(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 105379176 B
(45)授权公告日 2019.01.11

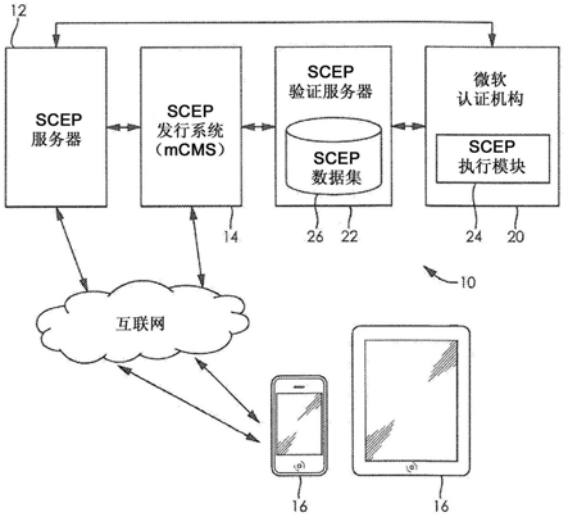
(21)申请号 201380075367.3
(22)申请日 2013.03.28
(65)同一申请的已公布的文献号
申请公布号 CN 105379176 A
(43)申请公布日 2016.03.02
(30)优先权数据
13/762,890 2013.02.08 US
(85)PCT国际申请进入国家阶段日
2015.09.30
(86)PCT国际申请的申请数据
PCT/US2013/034413 2013.03.28
(87)PCT国际申请的公布数据
WO2014/123557 EN 2014.08.14
(73)专利权人 安全认证解决方案公司
地址 美国俄亥俄州
(72)发明人 加里·A·加列豪斯
韦恩·A·哈里斯
爱德华·R·肖特
凯文·M·坦巴肖
(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
代理人 梁丽超 陈鹏
(51)Int.Cl.
H04L 9/32(2006.01)
H04W 12/06(2006.01)
(56)对比文件
US 2005039055 A1,2005.02.17,
WO 2012036971 A2,2012.03.22,
CN 102300026 A,2011.12.28,
EP 1549019 B1,2009.02.11,
US 8370428 B1,2013.02.05,
US 7007091 B2,2006.02.28,
审查员 罗啸
权利要求书3页 说明书7页 附图7页

(54)发明名称

用于验证SCEP证书注册请求的系统和方法

(57)摘要

一种用于验证SCEP证书注册的系统和方法，其执行SCEP口令密码和一组预期的证书请求内容的配对。通过将证书请求与注册的SCEP口令和相关联的预期的证书请求内容相比较，SCEP验证服务器或存在于另一个系统元件内的软件验证证书请求是否合法。该系统和方法解决了在可能造成实际攻击的现有基于SCEP的系统中的特权升级漏洞。



CN 105379176 B

1.一种用于验证SCEP证书注册请求的计算机实施的方法,所述方法包括以下步骤的组合:

(a)经由通信网络电子接收来自可信用户的预登记将用于随后的证书请求的SCEP口令的请求,并且响应于所述请求,生成并存储所述SCEP口令以及所述SCEP口令的相关联的预期证书内容;

(b)经由所述通信网络向发出请求的所述可信用户电子地发送所述SCEP口令;

(c)在步骤(a)和(b)之后,经由所述通信网络电子地接收包括所述SCEP口令的证书请求;

(d)通过检查所述证书请求的所述SCEP口令是否预登记,并且如果预登记则检查所述证书请求的内容是否与预登记的所述预期证书内容匹配,来电子地验证所述证书请求,所述预期证书内容与预登记的所述SCEP口令相关联;

(e)在步骤(d)之后,如果所述证书请求的所述SCEP口令预登记并且所述证书请求的内容与和预登记的所述SCEP口令相关联的预登记的所述预期证书内容匹配,则授权所述证书请求的证书,并且生成所述证书并经由所述通信网络向所述证书请求的发送者电子地发送所述证书;并且

(f)在步骤(d)之后,如果所述证书请求的所述SCEP口令并未预登记或者如果所述证书请求的内容与和预登记的所述SCEP口令相关联的预登记的所述预期证书内容不匹配,则拒绝所述证书请求。

2.根据权利要求1所述的计算机实施的方法,其中,所述证书请求是PKCS#10认证请求。

3.根据权利要求1所述的计算机实施的方法,其中,验证步骤通过SCEP验证服务器执行。

4.根据权利要求3所述的计算机实施的方法,其中,通过SCEP服务器经由所述通信网络接收所述证书请求,所述SCEP服务器将所述证书请求发送给认证机构,所述认证机构与所述SCEP验证服务器通信以验证所述证书请求。

5.根据权利要求4所述的计算机实施的方法,其中,所述认证机构经由SCEP执行模块与所述SCEP验证服务器通信。

6.根据权利要求4所述的计算机实施的方法,其中,SCEP执行模块实施为所述认证机构的策略模块。

7.根据权利要求6所述的计算机实施的方法,其中,所述SCEP执行模块使所有通信通过,除非接收到包含SCEP口令的所述证书请求。

8.根据权利要求3所述的计算机实施的方法,其中,所述SCEP验证服务器实施为面向服务的架构元件。

9.根据权利要求5所述的计算机实施的方法,其中,通过所述SCEP服务器经由所述通信网络接收所述证书请求,所述SCEP服务器在将所述证书请求发送给所述认证机构之前将所述证书请求发送给所述SCEP验证服务器以进行验证。

10.根据权利要求1所述的计算机实施的方法,其中,通过SCEP服务器经由所述通信网络接收所述证书请求,所述SCEP服务器在将所述证书请求发送给认证机构之前利用位于所述SCEP服务器内的软件验证所述证书。

11.根据权利要求1所述的计算机实施的方法,其中,通过SCEP服务器经由所述通信网

络接收所述证书请求，所述SCEP服务器将所述证书请求发送给认证机构，所述认证机构在授权所述证书请求之前利用位于所述认证机构内的软件验证所述证书请求。

12.一种用于验证SCEP证书注册请求的系统，所述系统包括以下的组合：

SCEP服务器，用于经由通信网络电子地接收来自可信用户的预登记将用于随后的证书请求的SCEP口令的请求，并且所述SCEP服务器用于经由所述通信网络电子地接收包括所述SCEP口令的证书请求；

SCEP发行系统，用于经由所述通信网络向所述可信用户电子地发送所述SCEP口令；

SCEP验证服务器，用于存储所述SCEP口令和所述SCEP口令的相关联的预期证书内容，并且所述SCEP验证服务器用于通过检查所述证书请求的所述SCEP口令是否预登记并且如果预登记则检查所述证书请求的内容是否与和预登记的所述SCEP口令相关联的预登记的所述预期证书内容匹配来验证所述证书请求；

其中，如果所述证书请求的所述SCEP口令预登记并且所述证书请求的内容与和预登记的所述SCEP口令相关联的预登记的所述预期证书内容匹配，则所述证书请求由所述SCEP验证服务器验证并且所述证书请求的证书被授权；并且

其中，如果所述证书请求的所述SCEP口令未预登记或者如果所述证书请求的内容与和预登记的所述SCEP口令相关联的预登记的所述预期证书内容不匹配，则所述证书请求不由所述SCEP验证服务器验证并且所述证书请求被拒绝。

13.根据权利要求12所述的系统，其中，所述证书请求是PKCS#10认证请求。

14.根据权利要求12所述的系统，进一步包括认证机构，所述认证机构从所述SCEP服务器接收所述证书请求并且与所述SCEP验证服务器通信以验证所述证书请求。

15.根据权利要求14所述的系统，其中，所述认证机构包括用于与所述SCEP验证服务器通信的SCEP执行模块。

16.根据权利要求15所述的系统，其中，所述SCEP执行模块实施为所述认证机构的策略模块。

17.根据权利要求16所述的系统，其中，所述SCEP执行模块使所有通信通过，除非接收到包含SCEP口令的所述证书请求。

18.根据权利要求12所述的系统，其中，所述SCEP验证服务器实施为面向服务的架构元件。

19.根据权利要求12所述的系统，其中，所述SCEP服务器在将所述证书请求发送给认证机构之前，将所述证书请求发送给所述SCEP验证服务器以进行验证。

20.一种用于验证SCEP证书注册请求的系统，所述系统包括以下的组合：

SCEP服务器，用于经由通信网络电子地接收来自可信用户的预登记将用于随后的证书请求的SCEP口令的请求，并且所述SCEP服务器用于经由所述通信网络电子地接收包括所述SCEP口令的证书请求；

SCEP发行系统，用于经由所述通信网络向所述可信用户电子地发送所述SCEP口令；

验证软件，被配置为存储所述SCEP口令和所述SCEP口令的相关联的预期内容并且验证所述证书请求；

其中，所述验证软件通过以下步骤来验证所述证书请求：检查所述证书请求的所述SCEP口令是否预登记，并且如果预登记则检查所述证书请求的内容是否与预登记的所述预

期证书内容匹配，所述预期证书内容与预登记的所述SCEP口令相关联；

其中，如果所述证书请求的所述SCEP口令预登记，并且所述证书请求的内容与和预登记的所述SCEP口令相关联的预登记的所述预期证书内容匹配，则所述验证软件验证所述证书请求并授权所述证书请求的证书；并且

其中，如果所述证书请求的所述SCEP口令未预登记或者所述证书请求的内容与和预登记的所述SCEP口令相关联的预登记的所述预期证书内容不匹配，则所述验证软件不验证所述证书请求并且拒绝所述证书请求。

21.根据权利要求20所述的系统，其中，所述证书请求是PKCS#10认证请求。

22.根据权利要求20所述的系统，进一步包括认证机构，所述认证机构从所述SCEP服务器接收所述证书请求。

23.根据权利要求22所述的系统，其中，所述验证软件存在于所述认证机构内。

24.根据权利要求20所述的系统，其中，所述验证软件存在于所述SCEP服务器内。

用于验证SCEP证书注册请求的系统和方法

技术领域

[0001] 本发明的领域总体上涉及计算机网络安全，并且更具体地，涉及用于针对请求访问基于SCEP的网络的计算装置实施和管理安全策略的系统和方法。

背景技术

[0002] 弗吉尼亚州Restin的Verisign公司为加州的圣何塞的Cisco Systems公司研制了简单证书注册协议(SCEP)，以主要用于允许网络管理员以可扩展的方式容易给网络计算装置注册证书。由于这些网络计算装置不可能具有其在企业目录或凭证储存器内表示的身份，所以SCEP不包括认证请求者的身份的规定。相反，SCEP允许两个不同的授权机构。第一授权机构是手动的，其中，在认证机构(CA)管理员或认证官方提交之后，请求者需要等待批准请求。第二授权方法是预先共享的密钥，其中，SCEP服务器创建必须以某种方式传输给请求者的“口令密码”，包括将提交返回给服务器。

[0003] 包围SCEP的创建的总体安全模型是控制较好的环境的模型。在SCEP初始被设计为解决的使用实例中，由高度可信的CA管理员检索口令密码，并且将这些密码提供给高度可信的网络管理员，以保证高度可信网络计算装置的证书。在很多情况下，可以由相同的管理员检索和使用SCEP口令。

[0004] 自从Windows Server 2003首次作为自由可下载的附加元件，然后，Windows Server 2008作为本地元件(通过网络装置注册服务(NDES)角色)，华盛顿州雷德蒙德的微软公司支持SCEP用于其CA软件。微软公司的SCEP实现方式比较完全的功能，并且允许各种配置选择，包括：设置SCEP口令密码的长度；打开或关闭SCEP口令的要求；允许或者禁止重新使用SCEP口令；以及设置未使用的SCEP口令应被视为无效的最大时间。

[0005] 当加州库比蒂诺的苹果公司将SCEP加入其移动操作系统(称为iOS)中时，显示SCEP的客户端计算装置的总体计数增大几个数量级。此外，远离其中最初使用协议的安全友好环境移动SCEP。在高度可信管理员的指导下，并非将证书用于密切控制的网络计算装置中，现在，可以通过互联网建造允许“不太可信”的计算装置及其用户的SCEP注册。实际上，很多移动装置管理(MDM)系统依赖于这种类型的架构。可能的安全模型的这种变化非常重要，下面进一步讨论。

[0006] SCEP口令密码的一个极其重要的方面在于，在提供授权以提交PKCS#10格式的证书请求时，实际上未认证请求者，甚至也未识别请求者。要注意的是，PKCS是由位于马萨诸塞州Bedford的RSA实验室产生的公共密钥密码标准。而且，SCEP口令和SCEP服务器本身都未对可以提交的请求的类型或内容发表任何陈述。实质上，具有有效的SCEP口令密码使持有人有权将具有完全自己选择的内容的证书请求提交给SCEP服务器。这在最初创建SCEP的原始的“仅仅管理员”安全模型中是优越的，但是在整体用于互联网上时引起顾虑。

[0007] 用户或计算装置可以采用其合法获得的SCEP口令密码，并且使用该密码通过更高的访问等级获得表示不同用户或计算装置的证书，或者甚至获得与预期的证书不同的类型的证书。由于攻击者不需要是合法用户，所以如果重新使用或禁用口令密码，那么后果甚至

更严重。

[0008] 这个问题实际上并非苹果公司、Cisco Systems公司、微软公司的“错误”，也并非利用SCEP的大量移动装置管理系统的“错误”。确切地说，这是由几个因素的组合引起的。首先，SCEP口令密码给某人提供将证书请求提交给SCEP服务器的许可，但是不对该提交的内容作出任何主张或执行。其次，iOS操作的计算装置的SCEP支持给SCEP请求开辟了起源于不可信网络并且起源于不太可信(非管理)用户的途径，并且很多移动装置管理系统需要这个。第三，很多企业CA安装(包括微软公司的CA的大部分默认安装)正在用于发行用作网络认证凭证的证书。还重要的是，要注意，执行攻击，不需要使用苹果计算装置，仅仅需要有效的SCEP口令密码以及与SCEP服务器通信的能力。因此，内部开发的SCEP服务器或者由反向代理或防火墙保护的服务器也易受影响。因此，需要一种改进的架构以验证SCEP证书注册请求。

发明内容

[0009] 在本文中公开了用于移动计算装置和非移动计算装置两者的数据安全系统和方法，其克服了现有技术的至少一个上述缺点。公开了一种用于验证SCEP证书注册请求的计算机实施的方法，包括以下步骤的组合：允许可信用户登记SCEP口令以及SCEP口令的相关联组的预期证书内容；通过通信网络电子地接收证书请求；以及通过检查证书请求的SCEP口令是否与一个先前登记的SCEP口令匹配，并且如果匹配则检查所述证书请求的内容是否与和匹配的登记的SCEP口令相关联的先前登记的预期的证书内容匹配，来电子地验证证书请求。如果证书请求的SCEP口令与先前登记的SCEP口令匹配，并且证书请求的内容与和匹配的登记的SCEP口令相关联的登记的预期的证书内容匹配，则授权证书。如果证书请求的SCEP口令与先前登记的SCEP口令不匹配，或者如果证书请求的内容与和匹配的登记的SCEP口令相关联的登记的预期的证书内容不匹配，则拒绝证书。

[0010] 还公开了一种用于验证SCEP证书注册请求的系统，所述系统包括以下的组合：SCEP服务器，用于电子地接收来自可信用户的登记SCEP口令以及SCEP口令的相关联组的预期证书内容的请求，并且用于通过通信网络电子地接收来自计算装置的证书请求；SCEP发行系统，用于向可信用户发行SCEP口令；以及SCEP验证服务器(validation service)，用于电子地验证证书请求。SCEP验证服务器通过检查证书请求的SCEP口令是否与先前登记的SCEP口令匹配，并且如果匹配则检查证书请求的内容是否与和匹配的登记的SCEP口令相关联的先前登记的预期的证书内容匹配，来电子地验证证书请求。如果证书请求的SCEP口令与登记的SCEP口令匹配，并且证书请求的内容与和匹配的登记的SCEP口令相关联的登记的预期的证书内容匹配，则SCEP验证服务器授权证书。如果证书请求的SCEP口令没有匹配的登记的SCEP口令或者证书请求的内容与和匹配的登记的SCEP口令相关联的登记的预期的该组证书内容不匹配，则SCEP验证服务器拒绝证书。

[0011] 还公开了一种用于验证SCEP证书注册请求的系统，所述系统包括以下的组合：SCEP服务器，用于电子地接收来自可信用户的登记SCEP口令以及SCEP口令的相关联组的预期证书内容的请求，并且用于通过通信网络电子地接收来自计算装置的证书请求；SCEP发行系统，用于向可信用户发行SCEP口令；以及验证软件，被配置为验证证书请求。验证软件通过检查证书请求的SCEP口令是否与先前登记的SCEP口令匹配，并且如果匹配则检查证书

请求的内容是否与和匹配的登记的SCEP口令相关联的先前登记的预期的证书内容匹配，来验证证书请求。如果证书请求的SCEP口令与登记的SCEP口令匹配，并且证书请求的内容与和匹配的登记的SCEP口令相关联的登记的预期的证书内容匹配，则验证软件授权证书。如果证书请求的SCEP口令没有匹配的登记的SCEP口令或者证书请求的内容与和匹配的登记的SCEP口令相关联的该组登记的预期的证书内容不匹配，则验证软件拒绝证书。

[0012] 通过前述公开内容和以下各种优选实施方式的更详细的描述，对于本领域的技术人员将显而易见的是，本发明在用于移动数据安全性的系统和方法的技术和领域中提供了重大进展。在这方面，特别重要的是本发明能够提供比较便宜并且有效的移动数据安全。鉴于下面提供的详细描述，更好地理解各种优选实施方式的额外特征和优点。

附图说明

[0013] 参照以下描述和示图，本发明的这些和进一步的特征将显而易见，其中：

[0014] 图1是根据本发明的第一示出的实施方式的用于通过通信网络从计算装置接收请求的数据安全系统的示意图；

[0015] 图2是图1的数据安全系统的SCEP注册过程的第一部分的示意图；

[0016] 图3是图1的数据安全系统的SCEP注册过程的第二部分的示意图；

[0017] 图4是根据本发明的第二示出的实施方式的用于通过通信网络从计算装置中接收请求的数据安全系统的示意图；

[0018] 图5是图4的数据安全系统的SCEP注册过程的第二部分的示意图，其中，SCEP注册过程的第一部分与在图2中示出的相似；

[0019] 图6是根据本发明的第三示出的实施方式的用于通过通信网络从计算装置中接收请求的数据安全系统的示意图；

[0020] 图7是用于图6的数据安全系统的SCEP注册过程的第二部分的示意图，其中，SCEP注册过程的第一部分与在图2中示出的相似；

[0021] 图8是根据本发明的第四示出的实施方式的用于通过通信网络从计算装置接收请求的数据安全系统的示意图；

[0022] 图9是图8的数据安全系统的SCEP注册过程的第二部分的示意图，其中，SCEP注册过程的第一部分与在图2中示出的相似；

[0023] 图10是根据本发明的进一步示出的实施方式的用于通过通信网络从计算装置接收请求的数据安全系统的示意图；

[0024] 图11是示出用于图1至图10的数据安全系统和方法的SCEP口令和相关联的验证数据的实例的表格。

具体实施方式

[0025] 对于本领域的技术人员(即，对于在该技术领域内具有知识或经验的人员)将显而易见的是，对于在本文中公开的数据安全性的系统和方法可以具有很多用途和设计变化。各种可替代和优选的实施方式的以下详细讨论将相对于iOS操作的移动计算装置示出本发明的一般原理，但是考虑到本公开的优点，适合于其他应用的其他实施方式和变化对于本领域的技术人员将是显而易见的。例如，其中移动计算装置是另外或者交替地运行的其他

操作系统和/或计算装置是另外或者交替地非移动装置的应用。移动计算装置是小型手持式计算装置，例如，移动电话、智能电话、平板电脑、个人数字助理(PDA)、企业数字助理、计算器、掌上游戏机、便携式媒体播放器、数码相机、数码摄像机、传呼机、个人导航设备(PND)等。非移动设备是并非小型手持装置的计算装置，例如，台式计算机、便携式计算机(膝上型电脑、笔记本电脑等)、上网本、工作站、服务器、大型机、超级计算机等。

[0026] 现在，参照示图，图1示出了根据本发明的第一示出的实施方式的用于验证SCEP证书注册请求的数据安全系统10。所示出的数据安全系统10包括SCEP服务器12和SCEP发行系统，其均通过通信网络18与多个计算装置16通信。SCEP服务器12可以是任何合适类型的服务器，并且与认证机构20直接通信。所示出的认证机构20是微软认证机构，但是可以可替代地使用任何其他合适的认证机构20。所示出的SCEP发行系统14是从俄亥俄州独立城的Certified Security Solutions公司(CSS公司)可购买到的移动证书管理系统(mCMS)，但是可以可替代的是任何其他合适的SCEP发行系统14。所示出的计算装置16是运行iOS的移动计算装置，诸如，例如从苹果公司可购买的iPhone、iPad以及iPod Touche等，但是计算装置16可以可替代地是任何其他合适类型的计算装置16和/或可以运行任何其他合适的操作系统，诸如，例如Mac OS、安卓、Windows Phone等。所示出的通信网络18是互联网，但是可以可替代地是任何其他合适类型的通信网络。

[0027] 为SCEP发行系统14提供验证服务的SCEP验证服务器22位于SCEP发行系统14与认证机构20之间。即，SCEP发行系统14与SCEP验证服务器22直接通信，并且SCEP验证服务器22与认证机构20直接通信。SCEP验证服务器22的主要功能在于，执行SCEP口令密码和一组预期的证书请求内容的配对。可在各种机构中指导SCEP验证服务器22执行这些配对。

[0028] 所示出的SCEP验证服务器22实施为典型的面向服务架构(SOA)元件，以能够通过服务合同松开捆绑以及提供多平台互操作性。所示出的SCEP验证服务器22的服务公开为在HTTPS上运行的基于SOAP的网络服务。可以在TCP或命名管道等上可替代地运行相同的服务，但是真实的“网络服务”在HTTPS上运行。所示出的网络服务通过.NET技术建立，并且将WCF用作网络服务框架。微软的互联网信息服务(IIS)网络服务器直接托管SCEP发行系统14以及SCEP验证服务器22。由于期望的基于HTTP的网络应用和网络服务在协议级别上通常没有状态，所以这两个系统可以在相同的物理机器上或者可分开到不同的机器中。然而，有状态的元件需要用作SCEP口令数据的数据模型，这是因为使用了HTTP的无状态性质。在由SCEP发行系统14提交数据时与在由SCEP执行模块24做出验证请求时之间，所示出的数据安全系统10需要可以在内存中保持SCEP口令的元件。所示出的SCEP验证服务器22充当这个角色，并且实施为有状态的单个元件，允许相同的实例在证书注册过程的整个使用期中保持有效。

[0029] SCEP执行模块24用于通过SCEP验证服务器22与认证机构20整合，并且由认证机构20托管。所示出的SCEP执行模块24实施为用于微软认证机构20的策略模块，并且遵循ICertPolicy2COM接口。微软公司的架构要求所有策略模块实施为支持ICertPolicy2接口的COM对象。在创建COM对象时，存在几个技术替换物，但是需要COM对象，与所使用的技术无关。由于所示出的微软认证机构24可仅仅具有一个策略模块，所以SCEP执行模块24主要用作“垫片(shim)”，使所有通信通过，进入原始策略模块中，直到接收到包含SCEP口令的证书请求。然后，SCEP执行模块24使用标准策略模块功能的组合并且通过解析证书请求，从证书

请求中获得相关信息，并且将该信息传递给SCEP验证服务器22，以用于检查。如果SCEP验证服务器22指示该信息与期望的信息不匹配，则SCEP执行模块24拒绝请求。

[0030] 如在图2中最佳地显示，SCEP验证服务器22允许SCEP发行系统24登记可信用户允许的SCEP口令数据集。在本文中以及权利要求中使用术语“可信用户”，以表示值得进行证书和内容提交的个人或计算机装置。在大部分情况下，做出请求的可信用户是软件，例如，CSS公司的mCMS，其指示装置注册证书。存储这些登记的SCEP口令数据集，直至从存储器卸载服务，或者从服务的验证侧去除单独数据集。SCEP口令数据集可以存储在任何合适的存储器或储存器内，例如，RAM(SRAM、DRAM)、闪存、ROM/PROM/EROM/EEROM/虚拟存储器、高速缓冲存储器、永久存储器、硬盘驱动器、磁带驱动器、磁盘、光盘等。iOS操作的计算装置16通过通信网络18与SCEP发行系统14开始会话，已进行登记，在所示出的实施方式中，该系统是mCMS网站。SCEP发行系统14将SCEP口令(即，SCEP口令密码)的请求发送给SCEP服务器12，并且SCEP服务器12将SCEP口令返回SCEP发行系统14。然后，SCEP发行系统14使用SCEP验证服务器22存储生成的SCEP口令密码。SCEP口令数据集可以存储在任何合适的存储器或储存器内，例如，RAM(SRAM、DRAM)、闪存、ROM/PROM/EROM/EEROM/虚拟存储器、高速缓冲存储器、永久存储器、硬盘驱动器、磁带驱动器、磁盘、光盘等。要注意的是，所示出的SCEP验证服务器22具有合适的数据库26以存储SCEP口令数据集。SCEP发行系统14还生成具有iOS操作的计算装置16的.mobileconfig文件的形式的移动配置，并且通过通信网络18将移动配置发送给计算装置16。然后，计算装置16生成密钥对。需要RSA密钥对，以生成PKCS#10请求。公开密钥在PKCS#10请求中提交并且嵌入CA发行的证书内。该设计允许在计算装置16上生成私有密钥，这提高了安全性，无需通过通信网络18传送密钥。

[0031] 如在图3中最佳示出的，在SCEP服务器12从计算装置16接收具有PKCS#10请求的形式的认证请求时，SCEP服务器12确定是否允许请求者请求该特定证书。通过将证书请求发送给认证机构20做出该确定，该证书请求由插入式策略模块或SCEP执行模块24接收(其通过SCEP验证服务器22检查以验证请求)。SCEP验证服务器22检查该请求是否与先前储存的任何登记的SCEP口令数据集(包括SCEP口令和证书请求的预期内容)匹配。图11示出了SCEP口令和相关验证数据的实例。如果发现匹配的SCEP口令数据集，则将肯定的响应返回给计算装置16，并且从内部数据储存器中去除SCEP口令数据集。通过SCEP验证服务器22将肯定的响应发送给插入式策略模块24，插入式策略模块24将授权响应发送给认证机构20，认证机构20将授权响应发送给SCEP服务器12，并且SCEP服务器12生成证书并且将证书发送给输入证书的计算装置16，从而将肯定的响应返回给计算装置16。由SCEP验证服务器22存储和管理允许的SCEP口令。允许的SCEP口令可以存储在任何合适的存储器或储存器内，例如，RAM(SRAM、DRAM)、闪存、ROM/PROM/EROM/EEROM/虚拟存储器、高速缓冲存储器、永久存储器、硬盘驱动器、磁带驱动器、磁盘、光盘等。如果没有发现匹配的SCEP口令数据集，则将否定的响应返回给计算装置16，并且不给计算装置16提供证书。

[0032] 图4示出了根据本发明的第二示出的实施方式的用于验证SCEP证书注册请求的数据安全系统10A。根据第二示出的实施方式的数据安全系统10A与在上文中描述的根据第一示出的实施方式的数据安全系统10大致相同，除了SCEP验证服务器22移动到SCEP服务器12前面。即，在将证书请求发送给认证机构20之前，SCEP服务器12使用SCEP验证服务器22来验证证书请求。所示出的系统10A包括彼此直接通信的并且均通过通信网络18与计算装置16

通信的SCEP服务器12和SCEP发行系统。SCEP服务器12与认证机构20直接通信。为SCEP发行系统14提供验证服务的SCEP验证服务器22与SCEP服务器12和SCEP发行系统14直接通信，并且SCEP服务器12位于SCEP验证服务器22与认证机构20之间。SCEP验证服务器22的主要功能是执行SCEP口令密码和一组预期的证书请求内容的配对。

[0033] 如在图5中最佳示出的，当SCEP服务器12从计算装置16接收到具有PKCS#10请求的形式的认证请求时，SCEP服务器12确定是否允许请求者请求该特定证书。通过请求SCEP验证服务器22验证请求，做出该确定。SCEP验证服务器22检查该请求是否与先前存储的任何登记的SCEP口令数据集(包括SCEP口令和证书请求的预期内容)匹配。如果发现匹配的SCEP口令数据集，则将肯定的响应返回给计算装置16，并且从内部数据储存器中去除SCEP口令数据集。通过SCEP验证服务器22将肯定的响应发送给SCEP服务器12，SCEP服务器12将证书请求发送给认证机构20，认证机构20将授权响应发送给SCEP服务器12，并且SCEP服务器12生成证书并且将证书发送给输入证书的计算装置16，从而将肯定的响应返回给计算装置16。由SCEP验证服务器22存储和管理允许的SCEP口令。如果没有发现匹配的SCEP口令数据集，则从认证机构20阻止证书请求，将否定的响应返回给计算装置16，并且不给计算装置16提供证书。

[0034] 图6示出了根据本发明的第三示出的实施方式的用于验证SCEP证书注册请求的数据安全系统10B。根据第三示出的实施方式的数据安全系统10B与在上文中描述的根据第二示出的实施方式的数据安全系统10A大致相同，除了由SCEP服务器12执行验证功能以外。即，在将证书请求发送给认证机构20之前，SCEP服务器12本身使用存在于SCEP服务器12内的软件来验证证书请求。所示出的系统10B包括彼此直接通信的并且均通过通信网络18与计算装置16通信的SCEP服务器12和SCEP发行系统。SCEP服务器12与认证机构20直接通信。为SCEP发行系统14提供验证服务的SCEP验证软件28存在于SCEP服务器12内。SCEP验证软件28的主要功能是执行SCEP口令密码和一组预期的证书请求内容的配对。

[0035] 如在图7中最佳示出的，当SCEP服务器12从计算装置16接收具有PKCS#10请求的形式的认证请求时，SCEP服务器12确定是否允许请求者请求该特定证书。使用SCEP验证软件28验证请求，在内部做出该确定。SCEP验证软件28检查该请求是否与先前存储的任何登记的SCEP口令数据集(包括SCEP口令和证书请求的预期内容)匹配。如果发现匹配的SCEP口令数据集，则将肯定的响应返回给计算装置16，并且从内部数据储存器中去除SCEP口令数据集。通过SCEP验证软件28提供肯定的响应，SCEP服务器12将证书请求发送给认证机构20，认证机构20将授权响应发送给SCEP服务器12，并且SCEP服务器12生成证书并且将证书发送给输入证书的计算装置16，从而将肯定的响应返回给计算装置16。由SCEP验证服务器22存储和管理允许的SCEP口令。如果没有发现匹配的SCEP口令数据集，则从认证机构20阻止证书请求，将否定的响应返回给计算装置16，并且不给计算装置16提供证书。

[0036] 图8示出了根据本发明的第四示出的实施方式的用于验证SCEP证书注册请求的数据安全系统10C。根据第四示出的实施方式的数据安全系统10C与在上文中描述的根据第一示出的实施方式的数据安全系统10大致相同，除了由认证机构20执行验证功能以外。即，在将授权发送给SCEP服务器之前，认证机构20本身使用存在于认证机构20内的软件来验证证书请求。所示出的系统10C包括彼此直接通信的并且均通过通信网络18与计算装置16通信的SCEP服务器12和SCEP发行系统。SCEP服务器12与认证机构20直接通信。为SCEP发行系统

14和认证机构20提供验证服务的SCEP验证软件28存在于认证机构20内。

[0037] 如在图9中最佳示出的，当SCEP服务器12从计算装置16接收具有PKCS#10请求的形式的认证请求时，SCEP服务器12确定是否允许请求者请求该特定证书。通过将证书请求发送给认证机构20(其利用SCEP验证软件28检查来验证请求)来做出该确定。SCEP验证软件28检查该请求是否与先前存储的任何登记的SCEP口令数据集(包括SCEP口令和证书请求的预期内容)匹配。如果发现匹配的SCEP口令数据集，则将肯定的响应返回给计算装置16，并且从内部数据储存器中去除SCEP口令数据集。通过SCEP验证软件28提供肯定的响应，认证机构20将授权响应发送给SCEP服务器12，并且SCEP服务器12生成证书并且将证书发送给输入证书的计算装置16，从而将肯定的响应返回给计算装置16。由SCEP验证服务器22存储和管理允许的SCEP口令。如果没有发现匹配的SCEP口令数据集，则将否定的响应返回给计算装置16，并且不给计算装置16提供证书。

[0038] 图10示出了根据本发明的第五示出的实施方式的用于验证SCEP证书注册请求的数据安全系统10D。根据第五示出的实施方式的数据安全系统10D与在上文中描述的根据第一示出的实施方式的数据安全系统10大致相同，除了如果证书请求有效则使用仅允许将证书请求传递给SCEP服务器12的SCEP代理28以外。通过这个实施方式，V-SCEP技术直接整合到SCEP代理28内。计算装置16首先通过通信网络18使用存在于网络服务器14内的mCMS注册。在该注册期间，在中央数据库26内登记SCEP数据集。对于证书实例，计算装置16生成其PKCS10请求并且将该请求发送给SCEP代理28。SCEP代理28比较来自计算装置16的PKCS10请求的内容和在数据库26内登记的SCEP数据集。如果请求内容的验证成功，则SCEP代理28将SCEP请求转发给实际的SCEP服务器12。然后，SCEP服务器12发行证书，并且将证书内容返回给SCEP代理12(其将发行的证书发送给计算装置16)。

[0039] 要注意的是，上面示出的实施方式的每个特征和变化可用于与其他示出的实施方式的每个特征和变化的任何组合中。

[0040] 通过上述公开内容，显而易见的是，上述数据安全系统和方法解决了在可能够造成实际攻击的现有的基于SCEP的系统中的理论上的特权升级漏洞(privilege-escalation vulnerability)。还显而易见的是，上述系统和方法通过性能效益和成本效益的方式解决了这个漏洞。进一步显而易见的是，可以通过任何合适的方式提供和执行验证步骤，诸如，例如执行验证步骤的软件可在系统内的任何合适的位置中存在于任何合适的元件内。

[0041] 通过某些优选实施方式的上述公开内容和详细描述，还显而易见的是，在不背离本发明的真实范围和精神的情况下，可以具有各种修改、增加以及其他替换的实施方式。选择并且描述所讨论的实施方式，以提供对本发明及其实际应用的原理的最佳说明，从而能够允许技术人员在各种实施方式中并且通过各种修改使用本发明，这些修改适合于预期的特定用途。在根据公平、合法以及公正享有的优点解释时，所有这些修改和变化均在由所附权利要求确定的本发明的范围内。

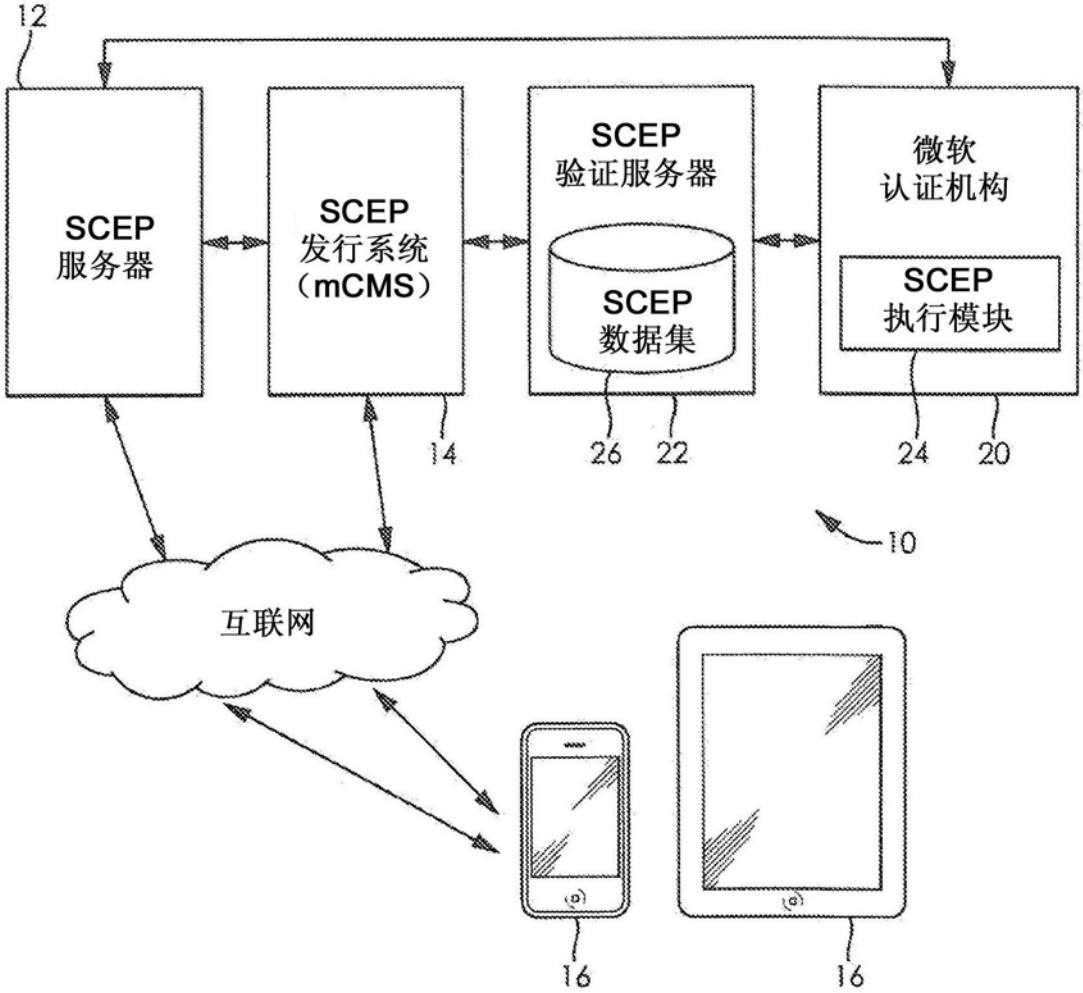

12
SCEP
服务器
SCEP
发行系统
（mCMS）
SCEP
验证服务器
SCEP
数据集
微软
认证机构
SCEP
执行模块
14
26
22
24
20
10
互联网
16
16

图1

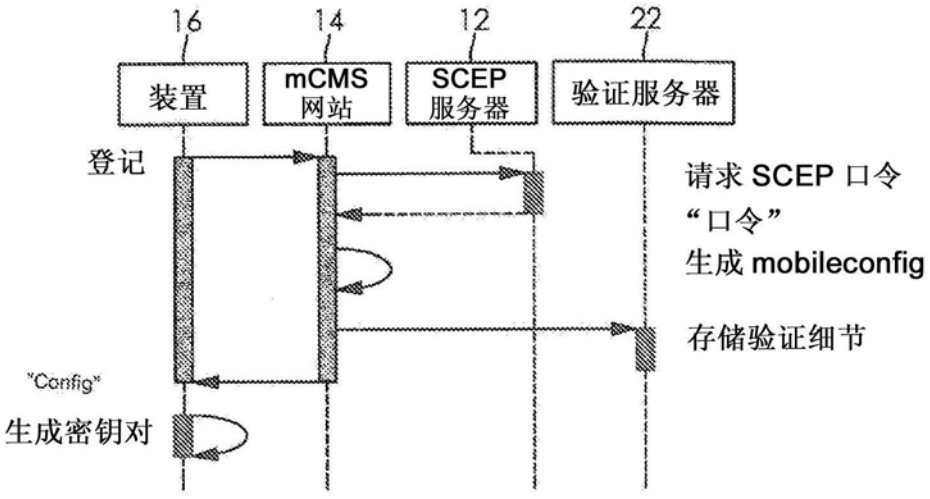

16
14
12
22
装置
mCMS
网站
SCEP
服务器
验证服务器
登记
请求 SCEP 口令
“口令”
生成 mobileconfig
存储验证细节
"Config"
生成密钥对

图2

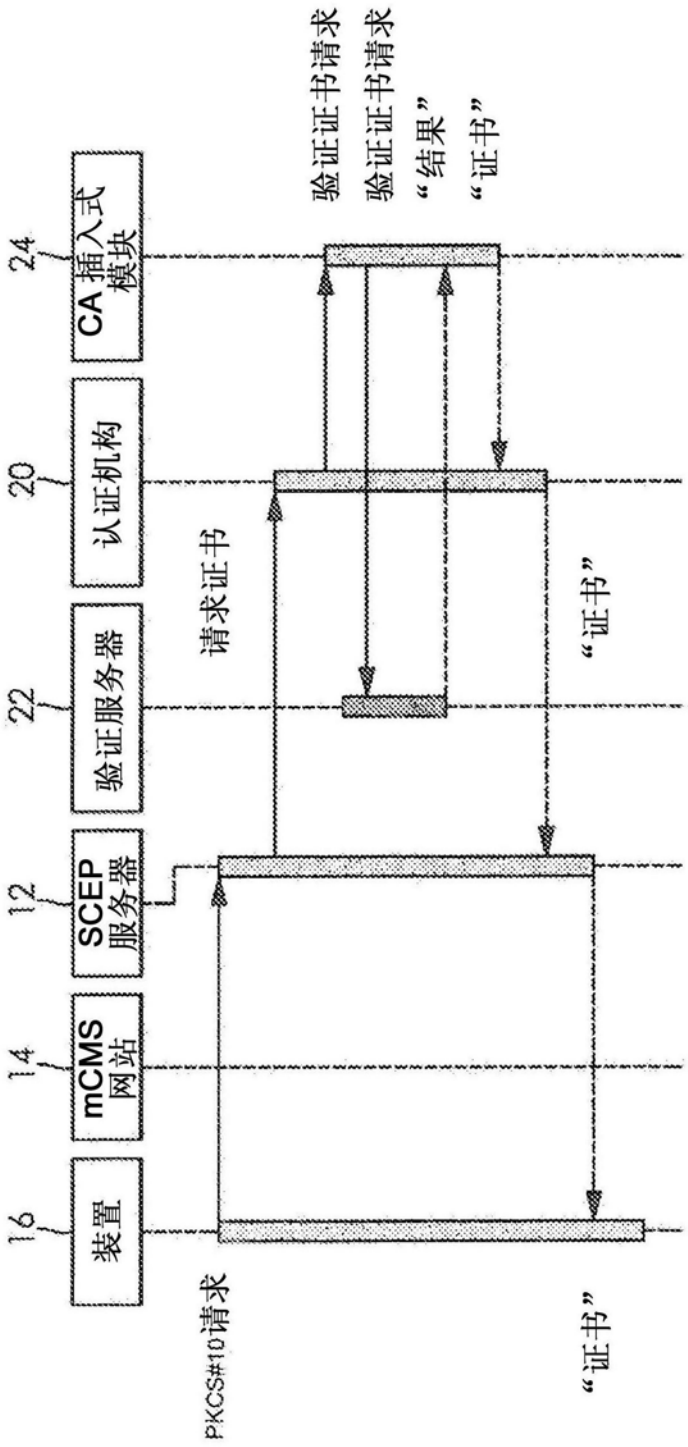

16
装置
14
mCMS
网站
12
SCEP
服务器
22
验证服务器
20
认证机构
24
CA 插入式
模块
PKCS#10请求
请求证书
验证证书请求
验证证书请求
“结果”
“证书”
“证书”
“证书”

图3

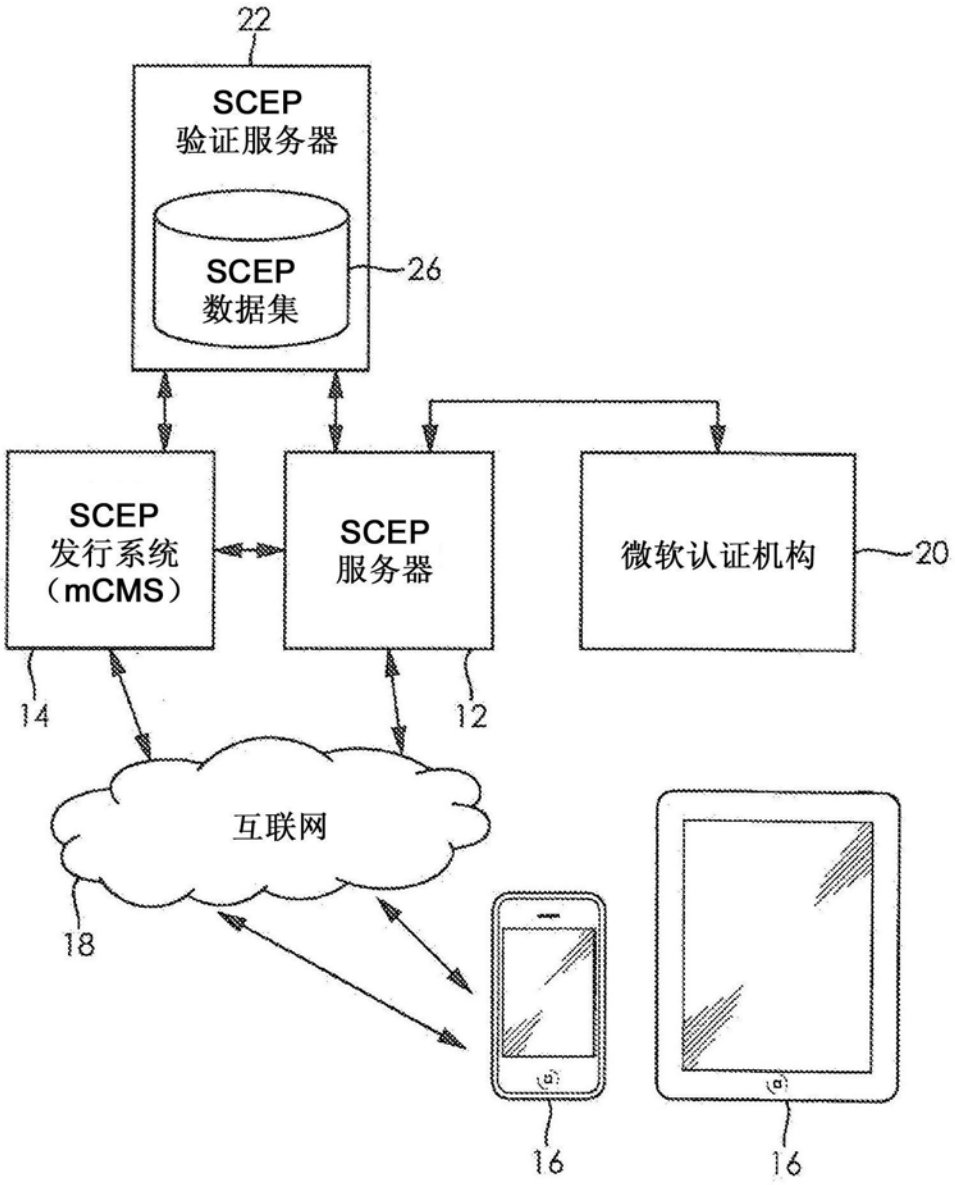

22
SCEP
验证服务器
SCEP
数据集
26
SCEP
发行系统
（mCMS）
SCEP
服务器
微软认证机构
20
14
12
互联网
18
16
16

图4

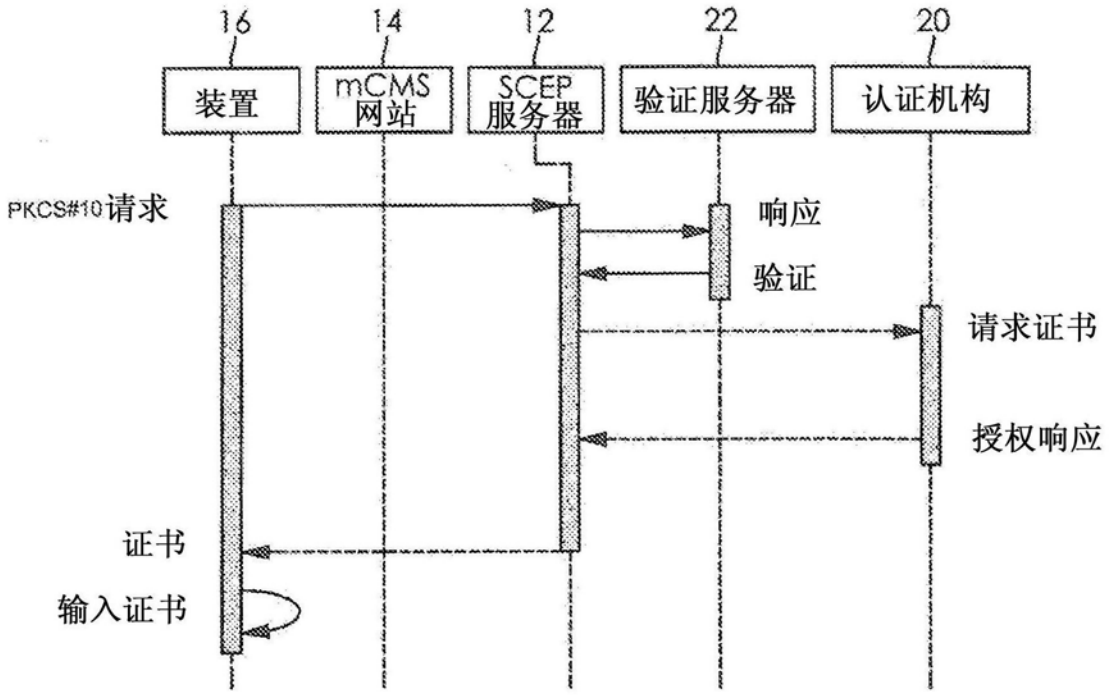

16
14
12
22
20
装置
mCMS 网站
SCEP 服务器
验证服务器
认证机构
PKCS#10请求
响应
验证
请求证书
授权响应
证书
输入证书

图5

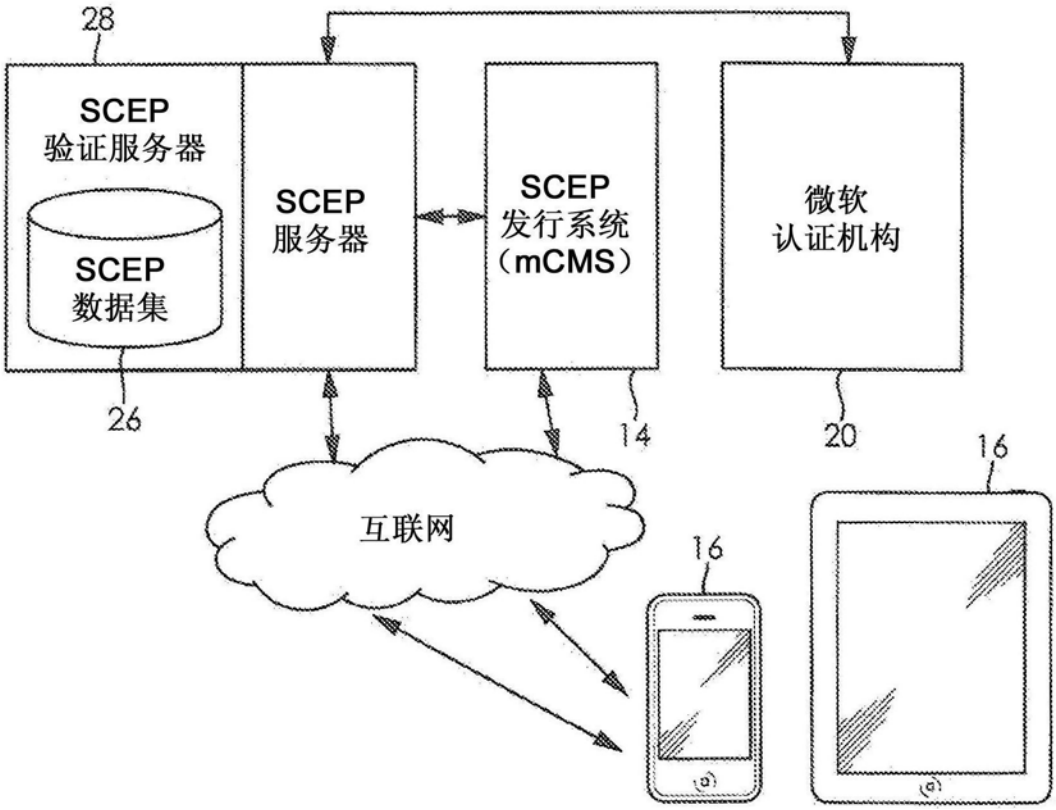

28
SCEP 验证服务器
SCEP 数据集
SCEP 服务器
SCEP 发行系统 (mCMS)
微软 认证机构
26
14
20
16
互联网
16

图6

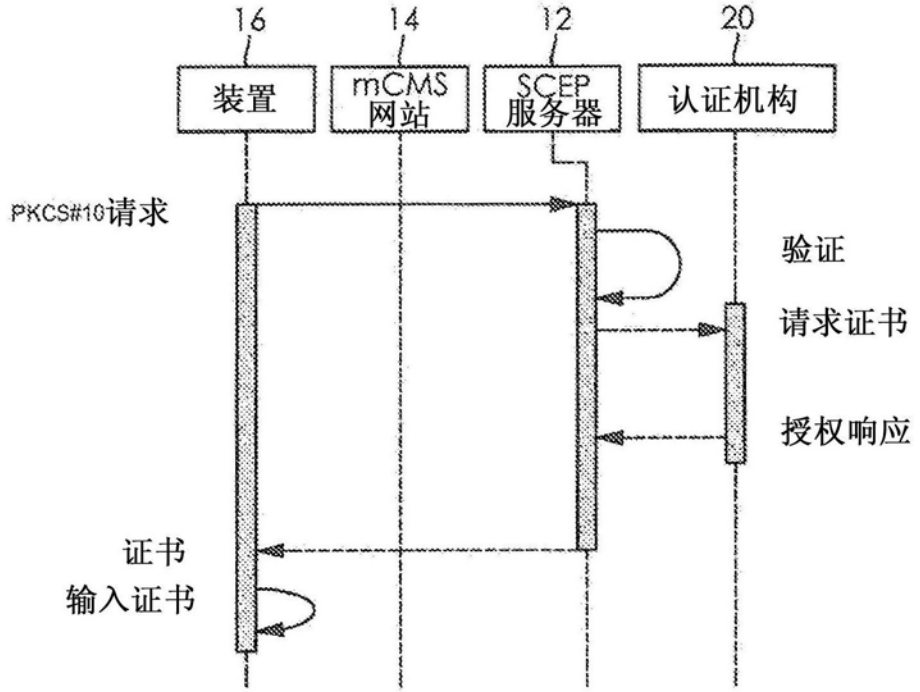

16
14
12
20
装置
mCMS
网站
SCEP
服务器
认证机构
PKCS#10请求
验证
请求证书
授权响应
证书
输入证书

图7

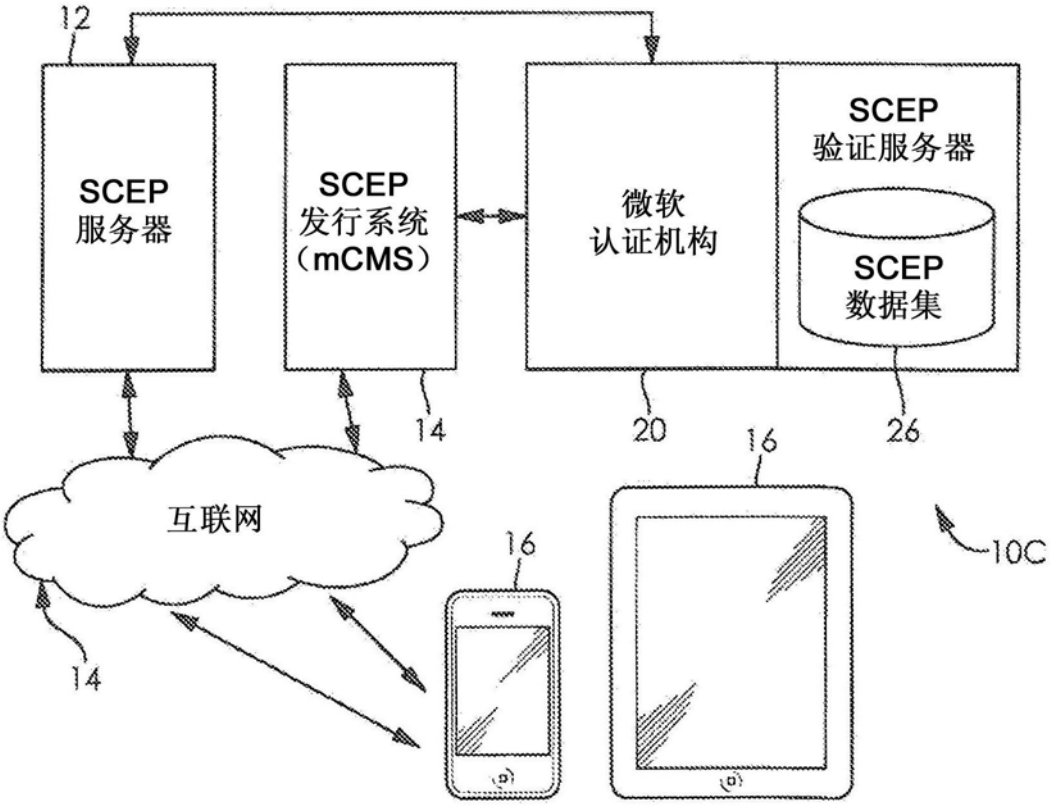

12
SCEP
服务器
SCEP
发行系统
(mCMS)
微软
认证机构
SCEP
验证服务器
SCEP
数据集
14
20
26
16
互联网
16
10C
14

图8

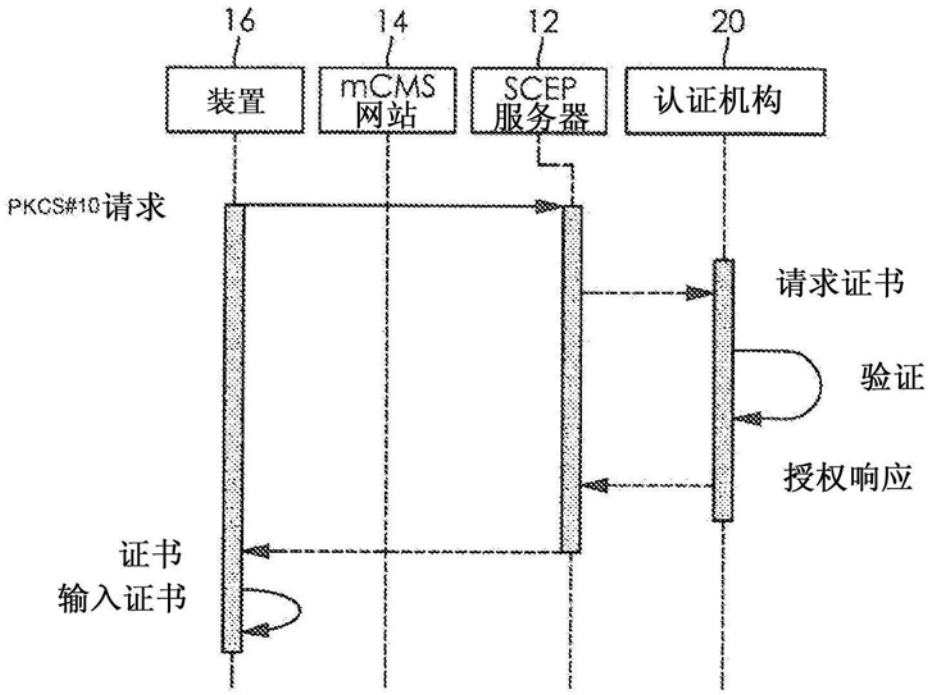

16
14
12
20
装置
mCMS 网站
SCEP 服务器
认证机构
PKCS#10请求
请求证书
验证
授权响应
证书
输入证书

图9

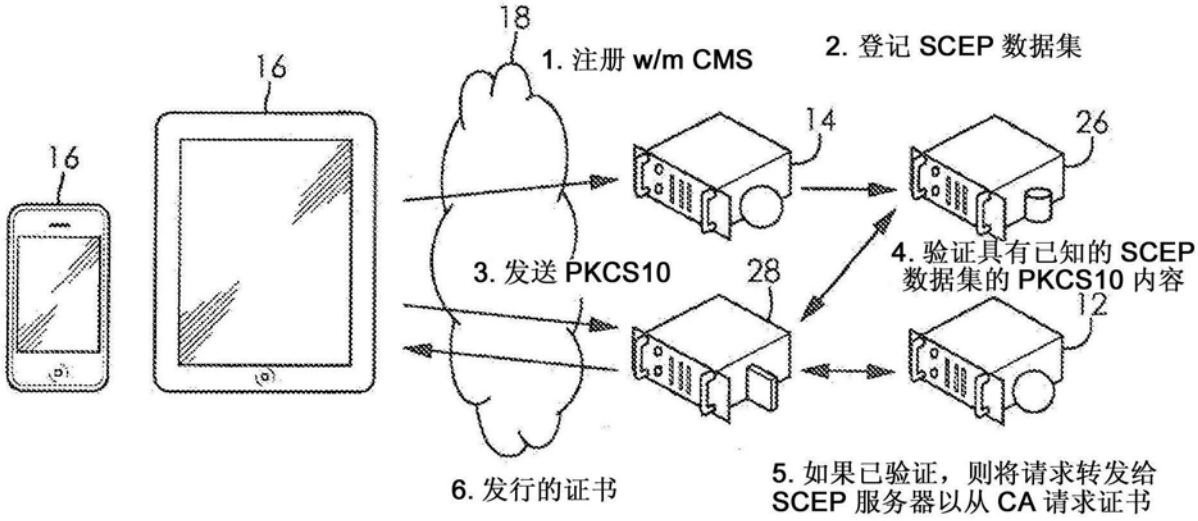

18
1. 注册 w/m CMS
2. 登记 SCEP 数据集
16
16
14
26
3. 发送 PKCS10
28
4. 验证具有已知的 SCEP 数据集的 PKCS10 内容
12
6. 发行的证书
5. 如果已验证，则将请求转发给 SCEP 服务器以从 CA 请求证书

图10

SCEP 口令	相应的证书内容说明				
	证书主题	证书主题 ALT 名称	密钥使用	扩展的密钥使用	证书模板
"EBF38299GHA994ST"	CN="JOHN SMITH"	UPN=JSMITH@CORP.COM	128	客户端认证; 文件签名	"XYZ CORP USER TEMPLATE"
"X99ABFF49923MM"	CN="FRED JONES" O="XYZ CORP"	UPN=FJONES@CORP.COM RFC822NAME=FRED. JONES@CORP.COM	(ANY)	(任意)	"AUTHENTICATED SESSION"
"45JK3342SDFMEEY5"	CN="MIKE WALLCE" OU="IPAD TESTING"	UPN=, MWALLACE@CORP.COM	64	(任意)	"XYZ CORP USER TEMPLATE"
"4409kel2SDNmE"	(ANY)	UPN=, BWILLIAMS@CORP.COM	(ANY)	(任意)	"IPAD TEST GENERAL"

图11