进行解密的器件。

44. 根据权利要求 43 所述的装置，还包括：

用于在所述解密已经成功完成之后，将软件模块安装在电子设备上的器件。

安全的软件更新

技术领域

[0001] 本发明涉及更新软件，更具体地说，涉及使用从远程服务器获得的更新的软件来更新客户机处的软件。

背景技术

[0002] 目前，对于电子设备而言，在它们的运行中使用软件是非常普遍的。使用软件的电子设备的示例包括计算机、个人数字助理、媒体播放器和移动电话。然而，有时希望改变或更新正在由这些电子设备使用的软件。

[0003] 在计算机的情况下，更新的软件（如较新的版本）能够通过下载处理从远程服务器获得。一旦获得，所述软件能够安装到计算机上。可以通过要求用户输入字母数字密钥或注册码来控制软件的安装处理。没有正确密钥或注册码，则更新的软件无法被安装。此外，用于更新计算机上的软件的传统方法要求相当多的用户参与。对用户协助的需要是成问题的，因为用户担心下载软件并将软件安装到计算机上有可能感染目前已经存在的计算机病毒。

[0004] 在使用软件的便携式电子设备（例如个人数字助理、媒体助理、移动电话）的情况下，所述软件通常在制造过程中被初装。结果，当用户收到该便携式电子设备时，所述软件已被预安装且所述便携式电子设备是全功能的。然而，当软件需要随后进行更新或修改时，在许多情况下，安装在便携式电子设备上的软件不能够被终端用户所改变。近来，一些便携式电子设备允许更新软件。例如，便携式电子设备能够连接到计算机，该计算机能够用更新的软件完全替换便携式电子设备上的现有软件。这导致的一个复杂性是便携式电子设备通常支持多个功能。这些不同的功能能够通过由不同销售商提供的不同的软件模块控制。因此，将便携式电子设备上的所有软件完全替换通常是不合适的。结果，需要能够更新不同的软件模块而不干扰其它模块的支持软件更新技术。

[0005] 因此，需要用于更新电子设备上的软件的自动安全的解决方案。

发明内容

[0006] 本发明属于更新电子设备内已在使用的软件的改进技术。在一个实施例中，软件能够利用密码术以安全和受控的方式被更新。更新的软件的真伪及其对于特定电子设备的适当性能够在更新之前被确认。所述软件也能够逐个模块地被更新。在一个实施例中，服务器容纳用于不同电子设备的软件更新，并且将合适的软件更新通过数据网络提供给电子设备。

[0007] 尽管本发明一般适用于很多种类型的更新软件，但是本发明尤其适于更新数字权限管理 (DRM) 软件。出于安全原因，可能需要更新电子设备中在使用的 DRM 软件。本发明的改进技术使得 DRM 软件能够以安全和受控的方式被更新。在一个实施方式中，对 DRM 软件的更新用来修改设置在电子设备上的 DRM 软件库。

[0008] 本发明适用于至少部分地根据软件运行的电子设备。例如，所述电子设备可以为

计算机、个人数字助理、媒体播放器或移动电话。

[0009] 本发明能够以多种方式实现，包括方法、系统、设备、装置或计算机可读介质。在下面论述本发明的几个实施例。

[0010] 作为一种用于对至少部分地根据软件运行的电子设备上的软件进行升级的方法，本发明的一个实施例至少包括以下步骤：将设备信息发送到主机设备；在电子设备处接收加密的软件模块，所述加密的软件模块先前在主机设备处被加密，专门供该电子设备使用；在电子设备处对加密的软件模块进行解密；以及此后将软件模块安装在电子设备上。

[0011] 作为一种用于对便携式电子设备上的软件进行升级的方法，本发明的一个实施例至少包括以下步骤：发送步骤，将设备信息发送到主机设备，所述设备信息包括设备描述信息、公共密钥和当前版本指示符；接收步骤，在便携式电子设备处接收加密的软件模块，所述加密的软件模块是如下获得的，即基于设备描述信息和当前版本指示选择对于主机设备可用的软件模块，然后利用由便携式电子设备提供的公共密钥对其进行加密；解密步骤，利用便携式电子设备所知的私有密钥在便携式电子设备处对加密的软件模块进行解密；认证步骤，对解密的软件模块进行认证；以及安装步骤，在所述解密步骤和认证步骤已经成功完成之后，将软件模块安装在便携式电子设备上。

[0012] 作为一种至少包括用于升级计算设备上的软件的计算机程序代码的计算机可读介质，本发明的一个实施例至少包括：用于将设备信息发送到主机设备的计算机程序代码，所述设备信息包括设备描述信息、第一密钥和当前版本指示符；用于在计算设备处接收加密的软件模块的计算机程序代码，所述加密的软件模块是如下获得的：基于设备描述信息和当前版本指示符选择对于主机设备可用的软件模块，然后利用由计算设备提供的第一密钥对其进行加密；用于利用计算设备所知的第二密钥在计算设备处对加密的软件模块进行解密的计算机程序代码；用于对解密的软件模块进行认证的计算机程序代码；和用于在所述解密和所述认证已经成功完成后将软件模块安装在计算设备上的计算机程序代码。

[0013] 作为一种用于对便携式电子设备上的软件模块进行升级的方法，本发明的另一个实施例至少包括以下步骤：接收步骤，在基于网络的服务器设备处接收设备信息，所述设备信息与便携式电子设备相关并且包括设备描述信息、公共密钥和便携式电子设备上的软件模块的当前版本指示符；确定步骤，确定是否可从服务器设备得到软件模块的更新版本，所述确定步骤基于与便携式电子设备相关的设备描述信息；加密步骤，当所述确定步骤确定出可从服务器设备得到软件模块的更新版本时，对软件模块的更新版本进行加密，所述加密步骤利用了由便携式电子设备提供的公共密钥；以及发送步骤，将加密的软件模块发送到便携式电子设备。

[0014] 作为一种至少包括用于升级计算设备上的软件模块的计算机程序代码的计算机可读介质，本发明的另一个实施例至少包括：用于在基于网络的服务器设备处接收设备信息的计算机程序代码，所述设备信息与计算设备相关并且包括设备描述信息、密钥和计算设备上的软件模块的当前版本指示符；用于确定是否可从服务器设备得到软件模块的更新版本的计算机程序代码，所述确定基于与计算设备相关的设备描述信息；用于当所述确定确定出可从服务器设备得到软件模块的更新版本时对软件模块的更新版本进行加密的计算机程序代码，所述加密使用了由计算设备提供的密钥；和用于将加密的软件模块发送到计算设备的计算机程序代码。

[0015] 作为一种至少包括用于升级电子设备上的软件的计算机程序代码的计算机可读介质，本发明的一个实施例至少包括：用于在主机设备处识别用于电子设备的更新软件模块的计算机程序代码；用于对用在电子设备上的更新软件模块进行加密的计算机程序代码；用于将加密的软件模块发送到电子设备的计算机程序代码；用于在电子设备处对加密的软件模块进行解密的计算机程序代码；和用于将软件模块安装在电子设备上的计算机程序代码。

[0016] 作为一种基于网络的软件更新系统，本发明的一个实施例至少包括：(i) 多个移动客户机设备，每个移动客户机设备根据驻留在相应移动客户机设备上的至少一个软件模块运行；(ii) 可访问多个软件模块的服务器设备，每个软件模块供所述多个移动客户机设备中的特定一个或多个使用；和 (iii) 可与服务器设备和移动客户机设备可操作地连接的至少一个客户机设备，所述客户机设备运行用于数字媒体资源的媒体管理应用。所述数字媒体资源由具有至少一个软件模块的数字权限管理库进行保护。客户机设备在第一数据链路上与服务器设备进行交互以检索用于待更新的移动客户机设备的更新软件模块，该更新软件模块属于数字权限管理库。此后客户机设备与移动客户机设备在第二数据链路上进行交互以将该更新软件模块提供给待更新的移动客户机设备。

[0017] 本发明的其它方面和优点根据下面结合附图的详细的描述而变得明显，所述附图通过示例说明本发明的原理。

附图说明

[0018] 通过下面结合附图进行的详细描述，本发明将变得容易理解，在附图中相似的标号表示相似的构成元件，并且在附图中：

[0019] 图 1A 是根据本发明一个实施例的软件更新系统的框图。

[0020] 图 1B 是在已发生软件更新之后的软件更新系统的框图。

[0021] 图 2 是根据本发明一个实施例的服务器软件更新处理的流程图。

[0022] 图 3 是根据本发明一个实施例的客户机软件更新处理的流程图。

[0023] 图 4A 和 4B 是根据本发明一个实施例的客户机软件更新处理的流程图。

[0024] 图 5A 和 5B 是根据本发明一个实施例的服务器软件更新处理的流程图。

[0025] 图 6 是根据本发明的一个实施例的移动客户机连接处理的流程图。

[0026] 图 7A 和 7B 是根据本发明一个实施例的移动客户机断开连接处理的流程图。

具体实施方式

[0027] 本发明属于更新电子设备中已在使用的软件的改进技术。在一个实施例中，能够利用密码术以安全和受控的方式来更新软件。更新软件的真伪及其针对特定电子设备的适当性能够在更新之前被确认。也可以逐个模块地更新软件。在一个实施例中，服务器容纳用于各种电子设备的软件更新，并且通过数据网络将合适的软件更新提供给电子设备。

[0028] 尽管本发明一般适用于很多种类型的更新软件，但是本发明尤其适于更新数字权限管理 (DRM) 软件。出于安全原因，可能需要更新电子设备中在使用的 DRM 软件。本发明的改进技术使得 DRM 软件能够以安全和受控的方式被更新。在一个实施方式中，对 DRM 软件的更新用来修改设置在电子设备上的 DRM 软件库。

[0029] 本发明适用于至少部分地根据软件运行的电子设备。例如，所述电子设备可以为计算机、个人数字助理、媒体播放器或移动电话。

[0030] 下面参考图 1A-7B 讨论本发明的实施例。然而，本领域技术人员能够容易地理解，这里参考这些附图而给出的详细描述旨在用于解释的目的，而本发明的范围超出这些有限的实施例。

[0031] 图 1A 是根据本发明一个实施例的软件更新系统 100 的框图。软件更新系统 100 包括客户机设备 102，客户机设备 102 包括媒体管理应用 (MMA)104。客户机设备 102 例如为计算机，如桌上型计算机。媒体管理应用 104 是用来管理在客户机设备 102 处可得到的媒体资源的应用程序。软件更新系统 100 还包括服务器设备 106，服务器设备 106 能够通过网络 108 连接到客户机设备 102。网络 108 可以是数据网络。网络 108 可包括全球网、广域网或局域网的至少一部分。网络 108 也可以是有线的和 / 或无线的。

[0032] 此外，软件更新系统 100 包括移动客户机设备 (MCD)110。MCD 110 能够通过有线或无线手段可操作地连接到客户机设备 102。在一个示例中，MCD 110 能够通过如 USB 电缆的外围总线电缆而连接到客户机设备 102。在另一个示例中，MCD 110 能够通过无线网络 (例如，蓝牙、WiFi、WiMax) 上的无线链路而连接到客户机设备 102。

[0033] 根据本发明，客户机设备 102 能够帮助更新存在于 MCD 110 上的软件模块。在这样做时，客户机设备 102 与服务器设备 106 通信。服务器设备 106 可访问可供分配给适当的移动客户机设备的多个软件模块。更具体而言，客户机设备 102 与 MCD 110 进行交互以识别安装在 MCD 110 上的软件模块 112，也就是软件模块 - 版本 1(SWM-V1)。然后客户机设备 102 存储与所识别的软件模块 112 相关联的版本指示 114。在图 1A 示出的示例中，版本指示 114 指示 MCD110 上安装的软件模块是版本 1(V1)。然后客户机设备 102 能够通过网络 108 与服务器设备 106 通信，以确定是否存在用在 MCD 110 上的软件模块的较新或更新版本。在此示例中，服务器设备 106 包括软件模块 116 和 118，其中软件模块 116 为版本 1(SWM-V1) 并且软件模块 118 为版本 2(SWM-V2)。在此示例中，软件模块 116 和 118 都被假定为适于用在 MCD 110 上。然后服务器 106 能够将更新的软件模块 118(即版本 2(SWM-V2)) 提供给客户机设备 102。然后，客户机设备 102 能够将软件模块 - 版本 2(SWM-V2) 转发到 MCD 110。

[0034] 尽管图 1A 中示出的软件更新系统 100 例示了单个客户机设备和单个 MCD，但是应该理解，软件更新系统 100 通常使单个服务器能够通过多个客户机设备来支持更新多个 MCD 上的软件模块。此外，尽管图 1A 中示出的软件更新系统 100 利用一个或更多个客户机设备，但是在另一个实施例中，软件更新系统在执行软件更新时不需要使用任何客户机设备。在这种情况下，MCD 能够连接到网络 108 且直接与服务器设备 106 通信。

[0035] 图 1B 是已发生软件更新后的软件更新系统 100’ 的框图。软件更新系统 100’ 代表 MCD 110 处的软件模块已经被更新后的软件更新系统 100。要注意，在图 1B 中，MCD 110 包括属于软件模块 - 版本 2(SWM-V2) 的软件模块 112’，且客户机设备 102 处的版本指示符 114’ 指示 MCD 110 现在使用版本 2(SWM-V2)。

[0036] 在一个实施例中，软件可属于数字权限管理 (DRM) 软件模块。软件模块也可属于软件库。作为示例，正被更新的软件模块可被称为 DRM 库。

[0037] 媒体管理应用的一个示例是由美国加利福尼亚州库珀蒂诺市的苹果计算机公司生产的 iTunes ® 应用。服务器设备的一个示例是同样由美国加利福尼亚州库珀蒂诺市的

苹果计算机公司提供的 iTunes® Music Store 服务器。

[0038] 图 2 是根据本发明一个实施例的服务器软件更新处理 200 的流程图。例如，由服务器执行服务器软件更新处理 200。服务器属于连接到客户机或在客户机上运行的软件程序的计算设备。服务器能够直接或通过网络连接到客户机。例如，服务器可属于图 1A 中示出的客户机设备 102 或服务器设备 106。

[0039] 服务器软件更新处理 200 最初从判定 202 开始，判定 202 确定是否要执行软件更新。当判定 202 确定软件更新将不被执行时，服务器软件更新处理 200 等待直到要进行软件更新。软件更新可自动执行或应用户的请求而执行。在任何情况下，当判定 202 确定需要软件更新时，对用于客户机的软件模块 (SWM) 进行识别 204。在软件模块已经被识别 204 之后，软件模块被加密 206 以供客户机访问。需要注意的是，被识别 204 的软件模块是为客户机专门设计的，且软件模块的加密是要限制客户机对它的使用。此后，加密的软件模块被发送到客户机 (208)。在操作 208 之后，服务器软件更新处理 200 结束。

[0040] 图 3 是根据本发明一个实施例的客户机软件更新处理 300 的流程图。例如，由根据本发明一个实施例运行的客户机来执行客户机软件更新处理 300。作为示例，客户机通常是使用软件的电子设备或在其上运行的软件程序。例如，客户机可属于图 1A 示出的移动客户机设备 110。

[0041] 客户机软件更新处理 300 从判定 302 开始，判定 302 确定软件模块是否要被安装到客户机上。当判定 302 确定软件模块将不被安装时，客户机软件更新处理 300 等待将软件模块安装到客户机上的需要。换言之，可以认为每当软件模块要被安装到客户机上时就调用客户机软件更新处理 300。一旦判定 302 确定要安装软件模块，加密的软件模块在客户机处被解密 304。在解密 304 之后，将软件模块安装 306 到客户机上。在软件模块已经安装 306 到客户机上之后，客户机软件更新处理 300 结束。

[0042] 图 4A 和 4B 是根据本发明一个实施例的客户机软件更新处理 400 的流程图。例如，由根据本发明一个实施例运行的客户机执行客户机软件更新处理 400。作为示例，参考图 1A，所述客户机可属于客户机设备 102 或在其上运行的媒体管理应用 104。

[0043] 客户机软件更新处理 400 从判定 402 开始，判定 402 确定媒体管理应用是否已启动。当判定 402 确定媒体管理应用尚未启动时，客户机软件更新处理 400 等待这样的事件。另一方面，一旦判定 402 确定媒体管理应用已启动，判定 404 就检查可用软件模块。这里，可用软件模块通常是适于用在对应的移动客户机设备 (MCD) 上的软件模块的较新版本。客户机软件更新处理 400 不需要在每次被启动时都检查可用软件模块，作为替代，这能够定期地（例如每周）进行。

[0044] 当判定 404 确定要进行对可用软件模块的检查时，向服务器发送 406 版本请求。该版本请求至少包括当前版本标识符和 MCD 描述信息。MCD 描述信息是描述 MCD 的一般特性、特征或属性的信息。

[0045] 接下来，判定 408 确定是否已经从服务器接收到版本响应。当判定 408 确定尚未接收到版本响应时，客户机软件更新处理 400 会等待这样的响应。然而，等待时段可以是有限的或在单独的无阻塞线程中处理。在任何情况下，一旦判定 408 确定已经接收到版本响应，将可用版本指示存储 410 在客户机中。版本响应将可用版本指示提供给客户机。在一个实施例中，可用版本指示可指示是否可从服务器得到用于 MCD 的更新的软件模块。

[0046] 在这点上，客户机软件更新处理 400 有效地等待直到 MCD 与客户机连接。虽然这在其它实施例中不是必须的，但所述连接能够允许 MCD 完成客户机软件更新处理 400 的平衡。在等待断开连接的时候，MCD 可执行与软件更新无关的其它操作。

[0047] 更具体而言，如图 4A 和 4B 所示，在框 410 之后或在没有发现可用软件模块时的判定 404 之后，判定 412 确定 MCD 是否与客户机连接。通常，判定 412 将涉及 MCD 近来是否已经被连接到客户机。当判定 412 确定到 MCD 没有被连接时，客户机可选地可执行其它处理 414。这样的其它处理 414 通常与对软件模块进行升级无关。然后判定 416 确定客户机软件更新处理 400 是否应当关闭。当判定 416 确定客户机软件更新处理 400 应当被关闭时，客户机软件更新处理 400 结束。另选地，当判定 416 确定不应关闭客户机软件更新处理 400 时，客户机软件更新处理 400 返回以重复判定 412，从而等待 MCD 被连接到客户机。

[0048] 一旦判定 412 确定 MCD 与客户机连接，判定 418 确定是否存在可用版本指示。可以回想到，可用版本指示先前基于设置在来自服务器的版本响应内的信息而被存储 410 在客户机中。当判定 418 确定存在可用版本指示时，针对用于 MCD 的可用软件模块的软件模块请求被发送 420。这里，软件模块请求被发送 420 到服务器并且请求向客户机提供可用软件版本模块。软件模块请求可包括用于期望的可用软件模块的版本标识符和用于加密可用软件模块的加密密钥，即公共加密密钥。接下来，判定 422 确定是否已经从服务器接收到软件模块响应。当判定 422 确定尚未接收到软件模块响应时，客户机软件更新处理 400 会等待这样的响应。一旦判定 422 确定已经接收到软件模块响应，可将由软件模块响应提供的加密的软件模块复制 424 到 MCD。在操作 424 之后或在确定不存在可用版本指示时的判定 418 之后，客户机软件更新处理 400 完成并结束。

[0049] 图 5A 和 5B 是根据本发明一个实施例的服务器软件更新处理 500 的流程图。例如，由根据本发明的一个实施例运行的服务器执行服务器软件更新处理 500。作为示例，参考图 1A，该服务器可属于服务器设备 106 或在其上运行的软件应用。

[0050] 通常，服务器能够执行多个不同的处理。服务器软件更新处理 500 被认为是能够由服务器执行的一个这样的处理。因此，图 5A 和 5B 中讨论的处理是针对用于客户机设备（例如移动客户机设备）的软件更新的处理，且这种处理可以与在服务器上执行的其它处理相交织。

[0051] 服务器软件更新处理 500 从判定 502 开始，判定 502 确定是否已经接收到版本请求。当判定 502 确定已经接收到版本请求时，基于 MCD 描述信息来确定 504 用于 MCD 的软件模块的最新版本。这里，已经从客户机接收的版本请求包括 MCD 上的软件模块的当前版本的指示和 MCD 描述信息。MCD 描述信息是描述 MCD 的一般特性、特征或属性的信息。

[0052] 接下来，判定 506 确定 MCD 上的软件模块的当前版本是否与可从服务器得到的最新版本相同。当判定 506 确定 MCD 上的软件模块的当前版本与可从服务器得到的最新版本相同时，向客户机发送 508 指示不存在用于 MCD 的软件模块的可用版本的版本响应。换言之，在此条件下，不需要更新 MCD 上的软件模块。另一方面，当判定 506 确定 MCD 上的软件模块的当前版本与可从服务器得到的最新版本不同时，向客户机发送 510 指示存在用于 MCD 的软件模块的可用版本的版本响应。

[0053] 在框 508 和 510 之后以及在尚未接收到版本请求时的判定 502 之后，当已接收到软件模块请求时，可通过服务器软件更新处理 500 执行另外的处理。具体地说，当判定 512

确定已接收到软件模块请求时，用于 MCD 的软件模块的最新版本被检索 514。这里，从服务器检索 514 用于 MCD 的软件模块的最新版本。换言之，服务器集中地使用于各种 MCD 的软件模块的各种版本可用。

[0054] 接下来，利用用于 MCD 的公钥对检索到的软件模块进行加密 516。这里，软件模块请求提供了在（直接或间接地）加密检索到的软件模块时要使用的公钥。公钥是与 MCD 特定相关的密钥对的一部分。在一个实施例中，密钥对存储在 MCD 上。在检索到的软件模块被加密 516 之后，向客户机发送 518 软件模块响应。软件模块响应至少包括用于 MCD 的加密的软件模块。

[0055] 此后，可以在服务器任选地执行其它处理 520。在此后的某时刻，判定 522 确定服务器软件更新处理 500 是否应当关闭。当判定 522 确定服务器软件更新处理 500 不应当关闭时，服务器软件更新处理 500 返回到其开始。另选地，当判定 522 确定服务器软件更新处理 500 应当关闭时，服务器软件更新处理 500 结束。

[0056] 通常，客户机或服务器可被视为主机设备。在图 4A 和图 5A 中，客户机与服务器进行交互以确定是否存在 SWM 的更新版本。在此实施例中，服务器确定 SWM 的更新版本是否存在，且如果存在的话则向客户机通知该更新版本。此后，在合适的时间，客户机将检索用于 MCD 的 SWM 的更新版本。

[0057] 然而，在另一个实施例中，客户机可确定 SWM 的更新版本是否存在。此实施例将代表与图 4A 和图 4B 中的实施例不同的实施例。在这种实施例中，客户机能够定期地向服务器查询多个不同设备的最新版本的表（或列表）。然后客户机存储所述表（所述表可包括代表不同设备的最新版本的版本号）。此后，当 MCD 与客户机相连时，客户机得到 MCD 描述信息（包括 MCD 上的当前版本）并且将其与存储的表中指示的可用于该设备的最新版本进行比较。如果存在可用软件版本，则客户机（例如，利用版本号）向服务器请求合适的软件更新。一旦接收到合适的软件更新，可将可用软件模块提供给 MCD。

[0058] 图 6 是根据本发明一个实施例的移动客户机连接处理 600 的流程图。例如，由根据本发明一个实施例运行的便携式客户机执行移动客户机连接处理 600。例如，便携式客户机可以是移动客户机设备 (MCD)。作为示例，参考图 1A，MCD 可属于移动客户机设备 110 或在其上运行的软件应用。

[0059] 移动客户机连接处理 600 从判定 602 开始，判定 602 确定 MCD 是否连接到客户机。当判定 602 确定 MCD 没有通过有线或无线手段连接到客户机时，移动客户机连接处理 600 等待这样的连接。换言之，移动客户机连接处理 600 可被认为一旦在 MCD 和客户机之间建立了连接就被调用。在任何情况下，一旦判定 602 确定在 MCD 和客户机之间存在连接，那么就将 MCD 描述信息和当前版本标识符提供 604 给客户机。这里，MCD 描述信息以及当前版本标识符是由 MCD 维护的。然后，可在 MCD 处执行其它处理 606。所述其它处理 606 通常不是移动客户机连接处理 600 的一部分，但是示出在图 6 中用于表明上下文关系。作为示例，能够被执行的一种类型的其它处理 606 是 MCD 和客户机之间的同步操作，例如使音乐库、日历等同步。关于数字资源或数据的同步的附加细节可在 2002 年 10 月 21 日提交的、名称为“INTELLIGENT INTERACTION BETWEEN MEDIA PLAYERAND HOST COMPUTER”的美国专利申请 No. 10/277418 中找到，该专利申请的内容在此通过引用并入。

[0060] 在 MCD 连接到客户机时的某时刻，将执行软件更新。以安全的方式执行软件更新。

因此，根据移动客户机连接处理 600，MCD 将从客户机接收加密的软件模块。移动客户机连接处理 600 包括判定 608，判定 608 确定是否已经接收到加密的软件模块。当判定 608 确定已经在 MCD 接收到加密的软件模块时，加密的软件模块被存储 610 在 MCD 的存储器内。存储器可具有许多不同类型，包括闪速存储器、盘驱动存储器等。在框 610 之后或在没有接收到加密软件模块时的判定 608 之后，移动客户机连接处理 600 结束。

[0061] 图 7A 和 7B 是根据本发明一个实施例的移动客户机断开连接处理 700 的流程图。例如由根据本发明一个实施例运行的便携式客户机执行移动客户机断开连接处理 700。例如，便携式客户机可以是移动客户机设备 (MCD)。作为示例，参考图 1A，MCD 可属于移动客户机设备 110 或在其上执行的软件应用。

[0062] 移动客户机断开连接处理 700 从判定 702 开始，判定 702 确定 MCD 是否已经从客户机断开连接。当判定 702 确定 MCD 尚未从客户机断开连接时，移动客户机断开连接处理 700 等待这样的断开连接。换言之，一旦 MCD 从客户机断开连接，移动客户机断开连接处理 700 就开始。因此，当判定 702 确定 MCD 已经从客户机断开连接时，判定 704 确定在 MCD 是否存在加密的软件模块。这里，如图 6 中的框 610 所示，移动客户机连接处理 600 进行操作以将合适的加密的软件模块存储到 MCD 上。这里，在判定 704 处，进行加密的软件模块是否已经存储在 MCD 上的确定。

[0063] 当判定 704 确定加密的软件模块已经存储在 MCD 上时，利用设置在 MCD 内的私钥来解密 706 加密的软件模块。这里，如上所述，MCD 包括一对密钥。这些密钥包括上述公钥以及一私钥。加密软件模块的解密是利用所需的私钥执行的。因此，仅当加密的软件模块是为用在该 MCD 上而被加密的时候，该加密的软件模块才能够被正确地解密。换言之，软件模块的加密是利用公钥执行的，所述公钥是存储在 MCD 内的私钥的对应物。

[0064] 假定解密 706 成功，则可对软件模块进行验证 700。在一个实施例中，可利用数字签名来验证 700 软件模块。通过对数字签名的验证，建立软件模块的有效性。例如，MCD 的制造商能够在软件模块被允许用在 MCD 上之前确保软件模块是可信的（即，得到制造商的批准）。然后判定 710 确定软件模块是否有效。这里，要想是有效的，软件模块必须不仅被正确地解密而且还要被成功地认证。

[0065] 当判定 710 确定软件模块有效时，判定 712 确定软件模块是否适于 MCD。这里，当软件模块与 MCD 紧密联系时，软件模块可被确定为适于该 MCD。当软件模块适于与 MCD 一起使用时，软件模块可正确地紧密联系。例如，判定 702 可确定软件模块是否适于用在 MCD 的该型号和 / 或硬件平台上。作为一具体示例，软件模块可包括一个或更多个用于 MCD 的型号和 / 或硬件平台的标识符，且这些标识符能够与存储在 MCD 中的类似标识符相比较。

[0066] 当判定 712 确定软件模块适于 MCD 时，可将软件模块安装 714 到 MCD 上。接下来，判定 716 确定软件模块的安装是否成功。当判定 716 确定安装尚未成功时，安装 714 可被重复。然而，如果软件模块的安装反复失败，则移动客户机断开连接处理 700 会在没有安装软件模块的情况下结束。另一方面，当判定 716 确定软件模块已经成功安装到 MCD 上时，未安装的软件模块可被删除 718。这里，未安装的软件模块被存储在 MCD 的存储器内（例如，图 6 中的框 610）；因此，将未安装的软件模块删除 718 是出于安全原因以及为了释放 MCD 的存储器。另外，MCD 的当前版本指示符被更新 720。当前版本指示符的更新 720 是适当的，因为 MCD 上的软件模块已经被更新并且由此现在是当前版本的软件模块。存储的当前版本指

示符也有助于将当前版本信息提供到客户机，如上所述（例如图 6 中的框 604）。在框 720 之后以及在估计的条件不存在时的判定 704、710 和 712 中任一个之后，移动客户机断开连接处理 700 完成并结束。

[0067] 关于认证，销售商可使用例如通过数字签名对软件模块进行的认证（如上所述）。例如，可针对第一销售商实现更新的软件模块，但是第二销售商可能要求软件模块在被安装到或以其它方式提供给电子设备之前得到他们的批准。例如，如果第一销售商是软件供应商而第二销售商是硬件平台供应商，那么第一销售商可将更新的软件模块以安全的方式提供给电子设备，但是第二销售商可能要求软件模块在安装到电子设备之前要进行认证或验证。另外，除了第一销售商提供的任何加密之外，第二销售商可能提供其自己的密码等级。因此，在一个实施方式中，在客户机可得到软件模块之前，可将第一销售商的软件模块打包成带有第二销售商的数字签名和 / 或加密。

[0068] 如上所述，密钥能够用于确保和控制软件更新处理。为了附加的安全或性能的原因，可使用密钥的组合。结果，就使用公钥而言，公钥不需要用来直接加密软件模块。在一个实施例中，加密处理如下进行。首先，生成一随机密钥（随机钥）。作为示例，随机密钥可以是 128 位 AES 密钥，其是随机对称密钥。首先使用随机密钥来加密软件模块。这产生加密的软件模块。另外，利用有电子设备提供的公钥来加密随机密钥。这产生加密的密钥。在一个示例中，加密的密钥是 1024 位 RSA 密钥。在此实施例中，电子设备（例如 MCD）接收第一电子文件内的加密的软件模块，并且接收第二电子文件内的加密的密钥。此后，为了将软件模块安装到电子设备上，利用驻留在电子设备内的私钥来解密第二电子文件内的加密的密钥。得到的密钥是所述随机密钥，该随机密钥然后可用于解密第一电子文件内的加密的软件模块。然后，软件模块是“明文的”（即未加密的），并且可被安装到电子设备上。

[0069] 根据本发明的软件模块更新能够以自动的方式提供。即，当客户机可操作地连接到服务器时，服务器能够在没有客户机用户参与的情况下向客户机提供任何更新的软件模块。另选地，在另一个实施例中，可在客户机（例如便携式电子设备）处向用户提示允许安装更新的软件模块。

[0070] 本发明的不同方面、实施例、实施方式或特征能够单独使用或者任意组合地使用。

[0071] 本发明优选由软件实现，但是也能够以硬件或硬件和软件的组合实现。本发明也能够被实施为计算机可读介质上的计算机可读代码。计算机可读介质是能够存储之后可由计算机系统读取的数据的任何数据存储设备。计算机可读介质的示例包括：只读存储器、随机存取存储器、CD-ROM、DVD、磁带、光学数据存储设备和载波。计算机可读介质也可分布在网络连接的计算机系统上，从而以分布式方式存储和执行计算机可读代码。

[0072] 本发明的优点众多。不同的方面、实施例或实施方式可以产生以下优点中的一个或多个优点。本发明的一个优点是：能够以安全的方式通过网络执行软件更新。软件更新的安全性质防止了软件的反向工程。例如，所加入的安全性确保了在软件正被传送到电子设备时防止对软件的未授权拦截和检查。本发明的另一个优点是电子设备使用的软件能够逐个模块地被更新，这在电子设备使用来自于不同销售商的软件或硬件的情况下特别有用。本发明的又一个优点是软件更新能够以自动的方式执行，且由此电子设备的用户无需承担软件更新的负担。

[0073] 根据书面的说明书，本发明的许多特征和优点变得明显。此外，由于本领域技术

人员可以容易地想到许多修改和变化，因此本发明不应限于所例示和描述的确切构造和操作。因此，所有合适的修改和等同物都可被视为落在本发明的范围内。

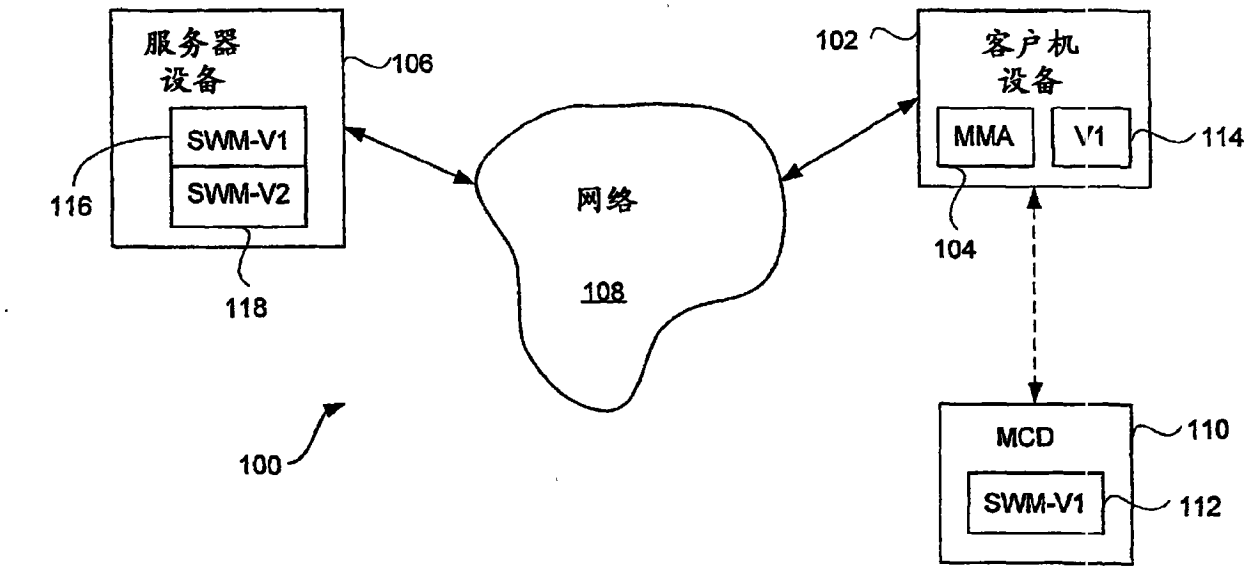

服务器
设备
106
SWM-V1
SWM-V2
116
118
网络
108
102
客户机
设备
MMA
V1
114
104
MCD
110
SWM-V1
112
100

图1A

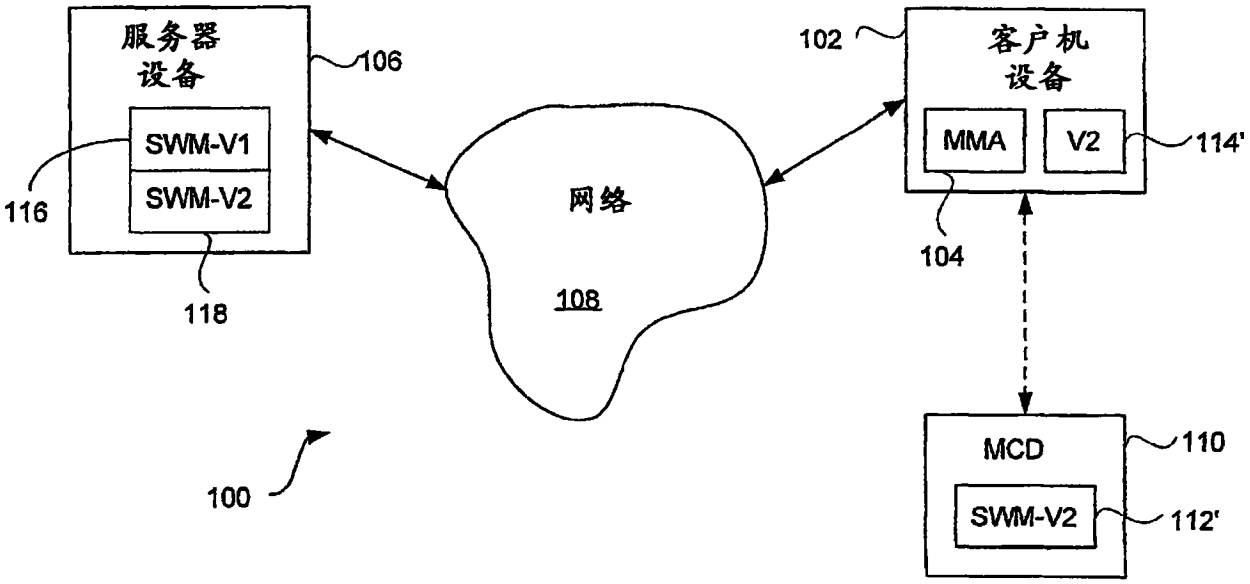

服务器
设备
106
SWM-V1
SWM-V2
116
118
网络
108
102
客户机
设备
MMA
V2
114'
104
MCD
110
SWM-V2
112'
100

图1B

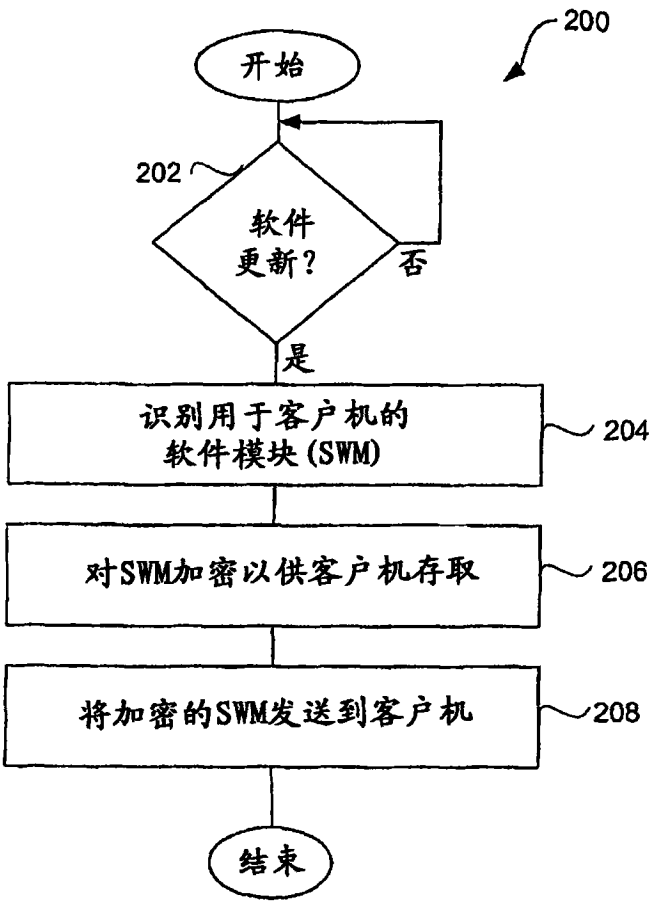

200
开始
202
软件
更新?
否
是
识别用于客户机的
软件模块(SWM)
204
对SWM加密以供客户机存取
206
将加密的SWM发送到客户机
208
结束

图2

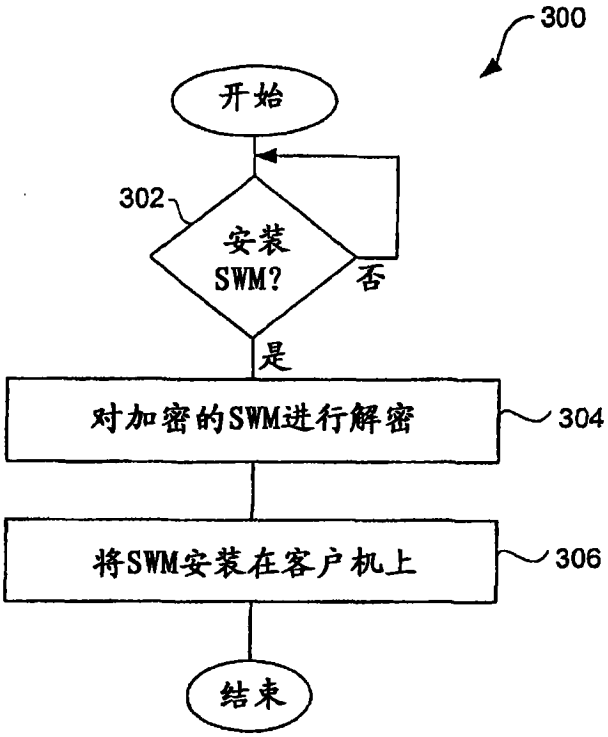


图 3

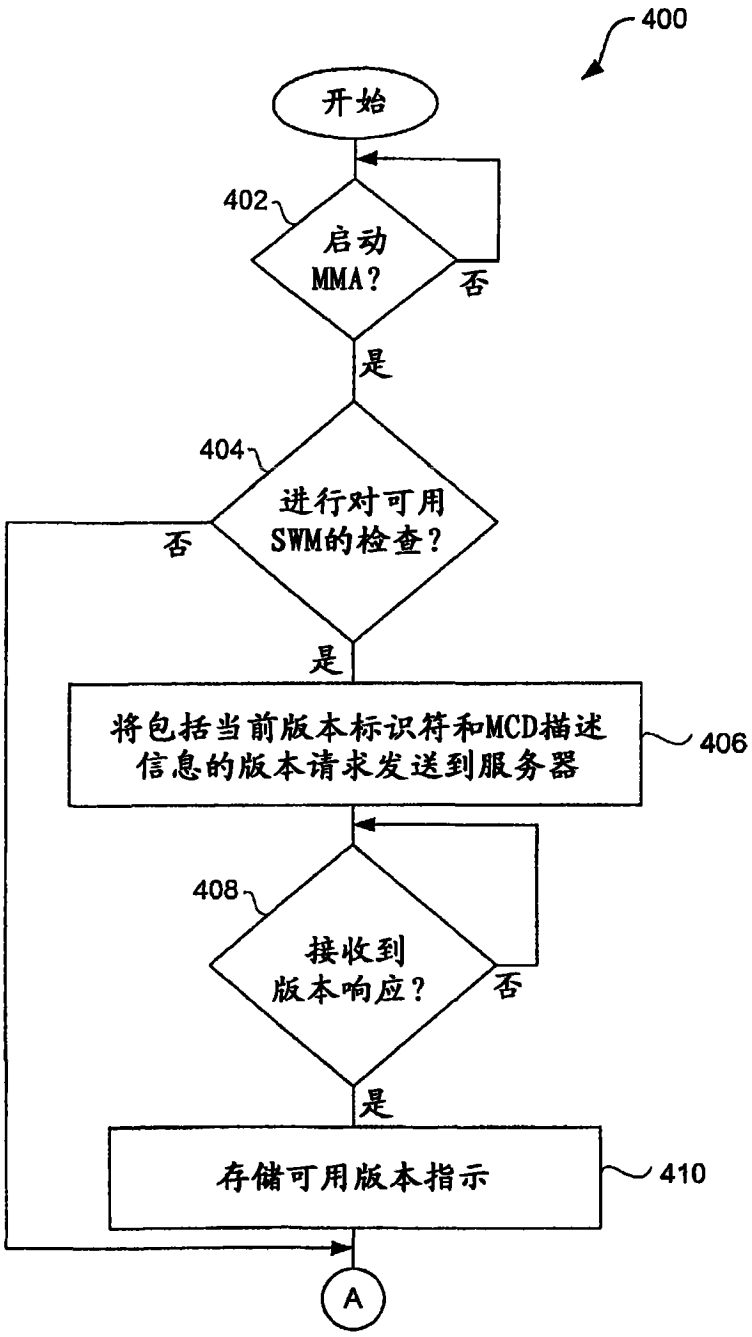

400
开始
402
启动 MMA?
否
是
404
进行对可用 SWM的检查?
否
是
将包括当前版本标识符和MCD描述信息的版本请求发送到服务器
406
408
接收到 版本响应?
否
是
存储可用版本指示
410
A

图4A

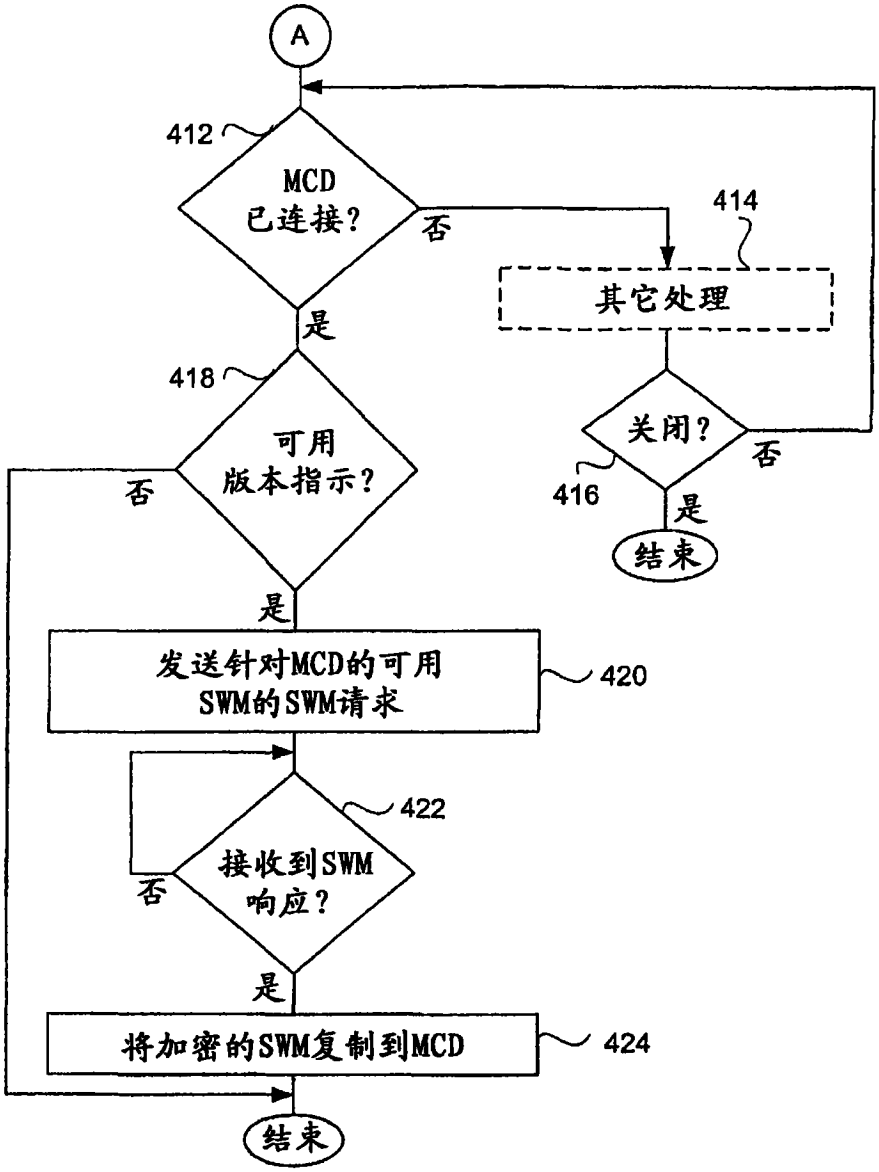

A
412
MCD
已连接?
否
414
其它处理
是
418
可用
版本指示?
否
关闭?
否
416
是
结束
是
发送针对MCD的可用
SWM的SWM请求
420
422
接收到SWM
响应?
否
是
将加密的SWM复制到MCD
424
结束

图4B

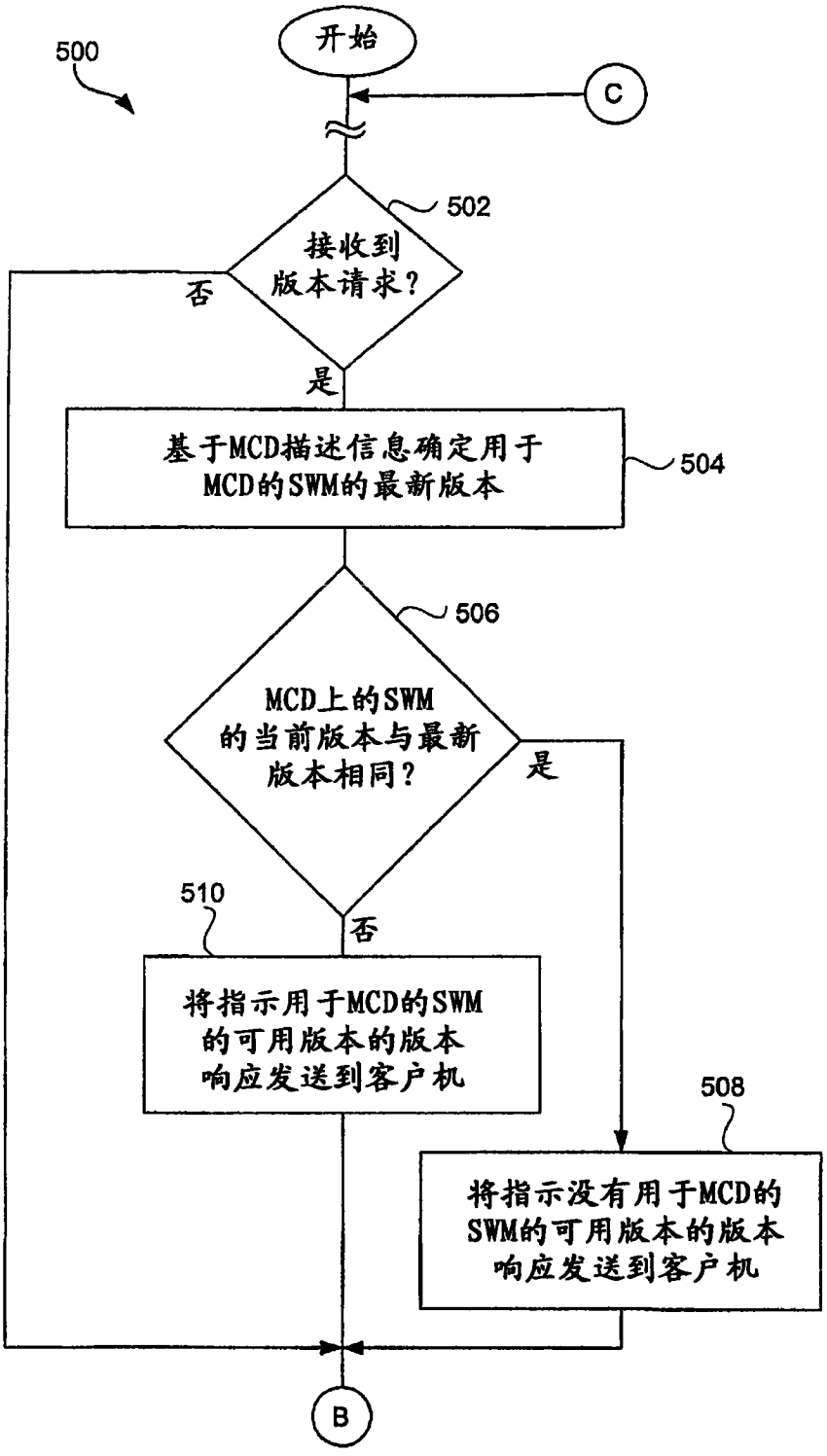

500
开始
C
502
接收到
版本请求?
否
是
基于MCD描述信息确定用于
MCD的SWM的最新版本
504
506
MCD上的SWM
的当前版本与最新
版本相同?
是
否
510
将指示用于MCD的SWM
的可用版本的版本
响应发送到客户机
508
将指示没有用于MCD的
SWM的可用版本的版本
响应发送到客户机
B

图5A

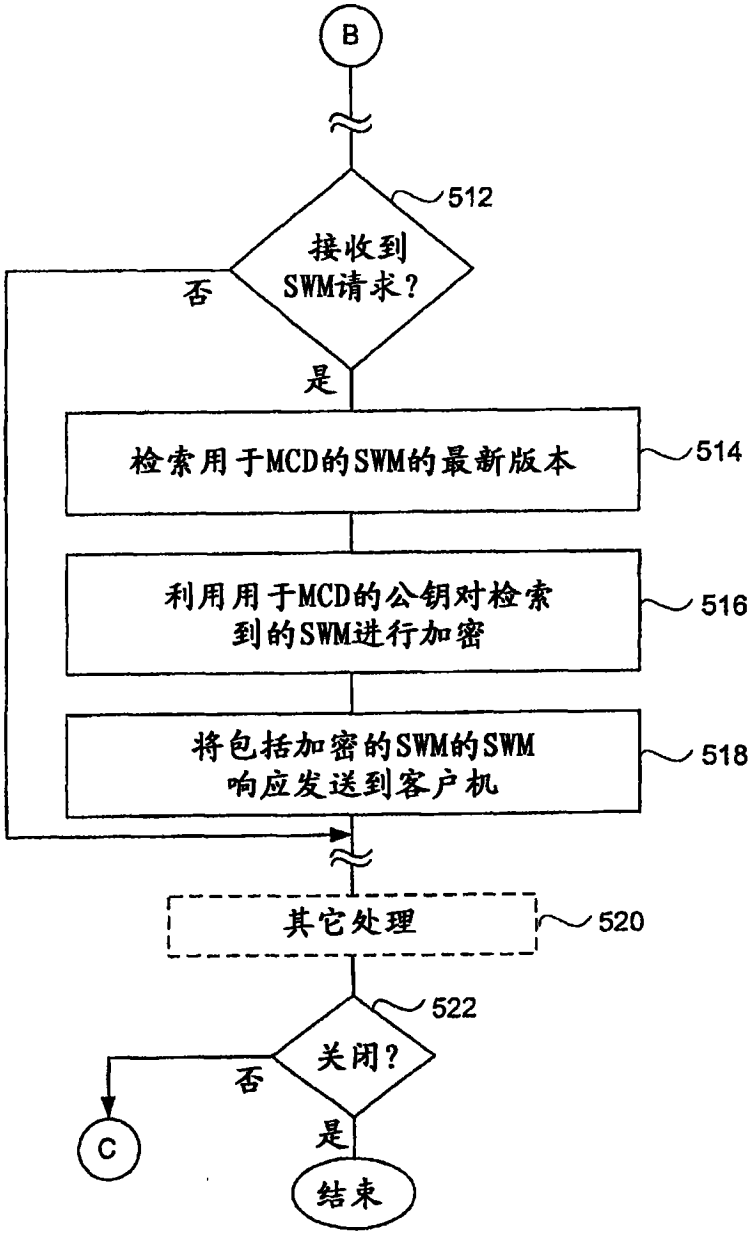

B
512
接收到SWM请求?
否
是
检索用于MCD的SWM的最新版本
514
利用用于MCD的公钥对检索到的SWM进行加密
516
将包括加密的SWM的SWM响应发送到客户机
518
其它处理
520
522
关闭?
否
是
C
结束

图5B

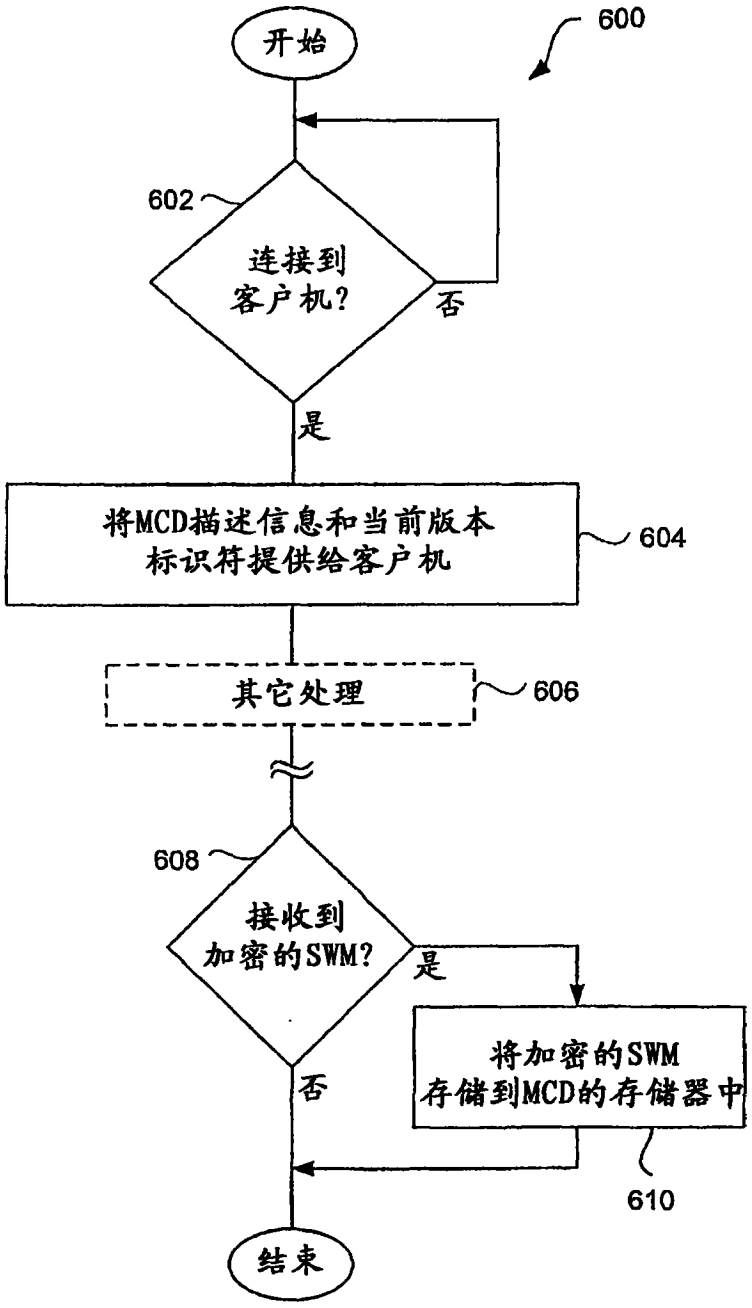

开始
600
602
连接到
客户机?
否
是
将MCD描述信息和当前版本
标识符提供给客户机
604
其它处理
606
608
接收到
加密的SWM?
是
否
将加密的SWM
存储到MCD的存储器中
610
结束

图6

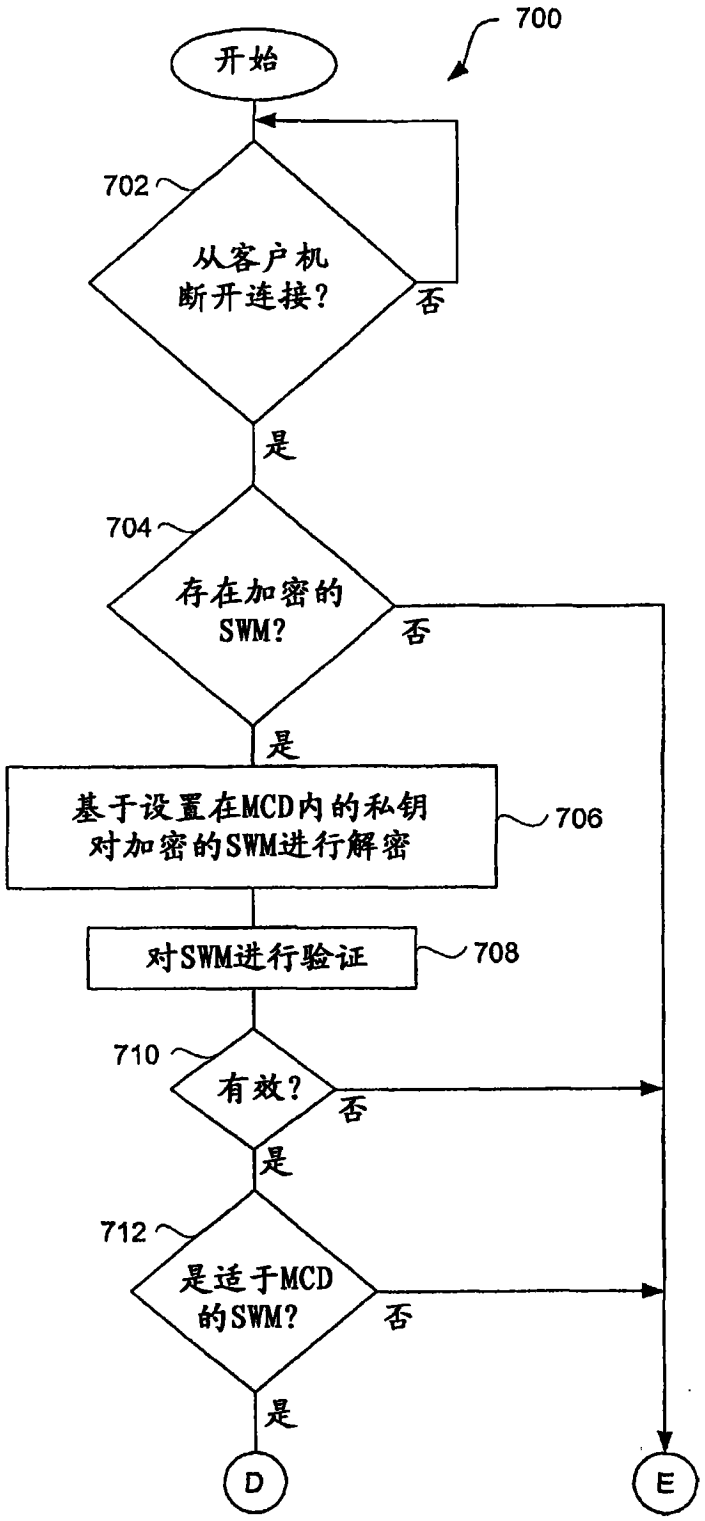

700
开始
702
从客户机
断开连接?
否
是
704
存在加密的
SWM?
否
是
基于设置在MCD内的私钥
对加密的SWM进行解密
706
对SWM进行验证
708
710
有效?
否
是
712
是适于MCD
的SWM?
否
是
D
E

图7A

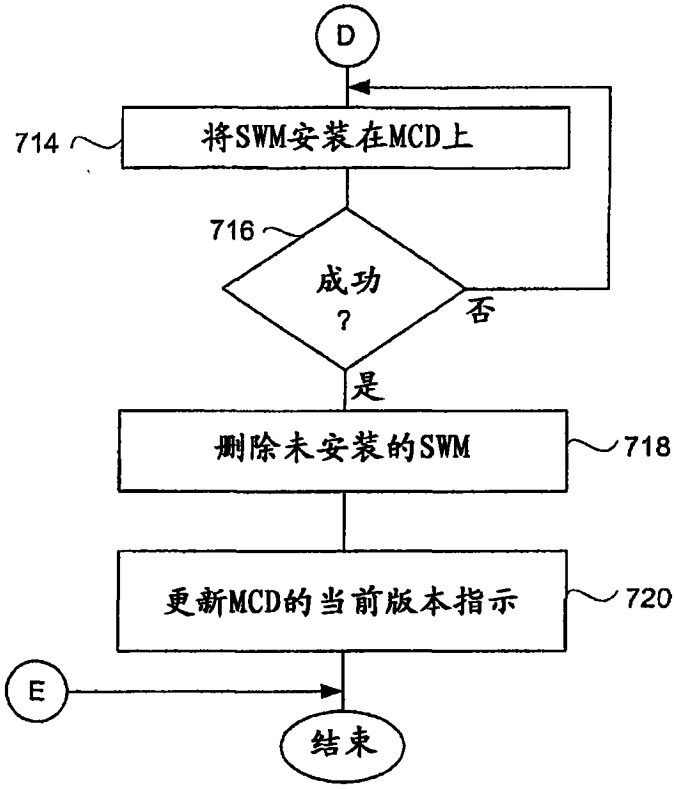

D
714
将SWM安装在MCD上
716
成功
?
否
是
删除未安装的SWM
718
更新MCD的当前版本指示
720
E
结束

图 7B