(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 107690771 B
(45)授权公告日 2021.01.29

(21)申请号 201680030577.4
(22)申请日 2016.04.14
(65)同一申请的已公布的文献号
申请公布号 CN 107690771 A
(43)申请公布日 2018.02.13
(30)优先权数据
14/736,055 2015.06.10 US
(85)PCT国际申请进入国家阶段日
2017.11.27
(86)PCT国际申请的申请数据
PCT/US2016/027436 2016.04.14
(87)PCT国际申请的公布数据
WO2016/200482 EN 2016.12.15
(73)专利权人 高通股份有限公司
地址 美国加利福尼亚州
(72)发明人 李攘翁 阿南德·帕拉尼古德 李秀范 拉贾特·普拉卡什
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 陈炜
(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/08(2006.01)
(56)对比文件
US 2011047373 A1,2011.02.24
CN 1685706 A,2005.10.19
US 2011047373 A1,2011.02.24
CN 1685706 A,2005.10.19
CN 103167497 A,2013.06.19
CN 101287099 A,2008.10.15
US 2009235068 A1,2009.09.17
审查员 赵勇达

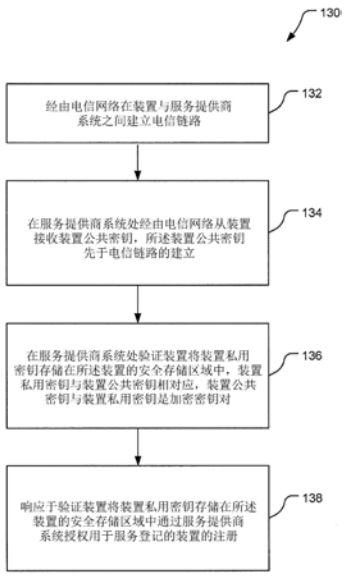
权利要求书4页 说明书14页 附图8页

(54)发明名称

用于证书管理的方法、设备和系统

(57)摘要

本发明提供一种用于证书管理的方法、设备和系统，所述方法包含：经由电信网络在装置与服务提供商系统之间建立电信链路；在所述服务提供商系统处经由所述电信网络从所述装置接收装置公共密钥，所述装置公共密钥先于所述电信链路的所述建立；在所述服务提供商系统处验证所述装置将装置私用密钥存储于所述装置的安全存储区域中，所述装置私用密钥与所述装置公共密钥相对应，所述装置公共密钥与所述装置私用密钥是加密密钥对；以及响应于验证所述装置将所述装置私用密钥存储于所述装置的所述安全存储区域中通过所述服务提供商系统授权用于服务登记的所述装置的注册。



CN 107690771 B

1.一种在服务提供商系统处执行的方法,其包括:

经由电信网络所述服务提供商系统与装置之间建立电信链路;

在所述服务提供商系统处经由所述电信网络从所述装置接收装置公共密钥,所述装置公共密钥先于所述电信链路的所述建立;

在所述服务提供商系统处验证所述装置是否将装置私用密钥存储在所述装置的安全存储区域中,所述装置私用密钥与所述装置公共密钥相对应,所述装置公共密钥与所述装置私用密钥是加密密钥对;以及

响应于验证所述装置将所述装置私用密钥存储在所述装置的所述安全存储区域中,由所述服务提供商系统授权所述装置对服务登记的注册。

2.根据权利要求1所述的方法,其中验证所述装置将所述装置私用密钥存储在所述装置的所述安全存储区域中包括如下中之一:

在与所述装置的制造商相关联的数据库中寻找所述装置公共密钥的指示,

或

在包括所述装置公共密钥且由受信任第三方证书颁发中心签名的证书中寻找安全密钥供应的指示。

3.根据权利要求1所述的方法,其中,所述装置公共密钥是装置证书的部分且所述装置公共密钥是由接收所述装置证书的所述服务提供商系统接收,并且其中对所述装置将所述装置私用密钥存储在所述装置的所述安全存储区域中的所述验证包括获得指示所述装置证书可信的装置根证书颁发中心证书,且针对将安全存储器用于所述装置私用密钥的指示而分析所述装置证书。

4.根据权利要求3所述的方法,其中所述分析包括针对将安全存储器用于所述装置私用密钥的所述指示而分析所述装置证书的扩展密钥使用部分。

5.根据权利要求1所述的方法,其中,授权所述装置对所述服务提供商系统的服务登记的注册包括:

在确定所述装置私用密钥存储在所述装置的所述安全存储区域中的情形下,向所述装置提供特定于服务提供商的定制证书。

6.根据权利要求5所述的方法,其进一步包括:

通过所述服务提供商系统产生服务提供商证书,其中所述服务提供商证书的公共密钥是所述装置公共密钥;

通过所述服务提供商系统对所述服务提供商证书进行签名以产生服务提供商签名证书;以及

将所述服务提供商签名证书从所述服务提供商系统发送到所述装置,

其中,所述特定于所述服务提供商的定制证书从所述服务提供商签名证书定制而来。

7.根据权利要求6所述的方法,其进一步包括:

基于所述服务提供商证书将证书签名请求从所述服务提供商系统的注册服务器发送到所述服务提供商系统的服务提供商证书颁发中心,所述服务提供商证书颁发中心执行所述服务提供商证书的所述签名;以及

在所述注册服务器处从所述服务提供商证书颁发中心接收所述服务提供商签名证书;

其中所述注册服务器执行所述服务提供商签名证书到所述装置的所述发送。

8.根据权利要求6所述的方法，其中执行所述服务提供商证书的所述产生以使得所述服务提供商证书的格式或内容中的至少一个是服务提供商服务器专用、服务提供商专用、装置用户专用、装置专用或订购专用中的至少一个。

9.一种服务提供商系统，其包括：

通信接口，其被配置成经由电信网络与装置建立电信链路；以及

基于硬件的处理器，其通信地耦合到所述通信接口且被配置成：

从所述装置接收装置公共密钥，所述装置公共密钥先于所述电信链路的所述建立；

验证所述装置是否将装置私用密钥存储在所述装置的安全存储区域中，所述装置私用密钥与所述装置公共密钥是加密密钥对；以及

响应于验证所述装置将所述装置私用密钥存储在所述装置的所述安全存储区域中，授权所述装置对服务登记的注册。

10.根据权利要求9所述的服务提供商系统，其中为了验证所述装置将所述装置私用密钥存储在所述装置的所述安全存储区域中，所述处理器被配置成：

在与所述装置的制造商相关联的数据库中寻找所述装置公共密钥的指示，或

在包括所述装置公共密钥且由受信任第三方证书颁发中心签名的证书中寻找安全密钥供应的指示。

11.根据权利要求9所述的服务提供商系统，其中所述装置公共密钥是装置证书的部分，且所述处理器被配置成通过接收所述装置证书来接收所述装置公共密钥，且其中为了验证所述装置将所述装置私用密钥存储在所述装置的所述安全存储区域中，所述处理器被配置成获得指示所述装置证书可信的装置根证书颁发中心证书，且针对将安全存储器用于所述装置私用密钥的指示而分析所述装置证书。

12.根据权利要求11所述的服务提供商系统，其中为了分析所述装置证书，所述处理器被配置成针对将安全存储器用于所述装置私用密钥的所述指示分析所述装置证书的扩展密钥使用部分。

13.根据权利要求9所述的服务提供商系统，其中，为授权所述装置对所述服务提供商系统的服务登记的注册，所述处理器配置成：

在确定所述装置私用密钥存储在所述装置的所述安全存储区域中的情形下，向所述装置提供特定于服务提供商的定制证书。

14.根据权利要求13所述的服务提供商系统，其中所述处理器进一步被配置成：

产生服务提供商证书，其中所述服务提供商证书的公共密钥是所述装置公共密钥；

对所述服务提供商证书进行签名以产生服务提供商签名证书；以及

将所述服务提供商签名证书发送到所述装置，

其中，所述特定于服务提供商的定制证书从所述服务提供商签名证书定制而来。

15.根据权利要求14所述的服务提供商系统，其中所述处理器进一步被配置成：

将证书签名请求从注册模块发送到服务提供商签名证书模块；

基于所述装置证书在所述服务提供商签名证书模块中产生所述服务提供商签名证书；

将所述服务提供商签名证书从所述服务提供商签名证书模块发送到所述注册模块；以及

在所述注册模块处从所述服务提供商签名证书模块接收所述服务提供商签名证书；

其中所述处理器被配置成将所述服务提供商签名证书从所述注册模块发送到所述装置。

16.根据权利要求14所述的服务提供商系统，其中所述处理器被配置成产生所述服务提供商证书，以使得所述服务提供商签名证书的格式或内容中的至少一个是服务提供商服务器专用、服务提供商专用、装置用户专用、装置专用或订购专用中的至少一个。

17.一种在通信装置处执行的方法，其包括：

经由电信网络在所述通信装置与服务提供商系统之间建立电信链路；

经由所述电信网络将装置证书从所述通信装置发送到所述服务提供商系统，所述装置证书包含装置公共密钥、装置标识和数字签名，所述装置公共密钥先于所述电信链路的所述建立，所述装置公共密钥与存储在所述通信装置的安全存储器中的装置私用密钥相对应，所述装置公共密钥与所述装置私用密钥是加密密钥对，所述装置证书进一步包含所述装置私用密钥存储在所述通信装置的所述安全存储器中的指示；以及

基于发送包含所述装置私用密钥存储在所述通信装置的所述安全存储器中的指示的所述装置证书，在所述通信装置处从所述服务提供商系统接收对所述通信装置注册服务登记的授权。

18.根据权利要求17所述的方法，其中发送所述装置证书包括将所述装置证书发送到多个服务提供商系统，所述方法进一步包括从所述多个服务提供商系统中的每一个接收相应的服务提供商签名证书。

19.根据权利要求18所述的方法，其中所述多个服务提供商签名证书中的每一个具有相应的服务提供商系统、相应的服务提供商、由所述通信装置的用户订购的服务、所述通信装置的用户或所述通信装置中的至少一个所专用的格式或内容中的至少一个。

20.根据权利要求17所述的方法，其进一步包括在所述通信装置的制造期间将所述装置私用密钥和所述装置公共密钥存储在所述通信装置中。

21.根据权利要求20所述的方法，其中在所述通信装置的制造期间所述存储将所述装置私用密钥存储在所述通信装置的受信任执行环境中。

22.根据权利要求17所述的方法，进一步包括：

从所述服务提供商系统接收特定于服务提供商的定制证书。

23.一种通信装置，其包括：

通信接口，其被配置成经由电信网络在所述通信装置与服务提供商系统之间建立电信链路；

安全存储器，其存储装置私用密钥；以及

处理器，其通信地耦合到所述通信接口和所述安全存储器且被配置成：

经由所述电信网络将装置证书从所述通信装置发送到所述服务提供商系统，所述装置证书包含与所述装置私用密钥相对应的装置公共密钥、装置标识和数字签名，所述装置公共密钥先于所述电信链路的建立，所述装置公共密钥与所述装置私用密钥是加密密钥对，所述装置证书进一步包含所述装置私用密钥存储在所述安全存储器中的指示；以及

基于发送包含所述装置私用密钥存储在所述通信装置的所述安全存储器中的指示的所述装置证书，经由所述通信接口从所述服务提供商系统接收与所述装置证书相对应的服务提供商签名证书或对所述通信装置注册服务登记的授权中的至少一个。

24.根据权利要求23所述的通信装置，其中所述处理器被配置成将所述装置证书发送到多个服务提供商系统并从所述多个服务提供商系统中的每一个接收相应的服务提供商签名证书。

25.根据权利要求24所述的通信装置，其中所述多个服务提供商签名证书中的每一个具有所述相应的服务提供商系统、相应的服务提供商、由所述通信装置的用户订购的服务、所述通信装置的用户或所述通信装置中的至少一个所专用的格式或内容中的至少一个。

26.根据权利要求23所述的通信装置，其中所述安全存储器是受信任执行环境。

27.根据权利要求23所述的通信装置，其中所述处理器进一步被配置成使用所述装置私用密钥来解密所述服务提供商签名证书。

28.根据权利要求23所述的通信装置，其中所述处理器进一步被配置成经由所述通信接口将所述服务提供商签名证书作为使服务提供商服务器将服务提供给所述通信装置的请求的至少部分发送到所述服务提供商服务器。

29.根据权利要求23所述的通信装置，其中所述处理器进一步配置成从所述服务提供商系统接收特定于服务提供商的定制证书。

用于证书管理的方法、设备和系统

背景技术

[0001] 电子通信通常用于获得广泛多种信息。举例来说，用户可获得当前或过去新闻、娱乐内容、研究信息、指导信息等。另外，所述信息可采取多种形式，例如出版物、图像、视频、音频和这些形式的组合。信息可使用提供接入和/或内容服务的一或多个服务提供商来获得。举例来说，信息可通过经由一或多个接入提供商(例如电信网络、网络网关等)与内容提供商通信并经由接入提供商从内容提供商下载所述信息的用户装置获得。所获得的信息可能是免费可用的获得，或可能需要由用户付费(例如付费订购)给内容提供商和/或接入提供商。举例来说，在服务提供商将向用户提供内容之前，用户可能需要向服务提供商付费订购。用户可能够从任何特定服务提供商中选择用户想要的服务，以使得不同服务提供商可向相同用户提供不同服务，且相同服务提供商可向不同用户提供不同服务。此外或替代地，用户可对接入网络付费，例如对通过宾馆所有的接入点接入到因特网而向宾馆付费。

[0002] 对于付费订购服务，确定请求方的真实性和所述请求方针对所请求服务的授权至关重要。用于获得所订购服务的一种现有技术使用户在服务登记期间建立用户名和密码。替代地，用户名和密码可至少初始地由服务提供商提供。每当服务是所期望的时，则使用用户名和密码。用于获得所订购服务的另一技术使装置将相同装置证书提供给每一服务提供商(来自其的服务是所期望的中)。证书包含信息，例如装置标识、与所述装置相关联的公开加密密钥(公共密钥)(即与由装置存储的私用密钥相对应)和数字签名。在用于每一服务提供商(SP)的相同装置证书的情况下，与提供可包含服务提供商专用(SP专用)信息(例如授权(例如付费)服务、用户的订购到期等)的定制证书的服务提供商相比，所述证书不具有可定制性。用于获得所订购服务的另一现有技术使服务提供商服务器提供可包含SP专用信息的定制证书。在这种技术中，用户装置和服务提供商服务器发起通信，且公共密钥/私用密钥对由与特定服务提供商相关联的用户装置产生。可不对所述密钥提供安全密钥供应，其中密钥对存储在可接入到外部源的高级操作系统(HLOS)存储器中。替代地，可对所述密钥提供安全密钥供应，其中私用密钥存储在安全存储器中，要求昂贵的硬件以容纳任何显著数量的服务提供商。虽然这种技术提供定制证书，但是要求密钥对的存储器是繁重的，如果私用密钥不存储在安全存储器中，那么导致安全问题，且确切地说，如果私用密钥存储在安全存储器中，那么增加用户订购的每一相异服务提供商的成本。

发明内容

[0003] 一种方法的实例包含：经由电信网络在装置与服务提供商系统之间建立电信链路；在服务提供商系统处经由电信网络从装置接收装置公共密钥，所述装置公共密钥先于电信链路的建立；在服务提供商系统处验证装置将装置私用密钥存储在装置的安全存储区域中，装置私用密钥与装置公共密钥相对应，装置公钥与装置私钥是加密钥对；以及响应于验证装置将装置私钥存储在所述装置的安全存储区域中而通过服务提供商系统授权用于服务登记的装置的注册。

[0004] 这类方法的实施方案可包含以下特征中的一或多个。验证装置将装置私用密钥存

储在所述装置的安全存储区域中包括在与装置的制造商相关联的白名单数据库中寻找装置公共密钥的指示。装置公共密钥是装置证书的部分且装置公共密钥由接收装置证书的服务提供商系统接收，且对装置将装置私用密钥存储在装置的安全存储区域中的验证包括获得指示装置证书可信的装置根证书颁发中心证书，且针对将安全存储器用于装置私用密钥的指示分析装置证书。所述分析包括针对将安全存储器用于装置私用密钥的指示而分析装置证书的扩展密钥使用部分。方法进一步包含：通过服务提供商系统产生服务提供商证书，其中服务提供商证书的公共密钥是装置公共密钥；通过服务提供商系统对服务提供商证书进行签名以产生服务提供商签名证书；以及将服务提供商签名证书从服务提供商系统发送到装置。方法进一步包含：基于服务提供商证书将证书签名请求从服务提供商系统的注册服务器发送到服务提供商系统的服务提供商证书颁发中心，所述服务提供商证书颁发中心执行服务提供商证书的签名；以及在注册服务器处从服务提供商证书颁发中心接收服务提供商签名证书；其中所述注册服务器执行服务提供商签名证书到装置的发送。执行服务提供商证书的产生以使得服务提供商证书的格式或内容中的至少一个是服务提供商服务器专用、服务提供商专用、装置用户专用、装置专用或订购专用中的至少一个。

[0005] 一种服务提供商系统的实例包含：被配置成经由电信网络与装置建立电信链路的通信接口；和通信地耦合到通信接口并被配置成进行以下操作的处理器：从装置接收装置公共密钥，所述装置公共密钥先于电信链路的建立；验证装置将装置私用密钥存储在装置的安全存储区域中，装置私用密钥与装置公共密钥是加密密钥对；且响应于验证装置将装置私用密钥存储在装置的安全存储区域中而授权用于服务登记的装置的注册。

[0006] 这种服务提供商系统的实施方案可包含以下特征中的一或多个。为了验证装置将装置私用密钥存储在所述装置的安全存储区域中，处理器被配置成在与装置的制造商相关联的白名单数据库中寻找装置公共密钥的指示。装置公共密钥是装置证书的部分且处理器被配置成通过接收装置证书来接收装置公共密钥，且其中为了验证装置将装置私用密钥存储在所述装置的安全存储区域中，处理器被配置成获得指示装置证书可信的装置根证书颁发中心证书，且针对将安全存储器用于装置私用密钥的指示分析装置证书。为了分析装置证书，处理器被配置成针对将安全存储器用于装置私用密钥的指示而分析装置证书的扩展密钥使用部分。处理器进一步被配置成：产生服务提供商证书，其中服务提供商证书的公共密钥是装置公共密钥；对服务提供商证书进行签名以产生服务提供商签名证书；且将服务提供商签名证书发送到装置。处理器进一步被配置成：将证书签名请求从注册模块发送到服务提供商签名证书模块；基于装置证书在服务提供商签名证书模块中产生服务提供商签名证书；将服务提供商签名证书从服务提供商签名证书模块发送到注册模块；且在注册模块处从服务提供商签名证书模块接收服务提供商签名证书；其中处理器被配置成将服务提供商签名证书从注册模块发送到装置。处理器被配置成产生服务提供商证书，以使得服务提供商签名证书的格式或内容中的至少一个是服务提供商服务器专用、服务提供商专用、装置用户专用、装置专用或订购专用中的至少一个。

[0007] 一种方法的另一实例包含：经由电信网络在装置与服务提供商系统之间建立电信链路；经由电信网络将装置证书从装置发送到服务提供商系统，所述装置证书包含装置公共密钥、装置标识和数字签名，所述装置公共密钥先于电信链路的建立，所述装置公共密钥与存储在装置的安全存储器中的装置私用密钥相对应，装置公共密钥与装置私用密钥是加

密密钥对，所述装置证书进一步包含装置私用密钥存储在所述装置安全存储器中的指示；以及在装置处从服务提供商系统接收与装置证书相对应的服务提供商签名证书，或注册用于服务登记的装置的授权中的至少一个。

[0008] 这类方法的实施方案可包含以下特征中的一或多个。发送装置证书包括将装置证书发送到多个服务提供商系统，且进一步包括接收的方法包括从服务提供商系统中的每一个接收相应的服务提供商签名证书。服务提供商签名证书中的每一个具有相应的服务提供商系统、相应的服务提供商、由装置的用户订购的服务、装置的用户或装置中的至少一个所专用的格式或内容中的至少一个。所述方法进一步包含在装置的制造期间将装置私用密钥和装置公共密钥存储在装置中。在装置的制造期间所述存储将装置私用密钥存储在装置的受信任执行环境中。

[0009] 一种装置的实例包含：被配置成经由电信网络在装置与服务提供商系统之间建立电信链路的通信接口；存储装置私用密钥的安全存储器；和通信地耦合到通信接口和安全存储器并被配置成进行以下操作的处理器：经由电信网络将装置证书从装置发送到服务提供商系统，所述装置证书包含与装置私用密钥相对应的装置公共密钥、装置标识和数字签名，所述装置公共密钥先于电信链路的建立，装置公共密钥与装置私用密钥是加密密钥对，所述装置证书进一步包含装置私用密钥存储在安全存储器中的指示；且经由通信接口从服务提供商系统接收与装置证书相对应的服务提供商签名证书，或注册用于服务登记的装置的授权中的至少一个。

[0010] 这类装置的实施方案可包含以下特征中的一或多个。处理器被配置成将装置证书发送到多个服务提供商系统且从所述服务提供商系统中的每一个接收相应的服务提供商签名证书。服务提供商签名凭证中的每一个具有相应的服务提供商系统、相应的服务提供商、由装置的用户订购的服务、装置的用户或装置中的至少一个所专用的格式或内容中的至少一个。安全存储器是受信任执行环境。处理器进一步被配置成使用装置私用密钥来解密服务提供商签名证书。处理器进一步被配置成经由通信接口将服务提供商签名证书作为使服务提供商服务器向装置提供服务的请求的至少部分发送到服务提供商服务器。

附图说明

[0011] 图1是电信系统的简化图。

[0012] 图2是展示于图1中的用户装置的框图。

[0013] 图3是展示于图2中的用户装置的功能框图。

[0014] 图4是展示于图1中的服务提供商系统的框图。

[0015] 图5是展示于图4中的服务提供商系统的功能框图。

[0016] 图6是授权注册和/或提供SP签名证书的过程的流程框图。

[0017] 图7是注册和/或请求SP签名证书的过程的流程框图。

[0018] 图8是在线订购和接收服务的过程的流程框图。

[0019] 图9是获得SP签名证书且使用所述SP签名证书来获得在线服务的消息流程图。

[0020] 图10是另一电信系统的简化图。

具体实施方式

[0021] 本文中论述用于服务的在线注册、用于针对获得服务而获得服务提供商签名证书(SP签名证书)获得和用于使用SP签名证书以获得所述服务的技术。举例来说，优选地在用户装置的制造期间产生加密密钥对，包含装置私用密钥和装置公共密钥。装置私用密钥存储在用户装置的安全存储区域或安全存储器中，例如受信任执行环境。用户装置经由通信网络联系在线注册服务器(OSUS)和OSUS认证用户装置。所述装置将装置公共密钥提供给OSUS且OSUS验证用户装置使用安全密钥供应，即与装置公共密钥相对应的装置私用密钥安全地存储在用户装置处。举例来说，OSUS在白名单数据库中寻找装置公共密钥或在含有装置公共密钥且由受信任第三方证书颁发中心签名的证书中寻找安全密钥供应的指示。一旦安全密钥供应被验证，OSUS就授权用户装置注册服务。用户给OSUS提供用户信息，包含付费信息和一或多个所期望服务的指示。将关于所订购服务和用户装置使用安全密钥供应的指示提供给服务提供商系统的服务提供商服务器。所述指示可由OSUS提供，或可由将装置证书和所订购服务的指示发送到服务提供商服务器的用户装置，或由其它技术提供。优选地，所述装置将装置证书提供给服务提供商服务器，服务提供商证书颁发中心对装置证书签名以产生SP签名证书，且服务提供商服务器将SP签名证书提供给用户装置。SP签名证书可经定制，例如基于所订购服务、用户装置、用户、服务提供商和/或服务提供商服务器。如果所请求服务是由用户装置订购，那么用户可请求服务且用户装置应将SP签名证书发送到将通过提供所请求服务(例如网络接入、内容等)来答复的服务提供商服务器(其可与提供SP签名证书的服务提供商服务器分离)。然而，这些实例并不是穷尽性的。

[0022] 本文中所描述的项目和/或技术可以提供以下能力中的一或多个以及未提及的其它能力。提供了较强的装置证书安全性和动态定制SP签名证书登记。用于不同服务提供商中的每一个的定制证书可由装置存储，但仅在装置中存储一个装置私用密钥，或至少不存储用于每一服务提供商的不同装置私用密钥。用于不同服务提供商中的每一个的定制证书可由装置来存储，其中每一定制证书含有定制信息(例如服务提供商信息、服务提供商所期望的定制格式和定制内容)，其中定制信息潜在地促进从服务提供商获得服务。可提供其它能力，且并不是根据本公开的每个实施方案都必须提供所论述能力中的任何一个，更不用说全部。

[0023] 参看图1，电信系统10包含用户装置12、接入点(AP)14、电信网络16、服务提供商系统18_1-18_2和白名单数据库20。系统10是电信系统，其中系统10的组件可彼此直接或间接地通信，例如经由电信网络16和/或接入点14(和/或未展示的一或多个其它装置，例如一或多个基地收发站，例如蜂窝塔)中的一或多者。所展示的实例用户装置12包含移动手机(包含智能手机)、笔记本计算机和平板计算机。还可使用其它用户装置，无论是当前现有的或将来开发的。虽然所展示的用户装置12是移动装置，但是仍可使用例如台式计算机、电视和/或通常不被视为移动装置的其它用户装置的用户装置。用户装置12是电信装置，即每一装置具有电信能力，即使这并不是装置的初始目的。

[0024] 尽管在图1中仅展示服务提供商系统18中的一个，此处为系统18_1，但是服务提供商系统18_1-18_2中的每一个包含注册服务器30、服务提供商服务器32或服务提供商证书颁发中心34中的一或多个。为简单起见，以下论述将服务提供商系统18_1笼统地识别为不具有下标的服务提供商系统18。注册服务器30被配置成认证联系注册服务器30的用户装置12中的

任何一个以验证安全密钥供应是由用户装置12使用，且从用户装置12获得用户信息(例如以识别所期望服务且提供所要求信息(例如付费信息))。服务提供商服务器32被配置成验证用户装置12使用安全密钥供应，以从服务提供商证书颁发中心34获得关于装置证书的签名来产生SP签名证书，且提供例如因特网接入或内容呈现的经授权(例如所订购)服务。服务提供商证书颁发中心34被配置成通过对由服务提供商服务器提供的装置证书签名来产生SP签名证书，且将SP签名证书提供给服务提供商服务器32以待提供给用户装置12。下文更详细地论述服务器30、32和证书颁发中心34。

[0025] 白名单数据库20存储关于采用安全密钥供应且由特定制造商制造的用户装置的信息。尽管为简单起见在图1中展示仅一个数据库，但将使用其它数据库，优选地其中每一数据库存储仅用于由对应制造商制造的装置的信息。数据库20存储与对应装置公共密钥相关联的用户装置的装置标识(ID)。白名单数据库20优选地存储仅用于使用安全密钥供应的用户装置12的ID和装置公共密钥，即每一白名单数据库将其相应的装置私用密钥存储在相应的用户装置12中的安全存储器中。替代地，数据库20可存储用于使用安全密钥供应的用户装置12和并不使用安全密钥供应的用户装置的装置ID和装置公共密钥。在此情况下，数据库20将提供哪些装置ID对应于使用安全密钥供应的用户装置12的指示。

[0026] 还参看图2，用户装置12中的一个的实例包括处理器40、接口49和包含安全存储区域(此处受信任执行环境(TEE)44、高级操作系统(HLOS)46和软件(SW)48)的存储器42。TEE 44是安全元件，其中TEE 44防止(若不是不可接入的)由元件外部的实体接入。相反地，HLOS 46较不安全且可从用户装置12外部的实体接入，使得HLOS易受黑客影响。处理器40优选地是例如中央处理单元(CPU)(例如由QUALCOMM®、ARM®、Intel®公司或AMD®制造或设计的那些)的智能硬件装置、微控制器、专用集成电路(ASIC)等。处理器40可包括可分布在用户装置12中的多个独立的物理实体。存储器42可包含随机存取存储器(RAM)和/或只读存储器(ROM)。存储器42是处理器可读存储媒体，其存储软件48，所述软件是处理器可读、处理器可执行的软件代码，所述软件代码含有被配置成在执行时使得处理器40执行本文中所描述的各种功能的指令(但所述描述可仅指代执行所述功能的处理器40)。替代地，软件48可能不可由处理器40直接执行，而是可被配置成(例如)在被编译和执行时使处理器40执行所述功能。处理器40通信地耦合到存储器42，即处理器40和存储器42被配置成彼此直接和/或间接地通信。接口49与处理器40通信地耦合且被配置成与AP 14、网络16和/或例如基地收发站的其它通信装置直接或间接地双向通信。接口49可建立到服务提供商系统18的电信链路，例如通过直接或间接地建立到网络16的电信链路，且网络16根据来自接口49的请求直接或间接地建立到服务提供商系统16的电信链路。接口49可因此将信息从处理器40发送到用户装置12外部的实体，且从用户装置12外部的实体接收信息并将此信息传递到处理器40。

[0027] 还参看图3，用户装置12包含处理器模块60，所述处理器模块包含装置密钥/证书模块(用于产生且提供装置密钥和装置证书的装置)50、注册模块(用于注册的装置和用于登记的装置)52和服务获取模块(用于获取服务的装置、用于获得服务的装置)54。模块60、50、52和54是由处理器40和存储于存储器42中的软件48实施的功能模块。因此，对执行或被配置成执行功能的模块60、50、52和54中的任何一个的参考是执行或被配置成执行根据软件42(和/或固件，和/或处理器40的硬件)的功能的处理器40的简要表述。类似地，对执行用

于产生或提供装置证书、注册用户装置12、登记用户装置12或获取或获得服务的功能的处理器40的参考等效于分别执行所述功能的装置证书模块50、注册模块52或服务获取模块54。

[0028] 装置密钥/证书模块50被配置成在用户装置12中启用和实施安全密钥供应。模块50被配置成例如在用户装置12的制造期间与用户装置12外部的实体交互以产生包含装置公共密钥和装置私用密钥的加密密钥对。模块50被配置成将装置私用密钥存储在安全存储器中，以使得装置私用密钥极不可能(如果不是不可能)从用户装置12外部的实体接入和/或由所述实体修改。举例来说，模块50可被配置成将装置私用密钥存储在TEE 44中且将装置公共密钥存储在HLOS 46中。模块50可被配置成将装置公共密钥发送到注册模块52但保持装置私用密钥加密，不与用户装置12外部的实体共享装置私用密钥(即将装置私用密钥发送到这类实体或允许由这类实体接入装置私用密钥)。

[0029] 另外，装置密钥/证书模块50可被配置成产生且提供装置证书。装置密钥/证书模块50可被配置成编译适当的信息以形成装置证书。装置证书优选地包含识别用户装置12、装置公共密钥和用于所述装置证书的数字签名的装置ID。模块50可被配置成使用已知技术产生装置证书的数字签名从而提供自签名装置证书。同样或替代地，模块50可被配置成获得证书授权签名装置证书。在此情况下，模块50被配置成通过接口49与第三方认证颁发中心(CA)22(参见图10)交互以给第三方CA 22提供装置证书信息，且从第三方CA 22接收装置证书，其中所述装置证书包含由第三方CA 22产生的数字签名。模块50被配置成将装置公共密钥提供给注册服务器30和/或将装置证书提供给注册模块52。

[0030] 注册模块52被配置成利用服务提供商系统18，确切地说利用注册服务器30注册且登记用户装置12以用于在线服务。模块52被配置成通过经由接口49联系服务提供商系统18且通过接口49将装置公共密钥和/或装置证书从装置密钥/证书模块50提供给服务提供商系统18来发起注册过程。模块52进一步被配置成与系统18双向通信以提供系统18所请求的信息。举例来说，注册模块52可提供用户信息、用户名、密码、付费信息(例如信用卡或银行账户信息)、所期望服务的指示和/或服务的所期望订购的长度，和/或其它信息。注册模块52可包含用户接口，用户通过所述用户接口提供用户信息。所期望服务可包含(例如)内容的类型(例如音频、视频、电影、电视节目等)和/或服务的格式(例如下载速率(例如5MB对20MB等))。另外，虽然本文中术语“服务”指代以单数形式，但如本文中所使用的术语“服务”还包含多个(服务)且因此对应术语(例如指示)也包含多个。也就是说，用户可订购单个服务或多个服务，即使描述以单数形式使用“服务”。因此，术语“服务”既不要求也不排除多于一个服务。注册模块52进一步被配置成从注册服务器30接收SP签名证书(下文进一步论述)且将SP签名证书提供给服务获取模块54。

[0031] 服务获取模块54被配置成从服务提供商系统18获取或获得服务。服务获取模块54被配置成将服务的服务请求发送到服务提供商系统18。所述服务请求可以是单个通信或多于一个通信且包含经由注册模块52从注册服务器30接收到的SP签名证书。服务提供商系统18(模块54将服务请求发送到此处)可以是提供SP签名证书的相同服务提供商系统18或可以是另一物理上相异的服务提供商系统18。模块54被配置成接收例如通信网络(例如因特网)接入的服务或内容(例如流式视频信号)，且将接收到的服务提供给处理器40以用于进一步适当的处理，例如通过网络建立到内容提供商的连接、将内容转发到显示器和/或扬声

器以供呈现给用户装置12的用户等。

[0032] 参看图4,进一步参看图1,服务提供商系统18中的一个的实例包括处理器70、包含软件(SW)74的存储器72和接口76。处理器70优选地是例如中央处理单元(CPU)(例如由QUALCOMM®、ARM®、Intel®公司或AMD®制造或设计的那些)的智能硬件装置、微控制器、专用集成电路(ASIC)等。处理器70可包括可分布在服务提供商系统18中的多个独立的物理实体。存储器72可包含随机存取存储器(RAM)和/或只读存储器(ROM)。存储器72是处理器可读存储媒体,其存储软件74,所述软件是处理器可读、处理器可执行的软件代码,所述软件代码含有被配置成在执行时使得处理器70执行本文中所描述的各种功能的指令(但所述描述可仅指代执行所述功能的处理器70)。替代地,软件74可能不可由处理器70直接执行,而是可被配置成(例如)在被编译和执行时使处理器70执行所述功能。处理器70通信地耦合到存储器72,即处理器70和存储器72被配置成彼此直接和/或间接地通信。接口76与处理器70通信地耦合且被配置成与AP 14、网络16和/或例如基地收发站的其它通信装置直接或间接地双向通信。接口76可与用户装置12中的任一个建立电信链路,例如通过直接或间接地建立到网络16的电信链路,其中网络16通常已根据来自用户装置12的请求直接或间接地建立到用户装置12的电信链路。接口76可因此将信息从处理器70发送到服务提供商系统18外部的实体,且从服务提供商系统18外部的实体接收信息且将此信息传递到处理器70。

[0033] 还参看图5,服务提供商系统18包含处理器模块80,所述处理器模块包含安全密钥验证模块(用于验证的装置)82、注册模块(用于注册的装置)84、SP签名证书模块(用于提供SP签名证书的装置)86和服务模块(用于提供服务的装置)88。服务模块88包含认证、授权和记账(AAA)服务器。模块80、82、84、86和88是由处理器70和存储于存储器72中的软件74实施的功能模块。因此,对执行或被配置成执行功能的模块80、82、84、86、88中的任一个的参考是执行或被配置成根据软件74(和/或固件,和/或处理器70的硬件)执行功能的处理器70的简要表述。类似地,对执行用于验证安全密钥供应是由用户装置12实施、注册用户装置12、产生或提供SP签名证书,或将服务提供给用户装置12的功能的处理器70的参考等效于分别执行所述功能的安全密钥验证模块82、注册模块84、SP签名证书模块86或服务模块88。

[0034] 如图1中所展示,服务提供商系统18可包含注册服务器30和服务提供商服务器32,以及服务提供商证书颁发中心34。因此,处理器70、包含软件74的存储器72,和接口76可以是安置于多个物理上独立的装置中的多个物理上独立的设备,但为简单起见,在图4中展示为单个系统中的单个设备。安全密钥验证模块82和注册模块84优选地完全实施于注册服务器30中。另外,SP签名证书模块86优选地完全实施于如下文另外所论述的服务提供商证书颁发中心34中,且服务模块88优选地完全实施于服务提供商服务器32中。

[0035] 安全密钥验证模块82被配置成认证请求用户装置12以验证请求用户装置12是否使用安全密钥供应,且至少告知注册模块52用户装置12是否使用安全密钥供应。模块82被配置成分析由用户装置12提供的装置公共密钥或装置证书以认证用户装置12。举例来说,模块82可被配置成确定据称来自用户装置12的请求是否确实来自用户装置12且尚未变更。另外,模块82被配置成分析已认证请求以便确定用户装置12是否使用安全密钥供应。举例来说,模块82被配置成读取发送到模块82的装置公共密钥,无论装置公共密钥是否是装置证书的部分。如果装置公共密钥不是装置证书的部分,那么模块82读取来自从用户装置12接收到的消息的装置公共密钥。如果装置公共密钥是自签名装置证书的部分,那么模块82

通过从自签名装置证书提取装置公共密钥来读取装置公共密钥。在任何情况下，模块82被配置成确定装置公共密钥是否出现在与用户装置12的制造商相对应的白名单数据库20中。为了做到这一点，模块82可将装置公共密钥发送到白名单数据库20且接收指示装置公共密钥是否在数据库20中的答复。替代地，模块82可分析数据库20的内容以确定装置公共密钥是否驻留于数据库20中。作为确定用户装置12是否使用安全密钥供应的另一实例，模块82可被配置成针对用户装置12使用安全密钥供应的指示分析CA签名装置证书的内容(例如如果使用第三方证书颁发中心22(参见图10)，那么在此情况下可能不使用或甚至不存在白名单数据库20(尽管展示于图10中))。在此情况下，模块82被配置成使用签名CA的公共密钥以验证CA签名装置证书的签名。一旦签名被验证，模块82就可信任CA签名装置证书的内容，且针对关于用户装置12是否使用安全密钥供应的指示分析CA签名装置证书的内容。举例来说，CA签名装置证书可明确地指示是否使用安全密钥供应，或可隐含地指示安全密钥供应不由不具有直接指示的装置证书使用。模块82被配置成通过授权用户装置12的注册来对确认用户装置12使用安全密钥供应作出响应，例如通过将用户装置12的注册授权发送到用户装置12(例如到注册模块52)以及发送到注册模块84。

[0036] 注册模块84被配置成与用户装置12交互以响应于接收到注册用户装置12的授权而获得用户信息。模块84可通过接口76双向通信以获得用户信息，其中通过用户将用户信息输入到用户装置12中。用户信息可包含关于用户装置12、用户(例如用户名和密码)、付费信息(例如信用卡详情)、所期望服务、所期望服务的持续时间等的信息。

[0037] 注册模块84进一步被配置成产生签名请求并将所述签名请求发送到SP签名证书模块86以从SP签名证书模块86接收SP签名证书且将SP签名证书发送到用户装置12。签名请求基于装置证书，例如其中签名请求包含装置证书，或至少来自装置证书的信息。注册模块84被配置成产生服务提供商(SP)证书。SP证书可包含装置公共密钥、装置ID、用户装置使用安全密钥供应的指示(例如在SP证书的扩展密钥使用(EKU)部分中)和/或调适内容和/或格式。举例来说，模块84优选地被配置成使用用户信息中的至少一些来产生SP证书。模块84可产生包含服务器专用、用户专用、订购专用、服务提供商专用和/或装置专用的内容和/或格式SP证书。服务器专用内容是与产生证书的服务器和/或提供服务的服务器相关的内容(例如服务器ID)。用户专用内容是关于用户装置12的用户(例如识别其、与其相关联、由其提供)的信息。订购专用内容是表征服务订购(例如所订购的特定服务、订购的持续时间等)的内容。装置专用内容是除装置ID和装置公共密钥之外的信息，所述装置专用内容与用于订购所述服务的用户装置12相关联(例如装置制造商、装置模型、一或多个装置能力(例如显示像素的数量)等)。关于服务器专用、用户专用、订购专用和/或装置专用的格式，模块84可产生具有取决于与产生SP证书且/或提供服务的服务器、用户装置12的用户、服务订购或用户装置12中的一或多个相关的信息的格式的SP证书，例如上文的内容实例中的任一个。模块84被配置成将SP证书作为使用装置公共密钥的证书签名请求的部分提供给模块86。模块84被配置成响应于发送签名请求而接收SP签名证书且将SP签名证书发送到用户装置12，例如经由接口76通过网络16。

[0038] SP签名证书模块86被配置成从模块84接收签名请求(其中所述签名请求包含SP证书)，对SP证书签名以产生SP签名证书且将SP签名证书发送到注册模块84。模块86被配置成验证用户装置12使用安全密钥供应(例如通过分析EKU)，对SP证书签名以产生SP签名证书，

且将SP签名证书发送到注册服务器30中的注册模块84。

[0039] 除装置公共密钥外，SP签名证书还可包含加密密钥。举例来说，模块86可获得(例如从存储器产生、撷取等)对称加密密钥且包含对称加密密钥作为SP签名证书的部分。模块86被配置成例如使用装置公共密钥对SP签名证书进行加密且优选地被配置成只要SP签名证书包含对称加密密钥就对SP签名证书进行加密。

[0040] 服务模块88被配置成将所订购服务提供给用户装置12。模块88被配置成接收且分析由用户装置12提供的SP签名证书。模块88可确定所提供的证书是否是真实的，例如通过将证书的内容和/或格式与预期内容和/或格式相比较。举例来说，预期内容可存储于存储器72中和/或从存储于存储器72中的信息导出。又举例来说，预期格式可由存储于存储器72中的信息指定和/或从存储于存储器72中的信息导出。模块88被配置成通过分析证书对确定所提供的SP签名证书是真实的作出响应以确定是否提供服务以及提供什么服务，并视需要提供所述服务。举例来说，模块88可分析证书以确定已订购(例如付费)的服务以及所述订购当前是否有效(例如尚未到期或否则已失效)。模块88进一步被配置成响应于确定所述订购当前有效而将所订购服务(例如网络接入、内容(例如游戏、音乐、电视、电影)等)提供给用户装置12。

[0041] 参看图6，进一步参看图1至5和7至8，供应装置公共密钥/证书和订购且获得在线服务的过程110包含所展示的阶段。然而，过程110仅仅是实例而非限制性的。可例如通过添加、移除、重新布置、组合、同时执行多个阶段和/或将单个阶段拆分成多个阶段而更改过程110。举例来说，阶段118可在阶段116之前执行。对如所展示及描述的过程110的再其它更改是有可能的。

[0042] 如下文进一步论述，过程110涉及用户装置12中的一个和服务提供商系统18中的一个两者。可针对其它用户装置12和/或针对其它服务提供商系统18重复过程110，但为简单起见，过程110的论述以单数形式指代用户装置12和服务提供商系统18。在过程110内的是子过程，例如从用户装置12的视角来看以及从服务提供商系统18的视角来看。

[0043] 举例来说，从服务提供商系统视角来看的过程110的阶段114和阶段116包含过程130(包含图7中展示的阶段)。过程130包含：经由电信网络在装置与服务提供商系统之间建立电信链路的阶段132；在服务提供商系统处经由电信网络从装置接收装置公共密钥的阶段134，所述装置公共密钥先于电信链路的建立；在服务提供商系统处验证装置将装置私用密钥存储在装置的安全存储区域中的阶段136，所述装置私用密钥与装置公共密钥相对应，装置公共密钥与装置私用密钥是加密密钥对；以及响应于验证装置将装置私用密钥存储在装置的安全存储区域中通过服务提供商系统授权用于服务登记的装置的注册的阶段138。然而，过程130仅仅是实例而非限制性的。可例如通过添加、移除、重新布置、组合、同时执行多个阶段和/或将单个阶段拆分成多个阶段而更改过程130。

[0044] 对于另一实例，从用户装置视角来看的过程110的阶段114和阶段116和/或阶段120包含获得注册授权和/或SP签名证书的过程140，其中过程140包含图8中展示的阶段。过程140包含：经由电信网络在装置与服务提供商系统之间建立电信链路的阶段142；经由电信网络将装置证书从装置发送到服务提供商系统的阶段144，所述装置证书包含装置公共密钥、装置标识和数字签名，装置公共密钥先于电信链路的建立，装置公共密钥与存储于安全存储器中的装置私用密钥相对应，装置公共密钥与装置私用密钥是加密密钥对，装置证

书进一步包含装置私用密钥存储在所述装置的安全存储器中的指示;以及在装置处从服务提供商系统接收授权以注册用于服务登记的移动装置的阶段146。

[0045] 下文关于对过程110的阶段114、116和120的论述来论述过程130、140。

[0046] 再次参看图6,还进一步参看图1至5和7至9,在阶段112处,过程110包含供应装置公共密钥/证书(即装置公共密钥和/或装置证书)。装置密钥/证书模块50存储装置公共密钥/证书,且可能在装置公共密钥/证书的产生中产生或协作。可在用户装置12的制造期间供应装置公共密钥/证书,其中所述装置公共密钥和装置私用密钥被产生且装置私用密钥通过处理器40存储在存储器42的安全存储区域中,例如在TEE 44中。同样或替代地,可在用户装置12的制造之后将装置公共密钥/证书存储在用户装置12中,但不作为用户装置12与服务提供商系统18之间的通信的部分,例如在用户装置12建立到服务提供商系统18的电信链路之前,装置公共密钥/证书存储在用户装置12中。

[0047] 在阶段114处,过程110包含发现网络16和服务提供商系统18。用户装置12,且确切地说处理器40经由接口49通过网络16来监听系统信息广播和/或将一或多个通信发送到网络16以发现网络16和服务提供商系统18,以便经由网络16将其它通信发送到服务提供商系统18。服务提供商系统18,且确切地说处理器70经由接口76从用户装置12接收通信且将答复发送到用户装置12。相应地,在阶段132、142处,过程130、140分别包含经由电信网络在装置与服务提供商系统之间建立电信链路。举例来说,用户装置12的处理器40经由接口49将通信发送到具有指示服务提供商系统18的目的地信息(例如统一资源定位符(URL))的网络16,且网络16将通信(具有适当的标头变化)转发到服务提供商系统18,确切地说转发到注册服务器30。注册服务器30通过使处理器70经由接口76将通信发送到用户装置12来答复用户装置12以完成与用户装置12的电信链路。

[0048] 在阶段116处,过程110包含针对服务的注册授权装置。从用户装置的视角来看,装置的授权包含过程140的阶段144和146,其中阶段146包含接收授权以注册用于服务登记的装置。从服务提供商系统的视角来看,对用于注册的装置的授权包含过程130的阶段134、136和138,其中阶段138授权用于服务登记的装置的注册。举例来说,在阶段134、144处,用户装置12,且确切地说装置密钥/证书模块50将装置公共密钥发送到注册服务器30。装置公共密钥(其对应于存储在用户装置12中的安全存储器中的装置私用密钥)可提供为进一步包含装置ID和来自用户装置12的数字签名的装置证书的部分(即自签名证书)。优选地,在阶段132、142中,装置公共密钥先于电信链路的建立,即在从用户装置12到服务提供商系统18的电信链路建立之前,装置公共密钥产生且存储在用户装置12中的安全存储器中。

[0049] 在阶段136处,服务提供商系统18,且确切地说此处注册服务器30的安全密钥验证模块82验证用户装置12将安全密钥供应至少用于与从用户装置12接收到的装置公共密钥相对应装置私用密钥。如果装置公共密钥提供为由用户装置12自签名的装置证书的部分,那么注册服务器30处理数字签名以验证装置证书可被信任是来自用户装置12。无论装置公共密钥是否提供为装置证书的部分,注册服务器30都联系白名单数据库20以确定从用户装置12接收到的装置公共密钥是否存在于白名单数据库20中,所述白名单数据库指示用户装置12将安全密钥供应用于对应装置私用密钥。举例来说,注册服务器30将从用户装置12接收到的装置公共密钥发送到数据库20,且数据库20通过将通信发送到指示装置公共密钥是否存在于数据库20中的注册服务器30来作出响应。

[0050] 作为一个替代方案，如果将第三方证书颁发中心22用作如图10中所展示的电信系统210的部分来对装置证书签名，那么阶段136可包括确定第三方签名的装置证书指示使用安全密钥供应。如果装置证书由第三方证书颁发中心22签名，那么注册服务器30联系第三方证书颁发中心22(其是装置根证书颁发中心)以获得证书颁发中心22的公共密钥。注册服务器30将对公共密钥的请求发送到证书颁发中心22，且证书颁发中心22发送具有证书颁发中心22的公共密钥的答复，而不是注册服务器30将装置公共密钥发送到数据库20且数据库20指示装置公共密钥是否存在于数据库20。注册服务器30使用证书颁发中心22的公共密钥以确定装置证书是可信的(例如通过使用证书颁发中心22的公共密钥来解密装置证书的全部或部分)。如果装置证书可被信任，那么注册服务器30针对用户装置12将安全密钥供应用于装置私用密钥的指示分析的装置证书。举例来说，注册服务器30针对此指示审核装置证书的EKU部分。如果装置证书指示用户装置12使用安全密钥供应，那么安全密钥供应的使用被验证，否则安全密钥供应的使用未被验证。

[0051] 在阶段138、146处，注册服务器30，且确切地说安全密钥验证模块82通过将授权发送到注册模块84和用户装置12(例如注册模块52)来对安全密钥供应的使用被验证作出响应，所述授权指示用户装置12可继续注册且订购所期望服务。如果已验证用户装置12将安全密钥供应用于装置私用密钥(例如装置公共密钥存在于数据库20中，或包含装置公共密钥的通信由可靠的第三方证书颁发中心22确认且包含使用安全密钥供应的指示)，那么可使用通过授权用户装置的注册响应的注册服务器30继续过程110。否则，过程110优选地结束以使得不准许用户装置12获得SP签名证书，或使用另一过程以向用户装置12提供SP签名证书。

[0052] 在阶段118处，过程110包含在线注册。用户装置12的注册模块52和注册服务器30的注册模块84参与双向通信，用户装置12通过所述双向通信向注册服务器30提供用户信息。注册服务器30(用户装置12向其提供用户信息)可以是相同物理实体或不同物理实体，但如果是不同物理实体，那么注册服务器30仍被视为相同服务提供商系统18的部分。用户装置12的用户提供关于用户和/或所期望服务的信息，包含选择所期望服务、提供付费信息、提供用户名和密码等。阶段118通常在阶段116之后且在阶段120之前执行，但可在阶段116之前执行，在此情况下阶段116将不包含发送注册授权。

[0053] 在阶段120处，过程110包含获得SP签名证书。此处，与上文提供的对这些阶段的论述类似，过程110可包含过程130的阶段134、136、138和过程140的阶段144、146，例如登记是通过物理上独立的注册服务器30而非用于注册。无论这种任选通信执行与否，注册服务器30中的注册模块84都产生SP证书(上文所论述)，视需要与服务提供商服务器32任选地通信。注册模块84将证书签名请求(包含SP证书)发送到服务提供商证书颁发中心34。服务提供商证书颁发中心34中的SP签名证书模块86例如通过分析SP证书中的EKU验证用户装置12使用安全密钥供应，且通过对SP证书签名以产生SP签名证书来对此验证(如果执行)作出响应。SP签名证书模块86将SP签名证书发送到注册服务器30中的注册模块84。注册模块84将SP签名证书发送到用户装置12，且任选地到服务模块88。

[0054] 在阶段122处，过程110包含下载订购信息。服务提供商服务器32在一或多个通信中将订购信息发送到用户装置12。所述订购信息可包含关于所订购服务、AAA服务器证书、策略信息、策略更新的频率的指示等的详细信息。

[0055] 在阶段124处，过程110包含建立到服务提供商的连接。用户装置12，且确切地说服务获取模块56建立与服务提供商系统18，且确切地说与服务提供商服务器32的服务模块88的连接。由用户装置12联系的特定服务提供商服务器32可以是或可以不是提供SP签名证书但将能够提供所订购服务的相同物理实体。举例来说，在阶段124处联系的服务提供商服务器32可在阶段124期间在物理上比提供SP签名证书的服务提供商服务器32更接近于用户装置12，其中两个服务提供商服务器32通常由共同实体拥有或控制。

[0056] 在阶段126处，过程110包含获得服务。用户装置12，且确切地说服务获取模块56使用所期望服务的指示(若需要)(例如在SP签名证书中不明确或暗示)将SP签名证书发送到服务提供商服务器32。服务提供商服务器32的服务模块88(确切地说服务模块88的AAA)视需要确定所提供的SP签名证书是否真实，且如果SP签名证书真实，那么将服务提供给用户装置12。

[0057] 过程110中的一些或全部可重复用于其它服务提供者和/或其它服务。举例来说，过程110的全部阶段可重复用于不同服务提供商系统18。优选地，尽管不是必须的，阶段112将从使用其它服务提供商系统18的过程110的重复中忽略。在任一情况下，用户装置12可将装置公共密钥(可能在装置证书中)发送到多个服务提供商系统18且从这些服务器提供商系统18获得相应的SP签名证书以用于获得对应服务。如果重复阶段112，那么在此阶段期间产生的装置私用密钥将存储在用户装置12的安全存储器中。作为另一实例，阶段124、126可利用相同服务提供商服务器32和/或不同服务提供商服务器32使用相同SP签名证书重复多次。

[0058] 参看图9，进一步参看图1至5，验证使用安全密钥供应、注册服务、获得SP签名证书且获得所订购服务的过程200包含所展示的阶段。然而，过程200仅仅是实例而非限制性的。可例如通过添加、移除、重新布置、组合、同时执行多个阶段和/或将单个阶段拆分成多个阶段而更改过程200。举例来说，阶段178和/或阶段180可忽略。对如所展示及描述的过程200的再其它更改是可能的。另外，虽然网络16未展示于图9中，但下文论述的通信中的许多通信可通过网络16发射，无论这被明确地提及与否。

[0059] 在阶段160、162、164、166、168、174处，验证安全密钥供应且对注册进行授权。在阶段160处，用户装置12经由接口49将通信发送到具有指示服务提供商系统18的目的地信息的网络16，且网络16将通信160转发到适当服务提供商系统18，尤其到注册服务器30。在阶段162处，注册服务器30答复用户装置12以完成在用户装置12与注册服务器30之间的电信链路。在阶段164处，用户装置12将用户装置12的装置公共密钥发送到注册服务器30。可发送不是装置证书的部分，或可以是自签名证书的部分或第三方签名证书的部分的公共密钥。如果提供不是证书的部分或是自签名证书的部分的装置公共密钥，那么在阶段166处，注册服务器30的安全密钥验证模块82将装置公共密钥发送到白名单数据库20(适当时优选地在从自签名证书提取装置公共密钥之后)。在阶段168处，白名单数据库20搜索装置公共密钥且向注册服务器30确认或否认装置公共密钥包含于白名单数据库20中，且因此安全密钥供应是否用于与从用户装置12接收到的装置公共密钥相对应的装置私用密钥。替代地，如果装置公共密钥是第三方签名证书的部分，那么替代阶段166、168，注册服务器30验证第三方签名的证书且分析所述证书以确定安全密钥供应是否用于与从用户装置12接收到的装置公共密钥相对应的装置私用密钥，。在阶段174处，已确定安全密钥供应用于与从用户

装置12接收到的装置公共密钥相对应的装置私用密钥的模块82将注册授权发送到用户装置12。

[0060] 在阶段176处，任选地阶段180、182和阶段182、184、186，用户注册所订购服务且获得SP签名证书。在阶段176处，用户装置12的注册模块52和注册服务器30的注册模块84参与双向通信，用户装置12通过所述双向通信向注册服务器30提供用户信息。阶段178是任选的，例如如果不同物理实体针对登记联系而非针对注册联系，那么安全密钥供应的确认由用户装置12使用。阶段180是注册模块84与服务提供商服务器32之间的任选通信以视需要获得SP证书的信息。在阶段182处，注册模块84产生SP证书且将SP证书的签名请求发送到服务提供商证书颁发中心34的SP签名证书模块86。在阶段184处，SP签名证书模块验证用户装置12使用安全密钥供应，对SP证书签名以产生SP签名证书，且将SP签名证书发送到注册模块84。如果模块86不验证安全密钥供应被使用，那么模块86不对SP证书签名，且将对签名请求的拒绝发送到注册模块84。在阶段186处，注册模块84将SP签名证书(或对这种证书的拒绝的指示)发送到用户装置12。

[0061] 在阶段188、190、192处，用户装置12获得所订购服务。在阶段188处，服务提供商服务器32，确切地说服务模块88视需要将订购信息提供给用户装置12。在阶段190处，用户装置将服务的请求发送到服务模块88。服务的请求优选地包含从与服务提供商服务器32相对应的注册服务器30接收到的SP签名证书，即其是服务提供商系统18与请求所发送到的服务提供商服务器32相同的部分。在阶段192处，服务模块88验证SP签名证书，确定所请求的服务是否是所订购的(例如付费)，且如果是，那么将所订购服务提供给用户装置。

[0062] 其它考虑因素

[0063] 其它实例和实施方案在本公开和所附权利要求书的范围及精神内。举例来说，归因于软件的性质，上文所描述的功能可使用由处理器、硬件、固件、硬连线或这些中的任何的组合执行的软件来实施。实施功能的特征也可在物理上位于各个位置处，包含分布以使得功能的部分在不同物理位置处实施。并且，如本文中所使用，以“中的至少一个”或“中的一或多个”为开始的项目列表中所使用的“或”指示分离性列表，以使得例如“A、B或C中的至少一个”的列表或“A、B或C中的一或多个”的列表意味着A或B或C或AB或AC或BC或ABC(即A和B和C)，或具有多于一个特征的组合(例如AA、AAB、ABBC等)。

[0064] 如本文中所使用，除非另有陈述，否则功能或操作是“基于”项目或条件的声明意味着所述功能或操作是基于所陈述的项目或条件且可基于除了所陈述的项目或条件之外的一或多个项目和/或条件。

[0065] 另外，将信息发送或发射“到”实体的指示或将信息发送或发射“到”实体的陈述不需要完成通信。这类指示或陈述包含信息从发送实体传送，但未到达信息的既定接收方。即使实际上未接收到信息，既定接收方仍可被称为接收实体，例如，接收执行环境。

[0066] 可根据特定要求进行实质性变化。举例来说，还可使用定制硬件，和/或可将特定元件实施于硬件、软件(包含便携式软件，例如小程序等)或两个中。另外，可采用到例如网络输入/输出装置的其它计算装置的连接。

[0067] 如本文中所使用，术语“机器可读媒体”和“计算机可读媒体”是指参与提供致使机器以特定方式操作的数据的任何媒体。使用计算机系统，各种计算机可读媒体可涉及将指令/代码提供到处理器以用于执行，且/或可用于存储且/或携载这类指令/代码(例如作为

信号)。在许多实施方案中,计算机可读媒体为物体和/或有形存储媒体。这类媒体可采用许多形式,包含但不限于非易失性媒体和易失性媒体。非易失性媒体包含例如光盘和/或磁盘。易失性媒体包含(而不限于)动态存储器。

[0068] 举例来说,物理和/或有形计算机可读媒体的常见形式包含软盘、柔性磁盘、硬盘、磁带,或任何其它磁性媒体、CD-ROM、任何其它光学媒体、打孔卡、纸带、具有孔图案的任何其它物理媒体、RAM、PROM、EPROM、FLASH-EPROM、任何其它存储器芯片或盒带、如下文所描述的载波,或计算机可以从中读取指令和/或代码的任何其它媒体。

[0069] 上文所论述的方法、系统和装置是实例。各种配置可视需要省略、取代或添加各种程序或组件。举例来说,在替代配置中,方法可以不同于所描述的次序来执行,且可添加、省略或组合各种步骤。并且,关于某些配置所描述的特征可以在各种其它配置中组合。可以类似方式组合配置的不同方面和元件。并且,技术发展,且因此所述元件中的许多元件为实例且并不限制本公开或权利要求书的范围。

[0070] 在描述中给出特定细节以提供对实例配置(包含实施方案)的透彻理解。然而,可在并无这些特定细节的情况下实践配置。举例来说,已在无不必要细节的情况下展示众所周知的电路、过程、算法、结构和技术以便避免混淆配置。此描述仅提供实例配置,且并不限制权利要求的范围、可应用性或配置。实际上,所述配置的前面描述提供用于实施所描述的技术的描述。可在不脱离本公开的精神或范围的情况下对元件的功能及布置作出各种改变。

[0071] 并且,可将配置描述为被描绘为流程图或框图的过程。尽管每一流程图或框图可将操作描述为依序过程,但许多操作可并行地或同时地执行。此外,可以重新布置所述操作的次序。过程可具有图中未包含的额外阶段或功能。此外,可通过硬件、软件、固件、中间件、微码、硬件描述语言或其任何组合来实施方法的实例。当以软件、固件、中间件或微码实施时,用以执行任务的程序代码或代码段可存储在例如存储媒体的非暂时性计算机可读媒体中。处理器可执行所描述的任务。

[0072] 图中展示和/或本文中论述为彼此相连接或通信的功能性或其它组件以通信方式耦合。即,其可直接或间接地连接以实现其间的通信。

[0073] 已描述若干实例配置,可在不脱离本公开的精神的情况下使用各种修改、替代构造合和等效物。举例来说,上文元件可为较大系统的组件,其中其它规则可优先于本发明的应用或以其它方式修改本发明的应用。并且,可在考虑上文元件之前、期间或之后进行许多操作。因此,上文描述并不约束权利要求书的范围。

[0074] 另外,可揭示超过一个发明。

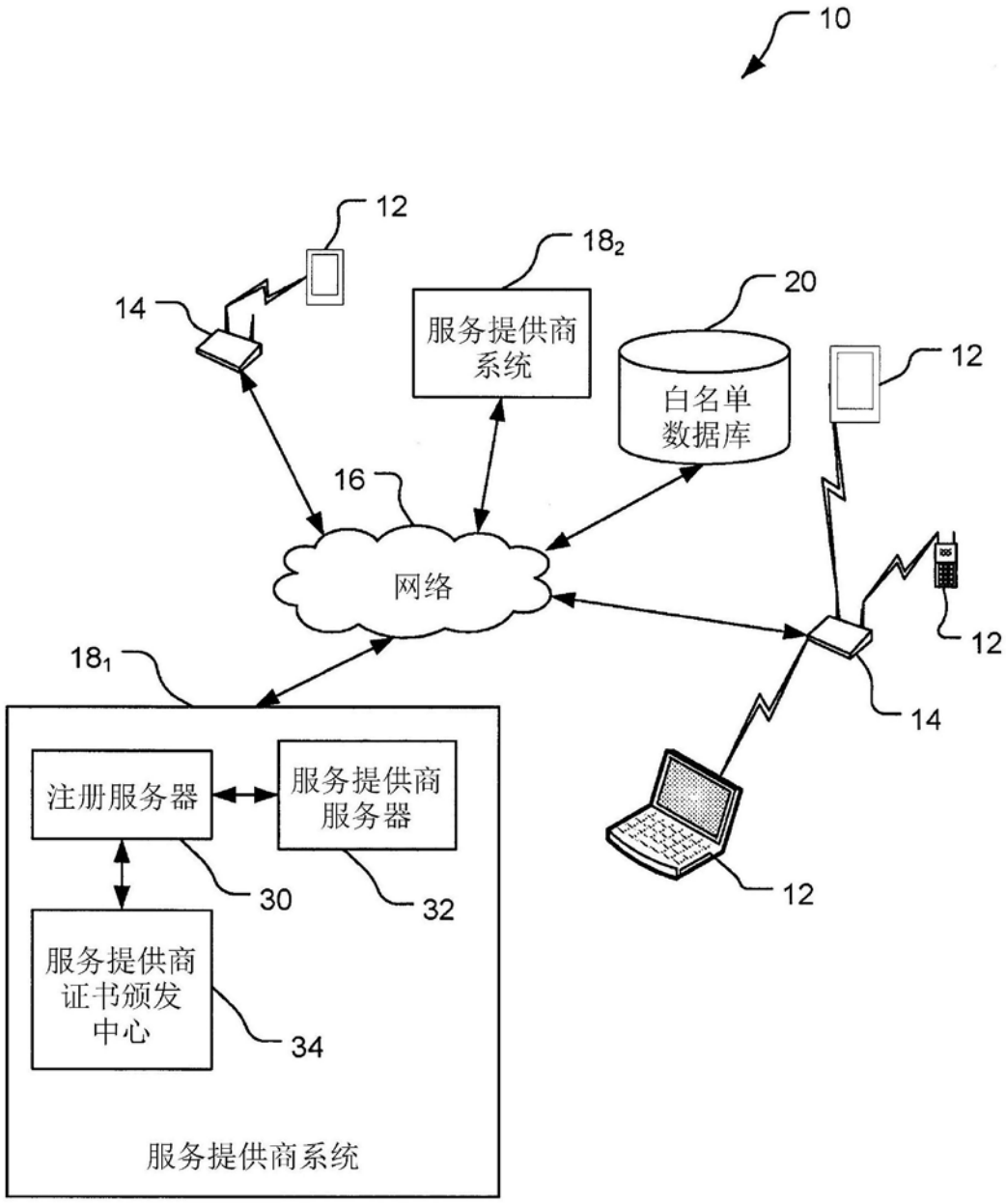

10
12
14
18₂
服务提供商系统
20
白名单数据库
12
16
网络
12
14
18₁
注册服务器
服务提供商服务器
30
32
服务提供商证书颁发中心
34
12
服务提供商系统

图1

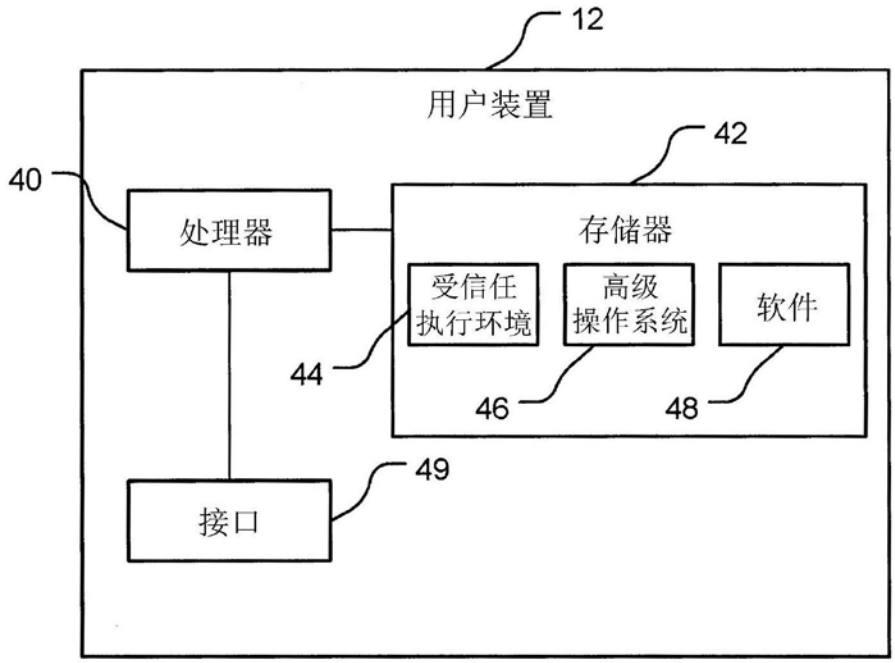

12
用户装置
42
40
处理器
存储器
受信任
执行环境
高级
操作系统
软件
44
46
48
49
接口

图2

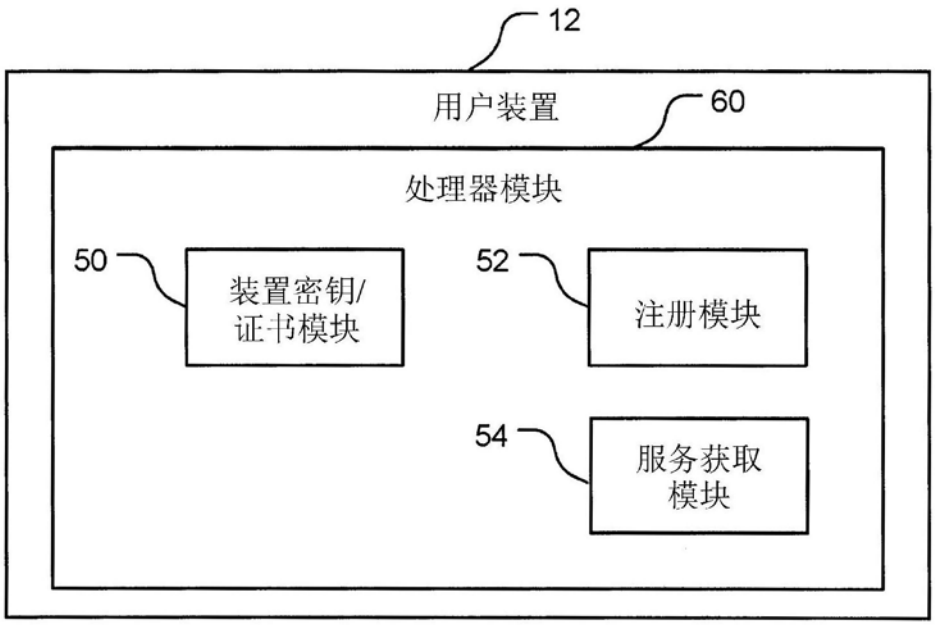

12
用户装置
60
处理器模块
50
装置密钥/
证书模块
52
注册模块
54
服务获取
模块

图3

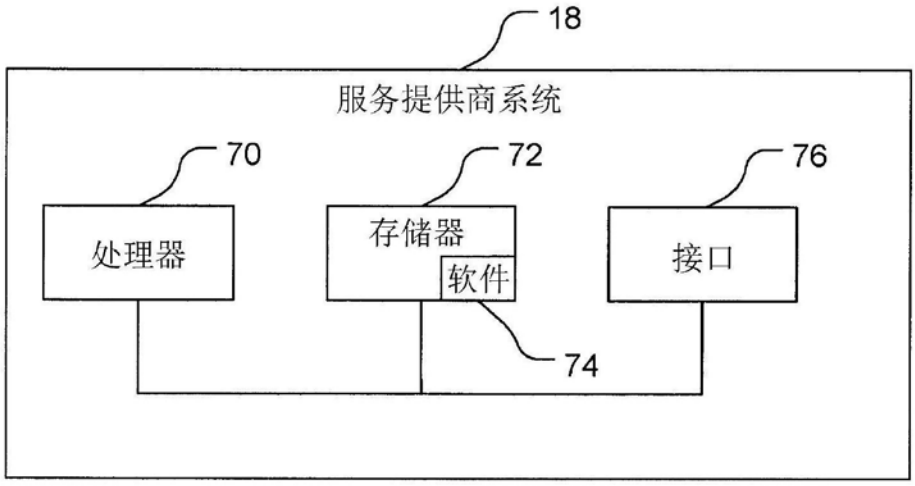

18
服务提供商系统
70
处理器
72
存储器
软件
74
76
接口

图4

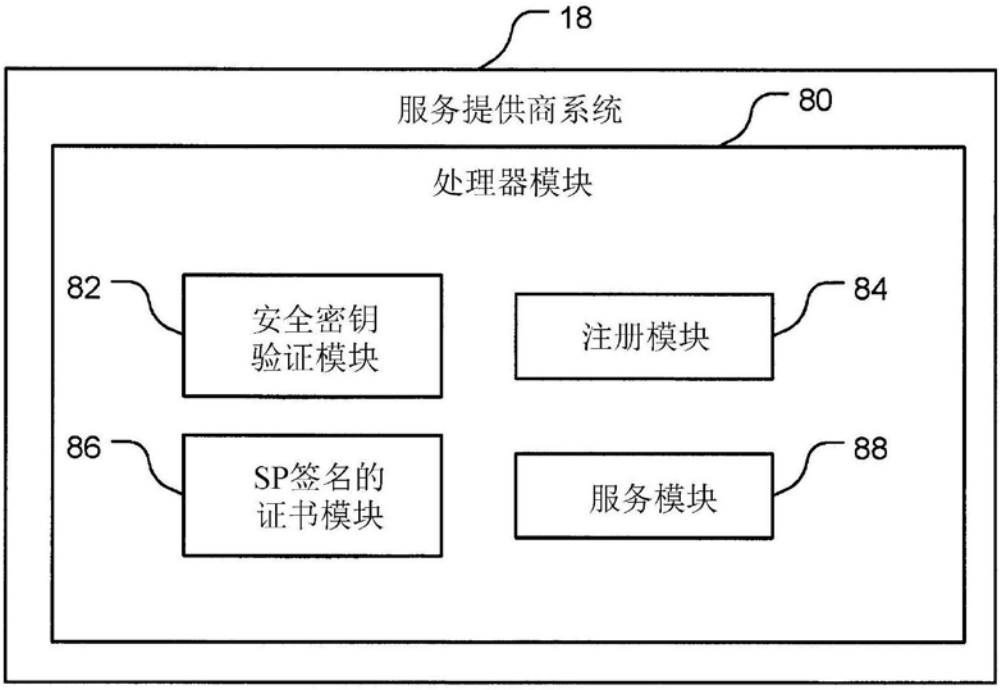

18
服务提供商系统
80
处理器模块
82
安全密钥
验证模块
84
注册模块
86
SP签名的
证书模块
88
服务模块

图5

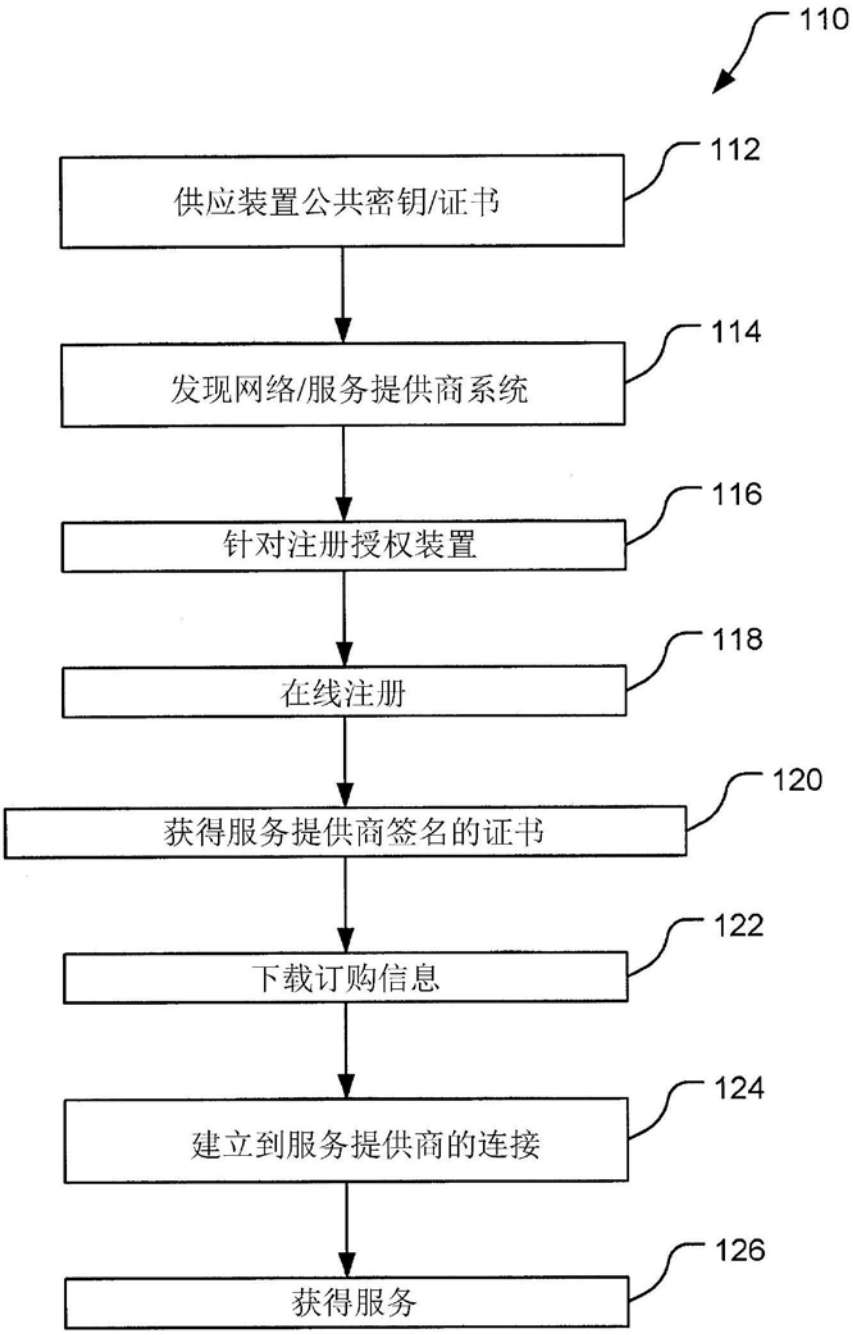

110
112
供应装置公共密钥/证书
114
发现网络/服务提供商系统
116
针对注册授权装置
118
在线注册
120
获得服务提供商签名的证书
122
下载订购信息
124
建立到服务提供商的连接
126
获得服务

图6

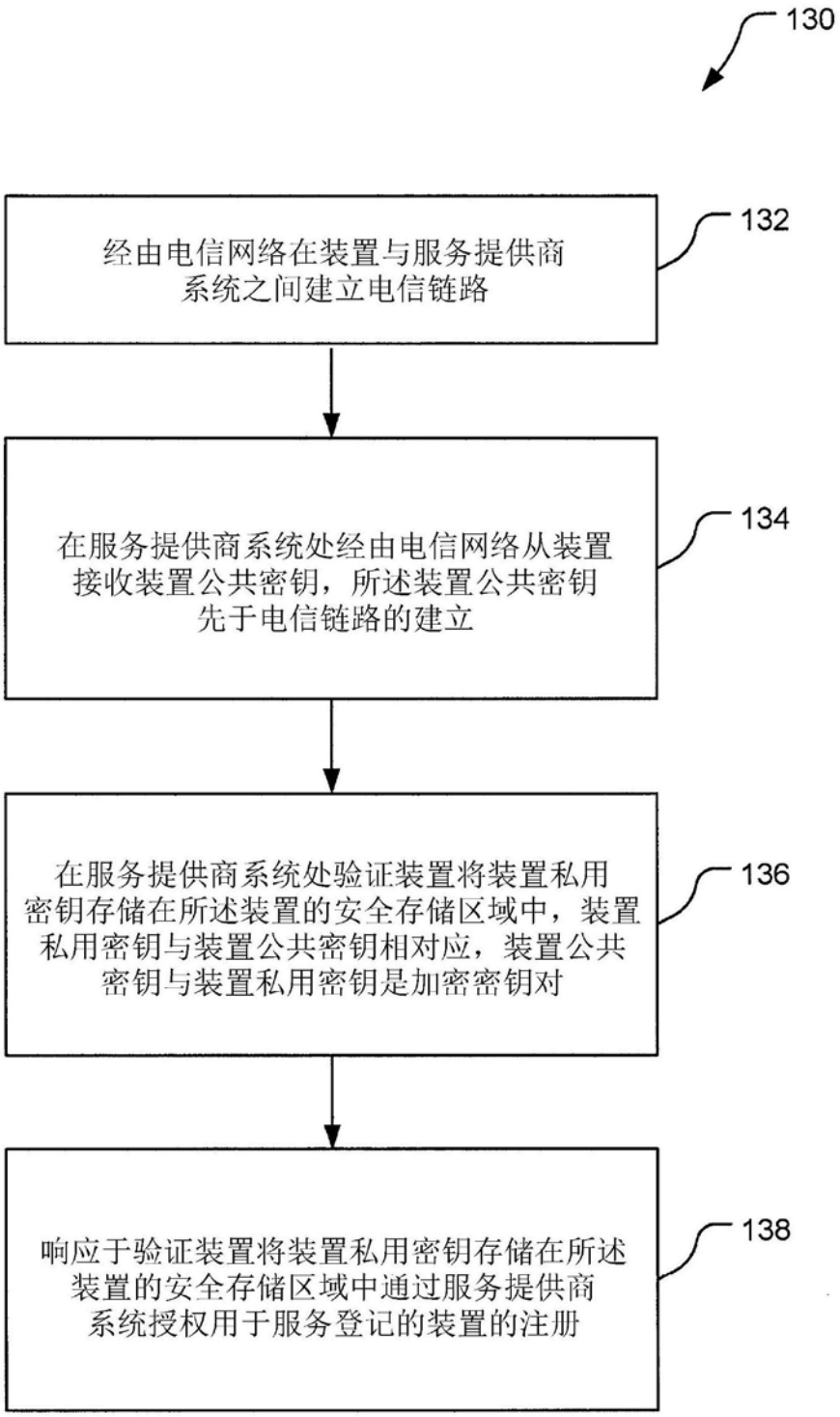

130
经由电信网络在装置与服务提供商系统之间建立电信链路
132
在服务提供商系统处经由电信网络从装置接收装置公共密钥，所述装置公共密钥先于电信链路的建立
134
在服务提供商系统处验证装置将装置私用密钥存储在所述装置的安全存储区域中，装置私用密钥与装置公共密钥相对应，装置公共密钥与装置私用密钥是加密密钥对
136
响应于验证装置将装置私用密钥存储在所述装置的安全存储区域中通过服务提供商系统授权用于服务登记的装置的注册
138

图7

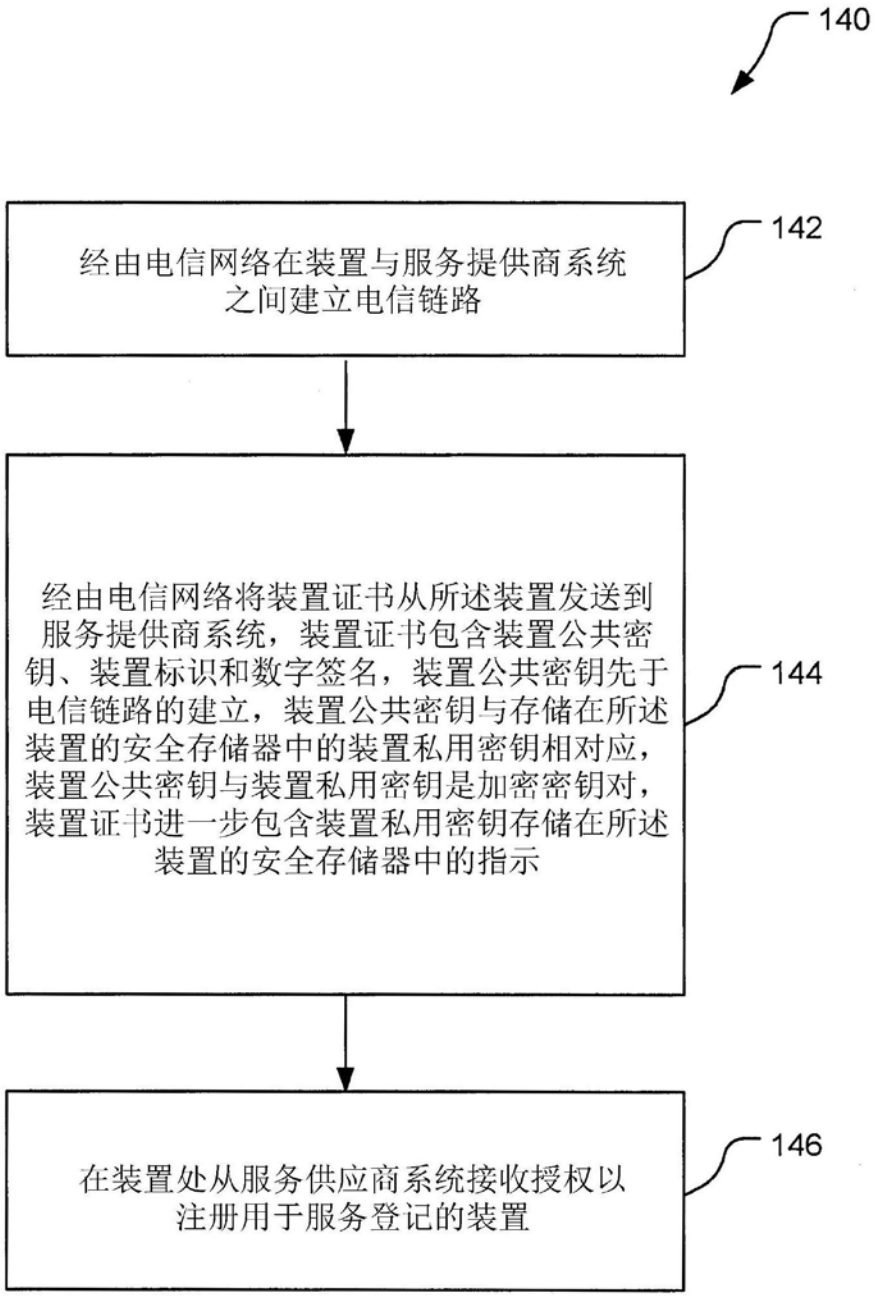

140
经由电信网络在装置与服务提供商系统之间建立电信链路
142
经由电信网络将装置证书从所述装置发送到服务提供商系统，装置证书包含装置公共密钥、装置标识和数字签名，装置公共密钥先于电信链路的建立，装置公共密钥与存储在所述装置的安全存储器中的装置私用密钥相对应，装置公共密钥与装置私用密钥是加密密钥对，装置证书进一步包含装置私用密钥存储在所述装置的安全存储器中的指示
144
在装置处从服务供应商系统接收授权以注册用于服务登记的装置
146

图8

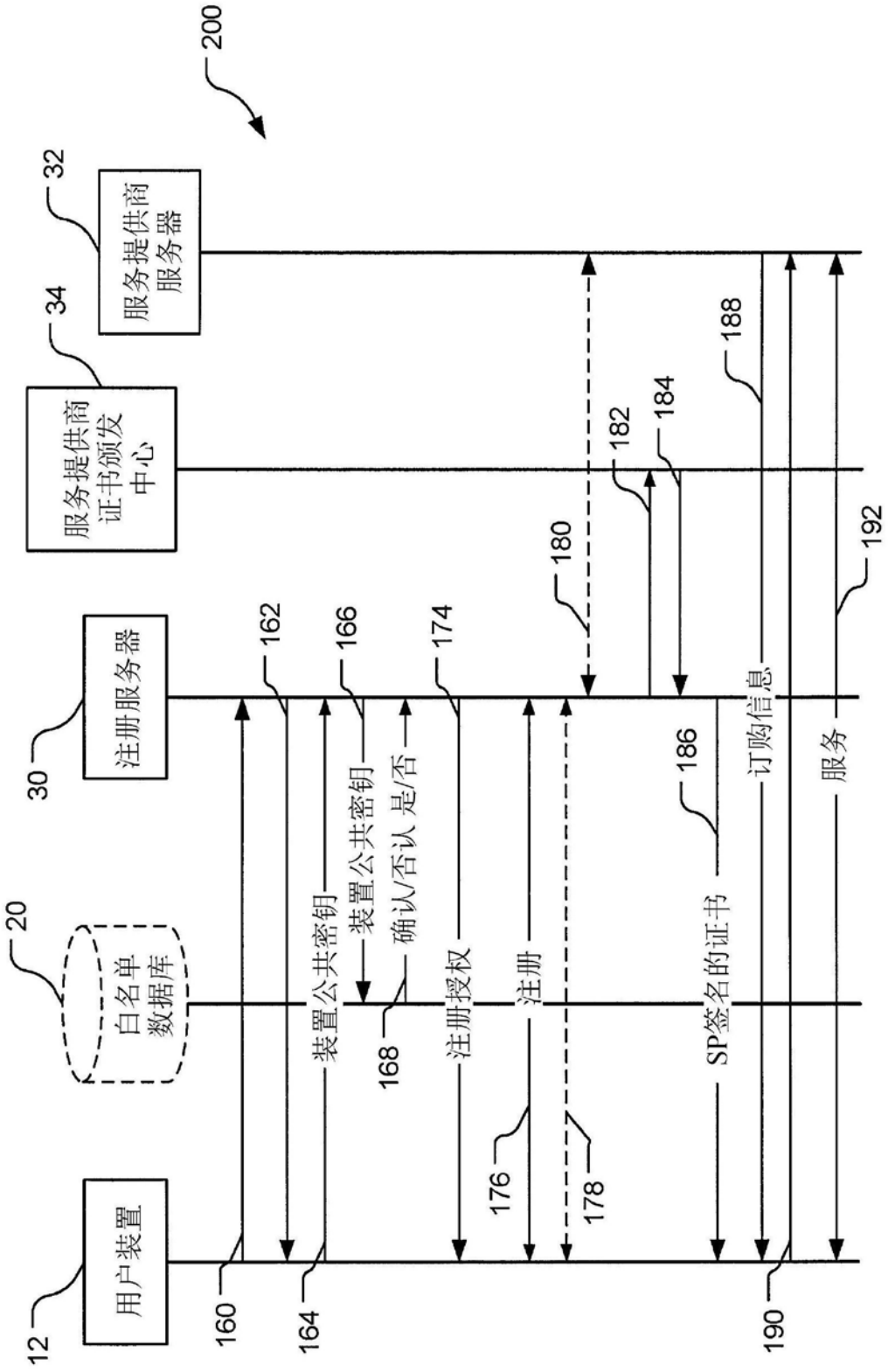

200
32
服务提供商服务器
34
服务提供商证书颁发中心
30
注册服务器
20
白名单数据库
12
用户装置
160
162
164
166
168
174
176
178
180
182
184
186
188
190
192
装置公共密钥
装置公共密钥
确认/否认 是/否
注册授权
注册
SP签名的证书
订购信息
服务

图9

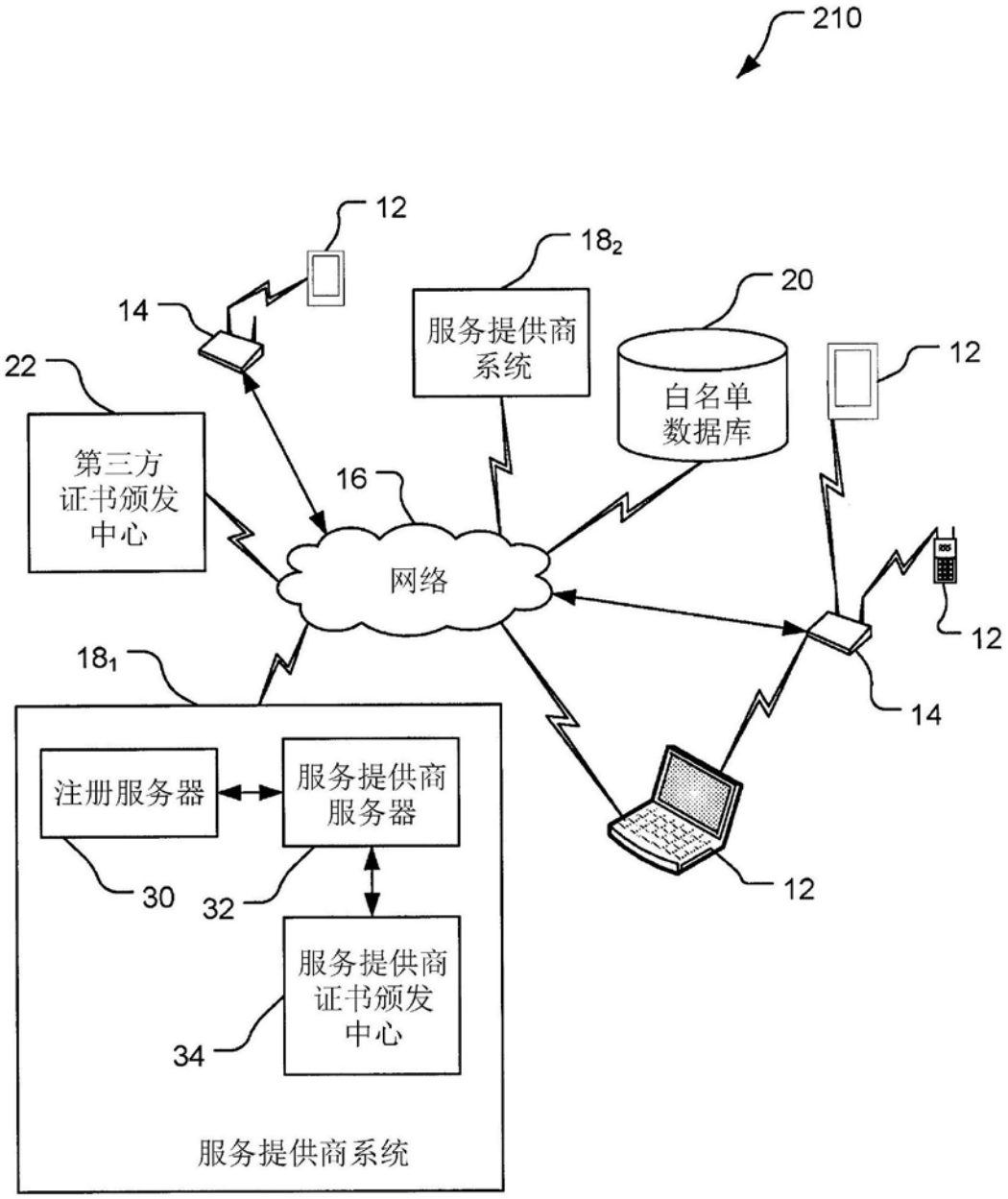

210
12
14
18_2
服务提供商系统
20
白名单数据库
12
22
第三方证书颁发中心
16
网络
12
18_1
14
注册服务器
服务提供商服务器
30
32
12
服务提供商证书颁发中心
34
服务提供商系统

图10