(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 104798430 B
(45)授权公告日 2018.09.21

(21)申请号 201380060673.X
(22)申请日 2013.06.05
(65)同一申请的已公布的文献号
申请公布号 CN 104798430 A
(43)申请公布日 2015.07.22
(30)优先权数据
13/728,606 2012.12.27 US
(85)PCT国际申请进入国家阶段日
2015.05.20
(86)PCT国际申请的申请数据
PCT/US2013/044238 2013.06.05
(87)PCT国际申请的公布数据
WO2014/105114 EN 2014.07.03
(73)专利权人 英特尔公司
地址 美国加利福尼亚州
(72)发明人 维韦克·G·古谱塔
内贾蒂·凯普莱特
(74)专利代理机构 北京东方亿思知识产权代理有限责任公司 11258
代理人 李晓冬
(51)Int.Cl.
H04L 29/06(2006.01)
H04W 12/04(2009.01)
H04W 84/12(2009.01)
H04W 4/50(2018.01)
(56)对比文件
US 2008220741 A1,2008.09.11,
US 2012036992 A1,2012.02.16,
US 2006045267 A1,2006.05.02,
审查员 李淼

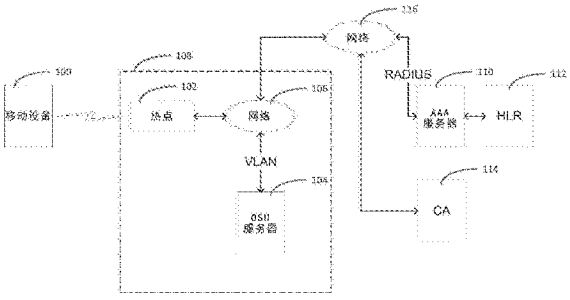
权利要求书3页 说明书11页 附图10页

(54)发明名称

无线设备的安全在线注册和配置

(57)摘要

本文一般描述了用于针对Wi-Fi热点的安全在线注册和证书的配置的移动设备和方法的实施例。在一些实施例中，配置通过使用服务集标识符(SSID)发生以关联热点并获取虚拟LAN(VLAN)标识符。VLAN标识符被用于完成注册和配置过程。在一些实施例中，热点可实施主SSID和从属SSID。移动设备通过使用从属SSID来关联热点以执行安全在线注册和配置过程。一旦通过使用注册和配置过程获取了证书，则该设备能够通过使用主SSID和已经配置的证书连接至热点。所配置的证书可包括凭证、用户名/密码或SIM类型证书。



CN 104798430 B

1.一种包括具有逻辑的一个或多个处理器的设备，所述逻辑用于：

通过使用从属服务集标识符SSID关联热点；

通过所述热点与在线注册OSU服务器建立传输层安全TLS会话；

与所述OSU服务器交换配置消息以注册订阅和配置证书；

从所述OSU服务器接收订阅管理对象；并且

与所述热点分离并通过使用主SSID和所述订阅管理对象关联所述热点。

2.根据权利要求1所述的设备，其中所述配置消息包括开放移动联盟设备管理OMA-DM消息。

3.根据权利要求1所述的设备，其中所述配置消息包括简单对象访问协议可扩展标记语言SOAP-XML消息。

4.根据权利要求1所述的设备，其中所述逻辑还用于发起用于对基于凭证的证书的配置的凭证登记协议；并且

其中在所述对基于凭证的证书的配置之后，所述逻辑还用于从所述OSU服务器接收命令以将位置添加到所述订阅管理对象。

5.根据权利要求1所述的设备，其中所述热点实施主基本服务集标识符BSSID和从属BSSID；并且

其中所述设备被配置成使用所述从属BSSID用于证书配置。

6.根据权利要求1所述的设备，其中所述从属SSID从所述主SSID中被导出。

7.根据权利要求1所述的设备，其中所述从属SSID被包含在供应商特定的消息元素中。

8.根据权利要求5所述的设备，其中所述主SSID和从属BSSID是所传输的配置文件的一部分；并且

其中所述从属SSID和从属BSSID是非传输的配置文件的一部分。

9.根据权利要求1所述的设备，其中所述逻辑还用于接收包括所述从属SSID的OSU提供者列表以用于在线注册。

10.根据权利要求1所述的设备，其中所述设备还包括：

包括一个或多个天线的收发器。

11.根据权利要求1所述的设备，其中所述逻辑还用于基于探测响应识别提供所述主SSID和所述从属SSID的所述热点。

12.一种包括具有逻辑的一个或多个处理器的设备，所述逻辑用于：

通过使用从属配置文件中的从属服务集标识符SSID关联热点，并建立与在线注册OSU服务器的安全连接；

与所述OSU服务器交换管理消息以注册订阅并标识对于创建具有证书部分的订阅管理对象来说必要的信息；

获取所述订阅管理对象；

与所述热点分离；以及

通过使用主配置文件中的主SSID和所述订阅管理对象的证书部分中的信息关联所述热点。

13.根据权利要求12所述的设备，其中所述从属配置文件是被包含为OSU提供者列表中的域的非传输的配置文件；并且

其中所述逻辑还用于获取所述OSU提供者列表。

14.根据权利要求12所述的设备，其中所述从属配置文件是Wi-Fi联盟WFA供应商特定的信息元素的一部分；并且

其中所述逻辑还用于解码所述供应商特定的信息元素以获取所述从属SSID。

15.根据权利要求12所述的设备，其中所述逻辑还用于向用户显示所述主SSID，并且当所述主SSID被显示时，隐藏所述从属SSID。

16.一种用于针对Wi-Fi网络的在线注册和配置的方法，包括：

由移动设备通过使用从属服务集标识符SSID关联热点并通过所述热点建立与在线注册OSU服务器的连接；

从所述OSU服务器接收包含与门户相关联的统一资源标识符URI的消息和由所述移动设备执行的Launch-Browser-to-URI命令；

在对所述消息的接收之后，由所述移动设备建立到所述URI的安全超文本传输协议HTTPS连接并且在HTTPS连接上向所述URI发送HTTP GET请求；

通过所述HTTPS连接与所述门户交换信息以用于包含证书部分的订阅管理对象的创建；

由所述移动设备接收包含所述证书部分的订阅管理对象；

与所述热点分离；以及

通过使用主SSID和所述订阅管理对象的证书部分中的信息由所述移动设备关联所述热点。

17.根据权利要求16所述的方法，还包括：

从所述OSU服务器接收包含凭证登记服务器的URI的可扩展标记语言XML实例文档；

通过使用所述URI建立到所述凭证登记服务器的连接并且与所述凭证登记服务器交换信息以配置凭证类型证书。

18.根据权利要求16所述的方法，还包括：

从所述OSU服务器接收包含URI的可扩展标记语言XML实例文档以获取认证、授权和计费AAA服务器信任根；

由所述移动设备获取在所述URI处的AAA服务器信任根。

19.根据权利要求16所述的方法，其中所述从属SSID是从所述主SSID中导出的。

20.一种存储指令的非暂态计算机可读存储介质，所述指令供一个或多个处理器运行以执行用于操作无线网络中的设备的操作，所述操作用于将所述设备配置成：

通过使用从属服务集标识符SSID关联热点；

通过所述热点与OSU服务器建立传输层安全TLS会话；

与所述OSU服务器交换配置消息以注册订阅和配置证书；

从所述OSU服务器获取订阅管理对象；并且

与所述热点分离并通过使用主SSID和所述订阅管理对象关联所述热点。

21.根据权利要求20所述的非暂态计算机可读存储介质，其中所述配置消息包括开放移动联盟设备管理OMA-DM消息。

22.根据权利要求20所述的非暂态计算机可读存储介质，其中所述配置消息包括简单对象访问协议可扩展标记语言SOAP-XML消息。

23.根据权利要求20所述的非暂态计算机可读存储介质，其中所述指令还将所述设备配置成：

发起用于对基于凭证的证书的配置的凭证登记协议；并且

其中在所述对基于凭证的证书的配置之后，所述指令还将所述设备配置成从所述OSU服务器接收命令以将位置添加到所述订阅管理对象。

无线设备的安全在线注册和配置

[0001] 相关申请

[0002] 本申请请求保护在2012年12月27日递交的美国专利申请序列号No.13/728,606的优先权的利益，该申请通过引用的方式被全部并入本文中。

技术领域

[0003] 本公开的实施例涉及无线通信。一些实施例涉及用于服务连接性的安全在线注册和证书的配置。一些实施例与热点2.0网络和热点2.0演进有关。

背景技术

[0004] 注册并且连接至Wi-Fi热点并非简单而用户友好的过程。用户可能不得不在不同的位置面对不同类型的网页、输入信息并选择他们的用户名/密码。目前，尚无为支持Wi-Fi功能的设备和热点定义安全在线注册机制的标准化机制。此外，当不同类型的证书(用户名/密码、凭证、用户信息模块(SIM)类型证书等等)被配置时，出现了额外的并发问题。

附图说明

[0005] 图1示出了根据一些实施例的无线网络；

[0006] 图2示出了根据一些实施例的在线注册和证书配置机制；

[0007] 图3示出了根据一些实施例的订阅管理对象的证书部分；

[0008] 图4示出了根据一些实施例的无线网络；

[0009] 图5示出了根据一些实施例的在线注册和证书配置机制；

[0010] 图6示出了根据一些实施例的在线注册和证书配置机制；

[0011] 图7示出了根据一些实施例的在线注册和证书配置机制；

[0012] 图8示出了根据一些实施例的在线注册和证书配置机制；

[0013] 图9示出了根据一些实施例的在线注册和证书配置机制；

[0014] 图10示出了根据一些实施例的系统框图。

具体实施方式

[0015] 下面的详细描述和附图充分地说明了具体实施例以使本领域的技术人员能够实践它们。其他实施例可包含结构的、逻辑的、电气的处理及其他变化。一些实施例中的部分及其特征可被包括在其他实施例的部分及其特征中或代替其他实施例的部分及其特征。在权利要求中提到的实施例包含那些权利要求的所有可用的等同物。

[0016] 图1示出了根据一些实施例的无线网络。根据一些实施例，网络为安全在线注册和证书的配置构成了可操作环境。在图1中，移动设备100(有时被称为用户装置(UE)、站点(STA)或无线设备)可以是被配置成关联Wi-Fi热点102并执行与安全在线注册和配置相关联的各种功能的支持Wi-Fi功能的设备。移动设备100可包括用以实现诸如，开放移动联盟设备管理(OMA-DM)协议、简单对象访问协议可扩展标记语言(SOAP-XML)协议或一些其他管

理协议之类的设备管理协议的设备管理客户端(未被示出)。

[0017] Wi-Fi热点102可以是Wi-Fi网络的一部分,并且可被耦合至网络106,其中网络106可以是局部网络或路由器,或者可以是通过其可访问诸如互联网之类的其他网络116的网关,或者是二者的组合。Wi-Fi热点102可作为Wi-Fi接入点(AP)进行操作。

[0018] Wi-Fi热点102可被耦合至各种网络元件,诸如,在线注册(OSU)服务器104,认证、授权和计费(AAA)服务器110,归属位置寄存器(HLR)112和证书授权(CA)114。在一些实施例中,OSU服务器104可实现OMA-DM协议。在其他实施例中,OSU服务器104可实现SOAP-XML协议或一些其他管理协议。在一些实施例中,OSU服务器104可用作其他服务器或设备(诸如,AAA服务器110、HLR 112和CA 114)的代理。

[0019] 根据本文的实施例,移动设备100可被配置用于针对Wi-Fi热点的在线注册和证书配置。如下面更加详细地描述的,这些可使用各种管理协议,诸如OMA-DM、SOAP-XML或一些其他协议。这可使在他们的后端核心网络中可能已经实施了这些协议中的一个或多个的蜂窝类型网络服务提供商能够使用相同的服务器和被安装的组件以将该功能扩展为用于服务Wi-Fi网络。通过这种方式,Wi-Fi网络可与相同的蜂窝网后端核心一起运行,这样以更加无缝和透明的方式实现了从蜂窝类型网络中卸载Wi-Fi。蜂窝类型网络可能指的是任何2G(例如,GSM、EDGE)或3G(例如,3GPP、3GPP2)或4G(例如,WiMAX、LTE)配置的网络。

[0020] 在图1中,Wi-Fi热点102和OSU服务器104能够组成强制门户108的一部分。强制门户能够阻止/拦截IP分组和将请求重新路由至指定的位置。出于安全目的,这能够提供例如,“带围墙的花园”。

[0021] 图2示出了根据一些实施例的在线注册和证书配置机制。在图2的实施例中,热点202具有单个服务集标识符(SSID),其中SSID可被诸如移动设备200之类的设备用来关联热点。此外,在图2中,热点202和OSU服务器204可以是强制门户的一部分(由虚线框206示出)。

[0022] 在图2中,如212和214所示,移动设备200使用热点202的单个SSID以认证和关联热点202。如所描述的,此过程使用带有服务器端认证和4次握手协议的匿名可扩展认证协议传输层安全(EAP-TLS)。移动设备200的证书是根据归属运营商的HLR验证的。作为初始关联过程的一部分,虚拟局域网(VLAN)标识符被传递至移动设备200以用于在线注册和证书配置。通过不同的路由策略,不同的VLAN配置能够被用于不同的移动设备。

[0023] 在移动设备具有VLAN标识符之后,它能够将该VLAN标识符用于在线注册和配置过程的剩余部分。这种在线注册和配置过程中的典型步骤通过216、218、220、222和224被示出。

[0024] 此过程通常从允许移动设备200与OSU服务器204建立联系的初始交换开始以启动该过程。在此初始交换216期间,OSU通常提供能够从其获取订阅率和其他类似的信息的统一资源标识符(URI)。初始交换216通常还包含用于使移动设备200通过从OSU服务器204获取的URI启动浏览器的命令。

[0025] 交换218示出了移动设备200和OSU服务器204如服务提供商所指定的那样交换注册数据的过程。此信息能够组成订阅管理对象的证书部分的一部分。在此信息被确定后,如果证书将是用户名/密码类型的(与基于凭证或用户身份模块(SIM)类型证书相反),则来自信任根AAA服务器208的证书被获取并被存储在订阅管理对象中,并且任意TLS会话被发布。这能够例如,通过交换224被示出。

[0026] 然而，如果在交换218之后，基于凭证的证书是所期望的，则凭证登记过程被发起。此过程在图2中通过交换220和交换222被示出。在交换220和222中，证书被CA 210获取并签名(验证)。这能够由例如，移动设备200通过使用互联网工程任务组(IETF)请求注解5967(RFC 5967)样式的公钥加密标准#10(PKCS#10)请求来实现。如此交换所指出的，当CA 210验证凭证时，OSU服务器204能够作为代理。当凭证已经由CA 210签名之后，OSU服务器204能够以RFC 5967样式的PKCS#7响应来应答。

[0027] 当基于凭证的证书是所期望的时，最终交换与此前结合交换224所描述的略有不同。当基于凭证的证书是所期望的时，在交换220和交换222之后，从OSU服务器204中获取标识了由交换220和222所创建的证书的订阅管理对象。最后，任意TLS会话被发布。

[0028] 一旦移动设备200具有订阅管理对象，则如226所示出的，该移动设备200与热点202分离。最后，如228所指出的，移动设备200通过使用它的SSID和在订阅管理对象中标识的证书来关联热点202。

[0029] 图3示出了根据一些实施例的订阅管理对象的示例证书部分。为了简单起见，订阅管理对象的剩余部分未被示出，但是根据热点2.0规范和演进的热点2.0规范，订阅管理对象可以是每提供者订阅(PerProviderSubcription)管理对象。在下面的详细描述中，在所示出的树中的节点将被称为节点、元素、域和/或参数。所有均意图表明相同的含义，并非意图表明差异。

[0030] 证书部分300包含创建数据302，其表示证书被创建或最近更新的日期。如果呈现了过期日期304，则其表示证书过期的日期。领域330说明了与证书相关联的领域。移动设备通过将该领域与在初始网络发现阶段期间返回到接入网络查询协议(ANQP)网络接入标识符(NAI)领域元素中的领域相比较来确定它是否应该能够成功地认证热点。支持IEEE 802.11u的移动设备将通过使用ANQP针对附加信息对支持IEEE 802.11u的热点进行查询。这可包括对于被称为NAI领域列表的元素的请求。NAI领域列表包括与该领域相关联的用于接入的一个或多个(根据RFC-4282定义的)NAI领域和可选EAP方法和认证参数。

[0031] 取决于所存储的证书的类型，证书部分300应包含用户名/密码参数306、数字凭证参数324或SIM参数332。

[0032] 用户名/密码参数306包括各种参数，其中包括用户名308和密码310。机器管理的参数312指定密码是否是机器管理的。SoftTokenApp(软令牌应用)314指定应当被用于生成密码的应用。当此参数出现时，密码应具有空值。AbleToShare(可共享)316表明证书是否仅在订阅的机器上是可用的(即，非AbleToShare)或者对该用户的其他机器也是可用的(即，AbleToShare)。EAP方法318包括EAP方法320和内部EAP方法322，其中EAP方法320表明EAP方法，而内部EAP方法322表明隧道式EAP方法(如果使用)。

[0033] 数字凭证参数324包括数字凭证类型326和certSHA256指纹328，其中数字凭证类型326表明数字凭证的类型(例如，802.1ar或x509v3)，certSHA256指纹328提供了用于订阅的凭证证书的SHA-256指纹。此参数指定了凭证证书中的发行者可识别名。结合凭证序列号，此参数唯一标识凭证。

[0034] SIM参数332包括国际移动设备用户识别(IMSI)码334和EAP方法336，其指定了被用于基于SIM的认证的EAP方法(例如，EAP-SIM、EAP认证和密钥协商(EAP-AKA)等等)。

[0035] 图4示出了根据一些实施例的无线网络。根据一些实施例，网络为安全在线注册和

证书的配置构成了可操作环境。在图4中，移动设备400(有时也被称为UE或无线设备)可以是被配置成关联Wi-Fi热点402并且执行与安全在线注册和配置相关联的各种功能的支持Wi-Fi功能的设备。移动设备400可包括设备管理客户端(未被示出)以实现诸如OMA-DM协议、SOAP-XML协议或一些其他管理协议之类的设备管理协议。

[0036] Wi-Fi热点402可以是Wi-Fi网络的一部分并且可被耦合至网络408，其中网络408可以是局部网络或路由器、通过其可以访问诸如互联网之类的其他网络(未被示出)的网关或二者的组合。Wi-Fi热点402可作为Wi-Fi AP操作。

[0037] 在图4所示的实施例中，热点402具有主SSID和基本服务集标识符(BSSID)404以及从属SSID和BSSID 406，它们共享同一物理网络。在此实施例中，主SSID由已经具有证书的设备使用，并且从属SSID由需要注册服务和配置证书的设备使用。主SSID和从属SSID以及BSSID可通过所定义的方式互相关联或者可以从彼此之中导出。例如，词组或其他标识符能够被添加到主SSID(或BSSID)以确定从属SSID(或BSSID)。在一个具体的实施例中，从属SSID通过向主SSID添加词组“HS-从属”被导出。因此，“Starbucks”的SSID将产生“HS-从属-Starbucks”。其他词组和/或标识符也可被使用或者一些其他功能或机制能够被用于从主SSID中导出从属SSID。

[0038] 希望对这种热点进行注册和证书配置的设备需要发现或标识从属SSID(以及从属BSSID)以便于适当地关联热点402并开始注册和配置过程。这能够通过各种方式来实现。在最简单的示例中，从属SSID就像主SSID一样被广播(或被包括作为探测响应的一部分)。当此过程发生时，所显示的SSID列表能够由诸如移动设备400之类的移动设备进行过滤以仅示出主SSID而不示出从属SSID。或者，如果从属SSID通过已知的或可预测的方式从主SSID中被导出，则该设备能够通过了解主SSID(其被广播在信标帧中或响应于探测请求被发送)从主SSID中计算或确定从属SSID。作为选择或作为附加地，从属SSID能够被包括在Wi-Fi联盟(WFA)供应商特定的信息元素中。在又一示例中，主SSID和主BSSID可以是被作为信标帧的一部分或响应于探测请求被发送的主配置文件的一部分，并且从属SSID和从属BSSID可以是未被发送的从属配置文件的一部分。从属配置文件可作为OSU提供商列表的一部分被包括在其中。在又一示例中，多个BSSID元素能够被包括在信标帧中，或作为对探测请求的响应。这些不同的示例和实施例能够通过各种方式进行结合以获得另外的实施例。取决于具体的实施例，主SSID和从属SSID可能具有相同的或不同的无线覆盖范围。

[0039] Wi-Fi热点402可被耦合至各种网络元件，诸如OSU服务器410、AAA服务器412、HLR 414和CA 416。在一些实施例中，OSU服务器410可实现OMA-DM协议。在其他实施例中，OSU服务器410可实现SOAP-XML协议或一些其他管理协议。在一些实施例中，OSU服务器410可作为其他服务器或设备(诸如，AAA服务器412、HLR 414和CA 416)的代理。

[0040] 根据本文的实施例，移动设备400可被配置用于针对Wi-Fi热点的在线注册和证书配置。如下面更加全面地描述的，这些过程可使用各种管理协议，诸如OMA-DM、SOAP-XML或一些其他协议。这可使在他们的后端核心网络中可能已经实施了这些协议中的一个或多个的蜂窝类型网络服务提供商能够使用相同的服务器和所安装的组件以将该功能扩展为用于服务Wi-Fi网络。通过这种方式，Wi-Fi网络可与相同的蜂窝网络后端核心一起运行，从而使Wi-Fi能够通过更加无缝和透明的方式从蜂窝类型网络中卸载。蜂窝类型网络可能指的是任何2G(例如，GSM、EDGE)或3G(例如，3GPP、3GPP2)或4G(例如，WiMAX、LTE)配置的网络。

[0041] 图5示出了根据一些实施例的在线注册和证书配置机制。在图5的实施例中，热点502具有主SSID 530和从属SSID 528。热点502还可具有主BSSID和从属BSSID(二者均未被示出)。如上面所描述的，它们能够以某种方式相关联或可导出。移动设备将使用从属SSID 528用于在线注册和证书配置，并且如果移动设备已经具有证书(或已经配置了证书)，则移动设备将使用主SSID 530用于正常连接以使用热点服务。

[0042] 注册和配置过程在交换510和交换512处开始，其中移动设备使用从属SSID来认证和关联热点502。此过程可使用带有服务器端认证的匿名EAP-TLS。如交换512所指出的，通过AAA服务器506，移动设备500的证书根据归属运营商的HLR进行验证。

[0043] 交换514允许移动设备500联系OSU服务器504以开始注册和配置过程。在此初始交换514期间，OSU服务器504提供能够从其获取订阅率和其他类似的信息的URI。初始交换514通常还包含用于使移动设备500通过从OSU服务器504获取的URI启动浏览器的命令。

[0044] 交换516示出了移动设备500和OSU服务器504如服务提供商所指定的那样交换注册数据的过程。此信息能够组成订阅管理对象的一部分。在此信息被确定后，如果证书将是用户名/密码类型的(与基于凭证或SIM类型证书相反)，则来自信任根AAA服务器506的证书被获取并被存储在订阅管理对象中，并且任意TLS会话被发布。这能够例如，通过交换522被示出。

[0045] 然而，如果在交换516之后，基于凭证的证书是所期望的，则凭证登记过程被发起。此过程通过交换518和交换538被示出。在交换518和538中，通过CA 508获取并注册(验证)凭证。这能够由例如，移动设备500通过使用IETF RFC 5967样式的PKCS#10请求来实现。如此交换所指出的，当CA 508验证凭证时，OSU服务器504能够作为代理。在凭证已经由CA 508验证之后，OSU服务器504能够通过RFC 5967样式的PKCS#7响应来应答。

[0046] 当基于凭证的证书是所期望的时，最终交换与之前结合交换522所描述的略有不同。当基于凭证的证书是所期望的时，在交换518和交换538之后，标识了由交换518和538所创建的证书的订阅管理对象从OSU服务器504中被获取。最后，任意TLS会话被发布。

[0047] 一旦移动设备500具有订阅管理对象，则如524所示出的，它即与热点502分离。最后，如526所指出的，移动设备500通过使用它的主SSID530和在订阅管理对象中标识的证书来关联热点502。

[0048] 图6示出了根据一些实施例的在线注册和证书配置机制。在此实施例中，配置是使用根据OMA-DM协议配置的OMA-DM管理消息针对用户名/密码类型证书进行的。这些消息被称为OMA-DM封包1消息、OMA-DM封包2消息、OMA-DM封包3消息和OMA-DM封包4消息。OMA-DM协议可由OMA-DM规范中的OMA-DM工作小组和数据同步(DM)工作小组来指定。

[0049] 在线注册和配置从移动设备600通过使用从属SSID 638关联热点602(未被示出)开始。在关联热点602之后，在交换606中移动设备600发起对OSU服务器604的TLS连接，并且通过使用安全超文本传输协议(HTTPS)执行服务器端认证。

[0050] 在交换608中，移动设备600向OSU服务器604发送DM封包1，其中DM封包1包含DevInfo和DevDetail管理对象，并且通用警报(Generic Alert)指出联系OSU服务器704的原因。通用警报中的原因元素被设置成“SubscriptionCreation(订阅创建)”，表明移动设备600的用户想要建立对此服务提供商的新的订阅。DevDetail管理对象包含通用移动设备信息，并且DevInfo管理对象包含用于OMA-DM或SOAP-XML服务器的信息。对这些管理对象的

详细说明可以在OMA移动设备管理树说明，版本1.2中找到。

[0051] 在交换610中，OSU服务器604可使用在DevInfo和DevDetail管理对象中提供的信息以确定用以配置的证书的类型(例如，用户名/密码或凭证)。在此示例中，OSU服务器604将配置用户名/密码类型证书。OSU服务器604通过用以在移动设备600上针对所包括的URI启动浏览器的命令Execute:LaunchBrowsertoURI向客户端返回DM封包2。

[0052] 在接收Execute:LaunchBrowsertoURI命令之后，移动设备启动浏览器，建立到交换610中返回的URI的安全HTTPS连接，并且向交换610中返回的OSU服务器URI发送HTTPS GET请求。这在图6中通过交换612被示出。出于本公开的目的，术语浏览器被用来指代能够在移动设备的用户界面上呈现页面的浏览器功能。这并非意图暗示独立的应用。例如，实施方式可包括连接管理器中的浏览器功能。

[0053] 在交换614中，移动设备600和OSU服务器604如服务提供商所指定的那样交换注册数据。在某些情况下，用户能够具有通过使用与当前所使用的移动设备不同的移动设备配置的订阅，或者原始移动设备可能已经被重新成像，或者该用户此前已经通过服务提供商(例如，通过他们的网站)设置了账户。在这些情境中，订阅已经被建立，但移动设备不具有用户名/密码证书。此步骤的消息流可适应此情境并允许用户利用绑定至此前建立的订阅的证书配置该移动设备。

[0054] 在订阅配置过程的结尾处，如交换616所示出的，OSU服务器604返回sppUserInputResponse XML实例文档。如果没有错误发生，则sppUserInputResponse是sppStatus和PerProviderSubscription管理对象URI的容器。sppUserInputResponse XML实例文档被返回，它的HTTP内容类型被设置成“application/vnd.wfa.cm+xml.”。

[0055] 如果订阅创建的状态为成功，则如交换618所示出的，移动设备600向OSU服务器604发送包含了此前命令执行的状态的DM封包3。如果在新订阅的建立中存在错误，则移动设备将接收DM封包4(未被示出)，表明OMA DM事务处理的结束。

[0056] 如交换620所示出的，OSU服务器604向移动设备600发送包含了PerProviderSubscription管理对象和命令ADD的DM封包4，指定被添加至移动设备600上的OMA-DM管理树的PerProviderSubscription管理对象的位置。在交换622中，移动设备600发送表明了此前操作的状态的DM封包3。作为响应，如624中所示出的，OSU服务器604发送DM封包4，其中DM封包4表明OMA DM事务处理的结束。

[0057] 在OMA-DM事务处理的结尾处，如626中所示出的移动设备600从PerProviderSubscription管理对象中所指定的URL获取AA服务器信任根。移动设备向OSU服务器604发送对于URL的HTTPS Get请求，OSU服务器604可提供HTTP代理服务，如果需要的话，以从URL中标识的主机中获取AAA服务器凭证(交换628)。

[0058] 在交换630中，移动设备600发布在606中建立的TLS会话。然后，如632所示出的，移动设备600从Wi-Fi接入网中分离。

[0059] 如果在618中成功地建立了订阅，则如634中所示出的，移动设备600可通过使用主SSID 640关联新的证书。

[0060] 图7示出了根据一些实施例的在线注册和证书配置机制。在此实施例中，配置是通过使用根据OMA-DM协议配置的OMA-DM管理消息针对凭证类型证书进行的。这些消息被称为OMA-DM封包1消息、OMA-DM封包2消息、OMA-DM封包3消息和OMA-DM封包4消息。

[0061] 在线注册和配置从移动设备700通过使用从属SSID 742关联热点702(未被示出)开始。在关联热点702之后,在交换708中移动设备700发起对OSU服务器704的TLS连接,并且通过使用安全HTTPS执行服务器端认证。

[0062] 在交换710中,移动设备700向OSU服务器704发送DM封包1,其中DM封包1包含DevInfo和DevDetail管理对象,并且通用警报(Generic Alert)指出联系OSU服务器604的原因。通用警报中的原因元素被设置成“SubscriptionCreation(订阅创建)”,表明移动设备700的用户想要建立对此服务提供商的新的订阅。DevDetail管理对象包含通用移动设备信息,并且DevInfo管理对象包含用于OMA-DM或SOAP-XML服务器的信息。对这些管理对象的详细说明可以在OMA移动设备管理树说明,版本1.2中找到。

[0063] 在交换712中,OSU服务器704可使用在DevInfo和DevDetail管理对象中提供的信息以确定用以配置的证书的类型(例如,用户名/密码或凭证)。在此示例中,OSU服务器704将配置凭证类型证书。OSU服务器704通过用以在移动设备700上针对所包括的URI启动浏览器的命令Execute:LaunchBrowsertoURI向客户端返回DM封包2。

[0064] 在接收Execute:LaunchBrowsertoURI命令之后,移动设备700启动浏览器,建立到交换712中返回的URI的安全HTTPS连接,并且向交换712中返回的OSU服务器URI发送HTTPS GET请求。这在图7中通过交换714被示出。

[0065] 在交换716中,移动设备700和OSU服务器704如服务提供商所指定的那样交换注册数据。在某些情况下,用户能够具有通过使用与当前所使用的移动设备不同的移动设备配置的订阅,原始的移动设备可能已经被重新成像或者用户此前已经通过服务提供商(例如,通过他们的网站)设置了账户。在这些情境中,订阅已经被建立,但移动设备不具有证书。此步骤的消息流可适应此情境并且允许用户利用绑定至此前建立的订阅的证书配置该移动设备。

[0066] 在交换718中,OSU服务器704返回订阅创建过程的状态。如果订阅创建过程的状态是成功的,则如交换720所示出的,移动设备700发送所执行的命令的状态为成功的DM封包3。如果在交换718中服务器指出错误,则在交换720中移动设备700将向服务器返回错误。

[0067] 在交换722中,OSU服务器704通过命令Execute:CertificateEnrollToURI(执行:到URI的凭证注册)向移动设备700发送DM封包4。此DM封包在数据域中包括getCertificate XML实例文档。移动设备700在724和726中执行凭证注册。在凭证注册程序期间,AAA服务器信任根被提供至移动设备700。

[0068] 如交换728所示出的,如果凭证注册执行是成功的,则移动设备700向OSU服务器704发送DM封包3。如果在凭证注册执行中存在错误,则其后移动设备进行至交换736。

[0069] 在交换730中,OSU服务器704向移动设备700发送包含了PerProviderSubscription管理对象和命令ADD的DM封包4,指定被添加至移动设备上的OMA-DM管理树的PerProviderSubscription管理对象的位置。在交换732中,移动设备700发送具有所执行的命令的状态的DM封包3。在交换734中,OSU服务器704发送DM封包4,其中DM封包4表明OMA DM事务处理的结束,并且如736中所示出的,移动设备700发布在交换708中所建立的TLS会话。

[0070] 如738所示出的,移动设备700从网络中分离。在交换740中,其后移动设备700通过使用在使用了主SSID 744的交换724和726中获取的证书能够关联热点702。

[0071] 图8示出了根据一些实施例的在线注册和证书配置机制。在此实施例中，配置是通过使用SOAP-XML管理消息针对用户名/密码类型证书进行的。

[0072] 在线注册和配置从移动设备800通过使用从属SSID 828关联热点802(未被示出)开始。在关联热点802后，在交换806中移动设备800发起对OSU服务器804的TLS连接，并且通过使用安全HTTPS执行服务器端认证。

[0073] 在交换808中，移动设备800向包括DevInfo和DevDetail管理对象的服务器发送sppPostDevData。requestReason(请求原因)的值被设置成“订阅注册”，表明移动设备800希望注册证书。OSU服务器804可使用DevInfo和DevDetail管理对象中所提供的信息以确定用以配置的证书的类型(例如，用户名/密码或凭证)。

[0074] 在交换810中，OSU服务器804向移动设备800发送sppPostDevDataResponse SOAP方法。响应方法的内容向移动设备800通知在线注册过程中的下一步。由于移动设备800已经就订阅注册发出信号，因而OSU服务器804返回使移动设备针对消息中所提供的URI启动浏览器的命令。如果没有错误发生，则sppStatus被设置成“OK”；sppStatus值为“OK”还表明证书配置过程未完成。

[0075] 在交换812中，移动设备800向sppPostDevDataResponse中所提供的URI发送HTTPS GET请求。

[0076] 在交换814中，移动设备800和OSU服务器804如服务提供商所指定的那样交换注册数据。在某些情况下，用户能够具有通过使用与当前所使用的移动设备不同的移动设备配置的订阅，原始移动设备可能已经被重新成像，或者该用户此前已经通过服务提供商(例如，通过他们的网站)设置了账户。在这些情境中，订阅已经被建立，但移动设备不具有用户名/密码证书。此步骤的消息流可适应此情境并允许用户利用绑定至此前建立的订阅的证书配置该移动设备。

[0077] 在注册数据的交换的结尾处，如交换816所示出的，移动设备800可从OSU服务器获取804sppUserInputResponse XML实例文档。如816所示出的，此XML实例文档可以是被包括在输入注册数据结束时被传送至移动设备800的网页中的隐藏文档，而不是单独的交换。如果没有错误发生，则sppUserInputResponse是sppStatus、addMO命令和PerProviderSubscription管理对象的容器。sppUserInputResponse XML实例文档可被返回，它的HTTP内容类型被设置成“application/vnd.wfa.cm+xml”。移动设备800的网络浏览器可将此XML实例文档传递至本地注册的帮助应用以用于处理(例如，连接管理器)。PerProviderSubscription管理对象包含用户名和密码以及辅助的配置数据。对被设置成“配置完成”的sppStatus的接收向移动设备800表明用户名和密码配置完成。

[0078] 在交换818中，移动设备800使用HTTPS以从PerProviderSubscription管理对象中所指定的URL中获取AAA服务器信任根。移动设备可向OSU服务器发送对URL的HTTPS GET请求，如果需要的话，其可提供HTTP代理服务以从URL中所标识的主机中获取AAA服务器凭证。交换818由交换820(HTTPS响应)确认。

[0079] 在822中，移动设备800发布其在交换806中建立的TLS会话。如824中所示出的，移动设备800能够与热点802分离，其后如826中所示出的，移动设备800通过使用新建立的证书和主SSID 830关联热点802。

[0080] 图9示出了根据一些实施例的在线注册和证书配置机制。在此实施例中，配置是通

过使用SOAP-XML管理消息针对凭证类型证书进行的。

[0081] 在线注册和配置从移动设备900通过使用从属SSID 934关联热点902(未被示出)开始。在关联热点902之后,在交换908中移动设备900发起对OSU服务器904的TLS连接,并且通过使用安全HTTPS执行服务器端认证。

[0082] 在交换910中,移动设备900向服务器发送包括DevInfo和DevDetail管理对象的sppPostDevData。requestReason的值被设置成“订阅注册”,表明移动设备900希望注册证书。OSU服务器904可使用DevInfo和DevDetail管理对象中所提供的信息以确定用以配置的证书的类型(例如,用户名/密码或凭证)。

[0083] 在交换912中,OSU服务器904向移动设备900发送sppPostDevDataResponse SOAP方法。响应方法的内容向移动设备900通知在线注册过程中的下一步。由于移动设备900已经就订阅注册发出信号,因而OSU服务器904返回使移动设备针对消息中所提供的URI启动浏览器的命令。如果没有错误发生,则sppStatus被设置成“OK”;sppStatus值为“OK”还表明证书配置过程未完成。

[0084] 在交换914中,移动设备900向sppPostDevDataResponse中所提供的URI发送HTTPS GET请求。

[0085] 在交换916中,移动设备900和OSU服务器904如服务提供商所指定的那样交换注册数据。在某些情况下,用户能够具有通过使用与当前所使用的移动设备不同的移动设备配置的订阅,原始移动设备可能已经被重新成像,或者该用户此前已经通过服务提供商(例如,通过他们的网站)设置了账户。在这些情境中,订阅已经被建立,但移动设备不具有证书。此步骤的消息流可适应此情境并允许用户利用绑定至此前建立的订阅的证书配置该移动设备。

[0086] 如交换918所示出的,在注册数据的交换的结尾处,移动设备900可从OSU服务器904获取sppUserInputResponse XML实例文档。此XML实例文档可以是被包括在输入注册数据结束时被传送至移动设备的网页中的隐藏文档,而不是作为交换918的一部分被返回。

[0087] 如果没有错误发生,则sppUserInputResponse是sppStatus和getCertificate exec命令的容器。sppUserInputResponse XML实例文档可被返回,它的HTTP内容类型被设置成“application/vnd.wfa.cm+xml”。网络浏览器可将此XML实例文档传递至本地注册的帮助应用以用于处理(例如,连接管理器)。XML实例文档包含凭证登记服务器的URI以及登记所需的其他元数据。

[0088] 在交换920和922中,移动设备900执行凭证登记。凭证登记过程在通常情况下应花费很短的时期。通常情况被定义为意味着Wi-Fi热点和服务提供商核心网络未发生拥堵,并且OSU服务器904和CA 906未超载。在成功程序的结尾处,移动设备900已经配置了服务提供商可用于认证移动设备900的凭证。当不成功时,移动设备900可被通知凭证登记。如果凭证响应花费了超出预期的时间,则移动设备900可能超时并且宣布凭证登记失败。如果移动设备900从OSU服务器904接收“待定”响应,则移动设备900可继续重试凭证请求,直到进行了给定次数的重试。如果OSU服务器904未随着这些重试作出响应,则移动设备900可能超时。

[0089] 需要注意的是,AAA服务器信任根是在凭证登记程序期间被提供给移动设备900的。对于使用了服务器凭证的那些EAP方法来说需要对AAA服务器凭证的验证。

[0090] 在交换924中,移动设备900向OSU服务器904发送sppPostDevData SOAP方法,包括

OMA-DM DevInfo和DevDetail管理对象。如果凭证登记成功了，则移动设备900可将requestReason的值设置成“凭证登记完成”，如果凭证登记失败了，则设置成“凭证登记失败”。

[0091] 在交换926中，如果凭证登记成功了，则OSU服务器904向移动设备900发送包括addMO命令和PerProviderSubscription管理对象的sppPostDevDataResponse SOAP方法。PerProviderSubscription管理对象包含将所配置的凭证绑定至订阅的凭证标识符以及辅助配置数据。在sppPostDevDataResponse SOAP方法中，sppStatus被设置成“配置完成”以表明订阅和凭证配置过程已经完成。

[0092] 如果凭证登记失败了，则OSU服务器904可通过下列操作之一进行响应。OSU服务器904可切换至配置机器管理的用户名/密码证书。在这种情况下，此交换中所返回的sppPostDevDataResponse SOAP方法可包含addMO命令和包含已配置的机器管理的用户名/密码证书的PerProviderSubscription管理对象。sppStatus可被设置成“配置完成”。

[0093] 或者，OSU服务器904可切换至配置用户所选择的用户名/密码证书。在这种情况下，此步骤中所返回的sppPostDevDataResponse SOAP方法可包含exec命令以针对所提供的URI启动浏览器。sppStatus可被设置成“OK”。消息流可如图8中所描述的进行至交换814。

[0094] 在又一示例中，OSU服务器904可放弃证书配置过程。在这种情况下，此步骤中所返回的sppPostDevDataResponse SOAP方法可包括被设置成“发生错误”的sppStatus，并且包括被设置成“此时无法配置证书”的errorCode(错误代码)的sppError元素可被返回。

[0095] 在交换928中，在交换908中所建立的TLS会话被发布。然后，移动设备900能够与热点902分离(如交换930中所示出的)，并且如932中所示出的，通过使用新建立的证书和主SSID 936关联热点902。

[0096] 图10示出了根据一些实施例的系统框图。图10示出了移动设备1000的框图。设备1000可包括处理器1004，存储器1006，收发器1008(包括至少一个天线1010)，指令1012、1014和可能的其他组件(未被示出)。尽管从框图的角度相似，但是对本领域的技术人员来说显而易见的是，不同的设备的操作的配置和细节可能是相似的或本质上不同的，这取决于具体的设备和职能。

[0097] 处理器1004包括一个或多个中央处理单元(CPU)、图形处理单元(GPU)、加速处理单元(APU)或它们的各种组合。处理器1004为设备1000提供处理和控制功能。

[0098] 存储器1006包括被配置成为设备1000存储指令和数据的一个或多个存储单元。收发器1008包括一个或多个收发器，其中该收发器包括用于适当的站点或响应者的用以支持多输入多输出(MIMO)通信的MIMO天线。尤其，收发器1008接收来自一个或多个网络中的其他设备的传输并将传输发送至一个或多个网络中的其他设备。

[0099] 指令1012、1014包括在计算设备(或机器)上执行以使这类计算设备(或机器)执行本文所讨论的任何方法的指令或软件的一个或多个集合。指令1012、1014(也被称为计算机或机器可执行指令)可在被设备1000执行期间完全或至少部分驻留在处理器1004和/或存储器1006内。尽管指令1012和1014被示为分离的，但是它们可以是同一整体的一部分。处理器1004和存储器1006还包括机器可读介质。

[0100] 在图10中，处理和控制功能被示为由处理器1004与相关联的指令1012、1014一起提供。然而，这些仅仅是包括(诸如，被包含在通用处理器或其他可编程处理器内的)可编程

逻辑或电路的处理电路的示例，其中可编程逻辑或电路由软件或固件临时配置以执行某些操作。在各实施例中，处理电路可包括(例如，在专用处理器、专用集成电路(ASIC)或阵列内)被永久配置以执行某些操作的专用电路或逻辑。应当理解的是对机械地实施处理电路、在专用和永久配置的电路中实施处理电路或在临时配置的(例如，由软件配置的)电路中实施处理电路的决定可由例如，成本、时间、能耗、包装尺寸或其他考量驱动。

[0101] 因此，术语“处理电路”应当被理解成包含有形的实体，即被物理构造的、永久配置的(例如，硬接线的)或临时配置的(例如，程序化的)用以按照本文所描述的某种方式运行或执行本文所描述的某些操作的实体。

[0102] 摘要被提供以遵守要求摘要的37C.F.R部分1.72(b)，这将使读者确定技术公开的本质和要点。这是在理解它将不被用于限制或解释权利要求的范围或含义的情况下被提交的。下面的权利要求据此被并入详细说明中，每一项权利要求作为单独的实施例独立存在。

[0103] 术语“计算机可读介质”、“机器可读介质”等等应当被视为包括存储一个或多个指令集的单个介质或多个介质(例如，集中式或分布式数据库和/或相关缓存和服务器)。该术语还应被视为包括能够存储、编码或携带由机器执行和使机器执行本公开的任何一个或多个方法的指令集的任何介质。因此，术语“计算机可读介质”、“机器可读介质”应被视为包括“计算机存储介质”、“机器存储介质”二者等等(有形来源包括固态存储器、光学和磁介质或其他有形设备和载体，而排除信号自身、载波和其他无形来源)以及“计算机通信介质”、“机器通信介质”等等(无形来源包括信号自身、载波信号等等)。

[0104] 出于清晰的目的，将理解的是上面的详细描述参考不同的功能单元或处理器描述了一些实施例。然而，功能在不同的功能单元、处理器或领域之间的功能的任何适当的分布均可被使用而不有损于本文的实施例。例如，所示出的由分开的处理器或控制器执行的功能可由同一处理器或控制器执行。因此，对具体功能单元的引用仅被视为对用于提供所描述的功能的适当方式的引用，而不是对严格的逻辑或物理结构或组织的说明。

[0105] 尽管本公开已经结合一些实施例进行了描述，然而不意图限制本文所提到的具体形式。本领域的技术人员将认识到所描述的实施例的各种特征可被合并。另外，将理解的是在不背离本公开的范围的情况下，本领域的技术人员可作出各种修改和改变。

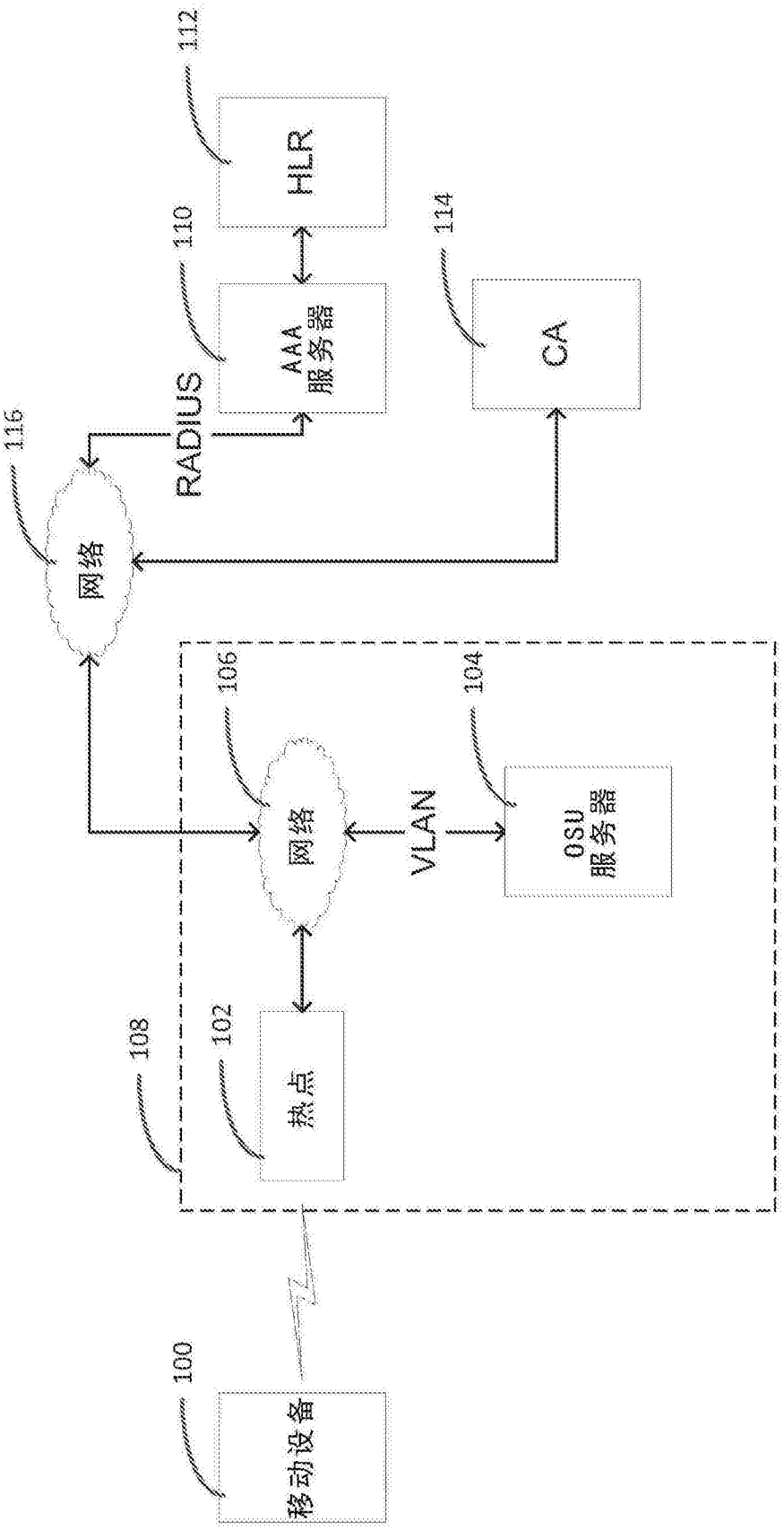

112
HLR
110
AAA
服务器
114
CA
RADIUS
116
网络
106
网络
104
VLAN
OSU
服务器
108
102
热点
100
移动设备

图1

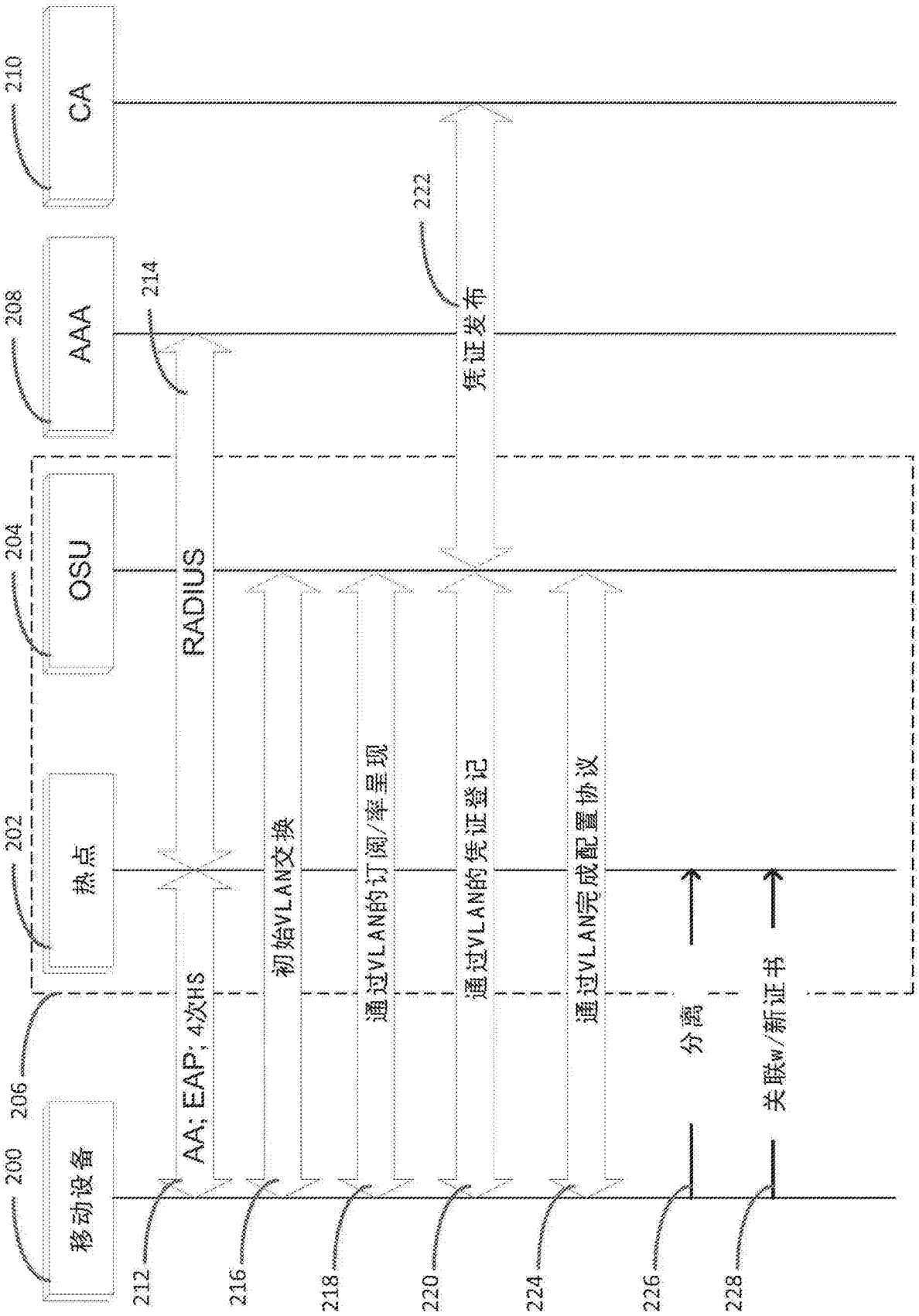

移动设备
200
热点
202
206
OSU
204
AAA
208
CA
210
AA; EAP; 4次HS
212
RADIUS
214
初始VLAN交换
216
通过VLAN的订阅/率呈现
218
通过VLAN的凭证登记
220
凭证发布
222
通过VLAN完成配置协议
224
分离
226
关联w/新证书
228

图2

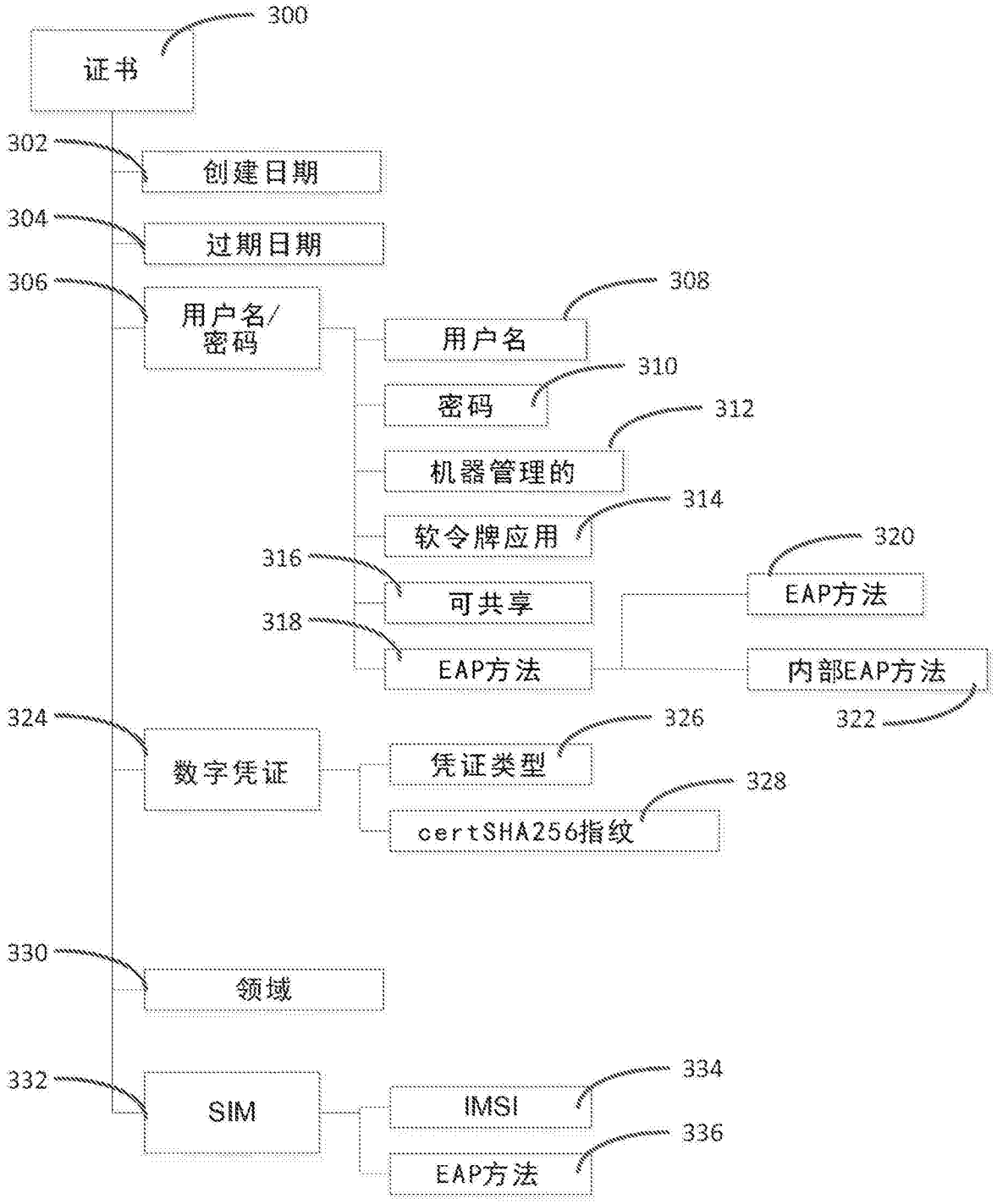

300
证书
302
创建日期
304
过期日期
306
用户名/
密码
308
用户名
310
密码
312
机器管理的
314
软令牌应用
316
可共享
318
EAP方法
320
EAP方法
内部EAP方法
322
324
数字凭证
326
凭证类型
328
certSHA256指纹
330
领域
332
SIM
334
IMSI
336
EAP方法

图3

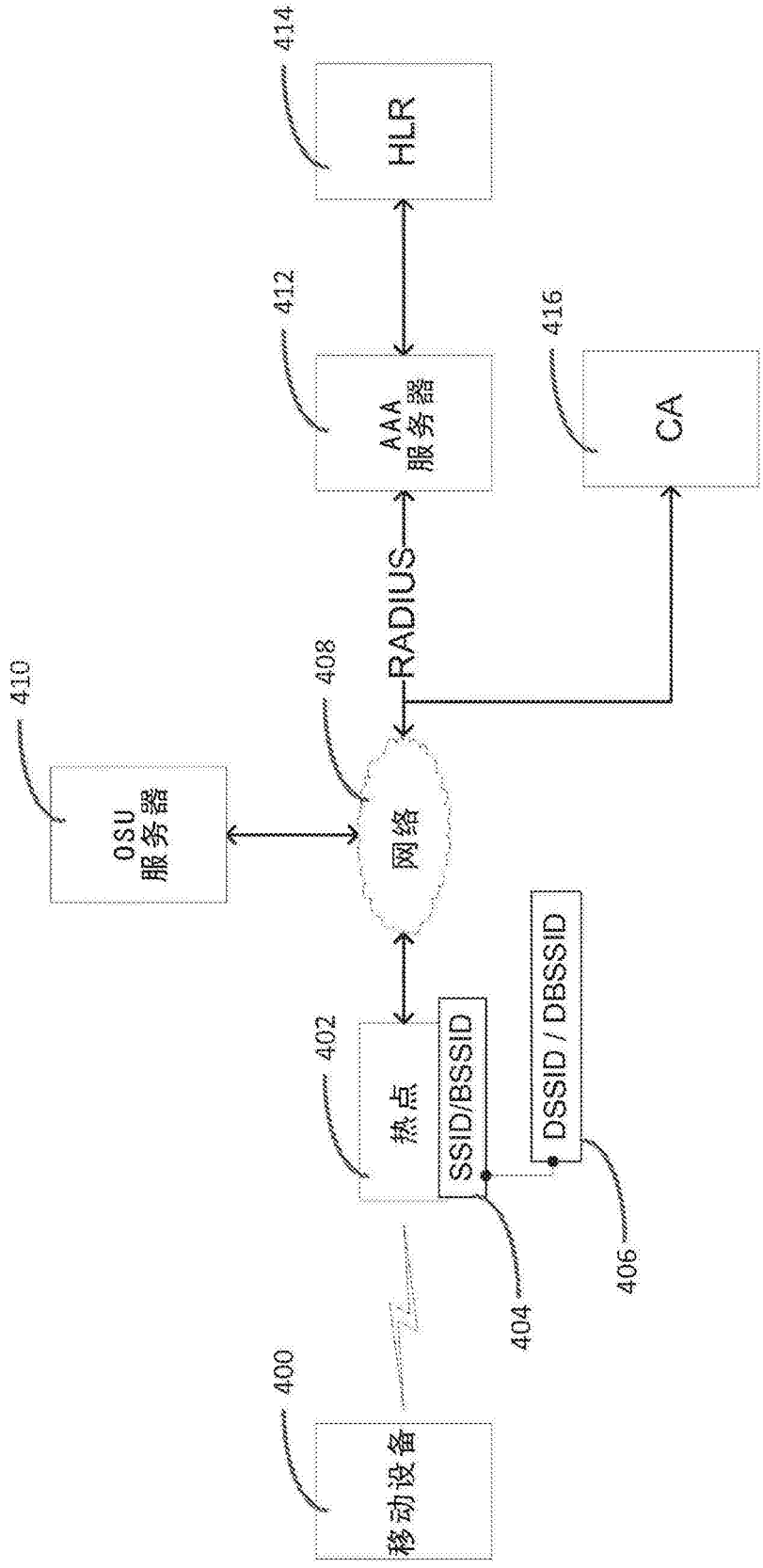

414
HLR
412
AAA
服务器
416
CA
RADIUS
410
OSU
服务器
408
网络
402
热点
SSID/BSSID
DSSID / DBSSID
404
406
400
移动设备

图4

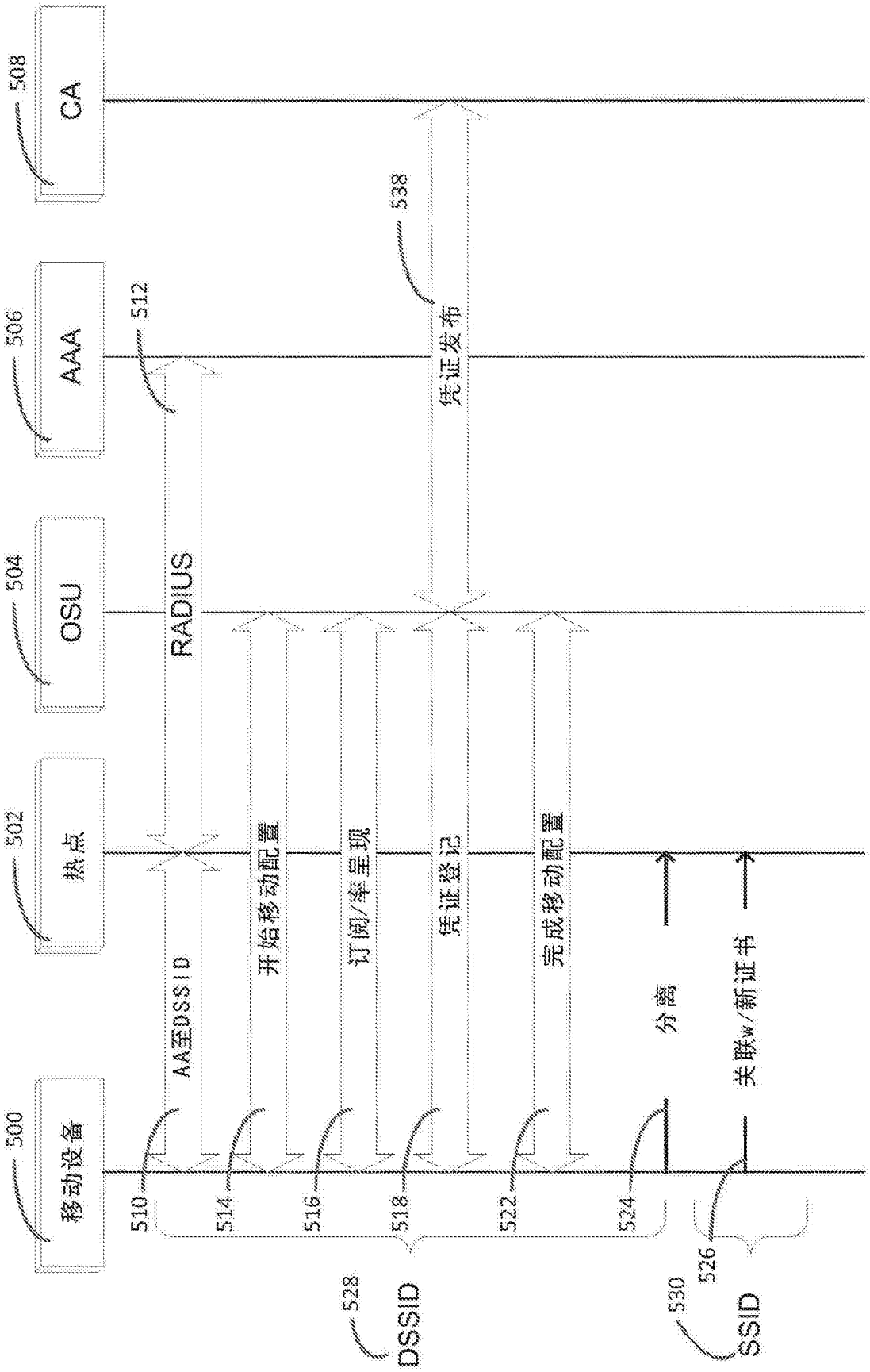

508
CA
538
506
AAA
512
凭证发布
504
OSU
RADIUS
502
热点
AA至DSSID
开始移动配置
订阅/率呈现
凭证登记
完成移动配置
分离
关联w/新证书
500
移动设备
510
514
516
518
522
524
526
528
DSSID
530
SSID

图5

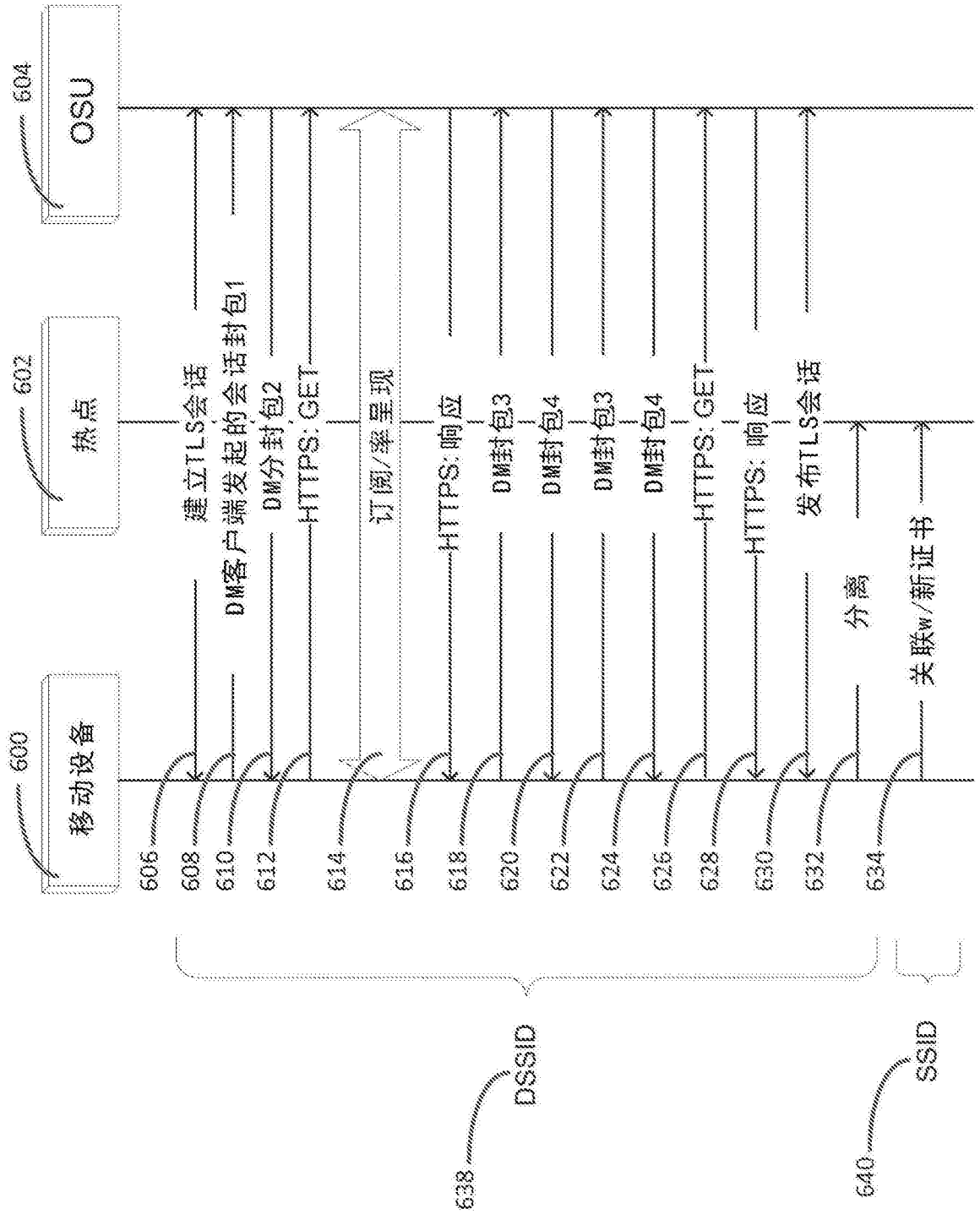

600
移动设备
602
热点
604
OSU
606
608
建立TLS会话
610
DM客户端发起的会话封包1
612
DM分封包2
614
HTTPS: GET
616
订阅/率呈现
618
HTTPS: 响应
620
DM封包3
622
DM封包4
624
DM封包3
626
DM封包4
628
HTTPS: GET
630
HTTPS: 响应
632
发布TLS会话
634
分离
关联w/新证书
638
DSSID
640
SSID

图6

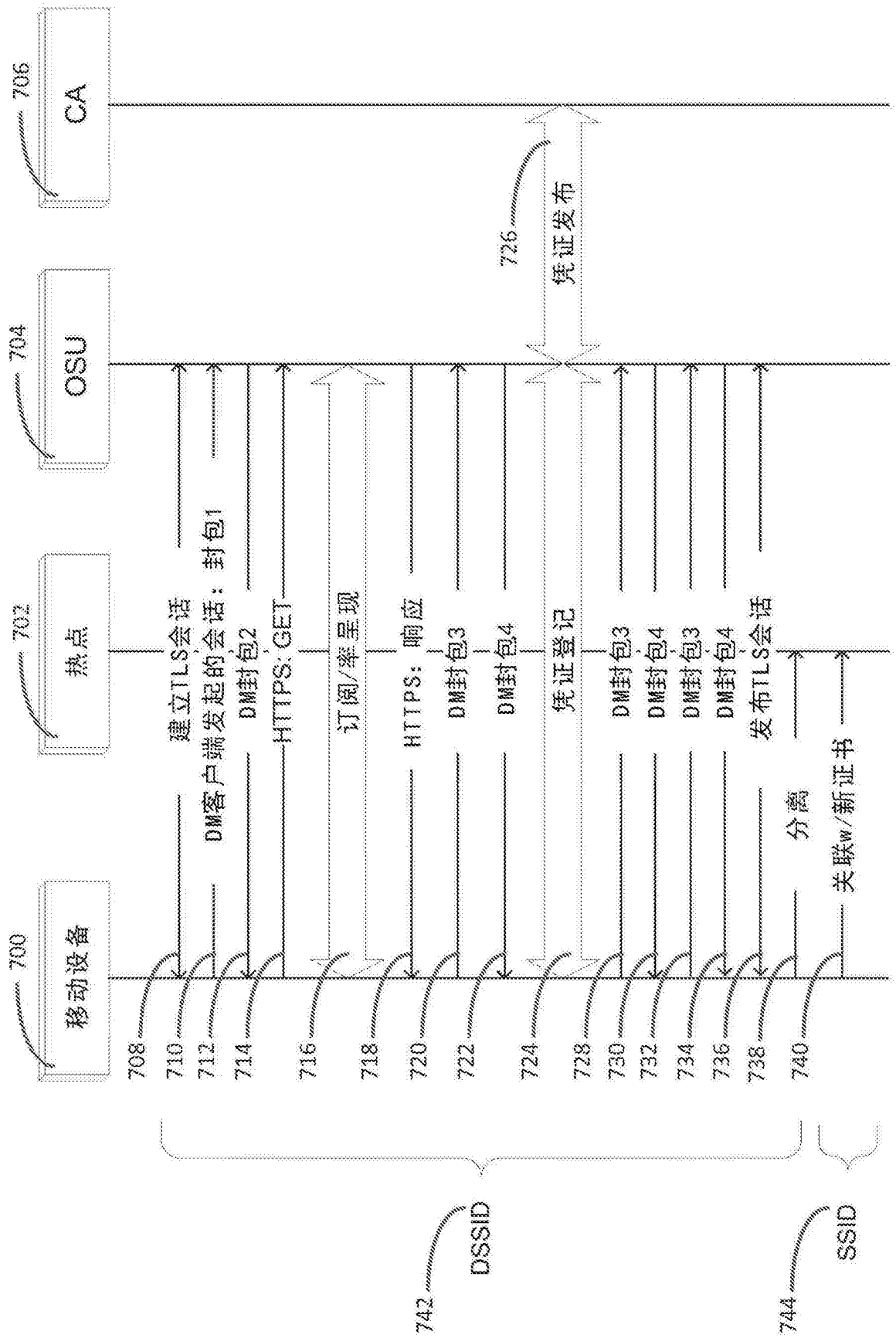

706
CA
704
OSU
702
热点
700
移动设备
726
凭证发布
建立TLS会话
DM客户端发起的会话：封包1
DM封包2
HTTPS: GET
订阅/率呈现
HTTPS：响应
DM封包3
DM封包4
凭证登记
DM封包3
DM封包4
DM封包3
DM封包4
发布TLS会话
分离
关联w/新证书
708
710
712
714
716
718
720
722
724
728
730
732
734
736
738
740
742
DSSID
744
SSID

图7

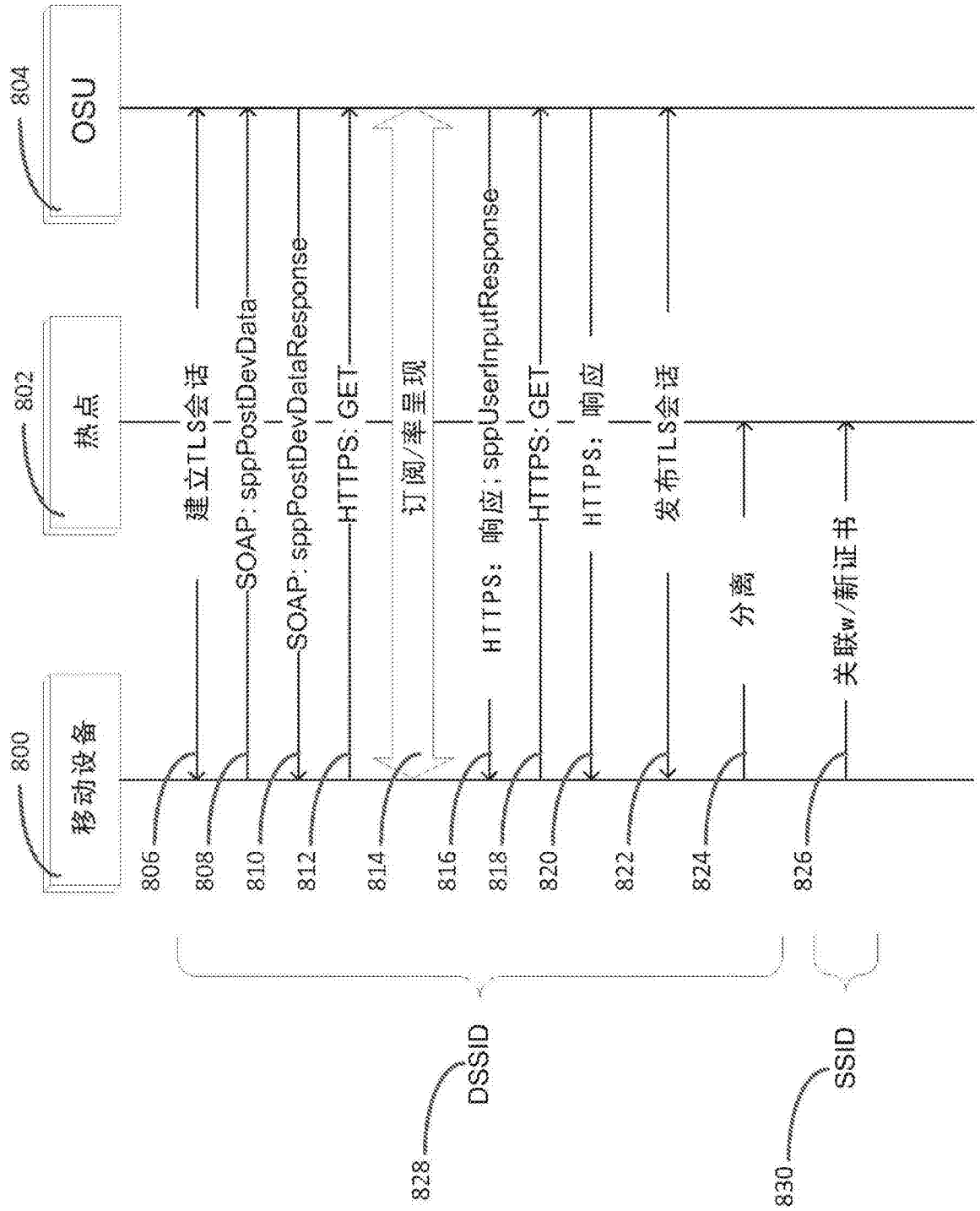

800
移动设备
802
热点
804
OSU
806
808
810
812
814
816
818
820
822
824
826
建立TLS会话
SOAP: sppPostDevData
SOAP: sppPostDevDataResponse
HTTPS: GET
订阅/率呈现
HTTPS：响应：sppUserInputResponse
HTTPS: GET
HTTPS：响应
发布TLS会话
分离
关联w/新证书
DSSID
828
SSID
830

图8

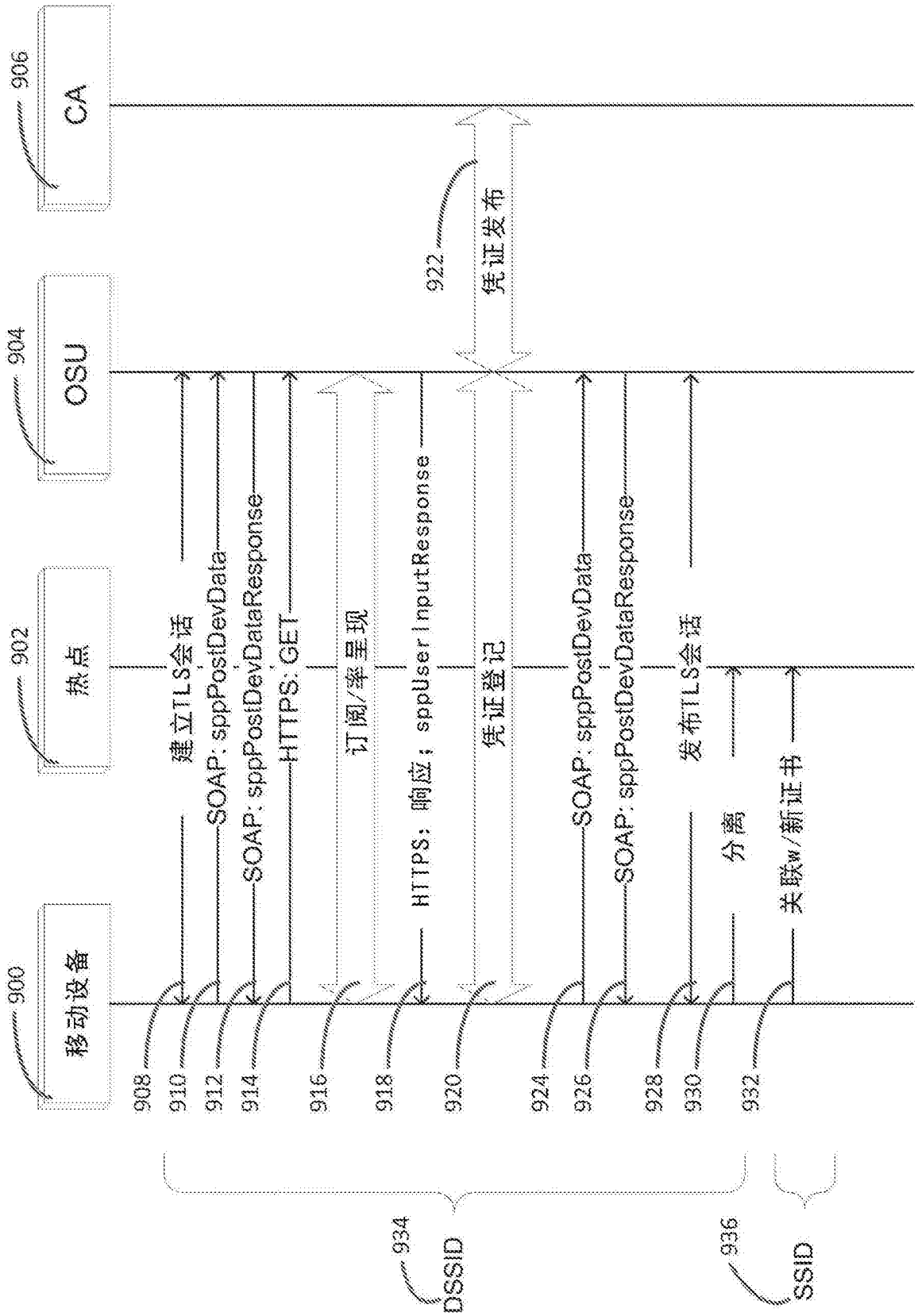

900
移动设备
902
热点
904
OSU
906
CA
908
910
建立TLS会话
912
SOAP: sppPostDevData
914
SOAP: sppPostDevDataResponse
916
HTTPS: GET
918
订阅/率呈现
920
HTTPS：响应；sppUserInputResponse
922
凭证发布
924
凭证登记
926
SOAP: sppPostDevData
928
SOAP: sppPostDevDataResponse
930
发布TLS会话
932
分离
关联w/新证书
934
DSSID
936
SSID

图9

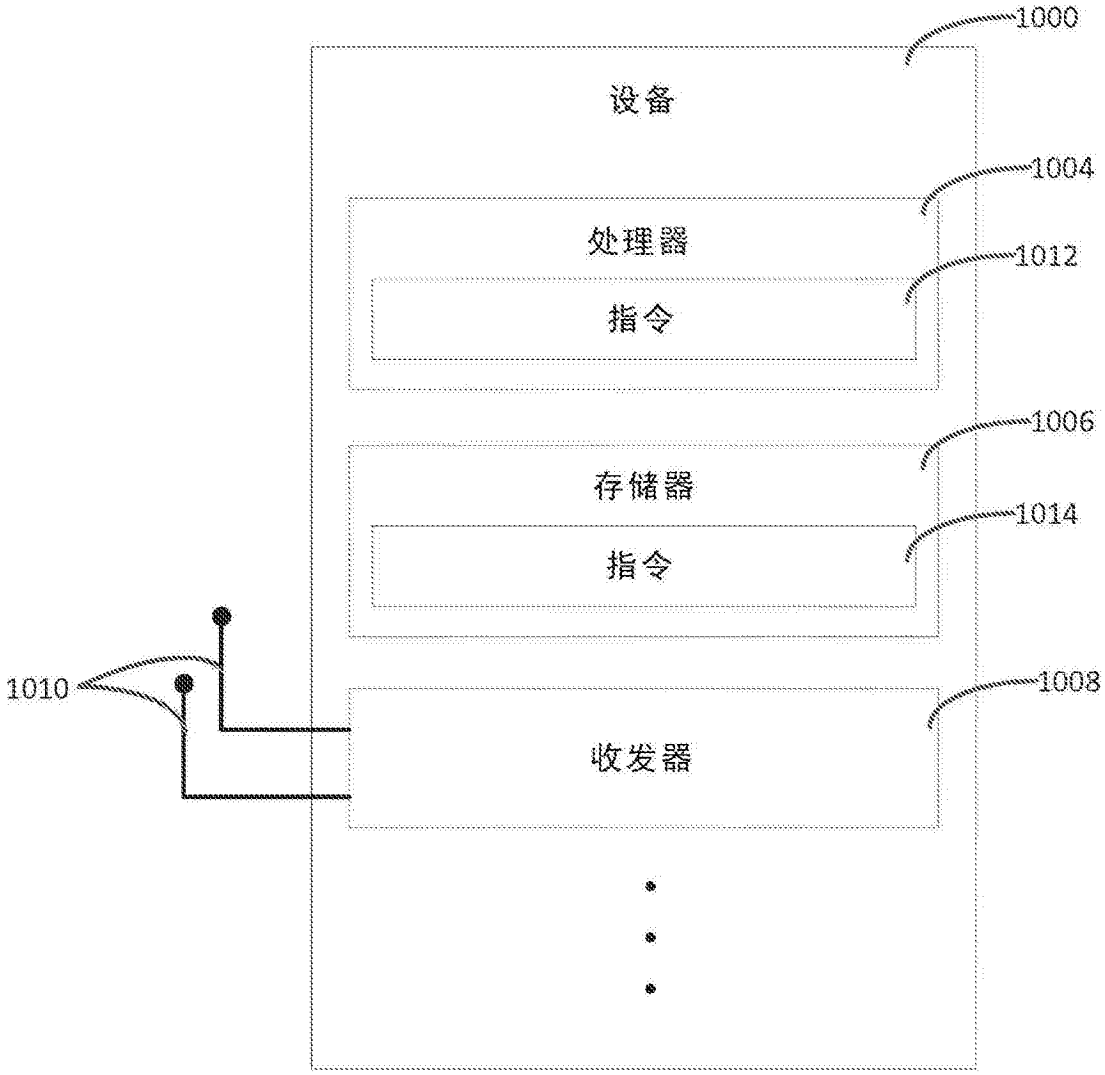


图10