



(12) 发明专利

(10) 授权公告号 CN 107547571 B

(45) 授权公告日 2021.06.22

(21) 申请号 201710928740.5

(22) 申请日 2013.11.20

(65) 同一申请的已公布的文献号
申请公布号 CN 107547571 A

(43) 申请公布日 2018.01.05

(30) 优先权数据
61/729,208 2012.11.21 US

(62) 分案原申请数据
201380060499.9 2013.11.20

(73) 专利权人 苹果公司
地址 美国加利福尼亚

(72) 发明人 C·B·夏普 Y·H·韦德 李莉
J·V·豪客 A·G·马赛厄斯
杨翔英 K·P·麦克劳克林

(74) 专利代理机构 中国贸促会专利商标事务所
有限公司 11038

代理人 李晓芳

(51) Int.Cl.
H04L 29/06 (2006.01)
H04W 12/08 (2021.01)
G06F 21/60 (2013.01)

(56) 对比文件
CN 101589361 A, 2009.11.25
WO 2012154600 A1, 2012.11.15
WO 2012058099 A1, 2012.05.03
CN 102487377 A, 2012.06.06
Apple. “eUICC Use Cases and Requirement on Policy Enforcement”.
《SCPREQ (12) 000051R3, ETSI TC SCP REQ#36》
.2012,

审查员 李珍珍

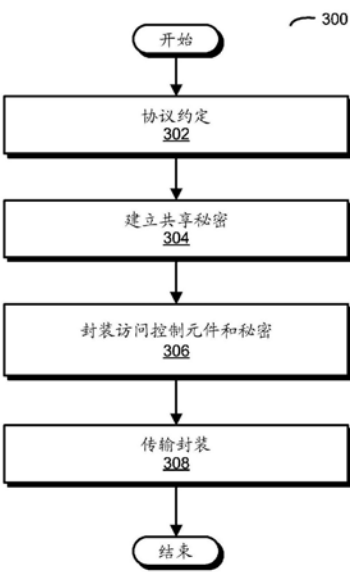
权利要求书3页 说明书23页 附图7页

(54) 发明名称

用于管理访问控制的方法和访问控制客户端供应服务器

(57) 摘要

本公开涉及用于管理访问控制的基于策略的技术。本发明描述了基于策略的框架。该基于策略的框架可用于为逻辑实体指定执行与位于电子设备中的安全元件内的访问控制元件(诸如, 电子用户身份模块)相关联的操作的特权。需注意, 不同逻辑实体可针对与相同或不同访问控制元件相关联的不同操作具有不同特权。此外, 基于策略的框架可指定逻辑实体在认证期间使用的凭证的类型, 使得不同类型的凭证可用于不同操作和/或由不同逻辑实体使用。此外, 基于策略的框架可指定逻辑实体在认证期间使用的安全协议和安全级别, 使得不同安全协议和安全级别可用于不同操作和/或由不同逻辑实体使用。



1. 一种用于保护第一设备和第二设备之间的访问控制客户端的传输的安全的方法,所述方法包括:

在存储所述访问控制客户端的所述第一设备处:

发起所述访问控制客户端到所述第二设备的传输;

识别由所述第二设备实现的至少一个安全策略;以及

当所述至少一个安全策略满足由所述第一设备实现的一个或多个安全策略时:

准备将被传输到所述第二设备的所述访问控制客户端,以及

将所述访问控制客户端传输到所述第二设备。

2. 根据权利要求1所述的方法,其中所述第一设备为第一移动无线设备,并且所述第二设备为第二移动无线设备。

3. 根据权利要求1所述的方法,其中所述第一设备为访问控制客户端供应服务器,并且所述第二设备为移动无线设备。

4. 根据权利要求1所述的方法,其中所述访问控制客户端是使用与所述第二设备相关联的第一公钥加密的。

5. 根据权利要求4所述的方法,其中准备将被传输到所述第二设备的所述访问控制客户端包括:

使用与所述第一公钥相关联的私钥来解密所述访问控制客户端;

识别与所述第二设备相关联的第二公钥,以及

使用所述第二公钥来加密所述访问控制客户端。

6. 根据权利要求1所述的方法,其中所述访问控制客户端为电子用户身份模块eSIM。

7. 根据权利要求1所述的方法,还包括在将所述访问控制客户端传输到所述第二设备之后:

对所述第一设备处的所述访问控制客户端去激活。

8. 一种访问控制客户端供应服务器,包括:

安全存储器,被配置为存储多个访问控制客户端;以及

处理器,被配置为使得所述访问控制客户端供应服务器执行以下步骤,所述步骤包括:

从移动无线设备接收将所述多个访问控制客户端中的特定访问控制客户端传输到所述移动无线设备的请求,

识别由所述移动无线设备实现的第一安全策略,

确定所述第一安全策略与由所述访问控制客户端供应服务器实现的第二安全策略一致,

准备将被传输到所述移动无线设备的所述特定访问控制客户端,以及

将所述特定访问控制客户端传输到所述移动无线设备。

9. 根据权利要求8所述的访问控制客户端供应服务器,其中所述第二安全策略指示与将访问控制客户端传输到目标移动无线设备相关联的要求,并且所述第一安全策略满足由所述第二安全策略指示的所述要求。

10. 根据权利要求8所述的访问控制客户端供应服务器,其中准备将被传输到所述移动无线设备的所述特定访问控制客户端包括:

获得与所述移动无线设备相关联的公钥,

生成对于所述移动无线设备的质疑,以及
使用所述公钥来加密所述特定访问控制客户端和所述质疑。

11. 根据权利要求10所述的访问控制客户端供应服务器,其中在将所述特定访问控制客户端传输到所述移动无线设备之后,所述步骤还包括:

从所述移动无线设备接收对所述质疑的响应;
当所述响应指示所述质疑得到满足时:
从所述多个访问控制客户端中去除所述特定访问控制客户端;以及
当所述响应指示所述质疑未得到满足时:
保留所述多个访问控制客户端内的所述特定访问控制客户端。

12. 根据权利要求8所述的访问控制客户端供应服务器,其中所述访问控制客户端供应服务器包括在被配置为彼此通信的一组访问控制客户端供应服务器中,并且所述特定访问控制客户端存储在包括在所述一组访问控制客户端供应服务器中的至少一个不同的访问控制客户端供应服务器上。

13. 根据权利要求12所述的访问控制客户端供应服务器,其中所述步骤还包括:

向所述至少一个不同的访问控制客户端供应服务器指示所述特定访问控制客户端正在被传输到所述移动无线设备。

14. 根据权利要求8所述的访问控制客户端供应服务器,其中所述多个访问控制客户端中的每个访问控制客户端为电子用户身份模块eSIM。

15. 一种访问控制客户端供应服务器,包括:

用于从设备接收将多个访问控制客户端中的特定访问控制客户端传输到所述设备的请求的装置,其中所述多个访问控制客户端由所述访问控制客户端供应服务器管理;

用于识别由所述设备实现的第一安全策略的装置;

用于确定所述第一安全策略与由所述访问控制客户端供应服务器实现的第二安全策略一致的装置;

用于准备将被传输到所述设备的所述特定访问控制客户端的装置;以及

用于将所述特定访问控制客户端传输到所述设备的装置。

16. 根据权利要求15所述的访问控制客户端供应服务器,其中所述第二安全策略指示与将访问控制客户端传输到目标设备相关联的要求,并且所述第一安全策略满足由所述第二安全策略指示的所述要求。

17. 根据权利要求15所述的访问控制客户端供应服务器,其中准备将被传输到所述设备的所述特定访问控制客户端包括:

获得与所述设备相关联的公钥,
生成对于所述设备的质疑,以及
使用所述公钥来加密所述特定访问控制客户端和所述质疑。

18. 根据权利要求17所述的访问控制客户端供应服务器,还包括用于在将所述特定访问控制客户端传输到所述设备之后,执行以下步骤的装置:

从所述设备接收对所述质疑的响应;
当所述响应指示所述质疑得到满足时:
从所述多个访问控制客户端中去除所述特定访问控制客户端;以及

当所述响应指示所述质疑未得到满足时：

保留所述多个访问控制客户端内的所述特定访问控制客户端。

19. 根据权利要求15所述的访问控制客户端供应服务器，其中所述访问控制客户端供应服务器包括在被配置为彼此通信的一组访问控制客户端供应服务器中，并且所述特定访问控制客户端存储在包括在所述一组访问控制客户端供应服务器中的至少一个不同的访问控制客户端供应服务器上。

20. 根据权利要求19所述的访问控制客户端供应服务器，还包括：

用于向所述至少一个不同的访问控制客户端供应服务器指示所述特定访问控制客户端正在被传输到所述设备的装置。

用于管理访问控制的方法和访问控制客户端供应服务器

[0001] 本申请是国际申请日为2013年11月20日、国家申请号为201380060499.9、发明名称为“用于管理访问控制的基于策略的技术”的进入中国国家阶段的PCT申请的分案申请。

技术领域

[0002] 所公开的实施例涉及用于促进无线系统中的认证和安全通信的技术。更具体地，所公开的实施例涉及用于管理逻辑实体的特权的技术，该逻辑实体执行与电子设备中的安全元件中的安全访问控制元件相关联的操作。

背景技术

[0003] 许多无线通信系统使用访问控制技术来确保安全通信。例如，访问控制技术可涉及：验证通信方的身份；以及授予与所验证的身份相称的访问水平。在蜂窝电话系统（诸如通用移动通信系统或UMTS）中，访问控制通常由在物理通用集成电路卡（UICC）上执行的访问控制元件或客户端（诸如，通用用户身份模块或USIM）来管理。访问控制客户端通常认证蜂窝网络的用户。在成功认证之后，用户可被允许访问蜂窝网络。在随后的讨论中，需注意，“访问控制客户端”通常指的是控制从电子设备到网络的访问的逻辑实体（可在硬件和/或软件中实现）。除了USIM之外，访问控制客户端可包括：CDMA用户身份模块（CSIM）、IP多媒体服务身份模块（ISIM）、用户身份模块（SIM）、可移除用户身份模块（RUIM）等。

[0004] 传统上，访问控制客户端执行认证和密钥协议（AKA）技术，其验证和解密应用数据和程序以确保安全初始化。具体地，访问控制客户端可：回答远程质疑以证明其对于网络运营商的身份，并且可发出质疑来验证网络的身份。

[0005] 尽管传统访问控制客户端解决方案在可移除集成电路卡（ICC）（有时称为“SIM卡”）内实施，但最新研究涉及在电子设备上执行的软件客户端内的虚拟化SIM操作。虚拟化SIM操作可减小设备尺寸，增加设备功能并提供更大的灵活性。注意“虚拟化SIM”可指电子SIM（eSIM）。

[0006] 然而，虚拟化SIM操作还为网络运营商和设备制造商呈现新的质疑。例如，传统SIM卡由可信SIM供应商制造并保证。这些传统SIM卡执行已永久烧录到SIM卡的单一安全版本的软件。一旦被烧录，SIM卡通常不能加以改变或篡改（在另外不损坏SIM卡的情况下）。

[0007] 相反，便携式电子设备由范围广泛的设备制造商制造，并且可执行由多个并且可能未知的第三方软件供应商提供的软件。另外，便携式电子设备经常利用能解决现有缺陷并且同时引入新缺陷的软件来“打补丁”。由此，该软件会易于受到损坏、蓄意破坏和/或滥用。

[0008] 此外，尽管物理SIM卡极难复制，但软件可容易被拷贝、倍增等。因为每个SIM代表约定对有限网络资源的访问量，所以对虚拟化SIM的非法使用会极大影响网络操作和用户体验（例如，此类非法使用可掠夺将另外对合法用户可用的资源网络，从而降级针对此类合法用户的服务速度、可用性等）。

[0009] 作为结果，需要新的解决方案来为通常与传统物理SIM类似的虚拟化SIM（以及，更

一般地,访问控制客户端)提供保护和其他属性。此外,需要改进的解决方案以用于存储和分发虚拟化访问控制客户端。理想地,这些解决方案可提供传统访问控制客户端操作的益处,其中虚拟操作提供增加的性能。

发明内容

[0010] 所述实施例涉及电子设备。该电子设备包括具有访问控制元件的安全元件,该访问控制元件识别服务的用户并且促进安全通信,其中访问控制元件与一组操作相关联。此外,安全元件包括处理器和存储器,该存储器存储程序模块和凭证管理模块,程序模块由该处理器执行,凭证管理模块为与一组操作相关联的逻辑实体指定具有一组特权的配置文件。此外,对于操作中的一些操作,逻辑实体中的一些逻辑实体具有不同特权。

[0011] 在一些实施例中,凭证管理模块包括程序模块指定该一组特权所使用的信息。

[0012] 需注意,访问控制元件可包括电子用户身份模块(eSIM)。

[0013] 此外,逻辑实体可位于电子设备的内部和/或外部。

[0014] 此外,访问控制元件可包括用于为逻辑实体和第二逻辑实体中的至少一者指定第二组特权的信息。在与该一组特权相关联的安全级别和与第二组特权相关联的第二安全级别之间发生冲突的情况下,安全元件可将安全级别和第二安全级别进行比较并且可选择该一组特权和第二组特征中的与较强安全性相关联的一者。另选地,在与该一组特权相关联的安全级别和与第二组特权相关联的第二安全级别之间发生冲突的情况下,安全元件可选择该一组特权。

[0015] 另外,该一组操作可包括:加载访问控制元件、启用访问控制元件、禁用访问控制元件、输出访问控制元件和/或删除访问控制元件。

[0016] 在一些实施例中,凭证管理模块包括与该一组操作相关联的对称加密密钥,并且给定的加密密钥有助于提供与该一组操作相关联的特权。另选地或除此之外,凭证管理模块可包括证书和与该一组操作相关联的非对称加密密钥以有助于非对称加密,并且给定的加密密钥和给定的证书可有助于提供与该一组操作相关联的特权。

[0017] 另一实施例提供了一种用于为逻辑实体指定一组特权的方法。在该方法期间,从第一逻辑实体和第二逻辑实体接收凭证。随后,基于凭证和凭证管理模块为第一逻辑实体和第二逻辑实体确定与该一组操作相关联的该一组特权。接下来,指定第一逻辑实体和第二逻辑实体的该一组特权的信息被提供给电子设备中的安全元件中的访问控制元件,其中访问控制元件识别服务的用户并有助于安全通信。此外,访问控制元件与该一组操作相关联,对于操作中的一些操作,第一逻辑实体和第二逻辑实体具有不同特权。

[0018] 在一些实施例中,使用电子设备中的处理器执行程序模块。

附图说明

[0019] 图1是示出了现有的认证和密钥协议(AKA)技术的图示。

[0020] 图2是示出了根据本公开的实施例的用于分发访问控制元件的网络架构的框图。

[0021] 图3是示出了根据本公开的实施例的用于将访问控制元件传输到电子设备的方法的流程图。

[0022] 图4是示出了根据本公开的实施例的针对与访问控制元件相关联的一组操作为逻

辑实体指定一组特权的方法的流程图。

[0023] 图5是示出了根据本公开的实施例的适用于存储一个或多个访问控制元件的电子通用集成电路卡 (eUICC) 装置的框图。

[0024] 图6是示出了根据本公开的实施例的适用于存储和使用一个或多个访问控制元件的电子设备的框图。

[0025] 图7是示出了根据本公开的实施例的电子设备的框图。

具体实施方式

[0026] 概述

[0027] 所公开的实施例提供了用于存储访问控制元件并将访问控制元件分发到电子设备诸如便携式电子设备 (例如, “智能电话”等) 的装置和技术。用于传输访问控制元件 (例如, eSIM) 的电子设备可通过确保仅借助可信目标电子设备执行传输来实施访问控制元件的唯一性和保护。在一个实施例中, 公开了在硬件安全模块 (HSM) 中实现的eUICC装置。每个HSM都可存储大量eSIM以有助于其存储和分发, 例如用于零售服务。eUICC装置可验证其对等eUICC装置根据达成一致的且可信的协议进行操作。如果eUICC装置两者达成协议, 则当源eUICC装置传输其eSIM时, 其将删除其eSIM或者以其他方式使其自身eSIM闲置。目标eUICC装置可保留eSIM的唯一现行版本。

[0028] 在另一实施例中, 当将访问控制元件从电子设备移动到另一个电子设备时, 接收或目标电子设备发出质疑或唯一标识符。发送电子设备可使用接收电子设备的公钥来加密访问控制元件并且可添加唯一标识符或质疑。此外, 还可对加密的访问控制元件和唯一标识符或质疑的组合进行签名。在传输之后, 发送电子设备可删除其访问控制元件。随后, 接收电子设备可验证加密的访问控制元件和唯一标识符。如果这些有效, 则接收电子设备可存储加密的访问控制元件和唯一标识符以用于未来使用。

[0029] 在示例性配置中, 仅在符合标准可信关系的电子设备之间传输访问控制元件。因为电子设备两者均根据达成一致的协议进行操作, 所以访问控制元件可在其整个传输过程中保持唯一和受保护的。此外, 通过确保访问控制元件仅针对目标电子设备加密并且从当前电子设备中删除, 介入的恶意方不会破坏或击垮传输过程。

[0030] 在下文更具体地描述了用于传输访问控制元件的各个其他实施例。

[0031] 另外, 描述了用于实施策略的系统和技术。该策略可用于将不同的访问控制元件相关操作与逻辑实体的不同组凭证和/或当执行操作时使用的不同安全协议相关联。以此方式, 不同逻辑实体可具有与不同操作相关联的不同特权。

[0032] 示例性实施例的详细描述

[0033] 现在详细描述本公开的示例性实施例和各方面。尽管这些实施例和方面主要是在GSM、GPRS/EDGE或UMTS蜂窝网络的用户身份模块 (SIM) 的上下文中讨论的, 但是本公开中的通信技术可用于各种通信系统中, 该各种通信系统可得益于存储访问控制元件和将访问控制元件 (可包括电子SIM或eSIM) 分发到电子设备, 诸如基于以下标准的那些电子设备: 电气和电子工程师协会 (IEEE) 802.11标准、Bluetooth™ (来自Kirkland, Washington的蓝牙特别兴趣小组) 和/或另一种类型的无线接口, 诸如近场通信标准或规范 (来自Wakefield, Massachusetts的NFC论坛)。尽管在本讨论中使用了术语“用户身份模块” (例如eSIM), 但是

该术语并不必意味着或需要：用户本身使用（例如，本公开可由用户或非用户来实践）；由单个个体使用（例如，本公开可代表一组个体诸如家庭或无形或虚拟实体诸如公司、组织或企业来实践）；和/或任何有形“模块”设备或硬件。

[0034] 现有用户身份模块 (SIM) 操作

[0035] 在示例性UMTS蜂窝网络的上下文内，用户设备 (UE) 可包括便携式电子设备和通用用户身份模块 (USIM)。USIM可为由物理通用集成电路卡 (UICC) 存储和执行的逻辑软件实体。通常，各种信息诸如用户信息以及用于与网络运营商进行认证以便获得无线网络服务的密钥和技术存储在USIM上。在一个实施例中，USIM软件基于Java Card™编程语言。Java Card为已被修改以用于嵌入式“卡”类型设备（诸如UICC）的Java™编程语言的子集。其他具体实施可包括所谓的“本地”软件具体实施和/或专有的具体实施等。

[0036] 通常，在用户分发之前利用USIM对UICC进行编程。该预编程或“个性化处理”可特定于每个网络运营商。例如，在部署之前，USIM可与国际移动用户身份 (IMSI)、唯一集成电路卡标识符 (ICC-ID) 和专用认证密钥 (K) 相关联。网络运营商可将该关联存储在包含在网络认证中心 (AuC) 内的注册表中。在个性化处理之后，UICC可被分发到用户。

[0037] 图1呈现了使用USIM的现有认证和密钥协议 (AKA) 技术。在AKA技术的正常认证期间，UE可从USIM获取国际移动用户身份 (IMSI)。随后，UE可将IMSI传递给网络运营商或被访问的核心网的服务网络 (SN)。SN可将认证请求转发给本地网络 (HN) 的AuC。此外，HN可将所接收的IMSI与AuC的注册表进行比较并且可获得适当的K。接下来，HN可生成随机数 (RAND) 并且可使用某种技术借助K对其进行签名以生成期望的响应 (XRES)。此外，HN可生成用于加密和完整性保护的加密密钥 (CK) 和完整性密钥 (IK) 以及使用各种技术的认证令牌 (AUTN)。另外，HN可将可包括RAND、XRES、CK和AUTN的认证矢量发送到SN。SN可存储仅用于一次认证过程的认证矢量，并且SN可将RAND和AUTN传递到UE。

[0038] 在UE接收到RAND和AUTN之后，USIM可验证所接收的AUTN是否有效。如果有效，则UE可使用所接收的RAND利用所存储的K和生成XRES的相同技术来计算其自身响应 (RES)。此外，UE将RES传递回到SN。随后，SN可将XRES与所接收的RES进行比较，如果它们匹配，则SN可授权UE使用运营商的无线网络服务。

[0039] 前述AKA技术可在SIM卡的物理介质中实施。通常，SIM卡通常具有至少两个不同且期望的属性：它们以加密方式为SIM数据（例如，账户信息、加密密钥等）提供安全存储；以及它们不会容易被克隆。

[0040] 此外，SIM卡可包括形成在通用集成电路卡 (UICC) 中的处理器和存储器。该SIM卡可填充有环氧树脂以防止对UICC上的数据信号的外部探测。然而，如果需要，其他防篡改结构可包括在UICC中（例如，屏蔽层、掩膜层等）。另外，SIM卡可具有至处理器的安全接口，并且处理器可具有至存储器的内部接口。需注意，UICC可从外部设备接收电力，这使得处理器能够执行来自存储器部件的代码。存储器部件自身可能是无法直接访问的（例如，内部文件系统可能对用户是隐藏的）并且可经由处理器进行访问。

[0041] 在正常操作期间，处理器可接受有限数量的命令。这些命令中的每个命令可能仅仅在一定条件下是可访问的。此外，访问条件可受限于命令的执行以防止未授权的访问。此外，访问条件可以或者可以不是分级的，例如用于一个水平的认证不能自动授予用于另一个水平的认证。例如，一组访问条件可包括：始终可访问、永不可访问、可访问第一账户、可

访问第二主等。可仅仅在成功完成正确的安全协议之后授予有条件的访问。需注意,用于验证用户的身份的技术可包括:密码、个人识别号码(PIN)、共享秘密的质疑等。

[0042] 有条件的访问、有限的命令集和/或受保护的存储器空间可确保SIM卡内存储的信息在外部访问中是受保护的。克隆SIM卡可意味着物理卡的构建和内部文件系统和数据的构建。这些特征的组合可使得物理SIM卡大体上不受实际伪造尝试的影响。

[0043] 电子用户身份模块(eSIM)操作

[0044] 简言之,如本文所用,术语“保护”、“加以保护”和“受保护的”可指代明显不能倍增或缩减的元件(或者物理的或者虚拟的)。例如,在正常操作期间不能模仿或复制受保护的eSIM。

[0045] 另外,如本文所用,术语“唯一的”和“唯一”(如同应用于物理或虚拟元件)可指代作为具有特定属性和/或特性的唯一的一个元件的元件。例如,唯一的eSIM不能具有复制的eSIM。

[0046] 如本文所用,术语“安全性”通常指代对数据和/或软件的保护。例如,访问控制数据安全性可确保与访问控制元件相关联的数据和/或软件免受盗窃、滥用、损坏、出版和/或被未经授权的活动和/或恶意的第三方篡改。

[0047] 此外,如本文所用,术语“用户认证”通常指代指定用户对资源的访问。需注意,在现有物理SIM卡的情况下,用户认证可利用物理SIM卡拥有权得以加强。由此,物理SIM卡可代表访问物理资源的用户认证。例如,当物理SIM卡从一个蜂窝电话移动到另一个蜂窝电话时,假定该移动是由用户执行的(并且被用户隐式授权)。在eSIM操作的上下文内,可能需要类似的性能以用于eSIM传输的用户认证。具体地,eSIM的“所有者”(以及还有网络)可能需要保证eSIM仅被传输到合法的设备。

[0048] 一般来讲,可理解软件比硬件更灵活。例如,软件通常易于拷贝、修改和分发。此外,软件常常可被做成比硬件等价物更便宜、更有功率效率且体积更小。因此,尽管常规SIM操作使用物理形状因数诸如卡(UICC),但是当前发展领域专注于在软件内的虚拟化SIM操作。然而,SIM数据的敏感性质(例如,用户专用信息等)通常需要特殊考虑。例如,SIM数据的各个部分对用户来说是唯一的并且应当小心警惕恶意的第三方。此外,如前所指出的,每个SIM均代表约定对有限网络资源的访问量。因此,可管理对SIM的复制、破坏和/或回收以防止对网络资源的过度使用和/或未充分使用,以及服务提供商的费用或收入的代位。因此,虚拟化SIM应理想地满足以下属性:安全性、唯一性和保护性。此外,应理想地以至少与现有网络基础结构比拟的成本来负担这些属性。

[0049] 在一些实施例中,SIM操作将UICC模拟作为虚拟或电子实体,诸如在下文称为“电子通用集成电路卡”(eUICC)的软件应用程序。eUICC能够存储和管理一个或多个SIM元件,下文称为“电子用户身份模块”(eSIM)。然而,虚拟化eSIM操作的解决方案通常必须提供与已由现有UICC提供的现有安全性性能相当的(或更好的)安全性。另外,现有基础结构通常需要适当的技术以用于加强对虚拟化eSIM的保护,使得虚拟化eSIM的数量在整个网络中得到控制(例如,虚拟化eSIM不被复制、丢失等)。

[0050] 图2呈现了示出包括以下各项的系统200的框图:SIM供应商202的数量、SIM供应服务器(SPS)204的数量(诸如于2010年11月22日提交的标题为“Wireless Network Authentication Apparatus and Methods”的共同拥有且共同未决的美国专利申请12/

952,082以及于2010年11月22日提交的标题为“Apparatus and Methods for Provisioning Subscriber Identity Data in a Wireless Network”的美国专利申请12/952,089中详细描述的那些,两个专利申请的内容以引用方式并入本文)、以及用户设备(UE)206的总数,其中每个UE均包含安全的eUICC。以下讨论描述了用于将eSIM从SIM供应商分发到安全的eUICC的不同实施例。

[0051] 在一个实施例中,UE206中的一者请求来自任何SPS204的eSIM,并且SPS从可信实体诸如SIM供应商202(或在其他情况下为移动网络运营商(MNO)、可信服务管理器(TSM)等)获取适当的eSIM。在此方法中,SIM供应商可容易地控制eSIM的分发。例如,每个最新请求的eSIM可能仅由SIM供应商授予。然而,因为SIM供应商可能为可分配eSIM的唯一方,所以如果在短时间内大量用户的请求涌入SIM供应商,则SIM供应商会产生“瓶颈”(常见于成功的产品发布时)。类似地,SIM供应商可为单个故障点。因此,在灾难或其他故障的情况下,eSIM发布可能会完全停止。

[0052] 在另一实施例中,每个SPS204从SIM供应商202获取一批eSIM,并且将该批eSIM存储在每个SPS内(针对每个SPS复制该批eSIM)。随后,SPS根据请求将eSIM分发到UE206。需注意,eSIM可能仅由安全的eUICC解密和使用。这种分布式SPS服务器模型不会由SIM供应商产生瓶颈。然而,该方法通常大致需要更多的基础结构。具体地,SPS的总数可能需要确保不分发复制的eSIM。因此,无论何时SPS授予eSIM,其他SPS可能需要诸如经由通信链路208被通知对其复制的eSIM去激活。这可确保eSIM是唯一的(例如,未分发复制的eSIM)。保持SPS之间的eSIM状态信息同步的通信可为网络基础结构上的显著的通信量。此外,缓慢网络连接或网络分发可进一步引起“竞争条件”。在计算机联网的上下文内,竞争条件通常指的是源自网络实体同步中的传播延迟的数据冲突。例如,不完美的同步可使得两个SPS同时输出相同的eSIM(产生竞争条件)。这会造成eSIM被意外克隆。

[0053] 在另一个实施例(未示出)中,SPS204和SIM供应商202基础结构以相同方式组合。例如,SIM供应商和SPS网络可一起被封装在共同设施中并且彼此自由访问,或者可能以其他方式逻辑地交织在一起。交织设施的成功操作可能需要SIM供应商和SPS网络运营商之间的可信商业关系,这可能是不可取的(例如,其中由于法律上反垄断考虑等,企业关注冲突)。

[0054] 每个前述实施例可涉及在传输期间同步各个网络实体的显著通信开销。例如,当eSIM从SPS成功地传输到便携式电子设备时,每个SPS可被通知eSIM无法再次传输(以防止同一eSIM的多次输送)。

[0055] 需注意,这些实施例被公开为使用用户设备处的eUICC设备来接收和利用eSIM数据。然而,为了适应系统内的传统设备的使用,前述实施例可在系统中实现,其中eUICC功能被布置在传统的SIM形状因数或卡上(如将在下文详述的)。

[0056] 方法

[0057] 因此,本公开的各个方面有利地启用虚拟化访问控制元件操作和分发,其提供了与现有解决方案相当和/或改进的性能(例如,基于物理卡的访问控制元件)。在示例性实施例中,自包含SIM供应服务(SPS)实体可与其他对等SPS设备一起操作,从而实现用于SIM供应的分布式对等模型(相对于从集中化数据库跟踪eSIM的集中化模型,或需要对等设备之间的同步的分布式技术)。此外,如本文更详细所述的,本公开的实施例有利地不特定于任

何特定网络基础结构,并且可灵活地适应虚拟化的任何配置。

[0058] 在本公开的一个方面,访问控制元件一次可存储并仅传输到电子设备中的一个安全元件。在一些实施例中,安全元件仅存储从具有相同或可比拟的协议的其他安全元件接收的访问控制元件(随后在本文详细描述)。类似地,安全元件可限制将访问控制元件传输到具有相同或可比拟的协议的其他安全元件。例如,安全元件可限制与满足某些安全要求的其他安全元件的交易。一些MNO可对其设备实施比其他MNO更高的安全性。在各个实施例中,安全元件可被授予不同的水平,并且访问控制元件可能需要某一认证水平。在传输过程期间,设备可去除(或使得不活动)其自身访问控制元件。通过确保传输中涉及的两个客户端为可信实体并且履行相同协议,访问控制元件在传输期间不会被倍增或缩减。

[0059] 需注意,安全元件可实施为执行来自受保护的存储介质的软件的处理或处理装置。在一些实施例中,受保护的存储介质可被加密,以便排除未授权的访问或篡改。此外,安全元件可被物理硬化或保护以防止访问存储介质和/或安全处理器。物理硬化的实例可包括:准备好用于在未授权的访问尝试的事件中自毁或使得设备不可访问的物理外壳或另一机构,和/或用于防止外部探测的树脂或其他材料中的嵌入电路。

[0060] 在一些实施例中,本公开的安全元件进一步限制和/或监测/标记异常访问。例如,将访问控制元件传输或存储到安全元件可能需要质疑响应和/或唯一标识符。不恰当的质疑响应或不正确的标识符可指示异常/欺诈活动。类似地,可加密安全元件之间的交易。因此,不正确的加密交易还可标记可疑行为。

[0061] 图3呈现了用于存储和传输访问控制元件的方法300的流程图。在一些实施例中,方法300涉及作为嵌入在HSM内的eUICC装置的至少一个设备,HSM可管理一个或多个eSIM的存储装置。另选地或除此之外,HSM可本地存储加密的eSIM或者可加密eSIM以用于存储在远程介质上(在一些情况下,存储在安全文件系统中)。

[0062] 在一些实施例中,至少一个设备为嵌入在物理SIM卡形状因数(例如,实现传统形状因数插座再利用,如下文参考图7进一步所述的)内的eUICC装置。

[0063] 在一些实施例中,至少一个设备为硬化设备诸如包括嵌入在安全元件中的eUICC装置的蜂窝电话(例如,在不损坏或以其他方式折中设备的完整性的情况下无法从设备移除安全元件)。

[0064] 在方法300中,源设备和目标设备达成协议(操作302)。在一些实施例中,协议类型基于所识别的软件的版本,例如纯文本格式。在其他实施例中,协议类型为以其他方式加密的初始通信所固有的。例如,加密的256-位质疑可固有地指定特定协议或协议组,而未加密质疑可固有地指定不同的协议。在其他实施例中,协议基于发现过程。例如,设备可向目录服务注册,其中注册表包括信息,该信息诸如:标识符、网络地址、支持的协议类型等。

[0065] 在示例性实施例中,协议类型由互相信信的发布方管理机构颁发的签名(数字)证书来确定。该数字证书可包括:序号(用于唯一标识该证书)、认证的设备、用于生成签名的签名技术、验证信息并对证书进行签名的发布方、有效范围(例如,有效期起始日期、有效期截止日期等)、加密密钥、和/或拇指指纹或验证哈希值(以验证证书的合法性)。该数字证书在相关领域是熟知的并且在本文中不再进一步描述。

[0066] 在一些实施例中,相互信任的发布方管理机构为激活管理机构,例如,MNO认证中心(AuC)。在其他实施例中,相互信任的发布方管理机构为可信第三方,例如SIM供应商、设

备制造商等。相互信任的发布方管理机构可不需要对于两个设备是相同的。例如,系统可具有多个可信实体(例如,多个可接受的MNO、多个可信设备制造商等)。此外,在某些系统中,可信实体可为用于另一未知实体的可信根基(例如,可信实体提供未知实体也可信的保证)。此类信任“链”可延伸贯穿任何数目的中间设备。每个中间设备可链接到其前任的可信水平,其前任延伸到可信根基实体。

[0067] 在其他实例中,eUICC装置可支持符合标准化规范等的任何电器。类似地,为了确保向后兼容性,eUICC装置的未来变形也可支持传统eUICC装置等。

[0068] 可用设备和/或用于可用设备的可接受协议例如可被存储在查找目录或类似服务中。例如,多个装置阵列可与为每个装置提供连接信息的目录服务服务器相匹配。请求方(源或目标)可从目录服务请求信息。

[0069] 在一些实施例中,协议根据软件版本或修订版本加以拷贝。例如,设备可验证其他设备包括可接受软件版本或修订版本。另选地,源和目标设备可遵从非正式或初始协议。例如,设备可动态协商或确定协议。在其他实施例中,没有协议协商是必要的(例如,仅支持单次传输协议的系统)。

[0070] 传输协议可指定传输期间的质疑-响应协议的类型、唯一标识符选择、传输加密、访问控制元件管理(例如,删除过程、确认过程等)。如前所述,为了确保在传输期间保持对访问控制元件的保护和唯一性属性,访问控制元件可针对目标设备具体加密,并且可从传输设备删除。例如,传输协议可指定:如果需要接收确认,在传输失败、可接受数量的重试进行尝试时和/或在源设备可删除加密的访问控制元件的条件下是否允许重新传输。

[0071] 应当理解,源设备可在不同时间处和/或不同条件下删除和/或去激活加密的访问控制元件,正如可能是便利的或者在各种情景下所需要的。在一些实施例中,删除有时可发生在传输之后。此类实施例可用于大量传输,以便最小化不必要的信令(例如,在传输另一个访问控制元件之前删除每个访问控制元件)。另选地,访问控制元件有时可在传输之前被去激活。在其他实施例中,“有效窗口”还可被指定用于传输,使得特定传输必须在预定时间窗口内完成,以便被认为有效。

[0072] 其他考虑包括设备考虑和/或访问控制元件考虑。例如,一些设备可能仅允许接收(或传输)访问控制元件。在示例性实施例中,便携式电子设备限于仅接收eSIM(一旦被分配,无法被返回等)。另选地,某些设备可仅用于“一次”传输(例如,用于提供一次eSIM的一次性设备。在一些情况下,设备可比对等设备更(或更不)安全。例如,用户设备可具有比eUICC装置更严格的安全性要求。具体地,eUICC装置可经由其他手段(例如,安全基础结构等)加以保护。安全用户设备还可将eSIM传输到较不安全的eUICC装置,只要较不安全的eUICC装置实现与其中包含的敏感信息的保护相称的最小安全级别即可。类似地,在一些情况下,访问控制元件可具有传输限制,该传输限制包括:所允许的传输总数、目标设备限制等。

[0073] 此外,应当理解,通信技术可对传输协议考虑具有明显影响。网络基础结构传输可使用高带宽协议和介质(例如T3、T1、Sonet(同步光联网)、吉比特以太网或10G等),而基于消费者的传输可在较低带宽连接(例如,蜂窝访问、WLAN(无线局域网)、以太网等)上执行。不同使用场景还可具有用于握手、传输时间需求的不同需求。例如,SIM供应商可将大量eSIM传输到eUICC装置(例如,诸如用于有助于SIM递送或其他功能)。类似地,在另一实例

中,eSIM集中化的大的储存库可在大量eUICC装置间自由传输。eUICC装置可在装置间传输eSIM以有利于加载管理等。针对这些大量传输场景的握手需求可能不太重要,因为eSIM可能不在循环中(例如,确认可集中在传输的结束,而不是针对每个单独的eSIM)。

[0074] 消费者应用程序可具有低得多的传输速率,但是握手可能更重要,因为eSIM应当被稳健地递送并且可加以使用。在一些实施例中,未完成握手过程会自动触发重试尝试。例如,eUICC装置、SPS或类似实体可直接传输eSIM以服务来自UE的即兴eSIM请求、或从桌面或便携式计算机执行的应用程序。在另一实例中,基于消费者的应用程序可执行能存储一个或多个eSIM(例如,一个用于工作,一个用于个人使用,几个用于漫游接入等)的小型内在化装置,使得消费者能够在其各个设备之间传输eSIM。

[0075] 随后,源和目标设备建立共享秘密(操作304)。在示例性实施例中,设备通过检查数字签名来验证对等设备身份,并且如果签名有效,则交换(或同意交换)质疑、唯一标识符或用于由访问控制元件加密的另一安全令牌。

[0076] 例如,设备可利用质疑和响应型握手,其中任何可信设备了解可用于生成多个质疑和相关联的响应的共同秘密(例如,共同密钥、一组密钥等)。在一种配置中,设备可被允许信任未知设备,只要它们可生成正确的质疑和/或适当的响应即可。然而,应当理解,在给与此类信任之前可应用另外的准则。

[0077] 在另一实例中,设备可使用目标设备根据访问控制元件请求生成的唯一标识符。源设备可将唯一标识符与访问控制元件包括在一起来识别提供被服务的请求。

[0078] 在其他实施例中,设备利用可信第三方(例如,可信第三方可为每个设备提供会话密钥)验证其对等设备。此类关系可直接或间接得到验证。例如,对等设备可在执行传输之前直接查询可信第三方,或者另选地,每个设备可呈现由可信第三方签名的证书等。

[0079] 本领域技术人员将借助本公开认识到其他类型的加密布置和可信技术。

[0080] 此外,源设备将访问控制元件与秘密例如质疑、唯一标识符或另一安全令牌封装一起(操作306)。在示例性实施例中,可使用目标设备的公钥另外加密该封装。在一些实施例中,在重新加密访问控制元件之前,源设备利用其自身私钥来解密访问控制元件。

[0081] 在利用目标设备的公钥加密之后,只有目标设备可解密访问控制元件以进行使用。用于传输访问控制元件的公钥和私钥加密的一个实例在于2010年10月28日提交的标题为“Methods and Apparatus for Storage and Execution of Access-Control Elements”的美国临时专利申请61/407,866中所有描述,该专利申请的内容以引用方式并入本文。例如,每个eUICC装置可具有唯一设备公/私钥对和背书证书。公/私钥对可基于秘密私钥和公开的公钥。需注意,公/私钥技术被认为是“非对称的”,这是因为用于加密和解密的密钥是不同的;由此,加密者和解密者不共享相同的密钥。

[0082] 进一步确认,方法300的操作306和304(除了别的以外)可被进一步组合、细分和/或颠倒。例如,源设备可确定会话密钥并且可利用会话密钥来加密访问控制元件。所得的封装可进一步封装有目标设备的公钥。在一些实施例中,会话密钥在接收时由目标设备来确定。

[0083] 另外,在一些实施例中,使用(私有/公有签名对的)私有加密密钥来对该封装进行进一步数字签名以提供对源设备的进一步验证。目标设备可利用公有加密密钥检查数字签名来验证源自源设备的封装(例如,访问控制元件和唯一标识符等)。此外,应当理解,数字

签名仅仅是电子签名的子集。因此,可类似地采用其他形式的源验证,包括:用户专用标识(例如,密码、生物计量学、质疑问题/语句等)、电子标识(例如,数字证书、加密等)等。

[0084] 接下来,封装的访问控制元件从源被传输到目标设备(操作308)。目标设备可验证共享的秘密,并且如果验证成功,则可存储加密的访问控制元件以用于未来使用。在一些实施例中,在启用目标设备的访问控制元件之前(例如,在传输之前、在完成传输之前、在确认传输成功之前等),访问控制元件在源设备处被删除、去激活或以其他方式变得不可用。

[0085] 在另一实施例中,访问控制元件的下载安全性通过使用在于2012年2月14日提交的标题为“Methods and Apparatus for Large Scale Distribution of Electronic Access Clients”的共同拥有共同未决的美国临时专利申请61/598,819中公开的安全协议来保证,该专利申请的内容以引用方式并入本文。如本文所述,可使用分层的安全软件协议。在示例性具体实施中,服务器eUICC和客户端eUICC软件可包括所谓的软件层的“叠层”。每个软件层可负责与其相对应等软件层协商的一组分级功能。

[0086] 实例操作

[0087] 作为根据本公开的典型操作的实例,在初始化期间,SIM供应商为eUICC装置提供eSIM的集合或“批次”。需注意,多个SIM供应商可独立地提供eSIM。在SIM供应商的一方可能不存在所需协作(尽管如果需要也可使用此类协作)。SIM供应商可利用用于eUICC装置的质疑或唯一标识符来加密每一个eSIM。

[0088] 如前所述,每个eSIM可包括虚拟化SIM和唯一的密钥关联和性能以执行前述AKA技术以用于验证至蜂窝网络的便携式电子设备。另外,每个eSIM可唯一地与根据每次传输而变化的质疑或标识符相关联。质疑或标识符的典型具体实施可包括:加密材料、计数器、伪随机序列、大型状态机等。

[0089] 例如,第一eUICC装置可启动至第二eUICC装置的eSIM传输(其当前针对第一eUICC装置被加密)。第一eUICC装置可启动与第二eUICC装置的安全通信。在一些实施例中,第一eUICC装置和第二eUICC装置两者同意基于由一个或多个相互信任的第三方签名的证书的传输。此外,第二eUICC装置可提供对第一eUICC装置的唯一标识符。随后,第一eUICC装置可利用其自身的私钥对eSIM解密,并且随后利用第二eUICC的公钥对eSIM重新加密(该公钥可由第二eUICC自由分发)。唯一标识符和重新加密的eSIM的组合可由第一eUICC装置签名(该签名可验证第一eUICC装置的身份)。此外,经过签名的组合可被封装用于第二eUICC。现在,只有第二eUICC可解密eSIM并且经过签名的组合可证明加密的eSIM封装对应于该唯一标识符。另外,第一eUICC装置可将最新加密的eSIM传输到第二eUICC装置。

[0090] 在一些实施例中,使用唯一标识符来保护免受重放攻击。例如,每个eSIM传输可唯一识别,使得该交易无法被“拷贝”和回放(例如,通过恶意第三方)。具体地,当装置A和装置B之间传输eSIM并且随后从装置B传输到装置C时,在eSIM仍处于装置C处的情况下无法重放装置A到装置B之间的传输。

[0091] 类似地,考虑eSIM从第一eUICC装置到便携式电子设备的传输。便携式电子设备可利用质疑及其公钥发出对eSIM的请求。第一eUICC装置可利用其自身私钥对eSIM解码,并且可生成正确的质疑响应。随后,eSIM可利用便携式电子设备的公钥重新加密。该重新加密的eSIM可与质疑响应相结合并且随后进行签名。接下来,便携式电子设备可验证质疑响应(其可将第一eUICC装置识别为合法源)并且如果成功的话,可解密eSIM以用于使用。即使恶意

第三方可能拦截加密的eSIM,但是由于eSIM被加密所以不能使用或者篡改eSIM。

[0092] 最后,考虑eSIM从便携式电子设备到第二便携式电子设备的传输。第一便携式电子设备可推送请求来将其eSIM传输到第二便携式电子设备。在一些实施例中,第一便携式电子设备或第二便携式电子设备的使用者共同接受该传输。如果接受,第二便携式电子设备可向第一便携式电子设备传输质疑。随后,第一便携式电子设备可利用其自身私钥对其存储的加密的eSIM解密,并且可利用包括正确响应的第二便携式电子设备的公钥(可总可用)对eSIM重新加密。接下来,可对该组合进行签名并传输。此外,第二便携式电子设备可验证质疑响应(其可将第一便携式电子设备识别为合法源)并且可对eSIM解密以用于使用。

[0093] 访问控制元件的基于策略的管理

[0094] 传统访问控制技术通常使得具有正确凭证的逻辑实体能够执行与访问控制元件相关的各种操作。然而,可能理想地是为某些操作诸如从远程服务器加载eSIM提供更多安全性。例如,恶意逻辑实体可使得虚拟SIM包含恶意代码或可允许加载恶意数据。另选地,其他操作(诸如允许用户启用已加载到eUICC中的eSIM)可包含较小安全风险并且因此可能不需要麻烦的安全措施诸如数字证书。相反,这些操作可使用更简单并且较少限制的安全手段,诸如PIN代码,或者没有专门的安全性,就像移除/插入传统UICC的情况那样。

[0095] 另外,在现有eUICC设计中,具有正确凭证的逻辑实体能够管理eSIM相关的操作,诸如加载eSIM或启用eSIM。然而,为了支持不同的商业模式,可能理想的是不同的逻辑实体能够管理不同的操作(即,不同逻辑实体可针对与访问控制元件诸如eSIM相关联的该一组操作具有不同特权)。需注意,不同逻辑实体可包括:用户、移动网络运营商雇用的安全服务承包商、移动网络运营商、设备制造商和/或可信OEM供应商。这些逻辑实体可利用UE内部(诸如便携式电子设备)和/或UE外部的硬件和/或软件管理不同操作。

[0096] 基于策略的框架可用于将每个eSIM相关操作与不同逻辑实体(即,可指定逻辑实体的特权)、不同组凭证和/或执行操作所要求的不同协议相关联。在eUICC中,存在与管理eSIM相关的多个基本操作,包括:eSIM加载、eSIM启用、eSIM禁用、eSIM删除和eSIM输出(可被认为以相反方向加载,或另选地可位于具有物理链路的两个eUICC之间)。该基于策略的框架可允许不同逻辑实体(具有其相关联的凭证)执行不同操作,并且还可允许将不同安全协议与不同操作或不同逻辑实体相关联。例如,为了从远程位置下载安全数据(诸如eSIM),基于策略的框架可提供强大安全性,这可设计要求在设备和远程服务器之间的相互认证。另一方面,理想的是允许用户容易执行操作来在设备上交换eSIM而无需强大安全性。例如,基于策略的框架可要求用户在交换eSIM之前仅输入PIN代码。由此,在一些实施例中,与输出或加载eSIM相关的操作可以是安全的,而与启用或禁用eSIM相关的操作可能是较不安全的。

[0097] 需注意,其他信息检索操作或UICC水平操作可得到基于策略的框架的支持。例如,基于策略的框架可支持安全策略以用于更新基于策略的框架。该基于策略的框架更新操作可要求更强大的认证(例如,仅允许设备制造商这样做)。

[0098] 在一些实施例中,安全性框架基于公钥基础结构(PKI)。例如,如果远程服务器想要执行eSIM相关操作,则基于策略的框架可要求远程服务器与有效的PKI数字证书相关联以能够执行eSIM相关操作。另选地,具有PIN代码的简单用户提示可满足本地用户的需要。(需注意,尽管PKI是有利的,但是可能不需要,并且可使用其他类型的加密,诸如对称密

钥)。

[0099] 图4呈现了示出用于针对与访问控制元件(诸如eSIM)相关联的一组操作作为逻辑实体指定一组特权的方法400的流程图,该方法可由电子设备中的处理器(诸如电子设备中的安全元件中的处理器)执行。在该方法期间,从逻辑实体和第二逻辑实体接收(操作402)凭证。需注意,逻辑实体和第二逻辑实体可位于电子设备内部和/或外部。例如,逻辑实体可包括在电子设备中和/或可经由网络远程访问电子设备。

[0100] 随后,基于凭证和凭证管理模块来确定(操作404)与针对逻辑实体和第二逻辑实体的一组操作相关联的一组特权。例如,该一组操作可包括:加载访问控制元件、启用访问控制元件、禁用访问控制元件、输出访问控制元件和/或删除访问控制元件。具体地,该一组操作可与识别服务的使用者并有助于安全通信的安全元件中的访问控制元件相关联,并且该一组特权中的给定的特权可指定是否允许逻辑实体和/或第二逻辑实体进行或执行该一组操作中的给定的操作。需注意,对于操作中的一次操作,逻辑实体和第二逻辑实体具有不同特权。在一些实施例中,使用处理器执行安全元件上的程序模块以提供信息。

[0101] 接下来,将指定逻辑实体和第二逻辑实体的该一组特权的信息提供(操作406)给安全元件的操作系统。这允许安全元件实施该一组特权。因此,可在平台或操作系统水平上执行特权的实施以确定可允许哪些访问控制元件操作。通常,策略可限定在eUICC水平(访问控制元件外)或访问控制元件中,但是策略的实施可处于eUICC操作系统水平(例如,在凭证管理模块中)。

[0102] 需注意,基于特权设置,一个或多个逻辑实体(诸如逻辑实体和第二逻辑实体)可被配置为授权以对访问控制元件执行给定的操作。这些逻辑实体是否同时操作取决于使用情况。例如,可同时从两个授权的服务器加载两种不同配置文件。然而,不希望两个不同逻辑实体同时启用/禁用一个或多个访问控制元件。

[0103] 除了支持不同计算平台上的不同安全域(其中不同机器具有不同安全域并且不同实体可在不同机器上的不同安全域中被授权)之外,作为替代的解决方案,基于策略的框架可在单一计算平台上操作。该基于策略的框架可取决于策略而非域操作来确定哪些逻辑实体被授权执行不同操作。

[0104] 如下文参考图6和7进一步所述的,上述基于策略的框架可在操作在设备内部的任何嵌入式UICC平台上执行,诸如嵌入在蜂窝电话中的UICC平台或另一计算平台。此外,基于策略的框架可在设备内的安全元件上实现,诸如焊接到设备中的嵌入式UICC卡。

[0105] 具体地,UICC卡可具有其自身软件,并且还可提供用于eSIM(并且更具体地,访问控制元件)的存储装置,该软件可运行并实施逻辑实体的指定特权和凭证数据库(数字证书、密码和/或PIN代码)的策略。例如,如下文参考图6和图7进一步所述的,UICC卡上的安全元件可包括实现基于策略的框架的凭证管理模块。另外,凭证管理模块可包括与该一组操作相关联的对称加密密钥,并且给定的加密密钥可有助于与该一组操作中的至少给定的操作相关联的特权。另选地或除此之外,凭证管理模块可包括证书和与该一组操作相关联的非对称加密密钥以有助于非对称加密,并且给定的加密密钥和给定的证书可有助于与该一组操作中的至少给定的操作相关联的特权。

[0106] 此外,UICC卡可经由标准化接口与设备(诸如智能电话)进行交互。在操作期间,设备可经由GUI接收输入并且可经由该接口向UICC卡发出命令。此外,远程处理器首先可连接

到设备并且然后可通过该设备建立服务器与嵌入式UICC之间的安全通道。

[0107] 在方法300 (图3) 和方法400 (图4) 的一些实施例中,可能存在另外的或较少的操作。例如,方法400中的访问控制元件可包括为逻辑实体和第二逻辑实体中的至少一者指定第二组特权的信息。在与该一组特权相关联的安全级别和与第二组特权相关联的第二安全级别之间出现冲突的情况下,安全元件可将安全级别和第二安全级别进行比较并且可选择该一组特权和第二组特权中的与较强安全性相关联的一者。另选地,在与该一组特权相关联的安全级别和与第二组特权相关联的第二安全级别之间出现冲突的情况下,安全元件可选择该一组特权。此外,如下文参考图6和图7进一步所述的,如果该特权至少部分地由访问控制元件限定,则在冲突或碰撞的情况下,可执行冲突解决方案。该冲突解决方案可包括选择与由凭证管理模块和访问控制元件所确定的不同特权相关联的较严格安全级别和/或默认为由凭证管理模块所确定的特权。然而,在一些实施例中,安全元件将管理权传递给访问控制元件,使得由访问控制元件所指定的特权和/或安全级别是默认的。此外,可改变操作的次序、和/或两个或更多个操作可组合成单个操作。

[0108] 在示例性实施例中,凭证管理模块可基于其凭证和一个或多个查找表来确定逻辑实体的授权。例如,逻辑机构可向凭证管理模块提供凭证。作为响应,凭证管理模块可使用查找表中的一个查找表来针对与至少一个访问控制元件相关联的特定操作确定逻辑实体的特权。这可允许逻辑实体执行与至少一个访问控制元件(例如,eSIM) 相关联的至少一个操作,诸如:将访问控制元件加载到电子设备上、启用电子设备上的访问控制元件、禁用电子设备上的访问控制元件、输出电子设备上的访问控制元件、和/或删除电子设备上的访问控制元件。在示例性实施例中,可允许UICC装置加载访问控制元件并且输出访问控制元件,可允许电子设备启用访问控制元件,可允许网络运营商禁用访问控制元件,并且可允许电子设备删除访问控制元件。

[0109] 凭证管理模块还可基于逻辑实体的凭证允许不同逻辑实体针对与不同访问控制元件相关联的不同操作具有不同的特权。因此,可允许一个逻辑实体执行与一个访问控制元件相关联的操作,但是不允许执行与另一个访问控制元件相关联的操作(或另一操作)。类似地,另一逻辑实体可针对与这些或其他访问控制元件相关联的这些或其他操作具有不同特权。

[0110] 此外,代表不同逻辑实体的凭证类型可针对不同逻辑实体、(与一个或多个访问控制元件相关联的) 不同操作和/或不同访问控制元件而不同。例如,PKI/RSA认证可用于某些操作和/或访问控制元件,而PIN代码可用于其他操作和/或访问控制元件。

[0111] 此外,由凭证管理模块所指定的特权可指示当针对与一个或多个访问控制元件相关联的不同操作和/或不同访问控制元件呈现凭证/验证逻辑实体时使用不同安全级别。例如,当呈现凭证时可使用对称加密法,该凭证认证逻辑实体以确定执行与访问控制元件相关联的特定操作的特权。然而,不同的安全协议可指定用于与访问控制元件相关联的了另一操作(诸如非对称加密法)。

[0112] 由此,凭证管理模块可指定确定针对不操作、不同访问控制元件和/或不同逻辑实体的特权、凭证和/或安全协议/水平的策略。需注意,由凭证管理模块所指定的策略可影响多个访问控制元件。然而,在一些实施例中,访问控制元件可为自身指定策略,即,策略可能仅影响针对与该特定访问控制元件相关联的操作相关的逻辑实体的特权。

[0113] 在其中存在由凭证管理模块所指定的安全元件中的全局策略和/或针对由访问控制元件所指定的特定访问控制元件的局部策略(有时称为“配置文件策略”)的实施例中,可能发生冲突。在发生冲突的情况下,例如全局策略可:指定使用基于RSA的共同认证来加载eSIM;当激活eSIM时将策略默认委托给那些配置文件策略;指定电子设备可去激活eSIM;指定使用基于RSA的相互认证来输出eSIM;以及当删除eSIM时将策略默认委托给那些配置文件策略。继而,eSIM配置文件策略可:不能进入与加载eSIM相关的特权;指定使用具有特定L3服务通称的基于RSA的相互认证来激活eSIM;不能进入与去激活eSIM相关的特权;指定使用具有特定L3服务通称的基于RSA的相互认证来输出eSIM;以及指定使用具有特定L3服务通称的基于RSA的相互认证来删除eSIM。通常,凭证管理模块可在全局和局部策略之间发生冲突的情况下处于默认状态。然而,凭证管理模块可委托给管理机构以指定针对特定操作的配置文件策略(在eSIM中所限定的)的特权。

[0114] 另选地,凭证管理模块可在发生冲突(或不同)情况下针对特定操作将全局和局部特权进行比较,并且可使用更严格的安全级别。例如,如果用于加载eSIM的全局策略使用基于RSA的相互认证来激活eSIM并且局部策略使用具有特定L3服务通称的基于RSA的相互认证来激活eSIM,则凭证管理模块可使用具有特定L3服务通称的基于RSA的相互认证。

[0115] 需注意,可远程修改凭证管理模块所指定的凭证/特权。例如,凭证管理模块可包括具有被授权的逻辑实体的第一列表和可修改第一列表的逻辑实体的第二列表的查找表。

[0116] 在先前实施例中的电子设备中的逻辑实体和安全元件(以及具体地,具有凭证管理模块)之间的通信可使用在本公开之前所述的通信技术和安全协议。

[0117] 装置

[0118] 现在详细描述用于与上述技术结合的装置的各个示例性实施例。

[0119] eUICC装置

[0120] 图5呈现了示出了eUICC装置500的框图。该eUICC装置可为独立实体,或者可与其他网络实体(例如,SPS等)结合。如图5所示,eUICC装置500通常包括处理子系统504、存储器子系统506和与通信网络进行交互的联网子系统502。处理子系统504可包括被配置为执行计算操作的一个或多个设备。例如,处理子系统504可包括一个或多个微处理器、专用集成电路(ASIC)、微控制器、可编程逻辑器件和/或一个或多个数字信号处理器(DSP)。

[0121] 此外,存储器子系统506可包括用于存储用于处理子系统504和/或网络接口502的数据和/或指令的一个或多个设备。例如,存储器子系统506可包括动态随机存取存储器(DRAM)、静态随机存取存储器(SRAM)和/或其他类型的存储器。在一些实施例中,用于存储器子系统506中的处理子系统504的指令包括:一个或多个程序模块或指令集,其可由处理子系统504执行。需注意,这一个或多个计算机程序可构成计算机程序机制。此外,存储器子系统506中的各种模块中的指令可在以下各项中实现:高级程序语言、面向对象的编程语言、和/或汇编或机器语言。此外,编程语言可被编译或解释,例如,可配置或被配置为(在该讨论中可互换使用)将由处理子系统504执行。

[0122] 此外,存储器子系统506可包括用于控制对存储器的存取的机构。在一些实施例中,存储器子系统506包括存储器分级结构,该存储器分级结构包括耦接至eUICC装置500中的存储器的一个或多个高速缓存。在这些实施例中的一些实施例中,高速缓存中的一个或多个高速缓存位于处理子系统504中。

[0123] 在一些实施例中,存储子系统506耦接至一个或多个大容量海量存储设备(未示出)。例如,存储子系统506可耦接至磁盘驱动器或光盘驱动器、固态驱动器、或另一类型的海量存储设备。在这些实施例中,存储子系统506可由eUICC装置500用作常用数据的快速存取存储装置,而海量存储设备用于存储不常使用的数据。

[0124] 联网子系统502包括被配置为耦接至有线和/或无线网络并在有线和/或无线网络(即,执行网络操作)上进行传送的一个或多个设备,包括接口电路(诸如近场通信电路)和天线。例如,网络子系统502可包括Bluetooth™联网系统、蜂窝联网系统(例如,5G/4G网络,诸如UMTS、LTE等)、通用串行总线(USB)联网系统、基于在IEEE 802.11(例如,Wi-Fi联网系统)所述的标准的联网系统、以太网联网系统和/或另一通信系统(诸如,近场通信系统)。

[0125] 此外,联网子系统502包括处理器、控制器、无线电部件/天线、插座/插头、和/或用于耦接至每个所支持的联网或通信系统、在每个所支持的联网或通信系统上进行传送并处理用于每个所支持的联网或通信系统的数据和事件的其他设备。需注意,用于针对每个网络系统用于耦接至网络、在网络上进行传送并处理网络上的数据和事件的机构有时统称为网络系统的“网络接口”。此外,在一些实施例中,eUICC装置或设备之间的“网络”还不存在。因此,eUICC装置500可使用联网子系统502中的机构以用于执行eUICC装置或设备之间的简单无线通信。在一些实施例中,联网子系统502与MNO基础结构通信,以便提供对其他eUICC装置的访问或对一个或多个便携式电子设备的直接或间接访问,虽然可替换其他配置和功能。

[0126] 在一种配置中,eUICC装置500为HSM。HSM可包括用于管理多个访问控制元件的一个或多个安全元件。在一些实施例中,访问控制元件被直接存储在HSM处。另选地,访问控制元件可被加密并存储在外部存储装置中。在此类外部(例如,远程)存储装置实施例中,加密可确保访问控制元件是安全的,即使在存储在物理上不安全的介质上时也是如此。

[0127] HSM可实现访问控制元件向和从另一HSM的传输,同时保留对访问控制元件的唯一性和保护。此外,在该实施例中访问控制元件向另一HSM之间的传输可使得去激活和/或删除本地存储的访问控制元件。如果HSM被篡改或者如果其完整性以其他方式受到破坏还可以自销毁或者自身禁用。

[0128] 在图5中,eUICC装置500包括在处理子系统504中运行的至少一个数据库508。尽管如在eUICC装置500上运行的单个应用程序所示的,应当理解,前述数据库功能可包括在彼此通信的多个设备上运行的分布式应用程序。

[0129] 数据库508的示例性具体实施可处理请求,该请求可包括:对存储访问控制元件(诸如eSIM)的请求和对传输当前存储的eSIM的请求。数据库508还可负责验证对确保从被授权作出此类请求的实体接收通信的请求(诸如在图3的方法300中的操作304期间)。

[0130] 在一些实施例中,数据库508被配置为执行质疑和响应(或质疑-响应)安全协议。质疑-响应安全协议可基于质疑和/或响应的恰当生成来验证未知第三方作出的请求。另选地,安全元件可验证由可信管理机构签名的数字证书。

[0131] 如图5所示,存储子系统506可适用于存储访问控制元件阵列。在一些实施例中,eUICC装置存储访问控制元件诸如eSIM的阵列。每个eSIM可包括小文件系统,该小文件系统包括计算机可读指令(诸如eSIM程序)和相关联的数据(例如,加密密钥、完整性密钥等)。另外,每个eSIM可另外利用eUICC装置的公钥进行加密。因此,每个eUICC只能由eUICC装置500

进行解密。在一些实施例中，每个加密的eSIM进一步由唯一标识符、质疑和/或质疑响应进行加密。加密的部件可进一步存储作为二进制大对象 (BLOB)。

[0132] 数据库508应用程序可管理可用的eSIM。如图5所示，数据库508可提供与特定eSIM BLOB、被授权使用eSIM的设备、当前状态和/或eSIM的当前状态（例如，“可用”、“不可用”、“陈旧的”等）相关的信息。也可维持另外的信息。此外，数据库508应用程序可更新或改变存储在数据库中的信息。

[0133] 当另一设备从eUICC装置500请求eSIM时，数据库508应用程序可检索所请求的eSIM当前状态。该信息可用于确定是否可提供所请求的eSIM。该有效性检查可在激活服务处、在eUICC装置500处执行，共享/分发，或发生在其他位置（例如，通过比较激活服务处的状态和eUICC装置500处的最后已知的状态）。类似地，当另外的设备将eSIM传输到eUICC装置500时，数据库508应用程序可更新所传输的eSIM的当前状态。

[0134] 在eUICC装置500中，处理子系统504、存储器子系统506、联网子系统502和数据库508可使用一个或多个互连结构诸如总线耦接在一起。这些互连结构可包括子系统或部件可用于在彼此中间传送命令和数据的电、光和/或光电连接件。需注意，不同实施例可在子系统或部件中包括不同数量或配置的电、光和/或光电连接件。

[0135] 尽管使用特定部件来描述eUICC装置500，但在另选的实施例中，不同的部件和/或子系统可存在于eUICC装置500中。例如，eUICC装置500可包括一个或多个另外的处理子系统、存储器子系统、联网子系统和/或数据库。另外，子系统或部件中的一者或多者可不存在于eUICC装置500中。此外，在一些实施例中，eUICC装置500可包括图5中未示出的一个或多个另外的子系统或部件。同样，尽管在图5中示出了独立的子系统或部件，但是在一些实施例中，给定的子系统或部件中的一些或全部可被集成到eUICC装置500中的其他子系统或部件中的一者或多者。

[0136] 此外，eUICC装置500中的电路和部件可使用模拟和/或数字电路的任何组合来实现，包括：双极性、PMOS和/或NMOS门或晶体管。此外，这些实施例中的信号可包括具有大致离散值的数字信号和/或具有连续值的模拟信号。此外，部件和电路可为单端型或差分型并且电源可为单极性或双极性。

[0137] 电子设备

[0138] 图6呈现了电子设备600（例如，UE）的框图。该电子设备包括处理子系统602、存储器子系统604、联网子系统606、用户接口子系统608和安全元件610。处理子系统602包括被配置为执行计算操作的一个或多个设备。例如，处理子系统602可包括一个或多个微处理器、专用集成电路（ASIC）、微控制器、可编程逻辑器件、现场可编程门阵列和/或一个或多个数字信号处理器（DSP）。

[0139] 此外，存储器子系统604可包括用于存储数据和/或指令的一个或多个设备，所述数据和/或指令用于处理子系统602和/或联网子系统606。例如，存储器子系统604可包括动态随机存取存储器（DRAM）、静态随机存取存储器（SRAM）和/或其他类型的存储器（诸如闪速存储器或SDRAM）。在一些实施例中，用于存储器子系统604中的处理子系统602的指令包括：一个或多个程序模块或指令集，其可由处理子系统602来执行。需注意，这一个或多个计算机程序可构成计算机程序机制。此外，存储器子系统604中的各种模块中的指令可在以下各项中实现：高级程序语言、面向对象的编程语言、和/或汇编或机器语言。此外，编程语言可

被编译或解释,例如可配置或被配置(其可在该讨论中互换使用)为将由处理子系统602来执行。

[0140] 此外,存储器子系统604可包括用于控制对存储器的存取的机构。在一些实施例中,存储器子系统604包括存储器分级结构,该存储器分级结构包括耦接至电子设备600中的存储器的一个或多个高速缓存。在这些实施例中的一些实施例中,所述高速缓存中的一个或多个高速缓存位于处理子系统602中。

[0141] 在一些实施例中,存储器子系统604耦接至一个或多个大容量海量存储设备(未示出)。例如,存储器子系统604可耦接至磁盘驱动器或光盘驱动器、固态驱动器、或另一类型的海量存储设备。在这些实施例中,存储器子系统604可被电子设备600用于经常使用的数据的快速存取存储装置,而海量存储设备被用于存储使用频率较低的数据。

[0142] 联网子系统606包括被配置成耦接至有线和/或无线网络并在有线和/或无线网络(即,执行网络操作)上进行传送的一个或多个设备,包括接口电路(诸如近场通信电路)和天线。例如,联网子系统606可包括Bluetooth™联网系统、蜂窝联网系统(例如,5G/4G网络诸如UMTS、GSM、CDMA、LTE/LTE-A等)、通用串行总线(USB)联网系统、基于IEEE 802.11(例如,Wi-Fi联网系统)中所述的标准的联网系统、以太网联网系统和/或另一通信系统(诸如近场通信系统)。

[0143] 此外,联网子系统606包括处理器、控制器、无线电部件/天线、插座/插头、和/或用于耦接至每个所支持的联网或通信系统、在每个所支持的联网或通信系统上进行传送并处理用于每个所支持的联网或通信系统的数据和事件的其他设备。需注意,用于针对每个网络系统用于耦接至网络、在网络上进行传送并处理网络上的数据和事件的机构有时统称为网络系统的“网络接口”。此外,在一些实施例中,一个或多个eUICC装置和电子设备600之间的“网络”还不存在。因此,电子设备600可使用网络接口中的机构用于在eUICC装置和电子设备600之间执行简单无线通信。

[0144] 用户接口子系统608包括任何数量的熟知的I/O设备,包括:键盘、触摸屏(例如,多触摸界面)、LCD显示器、背光源、扬声器和/或麦克风。然而,已经认识到,在某些应用程序中可去除这些部件中的一个或多个部件。例如,PCMCIA卡型客户端实施例可缺少用户接口(因为它们可能背负到它们物理和/或电气耦接的主机设备的用户接口上)。

[0145] 安全元件610可包含和操作eUICC应用程序。该安全元件能够存储和访问多个访问控制元件612以用于与网络运营商的认证。在该实施例中,安全元件610包括执行存储在安全介质中的软件的安全处理器。安全介质对于所有其他部件(除了安全处理器之外)可为不可访问的。此外,安全元件610可进一步硬化以防止篡改(例如,被封入树脂),并且可采用加密以用于保护其内容,如前所述。尽管使用eUICC作为安全元件610的示例证,但是也可使用其他具体实施,包括:(电子设备600中的电路板上的)嵌入式安全元件、智能安全数字(SD)卡、智能微SD卡等。需注意,安全元件610可包括在安全元件610的环境中(诸如,安全元件610的操作系统中和/或在安全元件610上执行的Java运行环境中)执行的一个或多个小程序或应用程序。

[0146] 此外,安全元件610能够接收和存储一个或多个访问控制元件612。在一些实施例中,安全元件610存储与用户相关联的eSIM阵列或多个eSIM(例如,一个用于工作,一个用于个人,几个用于漫游访问等),和/或根据另一逻辑技术或关系(例如,一个用于家庭或商业

实体的多个成员中的每个成员,一个用于家庭成员的个人和工作使用的每次使用等)。每个eSIM可包括小文件系统,该小文件系统包括计算机可读指令(诸如,eSIM程序)和相关联的数据(例如,加密密钥、完整性密钥等)。

[0147] 此外,安全元件610能够在eSIM和电子设备600之间传输。在示例性实施例中,电子设备600提供基于GUI确认以启动eSIM的传输。

[0148] 示例性实施例的各种实现可包括在被执行时启动质疑-响应安全协议的指令。质疑-响应安全协议可基于质疑和/或响应的恰当生成来验证未知第三方作出的请求。另选地,在示例性实施例中,安全元件610可验证由可信管理机构签名的数字证书。

[0149] 在一些实施例中,安全元件610保持所存储的访问控制元件612的列表或详单。该详单可包括有关所存储的访问控制元件612的当前状态的信息。此外,该信息可包括:可用性、完整性、有效性和/或先前经历的误差。详单可进一步链接或结合至用户接口子系统608,以便使得用户能够选择可用的访问控制元件。

[0150] 在示例性实施例中,安全元件610具有相关联的设备加密密钥。可使用这些设备密钥来保护访问控制元件612的交换。在一些实施例中,加密密钥为非对称公/私钥对。可自由分发公钥而不会折中私钥的完整性。例如,设备可被分配(或内部生成)RSA公/私钥。主要,公钥可用于部署后通信。

[0151] 在一些实施例中,安全元件610包括凭证管理模块614,该凭证管理模块为与该一组操作中的操作相关联的逻辑实体指定具有一组特权的配置文件(对应于基于策略的框架),该操作与访问控制元件612中的一个或多个访问控制元件相关联。此外,对于操作中的一些操作,逻辑实体中的一些逻辑实体具有不同特权。在一些实施例中,凭证管理模块614包括安全元件610中的程序模块用于指定该一组特权的信息。

[0152] 此外,访问控制元件612中的至少一个访问控制元件可包括为至少一个逻辑实体指定第二组特权的信息。在与由凭证管理模块614所指定的该一组特权相关联的安全级别和与第二组特权相关联的第二安全级别之间发生冲突的情况下,安全元件610可将安全级别和第二安全级别进行比较并且可选择该一组特权和第二组特权中的与较高安全性相关联的一者。另选地,在与该一组特权相关联的安全级别和与第二组特权相关联的第二安全级别之间发生冲突的情况下,安全元件610可选择该一组特权。

[0153] 在一些实施例中,凭证管理模块614包括与该一组操作相关联的对称加密密钥,并且给定的加密密钥有助于与该一组操作中的至少给定的操作相关联的特权。另选地或除此之外,凭证管理模块614可包括证书和与该一组操作相关联的非对称加密密钥以有助于非对称加密,并且给定的加密密钥和给定的证书可有助于与该一组操作中的至少给定的操作相关联的特权。

[0154] 在电子设备600中,处理子系统602、存储器子系统604、联网子系统606、用户接口子系统608和安全元件610可使用一个或多个互连结构诸如总线耦接在一起。这些互连结构可包括子系统或部件可用于在彼此之间传送命令和数据的电、光和/或光电连接件。需注意,不同实施例可包括子系统或部件之间的不同数量或配置的电、光和/或光电连接件。

[0155] 电子设备600可为(或可被包括在)具有至少一个网络接口的任何电子设备。例如,电子设备600可为(或可被包括在):台式计算机、膝上型计算机、服务器、媒体播放器(诸如MP5播放器)、装置、小型笔记本计算机/上网本、平板电脑、智能电话、蜂窝电话、一组测试设

备、“智能电表”、网络装置、机顶盒、个人数字助理(PDA)、玩具、控制器、数字信号处理器、游戏机、装置内的计算引擎、消费电子设备、便携式计算设备、个人备忘记事本和/或另一电子设备。

[0156] 虽然使用了特定部件来描述电子设备600,但在另选的实施例中,不同的部件和/或子系统可存在于电子设备600中。例如,电子设备600可包括一个或多个另外的处理子系统、存储器子系统、联网子系统、用户接口和/或安全元件。另外,子系统或部件中的一者或更多者可能不存在于电子设备600中。此外,在一些实施例中,电子设备600可包括未在图6中示出的一个或多个另外的子系统或部件。同样,尽管图6示出了独立的子系统或部件,但是在一些实施例中,给定的子系统或部件的一些或所有可被集成到电子设备600中的其他子系统或部件中的一者或更多者。

[0157] 此外,电子设备600中的电路和部件可使用模拟和/或数字电路的任一组合来实现,包括:双极性、PMOS和/或NMOS门或晶体管。此外,这些实施例中的信号可包括具有大致离散值的数字信号和/或具有连续值的模拟信号。此外,部件和电路可为单端型或差分型并且电源可为单极性或双极性。

[0158] 用于传统固定操作的装置

[0159] 图7呈现了电子设备700(例如,UE)的框图。电子设备包括处理子系统702、存储器子系统704、联网子系统706、用户接口子系统708和插座710。处理子系统702包括被配置为执行计算操作的一个或多个设备。例如,处理子系统702可包括一个或多个微处理器、专用集成电路(ASIC)、微控制器、可编程逻辑器件、现场可编程门阵列和/或一个或多个数字信号处理器(DSP)。

[0160] 此外,存储器子系统704可包括用于存储用于处理子系统702和/或联网子系统706的数据和/或指令的一个或多个设备。例如,存储器子系统704可包括动态随机存取存储器(DRAM)、静态随机存取存储器(SRAM)和/或其他类型的存储器(诸如闪速存储器或SDRAM)。在一些实施例中,用于存储器子系统704中的处理子系统702的指令包括:可由处理子系统702执行的一个或多个程序模块或指令集。需注意,这一个或多个计算机程序可构成计算机程序机制。此外,存储器子系统704中的各种模块中的指令可在以下各项中实现:高级程序语言、面向对象的编程语言、和/或汇编或机器语言。此外,编程语言可被编译或解释,例如可配置或被配置为(在该讨论中可互换使用)将由处理子系统702执行。

[0161] 此外,存储器子系统704可包括用于控制对存储器的存取的机构。在一些实施例中,存储器子系统704包括存储器分级结构,该存储器分级结构包括耦接至电子设备700的存储器的一个或多个高速缓存。在这些实施例的一些实施例中,所述高速缓存中的一个或多个高速缓存位于处理子系统702中。需注意,可经由存储器子系统704处的DMA硬件促进对存储器子系统704中的存储器的存取。

[0162] 在一些实施例中,存储器子系统704耦接至一个或多个高容量海量存储设备(未示出)。例如,存储器子系统704可耦接至磁盘驱动器或光盘驱动器、固态驱动器、或另一类型的海量存储设备。在这些实施例中,存储器子系统704可被电子设备700用于经常使用的数据的快速存取存储装置,而海量存储设备被用于存储使用频率较低的数据。

[0163] 联网子系统706包括被配置为耦接至有线和/或无线网络并在有线和/或无线网络(即,执行网络操作)上进行传送的一个或多个设备,包括接口电路(诸如近场通信电路)和

天线。例如,联网子系统706可包括Bluetooth™联网系统、蜂窝联网系统(例如,5G/4G网络,诸如UMTS、GSM、CDMA、LTE/LTE-A等)、通信串行总线(USB)联网系统、基于在IEEE 802.11(例如,Wi-Fi联网系统)所述的标准的联网系统、以太网联网系统和/或另一通信系统(诸如,近场通信系统)。

[0164] 此外,联网子系统706包括处理器、控制器、无线电部件/天线、插座/插头、和/或用于耦接至每个支持的联网或通信系统、在每个支持的联网或通信系统上进行传送并处理用于每个支持的联网或通信系统的数据和事件的其他设备。需注意,用于针对每个网络系统用于耦接至网络、在网络上进行传送并处理网络上的数据和事件的机构有时统称为用于网络系统的“网络接口”。此外,在一些实施例中,一个或多个UICC装置与电子设备700之间的“网络”还不存在。因此,电子设备700可使用网络接口中的用于执行eUICC装置或设备和电子设备700之间的简单无线通信的机构。

[0165] 用户接口子系统708包括任何数量的熟知的I/O设备,包括:键盘、触摸屏(例如,多触摸界面)、LCD显示器、背光源、扬声器和/或麦克风。然而,已经认识到,在某些应用程序中可消除这些部件中的一个或多个部件。例如,PCMCIA卡型客户端实施例可缺少用户接口(因为它们可能背负到它们物理和/或电气耦合的主机设备的用户接口上)。

[0166] 与前面公开的实施例相比,电子设备700包括接收包括安全元件714(可与图6中的安全元件610类似或相同)的存储介质712的插座710。在一些实施例中,存储介质712包括SIM型形状因数设备(尽管应当理解的是,可使用与本公开一致的其他类型和配置的卡),并且安全元件714包括在安全元件714上执行的eUICC应用程序。在当前上下文中,具有可移除地插入到用户设备的物理SIM形状因数(具有安全元件714)的用户设备或装置被称为“传统”设备。

[0167] 安全元件714可被预先配置为将eUICC结合到插入到电子设备700中的存储介质712上。另选地,eUICC可从网络下载到存储介质712(在插入到电子设备700中之后)。此类下载可能要求适当认证和用于确保下载安全性的其他机制(包括使用在于2012年2月14日提交的标题为“Methods and Apparatus for Large Scale Distribution of Electronic Access Clients”的美国临时专利申请61/598,819中所公开的协议,该专利申请的内容以引用方式并入本文)。

[0168] 此外,安全元件714可存储和访问多个访问控制元件612(图6)以用于与网络运营商进行认证。因此,在一些实施例中,安全元件714包括执行同样存储在存储介质712中的软件的安全处理器。

[0169] 此外,安全元件714可进一步硬化以防止篡改(例如,被封装在树脂中),并且可采用加密以用于保护其内容,如前所述。尽管使用eUICC作为对安全元件714的图示,但是可使用其他具体实施,该其他具体实施包括:嵌入式安全元件(电子设备700中的电路板)、智能安全数字(SD)卡、智能微SD卡等。需注意,安全元件714可包括在安全元件714的环境中(诸如,在安全元件714的操作系统中,和/或在安全元件714上执行的Java运行环境中)执行的一个或多个小程序或应用程序。

[0170] eUICC可被配置为识别或以其他方式确定经由存储介质712置于其中的设备(诸如电子设备700)的性能。例如,存储介质712可被物理地配置为基于设备性能水平以特定方式来与电子设备700的一个或多个物理特征部进行交互。这可包括在存储介质712上提供特定

数量的电接触部或电接触部阵列。当存储介质712被插入到具有性能降低的第一设备中时,交互可能不包括至某些接触部的连接部。然而,当将存储介质712插入到具有性能提高的设备中时,交互可能“完成”这是因为所有的接触部可与设备的相应特征部进行通信。在另一实例中,基于用户设备的性能,存储介质712的特征部可基于存储介质712插入到用户设备中被压缩或者保持部署。

[0171] 另选地,存储介质712(并且因此,安全元件714)可意识到经由与设备的信令通信插入到其中的设备的性能。

[0172] 在一些实施例中,可使用存在于存储介质712上的传感器。可使用各个另外的机构以有助于安全元件714确定插入其中的设备的特定性能,前述对于总体概念仅仅是示例性的。

[0173] 一旦确定设备性能,便可使用安全元件714的各种功能。例如,在具有有限性能的设备中,存储介质712(其包括安全元件714)的插入可仅仅使得设备根据与安全元件714相关联的默认访问控制元件而重启。在此情况下,尽管安全元件714被配置为存储多于一个访问控制元件,但是可能不能执行在这些访问控制元件之间切换的机制,从而模仿了传统访问控制元件(例如,传统SIM卡)的行为。可一直自动使用默认访问控制元件(由网络预先配置)。在一些实施例中,当被重置时,默认访问控制元件在向后兼容的操作模式中被设置为最后成功启用的操作配置文件。

[0174] 另选地,如果存储介质712被插入到具有性能增强的设备(“智能”设备)中,则安全元件714可被触发使得设备的用户访问与安全元件714相关联的其他功能。如上所指出的,安全元件714可存储与用户相关联的图6中的访问控制元件612阵列或多个访问控制元件612(例如,eSIM),和/或根据另一逻辑技术或关系(例如,一个用于家庭或商业实体的多个成员中的每个成员,一个用于家庭成员的个人和工作使用的每次使用等)。每个eSIM可包括小型文件系统,该小型文件系统包括计算机可读指令(诸如eSIM程序)以及相关的数据(例如,加密密钥、完整性密钥等)。当存储介质712插入到“智能”设备中时,新界面可在与该设备相关联的显示器上打开,使得用户从多个可用的访问控制元件612(图6)中进行选择。另外,每个访问控制元件可提供对其他访问控制元件不可用的不同性能或功能。

[0175] 例如,如在于2011年4月5日提交的标题为“Methods and Apparatus for Storage and Execution of Access Control Clients”的美国专利申请13/080,521中所公开(该专利申请的内容以引用方式并入本文),设备可激活或执行图6中的多个所存储的访问控制元件612中的一个访问控制元件(例如,eSIM),从而在加载eSIM时,操作系统可仅需要加载当前运行时间环境所必需的软件列表。该“沙箱化”效果可确保可在相同设备内使用多个eSIM而不会不恰当地访问其他eSIM。

[0176] 根据于2011年4月4日提交的标题为“Management Systems for Multiple Access Control Entities”的美国专利申请13/079,614中所讨论的示例性方法和装置还可提供多个eSIM中的切换,该专利申请的内容以引用方式并入本文。

[0177] 还应当理解,对于每个启用的eSIM,eUICC可支持逻辑信道以实现在每个eSIM和在eSIM上运行的正确应用程序之间的通信。在一些实施例中,每个eUICC eSIM被分配其自身的单独逻辑信道。在一些实施例中,逻辑信道仅专用于eSIM,并且该逻辑信道可能不携带任何东西。换句话说,eUICC可确保可在逻辑信道选择至多一个eSIM。需注意,针对eUICC上的

每个eSIM来运行多个应用程序。

[0178] 在一些实施例中,安全元件714实现访问控制元件与电子设备700之间的传输。在示例性实施例中,电子设备700提供基于GUI的确认以启动eSIM的传输。还应当理解,为了实现此类传输功能,可使用存储介质712或电子设备700处的HSM。如先前所指出的,HSM可加密信息(诸如eSIM和eSIM相关的信息)并且可在传输到另一实体之前将其存储。所存储的信息还可通过HSM与加密密钥封装在一起以用于进一步传输安全。

[0179] 另外,用户设备和任何可信第三方实体可相互彼此验证以进一步确保传输的安全性(诸如用户设备之间或用户设备和网络之间的访问控制元件612(图6)的传输,或者eUICC到传统设备的传输)。

[0180] 在一些实施例中,向第三方实体发布用于可信操作的凭证,甚至在已部署用户设备之后。例如,电子设备(例如,UMTS UE)可识别第三方eSIM(例如,虚拟或eSIM)供应商,并且启动可信对话来购买、获取或更新其eSIM。类似地,第三方eSIM供应商可验证UE为可信设备,并且可对eSIM安全地进行编码以用于递送。可信对话可基于唯一的设备密钥和背书证书。在示例性实施例中,设备密钥基于公/私钥加密法。

[0181] 此外,不同于现有的解决方案,本公开的这一特征可实现在不存在预先存在的访问控制元件的情况下将访问控制元件材料递送到传统设备,从而极大地增强了用户灵活性和用户体验。

[0182] 在一些实施例中,安全元件714包括凭证管理模块(可与图6中的凭证管理模块614类似或相同)。该凭证管理模块可为与一组操作中的操作相关联的逻辑实体指定具有一组特权的配置文件(对应于基于策略的框架),该操作与访问控制元件(图6)中的一个或多个访问控制元件相关联。此外,对于操作中的一些操作,逻辑实体中的一些逻辑实体具有不同特权。在一些实施例中,凭证管理模块614(图6)包括安全元件714中的程序模块指定该一组特权所使用的信息。

[0183] 此外,访问控制元件612(图6)中的至少一个访问控制元件可包括针对至少一个逻辑实体来指定第二组特权的信息。在与由凭证管理模块614(图6)所指定的该一组特权相关联的安全级别和与第二组特权相关联的第二安全级别之间发生冲突的情况下,安全元件714可将该安全级别和第二安全级别进行比较并且可选择该一组特权和第二组特权中的与较强安全性相关联的一者。另选地,在与该一组特权相关联的安全级别和与第二组特权相关联的第二安全级别之间发生冲突的情况下,安全元件714可选择该一组特权。

[0184] 在一些实施例中,凭证管理模块614(图6)包括与该一组操作相关联的对称加密密钥,并且给定的加密密钥有助于与该一组操作中的至少给定的操作相关联的特权。另选地或除此之外,凭证管理模块614(图6)可包括证书和与该一组操作相关联的非对称加密密钥以有助于非对称加密,并且给定的加密密钥和给定的证书可有助于与该一组操作中的至少给定的操作相关联的特权。

[0185] 在电子设备700内,处理子系统702、存储器子系统704、联网子系统706、用户接口子系统708和插座710可使用一个或多个互连结构诸如总线耦接在一起。这些互连结构可包括子系统或部件可用于在彼此间传送命令和数据的电、光和/或光电连接件。需注意,不同实施例可包括子系统或部件之间的不同数量或配置的电、光和/或光电连接件。

[0186] 电子设备700可为(或可被包括在)具有至少一个网络接口的任何电子设备。例如,

电子设备700可为(或可被包括在):台式计算机、膝上型计算机、服务器、媒体播放器(诸如,MP5播放器)、装置、小型笔记本计算机/上网本、平板电脑、智能电话、蜂窝电话、测试设备、“智能电表”、网络装置、机顶盒、个人数字助理(PDA)、玩具、控制器、数字信号处理器、游戏机、装置内的计算引擎、消费电子设备、便携式计算设备、个人备忘记事本/或另一电子设备。

[0187] 虽然使用了特定部件来描述电子设备700,但在另选的实施例中,不同的部件和/或子系统可存在于电子设备700中。例如,电子设备700可包括一个或多个另外的处理子系统、存储器子系统、联网子系统、用户接口和/或插座。另外,子系统或部件中的一者或多者可能不存在于电子设备700中。此外,在一些实施例中,电子设备700可包括图7中未示出的一个或多个另外的子系统或部件。同样,尽管图7中示出了独立子系统或部件,但在一些实施例中,给定的子系统或部件的一些或全部可被集成到电子设备700中的其他子系统或部件中的一者或多者中。

[0188] 此外,电子设备700中的电路和部件可使用模拟和/或数字电路的任一组合来实现,包括:双极性、PMOS和/或NMOS门或晶体管。此外,这些实施例中的信号可包括具有大致离散值的数字信号和/或具有连续值的模拟信号。此外,部件和电路可为单端型或差分型并且电源可为单极性或双极性。

[0189] 在前面的描述中,提到了“一些实施例”。需注意,“一些实施例”描述的是所有可能实施例的子集,但并非始终指定实施例的相同子集。

[0190] 前述描述旨在使得本领域的任何技术人员能够实现并使用本公开,并且在特定应用及其要求的上下文中提供。此外,仅出于例证和描述的目的,呈现本公开的实施例的前述描述。它们并不旨在为穷举性的或将本公开限制于所公开的形式。因此,许多修改和变型对于本领域熟练的从业者来说将是显而易见的,并且本文所定义的一般性原理可在不脱离本公开的实质和范围的前提下应用于其他实施例和应用。此外,前述实施例的论述并不旨在限制本公开。因此,本公开并不旨在限于所示出的实施例,而是被赋予与本文所公开的原理和特征一致的最宽范围。

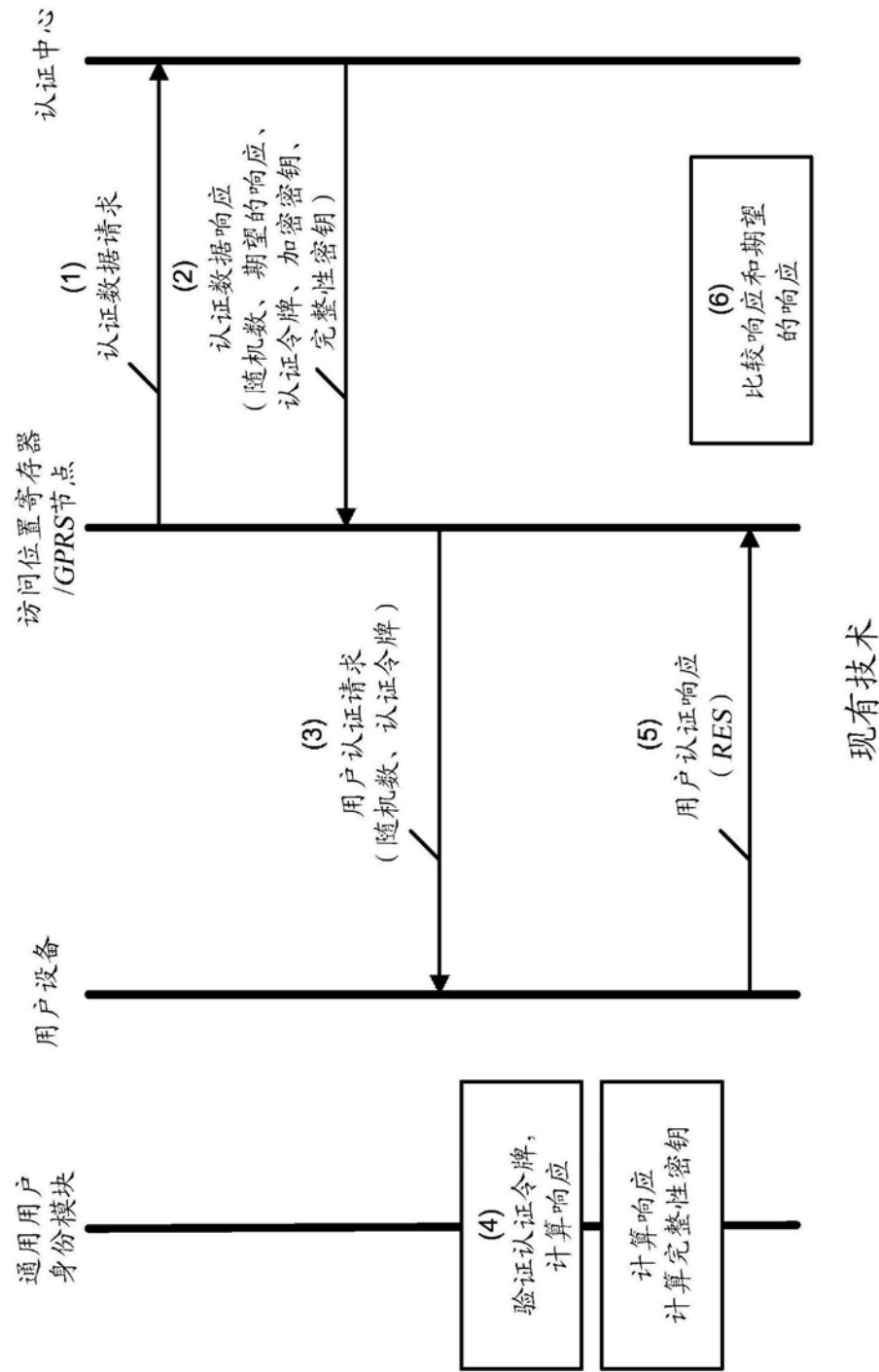


图1

系统
200

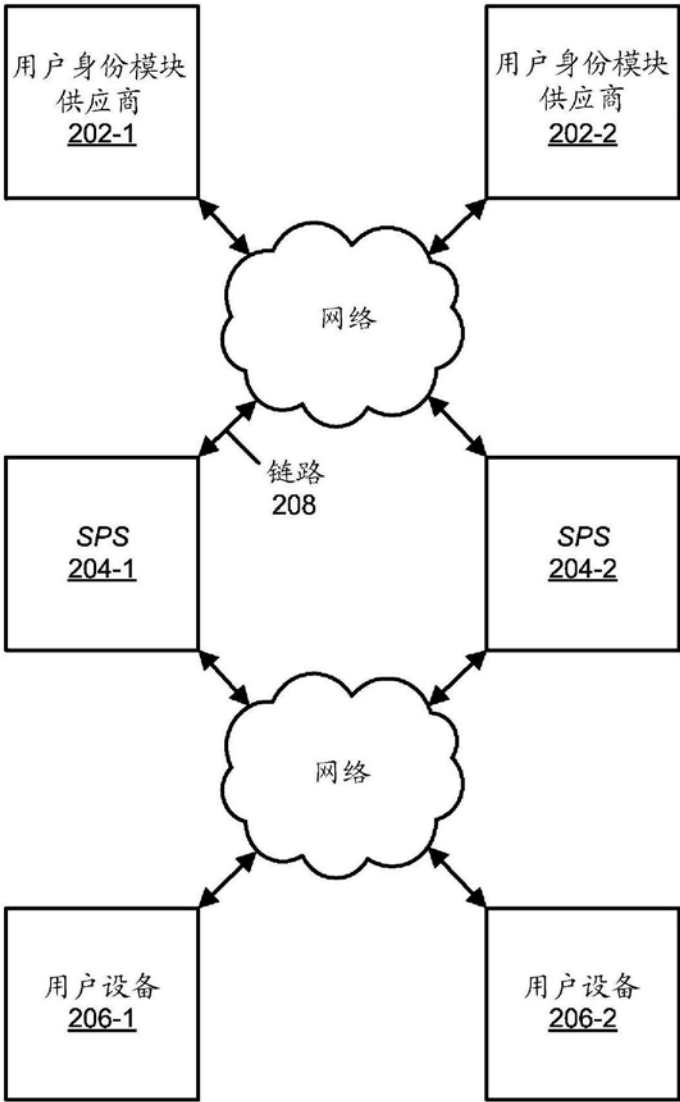


图2

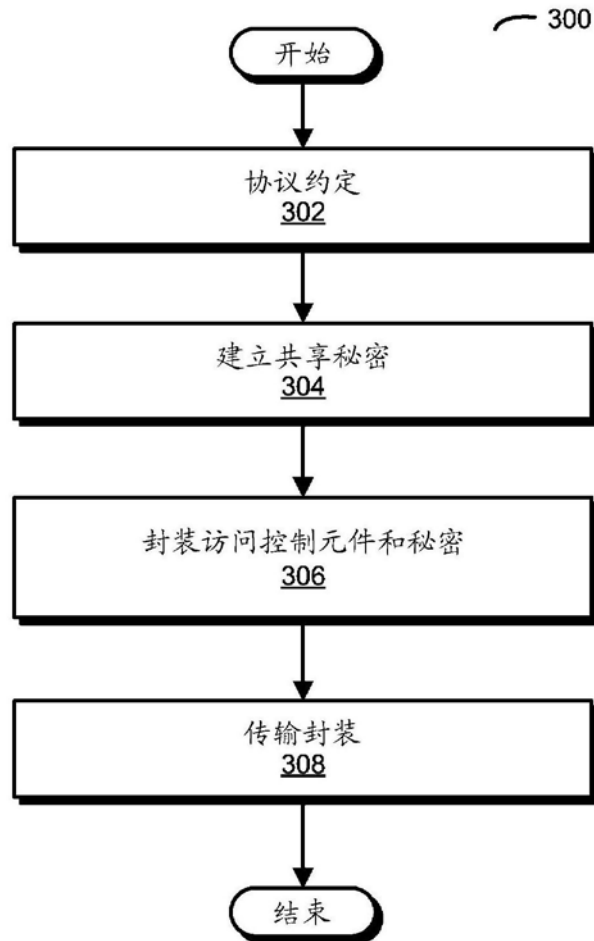


图3

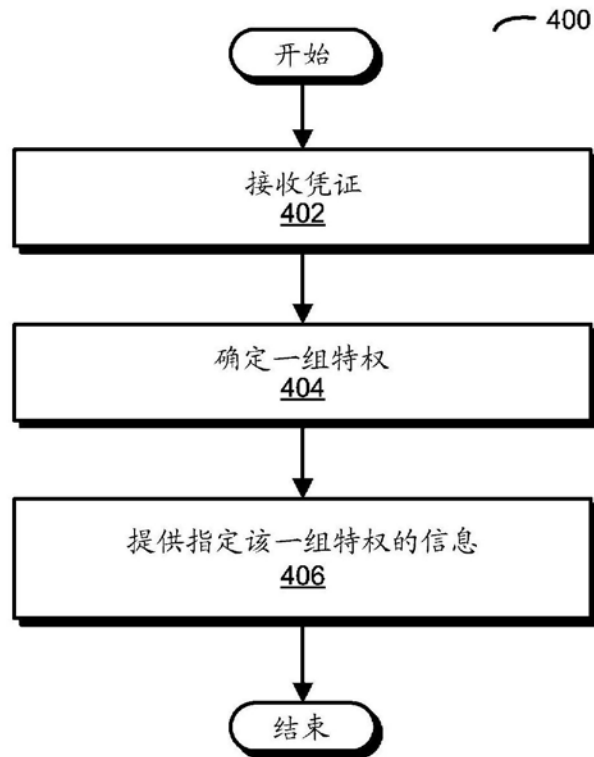


图4

电子通用集成
电路卡装置
500

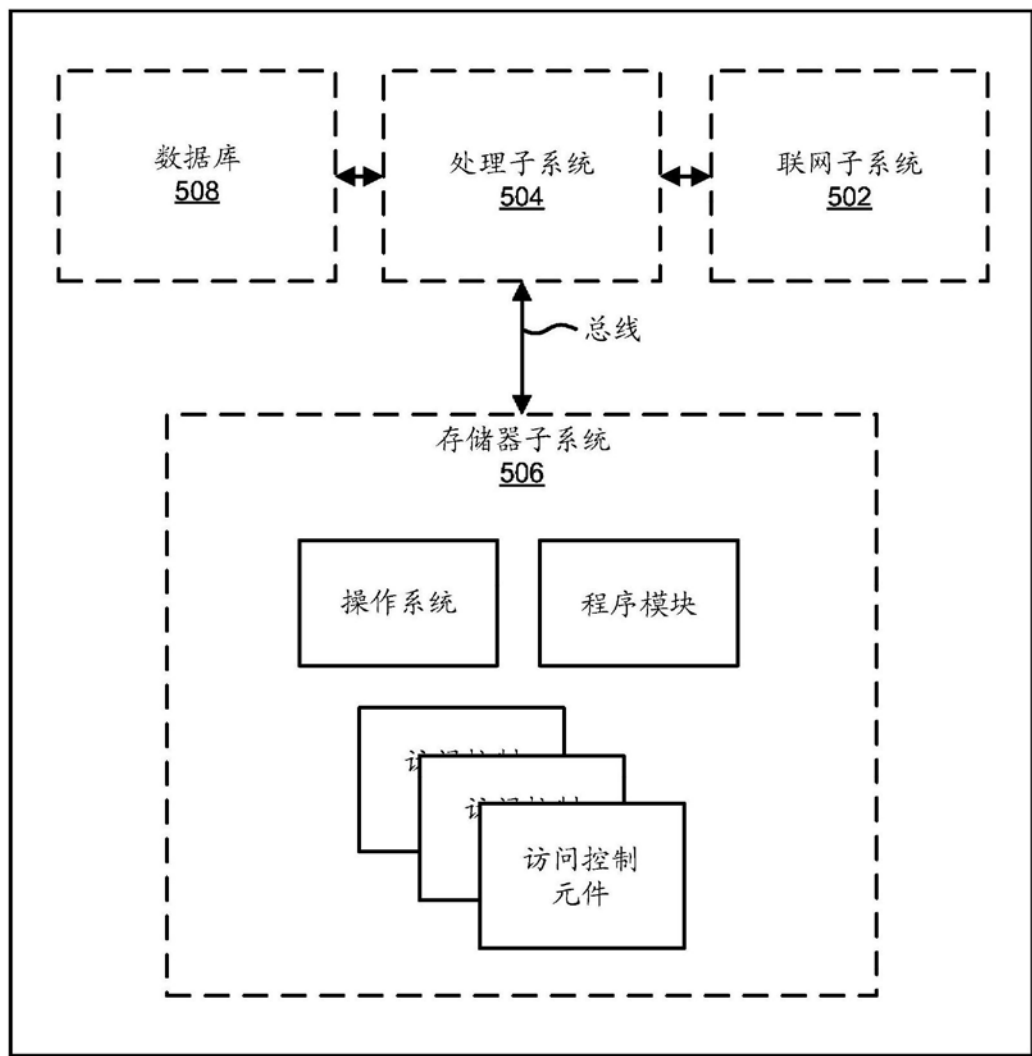


图5

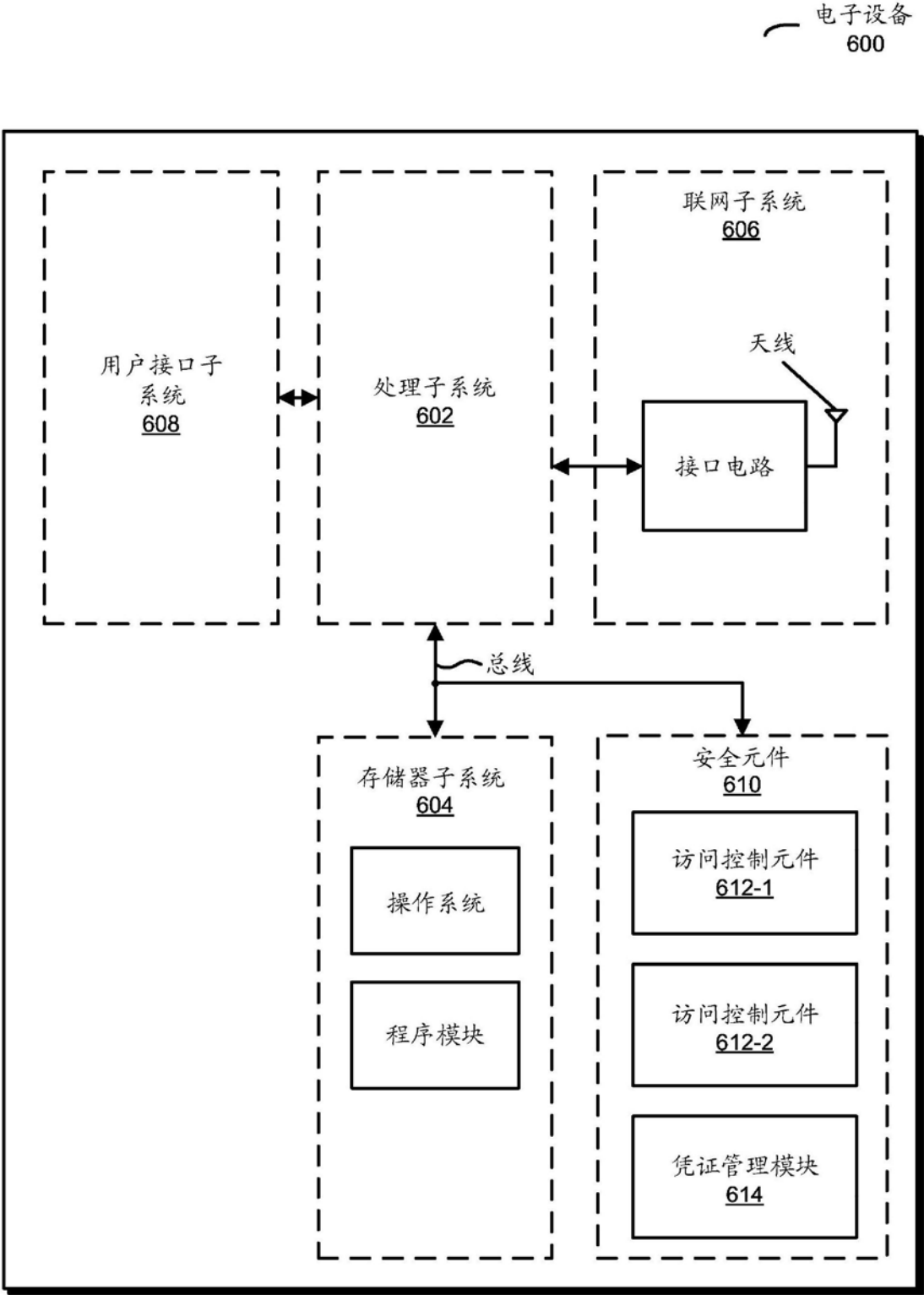


图6

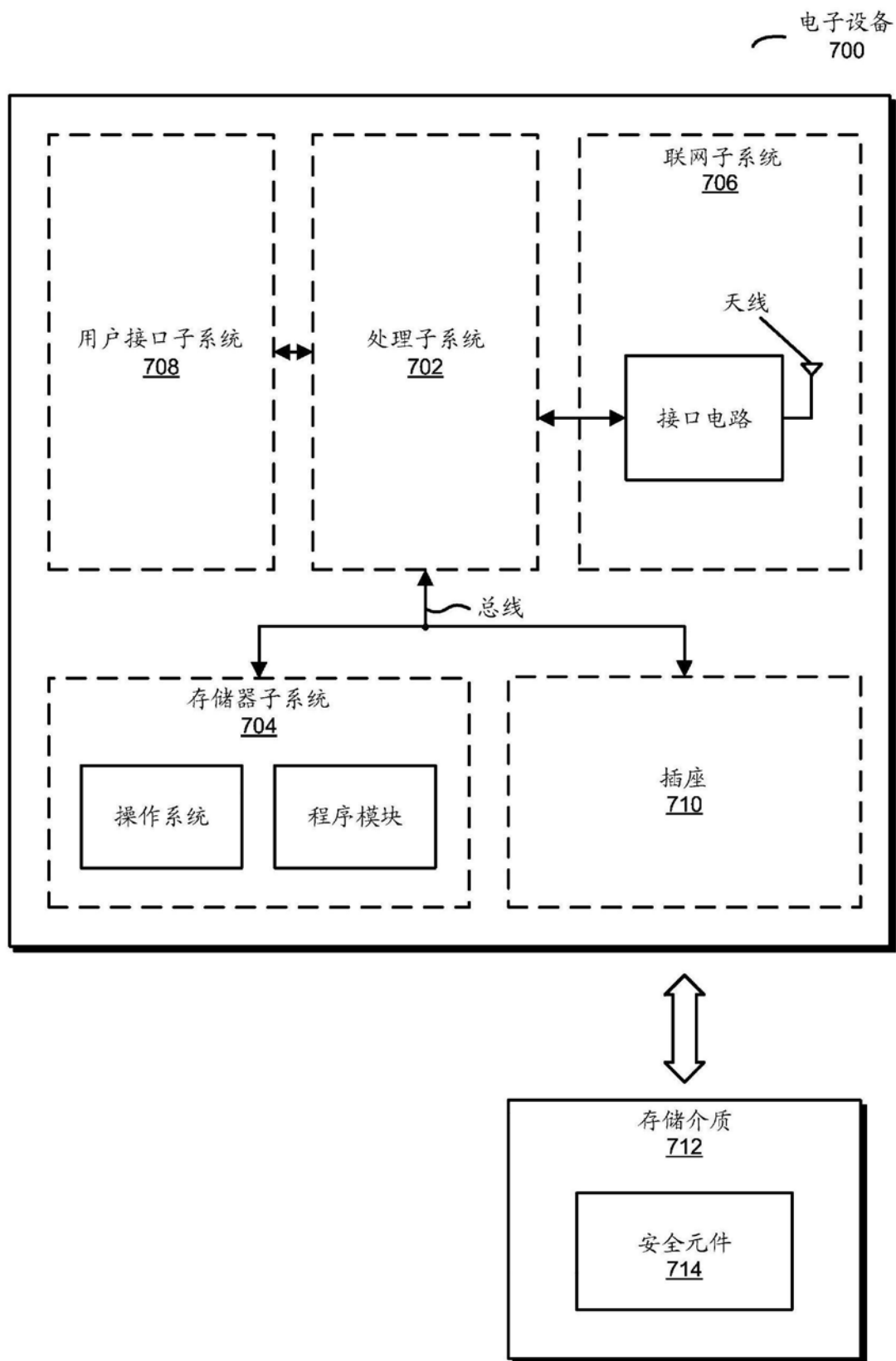


图7