(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 103596123 B
(45)授权公告日 2017.05.10

(21)申请号 201310625441.6

(22)申请日 2009.01.21

(65)同一申请的已公布的文献号
申请公布号 CN 103596123 A

(43)申请公布日 2014.02.19

(30)优先权数据
61/022,127 2008.01.18 US
61/025,163 2008.01.31 US
61/031,630 2008.02.26 US
61/127,792 2008.05.14 US
61/060,725 2008.06.11 US
61/141,569 2008.12.30 US
61/141,586 2008.12.30 US

(62)分案原申请数据
200980107750.6 2009.01.21

(73)专利权人 交互数字专利控股公司
地址 美国特拉华州

(72)发明人 I·查 Y·C·沙阿
A·U·施米特 M·V·迈尔施泰因

(74)专利代理机构 北京润平知识产权代理有限公司 11283
代理人 陈潇潇 刘国平

(51)Int.Cl.
*H04W 4/00*(2009.01)
*H04W 12/00*(2009.01)
*H04W 24/00*(2009.01)

(56)对比文件
CN 1969580 A,2007.05.23,
WO 2008/001322 A2,2008.01.03,

审查员 李晓

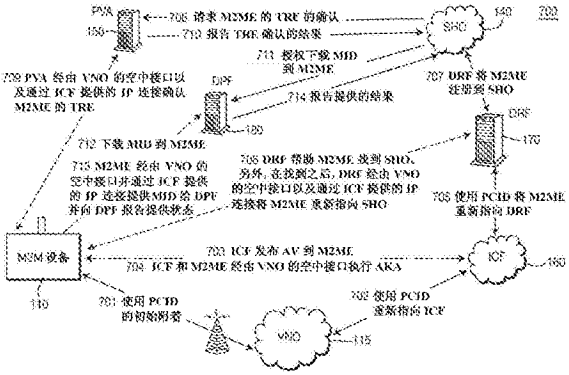
权利要求书1页 说明书34页 附图7页

(54)发明名称

一种由M2ME执行的方法

(57)摘要

公开了在包括访问网络运营商(VNO)、注册运营商(RO)和经由网络进行通信的机器对机器设备(M2ME)的系统中,一种由所述M2ME执行的方法,该方法包括:向所述VNO传送包括临时私人标识符的网络附着请求消息;使用所述临时私人标识符向所述VNO进行认证;当所述M2ME通过所述VNO而被认证时,接收互联网协议(IP)地址;使用所接收的IP地址建立经由所述VNO至所述RO的IP链路;从所述RO接收可管理标识(MID);以及在所述M2ME上供应所述MID并向所述RO报告成功消息。




CN 103596123 B

1.在包括访问网络运营商VNO、注册运营商RO和具有可信环境TRE的机器对机器设备M2ME的系统中，一种由所述M2ME执行的方法，其中所述VNO、所述RO和所述M2ME经由网络进行通信，该方法包括：

向所述VNO传送包括临时私人标识符的网络附着请求消息；

使用所述临时私人标识符向所述VNO进行认证，所述临时私人标识符是对于有效性周期有效的临时连接标识PCID；

所述TRE生成安全性关键可执行代码并向平台验证机构发送所述安全性关键可执行代码；

如果所述平台验证机构使用所述安全性关键可执行代码确认在所述M2ME中的所述TRE的完整性，则接收认证向量；

在所述M2ME通过所述VNO而被认证以及所述TRE被由所述平台验证机构确认之后，建立经由所述VNO至所述RO的互联网协议IP链路；

从所述RO接收可管理标识MID；

在所述M2ME上供应所述MID并向所述RO报告成功消息；以及

当所述有效性周期期满时，移除所述PCID由此另一个M2ME能够使用所述PCID。

2.根据权利要求1所述的方法，该方法进一步包括：

确认所述M2ME；以及

基于所述M2ME的确认，经由所述VNO向所述平台验证机构发送确认成功消息或确认失败消息。

3.根据权利要求2所述的方法，其中所述M2ME的确认基于由所述M2ME内的所述TRE执行的确认过程而至少部分被确定。

4.根据权利要求3所述的方法，其中所述确认过程在所述M2ME内被自发地执行。

5.根据权利要求3所述的方法，其中所述确认过程由所述M2ME半自发地执行。

6.根据权利要求1所述的方法，其中所述MID包括以下至少一者：通用移动电信UMTS用户识别模块USIM功能、凭证、或使所述M2ME能够向选择的家用运营商SHO认证的配置信息。

7.根据权利要求1所述的方法，其中所述RO包括初始连接功能ICF、发现及注册功能DRF和下载及供应功能DPF。

8.根据权利要求7所述的方法，其中所述初始连接功能ICF、所述发现及注册功能DRF和所述下载及供应功能DPF为所述网络中单独的实体。

# 一种由M2ME执行的方法

[0001] 本申请是申请日为2009年01月21日、申请号为200980107750.6、名称为“用于启用机器对机器通信的方法和设备”的发明专利申请的分案申请。

## 技术领域

[0002] 本发明涉及无线通信。

## 背景技术

[0003] 机器对机器(M2M)通信是一种实体之间的数据通信形式，当使用时，不必需要直接的与人交互。M2M通信的一个挑战是建立协议以使得使用的设备可以被远程管理而不需要任何的与人直接交互。

[0004] 已有的M2M方法缺少对通过空中对初步配置标识符的保护。这些方法在对设备的认证、注册以及供给的过程中没有利用关于M2M启用设备的信任状态(TS)的信息；它们不能保证M2M启用设备的已订运营商的安全改变；这些方法不能保证在M2M启用设备的初步认证中使用的认证和密钥协议凭证是可信任的；这些方法没有提供软件和固件的安全更新或M2M启用设备的重新配置。此外，M2M启用设备用户/订户的作用没有定义。因此，提供用于改进M2M性能、安全性以及可靠性的方法和设备是很有利的。

## 发明内容

[0005] 公开了一种用于执行安全的机器对机器(M2M)供给和通信的方法和设备。具体地，还公开了用于唯一识别机器对机器设备(M2ME)的临时私人标识符或临时连接性标识(PCID)。此外，还公开了用于在确认、认证以及供给M2ME中使用的方法和设备。公开的确认过程包括自发的、半自发的，且公开了远程确认。供给过程包括用于重新供给M2ME的方法。还公开了用于更新软件的过程以及检测对M2ME的损害。

## 附图说明

[0006] 从以下以示例的方式给出的并结合附图的描述中可以更详细地理解本发明，其中：

[0007] 图1示出了用于机器对机器(M2M)供给和通信的通信系统的示例框图；

[0008] 图2示出了机器对机器设备(M2ME)的示例框图；

[0009] 图3示出了自发确认过程的示例流程图；

[0010] 图4示出了半自发确认过程的示例流程图；

[0011] 图5示出了半自发确认的另一个过程的示例流程图；

[0012] 图6示出了远程确认过程的示例流程图；

[0013] 图7示出了M2ME的供给或预先供给的示例过程；

[0014] 图8示出了M2ME的供给或预先供给的可替换示例过程；

[0015] 图9示出了由新选择的家庭运营商使用的M2ME的预先供给的过程的示例流程图。

## 具体实施方式

[0016] 下文提到的术语“无线发射/接收单元(WTRU)”包括但不限于用户设备(UE)、移动站、固定或移动用户单元、寻呼机、蜂窝电话、个人数字助理(PDA)、计算机、M2M设备(M2ME)、家用节点B或能够在无线环境中操作的任意其它类型的设备。下文提到的术语“基站”包括但不限于节点B、站点控制器、接入点(AP)或能够在无线环境中操作的任意其它类型的借口设备。

[0017] 图1是用于机器对机器(M2M)供给和通信的通信系统100的示例框图。共享系统100包括M2M启用设备(M2ME)110、访问的网络运营商(VNO)115、注册运营商(RO)130、选择的家用运营商(SHO)140、平台验证机构(PVA)150。系统100还可以包括设备制造商/供应商(E/S)(未示出)。

[0018] 图1所示的VNO115为单个网络实体,但是为进行USIM/ISIM应用的初始注册和供给而被接入的所有接入网络可以被视为VNO。如果M2ME110针对不同SHO进行了注册,则VNO115保持VNO。如果M2ME110被注册到当前是VNO115的SHO140,则VNO115成为SHO。

[0019] VNO115用于提供对M2ME110的临时网络接入,其中可能需要接入凭证和认证。这可以基于临时网络接入凭证,例如PCID或任意其它的临时私人ID。当被认为是允许的时,VNO115可以提供对DRF170的开放网络接入,其中对接入到至少RO130的服务不需要凭证或而认证。例如,该功能在VNO115在注册和供给事件之后成为消费者的SHO时可以应用。在注册和供给过程被执行之后,VNO115将使用供给的USIM/ISIM应用提供完全的网络(和IMS)接入。

[0020] 所示的RO130包括ICF160、发现及注册功能(DRF)170、以及下载及供应功能(DPF)180。但是,本领域技术人员可以知道ICF160、DRF170以及DPF180还可以位于单独的实体中或集成到一个实体中。

[0021] ICF160是用于凭证确认的功能或机构,其允许为操作网络接入的注册和供应而临时接入到通信网络。ICF160的功能包括每个M2ME110的临时网络接入凭证和任意临时私人标识符的发行。这些功能可以用于认证初始临时网络接入以使USIM/ISIM应用供应过程发生。ICF160还可以被配置成通过空中给M2ME110供应可下载的M2M密钥、配置以及应用,用于下面论述的供应和重新供应过程。

[0022] ICF160还可以被配置成提供终端供应商以将M2ME110预先配置由ICF160发行的凭证。为了提供这些凭证,ICF160必须被配置成将凭证的安全传输提供给负责将该凭证嵌入到M2ME110的组织。ICF160还可以被配置成注册数据库中的凭证,并在信赖方请求时执行凭证的确认。这可以包括将认证向量和/或其它相关数据传输到该信赖方。应当注意到,在M2ME110成功注册到SHO140之前,所有的接入网络被视为被访问网络。这允许通过常规网络到SHO140的透明连接性,而不需要任意网络改变。

[0023] DRF170是具有特定SHO140的后购买选择以及M2ME110注册到SHO140的能力的功能。其可以是独立的服务,可替换地,其可以由SHO140操作,该SHO140的RO130可以是仅可经由SHO的3GPP网络连接的,或可经由因特网直接连接的,并且可发现的,例如通过使用M2ME110中的功能被发现。

[0024] DRF170应当支持至少以下使用相关的功能:(1)允许消费者在M2ME110递送后从供

应商选择SHO140；(2)允许M2ME110具有使用临时认证网络接入或限制的开放网络接入的到RO130的IP连接；(3)在M2ME110已与任意SHO140不相关联时，允许M2ME110经由被访问网络运营商请求USIM/ISIM应用供应发生；(4)批准供应请求并认证DPF180以供应M2ME110；以及(5)支持M2ME110的所有者注册M2ME110。

[0025] 为了支持上述的使用相关的功能，DRF170可以支持M2ME110与SHO140的关联性。可替换地，DRF170通过直接使用VNO网络提供的IP连接性可以是可发现的和可直接寻址的。在任意一种情况中，DRF170必须经由PVA150支持凭证的确认，M2ME110拥有该凭证作为其可信任环境(TRE)230的真实性的证明。DRF170还必须支持到DPF180的连接，以用于认证和核查。还应当注意到，确认不仅可以是凭证的确认而且还可以是TRE230以及可选地整个M2ME110的确认(如果TRE230期望如此)。例如，确认可以包括建立M2ME功能的信赖性。

[0026] DRF180还可以支持将被下载到M2ME110的数据分组(例如USIM/ISIM凭证、文件和可执行程序)的生成或获得。DRF180还可以被配置成将该数据安全地传送到PS。可替换地，这些功能可以由DPF180提供。

[0027] 最后，DRF180还可以促进M2ME110与DPF180之间的安全性关联的设置。这可能需要安全令牌的生成以及将该安全令牌通过安全信道传输到M2ME110和DPF180。

[0028] DPF180能够远程供应USIM/ISIM凭证给M2ME110。DPF180的功能包括从DRF170接收供应M2ME110的授权。这可以包括提供用于与M2ME110通信的安全令牌。DPF180还用于从DRF170接收将被下载的应用包。可替换地DPF180可以根据存储的规则生成该应用包，并告知DRF170凭证已经被下载到M2ME110。

[0029] DPF180还被配置成支持将USIM/ISIM应用或USIM/ISIM参数供给到M2ME110，这在下面描述。除了供给之外，DPF180还可以被配置成执行以后的对给USIM/ISIM应用或USIM/ISIM参数的更新、以及之后供给包含这些功能的新应用。DPF180还可以被配置成通知DRF170成功或不成功的供给事件。

[0030] SHO140是网络运营商，其与M2ME110的消费者或终端用户之间具有商业关系，且用于向消费者计费。SHO140可以担当一些或所有的其它角色，尤其是DRF170和DPF180，或它们都可以是单独商业实体，其与SHO140以及彼此之间具有可运作的关系。

[0031] M2ME110初始没有被安排与服务供应商进行操作，且由此与VNO115的通信建立到RO130的信道。为了供给服务，每个M2ME110具有其自身的临时私人标识，例如PCID，其能够使任意VNO115识别M2ME110并允许对其提供的服务的临时接入以及将初始连接性消息发给合适的网络组件，以下载服务并将服务提供给运营商。

[0032] PVA150是负责证明M2ME110中的安全设备(用于下载的USIM/ISIM应用的存储和执行)的真实性的凭证的机构。这种功能可以由发行凭证(例如证书和密钥对)和提供凭证确认服务的一个或多个商业组织来执行。安全设备可以是UICC、TRE或一些其它形式的内嵌到M2ME110的安全模块。在安全设备的强力认证是提供USIM/ISIM应用的前提时需要这种功能。PVA150还可以提供例如创建并发行用于证明M2ME110中安全设备的安全性的凭证的功能。但是，还有可能的是该功能可以由另一个实体来执行。当被使用了必需的协议信赖方请求时，PVA150还可以提供例如上述的凭证确认的功能。这可以包括将认证向量和/或其它相关数据安全传输到信赖方。PVA150还可以提供例如关于设备发行的凭证有效性的数据维护的功能。

[0033] 设备制造商/供应商(E/S)(未示出)还作为图1的通信系统100。具体地,M2ME110从ICF160安全地获得用于认证临时初始网络接入的凭证。E/S还可以在递送到消费者之前支持使用这些初步网络接入凭证对M2ME110进行重新配置以允许临时初始网络接入。此外,E/S可以从PVA150安全地获得凭证,该凭证用于经由ICF160向DRF170证明M2ME110编译有标准化的安全性需求集合。该活动可以外包(contract)给具有所需安全基础设施的被批准的组织。

[0034] E/S还可以用于在递送到消费者之前给M2ME110预先配置凭证。该预先配置活动可以外包给具有所需安全基础设施的被批准的组织。E/S还可以提供用于终端拥有者选择所期望的DRF170和SHO140的装置,或提供用于在终端连接到接入网络(AN)时使选择所期望的DRF170和SHO140自动发生的装置。

[0035] 图2示出了图1的M2ME110的示例图。M2ME110包括发射机215、接收机220、处理器225、可信环境(TRE)230。可选地,M2ME110可以包括全球定位系统(GPS)单元235、订户标识模块(SIM)240以安全时间单元。

[0036] M2ME110可以被配置成支持多个不同信任机制(例如TRE230)或任意其它可信处理或存储机制(例如SIM240或ISIM)。这些信任机制还可以更完全集成到公共AKA协议以包括“信任状态”信息和/或M2ME110中TRE230保护的任意密钥,以在完全AKA可以发生之前以及建立认证之后保护M2ME110和网络元件之间的任意通信(不仅仅是PCID的传输)。

[0037] 可选地,SIM240还可以被增强以包括可信处理模块(TPM)或移动可信模块(MTM)的功能以支持上述操作。可替换地,SIM240可以与M2ME110中的TPM或MTM紧密操作以实现期望的功能。还应当注意到SIM的功能还可以在TRE230中被实现。这允许标识管理中具有更大的灵活性。

[0038] 可选地,M2ME110可以被预先供给至少一个E/S安装的AKA根密码(secret),其中至少一个AKA根秘密在任意给定时间都是激活的。AKA根秘密可以由SIM240来保护,且应当没有被更改过。SIM240可以被配置成从激活的AKA根秘密中导出会话密钥。

[0039] M2ME110还可以被配置成提供信任状态信息给ICF160。AGI信任状态信息然后可以用于在M2ME110附着到VNO115时的初步认证。信任状态信息还可以用于导出会话密钥(CK和IK)。

[0040] 应当注意到,TRE230的功能可以专门在一个组件上被执行,或被分布到M2ME110中的内嵌可信组件之间。可替换地,TRE230的功能可以在可移动SIM模块上被执行。

[0041] 下面是将PCR寄存器值绑定到会话密钥CKn和Ikn的公式的示例,其中n指最近更新的CKn和Ikn的索引:

[0042]

$$CKn=f3_K(RAND \| PCR0_n)$$

$$Ikn=f4_K(RAND \| PCR0_n)$$

等式 1

[0043] 其中,$f3_K()$和$f4_K()$分别指共享主秘密K中的加密密钥和完整性密钥的AKA密钥导出函数,RAND是CATNA生成的认证向量(AV)(被发送到M2ME110并由此在AKA过程中由

M2ME110共享)中的随机的现时(nonce),以及$PCR0_n$指M2ME110上的MTME内的PCR0寄存器的最近值。注意到PCR0寄存器的当前值表示M2ME110的最近后置根信任状态的描述。

[0044] 注意到根据等式1,$CK_n$和$IK_n$的值在M2ME110的PCR0值在两个根之间改变时(以及在该情况下)发生改变。为了这种方案起作用,ICF160在M2ME110的后置根信任状态发生改变时必须还知道PCR0值的改变(或者,更一般地,M2ME110的"信任状态")。这在ICF160知道影响M2ME110的后置根信任状态的M2ME的OS、固件或应用的任意合法或授权的更新的调度和实质的情况下成为可能。这可以通过在下述过程中包含PVA150和/或ICF160来完成。根据合适的过程,可以确保在M2ME110与ICF160之间共享的AKA加密和完整性密钥被更新并对M2ME110的认证有用,由此会话密钥反映M2ME110的最当前"信任状态"值,从而增强AKA密钥导出过程的新颖度和安全性。

[0045] 应当注意到除等式1之外的其它绑定公式可以被考虑,只要会话密钥可以以M2ME110与ICF160之间相同的方式被更新、且在M2ME110处的更新过程本身在可信任执行环境中被实行(例如使用可信计算技术提供的可信任执行环境)。

[0046] TRE230是M2ME110中逻辑独立的区域(具有对该独立情况的硬件支持)。其不必是可移动模块,即可以是IC中的功能或可以分布到IC组之间的功能。TRE230定义到外部的逻辑和物理接口,该接口仅在被授权与TRE230直接通信的实体的控制下可用。

[0047] TRE230提供用于多个可管理标识(MID)和与MID的供给和管理有关的一些功能的安全存储和安全执行环境的信任根。MID是完全安全应用和其相关参数、凭证等的通用术语。MID可以结合任意预定管理功能,例如标准USIM应用和密钥,或其它安全应用,例如ISIM或安全支付应用。之后,MID可以用于指代可管理标识、预定管理标识、USIM应用、ISIM应用、虚拟SIM(vSIM)或任意其它动态安全标识方案。

[0048] TRE230还可以在安全带外设施中被预先提供有所需密码密钥和其它凭证。TRE230的其它安全性关键功能可以以相同的方式被预先提供给M2ME110。进一步的功能可以在M2ME110被发行后典型地通过下载来提供。

[0049] TRE230还提供对物理和逻辑攻击的保护程度,支持并增强其自身安全性策略且安全性足以允许当前仅在UICC或其它智能卡平台中被执行的MID的存储和执行。TRE230还具有连接M2ME110的位于TRE230外部的部分的接口。

[0050] TRE230具有其自身内嵌的唯一标识,其一般与M2ME110的标识相关联,当被使用时,M2ME110的标识也被嵌入到TRE230中。这样,TRE230可以被配置成使用标准协议向发行机构安全地认证这些标识。发行机构然后可以确认TRE的标识为发行的有效的TRE230和M2ME110的标识。这些标识中的每一个被内嵌作为在M2ME110被发行之前发生的物理上安全的带外过程的部分。

[0051] TRE230可以在具有一些增强功能的嵌入的UICC中被实现,或可替换地作为M2ME110上的结合方案使用M2ME110提供的硬件和软件组件来执行。如果TRE230在增强型UICC中被执行,则TRE230仍然支持MID和TRE230中可管理标识引擎(MIDE)的功能的下载以及远程供给和管理。

[0052] 如果TRE230被实现为M2ME110中的结合方案,则M2ME110支持构成TRE代码库的软件代码和数据的完整性检查。TRE代码在M2ME110加电/启动时间应当被检查至少一次。可选代码检查可以在可操作使用M2ME110期间进行以作为在定义的时间间隔或某些触发/事件

时的后台处理。此外，代码检查的覆盖可以扩展到覆盖全部或部分的M2ME110的检查。

[0053] 在可替换的增强中，TRE230可以包括对多个隔离的可信任域的支持，每个域由TRE230中的风险承担者所有人所拥有。这样的域可以彼此隔离，防止损害和未授权的接入，并提供域间服务，例如认证和/或证明功能。

[0054] 在一些使用的情况中，对于其多数部署循环，M2ME110可以工作在休眠状态下，并且只偶尔或频繁地连接到3G网络。在这样的情况中，TRE软件代码的运行事件完整性检查可以在休眠状态周期期间发生。这样，代码检查不会干扰TRE230或M2ME110中的其它进程，由此在M2ME110重新连接到SHO140时代码检查可以准备好。

[0055] 每个M2ME110必须被分配对于M2ME110来说唯一的临时私人标识，临时连接性标识(PCID)。PCID是唯一识别每个M2ME的临时私人标识。当需要时，该PCID需要由ES将其安装在M2ME110中，以允许M2ME在与任意特定SHO(例如SHO140)相关联之前在3GPP网络中注册。PCID初始由ICF160发行，该ICF160将PCID发送到与其有供应关系的ES。ES然后将PCID提供给M2ME110的TRE230。当PCID从M2ME110出现在VNO115中时，VNO115可以识别出该PCID具有标准IMSI的格式，且之后将M2ME110引导给RO130以建立用于供给的初始连接。

[0056] 在一个实施方式中，单个PCID可以在有限时间间隔(这里为“有效性周期”)是有效的(由M2ME110执行)。有效性周期可以专门由M2ME110的TRE230来控制。每个M2ME设备可以接收PCID和有效性周期。在时间期满后，M2ME110可以移除该PCID。PCID然后可以在被提供了相同PCID的另一个M2ME(未示出)尝试附着到核心网络时被重新使用。但是，一般来说，第二个M2ME的PCID的有效性周期不应该与之前的M2ME的PCID的有效性周期重叠。

[0057] 在第一个M2ME110不再使用PCID之后，在新M2ME110的合适有效性周期没有终止之前，一般PCID可以不再发送给新M2ME。

[0058] 在另一个实施方式中，PCID可以被系统地再分配(没有PCID的同时使用)。这可以包括M2ME110的寿命期。有限数量的PCID可以被系统地预先提供给M2ME110。这可以运行在开发TRE230的能力时的初始网络连接性的自发管理。假定M2ME110被释放在大小为N的组中。第j批的M2ME被称为M_i,j,其中j=1,…,M。PCID分配可以被初始化为具有大小为N×M的矩阵(P)_{i,j}。M2ME110M_i,1在产生期间将列P_i,*载入到TRE230中。当M2ME被释放时，安全计时器或单调计数器被初始化，激活并置于TRE230的控制下。批1的M2ME110(即M_i,1)使用P_i,1达到基于被初始化的时间或计数器的确定的时间间隔T或预定的次数。在给定时间(有效性周期)之后，M_i,1的TRE丢弃P_i,1并使用P_i,2。可以注意到时间间隔或使用次数应当使得第二批还没有被释放。当第二批M_i,2被释放时，还开始使用P_i,1，在这个时间点，该P_i,1被M_i,1释放。理想地，MxT包括需要得到网络支持的所有M2ME的整个操作时间。

[0059] 该实施方式可以允许网络确定设备在寿命周期中处于什么位置。之前的PCID可以被安全地再分配给信息设备。该方案利用M2ME制造商与TRE230的内在的信任关系。在TRE230中PCID列向量的处理以及TRE230进行的时限的执行产生对PLMN运营商的保证：阻止同时使用PCID，且M2ME110在其整个操作时间具有能使用的有效PCID。

[0060] 但是，该实施方式可能影响网络运营商，这是因为网络运营商可能在制作过程中的某个点将PCID集递送给制造商，或在释放之前将该PCID集安装到安全设施中。还有，M2ME可以被预先提供有多个PCID。M2ME可能支持后批PCID的重新供应。多个M2ME在任意给定时间共享相同批的PCID，这可能存在“机会”冲突，其中两个或更多个M2ME可能从同一批中选

择相同的PCID并尝试同时连接，这会导致“PCID冲突”。如果批的大小(行N的大小)大于使用相同批的PCID的M2ME的数量，并且如果M2ME以随机的方式选择PCID来使用，则PCID冲突的可能性可以更小。

[0061] 具有时间限制的PCID管理需要给定精确限制内的M2ME内部时钟的同步。这必须包括例如单个M2ME110的下电事件，在下电事件后可能需要再同步。因此，TRE230应当保持并管理时间基数并支持与网络中可信时间源的同步。可选地，TRE230可以依赖位于M2ME110中的可信时间源，如图2中所示。

[0062] M2ME110可以被配备有自发地理定位设备，例如GPS235。M2ME110的TRE230具有对地理定位设备的安全接入。

[0063] M2ME110可以被分布在不同区域中，并被布置为使得没有两个M2ME可以在物理位置上同时建立到相同接入网络(AN)小区或基站的无线电连接。因此多个M2ME可以被预先提供有相同的PCID，而且还提供有目的地理位置(D)以及容忍范围(r)，该目的地理位置(D)对于每个M2ME是唯一的。该数据可以被安全地存储在TRE230内或被安全加密，以使得只有TRE230能够接入该数据。

[0064] 在M2ME1100尝试初始接入网络之前，TRE230确定当前地理位置并检查该地理位置是否与容忍范围内的位置D一致。如果一致，则TRE230释放用于初始网络接入的PCID。这样可以向AN保证没有两个M2ME使用相同PCID经由同一个小区试图接入。

[0065] 但是，在一些情况中，AN可能需要区分从不同小区的使用相同PCID的同时接入尝试。因此，AN可能需要记录初始网络连接性服务中的(PCID，小区ID)配对。因此，在这种情况中对核心网络会有一些影响。

[0066] 在可替换实施方式中，M2ME110对网络的接入只经由预定网络小区才被允许。预定网络小区通过它们的网络小区标识符来识别，该标识符位于M2ME的TRE中。该标识符替代配对(D,r)。

[0067] 在另一个可替换实施方式中，M2ME在理位置上可以被移动。当M2ME110被移动时，网络接入被禁用。为了启用M2ME的移动性，M2ME110可以被预先提供有三元组(PCID,D,r)的集合，其指定可以使用某些PCID的不同的位置。在M2ME110的初始网络连接尝试之前，TRE230检查当前地理位置是否位于目的D中的一个的范围r中的一个之内，并且在检查成功的情况下释放相应PCID。

[0068] 此外，三元组(PCID,D,r)可以被分配寿命，即允许使用的时间寿命，其如上所述被使用和执行。凭证位于五元组(PCID,D,r,t1,t2)中，其中t1和t2表示有效性周期的开始时刻和结束时刻。这描述了M2ME110的可允许的运动路径。例如，M2ME110的运动可以在移动部署情形(例如在车中)中受到控制。当M2ME的TRE230被迫进行频繁重新连接、或以其它方式使用PCID时，网络服务可能检测到失败(以超时的形式)，并被理解为M2ME110离开确定的路径，由此报警。

[0069] 以上提出的方法和设备足够提供M2ME110在其整个寿命过程中的移动性和/或PCID管理需求。因此，期望一种管理，即重新提供和删除五元组(PCID,D,r,t1,t2)的方法。

[0070] 可以使用PCID更新服务(PUS)来重新提供该五元组。PUS可以识别出TRE230(唯一对应于M2ME110)在更新。PUS可以是CCIF服务的一部分或是网络中的单独组件。更新可以包括对一个或多个五元组(PCID,D,r,t1,t2)进行改变。TRE230标识(ID)可以被发送到网络服

务，该网络服务可以将TRE ID关联到当前网络(IP)地址。例如，网络实体可以是PVA150，其在获得完全网络连接的过程中确认TRE230和M2ME110的完整性，或可以是连接性凭证发行功能(CCIF)，其与PVA150一起工作以确认M2ME110的有效性，发行一个或多个新PCID并远程提供该一个或多个新PCID给M2ME110。该远程提供还可以被委派给网络中的DPF170。

[0071] 重新指向过程在PUS连接到目标M2ME110和TRE230并请求其状态确认(例如，经由下面描述并在图3-5中所示的平台确认过程)时开始。这可以向PUS指示TRE230将安全地丢弃旧的五元组(PCID,D,r,t1,t2)(的集合)并安装期望的新的五元组。在成功确认后，PUS可以递送新的五元组(PCID,D,r,t1,t2)和被丢弃的旧五元组(PCID,D,r,t1,t2)的列表。TRE230自发地安装新的五元组并(为了确保连续连接性)丢弃旧的五元组。

[0072] 在另一个实施方式中，TRE230能够产生(伪)随机数，其可以被连接到PCID以减缓冲突。可以使AN能够了解并区分另外的信息。

[0073] 通信实体是M2ME110、TRE230以及网络接入点(NAP)(未示出)。NAP可以是例如与VNO115相关联的e节点B(eNB)。TRE230在单次初始网络连接尝试中生成将被使用的随机数(RAND)。TRE230应用完整性保护方法，例如密钥散列函数，其中RAND输入第二参数，例如另外的需要的数据(D1)以及PCID。TRE230发送该数据为：

[0074] TRE→eNB:RAND||PCID||D1||M1:=MAC(PCID||D1,RAND)。

[0075] eNB验证消息认证码(MAC)并从有效载荷(D2)中建立返回包，而所接收的数据为：

[0076] eNB→TRE:D2||M2:=MAC(PCID||D2,M1，并将其发送给TRE。

[0077] 该方法扩展至在初始网络连接时交换的所有后续消息。后续消息的交换将包括包含任意新消息元素的数据元素的MAC和紧挨的之前交换的MAC。eNB和TRE230可以在使用上一个值$M_{n-1}$来建立新$M_n$的通信过程中区分消息。

[0078] 为了避免对这种通信的人为介入型攻击，用于通信方认证的消息中可以包含预先建立的、或商议/共享的秘密。

[0079] 在PCID中包括合适的MAC值这一动作是可选的，但是有利的是建立散列表并有效地区分具有不同和/或公共PCID的多个M2ME的同时活动的网络连接尝试。这可以防止在初始网路连接通信的每个消息中发送PCID(可能以明码报文的形式)，这也是安全性问题。

[0080] eNB可以保持表示使用PCID的所有同时活动的网络接入尝试(这里称为信道)的状态的表。对于每一个信道，其包含表1中的信息。

[0081] 表1

[0082]

| PCID索引 | 活动的散列值 | 数据历史 |
|---|---|---|
| I | $M_2$ | RAND,$D_1$,$D_2$ |

[0083] 第一列包含属于该特定信道的PCID索引，指向针对所有信道而当前活动的所有PCID的列表中的项，PL:=[PCID1,...PCIDN]。这节省了对上表的存储，但是如果存储器不是问题，则该列可以包含完整的PCID。

[0084] eNB接收信道上的第三消息：

[0085] TRE→eNB:D3||M3:=MAC(PCID||D3,M2)

[0086] 对于i=1,…,N，直到以下过程成功，eNB才从PL中选择$PCID_1$。对于第一单元(cell)中具有PCID索引I的所有表的行，eNB计算M:=MAC($PCID_1$||$D_3$,$M_2$)，其中$M_2$是从行中的第二个

单元中选取的。如果M=$M_3$，则达到成功状态，且搜索过程结束。对应于最后接收到的第三消息的信道行数被返回。$D_3$被添加到数据历史，且在所选表的行的激活散列值单元中$M_2$被$M_3$替换。该过程对所有之后的通信步骤被重复。

[0087] 可替换地，不是PCID，而是在第一消息之后的消息可以包含信道索引I以更有效地找到之后消息的相关联信道。

[0088] 在M2ME110和/或eNB的资源（尤其是存储器）被限制的情况下，活动的PCID可以被锁定。其优点在于防止M2ME110使用被锁定的PCID。

[0089] 例如，M2ME110打开与eNB的信道以获得PCID。具有第二TRE（未示出）的第二M2ME（未示出）尝试打开使用相同PCID的到eNB的信道，而第一信道仍然是打开的。eNB可以通过传送$M_1$来响应第二M2ME的TRE的第一消息。因此，第二TRE被通知该PCID当前被占用。第二TRE可以针对另一个信道开启尝试来使用安装的PCID池中的另一个PCID，或可以在再次使用相同PCID之前等待预定时间间隔。

[0090] 可替换地，PCID可以由涉及的实体活动地解除分配。M2ME的TRE230可以在PCID已经用于获得完全网络连接性时（即在下载了相关证书之后）丢弃使用过的PCID。多个事件可能导致丢弃PCID。例如，如果TRE230以及达到用于完全网络连接性的协议的成功运行保证完全网络连接性的状态，则可以触发丢弃PCID。如果有效性周期期满，则如果网络实体（例如eNB、安全性网关或专用PCID管理实体）强制进行丢弃，或如果网络外部的实体（例如M2ME110的制造商）强制进行丢弃，则可以触发丢弃PCID，这可以建立通过VNO115到M2ME110的安全连接。

[0091] 无论什么事件触发了丢弃，关于该事件的信息可以都用于适当地对该PCID进行解除分配，即释放该PCID以使其由其它M2ME再使用。可以建立从TRE230到M2ME的制造商的连接来发送解除分配事件。制造商可以更新释放的PCID的运行列表，并且在释放时再使用它们来将PCID施加到新M2ME上。

[0092] 可替换地，网络中的实体（例如，ES、已有的SHO140、新SHO（未示出）或ICF160）可以被配置成更新PCID，以在例如发起从一个SHO到另一个SHO的预定改变时促进进一步的连接性操作。一旦M2ME110被提供，则初始网络的更新值接入凭证，PCID可以作为MID被递送到M2ME110以在将来用于帮助向新SHO提供服务。凭证可以专门在M2ME110的TRE230中被提取、存储以及使用。

[0093] 在由于SHO的改变而导致的凭证重新提供过程之前，M2ME110可以被通知其已有的初始网络接入凭证，PCID已经期满或将要期满。M2ME110可以请求并接收来自E/S、已有SHO140、新SHO或ICF160的新的初始网络接入凭证。可替换地，M2ME110可以从这些网络组件中的一个网络组件接收源自E/S或新SHO的新PCID，使得在M2ME110从原始状态做出新的初始网络接入尝试时，该PCID可以将M2ME110路由至新SHO。

[0094] 在一个实施方式中，M2ME110可以被预先提供有U(I)SIM应用、PCID以及一个集合以上的AKA根秘密，其中一次使用一个活动的集合。在PCID改变后，M2ME110被命令使用下一个集合的AKA凭证使得这些凭证可以用于提供到M2ME110的3GPP连接，由此便于将运营商和预定重新提供改变到新SHO。

[0095] 以上描述了初始网络接入凭证和重新提供服务的替换的一些可能的方法。应当理解，所有解除分配过程中的安全性考虑需要PCID在解除分配过程中不以明码报文的方式传

输。此外，对于所有解除分配过程，在解除分配过程中通信方式应当被认证。

[0096] 对于执行TRE230或M2ME110的信任状态或相关数据和凭证的确认或认证来说，有三种基本不同的可能性，这些可能性包括：(1)自发确认；(2)半自发确认；以及(3)远程确认。每种可能性将参照图1所示的架构进行更详细地描述。

[0097] 自发确认是这样的过程：通过该过程，M2ME110的内部确认被认为在M2ME110允许其经历网络附着之前已经发生。

[0098] 半自发确认是这样的过程：通过该过程，不依赖外部网络实体，在M2ME110自身内评估M2ME110的有效性。这种确认的结果以及将TRE230的认证与M2ME110的有效性进行绑定所需的证据被发送到远程实体，例如PVA150，其基于来自M2ME110的消息的内容来做出决定。从M2ME110到PVA150的信令应当被保护。

[0099] 远程确认包括这样的过程：通过该过程，外部网络实体(例如PVA150)在其接收到M2ME的TRE230生成的确认证据以及在TRE230与M2ME110之间绑定的证据之后直接评估M2ME110的有效性/完整性。为了远程确认而在M2ME110与PVA150之间发生的通信应当被保护。

[0100] 如果TRE230执行M2ME110完整性的自发确认，则不给外界提供直接的确认证据。外界认为由于M2ME和TRE被指定并实施的方式，其内部完整性检查失败的M2ME110将由其TRE230阻止该M2ME110将其自身附着到网络或获得到远程实体的经认证的连接。例如，安全根过程促进M2ME110中代码的安全引出，但是并没有外部信令，这是与依赖完成该目的的设备不同的情况。

[0101] 图3示出了由TRE230执行以确认M2ME110完整性的自发确认过程300的示例。

[0102] 首先，TRE230检查TRE230是否达到安全启动的预定义状态(310)。接下来，TRE230检查M2ME110剩余的需要安全启动的预定部分是否达到预定义的安全启动状态(320)。

[0103] 然后TRE230自身或位于TRE230外部但受到该TRE230的完整性保护的M2ME110中的测量组件可以进行进一步检查(330)。在该后阶段检查中，M2ME110剩余部分的其它组件、配置或参数的完整性在它们被载入或启动时或在其它预定义运行时间事件时被检查，无论什么情况下该事件可用于测量组件。

[0104] 最后，TRE230允许M2ME110进行请求的认证过程(340)。

[0105] 自发确认是在需要外部通信的情况下最经济的方法。但是，自发确认不允许任意外部实体在网络接入期间或未中断联系阶段独自评估TRE230或M2ME110的完整性。也就是说，网络或其它通信方所认为的M2ME110的可信度只依赖于M2ME110的TRE230的安全性特性的技术规范，如同基于简单智能卡的认证的情况。

[0106] 因此，TRE230还可以存储确认过程以及该确认过程的响应于自发确认的每个事件的结果(例如，在网络接入尝试之前)的日志。例如，存储的测量日者和平台配置注册(PCR)值可以被存储并用于使用可信计算群组原则来保护M2ME110的完整性。

[0107] 该存储的数据还可以用于外部核查，因为该数据组成了核查记录。该核查数据被存储到安全内部档案中，该档案位于TRE230中或受到TRE230的保护，由此在没有检测到损害的情况下，该档位不能更改。由此提供数据的完整性保护。

[0108] 此外，核查数据专用于调用哪个自发确认(例如，在运行网络接入协议的特定情况下)。这可以通过在核查数据中包含唯一识别确认目的的数据来实现。

[0109] 例如，在接入协议中建立的共享秘密或凭证可以被附着到核查数据，且TRE230可以将数字签名应用到产生的数据集以保护其完整性。与M2ME110无关的实体然后可以在任意之后的时间点请求核查数据。例如，该实体可以周期性地请求核查数据来建立受质疑的M2ME110在每个早期的网络接入事件是否是可信赖的。该证据与TRE230和M2ME110的标识凭证然后可以与网络侧的关于网络接入尝试的协议一起进行反向检查，以进一步确认TRE230的标识和信赖性并检测M2ME110的损害。

[0110] 图4示出了TRE230执行M2ME110的完整性半自发确认的过程400。当过程400开始时，TRE230检查该TRE230是否已经达到安全启动的预定义状态(410)。接下来，TRE230检查需要安全启动的M2ME110的其余部分的预定义部分是否已经达到预定义的安全启动状态(420)。之后，TRE230自身、或位于TRE230外部但受到TRE230的完整性保护的M2ME110中的测量组件可以进行进一步的检查(430)。在该后阶段检查中，M2ME110的剩余部分的其它组件、配置或参数的完整性在它们被载入、启动时或在任意其它预定义运行时间事件(可用于测量组件)处被检查。

[0111] 例如PVA150的远程实体可以间接知道M2ME110已经通过半自动确认测试。存在到网络的关于确认结果的显式信令。该信令应该起源于TRE230中并应该通过加密方式来保护(440)。此外，信令在MID下载所需的M2ME110认证之前，确保是下载目标的M2ME110组件的完整性。该信令还可以包括TRE认证与用于实际有效性检查的M2ME110中的资源之间的绑定的证据。该证据还可以包括从M2ME110发送到网络的令牌，该令牌提供用于建立TRE230和M2ME110的验证的进一步信息。

[0112] 图5示出了TRE230的完整性半自动确认的可替换过程500。该过程500从PVA150或SHO140请求TRE230周期性地执行确认时开始(510)。该请求可以在M2ME110首次被注册后被发送，或该请求可以在M2ME110首次被SHO认证时被发送。

[0113] 可替换地，该请求可以被周期性地发送，作为来自PVA150或SHO140的受保护操作维护(OAM)消息。“周期性重新确认”的周期可以相对较长，但是仍然短到足够使SHO140对确认的“新鲜度”感到安全。

[0114] 接下来TRE230基于请求来执行确认过程(520)。一旦成功确认，则TRE230发送确认响应消息到PVA，该响应消息可以包括TRE230产生的用于指示上一个确认何时发生的时间戳(530)。可替换地，TRE230可以在周期性确认循环的当前回合终止之前发送描述最后的确认发生的消息。

[0115] 应当注意到没有关于确认“结果”的显式信令，只有作为认证请求部分的一些间接指示，用于指示预定周期性确认确实已发生。该指示可以包括数据或这一过程被执行的时刻。

[0116] 图6是远程确认M2ME完整性的过程600的示例。为了开始过程600，M2ME110可以在预定义的安全状态启动(610)。在达到安全状态后，M2ME110可以请求TRE230生成平台有效性的证据(620)。之后，TRE230收集用于产生来自M2ME110的其余部分的这种证据的材料(630)。例如，该材料可以包括M2ME110中的安全性关键可执行代码、用于M2ME操作系统(OS)的凭证、设备ID等。然后，TRE230生成用于确认M2ME110的证据，并以加密的方式保护该证据的完整性和/或保密性(640)。接下来，TRE230将该受保护的证据传递到M2ME110(650)。M2ME110将该受保护的证据转发到PVA150(660)。

[0117] 在接收到受保护的证据后，PVA150评估该证据并确定M2ME110是否足够值得信任以允许它继续执行设备认证以及允许下载MID(670)。

[0118] 可选地，上述过程的一些元素可以与用于M2ME认证的过程结合，该M2ME认证是MID下载的前提。应当注意到，TRE230与PVA150之间的通信应当被保护。

[0119] 在上述三个确认过程中的任意一个确认过程被执行后，在许多情形中期望M2ME确认与认证之间的绑定。在自发确认的情况中，确认可以是证明M2ME110的安全状态的M2ME110的某证书或凭证。在其它确认过程的情况中，确认可以包括M2ME110安全状态的验证的更多的安全方式。由于M2ME的TRE230是确保用于执行M2ME110的确认的M2ME内部资源的安全性属性的可信环境，因此应当存在凭证和/或凭证的确认结果的绑定来用于认证。

[0120] 存在认证M2ME110的三个过程。首先，作为初始网络连接的前提，初始M2ME110可以由ICF160来认证。其次，作为MID下载的前提(例如，具有其凭证的USIM应用)，M2ME110可以由例如DPF180之类的实体来认证以证明该M2ME110包含经认证的TRE230。第三，对于可操作的网络接入(例如使用下载的MID)，M2ME110可以由SHO140来认证。

[0121] 如上所述，自发确认是用于初始网络连接的认证过程的唯一的确认类型。上述其它两种方法需要PVA150的参与，但是没有初始连接且M2ME110不可能使PVA150参与确认。

[0122] 对于初始网络连接，将完整性/有效性绑定到网络接入认证只可以是隐式的，用于自发确认，因为在网络附着发生之后，没有执行基于网络的完整性/有效性检查。对于其它两种形式的确认，令牌(例如证明TRE230的凭证和验证的数字证书)可以在初始附着消息中被传递，该消息提供关于M2ME110中的TRE230的标识的进一步的信息，以及由此产生的TRE230的安全性功能和M2ME110的完整性。

[0123] 对于可操作的连接性，存在半自发确认和远程确认。此外，该确认方法可以绑定到后续的认证步骤。下面描述实现平台确认和认证的绑定的两种方式。

[0124] 首先，存在将持有认证凭证的TRE230到M2ME110的逻辑绑定。在认证期间，设备平台的完整性被确认。应当注意，之前的逻辑绑定的方案(例如SIM锁)已经被迅速绕开(circumvent)。但是，存在可以被成功应用的其它更新的方法，例如TCG。

[0125] 其次，存在TRE230到M2ME110的物理绑定。在TRE230认证期间，设备平台的完整性被确认。

[0126] 在以上两种情况中，平台资源的实际确认应当通过使用安全嵌入在M2ME110的硬件安全性组件(即，内嵌TRE)的功能或通过使用硬件安全性组件(其可以在TRE230外部但TRE230保证其安全性属性，且具有到TRE230的安全连接)来执行。应当注意到，用于3GPP AKA认证的凭证和应用没有被设计为用于确认主机设备中安全硬件的绑定。

[0127] 确认和认证的步骤可以被结合到公共协议的会话中。例如，3GPP使用IKEv2作为用于结合设备和主机方认证的方法。同样的协议还可以被认为用于在结合的确认/认证过程中使用。

[0128] 图7示出了在经认证接入情况中提供和重新提供MID到M2ME110的第一示例过程700。但是该过程是针对示例性的目的而提供的，在网络实体间的其它交互也可能有相同的结果。在图7中，箭头指示功能、服务供应商以及确认机构之间的连接。实线箭头指示从M2ME110到VNO115的初始网络接入的空中接口，虚线箭头指示经由VNO网络提供的空中接口的M2ME110与ICF160之间的连接，点划线箭头指示通过VNO网络和ICF160提供的IP连接的

M2ME110与DPF180、DPF170以及PVA150之间的连接。虽然ICF160、DRF170以及DPF180被显示为独立实体，但是本领域技术人员可以知道，它们也可以位于一个单个实体中(如图1所示)或为实现基本相同的功能的其它排列。

[0129] 在图7的过程700中，MID被下载和提供到M2ME110可以在M2ME110在其初始网络接入时接入到3G NVO网络时发生。NVO115根据以下过程提供到M2ME110的空中接口。

[0130] M2ME110可以使用标准GSM/UMTS规则(GPRS/PS)，例如用来对网络信息进行解码以及使用附着消息附着到VNO115的网络。在附着消息中，M2ME110发送临时M2ME ID或PCID到VNO115，且VNO115通过标准UMTS AKA过程来认证该M2ME110(701)。PCID的内容和结构使得VNO115将该PCID识别为IMSI。

[0131] 应当注意到，为了能够执行初始附着到VNO网络的客户端认证，M2ME110需要支持认证算法，例如Milenage算法，其由所有M2ME和VNO115共享。

[0132] 将PCID识别为用于M2ME110的ID的VNO115联系将接受PCID作为合法初步凭证的ICF160(702)。然后ICF160发布一组初步认证向量(AV)以保护与M2ME110的进一步通信，并开始提供到M2ME110的受保护的IP连接(703)。该通信使用VNO网络提供的空中接口而被执行。

[0133] 接下来，M2ME110和ICF160执行标准AKA进程以产生初步的AKA密钥来保护来自/到M2ME110的通信(704)。在下载并提供SHO的MID凭证后，直到M2ME110使用该SHO的MID凭证连接到网络时以及在此之后，M2ME110到各种网络实体的所有通信经由VNO网络提供的空中接口和ICF160提供的IP连接和加密保护而被完成。

[0134] 然后ICF160将M2ME110重新指向DPF180。在该过程中，ICF160可以发送PCID到DRF170(705)。之后，DRF170帮助M2ME110找到SHO140(706)。接下来，DRF170连接到SHO140并注册M2ME110以用于连接到SHO的网络(707)。在响应中，SHO140请求PVA150来确认M2ME110的TRE230的真实性和完整性(708)。之后，PVA150确认M2ME110的TRE230的真实性和完整性(709)。确认过程可以以与参考图3-5的上述确认过程相似的方式执行。

[0135] 在完成确认之后，PVA150将确认结果发回到SHO140(710)。SHO140联系DPF180并授权提供MID(USIM/ISIM应用)给M2ME110(711)。

[0136] 接下来，DPF180下载针对M2ME110的MID(712)。然后M2ME110提供下载的MID到TRE230中，并且将提供的成功/失败状态报告给DPF180(713)。M2ME110可能需要发送可以用于这种消息的验证的令牌。这种令牌需要是能够抵挡损害和重放攻击的形式。最后，DPF150将提供的成功/失败状态报告给SHO140(714)。

[0137] 图8示出了在经认证的接入的情况中提供和重新提供MID给M2ME110的另一个过程800。在该过程800中，下载并提供MID给M2ME110可以在M2ME110在其初始网络接入中接入到3G VNO网络时发生。ICF160在释放临时认证向量给M2ME110之前以及在允许到M2ME110的IP连接之前请求PVA150确认M2ME110的TRE230，而不是在SHO140授权下载并提供其MID之前使TRE230确认发生。

[0138] 该过程800在M2ME110使用例如标准GSM/UMTS规则(GPRS/PS)来对网络信息进行解码并附着到VNO115的网络时开始(801)。在附着消息中，M2ME110发送PCID到VNO115。VNO115通过标准UMTS AKA过程来认证M2ME110。

[0139] 识别用于M2ME110的PCID的VNO115联系接受PCID作为合法初步凭证的ICF160

(802)。接下来，ICF160请求PVA150来确认M2ME110的TRE230的真实性和完整性(803)。然后PVA150确认M2ME110的TRE230的真实性和完整性(804)。可以使用之前提到的确认过程中的一种来执行该确认。

[0140] 一旦PVA150将确认结果发送回ICF160(805)，则ICF发布一组初步认证向量(AV)以保护与M2ME110进行的进一步通信，并且开始提供到M2ME110的受保护IP连接(806)。该通信可以经由VNO的网络提供的空中接口被完成。

[0141] 接下来，M2ME110和ICF160执行标准AKA进程来产生用于保护来自/到M2ME110的通信的初步AKA密钥(807)。在下载并提供该SHO的U(I)SIM凭证之后，直到M2ME110使用该SHO的U(I)SIM凭证连接到网络时以及在此以后，M2ME110到各种网络实体之间的所有通信经由VNO的网络提供的空中接口以及ICF160提供的IP连接和加密保护而被完成。

[0142] 然后，ICF160将M2ME110重新指向DRF170(808)。在这样做的过程中，ICF160将PCID和关于TRE确认状态的信息发送到DRF170。DRF170帮助M2ME110找到其SHO140，并将M2ME110重新指向SHO140(809)。然后DRF170连接到SHO140并为连接到SHO140而注册M2ME110(810)。在这样做的过程中，DRF170还向SHO140传递关于TRE确认状态的信息。

[0143] 在检查SHO140从DRF170接收的TRE确认状态信息后，SHO140联系DPF180并授权提供MID(USIM/ISIM应用)给M2ME110(811)。作为响应，DPF180下载MID(U(I))SIM应用和凭证对象到M2ME(812)。

[0144] M2ME110提供下载的MID给TRE230并将提供成功/失败状态报告给DPF180(813)。M2ME110可以发送用于验证该消息的令牌。该令牌应该是抵挡损害和重放攻击的形式。最后，DPF180将提供成功/失败状态报告给SHO140。

[0145] 图9是针对新SHO(未显示)重新提供M2ME110的过程900的示例流程图。该过程900在M2ME持有者联系新SHO以传输M2ME参数时开始(910)。然后，M2ME110持有者联系M2ME以发起重新提供过程(920)。

[0146] 新SHO请求确认实体确认M2ME110(930)。然后PVA150确认M2ME110并发送成功/失败消息到新SHO(940)。在接收到成功通知后，新SHO请求DPF下载/提供新MID(即USIM应用和凭证)到M2ME110(950)。

[0147] 之后，DPF180安全地将新MID包下载到M2ME110(960)。M2ME110发送消息给已经丢弃旧MID的旧SHO(970)。之后，旧SHO发送ACK到M2ME110，该M2ME110然后将该ACK转发到DPF180，再转发到新SHO(980)。

[0148] M2ME110在DPF180的帮助下更新该M2ME110的系统并安装MID，并将成功/失败消息发回DPF180(990)。DPF180将该成功/失败消息报告给新SHO(992)。一旦成功，则提供过程完成(998)。

[0149] 在另一个重新提供过程中，M2ME110可以被置于初始状态并重新发起与图7和图8所述的初始提供过程相同类型的过程。

[0150] 在另一个实施方式中，PVA150用于确保在M2ME110仍然被预定到同一个SHO140时被执行的任意软件(SW)或固件(FW)更新以安全方式被执行。这可以包括更新或重新配置凭证。

[0151] 这意味着PVA150或DPF180应该监管例如通过空中(也可以通过线路)的SW/FW的安全下载和M2ME110和/或TRE230的重新提供的过程。因此，PVA150或DPF180可以使用例如OMA

DM和OMA FOTA规范中提供的这些可用的方法，以用于安全下载、FLASH更新和/或M2ME110的设备重新配置。

[0152] 此外，由于M2ME信任状态信息由于远程SW/FW更新或重新配置而改变，因此PVA150或DPF180在SW/FW更新或重新配置完成后应该能够发起并获得新验证根或M2ME110或TRE230的运行时间信任状态信息检查的结果。PVA150或DPF180还应当更新其自身的关于M2ME110的信任状态信息的数据库。在DPF180用于远程SW/FW更新或远程凭证重新配置的情况中，对关于M2ME110的“信任状态”信息的更新/重新配置的任意预计效果必须从DPF180被发送到PVA150，使得PVA150可以更新其M2ME110的“信任状态”信息的数据库。

[0153] 此外，公开了用于对M2ME110损害的后检查补救反应的检测的方案。为了使M2ME110不容易受到损害攻击，提出了一些方案。

[0154] 首先，M2ME110可以被配置成具有能够在其内部足够频繁(在规则调度检测尝试的情况下)和/或及时(在事件驱动的检测尝试的情况下)检测一些类型的对该M2ME110或任意子系统造成的“损害”的功能。该可检测的损害事件的示例可以包括但不限于：(1)由于错误或病毒导致的可补救和/或不可补救的OS的损害；(2)缓存器溢出事件；(3)无线电或较高层连接特性和/或环境读取的突发未预料或未授权的改变；(3)用于初步认证、注册或MID提供的M2ME请求的可信网络元件的接入或服务的过多次重复失败和/或拒绝；或者(4)关于远程MID管理功能的M2ME110或M2ME子系统的“信任状态”的后置根或运行时间读取的任意未预料/未授权的改变。网络元件(例如图1中所述的PVA150、ICF160或任意其它网络元件)还可以被配置成检测损害。例如，网络元件可以被配置成使用其自身的功能和/或M2ME110的功能来远程检测一些类型的对M2ME110的“损害”。此外，网络元件可以被配置成请求M2ME110报告任意损害检测事件。

[0155] 在对其任意损害的自检测后，M2ME110应当采取用于限制对其或其它网络元件的进一步损坏的步骤。例如，在检测到损害后，M2ME110可以被配置成禁用关于远程MID管理的功能。M2ME110还可以被配置成禁用M2ME110的内部资源(例如SW、或OS的某些部分)接入到M2ME110的预先指定的高敏感区域，例如TRE230，或保持远程MID管理相关数据、代码或凭证(例如SIM和/或TPM/MTM)的M2ME110的其它部分。

[0156] 在自检测损害后，M2ME110还可以被配置成向指定的网络元件(例如PVA)发送可疑或检测到的损害事件和M2ME110采取的后检测自补救或反作用行为的事件的报告。应当注意到这种事件报告还可以包括事件的时间戳或甚至事件的位置信息戳，例如M2ME110的最近GPS读取或邻近小区的列表。

[0157] 另外，在检测到损害后，M2ME110可以被配置成执行补救行为，例如删除、隔离或卸载当前SW更新或可疑病毒或错误代码或数据。M2ME110还可以被配置成删除任意预先设计的关于远程MID管理功能的数据集，例如来自短暂存储装置(例如RAM)和/或永久存储装置(例如，NVRAM、Flash、硬盘、SIM、TPM/MTM内部或加密的存储区等)的USIM相关密钥或凭证。

[0158] 最后，在检测到损害后，M2ME110还可以被配置成关闭对M2ME110的供电或对处理远程MID管理功能的终端的部分/子系统的供电。

[0159] 为了M2ME110，(其(1)具有报告的可疑或检测到损害事件；或(2)PVA150或与该M2ME110交互的其它网络元件怀疑该M2ME110已经遭遇损害事件)，一些网络元件，例如PVA150还可以用于并能够发起和执行远程“后检测”反应行为。

[0160] 上述的特征和实施方式可以适用于3G UMTS网络接入认证所需的认证协议以外的认证协议。这些协议的示例可以包括但不限于符合用于应用层认证的通用自展构架(GBA)、以及基于用于到非3G接入网络的GSM/UMTS终端认证的SIM(EAP-SIM)的可扩展认证协议。例如,图1中所述的网络元件可以存在并执行相似或相同功能以允许认证和用于服务、应用或(非3G)网络接入的M2ME设备的标识和认证的远程管理。

[0161] 虽然本发明的特征和元素以特定的结合进行了描述,但每个特征或元素可以在没有其它特征和元素的情况下单独使用,或在与或不与其它特征和元素结合的各种情况下使用。此处提供的方法或流程图可以在由通用计算机或处理器执行的计算机程序、软件或固件中实施,其中所述计算机程序、软件或固件是以有形的方式包含在计算机可读存储介质中的。计算机可读存储介质的实例包括只读存储器(ROM)、随机接入存储器(RAM)、寄存器、缓冲存储器、半导体存储设备、诸如内部硬盘和可移动磁盘之类的磁性介质、磁光介质和如CD-ROM光盘和数字多功能光盘(DVD)之类的光介质。

[0162] 举例来说,恰当的处理器包括:通用处理器、专用处理器、常规处理器、数字信号处理器(DSP)、多个微处理器、与DSP内核相关的一个或多个微处理器、控制器、微控制器、专用集成电路(ASIC)、现场可编程门阵列(FPGA)电路、任何其它类型的集成电路(IC)和/或状态机。

[0163] 与软件相关联的处理器可以用于实现一个射频收发机,以便在无线发射接收单元(WTRU)、用户设备(UE)、终端、基站、无线电网络控制器(RNC)或者任何主机计算机中加以使用。WTRU可以与采用硬件和/或软件形式实施的模块结合使用,例如照相机、摄像机模块、可视电话、扬声器电话、振动设备、扬声器、麦克风、电视收发信机、免提耳机、键盘、蓝牙®模块、调频(FM)无线电单元、液晶显示器(LCD)显示单元、有机发光二极管(OLED)显示单元、数字音乐播放器、媒体播放器、视频游戏机模块、因特网浏览器和/或任何无线局域网(WLAN)或超宽带(UWB)模块。

[0164] 实施例

[0165] 1.一种用于执行机器对机器(M2M)通信的方法。

[0166] 2.根据前述实施例中任一实施例所述的方法,其中所述通信包括认证、提供或重新提供中的一者或多者。

[0167] 3.根据前述实施例中任一实施例所述的方法,该方法还包括:

[0168] 在M2M启动设备(M2ME)处,连接到被访问网络运营商(VNO)的网络。

[0169] 4.根据前述实施例中任一实施例所述的方法,该方法还包括:接收用于连接到所选家庭运营商(SHO)的网络的授权。

[0170] 5.根据前述实施例中任一实施例所述的方法,该方法还包括:连接到SHO的网络。

[0171] 6.根据前述实施例中任一实施例所述的方法,其中所述VNO是单个网络实体。

[0172] 7.根据前述实施例中任一实施例所述的方法,其中所述VNO包括多个网络实体。

[0173] 8.根据前述实施例中任一实施例所述的方法,其中VNO是为了初始注册和提供而被接入的任意接入网络。

[0174] 9.根据前述实施例中任一实施例所述的方法,其中注册和提供包括USIM/ISIM应用的注册和提供。

[0175] 10.根据前述实施例中任一实施例所述的方法,该方法还包括:

[0176] M2ME向不是VNO的SHO注册;以及

[0177] 所述VNO仍为VNO。

[0178] 11.根据前述实施例中任一实施例所述的方法,该方法还包括:

[0179] M2ME向是VNO的SHO注册;以及

[0180] VNO成为SHO。

[0181] 12.根据前述实施例中任一实施例所述的方法,其中所述VNO用于提供到M2ME的临时网络接入。

[0182] 13.根据前述实施例中任一实施例所述的方法,其中临时网络接入基于临时网络接入凭证。

[0183] 14.根据前述实施例中任一实施例所述的方法,其中临时网络接入凭证包括PCID或任意其它临时私人ID。

[0184] 15.根据前述实施例中任一实施例所述的方法,该方法还包括:

[0185] VNO提供到发现和注册功能(DRF)的开放网络接入。

[0186] 16.根据前述实施例中任一实施例所述的方法,其中对于至少DRF的服务不需要凭证或认证。

[0187] 17.根据前述实施例中任一实施例所述的方法,其中VNO在VNO将成为SHO时提供到DRF的开放网络接入。

[0188] 18.根据前述实施例中任一实施例所述的方法,该方法还包括:

[0189] VNO使用所提供的USIM/ISM应用提供完全网络接入。

[0190] 19.根据前述实施例中任一实施例所述的方法,其中完全网络接入包括IMS。

[0191] 20.根据前述实施例中任一实施例所述的方法,其中RO包括ICF、DRF、以及下载和提供功能(DPF)中的一者或多者。

[0192] 21.根据前述实施例中任一实施例所述的方法,其中ICF、DRF以及DPF的每个位于单个实体中。

[0193] 22.根据前述实施例中任一实施例所述的方法,其中ICF用于凭证的确认,该凭证为了注册和提供可操作网络接入而允许到通信网络的临时接入。

[0194] 23.根据前述实施例中任一实施例所述的方法,该方法还包括:

[0195] ICF发布临时网络接入凭证。

[0196] 24.根据前述实施例中任一实施例所述的方法,该方法还包括:

[0197] ICF发布用于M2ME的临时私人标识符。

[0198] 25.根据前述实施例中任一实施例所述的方法,其中临时网络接入凭证或临时私人标识符用于经认证的初始临时网络接入。

[0199] 26.根据前述实施例中任一实施例所述的方法,该方法还包括:

[0200] ICF向M2ME提供M2M密钥、配置和应用中的一者或多者。

[0201] 27.根据前述实施例中任一实施例所述的方法,其中提供包括通过空中的提供。

[0202] 28.根据前述实施例中任一实施例所述的方法,该方法还包括:

[0203] ICF提供凭证给设备供应商(E/S)以预先配置M2ME。

[0204] 29.根据前述实施例中任一实施例所述的方法,其中ICF被配置成提供凭证的安全传输给用于将凭证嵌入到M2ME中的组织。

[0205] 30.根据前述实施例中任一实施例所述的方法，该方法还包括：

[0206] ICF注册数据库中的凭证。

[0207] 31.根据前述实施例中任一实施例所述的方法，该方法还包括：

[0208] ICF接收用于确认来自第三方的凭证的请求；以及

[0209] ICF执行凭证的确认。

[0210] 32.根据前述实施例中任一实施例所述的方法，其中凭证的确认包括到第三方的认证向量的安全传输。

[0211] 33.根据前述实施例中任一实施例所述的方法，其中认证向量包括相关数据。

[0212] 34.根据前述实施例中任一实施例所述的方法，其中所有接入网络在M2ME成功注册到SHO之前被认为是被访问网络。

[0213] 35.根据前述实施例中任一实施例所述的方法，其中M2ME通过常规网络透明地连接到SHO，而不需要网络改变。

[0214] 36.根据前述实施例中任一实施例所述的方法，其中DRF启用专用SHO的后支付选择、以及M2ME向所选SHO的注册。

[0215] 37.根据前述实施例中任一实施例所述的方法，其中DRF是独立服务。

[0216] 38.根据前述实施例中任一实施例所述的方法，其中DRF由SHO操作。

[0217] 39.根据前述实施例中任一实施例所述的方法，其中可以经由SHO的3GPP网络联系SHO的RO。

[0218] 40.根据前述实施例中任一实施例所述的方法，其中可以经由因特网联系SHO的RO。

[0219] 41.根据前述实施例中任一实施例所述的方法，其中SHO的RO是可发现的。

[0220] 42.根据前述实施例中任一实施例所述的方法，其中使用M2ME中的功能可以发现SHO的RO。

[0221] 43.根据前述实施例中任一实施例所述的方法，其中DRF允许消费者在M2ME被递送之后选择SHO。

[0222] 44.根据前述实施例中任一实施例所述的方法，其中DRF允许M2ME具有使用临时认证网络接入或受限开放网络接入的到RO的IP连接。

[0223] 45.根据前述实施例中任一实施例所述的方法，其中DRF允许M2ME经由VNO请求USIM/ISM应用的提供。

[0224] 46.根据前述实施例中任一实施例所述的方法，该方法还包括：

[0225] DRF批准提供请求；以及

[0226] 授权DPF提供M2ME。

[0227] 47.根据前述实施例中任一实施例所述的方法，其中DRF支持由M2ME的拥有者进行的M2ME的注册。

[0228] 48.根据前述实施例中任一实施例所述的方法，其中DRF支持M2ME与SHO的关联。

[0229] 49.根据前述实施例中任一实施例所述的方法，该方法还包括：

[0230] 经由PVA使用M2ME的批准来确认TRE的真实性。

[0231] 50.根据前述实施例中任一实施例所述的方法，该方法还包括：

[0232] DRF生成将被传输到M2ME的数据包。

[0233] 51.根据前述实施例中任一实施例所述的方法，该方法还包括：

[0234] DRF获得将被传输到M2ME的数据包。

[0235] 52.根据前述实施例中任一实施例所述的方法，该方法还包括：

[0236] DRF将数据安全地传输到PS。

[0237] 53.根据前述实施例中任一实施例所述的方法，该方法还包括：

[0238] DPF生成将被传输到M2ME的数据包。

[0239] 54.根据前述实施例中任一实施例所述的方法，该方法还包括：

[0240] DPF获得将被传输到M2ME的数据包。

[0241] 55.根据前述实施例中任一实施例所述的方法，该方法还包括：

[0242] DPF将数据安全地传输到PS。

[0243] 56.根据前述实施例中任一实施例所述的方法，该方法还包括：

[0244] DRF促进M2ME与DPF之间的安全性关联的建立。

[0245] 57.根据前述实施例中任一实施例所述的方法，该方法还包括：

[0246] DRF生成安全性令牌并通过安全信道将该安全性令牌传输到M2ME和DPF。

[0247] 58.根据前述实施例中任一实施例所述的方法，其中DPF能够远程提供USIM/ISM凭证给M2ME。

[0248] 59.根据前述实施例中任一实施例所述的方法，该方法还包括：

[0249] DPF从DRF接收提供M2ME的授权。

[0250] 60.根据前述实施例中任一实施例所述的方法，其中接收授权包括DPF接收用于与M2ME通信的安全性令牌。

[0251] 61.根据前述实施例中任一实施例所述的方法，该方法还包括：

[0252] DPF从DRF接收应用包。

[0253] 62.根据前述实施例中任一实施例所述的方法，该方法还包括：

[0254] DPF根据存储的规则生成应用包；以及

[0255] 告知DRF凭证已经被下载到DRF。

[0256] 63.根据前述实施例中任一实施例所述的方法，其中DPF被配置成提供USIM/ISM应用或USMI/ISIM参数给M2ME。

[0257] 64.根据前述实施例中任一实施例所述的方法，DPF被配置成执行对给M2ME的USIM/ISIM应用或USIM/ISIM参数的以后的更新。

[0258] 65.根据前述实施例中任一实施例所述的方法，其中DPF被配置成执行以后的新应用的提供。

[0259] 66.根据前述实施例中任一实施例所述的方法，其中DPF被配置成通知DRF成功或未成功提供事件。

[0260] 67.根据前述实施例中任一实施例所述的方法，其中SHO是与M2ME的用户有商业关系的网络运营商。

[0261] 68.根据前述实施例中任一实施例所述的方法，其中SHO用于对消费者进行计费。

[0262] 69.根据前述实施例中任一实施例所述的方法，其中SHO起着DRF的作用。

[0263] 70.根据前述实施例中任一实施例所述的方法，其中SHO起着DPF的作用。

[0264] 71.根据前述实施例中任一实施例所述的方法，其中SHO执行其它功能。

[0265] 72.根据前述实施例中任一实施例所述的方法，其中SHO与DRF和DPF具有可操作关系。

[0266] 73.根据前述实施例中任一实施例所述的方法，其中DRF和DPF彼此具有操作关系。

[0267] 74.根据前述实施例中任一实施例所述的方法，其中M2ME初始不用于与服务供应商进行操作。

[0268] 75.根据前述实施例中任一实施例所述的方法，其中与VNO通信的M2ME建立到RO的信道。

[0269] 76.根据前述实施例中任一实施例所述的方法，其中M2ME具有私人标识。

[0270] 77.根据前述实施例中任一实施例所述的方法，其中PCID是私人标识。

[0271] 78.根据前述实施例中任一实施例所述的方法，其中私人密钥使VNO能够识别M2ME以允许临时接入VNO服务，并将初始连接消息引向合适的网络组件以下载并提供运营商的服务。

[0272] 79.根据前述实施例中任一实施例所述的方法，其中PVA用于证明M2ME中安全设备的真实性的凭证，该安全设备用于存储和执行下载的USIM/ISIM应用。

[0273] 80.根据前述实施例中任一实施例所述的方法，其中PVA包括发布凭证并提供凭证确认服务的一个或多个商业组织。

[0274] 81.根据前述实施例中任一实施例所述的方法，其中凭证包括证书和密钥对。

[0275] 82.根据前述实施例中任一实施例所述的方法，其中M2ME中的安全设备是UICC、TRE或某些其它安全模块中的一者或多者。

[0276] 83.根据前述实施例中任一实施例所述的方法，其中当安全设备的强认证是提供USIM/ISIM应用的前提时，需要PVA功能。

[0277] 84.根据前述实施例中任一实施例所述的方法，该方法还包括：

[0278] 创建并发布用于证明M2ME中的安全设备的安全性的凭证。

[0279] 85.根据前述实施例中任一实施例所述的方法，其中由PVA来执行创建并发布用于证明M2ME中的安全设备的安全性的凭证。

[0280] 86.根据前述实施例中任一实施例所述的方法，其中PVA被配置成提供用于M2ME中的安全设备的凭证的确认。

[0281] 87.根据前述实施例中任一实施例所述的方法，其中PVA被配置成提供关于发布的凭证的有效性的数据的维护。

[0282] 88.根据前述实施例中任一实施例所述的方法，其中设备供应商(E/S)安全地从ICF获得用于临时初始网络连接认证的凭证。

[0283] 89.根据前述实施例中任一实施例所述的方法，其中E/S被配置成支持M2ME的重新配置。

[0284] 90.根据前述实施例中任一实施例所述的方法，其中重新配置包括给M2ME提供初步网络接入凭证。

[0285] 91.根据前述实施例中任一实施例所述的方法，其中E/S被配置成从PVA150安全地获得凭证，该凭证用于经由ICF160向DRF170证明M2ME符合安全性需求的标准集合。

[0286] 92.根据前述实施例中任一实施例所述的方法，其中E/S被配置成将M2ME配置为具有凭证。

[0287] 93.根据前述实施例中任一实施例所述的方法，其中E/S被配置成提供用于M2ME持有者选择期望DRF和SHO的装置。

[0288] 94.根据前述实施例中任一实施例所述的方法，其中E/S被配置成提供在M2ME被连接到接入网络时发生的自动DRF和SHO选择。

[0289] 95.根据前述实施例中任一实施例所述的方法，其中M2ME包括发射机、接收机、处理器、可信环境(TRE)、全球定位系统(GPS)、用户标识模块(SIM)、以及安全时间单元中的一者或多者。

[0290] 96.根据前述实施例中任一实施例所述的方法，其中M2ME被配置成支持多个不同的信任机制。

[0291] 97.根据前述实施例中任一实施例所述的方法，其中M2ME被配置成支持TRE、SIM或ISIM中的一者或多者。

[0292] 98.根据前述实施例中任一实施例所述的方法，其中信任机制被完全集成到公共AKA协议中。

[0293] 99.根据前述实施例中任一实施例所述的方法，其中公共AKA协议包括信任状态信息或受TRE保护的密钥中的一者或多者。

[0294] 100.根据前述实施例中任一实施例所述的方法，其中AKA协议在完全AKA发生之前以及已经建立认证之后保护M2ME与网络元件之间的任意通信。

[0295] 101.根据前述实施例中任一实施例所述的方法，其中SIM被增强以包括可信处理模块(TPM)或移动可信模块(MTM)的功能。

[0296] 102.根据前述实施例中任一实施例所述的方法，其中SIM被配置成与TPM或MTM紧密操作。

[0297] 103.根据前述实施例中任一实施例所述的方法，其中TRE被配置成执行SIM的功能。

[0298] 104.根据前述实施例中任一实施例所述的方法，其中M2ME被提供有AKA根秘密。

[0299] 105.根据前述实施例中任一实施例所述的方法，其中根秘密由E/S提供。

[0300] 106.根据前述实施例中任一实施例所述的方法，其中根秘密由USIM来保护。

[0301] 107.根据前述实施例中任一实施例所述的方法，其中根秘密从不改变。

[0302] 108.根据前述实施例中任一实施例所述的方法，其中处理器被配置成从AKA根秘密中导出会话密钥。

[0303] 109.根据前述实施例中任一实施例所述的方法，其中M2ME被配置成提供信任状态信息给ICF。

[0304] 110.根据前述实施例中任一实施例所述的方法，其中在M2ME附着到VNO时，信任状态信息可以用于初步认证。

[0305] 111.根据前述实施例中任一实施例所述的方法，其中信任状态信息用于导出会话密钥。

[0306] 112.根据前述实施例中任一实施例所述的方法，其中n指会话密钥$CK_n$和$IK_n$的最当前更新的索引，且$CK_n=f3K(RAND||PCR0n)$，$IKn=f4K(RAND||PCR0n)$，其中$f3_K()$和$f4_K()$分别指加密密钥和完整性密钥的AKA密钥导出函数(从共享主秘密K中导出)，RAND是CATNA生成的认证向量(AV)中的随机现时，该AV在AKA过程中被发送到M2ME110并由其共享，而$PCR0_n$指

M2ME110上的MTME内的PCR0寄存器的最近值。

[0307] 113.根据前述实施例中任一实施例所述的方法，其中，PCR0寄存器的当前值表示M2ME的最近后置根信任状态的描述。

[0308] 114.根据前述实施例中任一实施例所述的方法，其中当PCR0的值在根之间改变时，$CK_n$和$IK_n$的值改变。

[0309] 115.根据前述实施例中任一实施例所述的方法，其中ICF知道M2ME的信任状态的改变。

[0310] 116.根据前述实施例中任一实施例所述的方法，其中M2ME的信任状态的改变包括PCR0值的改变。

[0311] 117.根据前述实施例中任一实施例所述的方法，其中ICF被通知对M2ME的OS、固件或应用的更新的调度和内容。

[0312] 118.根据前述实施例中任一实施例所述的方法，其中ICF被通知影响M2ME的信任状态的对M2ME的任何改变。

[0313] 119.根据前述实施例中任一实施例所述的方法，其中M2ME与ICF之间共享的AKA加密和完整性密钥被更新，并对M2ME的认证是有用的。

[0314] 120.根据前述实施例中任一实施例所述的方法，其中会话密钥反映M2ME的最近信任状态。

[0315] 121.根据前述实施例中任一实施例所述的方法，其中会话密钥加强AKA密钥导出过程的安全性。

[0316] 122.根据前述实施例中任一实施例所述的方法，其中TRE是M2ME中逻辑上独立的区域。

[0317] 123.根据前述实施例中任一实施例所述的方法，其中存在对TRE的逻辑独立的硬件支持。

[0318] 124.根据前述实施例中任一实施例所述的方法，其中TRE是可移动模块。

[0319] 125.根据前述实施例中任一实施例所述的方法，其中TRE是固定模块。

[0320] 126.根据前述实施例中任一实施例所述的方法，其中TRE与集成电路(IC)一起运行。

[0321] 127.根据前述实施例中任一实施例所述的方法，其中TRE的功能被分布到多个IC之间。

[0322] 128.根据前述实施例中任一实施例所述的方法，其中TRE定义到外部的逻辑和物理接口。

[0323] 129.根据前述实施例中任一实施例所述的方法，其中被TRE暴露的接口在授权实体的控制下是可用的。

[0324] 130.根据前述实施例中任一实施例所述的方法，其中TRE提供用于多个管理标识(MID)的安全存储和安全执行环境的信任根。

[0325] 131.根据前述实施例中任一实施例所述的方法，其中TRE提供MID的提供和管理。

[0326] 132.根据前述实施例中任一实施例所述的方法，其中MID是安全应用。

[0327] 133.根据前述实施例中任一实施例所述的方法，其中MID包括预定管理功能、安全支付应用、预定管理标识、USIM应用、ISIM应用、虚拟SIM(vSIM)或动态安全性标识方案中的

一者或多者。

[0328] 134.根据前述实施例中任一实施例所述的方法，其中TRE被提供在安全、带外设施中，具有任何所需的密码密钥和其它凭证。

[0329] 135.根据前述实施例中任一实施例所述的方法，其中TRE提供防止物理和逻辑攻击的保护。

[0330] 136.根据前述实施例中任一实施例所述的方法，其中TRE执行其自身安全性策略。

[0331] 137.根据前述实施例中任一实施例所述的方法，其中TRE足够安全以允许MID的存储和执行。

[0332] 138.根据前述实施例中任一实施例所述的方法，其中TRE具有到位于TRE外面的M2ME的部分的接口。

[0333] 139.根据前述实施例中任一实施例所述的方法，其中TRE具有内嵌的唯一标识。

[0334] 140.根据前述实施例中任一实施例所述的方法，其中TRE的标识与M2ME的标识相关联。

[0335] 141.根据前述实施例中任一实施例所述的方法，其中TRE被配置成使用标准协议来安全认证该TRE发布授权的标识。

[0336] 142.根据前述实施例中任一实施例所述的方法，其中TRE在UICC中被实施。

[0337] 143.根据前述实施例中任一实施例所述的方法，其中使用M2ME提供的硬件和软件组件将TRE实施为M2ME上的集成的方案。

[0338] 144.根据前述实施例中任一实施例所述的方法，其中TRE支持MID的下载和远程提供以及管理。

[0339] 145.根据前述实施例中任一实施例所述的方法，其中TRE支持管理标识可执行程序(MIDE)的功能。

[0340] 146.根据前述实施例中任一实施例所述的方法，其中M2ME支持构成TRE代码库的软件代码和数据的完整性检查。

[0341] 147.根据前述实施例中任一实施例所述的方法，其中TRE在M2ME的供电/启动时刻被检查。

[0342] 148.根据前述实施例中任一实施例所述的方法，其中在操作使用M2ME期间进行代码检查。

[0343] 149.根据前述实施例中任一实施例所述的方法，其中代码检查在定义的时间间隔或在某些触发时被执行以作为后台处理。

[0344] 150.根据前述实施例中任一实施例所述的方法，其中代码检查包括M2ME的部分或全部检查。

[0345] 151.根据前述实施例中任一实施例所述的方法，其中TRE包括对多个隔离可信域的支持。

[0346] 152.根据前述实施例中任一实施例所述的方法，其中每个域由风险承担者持有人拥有。

[0347] 153.根据前述实施例中任一实施例所述的方法，其中每个域彼此隔离。

[0348] 154.根据前述实施例中任一实施例所述的方法，其中每个域被保护不受损害和未授权接入。

[0349] 155.根据前述实施例中任一实施例所述的方法，其中TRE提供域间服务。

[0350] 156.根据前述实施例中任一实施例所述的方法，其中域间服务包括认证和证明功能中的一者或多者。

[0351] 157.根据前述实施例中任一实施例所述的方法，其中M2ME偶尔或很少连接到网路。

[0352] 158.根据前述实施例中任一实施例所述的方法，其中M2ME在休眠状态下操作。

[0353] 159.根据前述实施例中任一实施例所述的方法，其中TRE软件代码的运行时间完整性检查被配置成在M2ME在休眠状态下操作时发生。

[0354] 160.根据前述实施例中任一实施例所述的方法，其中完整性检查不会干扰其它M2ME或TRE处理。

[0355] 161.根据前述实施例中任一实施例所述的方法，其中当M2ME连接到SHO时，完整性检查状态已经准备好。

[0356] 162.根据前述实施例中任一实施例所述的方法，其中M2ME被分配对于M2ME来说唯一的临时私人标识。

[0357] 163.根据前述实施例中任一实施例所述的方法，其中PCID在时间受限的有效性周期有效。

[0358] 164.根据前述实施例中任一实施例所述的方法，其中有效性周期是由M2ME实施的。

[0359] 165.根据前述实施例中任一实施例所述的方法，其中TRE控制有效性周期。

[0360] 166.根据前述实施例中任一实施例所述的方法，该方法还包括：

[0361] 移除PCID。

[0362] 167.根据前述实施例中任一实施例所述的方法，其中PCID可以由多个M2ME在不同时间使用。

[0363] 168.根据前述实施例中任一实施例所述的方法，其中PCID被系统地重分配。

[0364] 169.根据前述实施例中任一实施例所述的方法，其中多个PCID被提供给M2ME。

[0365] 170.根据前述实施例中任一实施例所述的方法，其中M2ME以大小为N的组被释放。

[0366] 171.根据前述实施例中任一实施例所述的方法，其中第j批的M2ME被称为M_i,j，其中j=1,…,M。

[0367] 172.根据前述实施例中任一实施例所述的方法，其中PCID分配可以被初始化具有大小为N×M的矩阵(P)_{i,j}。

[0368] 173.根据前述实施例中任一实施例所述的方法，其中M2ME M_i,1在创建期间获得载入到TRE中的列P_i,*。

[0369] 174.根据前述实施例中任一实施例所述的方法，其中安全计时器或单调计数器被初始化、激活并受到TRE的控制。

[0370] 175.根据前述实施例中任一实施例所述的方法，其中M2ME M_i,1使用P_i,1达到基于被初始化的时间或计数器的确定的时间间隔T或预定次数。

[0371] 176.根据前述实施例中任一实施例所述的方法，其中TRE丢弃P_i,1并使用P_i,2。

[0372] 177.根据前述实施例中任一实施例所述的方法，其中网络被配置成确定设备处于寿命周期的哪个位置。

[0373] 178.根据前述实施例中任一实施例所述的方法，其中用TRE处理PCID列向量且TRE执行时间限制防止PCID的同时使用并确保M2ME在其整个操作时间具有有效PCID。

[0374] 179.根据前述实施例中任一实施例所述的方法，其中M2ME被配置成重新提供PCID。

[0375] 180.根据前述实施例中任一实施例所述的方法，其中至少两个M2ME尝试同时使用相同的PCID。

[0376] 181.根据前述实施例中任一实施例所述的方法，其中PCID的数目远大于一批中的M2ME的数目。

[0377] 182.根据前述实施例中任一实施例所述的方法，其中随机地选择PCID。

[0378] 183.根据前述实施例中任一实施例所述的方法，其中多个M2ME的时钟被同步。

[0379] 184.根据前述实施例中任一实施例所述的方法，其中所述M2ME的时钟与多个M2ME重新同步。

[0380] 185.根据前述实施例中任一实施例所述的方法，其中TRE被配置成保持并管理时基。

[0381] 186.根据前述实施例中任一实施例所述的方法，其中TRE被配置成支持与可信时间源的同步。

[0382] 187.根据前述实施例中任一实施例所述的方法，其中TRE依赖位于M2ME中的可信时间单元。

[0383] 188.根据前述实施例中任一实施例所述的方法，其中M2ME包括自发地理定位设备。

[0384] 189.根据前述实施例中任一实施例所述的方法，其中TRE具有到地理定位设备的安全接入。

[0385] 190.根据前述实施例中任一实施例所述的方法，其中两个M2ME不会同时在物理位置上建立到相同接入网络的无线电连接。

[0386] 191.根据前述实施例中任一实施例所述的方法，其中M2ME被提供有目的地理位置(D)以及容忍范围(R)。

[0387] 192.根据前述实施例中任一实施例所述的方法，其中D和R的值被存储在TRE中。

[0388] 193.根据前述实施例中任一实施例所述的方法，其中D和R的值通过加密的方式被保护，以使得只有TRE能够接入数据。

[0389] 194.根据前述实施例中任一实施例所述的方法，该方法还包括：

[0390] TRE确定其当前地理位置；

[0391] 将当前地理位置与R内的D进行比较；以及

[0392] 释放用于网络接入的PCID。

[0393] 195.根据前述实施例中任一实施例所述的方法，其中接入网络保持PCID、小区ID对的记录。

[0394] 196.根据前述实施例中任一实施例所述的方法，其中在预定多个小区处允许M2ME接入网络。

[0395] 197.根据前述实施例中任一实施例所述的方法，其中M2ME被配置有多个网络小区标识符。

[0396] 198.根据前述实施例中任一实施例所述的方法，其中M2ME在地理位置上被移动。

[0397] 199.根据前述实施例中任一实施例所述的方法，其中当M2ME被移动时，网络接入被禁用。

[0398] 200.根据前述实施例中任一实施例所述的方法，M2ME被提供有多个三元组，该三元组指定可以使用PCID的位置。

[0399] 201.根据前述实施例中任一实施例所述的方法，其中三元组包括PCID、D、以及R。

[0400] 202.根据前述实施例中任一实施例所述的方法，该方法还包括：

[0401] 确定TRE的当前地理位置；

[0402] 将该当前地理位置与多个三元组进行比较；以及

[0403] 释放与当前地理位置相关联的PCID。

[0404] 203.根据前述实施例中任一实施例所述的方法，其中M2ME被提供有多个五元组。

[0405] 204.根据前述实施例中任一实施例所述的方法，其中五元组包括PCID、D、R、t1和t2，其中t1表示有效性周期的开始时刻，t2表示有效性周期的结束时刻。

[0406] 205.根据前述实施例中任一实施例所述的方法，其中五元组描述M2ME的路径。

[0407] 206.根据前述实施例中任一实施例所述的方法，其中在预定时刻M2ME连接网络失败触发警报。

[0408] 207.根据前述实施例中任一实施例所述的方法，其中五元组可以被重新提供。

[0409] 208.根据前述实施例中任一实施例所述的方法，其中可以使用PCID更新服务(PUS)来重新提供五元组。

[0410] 209.根据前述实施例中任一实施例所述的方法，其中PUS被配置成标识TRE。

[0411] 210.根据前述实施例中任一实施例所述的方法，其中ICF包括PUS。

[0412] 211.根据前述实施例中任一实施例所述的方法，其中PUS是单独网络组件。

[0413] 212.根据前述实施例中任一实施例所述的方法，其中五元组的重新提供包括一个或多个五元组的改变。

[0414] 213.根据前述实施例中任一实施例所述的方法，其中TRE的标识被发送到网络服务器，该网络服务器能够将TRE与当前网络IP地址相关联。

[0415] 214.根据前述实施例中任一实施例所述的方法，其中远程提供被委派给DPF。

[0416] 215.根据前述实施例中任一实施例所述的方法，该方法还包括：

[0417] PUS连接到M2ME和TRE；

[0418] PUS请求确认TRE；

[0419] PUS递送新的多个五元组和将被丢弃的旧的五元组的列表；以及

[0420] TRE安装新的五元组并丢弃旧的五元组。

[0421] 216.根据前述实施例中任一实施例所述的方法，其中TRE被配置成生成能够与PCID结合的伪随机数。

[0422] 217.根据前述实施例中任一实施例所述的方法，其中接入网络被配置成了解并区分伪随机数。

[0423] 218.根据前述实施例中任一实施例所述的方法，其中通信实体是M2ME、TRE和网络接入点(NAP)。

[0424] 219.根据前述实施例中任一实施例所述的方法，其中NAP是与VNO相关联的e节点

B。

[0425] 220.根据前述实施例中任一实施例所述的方法，其中TRE被配置成生成将在单个初始网络连接中使用的随机数(RAND)。

[0426] 221.根据前述实施例中任一实施例所述的方法，该方法还包括：

[0427] TRE应用完整性保护方法。

[0428] 222.根据前述实施例中任一实施例所述的方法，其中完整性保护方法是键控函数，其中RAND输入第二参数、需要的另外数据(DI)以及PCID。

[0429] 223.根据前述实施例中任一实施例所述的方法，该方法还包括：

[0430] TRE发送TRE→eNB:RAND||PCID||D1||M1:=MAC(PCID I I D1,RAND)到eNB；

[0431] eNB验证消息认证码(MAC)；

[0432] eNB从有效载荷数据D2中建立返回包；以及

[0433] eNB发送该返回包给TRE，为eNB→TRE:D2||M2:=MAC(PCID||D2,M1。

[0434] 224.根据前述实施例中任一实施例所述的方法，其中后续消息交换包括数据元素的MAC，其包括任意新消息元素和刚交换的MAC。

[0435] 225.根据前述实施例中任一实施例所述的方法，其中eNB和TRE能够在使用上一个值$M_{n-1}$建立新的$M_n$的通信期间区分消息。

[0436] 226.根据前述实施例中任一实施例所述的方法，其中人为介入的攻击被避免。

[0437] 227.根据前述实施例中任一实施例所述的方法，其中共享秘密被包含在用于通信方认证的消息中。

[0438] 228.根据前述实施例中任一实施例所述的方法，其中共享的秘密是协商的秘密。

[0439] 229.根据前述实施例中任一实施例所述的方法，其中MAC值包括PCID。

[0440] 230.根据前述实施例中任一实施例所述的方法，其中eNB保留表示使用PCID的所有同时活动的网络接入尝试(信道)的状态。

[0441] 231.根据前述实施例中任一实施例所述的方法，其中表中的第一列包含属于信道的PICD的索引。

[0442] 232.根据前述实施例中任一实施例所述的方法，其中索引指向用于所有信道的当前活动的所有PCID的列表中的项。

[0443] 233.根据前述实施例中任一实施例所述的方法，其中索引是PCID值。

[0444] 234.根据前述实施例中任一实施例所述的方法，该方法还包括：

[0445] eNB接收信道上的消息TRE→eNB:D3||M3:=MAC(PCID I I D3,M2)。

[0446] 235.根据前述实施例中任一实施例所述的方法，该方法还包括：

[0447] eNB从i-1至N的PL中选择$PCID_i$。

[0448] 236.根据前述实施例中任一实施例所述的方法，该方法还包括：

[0449] 对于第一个单元中的PCID索引I的所有的表的行，eNB计算M:=MAC($PCID_i$||$D_3$,$M_2$)，其中$M_2$选自行中第二个单元。

[0450] 237.根据前述实施例中任一实施例所述的方法，该方法还包括：

[0451] 达到成功状态且搜索过程结束。

[0452] 238.根据前述实施例中任一实施例所述的方法，其中对应于最后接收第三消息的信道的行号被返回。

[0453] 239.根据前述实施例中任一实施例所述的方法，其中D3被添加到数据历史且在所选的表的行的活动散列值单元中，M2被M3替换。

[0454] 240.根据前述实施例中任一实施例所述的方法，其中消息包含用于找到后续消息的相关联信道的信道索引I。

[0455] 241.根据前述实施例中任一实施例所述的方法，其中活动PCID被锁定。

[0456] 242.根据前述实施例中任一实施例所述的方法，其中PCID被活动地解除分配。

[0457] 243.根据前述实施例中任一实施例所述的方法，其中当旧的PCID已经用于获得完全网络连接时，TRE丢弃使用过的PCID。

[0458] 244.根据前述实施例中任一实施例所述的方法，其中在有效周期期满则丢弃PCID。

[0459] 245.根据前述实施例中任一实施例所述的方法，其中响应于请求，而丢弃PCID。

[0460] 246.根据前述实施例中任一实施例所述的方法，其中不同的M2ME使用丢弃的PCID。

[0461] 247.根据前述实施例中任一实施例所述的方法，其中从TRE到E/S的连接被建立以发送解除分配事件。

[0462] 248.根据前述实施例中任一实施例所述的方法，其中E/S保留解除分配的PCID的列表。

[0463] 249.根据前述实施例中任一实施例所述的方法，其中在解除分配过程期间，不以明码报文的形式传输PCID。

[0464] 250.根据前述实施例中任一实施例所述的方法，其中自发地执行确认。

[0465] 251.根据前述实施例中任一实施例所述的方法，其中半自发地执行确认。

[0466] 252.根据前述实施例中任一实施例所述的方法，其中远程执行确认。

[0467] 253.根据前述实施例中任一实施例所述的方法，其中在M2ME允许其经历网络附着之前执行自发确认。

[0468] 254.根据前述实施例中任一实施例所述的方法，其中半自发确认包括不依赖外部网络实体而评估M2ME的有效性。

[0469] 255.根据前述实施例中任一实施例所述的方法，其中半自发确认的结果被报告给远程实体。

[0470] 256.根据前述实施例中任一实施例所述的方法，其中结果包括将TRE的认证与M2ME绑定的证据。

[0471] 257.根据前述实施例中任一实施例所述的方法，其中远程实体是PVA。

[0472] 258.根据前述实施例中任一实施例所述的方法，其中M2ME和远程实体之间的信令被保护。

[0473] 259.根据前述实施例中任一实施例所述的方法，其中远程确认包括外部网络实体在接收到TRE生成的确认证据以及TRE与M2ME之间的绑定证据之后直接评估M2ME的有效性和完整性。

[0474] 260.根据前述实施例中任一实施例所述的方法，其中外部网络实体是PVA。

[0475] 261.根据前述实施例中任一实施例所述的方法，其中M2ME与外部网络实体之间的通信被保护。

[0476] 262.根据前述实施例中任一实施例所述的方法，其中自发确认被执行且没有确认的直接证据被提供给外界。

[0477] 263.根据前述实施例中任一实施例所述的方法，其中M2ME确认失败且TRE阻止M2ME附着到网络或获得到远程实体的经认证的连接。

[0478] 264.根据前述实施例中任一实施例所述的方法，该方法还包括：

[0479] TRE检查其是否已经达到安全启动的预定义状态。

[0480] 265.根据前述实施例中任一实施例所述的方法，该方法还包括：

[0481] 检查M2ME的其余部分中的需要安全启动的预定义部分是否已经达到安全启动的预定义状态。

[0482] 267.根据前述实施例中任一实施例所述的方法，其中TRE执行进一步的检查。

[0483] 268.根据前述实施例中任一实施例所述的方法，其中M2ME中的位于TRE外部但受TRE的完整性保护的测量组件执行进一步的检查。

[0484] 269.根据前述实施例中任一实施例所述的方法，其中TRE允许M2ME参与请求的认证过程。

[0485] 270.根据前述实施例中任一实施例所述的方法，其中自发确认在所需的外部通信方面是最经济的方法。

[0486] 271.根据前述实施例中任一实施例所述的方法，其中自发确认不允许任意外部实体在网络接入期间或在未中断连接阶段独立评估TRE的完整性。

[0487] 272.根据前述实施例中任一实施例所述的方法，其中TRE存储确认过程和其结果的日志。

[0488] 273.根据前述实施例中任一实施例所述的方法，其中日志构成核查记录。

[0489] 274.根据前述实施例中任一实施例所述的方法，其中核查数据被存储在安全内部文件中。

[0490] 275.根据前述实施例中任一实施例所述的方法，其中安全内部文件在TRE中。

[0491] 276.根据前述实施例中任一实施例所述的方法，其中TRE保护安全内部文件。

[0492] 277.根据前述实施例中任一实施例所述的方法，其中检测对安全内部文件的损害。

[0493] 278.根据前述实施例中任一实施例所述的方法，其中提供数据的完整性保护。

[0494] 279.根据前述实施例中任一实施例所述的方法，其中核查数据专用于调用自发确认。

[0495] 280.根据前述实施例中任一实施例所述的方法，其中数据包括确认的目的。

[0496] 281.根据前述实施例中任一实施例所述的方法，其中在接入协议中建立的共享秘密或凭证被附着到核查数据，且TRE将数字签名应用于产生的数据以保护其完整性。

[0497] 282.根据前述实施例中任一实施例所述的方法，其中独立于M2ME的实体周期性地请求核查数据以确定在每个早期的网络接入事件M2ME是否是可信的。

[0498] 283.根据前述实施例中任一实施例所述的方法，其中使用关于网络接入尝试的网络侧协议对数据进行反向检查以检测损害。

[0499] 284.根据前述实施例中任一实施例所述的方法，其中当M2ME的其余部分的其它组件、配置或参数被载入、启动、或在可用于测量组件的任意其它预定义运行时间的时间事件

时，这些其它组件、配置或参数的完整性被检查。

[0500] 285.根据前述实施例中任一实施例所述的方法，其中远程实体间接知道M2ME已经通过半自发确认测试。

[0501] 286.根据前述实施例中任一实施例所述的方法，其中存在到网络的半自发确认结果的显式信令。

[0502] 287.根据前述实施例中任一实施例所述的方法，其中信令以加密的方式被保护。

[0503] 288.根据前述实施例中任一实施例所述的方法，其中信令在MID下载所需的M2ME认证之前。

[0504] 289.根据前述实施例中任一实施例所述的方法，其中信令包括TRE认证与用于有效性检查的M2ME中的资源之间的绑定的证据。

[0505] 290.根据前述实施例中任一实施例所述的方法，其中证据包括从M2ME发送到网络的令牌，该令牌提供用于建立TRE和M2ME的验证的进一步信息。

[0506] 291.根据前述实施例中任一实施例所述的方法，其中PVA或SHO请求TRE周期性地执行确认。

[0507] 292.根据前述实施例中任一实施例所述的方法，其中安全性网关(SeGW)请求确认。

[0508] 293.根据前述实施例中任一实施例所述的方法，其中在M2ME被注册后，请求被发送。

[0509] 294.根据前述实施例中任一实施例所述的方法，其中在首次认证家庭e节点B(H(e)NB)时由SeGW发送请求。

[0510] 295.根据前述实施例中任一实施例所述的方法，其中请求作为受保护操作和维护(OAM)消息从PVA、SHO、SeGW中的一者或多者被周期性地发送。

[0511] 296.根据前述实施例中任一实施例所述的方法，其中周期性重新确认的周期相对较长，但足够短以使得SHO在确认的新颖性方面觉得安全。

[0512] 297.根据前述实施例中任一实施例所述的方法，其中TRE基于请求执行确认过程。

[0513] 298.根据前述实施例中任一实施例所述的方法，其中TRE生成指示最后成功确认的时间戳。

[0514] 299.根据前述实施例中任一实施例所述的方法，其中TRE发送指示最后的确认在周期确认的当前回合终止之前发生的消息。

[0515] 300.根据前述实施例中任一实施例所述的方法，其中不存在关于确认结果的显式信令。

[0516] 301.根据前述实施例中任一实施例所述的方法，其中M2M1E启动到预定安全状态。

[0517] 302.根据前述实施例中任一实施例所述的方法，其中M2ME请求TRE生成平台有效性的证据。

[0518] 303.根据前述实施例中任一实施例所述的方法，其中TRE从M2ME的其余部分收集用于生成平台有效性的证据的材料。

[0519] 304.根据前述实施例中任一实施例所述的方法，其中证据包括安全性临界可执行代码、用于M2ME操作系统的凭证、以及设备ID。

[0520] 305.根据前述实施例中任一实施例所述的方法，其中TRE生成用于M2ME的确认的

证据，并通过加密的方式保护其完整性和私密性。

[0521] 306.根据前述实施例中任一实施例所述的方法，其中M2ME将受保护的证据转发到PVA。

[0522] 307.根据前述实施例中任一实施例所述的方法，其中PVA接收受保护的证据，并评估该证据以确定M2ME是否值得足够信任以继续执行MID的认证和下载。

[0523] 308.根据前述实施例中任一实施例所述的方法，其中M2ME确认与认证之间的绑定被执行。

[0524] 309.根据前述实施例中任一实施例所述的方法，其中绑定包括证实M2ME的安全状态的M2ME的证书或凭证。

[0525] 310.根据前述实施例中任一实施例所述的方法，其中绑定包括更安全的验证方式。

[0526] 311.根据前述实施例中任一实施例所述的方法，其中ICF认证M2ME以作为初始网络连接的前提。

[0527] 312.根据前述实施例中任一实施例所述的方法，其中在下载MID之前，DPF认证M2ME以证明该M2ME包含经认证的TRE。

[0528] 313.根据前述实施例中任一实施例所述的方法，其中SHO在可操作的网络接入之前认证M2ME。

[0529] 314.根据前述实施例中任一实施例所述的方法，其中对于自发确认，有效性到网络接入认证的绑定是隐式的。

[0530] 315.根据前述实施例中任一实施例所述的方法，其中令牌在初始附着消息中被传递，该消息提供关于TRE的标识的进一步信息。

[0531] 316.根据前述实施例中任一实施例所述的方法，其中存在持有认证凭证的TRE到M2ME的逻辑绑定。

[0532] 317.根据前述实施例中任一实施例所述的方法，其中设备平台的完整性在认证期间被确认。

[0533] 318.根据前述实施例中任一实施例所述的方法，其中存在TRE到M2ME的逻辑绑定。

[0534] 319.根据前述实施例中任一实施例所述的方法，其中设备平台的完整性在TRE认证期间被确认。

[0535] 320.根据前述实施例中任一实施例所述的方法，其中通过使用安全嵌入到M2ME的硬件安全性组件的功能来执行平台资源的实际确认。

[0536] 321.根据前述实施例中任一实施例所述的方法，其中通过使用在TRE外部但TRE确保其安全性属性且具有到TRE的安全连接的硬件安全性组件来执行平台资源的实际确认。

[0537] 322.根据前述实施例中任一实施例所述的方法，其中确认和认证被结合到公共协议的会话中。

[0538] 323.根据前述实施例中任一实施例所述的方法，其中IKEv2被用于结合的确认和认证过程中。

[0539] 324.根据前述实施例中任一实施例所述的方法，其中ICF、DRF和DPF是单独实体。

[0540] 325.根据前述实施例中任一实施例所述的方法，其中ICF、DRF和DPF被结合。

[0541] 326.根据前述实施例中任一实施例所述的方法，其中当M2ME在初始网络接入时接

入3G VNO的网络时，将MID下载并提供到M2ME的过程发生。

[0542] 327.根据前述实施例中任一实施例所述的方法，其中VNO提供到M2ME的空中接口。

[0543] 328.根据前述实施例中任一实施例所述的方法，其中M2ME使用标准GSM/UMT规则来解码网络信息并使用附着消息附着到VNO的网络。

[0544] 329.根据前述实施例中任一实施例所述的方法，其中附着消息包含临时M2ME ID(PCID)。

[0545] 330.根据前述实施例中任一实施例所述的方法，其中VNO使用标准UMTS AKA过程来认证M2ME。

[0546] 331.根据前述实施例中任一实施例所述的方法，其中VNO基于PCID的内容和结构将该PCID识别为IMSI。

[0547] 332.根据前述实施例中任一实施例所述的方法，其中M2ME和VNO支持公共认证算法。

[0548] 333.根据前述实施例中任一实施例所述的方法，其中公共认证算法是Milenage.

[0549] 334.根据前述实施例中任一实施例所述的方法，其中将PCID识别为M2ME的ID的VNO联系将接受PCID为合法初步凭证的ICF。

[0550] 335.根据前述实施例中任一实施例所述的方法，其中ICF发布一组用于保护与M2ME的进一步通信的初步AV，并开始提供到M2ME的受保护的IP连接。

[0551] 336.根据前述实施例中任一实施例所述的方法，其中M2ME和ICF执行标准AKA过程来产生用于保护与M2ME的通信的初步AKA密钥。

[0552] 337.根据前述实施例中任一实施例所述的方法，其中ICF将M2ME重新指向DPF。

[0553] 338.根据前述实施例中任一实施例所述的方法，其中ICF发送PCID到DRF。

[0554] 339.根据前述实施例中任一实施例所述的方法，其中DRF帮助M2ME找到SHO。

[0555] 340.根据前述实施例中任一实施例所述的方法，其中DRF连接到SHO并注册M2ME以连接到SHO的网络。

[0556] 341.根据前述实施例中任一实施例所述的方法，其中SHO请求PVA确认TRE的真实性和完整性。

[0557] 342.根据前述实施例中任一实施例所述的方法，其中PVA确认TRE的真实性和完整性。

[0558] 343.根据前述实施例中任一实施例所述的方法，其中PVA发送确认结果到SHO。

[0559] 344.根据前述实施例中任一实施例所述的方法，其中SHO联系DPF并授权提供MID给M2ME。

[0560] 345.根据前述实施例中任一实施例所述的方法，其中DPF将MID下载到M2ME。

[0561] 346.根据前述实施例中任一实施例所述的方法，其中M2ME提供下载的MID给TRE并向DPF报告提供的状态。

[0562] 347.根据前述实施例中任一实施例所述的方法，其中M2ME发送用于验证状态消息的令牌。

[0563] 348.根据前述实施例中任一实施例所述的方法，其中令牌能抵抗损害和重放攻击。

[0564] 349.根据前述实施例中任一实施例所述的方法，其中DPF向SHO报告提供的状态。

[0565] 350.根据前述实施例中任一实施例所述的方法，其中当M2ME在初始网络接入时接入3G VNO的网络时，MID的下载和提供的过程发生。

[0566] 351.根据前述实施例中任一实施例所述的方法，其中在释放临时向量到M2ME之前以及在允许到M2ME的IP连接之前，ICF请求PVA确认TRE。

[0567] 352.根据前述实施例中任一实施例所述的方法，其中M2ME持有者联系新SHO以传输M2ME参数。

[0568] 353.根据前述实施例中任一实施例所述的方法，其中M2ME持有者联系M2ME以发起重新提供。

[0569] 354.根据前述实施例中任一实施例所述的方法，其中新SHO请求确认实体确认M2ME。

[0570] 355.根据前述实施例中任一实施例所述的方法，其中确认实体确认M2ME并发送结果到新SHO。

[0571] 356.根据前述实施例中任一实施例所述的方法，其中新SHO请求DPF下载并提供新MID到M2ME。

[0572] 357.根据前述实施例中任一实施例所述的方法，其中DPF安全地将新MID包下载到M2ME。

[0573] 358.根据前述实施例中任一实施例所述的方法，其中M2ME发送已经丢弃了旧的MID的消息给旧的SHO。

[0574] 359.根据前述实施例中任一实施例所述的方法，其中旧的SHO发送ACK到M2ME。

[0575] 360.根据前述实施例中任一实施例所述的方法，其中M2ME将ACK转发给DPF和新SHO。

[0576] 361.根据前述实施例中任一实施例所述的方法，其中M2ME在DPF的帮助下更新该M2ME的系统并安装MID。

[0577] 362.根据前述实施例中任一实施例所述的方法，其中M2ME发送状态到DPF。

[0578] 363.根据前述实施例中任一实施例所述的方法，其中DPF向新SHO报告状态。

[0579] 364.根据前述实施例中任一实施例所述的方法，其中M2ME被置于初始状态并运行初始提供过程。

[0580] 365.根据前述实施例中任一实施例所述的方法，其中PVA用于确保在M2ME仍然预定到相同SHO时被执行的任意软件或固件(SW/FW)更新以安全的方式完成。

[0581] 366.根据前述实施例中任一实施例所述的方法，其中PVA或DPF监管例如安全的空中或通过有线的SW/FW的下载以及M2ME或TRE的重新提供的过程。

[0582] 367.根据前述实施例中任一实施例所述的方法，其中PVA或DPF使用OMA DM和OMA FOTA过程。

[0583] 368.根据前述实施例中任一实施例所述的方法，其中M2ME的信任状态信息由于远程SW/FW更新或重新配置而被改变。

[0584] 369.根据前述实施例中任一实施例所述的方法，其中PVA或DPF被配置成发起M2ME或TRE的新的可验证根或运行时间信任状态信息检查并获得其结果。

[0585] 370.根据前述实施例中任一实施例所述的方法，其中M2ME被配置成检查损害。

[0586] 371.根据前述实施例中任一实施例所述的方法，其中检测损害包括对任意子系统

的损害。

[0587] 372.根据前述实施例中任一实施例所述的方法，其中损害检测被频繁执行。

[0588] 373.根据前述实施例中任一实施例所述的方法，其中损害事件包括以下中的一者或多者：由于错误或病毒导致的可补救和/或不可补救的泄密，缓存器溢出事件，无线电或更高层连接特性和/或环境读取的突发未预料或未授权改变，可信网络元件造成的用于初步认证、注册或MID提供的M2ME请求的接入或服务的过度重复失败和/或拒绝，或关于远程MID管理功能的M2ME或M2ME子系统的信任状态的后置根或运行事件读取的任意未预料/未授权的改变。

[0589] 374.根据前述实施例中任一实施例所述的方法，其中其它网络元件被配置成检测损害。

[0590] 375.根据前述实施例中任一实施例所述的方法，其中M2ME响应于损害检测而采用步骤来限制损坏。

[0591] 376.根据前述实施例中任一实施例所述的方法，其中M2ME被配置成禁用远程MID管理。

[0592] 378.根据前述实施例中任一实施例所述的方法，其中M2ME被配置成向指定网络元件报告损害事件。

[0593] 379.根据前述实施例中任一实施例所述的方法，其中M2ME被配置成执行可补救行动，例如删除、隔离或卸载当前软件更新或可以病毒或错误代码或数据。

[0594] 380.根据前述实施例中任一实施例所述的方法，其中M2ME被配置成删除与MID管理功能相关的任意预先指定的数据集。

[0595] 381.根据前述实施例中任一实施例所述的方法，其中M2ME被配置成给M2ME或M2ME的部分或子系统断电。

[0596] 382.根据前述实施例中任一实施例所述的方法，其中网络元件被配置成执行后置损害补救措施。

[0597] 383.一种无线发射/接收单元(WTRU)，该WTRU被配置成执行上述实施例中任一实施例的至少一部分。

[0598] 384.一种机器对机器(M2M)设备，该M2M设备被配置成执行上述实施例中任一实施例的至少一部分。

[0599] 385.一种网络实体，该网络实体被配置成执行上述实施例中任一实施例的至少一部分。

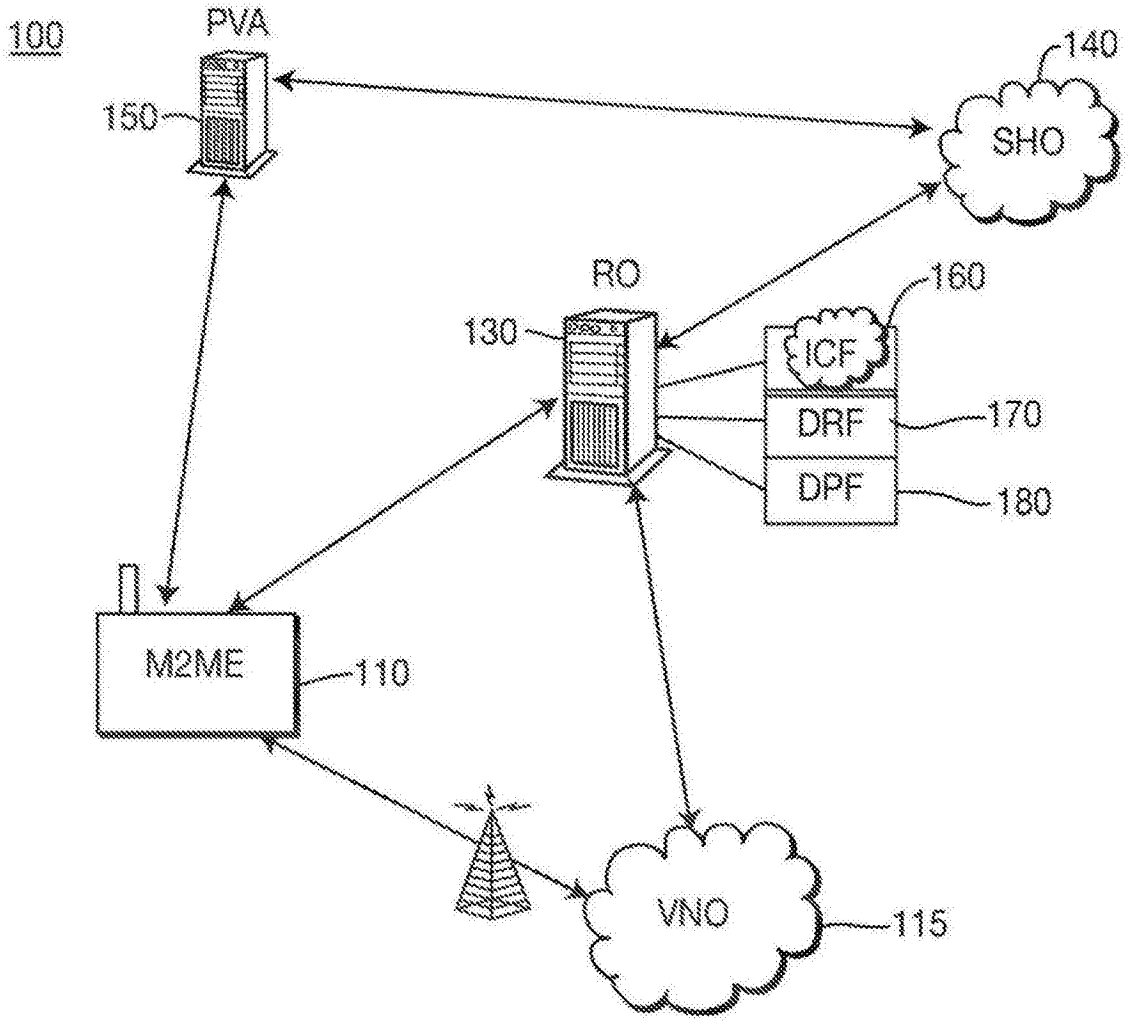

100
PVA
150
140
SHO
RO
130
160
ICF
DRF
170
DPF
180
M2ME
110
VNO
115

图1

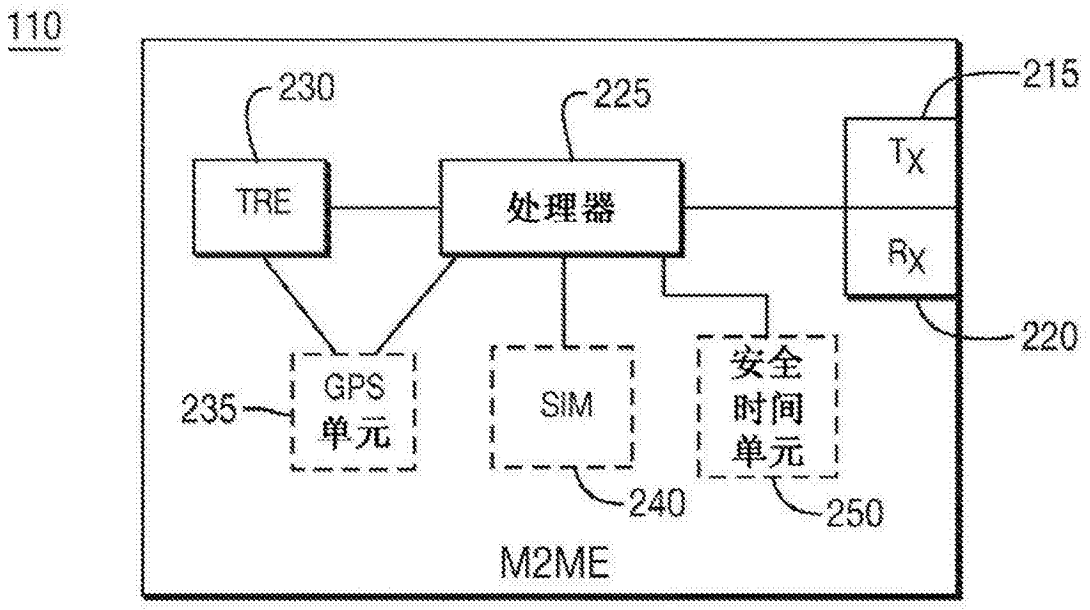

110
230
225
215
TRE
处理器
Tx
Rx
220
GPS
单元
235
SIM
240
安全
时间
单元
250
M2ME

图2

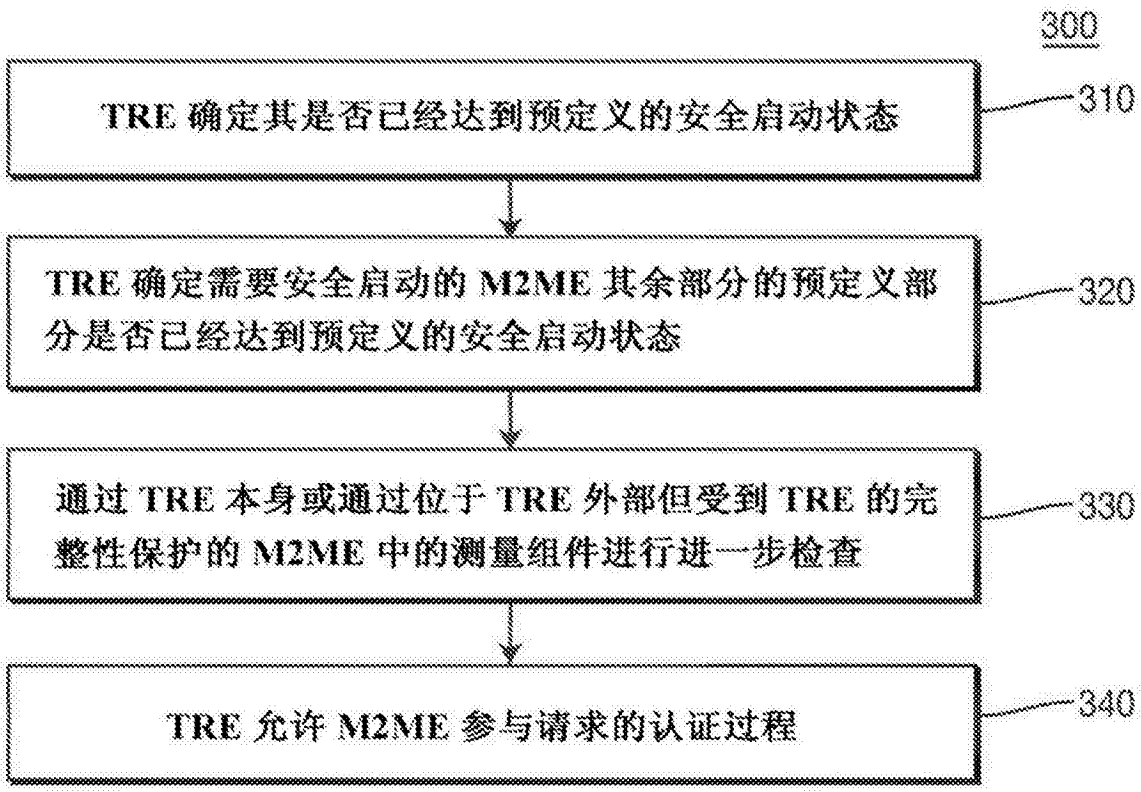

300
TRE 确定其是否已经达到预定义的安全启动状态
310
TRE 确定需要安全启动的 M2ME 其余部分的预定义部分是否已经达到预定义的安全启动状态
320
通过 TRE 本身或通过位于 TRE 外部但受到 TRE 的完整性保护的 M2ME 中的测量组件进行进一步检查
330
TRE 允许 M2ME 参与请求的认证过程
340

图3

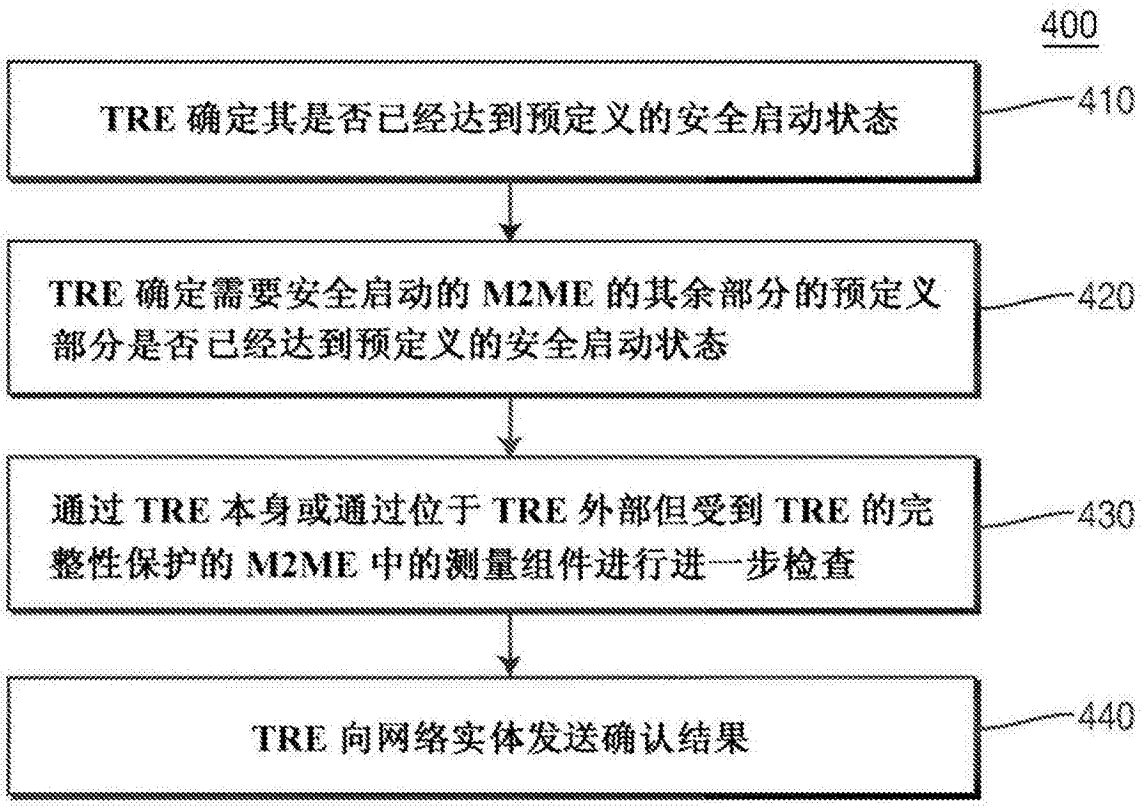

400
TRE 确定其是否已经达到预定义的安全启动状态
410
TRE 确定需要安全启动的 M2ME 的其余部分的预定义部分是否已经达到预定义的安全启动状态
420
通过 TRE 本身或通过位于 TRE 外部但受到 TRE 的完整性保护的 M2ME 中的测量组件进行进一步检查
430
TRE 向网络实体发送确认结果
440

图4

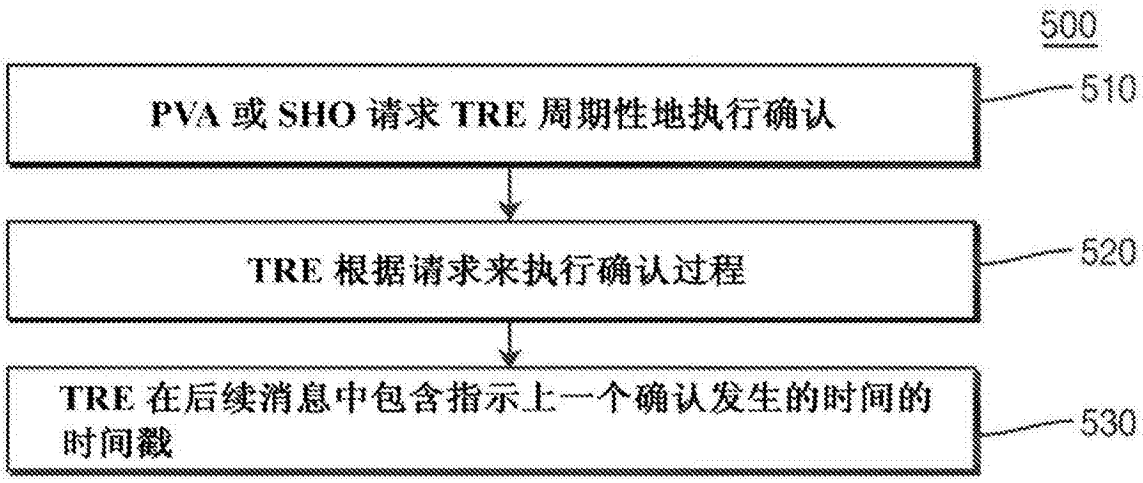

500
PVA 或 SHO 请求 TRE 周期性地执行确认
510
TRE 根据请求来执行确认过程
520
TRE 在后续消息中包含指示上一个确认发生的时间的时间戳
530

图5

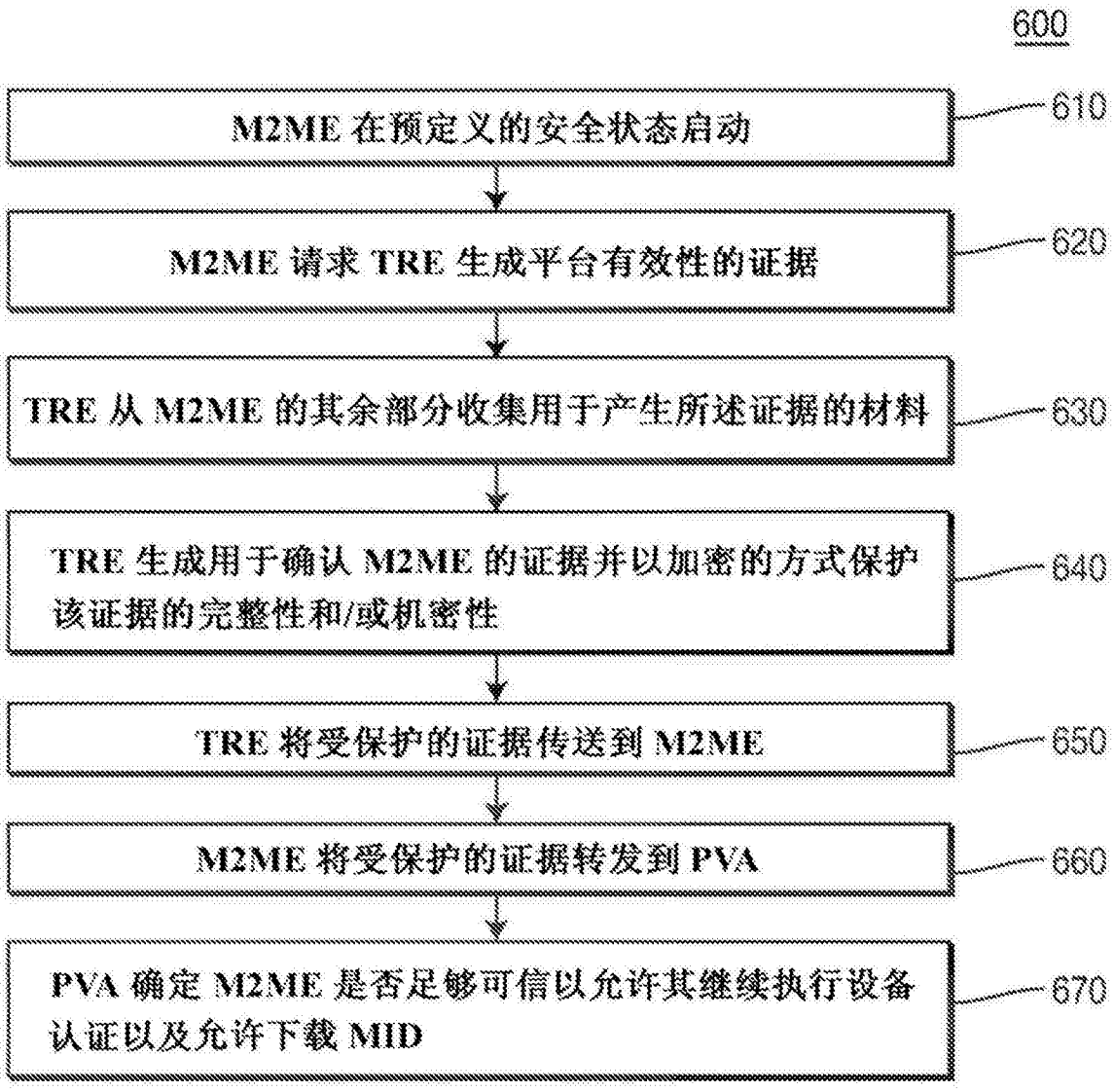

600
M2ME 在预定义的安全状态启动
610
M2ME 请求 TRE 生成平台有效性的证据
620
TRE 从 M2ME 的其余部分收集用于产生所述证据的材料
630
TRE 生成用于确认 M2ME 的证据并以加密的方式保护该证据的完整性和/或机密性
640
TRE 将受保护的证据传送到 M2ME
650
M2ME 将受保护的证据转发到 PVA
660
PVA 确定 M2ME 是否足够可信以允许其继续执行设备认证以及允许下载 MID
670

图6

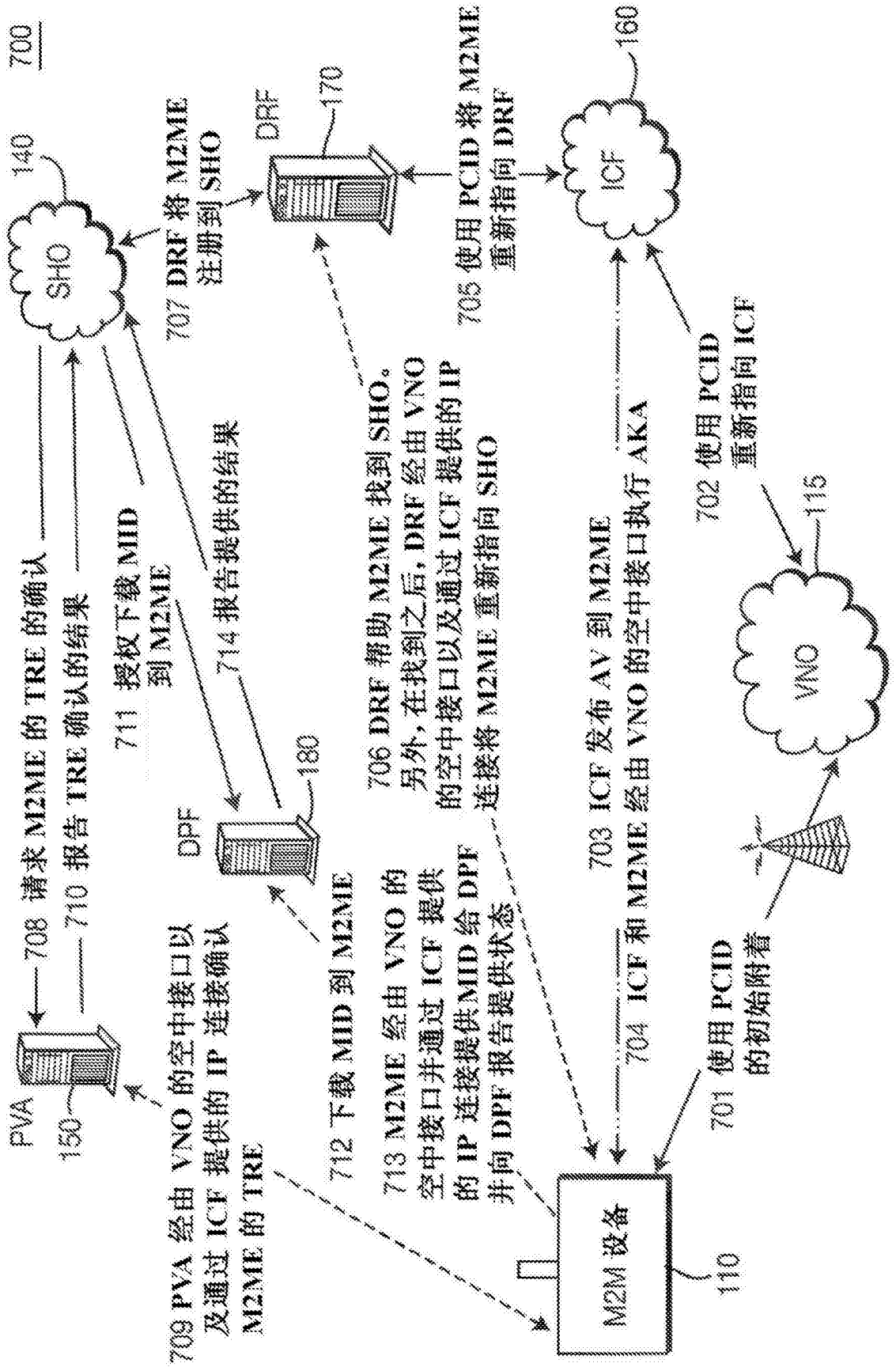

700
PVA
150
SHO
140
DRF
170
DPF
180
ICF
160
VNO
115
M2M 设备
110
708 请求 M2ME 的 TRE 的确认
710 报告 TRE 确认的结果
711 授权下载 MID 到 M2ME
707 DRF 将 M2ME 注册到 SHO
714 报告提供的结果
709 PVA 经由 VNO 的空中接口以及通过 ICF 提供的 IP 连接确认 M2ME 的 TRE
712 下载 MID 到 M2ME
713 M2ME 经由 VNO 的空中接口并通过 ICF 提供的 IP 连接提供 MID 给 DPF 并向 DPF 报告提供状态
706 DRF 帮助 M2ME 找到 SHO。另外，在找到之后，DRF 经由 VNO 的空中接口以及通过 ICF 提供的 IP 连接将 M2ME 重新指向 SHO
705 使用 PCID 将 M2ME 重新指向 DRF
703 ICF 发布 AV 到 M2ME
704 ICF 和 M2ME 经由 VNO 的空中接口执行 AKA
702 使用 PCID 重新指向 ICF
701 使用 PCID 的初始附着

图7

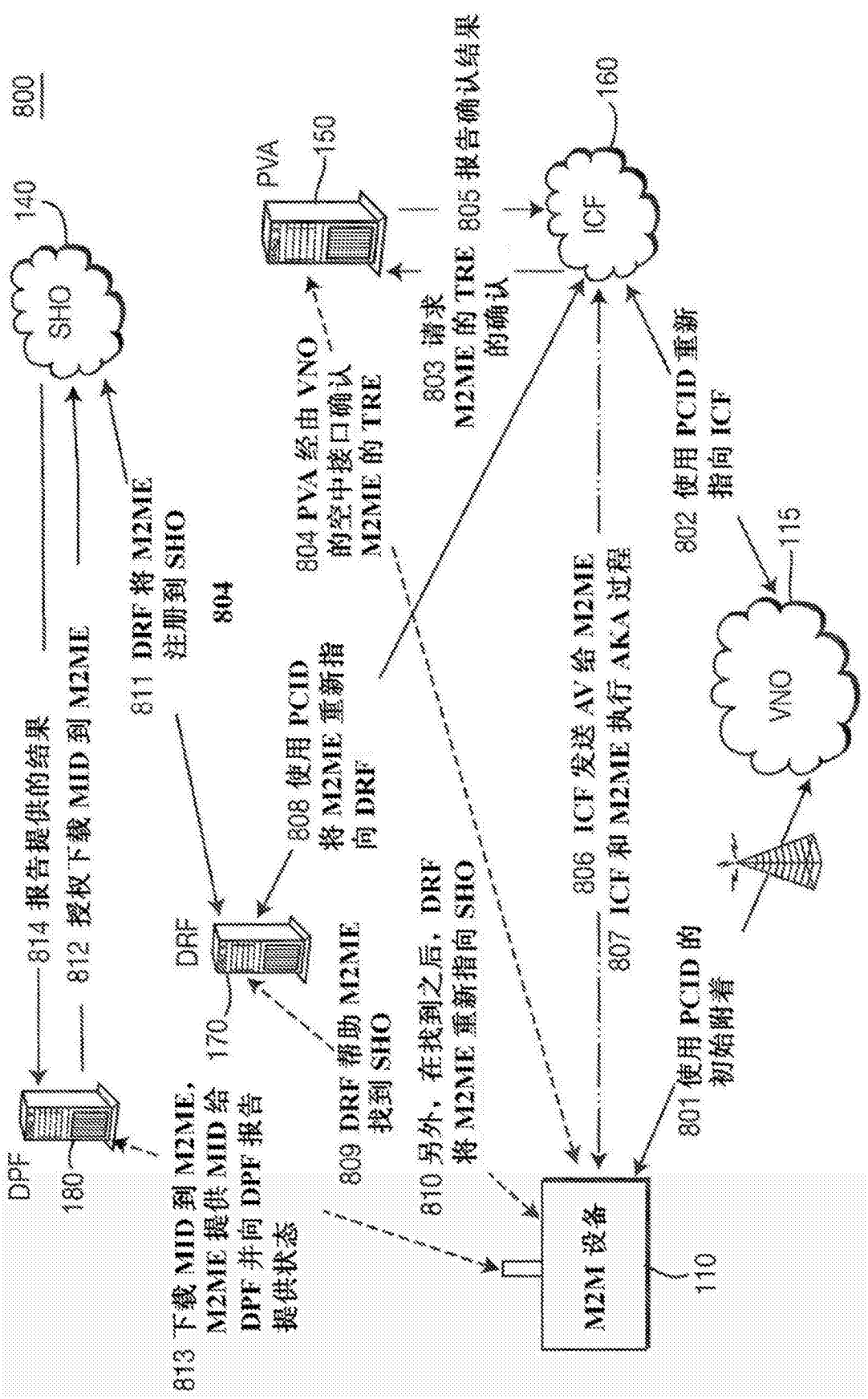

800
140
SHO
PVA
150
160
ICF
814 报告提供的结果
812 授权下载 MID 到 M2ME
811 DRF 将 M2ME 注册到 SHO
804
804 PVA 经由 VNO 的空中接口确认 M2ME 的 TRE
803 请求 M2ME 的 TRE 的确认
805 报告确认结果
802 使用 PCID 重新指向 ICF
DRF
170
808 使用 PCID 将 M2ME 重新指向 DRF
115
VNO
DPF
180
813 下载 MID 到 M2ME，M2ME 提供 MID 给 DPF 并向 DPF 报告提供状态
809 DRF 帮助 M2ME 找到 SHO
810 另外，在找到之后，DRF 将 M2ME 重新指向 SHO
806 ICF 发送 AV 给 M2ME
807 ICF 和 M2ME 执行 AKA 过程
801 使用 PCID 的初始附着
M2M 设备
110

图8

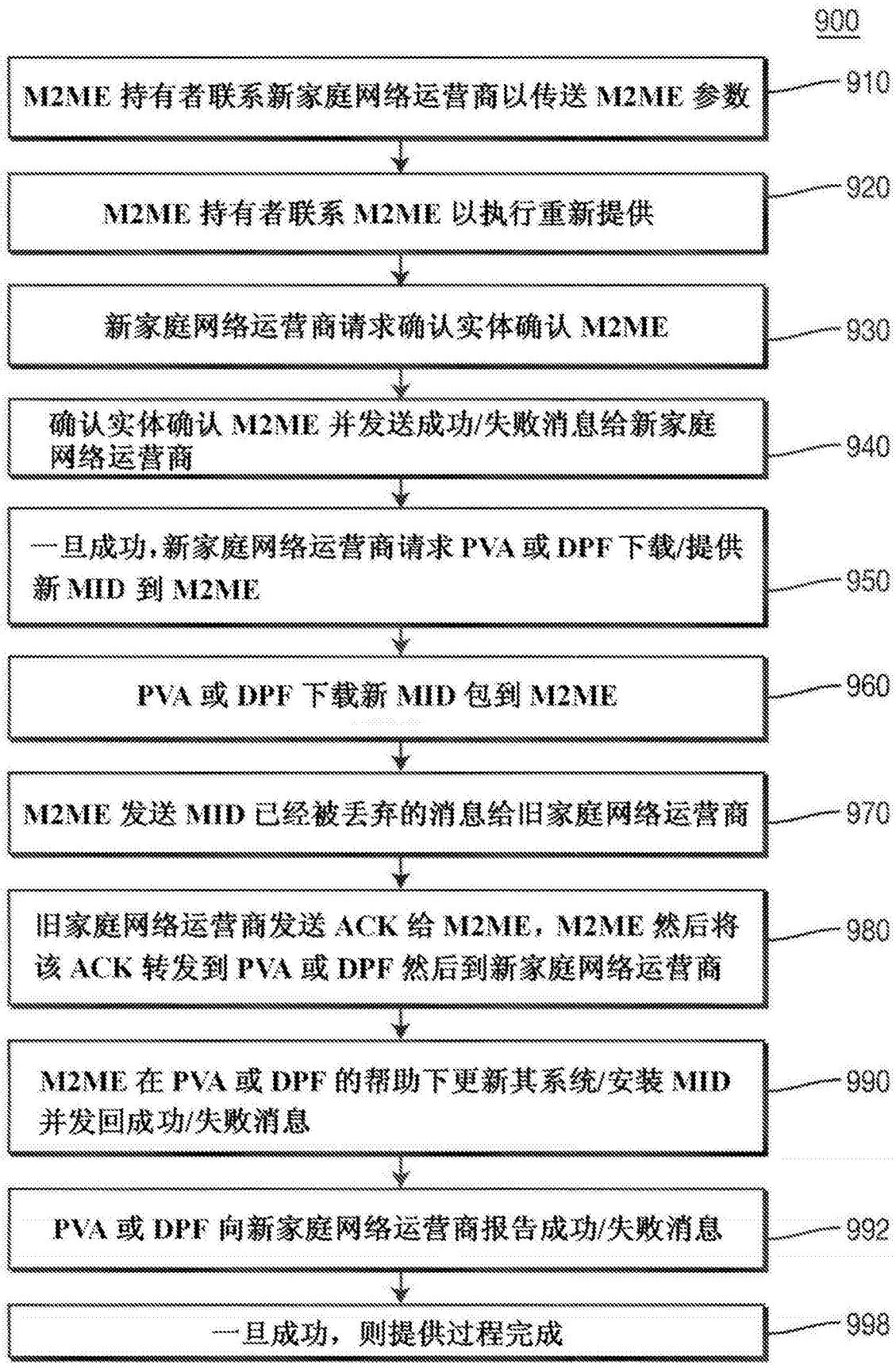

900
M2ME 持有者联系新家庭网络运营商以传送 M2ME 参数
910
M2ME 持有者联系 M2ME 以执行重新提供
920
新家庭网络运营商请求确认实体确认 M2ME
930
确认实体确认 M2ME 并发送成功/失败消息给新家庭网络运营商
940
一旦成功，新家庭网络运营商请求 PVA 或 DPF 下载/提供新 MID 到 M2ME
950
PVA 或 DPF 下载新 MID 包到 M2ME
960
M2ME 发送 MID 已经被丢弃的消息给旧家庭网络运营商
970
旧家庭网络运营商发送 ACK 给 M2ME，M2ME 然后将该 ACK 转发到 PVA 或 DPF 然后到新家庭网络运营商
980
M2ME 在 PVA 或 DPF 的帮助下更新其系统/安装 MID 并发回成功/失败消息
990
PVA 或 DPF 向新家庭网络运营商报告成功/失败消息
992
一旦成功，则提供过程完成
998

图9