(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 108810084 B
(45)授权公告日 2022.05.10

(21)申请号 201810389388.7

(22)申请日 2018.04.26

(65)同一申请的已公布的文献号
申请公布号 CN 108810084 A

(43)申请公布日 2018.11.13

(30)优先权数据
15/499356 2017.04.27 US

(73)专利权人 奥的斯电梯公司
地址 美国康涅狄格州

(72)发明人 D.M.施拉 A.T.格伦丁
M.加芬克尔 T.E.洛维特

(74)专利代理机构 中国专利代理(香港)有限公司 72001
专利代理师 姜冰 张金金

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 67/10(2022.01)
G06F 8/61(2018.01)

(56)对比文件
US 2017070362 A1,2017.03.09
WO 2016078710 A1,2016.05.26

审查员 王绮宇

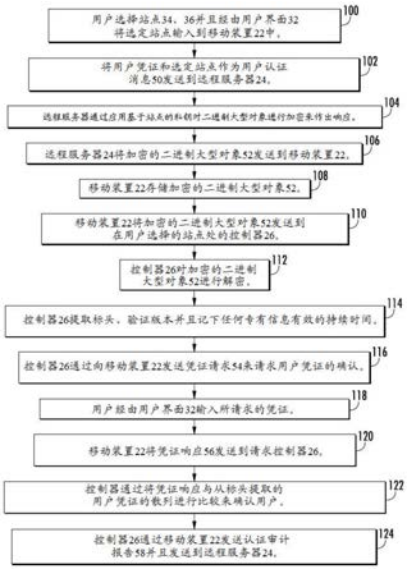
权利要求书2页 说明书4页 附图2页

(54)发明名称

使用加密代码卸载的基于移动的设备服务系统

(57)摘要

一种基于移动的设备服务系统包括远程服务器、移动装置和至少一个设备控制器。所述移动装置包括用户界面并且被配置来将由用户经由所述用户界面发起的用户认证消息发送到所述远程服务器。所述远程服务器被配置来经由所述用户认证消息来验证所述用户,并且一旦被验证,就响应于所述用户认证消息而将加密的二进制大型对象(blob)发送到所述移动装置。至少一个设备控制器被配置来从所述移动装置接收并解密所述加密的二进制大型对象。



CN 108810084 B

1.一种由用户应用的基于移动的设备服务系统,所述基于移动的设备服务系统包括:

远程服务器;

至少一个设备控制器,

至少一个站点,其中所述至少一个站点中的每个站点包括所述至少一个设备控制器中的至少一个相应的设备控制器,

移动装置,所述移动装置包括用户界面,所述移动装置被配置来将由所述用户经由所述用户界面发起的用户认证消息发送到所述远程服务器,其中所述远程服务器被配置来经由所述用户认证消息来验证所述用户,并且一旦被验证,就响应于所述用户认证消息而将加密的二进制大型对象发送到所述移动装置;

其中所述加密的二进制大型对象通过所述远程服务器经由与所述至少一个站点中的相应站点相关联的唯一私钥来进行保护,并且其中所述至少一个设备控制器被配置成从所述移动装置接收所述加密的二进制大型对象并使用所述唯一私钥来解密所述加密的二进制大型对象。

2.根据权利要求1所述的基于移动的设备服务系统,其中所述加密的二进制大型对象包括固件和标头,所述标头被配置来由所述至少一个设备控制器中的相应的设备控制器来提取。

3.根据权利要求2所述的基于移动的设备服务系统,其中所述标头包括所述唯一私钥以及用于认证的持续时间。

4.根据权利要求3所述的基于移动的设备服务系统,其中所述标头包括由所述相应的设备控制器验证的版本。

5.根据权利要求1所述的基于移动的设备服务系统,其中所述至少一个站点是多个建筑物。

6.根据权利要求1所述的基于移动的设备服务系统,其中所述至少一个站点是多个地理区域。

7.根据权利要求1所述的基于移动的设备服务系统,其中所述至少一个设备控制器是至少一个电梯控制器。

8.根据权利要求1所述的基于移动的设备服务系统,其中所述至少一个设备控制器不具有互联网连接性。

9.根据权利要求1所述的基于移动的设备服务系统,其中所述至少一个设备控制器被配置来回复请求来自所述用户的所述用户认证消息的所述移动装置。

10.根据权利要求1所述的基于移动的设备服务系统,其中所述加密的二进制大型对象是非对称加密的。

11.一种操作基于移动的设备服务系统的方法,其包括:

将选定站点从移动装置发送到远程服务器,其中所述选定站点由所述移动装置的用户选择并且作为包括所述用户的凭证的认证消息的一部分发送到所述远程服务器;

所述远程服务器经由所述认证消息来验证所述用户;

由所述远程服务器使用与所述选定站点相关联并且被预编程到所述远程服务器中的私钥来对二进制大型对象进行加密;

将所述加密的二进制大型对象发送到所述移动装置;

将所述加密的二进制大型对象从所述移动装置发送到与所述选定站点相关联的设备控制器;以及

通过所述设备控制器利用预编程到所述设备控制器中的所述私钥来对所述加密的二进制大型对象进行解密。

12.根据权利要求11所述的方法,其还包括:

将凭证请求从所述设备控制器发送到所述移动装置;

由用户将凭证输入到所述移动装置中;以及

将所述凭证从所述移动装置发送到所述设备控制器。

13.根据权利要求12所述的方法,其还包括:

将从所述移动装置发送的所述凭证与由所述设备控制器作为所述加密的二进制大型对象的一部分发送的凭证的散列进行比较。

14.根据权利要求11所述的方法,其中所述远程服务器是基于云的。

15.根据权利要求11所述的方法,其中所述移动装置是智能电话。

16.根据权利要求11所述的方法,其中所述选定站点是建筑物,并且所述设备控制器是电梯控制器。

使用加密代码卸载的基于移动的设备服务系统

背景技术

[0001] 本公开涉及设备服务系统，并且更具体地涉及使用加密代码卸载的基于移动的设备服务系统。

[0002] 用于访问设备控制器(例如，电梯控制器)的当前服务工具可依靠使用单独的硬件工具，所述硬件工具可安全地向控制器认证，同时防止专有代码的逆向工程和篡改攻击。遗憾的是，此类基于硬件的功能可能不是成本有效的。替代地，使用移动装置作为服务工具可能是可行的，但是此类移动装置无法控制提供设备服务的公司。执行安全要求以促进防篡改硬件和执行环境可能会更加困难。

发明内容

[0003] 一种由用户应用的基于移动的设备服务系统，根据本公开的一个非限制性实施方案的所述基于移动的设备服务系统包括：远程服务器；移动装置，所述移动装置包括用户界面，所述移动装置被配置来将由所述用户经由所述用户界面发起的用户认证消息发送到所述远程服务器，其中所述远程服务器被配置来经由所述用户认证消息来验证所述用户，并且一旦被验证，就响应于所述用户认证消息而将加密的二进制大型对象(blob)发送到所述移动装置；以及至少一个设备控制器，所述至少一个设备控制器被配置来从所述移动装置接收并解密所述加密的二进制大型对象。

[0004] 除了前述实施方案之外，所述基于移动的设备服务系统还包括至少一个站点，其中所述至少一个站点中的每个站点包括所述至少一个设备控制器中的至少一个相应的设备控制器，其中所述加密的二进制大型对象通过所述远程服务器经由与所述至少一个站点中的相应站点相关联的唯一私钥来进行保护。

[0005] 替代地或除了上述情况之外，在前述实施方案中，所述用户认证消息包括由所述用户选择的所述至少一个站点中的选定站点。

[0006] 替代地或除了上述情况之外，在前述实施方案中，所述加密的二进制大型对象包括固件和标头，所述标头被配置来由所述至少一个设备控制器中的相应的设备控制器来提取。

[0007] 替代地或除了上述情况之外，在前述实施方案中，所述标头包括所述唯一私钥以及用于认证的持续时间。

[0008] 替代地或除了上述情况之外，在前述实施方案中，所述标头包括由所述相应的设备控制器验证的版本。

[0009] 替代地或除了上述情况之外，在前述实施方案中，所述至少一个站点是多个建筑物。

[0010] 替代地或除了上述情况之外，在前述实施方案中，所述至少一个站点是多个地理区域。

[0011] 替代地或除了上述情况之外，在前述实施方案中，所述至少一个设备控制器是至少一个电梯控制器。

[0012] 替代地或除了上述情况之外，在前述实施方案中，所述至少一个设备控制器不具有互联网连接性。

[0013] 替代地或除了上述情况之外，在前述实施方案中，所述至少一个设备控制器被配置来回复请求来自所述用户的所述用户认证消息的所述移动装置。

[0014] 替代地或除了上述情况之外，在前述实施方案中，所述加密的二进制大型对象是非对称加密的。

[0015] 一种根据另一非限制性实施方案的操作基于移动的设备服务系统的方法包括：将选定站点从移动装置发送到远程服务器；由所述远程服务器使用与所述选定站点相关联并且被预编程到所述远程服务器中的私钥来对二进制大型对象进行加密；将所述加密的二进制大型对象发送到所述移动装置；将所述加密的二进制大型对象从所述移动装置发送到与所述选定站点相关联的控制器；以及通过所述控制器利用预编程到所述控制器中的所述私钥来对所述加密的二进制大型对象进行解密。

[0016] 除了前述实施方案之外，所述选定站点由所述移动装置的用户选择并且被作为包括所述用户的凭证的认证消息的一部分发送到所述远程服务器。

[0017] 替代地或除了上述情况之外，在前述实施方案中，所述方法包括：将凭证请求从所述控制器发送到所述移动装置；由用户将凭证输入到所述移动装置中；以及将所述凭证从所述移动装置发送到所述控制器。

[0018] 替代地或除了上述情况之外，在前述实施方案中，所述方法包括：将从所述移动装置发送的凭证与由所述控制器作为所述加密的二进制大型对象的一部分发送的凭证的散列进行比较。

[0019] 替代地或除了上述情况之外，在前述实施方案中，所述远程服务器是基于云的。

[0020] 替代地或除了上述情况之外，在前述实施方案中，所述移动装置是智能电话。

[0021] 替代地或除了上述情况之外，在前述实施方案中，所述选定站点是建筑物，并且所述控制器是电梯控制器。

[0022] 前述特征和元件可以各种组合非排他性地进行组合，除非另有明确指示。这些特征和元件以及其操作将根据以下描述和附图变得更显而易见。然而，应理解，以下描述和附图意图在本质上是示例性的并且是非限制性的。

附图说明

[0023] 各种特征通过公开的非限制性实施方案的以下详细描述对于本领域技术人员将变得显而易见。随附于详细描述的附图可简要描述如下：

[0024] 图1是作为本公开的一个非限制性示例性实施方案的基于移动的设备服务系统的示意图；并且

[0025] 图2是示出操作基于移动的设备服务系统的方法的流程图。

具体实施方式

[0026] 参考图1，可为基于移动的设备服务系统20的示例性实施方案通常采用代码卸载架构和非对称加密。设备服务系统20可包括移动装置22、远程服务器24和至少一个设备控制器26，或可使用以上各项的多个部分。移动装置22可通过可为有线或无线的相应通路28、

30来与远程服务器24和设备控制器26进行通信。如果是无线的，那么通路28、30可与诸如蓝牙®、Wi-Fi、近场通信(NFC)等的通信协议相关联。移动装置22可包括有助于与用户(例如，设备修理工)进行系统交互的用户界面32。移动装置22的非限制性示例可包括智能电话、平板电脑等。远程服务器24可为基于云的(即，云24)。设备服务系统20通常使得能够在云24和/或设备控制器26处执行代码。移动22可不执行代码，而是可仅仅为代码的载体。在一个实施方案中，远程服务器24和控制器26可由普通公司拥有并控制。

[0027] 设备服务系统20还可包括至少一个站点(即，在图1中示出为34、36的两个站点)。每个站点34、36可包括至少一个设备控制器26(即，针对每个站点34、36示出的三个设备控制器)。站点34、36的非限制性示例可为建筑物、地理区域等。设备控制器26的非限制性示例可为可由电梯制造商维修的电梯控制器。移动装置22、远程服务器24和设备控制器26可各自包括相应的处理器38、40、42(例如，微处理器)以及存储介质44、46、48，所述存储介质可为计算机可写入和可读取的。

[0028] 参考图2，示出一种操作设备服务系统20的方法。在方框100处，用户选择站点34、36并且经由用户界面32将选定站点输入到移动装置22中。在一个实施方案中，出于安全原因，用户还可将用户凭证输入到移动装置22中。替代地，移动装置22可包括可在内部识别用户凭证的应用。在方框102处，用户凭证和选定站点被作为用户认证消息发送到远程服务器24(参见箭头50)。

[0029] 在方框104处，远程服务器24利用与由用户提供的选定站点相关联的基于站点的私钥来对二进制大型对象进行加密。远程服务器24可包括预编程有用于每个相应站点34、36的唯一私钥并且存储所述唯一私钥的应用。也就是说，站点34被分配与站点36的私钥不同的私钥。二进制大型对象52的加密可为用于保护二进制大型对象52内包含的专有信息的非对称加密。在方框106处，远程服务器24将加密的二进制大型对象(参见箭头52)发送到移动装置22。

[0030] 二进制大型对象52可包括标头和固件。标头可包括版本(即，二进制大型对象的版本)、持续时间、用户凭证的散列(例如，用户密码)、设备控制器标识以及设备所属的区域或建筑物代码。所述版本通常可为索引。所述持续时间可为旨在提供特定可执行文件有效的有效时间限制的认证持续时间。用户凭证的散列旨在供控制器26使用。

[0031] 在方框108处，移动装置22可存储加密的二进制大型对象52。移动装置22的用户可不是或者不需要知道正在由移动装置22接收和/或存储的加密的二进制大型对象52。在方框110处，移动装置22可将加密的二进制大型对象52发送到由用户基于需要而选择的并且在用户选择的站点(即，站点34或站点36)处选择的控制器26。也就是说，当用户最初向云进行认证时，用户可请求访问给定站点。云可在内部包括数据库以检查请求的用户是否具有访问相关联站点和/或控制器的权限，并且可随后为所述控制器生成二进制大型对象。在方框112处，接收加密的二进制大型对象52的控制器26可使用接收二进制大型对象的站点的私钥来对二进制大型对象进行解密。在方框114处，控制器26可随后提取标头、验证版本并且还记下任何专有信息有效的持续时间。在方框116处，控制器26可通过向移动装置22发送凭证请求(参见箭头54)来请求用户凭证的确认。在方框118处，用户可经由用户界面32输入所请求的凭证(例如，用户密码)。在方框120处，移动装置22可将凭证响应(参见箭头56)发送到请求控制器26。在方框122处，控制器可通过将凭证响应与从标头提取的用户凭证的散

列进行比较来确认用户。

[0032] 在方框124处，控制器26可通过移动装置22发送认证审计报告(参见箭头58)并且发送到远程服务器24。认证审计报告可包括基于站点的私钥，从而向远程服务器24通知审计报告的来源。此时，用户现在可经由例如菜单来访问命令。

[0033] 本公开的优点和益处包括公司云与控制器之间的移动装置的安全使用。其它优点包括永远不会暴露给不期望的个人的专有信息、攻击者无法执行动态内存分析的系统、无法被篡改或修改的代码、具有用于增加安全性的持续时间限制的编码系统并且防止用户使用编码用户身份进行欺骗。

[0034] 上述各种功能可由计算机程序来实现或支持，所述计算机程序由计算机可读程序代码形成并且体现在计算机可读介质中。计算机可读程序代码可包括源代码、目标代码、可执行代码等。计算机可读介质可为能够由计算机访问的任何类型的介质，并且可包括只读存储器(ROM)、随机存取存储器(RAM)、硬盘驱动器、光盘(CD)、数字视频光盘(DVD)或其它形式。

[0035] 本文使用的诸如部件、模块、系统等的术语旨在指代计算机相关的实体，其是硬件、硬件与软件的组合或执行中的软件。通过举例，部件可以是但不限于在处理器上运行的进程、处理器、对象、可执行文件、执行线程、程序和/或计算机。应理解，在服务器上运行的应用和服务器都可以是部件。一个或多个部件可驻留在进程和/或执行线程内，并且部件可位于一个计算机上和/或分布在两个或更多个计算机之间。

[0036] 虽然参考示例性实施方案描述了本公开，但是本领域技术人员将理解，可以进行各种改变以及可以替换成等效物而不脱离本公开的精神和范围。此外，各种修改可应用来使本公开的教示适于特定情况、应用和/或材料而不脱离本公开的实质范围。本公开因此不限于本文所公开的特定示例，而是包括落入所附权利要求书的范围内的所有实施方案。

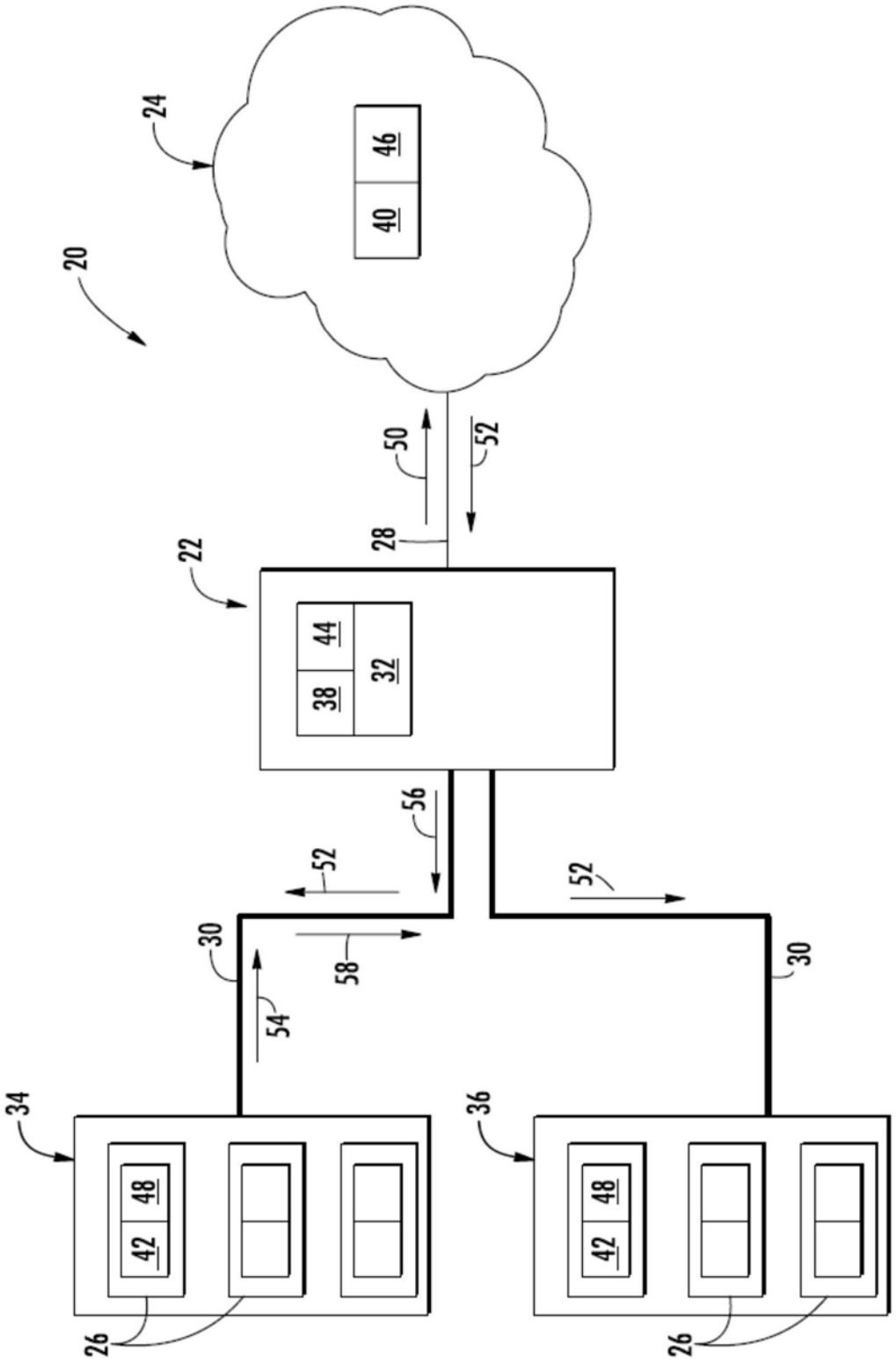

20
24
46
40
50
52
28
22
44
38
32
56
52
52
30
58
54
30
34
36
48
42
48
42
26
26

图1

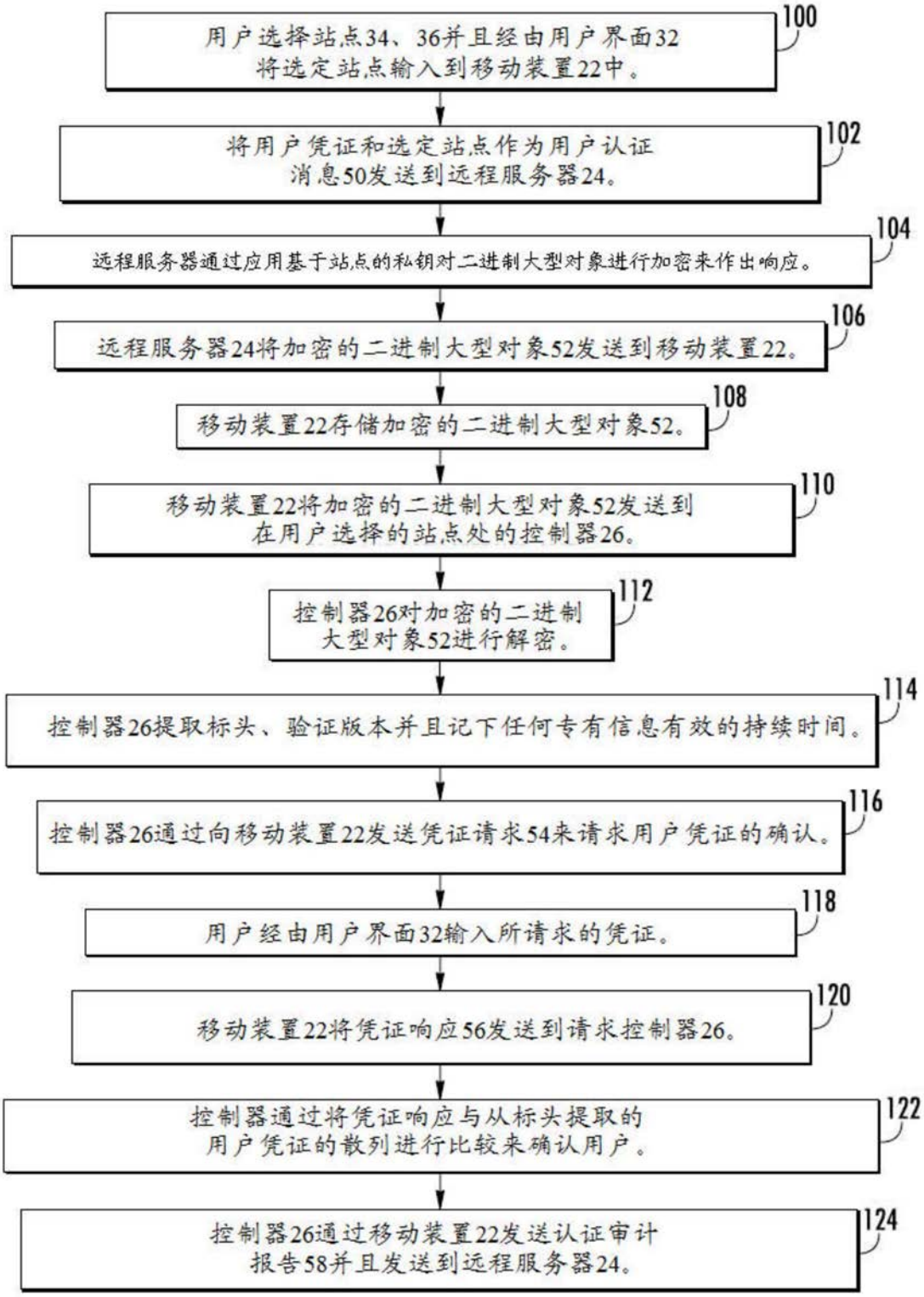

用户选择站点34、36并且经由用户界面32将选定站点输入到移动装置22中。
100
将用户凭证和选定站点作为用户认证消息50发送到远程服务器24。
102
远程服务器通过应用基于站点的私钥对二进制大型对象进行加密来作出响应。
104
远程服务器24将加密的二进制大型对象52发送到移动装置22。
106
移动装置22存储加密的二进制大型对象52。
108
移动装置22将加密的二进制大型对象52发送到在用户选择的站点处的控制器26。
110
控制器26对加密的二进制大型对象52进行解密。
112
控制器26提取标头、验证版本并且记下任何专有信息有效的持续时间。
114
控制器26通过向移动装置22发送凭证请求54来请求用户凭证的确认。
116
用户经由用户界面32输入所请求的凭证。
118
移动装置22将凭证响应56发送到请求控制器26。
120
控制器通过将凭证响应与从标头提取的用户凭证的散列进行比较来确认用户。
122
控制器26通过移动装置22发送认证审计报告58并且发送到远程服务器24。
124

图2