(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112566073 B
(45)授权公告日 2024.07.05

(21)申请号 202011400447.X
(22)申请日 2015.11.17
(65)同一申请的已公布的文献号
申请公布号 CN 112566073 A
(43)申请公布日 2021.03.26
(30)优先权数据
62/080,910 2014.11.17 US
(62)分案原申请数据
201580062364.5 2015.11.17
(73)专利权人 三星电子株式会社
地址 韩国京畿道
(72)发明人 朴钟汉 李德基
(74)专利代理机构 北京市柳沈律师事务所 11105
专利代理师 梁栋国
(51)Int.Cl.
H04W 4/50(2018.01)
H04W 4/60(2018.01)
H04W 8/20(2009.01)
H04W 12/30(2021.01)
H04W 12/02(2009.01)
H04W 12/04(2021.01)
H04L 67/30(2022.01)
H04L 9/40(2022.01)

(56)对比文件
US 2012108205 A1,2012.05.03
US 2014235210 A1,2014.08.21

审查员 董智青

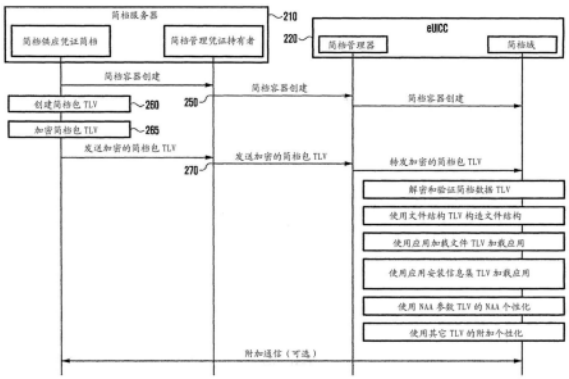
权利要求书3页 说明书33页 附图18页

(54)发明名称

用于通信系统中的简档安装的装置和方法

(57)摘要

本公开涉及一种电子装置及其方法,所述方法包括:从简档服务器接收包括多个数据的简档包信息,所述多个数据从未保护的简档包中分段出来并且基于密钥加密,其中,所述未保护的简档包包括至少一个简档元素,并且所述至少一个简档元素中的每一个将独立于其他简档元素被处理;从简档包信息中获取至少一个数据单元;以及将所述至少一个数据单元传送到与所述电子装置相关联的通用集成电路卡UICC。



CN 112566073 B

1.一种由电子装置执行的方法,所述方法包括:

从简档服务器接收包括多个数据的简档包信息,所述多个数据从未保护的简档包中分段出来并且基于密钥加密,其中,所述未保护的简档包包括至少一个简档元素,并且所述至少一个简档元素中的每一个将在通用集成电路卡UICC中独立于其他简档元素被处理;

从简档包信息中获取至少一个数据单元;以及

将所述至少一个数据单元传送到与所述电子装置相关联的UICC。

2.根据权利要求1所述的方法,其中,所述简档包信息包括与所述密钥相关联的参数,以及

其中,对应于未保护的简档包的简档包括应用程序或文件系统中的至少一个。

3.根据权利要求1所述的方法,其中,所述至少一个数据单元的格式是应用协议数据单元APDU,并且

其中,所述至少一个简档元素的格式是标签长度值TLV形式。

4.根据权利要求1所述的方法,其中,所述至少一个数据单元是通过由用于将所述至少一个数据单元传送到UICC的格式来分割所述简档包信息而获得的,

其中,所述至少一个数据单元以用于UICC解密的格式组合,并且

其中,在不考虑所述至少一个简档元素的结构的情况下,从所述未保护的简档包分段出所述多个数据。

5.一种由与电子装置相关联的通用集成电路卡UICC执行的方法,所述方法包括:

从所述电子装置获得从简档包信息中分段出的至少一个数据单元,其中,所述简档包信息包括从未保护的简档包中分段出来并基于密钥加密的多个数据,并且其中,所述未保护的简档包包括至少一个简档元素;

基于所述至少一个数据单元获得所述至少一个简档元素,其中,所述至少一个简档元素中的每一个将在UICC中独立于其他简档元素进行处理;以及

在UICC中安装所述至少一个简档元素。

6.根据权利要求5所述的方法,其进一步包含:

将所述至少一个数据单元组合成用于解密的格式的至少一个数据;

对用于解密的格式的所述至少一个数据进行解密;以及

基于解密的至少一个数据来标识至少一个简档元素。

7.根据权利要求5所述的方法,其中,所述简档包信息包括与所述密钥相关联的参数,以及

其中,对应于未保护的简档包的简档包括应用程序或文件系统中的至少一个。

8.根据权利要求5所述的方法,其中,所述至少一个数据单元的格式是应用协议数据单元APDU,

其中,所述至少一个简档元素的格式是标签长度值TLV形式,以及

其中,在不考虑所述至少一个简档元素的结构的情况下,从所述未保护的简档包分段出所述多个数据。

9.一种由简档服务器执行的用于向电子装置提供与所述电子装置相关联的通用集成电路卡UICC的简档包信息的方法,所述方法包括:

生成由至少一个简档元素组成的未保护的简档包,其中,所述至少一个简档元素中的

每一个将在UICC中独立于其他简档元素进行处理;

在不考虑所述至少一个简档元素的结构的情况下,获得从未保护的简档包中分段出来的、并基于密钥加密的多个数据;以及

向所述电子装置发送包括所述多个数据的简档包信息。

10.根据权利要求9所述的方法,其中,所述简档包信息包括与所述密钥相关联的参数,以及

其中,对应于未保护的简档包的简档包括应用程序或文件系统中的至少一个。

11.根据权利要求9所述的方法,其中,从所述多个数据获得的至少一个数据单元的格式是用于将所述至少一个数据单元传送到与所述电子装置相关联的UICC的应用协议数据单元APDU,以及

其中,所述至少一个简档元素的格式是标签长度值TLV形式。

12.一种电子装置,包括:

收发器;以及

控制器,其与所述收发器耦合并被配置为:

从简档服务器接收包括多个数据的简档包信息,其中所述多个数据从未保护的简档包中分段出来并基于密钥进行加密,其中,所述未保护的简档包包括至少一个简档元素,并且所述至少一个简档元素中的每一个都将在通用集成电路卡UICC中独立于其他简档元素进行处理,

从所述简档包信息中获取至少一个数据单元,以及

将所述至少一个数据单元传送到与所述电子装置相关联的UICC。

13.根据权利要求12所述的电子装置,其中,所述简档包信息包括与所述密钥相关联的参数,以及

其中,对应于所述未保护的简档包的简档包括应用程序或文件系统中的至少一个。

14.根据权利要求12所述的电子装置,其中,所述至少一个数据单元的格式是应用协议数据单元APDU,

其中,所述至少一个简档元素的格式是标签长度值TLV形式,并且

其中,在不考虑所述至少一个简档元素的结构的情况下,从所述未保护的简档包分段出所述多个数据。

15.根据权利要求12所述的电子装置,其中,所述至少一个数据单元是通过由用于将所述至少一个数据单元传送到UICC的格式来分割所述简档包信息而获得的,

其中,所述至少一个数据单元以用于UICC解密的格式组合,并且

其中,在不考虑所述至少一个简档元素的结构的情况下,从所述未保护的简档包分段出所述多个数据。

16.一种与电子装置相关联的通用集成电路卡UICC,所述UICC包括:

控制器,其被配置为:

从所述电子装置获得从简档包信息中分段出的至少一个数据单元,其中,所述简档包信息包括从未保护的简档包中分段出并基于密钥加密的多个数据,并且其中,所述未保护的简档包包括至少一个简档元素,

基于所述至少一个数据单元获得所述至少一个简档元素,其中,所述至少一个简档元

素中的每一个将在UICC中独立于其他简档元素进行处理,并且

在所述UICC中安装所述至少一个简档元素。

17.根据权利要求16所述的UICC,其中,所述控制器进一步被配置为:

将所述至少一个数据单元组合成用于解密的格式的至少一个数据,

对用于解密的格式的所述至少一个数据进行解密,并且

基于解密的至少一个数据标识至少一个简档元素。

18.根据权利要求16所述的UICC,其中,所述简档包信息包括与所述密钥相关联的参数,以及

其中,对应于所述未保护的简档包的简档包括应用程序或文件系统中的至少一个。

19.根据权利要求16所述的UICC,其中,所述至少一个数据单元的格式是应用协议数据单元APDU,

其中,所述至少一个简档元素的格式是标签长度值TLV形式,并且

其中,在不考虑所述至少一个简档元素的结构的情况下,从所述未保护的简档包分段出所述多个数据。

20.一种简档服务器,用于向电子装置提供用于与所述电子装置相关联的通用集成电路卡UICC的简档包信息,所述简档服务器包括:

收发器;以及

控制器,其与所述收发器耦合并被配置为:

生成由至少一个简档元素组成的未保护的简档包,其中,所述至少一个简档元素中的每一个将在UICC中独立于其他简档元素进行处理;

在不考虑所述至少一个简档元素的结构的情况下,获得从未保护的简档包中分段出来的、并基于密钥加密的多个数据;以及

向所述电子装置发送包括所述多个数据的简档包信息。

21.根据权利要求20所述的简档服务器,其中,所述简档包信息包括与所述密钥相关联的参数,以及

其中,对应于所述未保护的简档包的简档包括应用程序或文件系统中的至少一个。

22.根据权利要求20所述的简档服务器,其中,从所述多个数据中获得的至少一个数据单元的格式是用于将所述至少一个数据单元传送到与所述电子装置相关联的UICC的应用协议数据单元APDU,以及

其中,所述至少一个简档元素的格式是标签长度值TLV形式。

用于通信系统中的简档安装的装置和方法

[0001] 本案是申请日为2015年11月17日、申请号为201580062364.5、发明名称为“用于通信系统中的简档安装的装置和方法”的发明专利申请的分案申请。

技术领域

[0002] 本公开涉及一种由通信系统中的用户设备(UE)选择通信服务以执行通信连接的方法和装置。

背景技术

[0003] 为了满足对自从4G通信系统部署以来已增长的对无线数据业务的需求,已经做出努力来开发改进的5G或准5G通信系统。因此,5G或准5G通信系统也被称为“超4G网络”或“后LTE系统”。考虑在更高的频率(mmWave)带(例如60GHz带)中实现5G通信系统以便实现更高的数据速率。为了减少无线电波的传播损耗并增加传输距离,在5G通信系统中讨论波束成形、大规模多输入多输出(MIMO)、全维度MIMO(FD-MIMO)、阵列天线、模拟波束成形、大规模天线技术。另外,在5G通信系统中,对系统网络改进的开发正基于如下来进行:先进小小区、云无线电接入网(RAN)、超密集网络、设备到设备(D2D)通信、无线回程、移动网络、协同通信、协调多点(CoMP)、接收端干扰消除等等。在5G系统中,已经开发作为高级编码调制(ACM)的混合FSK和QAM调制(FQAM)以及滑动窗口叠加编码(SWSC),以及作为高级接入技术的滤波器组多载波(FBMC)、非正交多址(NOMA)和稀疏代码多址(SCMA)。

[0004] 互联网(其是以人为中心的连接性网络,在其中人类生成和消费信息)现在演变到物联网(IoT),在其中诸如物之类的分布式实体交换和处理信息而无需人工干预。已经浮现出万物互联(IoE),其是通过与云服务器的连接的IoT技术和大数据处理技术的组合。由于对IoT实现方式已经需要诸如“传感技术”、“有线/无线通信和网络基础设施”、“服务接口技术”和“安全性技术”之类的技术元素,所以最近已经研究传感器网络、机器对机器(M2M)通信、机器类型通信(MTC)等等。这样的IoT环境可提供智能互联网技术服务,其中智能互联网技术服务通过收集和分析在连接的物之间生成的数据来向人类生活创造新的价值。IoT可通过在现有信息技术(IT)与各种工业应用之间的融合和组合而应用于各种领域,包括智能家居、智能建筑、智能城市、智能汽车或联网汽车、智能电网、卫生保健、智能家电和高级医疗服务。

[0005] 与此相符,已经进行各种尝试来将5G通信系统应用于IoT网络。例如,可通过波束成形、MIMO和阵列天线来实现诸如传感器网络、机器类型通信(MTC)和机器对机器(M2M)通信之类的技术。作为上述大数据处理技术的云无线电接入网络(RAN)的应用也可被认为是5G技术与IoT技术之间的融合的示例。

[0006] 通用集成电路卡(UICC)对应于在被插入到移动通信UE中的同时使用的智能卡等,也被称为UICC卡。UICC可包括用于接入移动通信提供商的网络的接入控制模块。接入控制模块的示例包括通用订户身份模块(USIM)、订户身份模块(SIM)、IP多媒体服务身份模块(ISIM)等。包括USIM的UICC通常可被称为USIM卡。类似地,包括SIM模块的UICC通常可被称

为SIM卡。在本公开的下面的描述中,SIM卡将用作包括UICC卡、USIM卡、包括ISIM的UICC等的一般含义。也就是说,当提及SIM卡时,该技术可以同样应用于USIM卡、ISIM卡或通常的UICC卡。

[0007] SIM卡存储移动通信订户的私有信息,并且当订户接入移动通信网络时认证订户并创建业务安全密钥,从而使得能安全使用移动通信。

[0008] 在本公开的建议中,SIM卡通常作为特定移动通信提供商的专用卡、响应于对应的提供商的请求而被制造,并且在用于对应的提供商的网络接入的认证信息(例如USIM应用、国际移动订户身份(IMSI)、k值、OPc值等)被预先存储在其中的同时被发布。因而,对应的移动通信服务提供商接收制造的SIM卡的交付以将其提供给订户,并且此后在必要时使用诸如空中下载(OTA)等之类的技术来执行UICC中的应用的管理,诸如安装、修改、删除等等。订户可将UICC卡插入他/她的移动通信UE中以使用对应的移动通信服务提供商的网络和应用服务,并且在更换UE时,订户可将UICC卡从现有的UE移去并插入到新的UE,以如他们那样在新的UE中使用存储在UICC卡中的认证信息、移动通信电话号码、个人电话号码列表等等。

[0009] 然而,对于SIM卡来说允许移动通信UE用户接收另一个移动通信提供商的服务是不方便的。存在不便,在于:移动通信UE用户应当物理地获取SIM卡,以便从移动通信提供商接收服务。例如,存在不便,在于:当旅行到其它国家时,移动通信UE用户应当获取本地SIM卡,以便接收本地移动通信服务。漫游服务可以在一定程度上解决该不便,但是其费用昂贵。此外,当通信提供商之间的合同未建立时,不能接收服务。

[0010] 同时,当将SIM模块远程下载到UICC卡并在UICC卡中安装时,可以显著地解决这样的不便。也就是说,在必要时用户可以将对应于移动通信服务的SIM模块下载到UICC卡。此外,这样的UICC卡可以下载和安装多个SIM模块,并且可以从其之中选择和使用仅仅一个SIM模块。这样的UICC卡可将SIM模块固定到UE,或者可不将SIM模块固定到UE。特别地,在固定到UE的同时使用的UICC被称为嵌入式UICC(eUICC)。通常,eUICC表示在固定到UE的同时使用的UICC卡,并且可以远程下载和选择SIM模块。在本公开中,可以远程下载和选择SIM模块的UICC卡一般被称为eUICC。也就是说,在可以远程下载和选择SIM模块的UICC卡之中的固定到或不固定到UE的UICC卡一般被称为eUICC。此外,关于下载的SIM模块的信息用作被称为eUICC简档的术语。

发明内容

[0011] 技术问题

[0012] 为了解决以上讨论的缺陷,主要目的是提供一种用于在无线通信系统中UE的用户接收移动通信提供商的服务的装置和方法。

[0013] 技术方案

[0014] 根据本公开一实施例的在无线通信系统中的UE包括:用于从简档管理服务器接收简档的接收单元,用于显示通信服务信息的显示单元,以及用于接收待连接到通信服务的简档的控制器。

[0015] 根据本公开一实施例的用于在无线通信系统中提供简档的服务器包括:用于生成和加密简档的控制器,以及用于将加密的简档发送到用于管理简档的服务器的发送单元。

[0016] 根据本公开一实施例的无线通信系统中的用于管理简档的服务器包括:用于从用

于提供简档的服务器接收加密的简档的接收单元;以及用于使用eUICC执行到UE的传送的发送单元。

[0017] 根据本公开一实施例的在无线通信系统中的UE的方法包括:从简档管理服务器接收简档,显示通信服务信息,以及接收待连接到通信服务的简档。

[0018] 根据本公开一实施例的在无线通信系统中的服务器的提供简档的方法包括:生成和加密简档,以及将加密和生成的简档发送到用于管理简档的服务器。

[0019] 根据本公开一实施例的在无线通信系统中的用于管理简档的服务器的管理简档的方法包括:从用于提供简档的服务器接收加密的简档,以及使用eUICC执行到UE的传送。

[0020] 此外,根据本公开一实施例,提供由简档服务器提供简档包的方法。该方法包括:生成简档包;将简档包划分为可安装在电子设备的UICC中的单元,在可加密单元中重新配置划分的简档信息;以及将重新配置的简档信息发送到电子设备。

[0021] 此外,根据本公开一实施例,提供用于提供简档包的简档服务器。简档包包括:发送/接收信号的传输/接收单元,以及控制器,该控制器生成简档包,在可安装在电子设备的UICC中的单元中划分简档包,在可加密单元中重新配置划分的简档信息,以及将重新配置的简档信息发送到电子设备。

[0022] 此外,根据本公开一实施例,提供由电子设备下载简档包的方法。该方法包括:从简档服务器接收构成简档包的可加密单元中的第一简档信息;将可加密单元中的第一简档信息发送到电子设备的UICC;解码已经被发送到UICC的可加密单元中的第一简档信息,从解码的简档信息获取可安装单元中的第一简档信息;以及安装获取的可安装单元中的第一简档信息。

[0023] 此外,根据本公开的实施例,提供用于下载简档包的电子设备。该电子设备包括:发送/接收信号的通信单元,下载和安装简档的UICC;以及控制器,该控制器进行控制以从简档服务器接收构成简档包的可加密单元中的第一简档信息,以及将可加密单元中的第一简档信息发送到电子设备的UICC,其中UICC解码已被发送到UICC的可加密单元中的第一简档信息,从解码的简档信息获取可安装单元中的第一简档信息,以及在可安装单元中安装获取的简档信息。

[0024] 此外,根据本公开一实施例,提供一种由电子装置执行的方法,所述方法包括:从简档服务器接收包括多个数据的简档包信息,所述多个数据从未保护的简档包中分段出来并且基于密钥加密,其中,所述未保护的简档包包括至少一个简档元素,并且所述至少一个简档元素中的每一个将在通用集成电路卡UICC中独立于其他简档元素被处理;从简档包信息中获取至少一个数据单元;以及将所述至少一个数据单元传送到与所述电子装置相关联的UICC。

[0025] 此外,根据本公开一实施例,提供一种由与电子装置相关联的通用集成电路卡UICC执行的方法,所述方法包括:从所述电子装置获得从简档包信息中分段出的至少一个数据单元,其中,所述简档包信息包括从未保护的简档包中分段出来并基于密钥加密的多个数据,并且其中,所述未保护的简档包包括至少一个简档元素;基于所述至少一个数据单元获得所述至少一个简档元素,其中,所述至少一个简档元素中的每一个将在UICC中独立于其他简档元素进行处理;以及在UICC中安装所述至少一个简档元素。

[0026] 此外,根据本公开一实施例,提供一种由简档服务器执行的用于向电子装置提供

与所述电子装置相关联的通用集成电路卡UICC的简档包信息的方法,所述方法包括:生成由至少一个简档元素组成的未保护的简档包,其中,所述至少一个简档元素中的每一个将在UICC中独立于其他简档元素进行处理;在不考虑所述至少一个简档元素的结构的情况下,获得从未保护的简档包中分段出来的、并基于密钥加密的多个数据;以及向所述电子装置发送包括所述多个数据的简档包信息。

[0027] 此外,根据本公开一实施例,提供一种电子装置,包括:收发器;以及

[0028] 控制器,其与所述收发器耦合并被配置为:从简档服务器接收包括多个数据的简档包信息,其中所述多个数据从未保护的简档包中分段出来并基于密钥进行加密,其中,所述未保护的简档包包括至少一个简档元素,并且所述至少一个简档元素中的每一个都将在通用集成电路卡UICC中独立于其他简档元素进行处理,从所述简档包信息中获取至少一个数据单元,以及将所述至少一个数据单元传送到与所述电子装置相关联的UICC。

[0029] 此外,根据本公开一实施例,提供一种与电子装置相关联的通用集成电路卡UICC,所述UICC包括:控制器,其被配置为:从所述电子装置获得从简档包信息中分段出的至少一个数据单元,其中,所述简档包信息包括从未保护的简档包中分段出并基于密钥加密的多个数据,并且其中,所述未保护的简档包包括至少一个简档元素,基于所述至少一个数据单元获得所述至少一个简档元素,其中,所述至少一个简档元素中的每一个将在UICC中独立于其他简档元素进行处理,并且在所述UICC中安装所述至少一个简档元素。

[0030] 此外,根据本公开一实施例,提供一种简档服务器,用于向电子装置提供用于与所述电子装置相关联的通用集成电路卡UICC的简档包信息,所述简档服务器包括:收发器;以及控制器,其与所述收发器耦合并被配置为:生成由至少一个简档元素组成的未保护的简档包,其中,所述至少一个简档元素中的每一个将在UICC中独立于其他简档元素进行处理;

[0031] 在不考虑所述至少一个简档元素的结构的情况下,获得从未保护的简档包中分段出来的、并基于密钥加密的多个数据;以及向所述电子装置发送包括所述多个数据的简档包信息。

[0032] 将在本公开中实现的技术问题不限于以上提及的技术问题,并且以下面的描述为基础的其它未提及的技术问题可能由本公开所属领域中的技术人员容易地理解。

[0033] 在进行以下具体实施方式之前,阐述贯穿本专利文档使用的某些词语和短语的定义可能是有利的:术语“包括(include)”和“包括(comprise)”以及其派生词意为没有限制的包括;术语“或”是包括性的,意为和/或;短语“与……相关联”和“与其相关联”以及其派生词可意为包括、被包括在……内、与……互联、包含、被包含在……内、连接到……或与……连接、耦合到……或与……耦合、与……可通信、与……合作、交织、并列、接近……、被绑定到……或与……绑定、具有、具有……的属性等等;并且术语“控制器”或“处理器”意为控制至少一个操作的任何设备、系统或其部件,这样的设备可以硬件、固件或软件、或者它们中的至少两个的一些组合来实现。应当注意的是:与任何特定控制器相关联的功能性可以是集中式或分布式的,无论本地还是远程。贯穿本专利文档提供对某些词语和短语的定义,本领域普通技术人员应当理解:在许多实例中(如果不是大多数实例中),这样的定义适用于这样定义的词语和短语的现有的以及未来的使用。

[0034] 有益技术效果

[0035] 根据本公开,在无线通信系统中,可以通过其使用通信服务的简档可被自动安装

在移动通信UE中。

附图说明

[0036] 为了更全面地了解本公开及其优点,现在参考下面结合附图的描述,在附图中相同的附图标记表示相同的部件:

[0037] 图1示意性地图示通过可以插入到UE中以及可以从UE拆卸的可拆卸UICC的移动通信网络的连接方法以及通过嵌入在UE中的嵌入式UICC(eUICC)的移动通信网络的连接方法;

[0038] 图2是图示根据本公开一实施例的在无线通信网络中安装简档的过程的信号流程图;

[0039] 图3图示根据本公开一实施例的发送简档包的过程;

[0040] 图4图示根据本公开一实施例的划分和发送简档包的方法;

[0041] 图5图示根据本公开一实施例的发送划分的简档包的方法;

[0042] 图6图示根据本公开一实施例的生成和加密简档包的过程;

[0043] 图7是图示根据本公开一实施例的发送和安装简档包的方法的流程图;

[0044] 图8图示在选择简档和简档的文件结构之后激活简档的方法;

[0045] 图9图示用于在eSIM简档内执行USIM的认证的AKA认证过程;

[0046] 图10至13图示根据本公开附加实施例的发送简档信息的操作;

[0047] 图14是图示根据本公开一实施例的发送和安装eUICC简档的过程的信号流程图;

[0048] 图15是图示根据本公开另一实施例的发送和安装eUICC简档的过程的信号流程图;

[0049] 图16a和16b图示根据本公开另一实施例的发送和安装eUICC简档的过程;

[0050] 图17图示根据本公开一实施例的简档服务器;以及

[0051] 图18图示根据本公开一实施例的UE。

具体实施方式

[0052] 下面讨论的图1至图18以及用于在本专利文档中描述本公开的原理的各种实施例仅仅通过举例说明的方式,而不应当以任何方式解释为限制本公开的范围。本领域技术人员将理解:本公开的原理可以以任何适当布置的电信技术来实现。此后,将参照附图详细描述本公开的实施例。

[0053] 在描述实施例时,将省略对在本公开所属技术领域中广为人知的并且与本公开不直接相关的技术特征的描述。这是为了通过省略不必要的描述来更清楚地描述本公开的主题,而没有混淆。

[0054] 在下面的描述中使用的特定术语被提供以帮助理解本公开,并且可以变化成各种形式而不脱离本公开的技术精神。

[0055] 此外,将定义本说明书中的术语。

[0056] 在本说明书中,作为在插入在移动通信UE中的同时使用的智能卡的UICC表示存储诸如网络接入认证信息。电话号码和短消息服务(SMS)之类的移动通信订户的私有信息的芯片,并且当接入诸如全球移动通信系统(GSM)、宽带码分多址(WCDMA)和长期演进(LTE)等

之类的移动通信网络时执行用户认证和流量安全性密钥生成,从而使得能够安全地使用移动通信。UICC具有安装到其的通信应用,诸如订户身份模块(SIM)、通用SIM(USIM)和IP多媒体SIM(ISIM),并且可以提供用于安装诸如电子钱包、票务和电子护照之类的各种应用的高级安全性功能。

[0057] 在本说明书中,eUICC是安全性模块,该安全性模块不是插入在UE中以及从UE拆卸的可拆卸类型的芯片,而是嵌入在UE中的芯片。eUICC可以使用空中下载(OTA)技术下载和安装简档。

[0058] 在本说明书中,在eUICC中使用OTA技术下载简档的方法甚至可以应用于可以插入到UE中以及可以从UE拆卸的可拆卸类型的UICC。

[0059] 在本说明书中,术语“UICC”可以与SIM混合使用,术语“eUICC”可以与eSIM混合使用。

[0060] 在本说明书中,简档可以表示通过以软件形式封装存储在UICC中的应用、文件系统和认证密钥值等获得的东西。

[0061] 在本说明书中,USIM简档可以表示通过以软件形式在简档中封装包括在USIM应用中的信息获得的简档。

[0062] 在本说明书中,操作简档可以表示通过以软件形式封装UE的用户所注册到的移动通信提供商的订户信息获得的东西。

[0063] 在本说明书中,供应简档可以表示预安装到eUICC的简档,这对于在用户订阅特定通信提供商之前允许UE接入预定国家的预定移动通信网络是必要的。

[0064] 在本说明书中,简档供应服务器可以被表达为订阅管理器数据准备(SM-DP)、简档域的离卡(off card)实体、简档加密服务器、简档生成服务器、简档供应器(PP)、简档提供器和简档供应凭证持有者(PPC持有者)。

[0065] 在本说明书中,简档管理服务器可以被表达为订阅管理器安全路由、eUICC简档管理器的离卡实体或者简档管理凭证持有者(PMC持有者)。

[0066] 在本说明书中,eUICC简档管理器可被表达为ISD-R、简档管理域等等。

[0067] 本说明书中使用的术语“终端”可以被称为移动站(MS)、用户设备(UE)、用户终端(UT)、无线终端、接入终端(AT)、终端、订户单元、订户站(SS)、无线设备、无线通信设备、无线发送/接收单元(WTRU)、移动节点、移动或其它术语。UE的各种实施例可以包括蜂窝电话、具有无线通信功能的智能手机、具有无线通信功能的个人数字助理(PDA)、无线调制器/解调器(MODEM)、具有无线通信功能的便携式计算机、诸如具有无线通信功能的数码相机之类的拍摄装置、具有无线通信功能的游戏设备、具有无线通信功能的音乐存储和再现家用电器、能够进行无线互联网接入和浏览的互联网家用电器以及具有所述功能的组合的便携式单元或UE。此外,UE可以包括机器对机器(M2M)UE和机器类型通信(MTC)UE/设备,但是本公开不限于此。

[0068] 在本说明书中,电子设备可以包括嵌入在其中的能够下载和安装简档的UICC。当UICC未嵌入在电子设备中时,与电子设备物理分离的UICC可以在插入到电子设备中的同时连接到电子设备。例如,UICC可以以卡的形式插入到电子设备中。电子设备可以包括UE。此时,UE可以是包括可以下载和安装简档的UICC的UE。UICC可以嵌入在UE中,并且当UE和UICC彼此分离时,可以将UICC插入到UE中,并且可以在插入到UE中的同时连接到UE。可以下载和

安装简档的UICC例如被称为eUICC。

[0069] 在本说明书中,简档标识符可以被称为与简档ID、集成电路卡ID(ICCID)和发行者安全性域简档(ISD-P)匹配的因素。简档ID可以指示每个简档的唯一标识符。

[0070] 在本说明书中,eUICC ID可以是嵌入在UE中的eUICC的唯一标识符,并且可以被称为EID。此外,当供应简档被预先安装到eUICC时,eUICC ID可以是对应的供应简档的简档ID。此外,当UE和eUICC(或eSIM))芯片未彼此分离时,如在本公开的实施例中,eUICC ID可以是UE ID。此外,eUICC ID可以被称为eSIM芯片的特定安全域。

[0071] 在本说明书中,简档容器可以被称为简档域。简档容器可以是安全性域。

[0072] 在本说明书中,应用协议数据单元(APDU)可以是用于允许UE与eUICC交互工作的消息。此外,APDU可以是用于允许PP或PM与eUICC交互工作的消息。

[0073] 在本说明书中,简档供应凭证(PPC)可以是用于PP与eUICC之间的相互认证、简档加密以及签名的手段。PPC可以包括对称密钥、RSA认证证书和私有密钥、ECC认证证书和私有密钥以及根CA和认证证书链中的一个或多个。此外,当存在多个PP时,可以在eUICC中存储或者可以使用用于多个PM中的每一个的不同PMC。

[0074] 在本说明书中,简档管理凭证(PMC)可以是用于PM与eUICC之间的相互认证、传输数据加密以及签名的手段。PMC可以包括对称密钥,RSA认证证书和私有密钥、ECC认证证书和私有密钥以及根CA和认证证书链中的一个或多个。此外,当存在多个PM时,可以在eUICC中存储或者可以使用用于多个PM中的每一个的不同PMC。

[0075] 在本说明书中,AID可以是应用标识符。该值可以是通过其来标识eUICC内的不同应用的标识符。

[0076] 在本说明书中,TAR可以是工具包应用参考。该值可以是通过其来标识工具包应用的标识符。

[0077] 在本说明书中,简档包TLV可以被称为简档TLV。简档包TLV可以是以TLV(标签、长度、值)的形式表达构成简档的信息的数据集。

[0078] 在本说明书中,AKA可以指示认证和密钥协议,并且可以指示用于接入3GPP和3GPP2网络的认证算法。

[0079] 在本说明书中,K对应于存储在eUICC中的用于AKA认证算法的加密密钥值。

[0080] 在本说明书中,OPc对应于存储在eUICC中的用于AKA认证算法的参数值。

[0081] 在本说明书中,作为网络接入应用程序的NAA可以是存储在UICC中以便接入网络的诸如USIM或ISIM之类的应用程序。NAA可以是网络接入模块。

[0082] 在本说明书中,AMF可以是认证管理字段值。

[0083] 在本说明书中,SQN可以是序列号值。

[0084] 在本说明书中,L是可以存储在NAA中的值,并且可以是在AKA认证过程期间在SQN验证时使用的参数。

[0085] 在本说明书中,增量值是可以存储在NAA中的值,并且可以是在AKA认证过程期间在SQN验证时使用的参数。

[0086] 此外,在下面对本公开的描述中,当在此并入的对相关已知功能或配置的详细描述可能使得本公开的主题相当不清楚时,其将被省略。

[0087] 图1示意性地图示通过可以插入到UE中以及可以从UE拆卸的本领域中的可拆卸

UICC的移动通信网络的连接方法以及通过嵌入在UE中的嵌入式UICC(eUICC)的移动通信网络的连接方法。

[0088] 参考图1,可拆卸UICC可以插入到UE中(如由附图标记101所指示)。简档可以被预先安装到可拆卸UICC中。UE可以使用安装的简档连接到移动网络(如由附图标记102所指示)。

[0089] UE具有嵌入在其中的eUICC。eUICC可以具有预先安装到其的供应简档。UE可以使用安装的供应简档来接入用于供应的移动网络。UE可以通过接入用于供应的临时移动网络来从移动网络服务器下载简档。临时移动网络是用于下载简档的移动网络。UE可以安装下载的简档,并且可以使用该简档连接到移动网络(如由附图标记105所指示)。

[0090] 图2图示根据本公开的实施例的在无线通信网络中安装简档的实施例。简档服务器210可以包括PP和PM。eUICC 220可以包括简档管理器和简档域。因而,以下将描述的PP和PM的操作可以由简档服务器210执行,而简档管理器和简档域的操作可以由eUICC执行。

[0091] 参考图2,在操作250,简档服务器210可以请求生成来自eUICC 220的简档容器。PP可以在与PM通信的同时执行对特定eUICC的简档容器生成请求。简档容器生成请求可以是简档下载请求命令。可以在PP与PM之间使用加密的通信,并且可以通过配置对称密钥来使用或者可以在认证证书方案中使用加密的通信。首先,作为基于认证证书的加密的通信的示例,当PP生成加密对称密钥,通过PM的公开密钥加密生成的加密对称密钥,并将加密的对称密钥发送到PM时,PM通过PM的私有密钥解码加密对称密钥,并且然后对于用PP加密的密钥商业使用对应的对称密钥。

[0092] 简档容器创建命令可以在被包括在HTTP消息中的同时被发送。已经接收到简档容器创建命令的PM可以在与eUICC通信的同时请求简档容器创建(或者可以被表达为简档生成、简档域生成等等)。作为示例,在该过程中,PM可以使用SMS消息,以便与eUICC通信。详细地,PM可以允许eUICC在SMS-PP消息中包括表示简档容器创建的APDU。这样的APDU消息的一个示例可以包括PUSH(推)APDU命令。这样的APDU消息的另一个示例可以是STORE(存储)消息。此外,当生成SMS-PP消息时,PM可以加密APDU消息。此时,可以在PM与eUICC之间共享并且存储待使用的加密密钥。简档容器生成请求可以首先被发送到移动通信UE,并且移动通信UE生成APDU消息并将APDU消息发送到eUICC。

[0093] 此外,可以使用HTTP消息执行PM与eUICC之间的消息传输。详细地,在PM与eUICC之间使用先前生成和存储的对称密钥或认证证书建立TLS通信信道,并且然后可以使用HTTP消息来发送消息。以这种方式,当不使用SMS而是使用HTTP时,存在优点:可以使用利用移动通信网络的IP通信,或者可以使用利用Wi-Fi或蓝牙的IP网络执行PM与eUICC之间的通信。

[0094] 已经从PM发送的简档容器创建请求消息可以由eUICC内的eUICC简档管理器处理。eUICC简档管理器可以解码包括请求存储在eUICC中的PMC之中的一个值的请求的通信消息,并且使用配置值来验证解码的值,并且当验证通过时,在eUICC内生成简档容器。可以向简档容器分配用于生成eUICC内的简档、AID值等等所必需的存储器。

[0095] 同时,PP可以生成(如由附图标记260所指示)和加密(如由附图标记265所指示)简档包TLV,以便在eUICC中生成的简档容器中安装简档。简档服务器210可以生成简档包(操作260)。简档包可以具有标签长度值(TLV)形式。具有TLV形式的简档包可以被称为简档包TLV。简档服务器210可以生成被划分为可安装单元中的n条信息的简档包。此外,简档服务

器可以在生成简档包之后将简档包划分为可安装单元中的信息。可安装单元中的信息可以表示整个简档包信息的一部分,该可安装单元中的信息被配置成当信息被发送到eUICC 220时即使整个简档包未被发送到eUICC也安装在eUICC中的信息。

[0096] 简档服务器210可以加密生成的简档包(操作265)。简档服务器可以将通过可安装单元中的n条信息配置的简档包加密成可加密单元中的m条信息。n和m可以彼此相等,或者可以彼此不同。简档服务器210可以将配置可加密单元中的简档包发送到电子设备。简档服务器可以在可发送单元中配置在可加密单元中配置的简档包,并且然后将简档包发送到电子设备。此时,可发送单元可以对应于下述尺寸,其中已经接收简档包的电子设备可以以该尺寸将接收的简档包发送到电子设备的UICC。例如,可发送单元可以是APDU的数据单元。

[0097] 此后,将描述由PP生成简档包TLV的过程。

[0098] 然而,TLV形式仅仅是简档包的示例,并且在本公开的实施例中,简档包的形式不限于TLV形式。表1图示简档包TLV的结构。这里,以标签-长度-值形式记录数据的方案一般被称为TLV。简档包TLV可以被称为简档TLV。参考表1,表中的名称字段对应于TLV的名称,并且不是实际包括在数据中的值。在M/O/C字段的情况下,M的值表示必然包括数据,O的值表示不可以包括数据,并且C的值表示有条件地包括数据。M/O/C字段不可以是实际包括在数据中的值。然而,M/O/C字段可以存储在eUICC内的源代码中,并且用于验证对应数据的有效性。

[0099] [表1]配置包TLV结构

[0100]

名称	M/O/C	标签	长度	值
简档包	M	A1	L1	如在表1-1中编码的

[0101] 在表1中,简档包TLV的标签值在表1中被表达为A1,该标签值是具有1字节的尺寸的数据值。A1值可以采用选自十六进制形式的从“00”到“FF”的256个值中的一个值。例如,A1值可以是“8E”。

[0102] 在表1中,简档包TLV的长度值是指示存储在简档TLV的值字段中的数据的长度的值,并且长度字段的长度可以被固定或配置成2字节或3字节。作为示例,当长度字段的长度固定为3字节时,长度字段的值可以具有十六进制形式的值“000000”-“FFFFFF”,并且因而可以最大表示2^24字节或16M字节的数据长度。作为示例,为“020001”的长度字段的值指示值字段的长度为128K字节。此外,作为示例,当长度字段的长度固定为2字节时,长度字段的值可以具有十六进制形式的值“0000”-“FFFF”,并且因而可以最大表示2^16字节或64K字节的数据长度。

[0103] 表1中的简档包TLV的值字段包括用于安装简档的各条信息,并且使用如在表1-1中的对应信息来配置数据。

[0104] 参考表1-1,简档TLV的值字段可以包括文件结构TLV数据。文件结构TLV是用于包括简档的文件结构、属性和文件内容的数据。文件结构TLV的标签值被表达为表1-1中的A2,该标签值是具有1字节尺寸的数据值。A2值可以采用选自十六进制形式的从“00”到“FF”的256个值中的一个。例如,A1值可以是“01”。

[0105] [表1-1]简档包TLV的值部分的结构

[0106]

名称	M/O/C	标签	长度	值
文件结构	M	A6	1～n字节	如在表2中编码的

NAA参数	M	'00' ~ 'FF'	1～n字节	如在表3中编码的
NAA参数	O	'00' ~ 'FF'	1～n字节	如在表3中编码的
…	O	'00' ~ 'FF'		
加载文件包	O	'00' ~ 'FF'	1～n字节	如在表4中编码的
加载文件包	O	'00' ~ 'FF'	1～n字节	如在表4中编码的
…				
RFU				

[0107] 在表1-1中,文件结构数据TLV的长度值是指示存储在文件结构TLV的值字段中的数据的长度的值,并且长度字段的长度可以被固定或配置成2字节或3字节。当长度字段的长度被固定3字节时,长度字段的值可以具有十六进制形式的值"000000"-"FFFFFF",并且因而可以最大表示2^24字节或16M字节的数据长度。例如,是"020001"的长度字段的值指示值字段的长度为128K字节。此外,当长度字段的长度固定为2字节时,长度字段的值可以具有十六进制形式的值"0000"-"FFFF",并且因而可以最大表示2^16字节或64K字节。文件结构数据TLV的值可以包括各条文件信息,并且其结构可以是如表2中的数据结构。

[0108] [表2]文件结构TLV的值部分的结构

[0109]

名称	M/O/C	标签	长度	值
文件	M	A6	1~3 字节	对于 MF、DF 或 ADF，如在表 2-1 中编码
文件	O	A6	1~3 字节	对于 DF 或 ADF，如在表 2-1 中编码，以及对于 EF，如在表 2-2 中编码
…	…	…	…	…
文件	O	A6	1~3 字节	对于 DF 或 ADF，如在表 2-1 中编码，以及对于 EF，如在表 2-2 中编码

[0110] 参考表2,文件结构TLV的值可以包括至少一条或多条文件TLV数据。每个文件TLV可以包括MF文件、DF文件、ADF文件或EF文件的数据。这里,MF文件表示主文件或主DF文件,并且DF文件表示专用文件,并且ADF文件表示应用程序专用文件,并且EF文件表示基本文件。在一个文件结构TLV中,可以存在一个包括MF文件信息的文件TLV,或者可以不存在包括MF文件信息的文件TLV。文件TLV的标签值被表达为表2中的A6,该标签值是具有1字节尺寸的数据值。A6值可以采用选自十六进制形式的从"00"到"FF"的256个值中的一个。例如,A6值可以是"02"。文件TLV的长度值可以在固定为1字节或2字节或配置成其它值的同时被使用。可以以如表2-1或表2-2中的数据结构生成文件TLV的值部分。当文件TLV包括关于MF文件、DF文件或ADF文件的信息时,对应文件TLV的值部分的数据可以如表2-1中来配置,而当文件TLV包括关于EF文件的信息时,对应文件TLV的值部分的数据可以如表2-2中来配置。

[0111] [表2-1]文件TLV的值部分的结构,包括关于MF文件、DF文件和ADF文件的信息

[0112]

名称	M/O/C	描述	长度
A6	M	标签：文件	1字节
		文件的长度(下一个字节到结尾)	1~n字节
	M	如在TS 102.222中编码的FCP模板TLV(参见注释)	1~n字节
A7	O	标签：文件路径	1字节
		文件路径的长度	1字节
		文件路径字节(文件ID的拼接)	2×n字节
注释：FCP模板TLV是用于ETSI TS 102.222中的CREATE命令的确切相同的一个。 如果是MF，则FCP模板TLV中的文件ID应当被编码为‘3F00’，并且FCP模板TLV中的文件描述符字节的文件类型比特应当被编码为‘111’。			

[0113] 参考表2-1,当文件TLV包括关于MF文件、DF文件或ADF文件的信息时,文件TLV可以包括在标签和长度字段下面的FCP模板TLV和文件路径TLV数据。FCP模板TLV可以使用包括关于文件ID等的信息的值作为具有ETSI TS102.222标准的文件控制参数TLV。文件路径是指示对应文件TLV的文件路径的值,并且例如是表达文件ID的值。可以在文件TLV中包括或不包括文件路径TLV。当不包括文件路径时,即使没有对应文件的文件路径,也可以执行确定。例如,当对应于DF文件的文件TLV和对应于EF文件的文件TLV在文件结构TLV内彼此连接,并且对应于EF文件的文件TLV不包括文件路径TLV时,可以在其中对应的EF文件被认为是包括在DF文件下面的EF文件的状态下生成文件。当使用这样的方案生成文件时,可以通过减少关于文件路径的信息来减少待发送的简档数据的尺寸。

[0114] [表2-2]文件TLV的值部分的结构,包括关于EF文件的信息

[0115]

名称	M/O/C	描述	长度
A6	M	标签：文件	1字节~n字节
		文件的长度(下一个字节到结尾)	1字节~n字节
	M	如在TS 102.222中编码的FCP模板TLV	1~n字节
A7	O	标签：文件路径	1字节~n字节
		文件路径的长度	1字节~n字节
		文件路径字节(文件ID的拼接)	2×n字节
A8	C3	标签：文件二进制	1字节~n字节
		文件二进制的长度	1字节~n字节
		文件二进制	1字节~n字节
A9	C3	标签：文件记录序列	1字节~n字节
		文件记录序列的长度	1字节~n字节
		文件记录序列	1字节~n字节
B1	C4	标签：文件数据	1字节~n字节
		文件数据的长度	1字节~n字节
		文件数据	1字节~n字节
C2：二进制TLV用于透明的EF。 C3：文件记录序列TLV用于线性固定或循环EF。 C4：文件数据TLV用于BER-TLV EF。			

[0116] 参考表2-2,当文件TLV包括关于EF文件的信息时,文件TLV可以在标签和长度字段下面包括FCP模板TLV和文件路径TLV,并且可以另外包括下面的三个TLV之一,而没有例外:

[0117] -文件二进制TLV;

[0118] -文件记录序列TLV;

[0119] -文件数据TLV。

[0120] 当EF文件具有透明结构时,文件TLV包括以上三个TLV之中的文件二进制TLV,并且文件二进制TLV的值可以具有二进制形式。

[0121] 当EF文件具有线性固定结构或循环结构时,文件TLV包括以上三个TLV之中的文件记录序列TLV,并且文件记录序列TLV的值可以是通过将序列字节附连到EF文件中包括的记录数据而拼接的值。表YY图示文件记录序列TLV的结构。在文件记录序列TLV中,连接标签值、长度值、记录号码字节和记录数据。表2-3图示三个记录被更新到EF文件。例如,当EF文件对应于通过10条记录配置的线性固定类型,并且十条记录之中的仅仅三条记录被更新时,文件记录序列TLV被如表2-3中配置。此时,记录号可以是指示总记录之中的特定记录的

顺序的值。

[0122] [表2-3]

[0123]

名称	M/O/C	描述	长度
A9	C3	标签:文件记录序列	1字节～n字节
		文件记录序列的长度	1字节～n字节
		记录号	1字节
		记录	1字节～n字节
		记录号	1字节
		记录	1字节～n字节
		记录号	1字节
		记录	1字节～n字节

[0124] 当EF文件具有BER-TLV结构时,包括三个TLV中的文件数据TLV,并且文件数据TLV可以是通过TLV结构配置其数据的数据。

[0125] [表3]NAA参数TLV的值部分的结构

[0126]

名称	M/O/C	标签	长度	值
NAA 类型	M	TBD	1 字节	'01': USIM '02': ISIM '03'-: FFS

[0127]

MILENAGE 参数	C1	TBD	1 字节~n 字节	…
TUAK 参数	C2	TBD	1 字节~n 字节	…
本地 NAA 指示符	O	TBD	1 字节	'01': 使用由 eUICC 平台提供的 NAA '02': 使用在加载文件包 TLV 中下载的 NAA
RFU				
C1: 如果 MILENAGE 不被 eUICC 平台支持, 则不应当包括 MILENAGE 参数 TLV。 C2: 如果 TUAK 不被 eUICC 平台支持, 则不应当包括 TUAK 参数 TLV。				

[0128] 返回来参考表1-1,简档包TLV的值数据可以包括一个或多个NAA参数TLV。这样的NAA参数TLV的标签值可以采用选自十六进制形式的从“00”到“FF”的256个值中的一个。

[0129] 参考表3,可以将NAA类型TLV插入到这样的NAA参数TLV的值区域中。NAA类型TLV的值对应于确定网络接入模块类型(诸如USIM或ISIM)的值。作为示例,在USIM的情况下,值可以是“01”,并且在ISIM的情况下,值可以是“02”。此外,在其中NAA支持MILENAGE算法的情况下,可以包括MILENAGE参数TLV。作为示例,MILENAGE参数TLV可以包括K值、OPc值、r1-r5值

和c1-c5值。此外,在其中NAA支持TUAK算法的情况下,可以包括TUAK参数TLV。作为示例,TUAK参数TLV可以包括K值、OPc值和RES长度值。

[0130] 同时,NAA参数TLV可以包括本地NAA指示器TLV。当下载对应的简档并且然后安装网络接入模块时,该值通知:是使用由eUICC平台提供的网络接入模块应用程序安装网络接入模块,还是使用如下所述地在被包括在加载文件包TLV的同时发送的网络接入应用程序安装网络接入模块。在前一种情况下(即,当下载简档并且然后安装网络接入模块时,网络接入模块应用程序由eUICC平台提供),仅仅可以使用由eUICC平台提供的AKA认证逻辑。然而,在后一种情况下(即,使用当被包括在加载文件包TLV中的同时发送的网络接入应用程序安装网络接入模块),AKA认证机制可以被下载,同时被包括在简档中包括的应用程序中并被安装。同时,在后一种情况下,可以使用由OS或eUICC的平台提供的核心认证功能。

[0131] 作为示例,后者具有优点:在应用程序中包括在AKA认证期间由UICC验证序列号的方法,并且可以根据商业操作者使用不同的方法。作为另一个示例,在AKA认证期间,可以根据AMF值不同地配置和使用认证算法和认证密钥(例如K值)。

[0132] 同时,这样的TLV可以包括用于NAA的个性化的配置值。这样的配置值的示例可以包括:诸如K值、OPc值等之类的加密密钥值,以及AKA算法参数值。AKA算法参数值可以包括配置值,诸如当验证序列号(SQN)值时使用的L值或增量值。此外,作为这样的配置值的示例,可以配置根据AMF值的算法标识符、根据AMF值的加密值等。

[0133] 返回来参考表1-1,简档包TLV的值数据可以包括加载文件包TLV。加载文件包TLV对应于包括用于由eUICC执行的一个或多个应用程序的安装文件和安装信息的TLV。表4图示加载文件包TLV的值部分的结构。

[0134] [表4]

[0135]

名称	M/O/C	标签	长度	值
加载文件	O	TBD	2字节～n字节	…
应用安装信息	M	TBD	2字节～n字节	…
…	…	…	…	…
应用安装信息	O	TBD	2字节～n字节	…

[0136] 参考表4,加载文件包TLV的值可以包括一个加载文件TLV和一个或多个应用安装信息TLV。加载文件TLV可以包括应用程序的一条或多条安装文件信息。应用安装信息TLV包括用于使用包括在加载文件TLV中的应用程序的安装文件或先前存储的安装文件来安装应用程序的信息。作为示例,该值可以包括安全域的AID值。

[0137] 返回来参考图2,PP可以生成简档包TLV,并且然后使用简档供应凭证加密生成的简档包TLV。此外,加密的简档包TLV可以使用对称密钥或认证证书私有密钥来签名。然后,PPC持有者可以将加密的简档TLV和加密的签名值发送到PMC持有者,并且PMC持有者可以将其发送到eUICC 220的简档管理器(如由附图标记270所指示)。简档服务器210可以将通过在可加密单元中加密的信息配置的简档包发送到eUICC 220。简档包可以被配置为在可加密单元中加密的m条信息。在可加密单元中加密的信息可以包括在可安装单元中划分的简档包信息。

[0138] 然后,eUICC 220简档管理器可以将其发送到简档容器。然后,简档容器可以接收它,并且然后使用签名值来验证数据是否被调制。当验证通过时,简档容器可以解码加密的

简档包TLV。接下来,简档容器使用简档包TLV内的文件结构TLV在简档容器内部生成文件结构。此外,简档容器可以使用简档包TLV内的加载文件包TLV在eUICC 220的存储地点中存储安装文件或加载文件,并且使用加载文件包TLV内的应用安装信息TLV安装来自加载模块的先前存储在简档容器内部的eUICC中的加载文件或应用。此外,简档容器可以使用NAA参数TLV安装NAA应用,或者生成NAA应用的实例。

[0139] 电子设备可以从简档服务器210接收在可加密单元中加密的简档包。电子设备可以在可发送到eUICC 220的单元中划分接收的简档包,并将划分的简档包发送到eUICC 220。eUICC 220可以接收在可发送单元中划分和加密的简档包信息。eUICC 220可以组合在可发送单元中划分的、在可加密或可解码单元中的简档包信息。可加密单元和可解码单元可以彼此相同。也就是说,通过在划分之前将信息与可加密单元中的简档包信息组合,eUICC 220可以解码在可发送单元中划分的信息。eUICC 220可以解码在可加密单元中组合的简档包信息。eUICC 220可以将解码的简档包信息识别为可安装单元中的信息,并且组合信息。eUICC 220可以开始在可安装单元中安装简档包信息。也就是说,当包括可安装单元中的简档包信息作为解码结果时,eUICC 220可以开始优先安装关于在可安装单元中的简档包信息的简档包。在解码的信息内排除可安装单元中的简档包信息的剩余信息可以存储在缓冲器中。eUICC 220另外接收可发送单元中的简档包信息,在可加密单元中组合可发送单元中的简档包信息,并且解码组合的信息。eUICC 220组合关于简档的解码的信息和存储在缓冲器中的剩余简档包信息,并且识别可安装单元中的简档包信息。eUICC 220优先在可安装单元中安装简档包信息,并在缓冲器中存储剩余的简档包信息。

[0140] 此外,简档包TLV可以包括NAA应用本身。在这种情况下,eUICC 220可以确定是使用先前存储的NAA应用还是使用包括在简档TLV中的NAA应用。作为示例,当NAA应用被包括在简档包TLV中时,eUICC 220可以优先使用对应的NAA应用。作为另一个示例,简档TLV可以包括可以通过其选择NAA应用的标识符信息,并且eUICC 220可以使用所述值确定是使用包括在简档TLV中的NAA应用还是使用先前存储的NAA应用。

[0141] 此外,eUICC 220可以使用简档包TLV中的附加TLV值来执行附加个性化。作为示例,eUICC 220可以使用简档包TLV内的数据来配置PIN值和PUK值。

[0142] 图3图示根据本公开的实施例的发送简档包TLV的过程。首先,可以在简档服务器中生成简档包TLV。为方便起见,简档包TLV的数据的尺寸被称为N。作为示例,N可以是几百K字节。此后,简档服务器可以使用简档供应凭证加密简档包TLV,并且如果必要的话包括用于完整性检查的签名值。通常,加密的数据的尺寸可以等于或稍微大于纯文本数据的尺寸。此时,在本实施例中假设大小彼此相等。此后,PP将加密的简档包TLV发送到PM。此后,在简档服务器与eUICC之间使用加密通信安全地发送数据,该加密通信使用eUICC与PM之间的PMC凭证。图3将该过程图示为PM隧道。eUICC可以将简档包TLV存储在用于存储加密的简档包TLV的存储地点中。为方便起见,这被称为eUICC缓冲器1。eUICC缓冲器1的大小最小等于或大于N。此后,eUICC解码简档包TLV,并且然后将纯文本简档包TLV存储在临时存储地点中。为方便起见,存储地点被称为eUICC缓冲器2。eUICC缓冲器2的尺寸最小等于或大于N。此后,eUICC可以在简档容器中使用纯文本简档包TLV安装简档。

[0143] 由于上述方法将整个简档数据完全发送到eUICC,并且然后解码简档数据,所以可以识别:除了存储地点之外,具有大于存储地点的尺寸的两倍的尺寸的缓冲存储地点是必

要的。此外,甚至当纯文本简档包TLV数据中存在错误时,eUICC也可以仅仅在将整个数据发送到eUICC并且然后被解码之后发现该错误,使得预测很多不便。作为示例,消耗几分钟的时间以将简档数据发送到eUICC,并且当简档被下载时,即使在对应的简档包TLV中存在错误,也消耗几分钟的时间来发现错误并由eUICC发送错误消息。

[0144] 图4图示根据本公开的实施例的划分和发送简档包的方法。参考图4,可以在简档服务器中生成简档包TLV。为方便起见,简档包TLV的数据的尺寸被称为N。作为示例,N可以是几百K字节。

[0145] 简档服务器可以将简档包TLV划分为m个部分以生成m个简档包TLV,并且使用简档供应凭证加密它们中的每一个。当将简档包划分为m个部分时,简档服务器可以将简档包划分为可安装在eUICC中的单元中的信息。简档服务器可以在可发送单元中加密已经被划分为m条可安装信息的简档包。为方便起见,加密和划分的简档包TLV的数据的尺寸被称为n。作为示例,当N为100K字节并且m为10时,n可以是10K字节。此后,PP可以将m个加密和划分的简档包TLV发送到PM。然后,简档服务器可以逐个将加密和划分的简档包TLV发送到eUICC,或者可以将简档包TLV一起发送。当简档包TLV被逐个发送时,用于存储加密的简档包TLV的eUICC缓冲器1的尺寸最小等于或大于n。此后,eUICC解码简档包TLV,并且然后将纯文本简档包TLV存储在临时存储地点中。为方便起见,存储地点被称为eUICC缓冲器2。此后,eUICC获取关于划分的纯文本简档包TLV的信息。此后,eUICC可以使用关于划分的简档包TLV的信息安装整个简档的一部分,或者可以在划分的简档包TLV彼此合并以生成一个简档包TLV之后安装简档。eUICC可以接收在可发送单元中划分的简档包信息,并且在可加密单元中组合划分的简档包信息。eUICC可以解码在可加密单元中组合的信息。当作为解码在可加密单元中组合的简档包信息的结果而包括可安装单元中的简档包信息时,eUICC可以在可安装单元中安装简档包信息。排除可安装单元中的简档包信息的剩余信息可以存储在缓冲器中。eUICC另外接收在可发送单元中划分的简档包信息,并且如上在可加密单元中组合和解码另外接收的信息。eUICC可以组合解码的简档包信息和存储在缓冲器中的剩余信息,并将组合的信息识别为可安装单元中的信息。eUICC开始在可安装单元中安装简档包信息,并将剩余的简档包信息存储在缓冲器中。在接收划分的简档信息之后,eUICC在接收关于划分的简档的信息之后验证TLV信息。当在TLV信息中发现错误时,eUICC可以在整个简档包TLV之中选择整个简档包TLV或划分的简档包TLV中的一些,并请求其重新传输。作为示例,这样的验证TLV的方法可以包括下面的方法:

[0146] -当包括未识别出的标签时,识别出存在错误;

[0147] -当值区域与长度的尺寸相比短或大时,识别出存在错误;

[0148] -当值的范围对应于未认别出的值时,识别出存在错误。

[0149] 同时,如图4中所图示,当划分和发送简档包TLV时,与其中简档包TLV在如图3中所图示地未被划分的同时被发送的情况相比,可以减小eUICC缓冲器1的尺寸。作为示例,当m=10时,eUICC缓冲器1的尺寸可以减小到1/10。

[0150] 如图4中所图示,当简档包TLV被划分和发送时,eUICC应当能够识别出:对应的简档包TLV被划分并且能够识别出简档包TLV被划分的数量以及划分的简档包TLV的顺序序列。

[0151] 参考表1-2,为了表达关于划分的简档包TLV的信息,在本公开的实施例中,拆分数

量TLV和拆分总数量TLV可以被可选地添加到简档包TLV的Value(值)部分。

[0152] 拆分数量TLV表示划分的简档包TLV的总数量(图4中的m值),并且拆分数量TLV指示包括在整个划分的简档包TLV之中的对应的拆分数量TLV的特定的划分的简档包TLV的顺序序列。当接收拆分数量TLV和拆分总数量TLV时,eUICC可以识别出与划分的简档包TLV相同的简档包TLV,并且在图4的方法中将其进行处理。

[0153] 作为示例,eUICC可以解码加密和划分的简档包TLV,识别在划分的简档包TLV内的拆分数量TLV,将识别的拆分数量TLV存储在eUICC缓冲器2中,将多个划分的简档包TLV存储在eUICC缓冲器2中,并且然后将它们合并成在划分之前的简档包TLV。合并可以包括下面的方案:

[0154] -数据内容可以简单和连续地彼此附连;

[0155] -数据内容可以以拆分数量TLV的次序简单和连续地彼此连接。

[0156] 作为示例,eUICC应当接收整个m个划分的简档包TLV(即,当拆分总数量为m时)。此时,当未接收到划分的简档包TLV中的一些时,eUICC可以请求将对应的TLV数据重新传输到PM。

[0157] [表1-2]

[0158]

名称	M/O/C	标签	长度	值
拆分数量	O	TBD	TBD	
拆分总数量	O	TBD	TBD	
…				

[0159] 图5图示根据本公开的实施例的发送划分的简档包的方法。首先,参考图5中的510,如表1-2中所表示,整个简档包TLV的划分数量(拆分总数量TLV)以及指示划分的简档包TLV的顺序序列的拆分次序编号包括在简档包TLV中,并且可以被使用APDU消息发送到eUICC。可能的是:划分数量和拆分次序编号稍微有变化,并且以不是APDU消息而是另一个消息的形式发送。例如,可以通过使用BIP通信而使用HTTPS协议发送TLV数据。

[0160] 参考图5中的520,整个简档包TLV的划分数量(拆分总数量TLV)以及指示简档包TLV的顺序序列的拆分次序编号不包括在简档包TLV中,并且对应的信息可以在被包括在用于发送简档包TLV的消息中的同时与划分的简档包TLV一起被发送。作为示例,当使用APDU命令时,可以在分别在P1字节和P2字节中包括拆分次序编号和拆分总数量的同时发送信息。作为另一示例,可能的是:以不是APDU消息而是另一个消息的形式发送划分数量和拆分次序编号。例如,当TLV数据在被包括在HTTP消息中的同时而被通过使用BIP通信、使用HTTPS协议发送时,划分信息可以与TLV一起被发送。

[0161] 当简档被完全安装时,eUICC可以存储一个或多个简档。此时,当激活特定简档时,可以由具有安装到其的eUICC的移动通信UE使用对应的简档来使用移动通信功能。

[0162] 图6图示根据本公开的实施例的生成和加密简档包的过程。

[0163] 参考图6,附图标记610对应于简档包。附图标记620对应于在可安装单元中划分的一组简档包信息。在图6中,简档包610可以被划分为可安装单元中的5条简档包信息。简档服务器可以将简档包610划分为可安装单元中的简档包信息。可以与其它划分的简档包信息分开地在eUICC中分别安装在可安装单元中的简档包信息621、622、623、624和625。例如,当eUICC接收到简档包信息621的全部和简档包信息622的一部分时,eUICC可以在可安装单

元中安装简档包信息621,而不管简档包信息622的未接收的剩余信息。

[0164] 在图6中,附图标记630是在可加密单元中配置的一组简档包信息631、632和633。可加密单元中的简档包信息可以通过在可安装单元中划分的简档包信息的组合来配置。例如,可加密单元中的简档包信息631可以包括在可安装单元中的简档包信息之中的简档包信息621的全部和简档包信息622的一部分。可加密单元中的简档包信息632可以包括在可安装单元中的简档包信息之中的简档包信息622之中的未包括在简档包信息631中的剩余信息,并且可以包括简档包信息623的全部和简档包信息624的一部分。可加密单元中的简档包信息633可以包括在可安装单元中的简档包信息之中的简档包信息624之中的未包括在简档包信息632中的剩余信息,并且可以包括简档包信息625的全部。

[0165] 简档服务器可以加密和发送可加密单元中的简档包信息631、632和633。简档服务器可以加密可加密单元中的每个简档包信息,并将加密的简档包信息发送到包括eUICC的电子设备。

[0166] 电子设备可以接收在可加密单元中发送的简档包信息631、632和633。电子设备可以在可发送单元中划分可加密单元中的接收的简档包信息631、632和633,并将划分的简档包信息发送到eUICC。eUICC可以将在可发送单元中划分的简档包信息组合到可加密单元中的信息。也就是说,eUICC可以将在可发送单元中划分的简档包信息分别组合到简档包信息631、632和633。当简档包信息631、632和633已经被加密时,eUICC可以解码简档包信息631、632和633。eUICC可以将解码的信息识别/组合为/成可安装单元中的简档包信息。当在可安装单元中存在简档包信息621、622、623、624和625时,eUICC可以开始优先在可安装单元中安装获取的简档包信息。eUICC可以解码可安装单元中的简档包信息621的全部和可安装单元中的简档包信息622的一部分。

[0167] 例如,当可加密单元中的简档包信息631被解码时,eUICC可以在可安装单元中安装在简档包信息之中的对应于简档包信息621的信息。由于未获取简档包信息622的全部,并且仅仅获取可安装单元中的简档包信息的一部分,所以eUICC可以在缓冲器中存储在解码的信息之中的对应于简档包信息622的信息。接下来,eUICC可以解码简档包信息632。当解码简档包信息632时,可以解码在简档包信息622之中的未包括在简档包信息631中的信息、简档包信息623的全部和简档包信息624的一部分。通过组合存储在缓冲器中的简档包信息622的一部分和通过解码获取的简档包信息622的一部分,eUICC可以获取简档包信息622的全部和简档包信息623的全部。由于简档包信息622的全部和简档包信息623的全部被获取,所以eUICC可以安装简档包信息622和623。由于未获取简档包信息624的全部,所以可以在缓冲器中存储通过解码简档包信息634获取的简档包信息624的一部分。以这种方式,eUICC可以接收在可发送单元中划分和发送的信息,将接收的信息组合和解码到可加密单元中的信息,并将解码的信息识别/组合为/成可安装单元中的信息,从而安装简档包。

[0168] 图7图示根据本公开的实施例的发送和安装简档包的方法。在图7中,UE是包括eUICC或UICC的电子设备的实施例。在图7中,UE对应于包括eUICC或UICC的UE。下面的操作可以由UE的UICC或eUICC执行。

[0169] 在操作730中,简档服务器710可以生成简档包。简档包可以是具有TLV形式的简档包。将参照图6描述图7的实施例中的简档包的结构。简档服务器710可以在可安装单元中生成简档包信息621、622、623、624和625。简档服务器710可以在可安装单元中划分生成的简

档包信息,并且当生成简档包信息时可以在可安装单元中划分地生成简档包信息。

[0170] 在操作735中,简档服务器可以将可安装单元中的简档包信息重新配置为可加密单元中的简档包信息。可加密单元中的简档包信息631、632和633可以通过在可安装单元中划分的简档包信息的组合来配置。简档服务器710可以在可发送单元中加密和发送简档包信息631、632和633。简档服务器可以加密加密单元中的简档包信息631、632和633中的每一个。

[0171] 在操作740中,简档服务器710可以将简档包信息发送到UE 720。在UE 720中,简档服务器710可以在可发送单元中配置并将加密的简档包信息631、632和633发送到UE 720的eUICC。当通过m条可发送简档包信息配置简档包信息的全部时,可以执行操作740,直到发送了可加密单元中的m条简档包信息的全部。

[0172] UE 720可以接收简档包信息。简档包信息可以被加密。UE 720可以将接收的简档包信息发送到UE 720的eUICC。UE可以在可发送单元中划分加密的简档包信息631、632和633,并将划分的简档包信息发送到eUICC。

[0173] eUICC可以组合在可发送单元中划分的简档包信息,并且可以在可加密单元中配置简档包信息。

[0174] 在操作745中,UE的eUICC可以解码加密的简档包信息631、632和633。为了在eUICC中安装简档,简档服务器和UE 720或eUICC可以执行密钥协议的相互认证过程。简档包信息可以包括生成用于解码由eUICC加密的简档包信息的加密密钥所必需的参数。eUICC可以从简档包信息提取用于生成加密密钥所必需的参数,在提取的参数的基础上生成加密密钥,并且然后使用生成的加密密钥执行解码操作。

[0175] 当解码接收的简档包信息631时,可以解码可安装单元中的简档包信息621的全部和可安装单元中的简档包信息的一部分。在操作750中,UE 720可以使用解码的信息处理可安装单元中的简档包信息。当获取可安装单元中的简档包信息时,UE可以安装可安装单元中的获取的简档包信息。例如,当可加密单元中的简档包信息631被接收和解码时,eUICC可以安装在可安装单元中的简档包信息之中的对应于简档包信息621的信息。eUICC可以存储在解码的信息之中的对应于简档包信息的信息到缓冲器中。

[0176] 在操作755中,UE 720可以确定是否完全安装简档包信息。当安装未被完全执行时,过程可以继续进行到操作740、745和750。当简档包信息未被完全接收时,过程可以继续进行到操作740,当简档包信息未被完全解码时,继续进行到操作745,并且当简档包信息被完全接收和解码但未被完全安装时,继续进行到操作750。同时,当在接收的简档包信息中存在错误时,UE可以请求简档服务器710重新发送对应的信息。在本公开的实施例中,由于简档服务器710分开发送可发送单元中的简档包信息,所以当特定信息中存在错误时,简档服务器710可以仅仅重新发送在其中已经发生错误的简档包信息,而不重新发送简档包信息的全部。

[0177] 当简档包信息被完全安装时,UE 720可以终止安装相关的操作。在操作760中,UE可以向简档服务器710发送简档包安装完成消息。

[0178] 图8图示在选择简档和简档的文件结构之后激活简档的方法。

[0179] 参考图8,可以在eUICC平台中安装个人简档。此时,单个简档的文件结构可以包括一个MF文件。eUICC平台可以做出选择,以由UE示出在多个简档之中的一个简档。eUICC平

台、UE或SM-SR可以选择简档中的一个。当UE选择简档时,eUICC可以立即执行从UE接收的命令。否则,当简档由UE选择时,eUICC可以验证签名值并执行从UE接收的命令,而不立即执行命令。这样的签名值可以按下面的方案处理:

[0180] -在使用对称密钥的签名值的情况下,使用对称密钥验证签名值;

[0181] -在使用RSA认证证书的私有密钥的签名值的情况下,使用RSA公开密钥来验证签名值;

[0182] -在使用ECC认证证书的私有密钥的ECDSA签名值的情况下,使用ECC认证证书的公开密钥验证ECDSA签名。

[0183] 同时,存储在PP中的简档的格式可以具有下面的结构。对应的格式可以被转换为简档包TLV或远程APDU的形式,以便将简档下载到eUICC。

[0184] 表5描述了简档包的内容。简档包可以包括表5的内容的全部或一部分。

[0185] [表5]

[0186]

项	功能	状态	值类型
卡简档			
报头		M	
模板信息	该部分描述将捕获关于框架的细节的所有属性	M	
模板版本	参考已经根据哪个框架版本产生该文件。 值：1.0	M	可变串
…			
SIMCardProfileReference	简档参考信息	M	
MobileCountryCode	移动国家代码	M	3 INT
MobileNetworkCode	移动网络代码	M	3 INT
…			
…			
CardBody			
MF_DF		R	
文件名称	MF 或 DF 的名称	M	可变串
文件类型	ENUM 值：对于 MF 是 '00'，对于 DF 是 '11'	M	ENUM
…			
ADF		O/R	
文件名称	ADF 的名称。	M	可变串
文件类型	ENUM 值：对于 USIM 是 '00'	M	ENUM
EF		O/R	
文件名称	EF 的名称	M	可变串

[0187]

…		
Card_Management		M	
认证	定义认证所需的要求	M	
Authentication3G		O/R	
Authentication3GAlgorithm	认证算法：ENUM 值：对于 MILENAGE 是‘ 00’，对于 TUAK 是‘ 01’	O/R	ENUM
Authentication3GSeqNb	链接到根据 TS 33.102 激活与否的认证的序号	O	布尔(是或否)
Authentication3GFreshnessTest	定义是否根据 TS 33.102 激活新鲜度测试与否	O	布尔(是或否)
Authentication3GAgeLimitTest	定义是否根据 TS 33.102 设置年代限制测试与否	O	布尔(是或否)
Authentication3GWrapAroundProtection	定义是否根据 TS 33.102 设置保护回绕与否	O	布尔(是或否)
Authentication3GDeltaValue	用于根据 TS 33.102 的回绕的增量的值	C	可变十六进制
Authentication3G_L_Value	用于根据 TS 33.102 的年代	C	可变十六进制

					限制的 L 的值		

[0188]

				Authentication3G_SQN_Index	根据 TS 33.102 的 SQN 阵列的长度(默认：32)	C	可变十六进制
				Authentication3GRESLength	用于 TUAK 的 RES 长度的值 ENUM 值：对于 64 是‘ 00’ ，对于 128 位是‘ 01’	C	ENUM
				Authentication3G_Ri_Ci_ValueType	用于 MILENAGE 的 MNO 特定配置 ENUM 值：对于根据 TS 35.206 的默认 Ri 和 Ci 值是‘ 00’ ，对于 MNO 特定 Ri 和 Ci 值是‘ 01’	C	ENUM
				Authentication3G_R1	MNO 特定 r1 值	O	INT
				Authentication3G_R2	MNO 特定 r2 值	O	INT
				Authentication3G_R3	MNO 特定 r3 值	O	INT
				Authentication3G_R4	MNO 特定 r4 值	O	INT
				Authentication3G_R5	MNO 特定 r5 值	O	INT
				Authentication3G_Ci	MNO 特定 ci 值 值：与以十六进制格式的 c1、c2、c3、c4 和 c5 拼接	O	十六进制的 80
				Authentication3G_TUAK_Iteration	根据 TS 35.231 的 Keccak 置换的迭代的数量	O	INT
				Authentication3G_K	用于 MILENAGE 或	M	十六进

					TUAK 的 128 位		制的 16
				Authentication3G_OP	根据 3GPP TS 35.206，MILENAGE OP	C	十六进制的 16
				Authentication3G_OPc	根据 3GPP TS 35.206，MILENAGE OPc	C	十六进制的 16
				Authentication3G_TOP	根据 3GPP TS 35.206，TUAK TOP	C	十六进制的 32
				Authentication3G_TOPc	根据 3GPP TS 35.206，TUAK TOPc	C	十六进制的 32
				…			
			…				
		…					

[0189]

应用			为了捕获关于安装在卡上的应用、AID 结构、小程序状态的细节。	M	
	RFM 应用			O/R	
		TAR	工具包应用参考	M	十六进制的 3
		…			
	RAM 应用			O/R	
		TAR	工具包应用	M	十六进制的 3
		…			
小程序					
	…				

[0190] 注释:参数应当被进一步分类和添加到该表中,以完整地描述简档。

[0191] 注释:状态的值(M:强制的,O:可选的,C:有条件的,R:可重复的)。

[0192] 根据每个AMF值,简档可以包括分离的NAA算法的类型、NAA算法的参数和NAA密钥值(例如,对于USIM是K和对于SIM是K)。在这种情况下,根据每个AMF,eUICC可以执行NAA应

用程序以对应于分离的NAA算法的类型、NAA算法的参数和NAA密钥值(例如,对于USIM是K和对于SIM是K)。

[0193] 图9图示用于在eSIM简档内执行USIM的认证的AKA认证过程。

[0194] 当安装在简档中的NAA对应于USIM时,可以执行AKA认证过程。

[0195] NAA可以在被包括在简档中的同时被发送,或者可以先前存在于eUICC平台中。

[0196] 当NAA包括在简档中时,对应的NAA不执行图9的f1功能、f2功能、f3功能和f4功能,并且可以被实现成调用在eUICC平台中执行的功能。此外,当调用f1功能、f2功能、f3功能和f4功能时,eUICC可以选择和使用从UE发送的对应于AMF字段的参数。例如,eUICC可以选择和使用根据AMF值的认证加密密钥(K)值。作为另一个示例,eUICC可以使用根据AMF值的不同的认证算法配置值(例如MILENAGE算法的r1-r5、c1-c5等)。

[0197] 在图9中,用于验证SQN是否被包括在正确范围中的逻辑可以在被包括在简档信息中的同时被下载。对应的逻辑可以被包括在排除f1功能、f2功能、f3功能和f4功能的NAA应用中。

[0198] 图10至13图示根据本公开的附加实施例的发送简档信息的操作。

[0199] 参考图10,首先,简档服务器可以配置以简档包TLV形式构成简档的信息。简档服务器可以通过在可安装单元中划分简档包信息来配置简档包信息。

[0200] 简档包TLV包括在被发送到UE的eUICC之后可以通过其在eUICC中安装简档的信息。

[0201] 简档服务器可以在具有APDU形式的消息中包括简档包TLV。通常,可以包括在APDU中的数据具有最大255字节的尺寸,并且简档包TLV具有几十kB到几百Kb的尺寸。因而,当简档包TLV包括在APDU中时,在其中划分简档包TLV的状态下,简档包TLV被包括在单独的APDU中。APDU可以是用于简档包的可发送单元。

[0202] 可以在发送过程或先前的步骤中加密划分的APDU。简档服务可以在可发送单元中加密简档包信息,并且然后在APDU中包括加密的简档包信息。简档服务器可以将加密的APDU或者包括加密的简档包信息的APDU从PP发送到PM。此时,可以使用诸如VPN和IPSEC之类的通信信道安全性方案来额外保护数据。此外,PP可以在将APDU数据发送到AP之前与eUICC执行相互认证过程。这样的相互认证过程将如下:

[0203] -基于ECC认证证书执行认证;

[0204] -基于ECC认证证书通过ECKA过程生成对称密钥,并且然后基于生成的对称密钥执行认证;

[0205] -基于RSA认证证书执行相互认证;

[0206] -当基于RSA认证证书执行相互认证时,生成对称密钥,并且然后基于生成的对称密钥执行认证;

[0207] -在RSA认证证书的基础上加密生成的对称密钥,发送加密的对称密钥,并且然后由PP基于相互密钥执行相互认证。

[0208] 简档服务器可以通过与eUICC的TLS握手来生成TLS通信信道。可以使用RSA认证证书或先前存储的对称密钥执行这样的TLS握手。

[0209] 在其中简档包TLV包括在HTTP消息中的状态下,简档服务器可以使用TLS通信信道将加密的简档包TLV或者划分和加密的简档包TLV发送到UE。此时,简档包TLV在被包括在

HTTP消息中的同时被发送的实现方式仅仅对应于实现方式的示例,并且简档包TLV可以在被包括在另一个通信协议中的同时被发送。

[0210] 例如,简档包TLV可以被发送到UE的MODEM(调制解调器)单元。在其中IP分组被包括在TERMINAL RESPONSE(终端响应)APDU消息中的状态下,UE的MODEM单元可以将接收的IP分组发送到eUICC。为此,简档服务器可以预先使用SMS消息生成与eUICC的独立承载协议信道。SMS消息可以包括加密的PUSH(推)ADPU命令。SMS消息可以在被包括在ENVELOPE(信封)APDU中的同时被从UE的MODEM单元发送到eUICC,并且PUSH APDU命令可以在包括在ENVELOPE消息中的SMS消息内的加密的PUSH APDU命令被解码之后被处理。

[0211] eUICC可以在处理PUSH APDU之后使用OPEN CHANNEL(开信道)主动式(proactive)命令生成BIP信道。TERMINAL RESPONSE(终端响应)可以是下述APDU命令,通过该APDU命令将存储在UE的MODEM单元的接收缓冲器中的IP分组发送到eUICC。此时,TERMINAL RESPONSE可以是从eUICC发送的RECEIVE DATA(接收数据)主动式命令。通常,由于TERMINAL RESPONSE APDU中的数据的尺寸在255字节内,所以可以发送TERMINAL RESPONSE APDU几次,以便发送具有大于255字节的尺寸的数据。

[0212] eUICC可以立即处理通过接收TERMINAL RESPONSE发送的数据,并在接收多个TERMINAL RESPONSE之后一起处理接收的数据。详细地,可以通过聚合包括在多个TERMINAL RESPONSE中的数据来恢复HTTP消息。当HTTP被恢复时,eUICC使用报头区域中的AID值或TAR值提取在HTTP消息的正文文本中的加密的APDU命令,并且然后将加密的APDU命令发送到安全性域、简档域或者对应于AID值或TAR值的应用。然后,安全性域(或者简档域或应用)可以解码并且然后处理加密的APDU命令。

[0213] 当加密的APDU消息包括在HTTP消息中时,如果用户想要以STRING形式表达加密的APDU消息,则用户可以使用下面的方案:

[0214] -将通过以十六进制形式转换APDU二进制数据获得的值转换为字符串:在这种情况下,十六进制数据的1给字节被转换为两个字符,包括在最终http消息中的数据的尺寸可以增加两倍;

[0215] -APDU二进制数据被Base-64编码以转换为字符串:在这种情况下,数据的尺寸可以增加约33%。

[0216] 如上,当APDU命令被以STRING(串)形式转换并被发送时,在终端与eUICC之间发送的消息的量增加两倍,从而大大增加在其间下载简档的时间段。因而,优选的是:APDU命令不被转换为字符串并且以二进制数据形式发送。

[0217] eUICC解码接收的APDU。当作为解码结果而包括可安装单元中的简档包信息时,eUICC可以在可安装单元中安装简档包信息。排除关于可安装单元中的简档包的信息的剩余信息可以被存储在缓冲器中。eUICC可以另外接收APDU,并且解码APDU。除了存储在缓冲器中的剩余数据之外,eUICC还可以使用接收的APDU的解码信息在可安装单元中安装简档包信息。

[0218] 参考图11,首先,简档服务器可以配置以简档包TLV形式构成简档的信息。

[0219] 简档包TLV包括下述信息,通过该信息,简档可以在被发送到eUICC之后被安装在eUICC中。

[0220] 简档服务器可以照原来的样子加密简档包TLV。否则,PP可以将简档包TLV划分为

几个部分,并且然后将其加密。简档服务器可以将简档包TLV划分为可安装单元和/或可发送单元中的简档包信息,并且加密划分的简档包信息。

[0221] PP可以将加密的简档包TLV发送到PM。此时,可以使用诸如VPN和IPSEC之类的通信信道安全性方案来额外保护数据。此外,PP可以在将加密的简档包TLV发送到PM之前执行与eUICC相互认证过程。这样的相互认证过程将如下:

[0222] -基于ECC认证证书执行认证;

[0223] -基于ECC认证证书通过ECKA过程生成对称密钥;并且然后基于生成的对称密钥执行认证;

[0224] -使用RSA认证证书执行相互认证;

[0225] -当基于RSA认证证书执行相互认证时,生成对称密钥,并且然后基于生成的对称密钥执行认证;

[0226] -使用RSA认证证书加密生成的对称密钥,发送加密的对称密钥,并由PP使用发送的对称密钥执行相互认证。

[0227] PM可以通过与eUICC的TLS握手一起生成TLS通信信道。可以使用RSA认证证书或先前存储的对称密钥执行这样的TLS握手。

[0228] 简档服务器可以在HTTP消息中包括一个APDU消息或多个APDU消息,并且使用TLS通信信道将HTTP消息发送到UE。例如,简档包TLV可以被发送到UE的MODEM单元。在其中IP分组被包括在TERMINAL RESPONSE APDU消息中的状态下,UE的MODEM单元可以将接收的IP分组发送到eUICC。为此,PM可以预先使用SMS消息生成与eUICC的独立承载协议信道。SMS消息可以包括加密的PUSH ADPU命令。SMS消息可以在被包括在ENVELOPE APDU中的同时被从UE的MODEM单元发送到eUICC,并且PUSH APDU命令可以在包括在ENVELOPE消息中的SMS消息内的加密的PUSH APDU命令被解码之后被处理。eUICC可以在处理PUSH APDU之后使用OPEN CHANNEL主动式命令生成BIP信道。TERMINAL RESPONSE可以是下述APDU命令,通过该APDU命令将存储在UE的MODEM单元的接收缓冲器中的IP分组发送到eUICC。此时,TERMINAL RESPONSE可以是从eUICC发送的RECEIVE DATA主动式命令。通常,由于TERMINAL RESPONSE APDU中的数据的尺寸在255字节内,所以可以发送TERMINAL RESPONSE APDU几次,以便发送具有大于255字节的尺寸的数据。

[0229] eUICC可以立即处理通过接收TERMINAL RESPONSE发送的数据,并且在接收多个TERMINAL RESPONSE之后一起处理接收的数据。详细地,可以通过聚合包括在多个TERMINAL RESPONSE中的数据来恢复HTTP消息。当HTTP被恢复时,eUICC可以使用报头区域中的AID值或TAR值提取在HTTP消息的正文文本中的加密的简档包TLV,并且然后将加密的简档包TLV命令发送到安全性域、简档域或者对应于AID值或TAR值的应用。然后,安全性域(或者简档域或应用)可以解码加密的简档包TLV,并且然后使用解码的简档包TLV安装简档。

[0230] 当简档包TLV被包括在HTTP消息中时,如果用户想要以STRING形式表达简档包TLV,则用户可以使用下面的方案:

[0231] -将通过以十六进制形式变换APDU二进制数据获得的值转换为字符串:在这种情况下,1字节的十六进制数据被转换为两个字符,并且因而最终包括在http消息中的数据的尺寸可以增加两倍;

[0232] -APDU二进制数据被Base64编码以被转换为字符串:在这种情况下,数据的尺寸可

以增加达33％。

[0233] 如上,当简档包TLV被以STRING形式转换并被发送时,在UE与eUICC之间发送的消息的量增加两倍,从而大大增加在其间下载简档的时间段。因而,优选的是:简档包TLV不被转换为字符串并且被以二进制数据形式发送。

[0234] 参考图12,首先,简档服务器可以配置以APDU形式构成简档的信息。APDU可以是简档包的可发送单元,并且可以包括可安装单元中的简档包信息。

[0235] PP可以在发送过程或先前的步骤中加密APDU。简档服务可以加密可发送单元中的简档包信息,并且然后在APDU中包括加密的简档包信息。简档服务器可以将加密的APDU或者包括加密的简档包信息的APDU从PP发送到PM。此时,可以使用诸如VPN和IPSEC之类的通信信道安全性方案来额外保护数据。此外,PP可以在将APDU数据发送到AP之前执行与eUICC的相互认证过程。这样的相互认证过程将如下:

[0236] -基于ECC认证证书执行认证;

[0237] -基于ECC认证证书通过ECKA过程生成对称密钥,并且然后基于生成的对称密钥执行认证;

[0238] -使用RSA认证证书执行相互认证;

[0239] -当基于RSA认证证书执行相互认证时,生成对称密钥,并且然后基于生成的对称密钥执行认证;

[0240] -使用RSA认证证书加密生成的对称密钥,发送加密的对称密钥,并且然后由PP使用发送的对称密钥执行相互认证。

[0241] 简档服务器可以通过与eUICC的TLS握手生成TLS通信信道。可以使用RSA认证证书或先前存储的对称密钥执行这样的TLS握手。

[0242] PM可以将加密的APDU发送到UE的AP。当PM与eUICC直接通信时,可以降低通信成功的概率,并且因而通过诸如3G通信或LTE通信之类的高速通信将数据稳定地下载到UE的AP上,并且然后经由MODEM或直接将APDU消息从UE的AP发送到eUICC。

[0243] 在这种情况下,由于ETSI TS102.226远程应用管理(RAM)应用或远程文件管理(RFM)应用不可以处理待发送到UE的消息,所以在eUICC中分离地需要用于处理从UE接收的消息并安装文件系统和应用的专用简档安装应用。为方便起见,用于安装简档的APDU可以是简档下载消息。简档下载消息的报头可以包括CLA字节、INS字节、P1字节和P2字节。

[0244] 此外,UE可以在发送包括简档信息的APDU之前将简档下载APDU或另一个APDU消息发送到eUICC,并且在其中APDU包括下述信息的状态下将APDU发送到eUICC,该信息关于包括简档信息的APDU由哪个安全性域或简档域或应用处理。此外,即使当另一个应用程序存在于eUICC中时,APDU消息也可以使用使用CLA字节的不同于0的值的逻辑信道发送简档。

[0245] 同时,UE可以使用简档下载APDU将简档信息发送到eUICC,并且然后另外将分离的APDU命令发送到eUICC,从而安装简档。

[0246] 在以上方法中,由于APDU在被包括在HTTP消息中的同时不被发送,所以不必将APDU命令转换为字符串,并且由于直接发送具有二进制形式的APDU消息,所以其效率增加达33％-100％。

[0247] 参考图13,首先,简档服务器可以生成并且然后加密包括构成简档的信息的简档包TLV。此外,可以在其中以特定尺寸划分简档包TLV的状态下加密简档包TLV。简档服务器

可以将生成的简档包信息划分并生成可安装单元中的多个简档包信息。此外,简档服务器可以加密可加密单元中的简档包信息,该简档包信息包括可安装单元中的简档包信息。

[0248] 此外,简档服务器可以在发送过程或先前步骤中加密简档包TLV。

[0249] 简档服务器可以将加密的简档包TLV从PP发送到PM。此时,可以使用诸如VPN和IPSEC之类的通信信道安全性方案来另外保护数据。此外,PP可以在将简档包TLV发送到PM之前执行与eUICC的相互认证过程。这样的相互认证过程将如下:

[0250] -基于ECC认证证书执行认证;

[0251] -基于ECC认证证书通过ECKA过程生成对称密钥,并且然后基于生成的对称密钥执行认证;

[0252] -使用RSA认证证书执行相互认证;

[0253] -当基于RSA认证证书执行相互认证时,生成对称密钥,并且然后基于生成的对称密钥执行认证;

[0254] -使用RSA认证证书加密生成的对称密钥,发送加密的对称密钥,并且然后由PP使用发送的对称密钥执行相互认证。

[0255] 简档服务器可以将加密的简档包TLV发送到UE的AP。此时,简档服务器可以在其中简档包TLV被划分为APDU的状态下发送简档包TLV,或者可以使用应用协议发送简档包TLV。应用协议的示例可以对应于HTTP协议。当简档服务器与eUICC直接通信时,可以降低通信成功的概率,并且因而通过诸如3G通信或LTE通信之类的高速通信将数据稳定地下载到UE的AP,并且然后经由MODEM或直接将APDU消息从UE的AP发送到eUICC。

[0256] 在这种情况下,由于ETSI TS102.226远程应用管理(RAM)应用或远程文件管理(RFM)应用不可以处理待发送到UE的消息,所以在eUICC中分离地需要用于处理从UE接收的消息并且安装文件系统和应用的专用简档安装应用。为方便起见,用于安装简档的APDU可以是简档下载消息。简档下载消息的报头可以包括CLA字节、INS字节、P1字节和P2字节。

[0257] 此外,UE可以在发送包括简档信息的APDU之前将简档下载APDU或另一个APDU消息发送到eUICC,并且在其中APDU包括下述信息的状态下将APDU发送到eUICC,该信息关于包括简档信息的APDU由哪个安全性域或简档域或应用处理。此外,即使当另一个应用程序存在于eUICC中时,APDU消息也可以使用利用CLA字节的不同于0的值的逻辑信道发送简档。

[0258] 同时,UE可以使用简档下载APDU将简档信息发送到eUICC,并且然后另外将分离的APDU命令发送到eUICC,从而安装简档。

[0259] 在以上方法中,由于APDU在被包括在HTTP消息中的同时不被发送,所以不必将APDU命令转换为字符串,并且由于直接发送具有二进制形式的APDU消息,所以其效率增加达33%-100%。

[0260] 图14图示根据本发明的实施例的生成和安装eUICC的简档的过程。

[0261] 参考图14,在操作1450中,移动网络运营商(MNO)1410可以在简档被安装在具体UE 1440之前请求SM-DP 1420准备大量的简档。在操作1455中,SM-DP 1420可以生成并存储简档。此时,SM-DP 1420可以先前生成简档,存储简档ID(例如ICCID)、IMSI、K和OPc值,并将其提供给MNO 1410。然后,MNO 1410可以存储对应的信息,甚至在MNO服务器中。此后,MNO 1410可以请求SM-DP 1420将简档之中的一个简档下载到特定eUICC。在这种情况下,MNO 1410可以向SM-DP 1420发送可以通过其分类特定eUICC的EID值,以及可以通过其分类简档

的简档ID或ICCID值。此外,MNO 1410可以更新MNO服务器的数据值或配置信息,以允许使用存储在MNO服务器中的IMSI、K值、OPc值的UE 1440的接入,该UE 1440使用对应的简档请求网络接入。可以以HTTP消息或SOAP消息的形式发送由MNO 1410发送到SM-DP 1420的信息。

[0262] 此后,如在本公开的每个实施例中所述的,SM-DP 1420可以通过下载简档的过程来将简档安装在eUICC中。可以在操作1460和操作1465的基础上将简档包发送到UE 1440。UE的eUICC可以安装接收的简档包。通过允许MNO 1410从SIM制造商订购现有UICC卡并且向客户提供UICC卡,以上方法类似于先前准备现有UICC卡的程序,从而提供服务。同时,与物理SIM不同,eSIM简档可以被远程下载,并且因而事先不大量产生简档并实时发送信息是有效的。例如,当MNO 1410应当与多个SM-DP 1420交互工作时,更好的是:当如图15中所图示地将简档下载到单独的eUICC时,与其中先前在多个SM-DP中产生简档的情况相比,通过发送所需的信息来产生简档。

[0263] 参考图15,在操作1550中,MNO 1510可以将简档下载请求消息发送到SM-DP 1520,并且除了EID和简档ID(例如ICCID)之外,简档下载请求消息还可以包括IMSI、K值和OPc值。

[0264] 在操作1555中,SM-DP 1520可以实时地或在配置的时间使用信息生成简档,以实时地或在配置的时间下载简档。与MNO服务器和SM-DP 1520相关的示例可以对应于其中混合使用图6的操作方法和图7的操作方法的情况。作为示例,当从MNO 1510接收的简档下载请求消息包括IMSI、K值和OPc值时,SM-DP 1520可以使用对应的信息生成简档并下载简档,当从MNO接收的简档下载请求消息不包括IMSI、K值和OPc值并且仅仅包括EID值和ICCID值时识别是否存在先前生成的对应于ICCID或简档ID的简档,并且当识别出存在简档时使用对应的简档来下载简档。因而,为特定UE的大量发布做准备时,预先生成和下载简档,否则实时地下载简档。如上,两种类型的简档信息传送方案可以被彼此独立地使用,并且可以根据情况选择性地操作。在操作1560和操作1565的基础上,可以将简档包发送到UE 1540。UE 1540的eUICC可以安装接收的简档包。

[0265] 图16a和16b图示根据本公开另一实施例的发送和安装eUICC简档的过程。

[0266] 参考图16a和16b,为了安装简档,可以提供简档服务器1610和电子设备1620,并且可以提供包括在电子设备1620中或可以耦合到电子设备1620的eUICC 1625。

[0267] 在操作1650中,简档服务器1610可以准备简档包。简档服务器1610可以生成简档包。简档包可以具有TLV形式。具有TLV形式的简档包可以被称为简档包TLV。

[0268] 在操作1655中,简档服务器1610可以将准备的简档包划分为可安装单元中的信息。简档服务器1610可以准备简档包,在可安装单元中划分简档包信息,并且可以在生成简档包时在可安装单元中划分地生成简档包信息。即使在将可安装单元中的信息发送到eUICC 1625时不将整个简档包发送到eUICC 1625,作为被配置成安装在eUICC 1625中的信息的可安装单元中的信息也可以表示整个简档包的信息的一部分。

[0269] 在操作1660中,简档服务器1610可以在可加密单元中配置在可安装单元中划分的信息。可加密单元可以是预定尺寸。简档服务器可以将通过可安装单元中的m条信息配置的简档包重新配置为可加密单元中的n条信息。n和m可以彼此相等,或者可以彼此不同。关于在为每个可加密单元加密期间生成的数据,可以将用于可加密单元的完整性保证数据添加到通过加密可加密数据获得的数据。完整性保证数据可以是消息认证码。

[0270] 在操作1665中,简档服务器1610可以加密在可加密单元中重新配置的信息。

[0271] 在操作1670中,简档服务器1610可以将可加密单元中的加密的信息发送到电子设备1620。电子设备可以下载n条加密的信息。简档服务器1610可以将加密的信息划分为可发送单元中的信息,并将划分的信息发送到电子设备1620。此时,可发送单元可以对应于下述尺寸,其中已经接收简档包的电子设备可以以该尺寸将接收的简档包发送到电子设备1620的UICC。

[0272] 在操作1675中,电子设备1620可以将接收的简档包信息发送到嵌入其中或耦合到其的eUICC 1625。电子设备1620可以将接收的信息划分为可发送单元中的信息,并将划分的信息发送到eUICC 1625。当简档服务器1610划分和发送可发送单元中的信息时,接收的信息可以被照原来的样子发送到eUICC 1625。

[0273] 在操作1680中,eUICC 1625可以接收可发送单元中的划分和加密的简档包信息。eUICC 1625可以组合在可发送单元中、在可加密或可解码单元中划分的简档包信息。可加密单元和可解码单元可以彼此相同。也就是说,通过在划分之前将信息与可加密单元中的简档包信息组合,eUICC 1625可以解码在可发送单元中划分的信息。

[0274] 在操作1685中,eUICC 1625可以解码在可加密单元中组合的简档包信息。为了在eUICC 1625中安装简档,简档服务器和电子设备或eUICC 1625可以执行密钥协议的相互认证过程。简档包信息可以包括用于生成用于解码由eUICC加密的简档包信息的加密密钥所必需的参数。eUICC可以从简档包信息提取用于生成加密密钥所必需的参数,在提取的参数的基础上生成加密密钥,并且然后使用生成的加密密钥执行解码操作。

[0275] 在操作1690中,eUICC 1625可以将解码的简档包信息识别为可安装单元中的信息,并且组合识别的信息。eUICC 1625可以解码加密信息,并将解码的信息与存储在缓冲器中的信息组合,从而获取可安装单元中的简档包信息。

[0276] 在操作1695中,eUICC 1625在缓冲器中存储除了可安装单元中的简档包信息之外的剩余信息。通过将存储在缓冲器中的信息和稍后待解码的信息组合,存储在缓冲器中的信息可以用于获取可安装单元中的简档包信息。

[0277] 在操作1697中,eUICC 1625可以开始在可安装单元中安装简档包信息。在以上方法中,eUICC 1625可以首先开始在可安装单元中安装较早获取的简档包信息。

[0278] 当简档包未被完全安装时,过程继续进行到操作1675并重复以上操作。例如,当电子设备1620从简档服务器1610接收n条加密的信息时,过程可以重复执行操作1675至操作1697n次。同时,eUICC 1625可以通过并行执行操作1675至操作1697来缩短简档安装时间。在操作1675至操作1697中,eUICC 1625接收在可发送单元中划分的简档包信息,并将接收的信息组合到可加密单元中的信息。可以解码可加密单元中的组合的信息,并且可以为每个可安装单元安装简档。甚至在执行操作1675至操作1697的同时,也可以并行执行对新接收的信息的操作1675至操作1697。也就是说,在执行对于特定的第k个信息的操作1675至操作1697之后,可以执行对于(k+1)个信息的操作1675至操作1697。此外,在执行对于特定的第k个信息的操作1675至操作1697的同时,可以执行对于第(k+1)个信息的操作1675至操作1697。

[0279] 同时,可以根据存储在缓冲器中的信息的量来控制并行处理的操作。例如,当存储在缓冲器中的信息的量等于或大于预定值时,在并行处理中,终止解码操作,并且优先执行正在缓冲器中被处理的在可安装单元中的简档包信息,使得可以降低缓冲器值。当降低缓

冲器值时,重新开始解码操作,使得可以有效地操作系统。不终止并行处理,可以执行控制以使得解码速度更慢,并且使得用于安装单元中的简档包信息的安装速度更快。当存储在缓冲器中的在可安装单元中的简档包信息超过预定阈值时,以上操作可以如上所述地控制并行处理。也就是说,终止解码操作,或者使得解码速度更慢,直到缓冲器值(存储在缓冲器中的信息的量)变得等于或低于预定参考值。

[0280] 图17图示根据本公开的实施例的简档服务器。

[0281] 参考图17,简档服务器1700可以包括:从另一个节点接收信号或将信号发送到另一个节点的发送/接收单元1710,控制简档服务器的整体操作的控制器1730,以及存储简档和关于简档的信息的存储单元1720。

[0282] 根据本公开的实施例,控制器1730可进行控制以生成简档包,在可安装在电子设备的UICC中的单元中划分简档包,在可加密单元中重新配置划分的简档信息,并且将重新配置的简档信息发送到电子设备。

[0283] 此外,控制器1730可以进行控制以加密可加密单元中的简档信息。

[0284] 简档包可以通过在可安装单元中划分的n条简档信息配置,并且n条简档信息可以被重新配置为可加密单元中的m条简档信息。此外,简档包可以具有TLV形式。

[0285] 控制器1730可以控制根据如通过图1至15所述的本公开的实施例的简档服务器的操作。

[0286] 图18图示根据本公开的实施例的电子设备。

[0287] 参考图18,电子设备1800可以包括:从另一个节点接收信号以及将信号发送到另一个节点的发送/接收单元1810,以及控制电子设备1800的整体操作的控制器。此外,电子设备1800可以包括从简档服务器下载简档并安装下载的简档的UICC 1820。控制器1830可以控制UICC 1820的操作。电子设备1800可以是UE。UICC 1820可以包括用于在UICC中安装简档的处理器或控制器。

[0288] 控制器1830可以进行控制以从简档服务器接收构成简档包的在可加密单元中的第一简档信息,并将可加密单元中的第一简档信息发送到电子设备的UICC。处理器可以进行控制以解码发送到UICC的在可加密单元中的第一简档信息,从解码的简档信息获取可安装单元中的第一简档信息,并按照获取的在可安装单元中的第一简档信息。

[0289] 此外,处理器可以进行控制以在缓冲器中存储在解码的简档信息之中的排除可安装单元中的简档信息的剩余简档信息。

[0290] 此外,处理器可以进行控制以从简档服务器接收构成简档包的可加密单元中的第二简档信息,将可加密单元中的第二简档信息发送到电子设备的UICC,解码发送到UICC的在可加密单元中的第二简档信息,在存储在缓冲器中的剩余简档信息和解码的第二简档信息的基础上获取可安装单元中的第二简档信息,在可安装单元中安装获取的第二简档信息,并且在缓冲器中存储在可加密单元中的第二简档信息之中的剩余简档信息。

[0291] 此外,控制器1830可以进行控制以将可发送单元中的第一简档信息划分并将划分的第一简档信息发送到UICC。处理器可以进行控制以将在可发送单元中划分的信息组合到可加密单元中的第一简档信息,并且解码组合的信息。

[0292] 简档包可以通过可安装在UICC中的单元中的简档信息来配置,并且可加密单元中的简档信息可以被重新配置为在可安装在UICC中的单元中划分的简档信息。可以根据可发

送单元中的每个简档信息加密简档包,并从简档服务器发送到电子设备。简档包可以具有TLV形式。

[0293] 控制器1830可以控制根据如通过图1至16所述的本公开的实施例的电子设备(或eUICC)的操作。此外,处理器可以控制根据如通过图1至16所述的本公开的实施例的eUICC的操作。

[0294] 控制器1830可以控制eUICC 1820的处理器的操作,并且可以被实现成执行处理器的操作。

[0295] 在本公开的上述实施例中,根据呈现的详细实施例,包括在本公开中的组件被表达为单数形式或复数形式。然而,为了便于描述,单数表达或复数表达已经被选为仅仅适用于呈现的情况,本公开不限于单数或复数组件,由复数形式表达的组件可以被配置为单数组件,并且由单数形式表达的组件可以被配置为复数组件。

[0296] 虽然已经用示范性实施例描述了本公开,但是可向本领域技术人员提出各种改变和修改。其意图是:本公开涵盖如落入所附权利要求的范围内的这样的改变和修改。

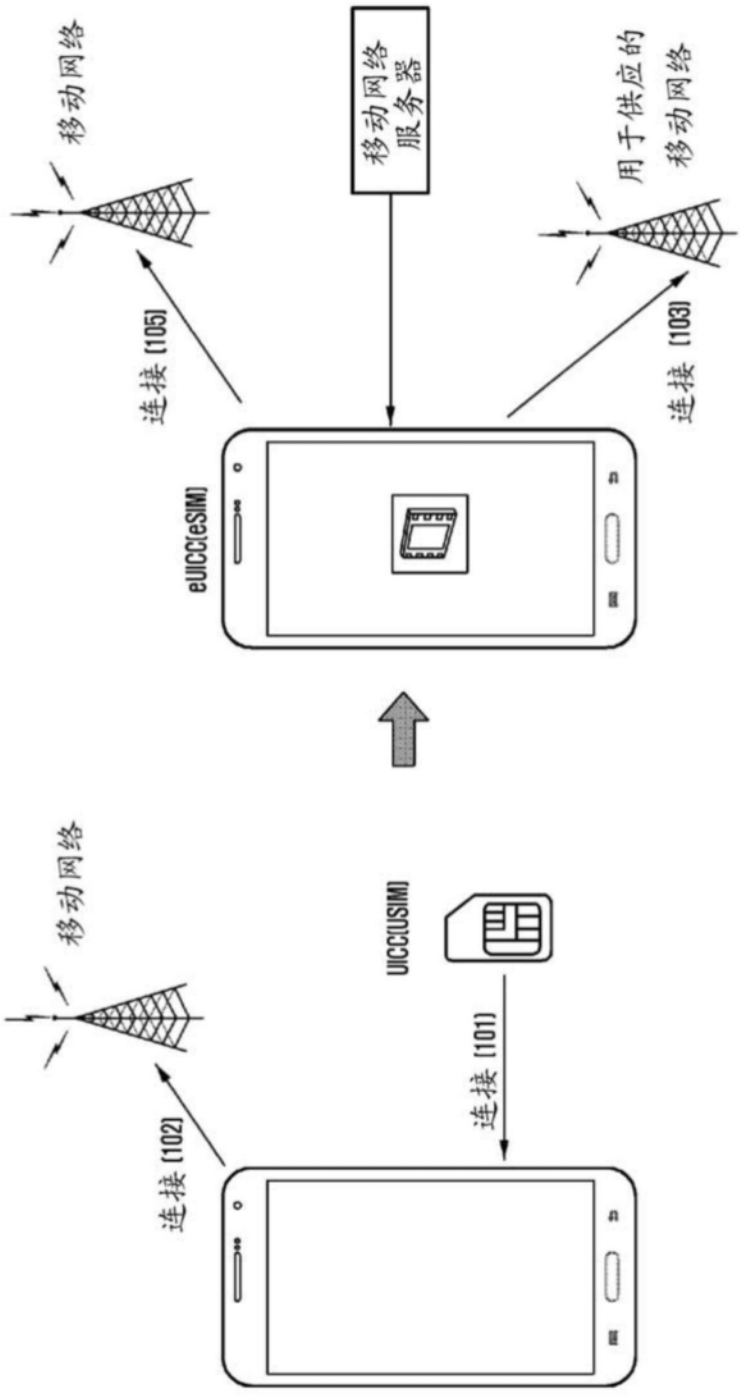

移动网络
移动网络服务器
用于供应的移动网络
连接 [105]
连接 [103]
eUICC(eSIM)
移动网络
UICC(USIM)
连接 [101]
连接 [102]

图1

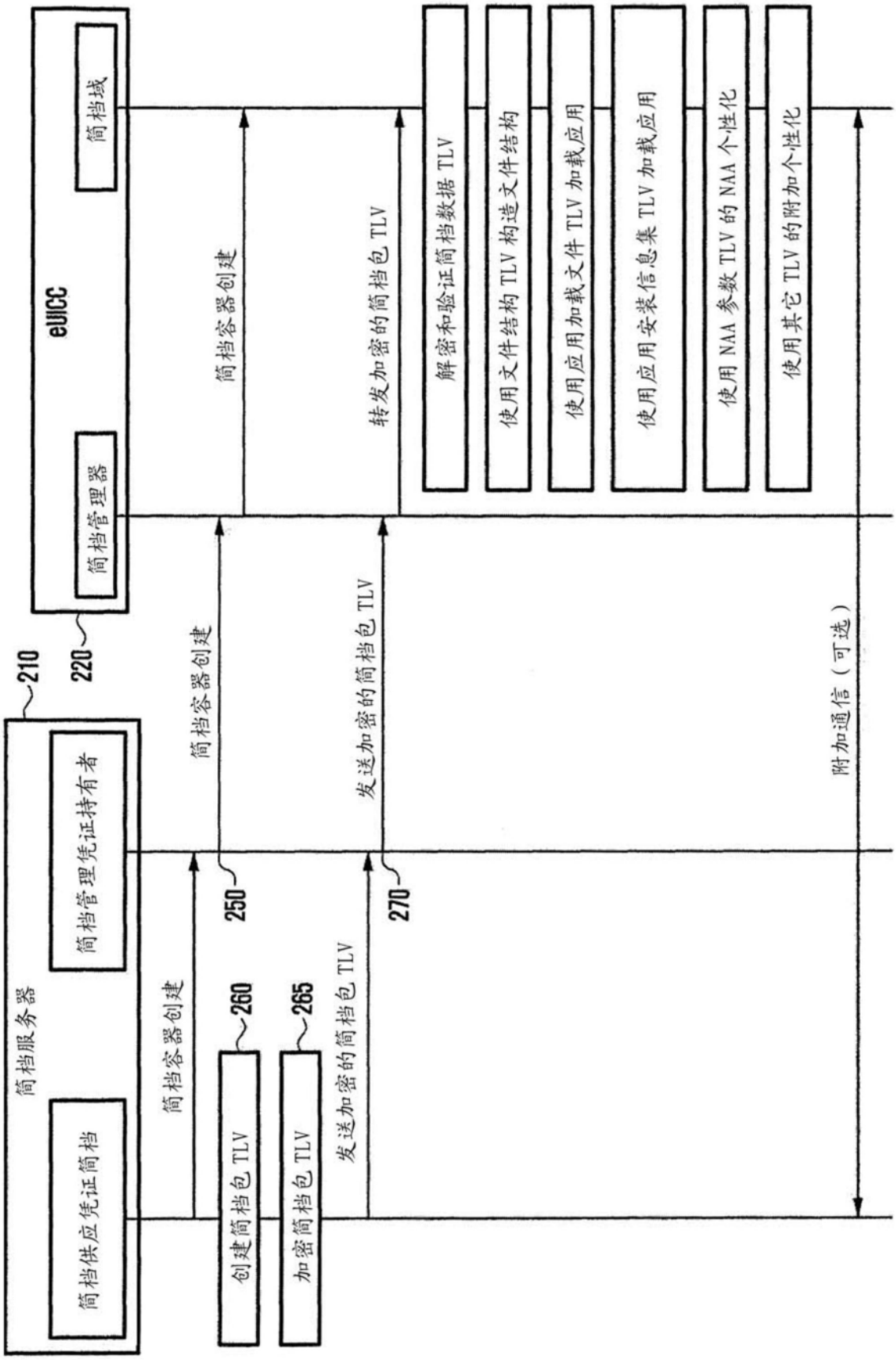

简档服务器
210
简档供应凭证简档
简档管理凭证持有者
220
eUICC
简档管理器
简档域
简档容器创建
250
创建简档包 TLV
260
加密简档包 TLV
265
发送加密的简档包 TLV
270
转发加密的简档包 TLV
解密和验证简档数据 TLV
使用文件结构 TLV 构造文件结构
使用应用加载文件 TLV 加载应用
使用应用安装信息集 TLV 加载应用
使用 NAA 参数 TLV 的 NAA 个性化
使用其它 TLV 的附加个性化
附加通信（可选）

图2

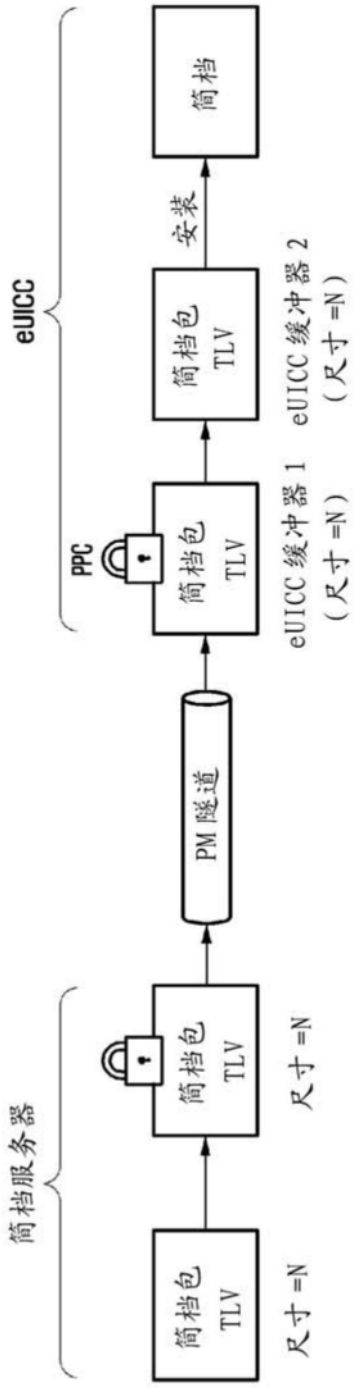

简档服务器
简档包
TLV
尺寸=N
简档包
TLV
尺寸=N
PM 隧道
eUICC
PPC
简档包
TLV
eUICC 缓冲器 1
（尺寸=N）
简档包
TLV
eUICC 缓冲器 2
（尺寸=N）
安装
简档

图3

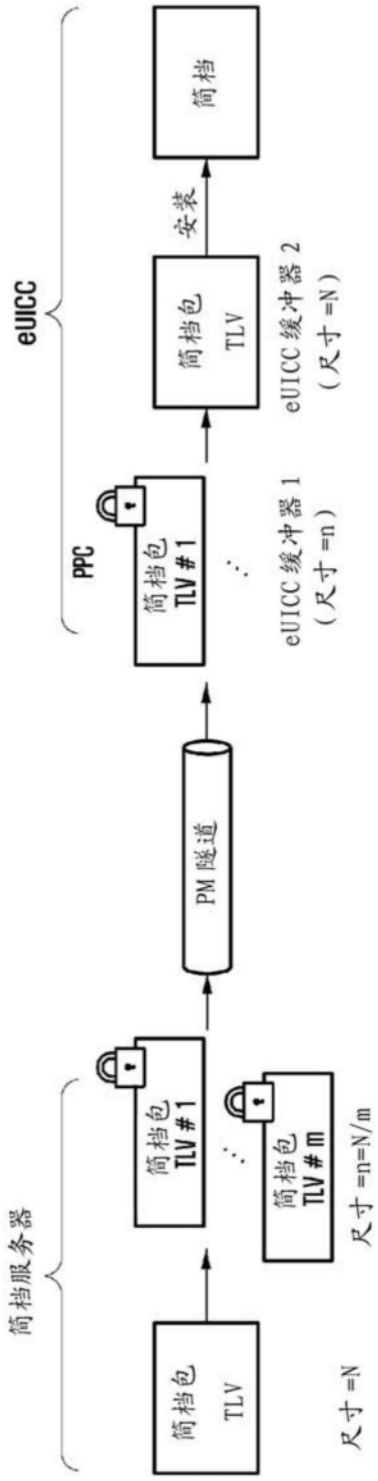

简档服务器
简档包
TLV
尺寸 =N
简档包
TLV # 1
简档包
TLV # m
尺寸 =n=N/m
PM 隧道
eUICC
PPC
简档包
TLV # 1
eUICC 缓冲器 1
（尺寸 =n）
简档包
TLV
eUICC 缓冲器 2
（尺寸 =N）
安装
简档

图4

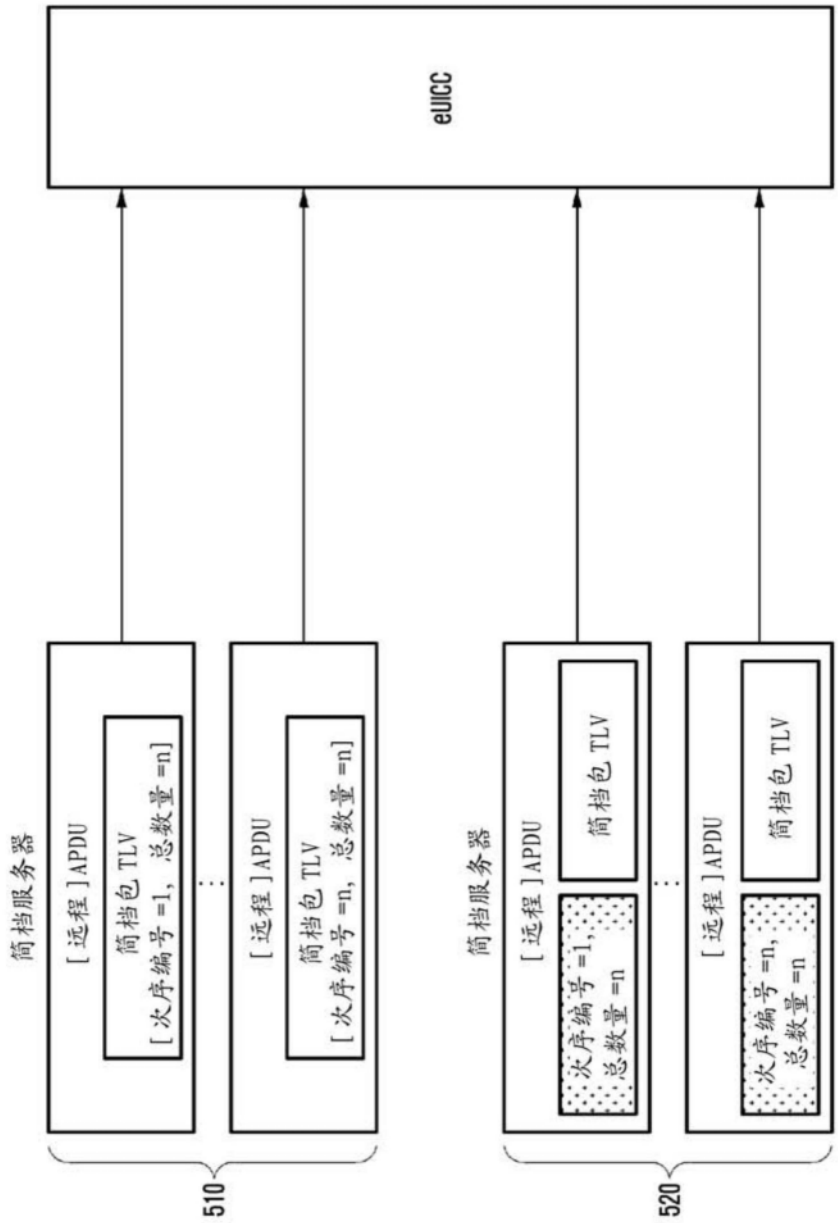

eUICC
简档服务器
[远程]APDU
简档包 TLV
[次序编号 =1, 总数量 =n]
[远程]APDU
简档包 TLV
[次序编号 =n, 总数量 =n]
510
简档服务器
[远程]APDU
次序编号 =1,
总数量 =n
简档包 TLV
[远程]APDU
次序编号 =n,
总数量 =n
简档包 TLV
520

图5

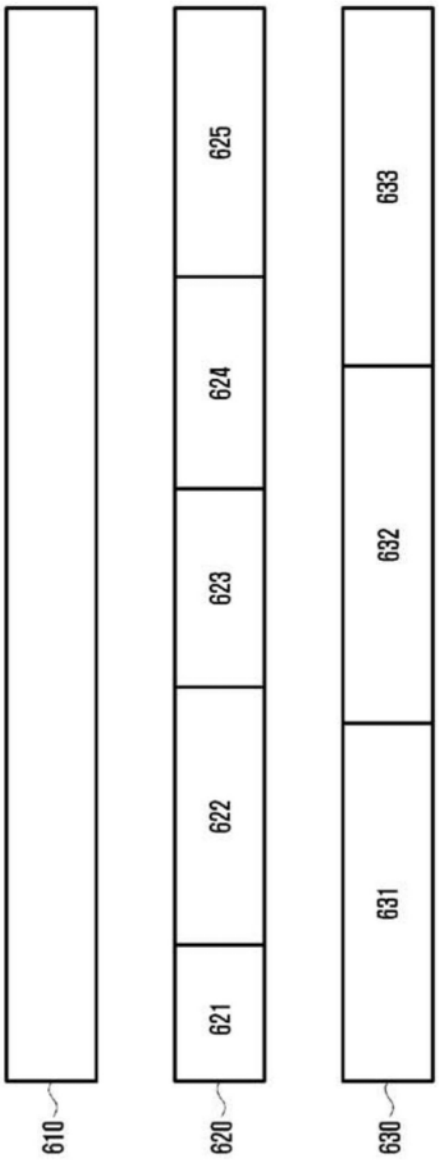


图6

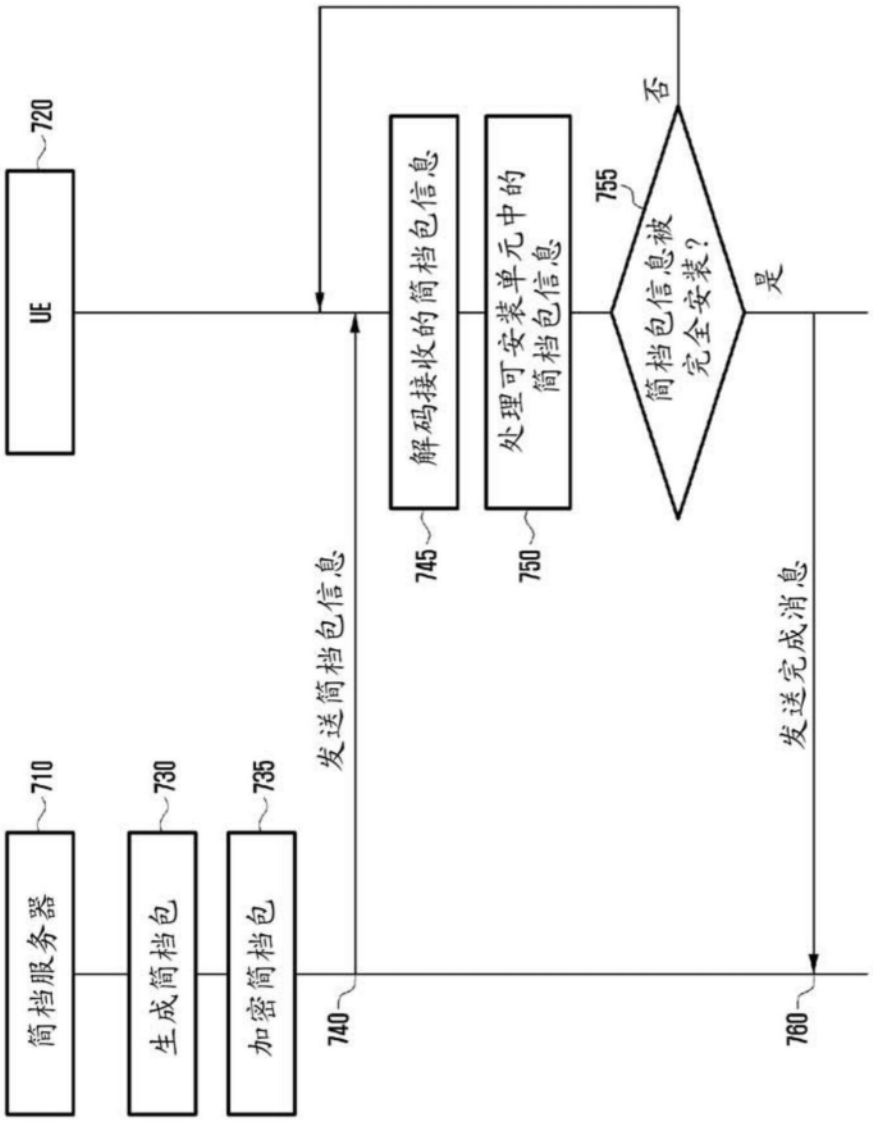

UE
720
简档服务器
710
生成简档包
730
加密简档包
735
发送简档包信息
740
解码接收的简档包信息
745
处理可安装单元中的简档包信息
750
简档包信息被完全安装?
755
否
是
发送完成消息
760

图7

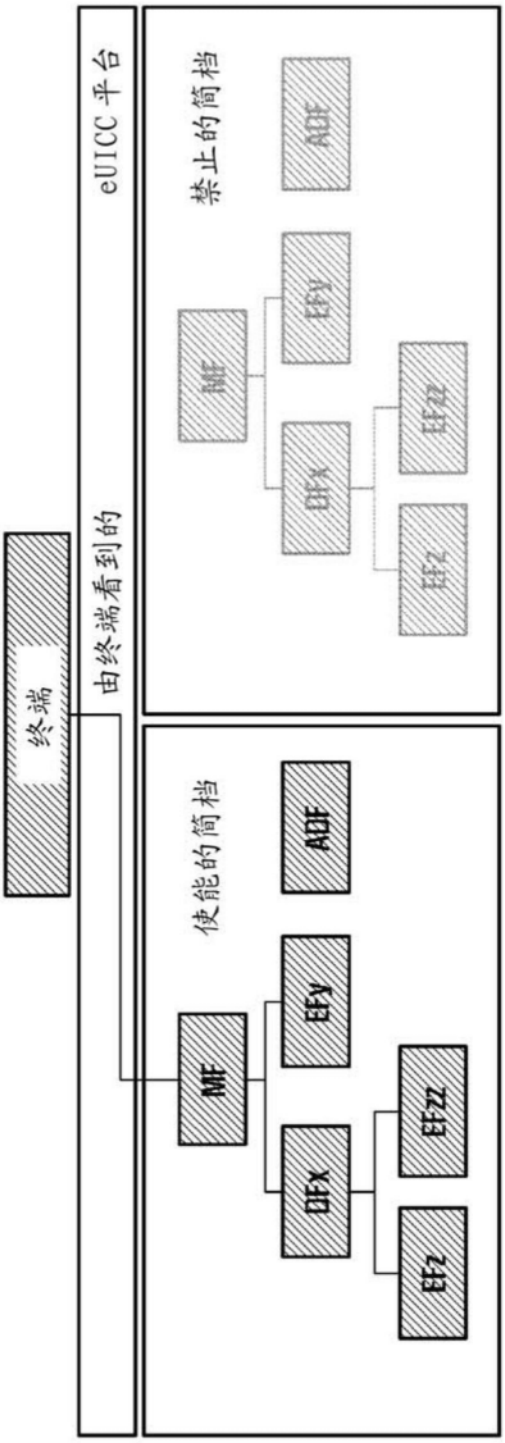

eUICC 平台
由终端看到的
终端
禁止的简档
ADF
MF
EFy
DFx
EFzz
EFz
使能的简档
ADF
MF
EFy
DFx
EFzz
EFz

图8

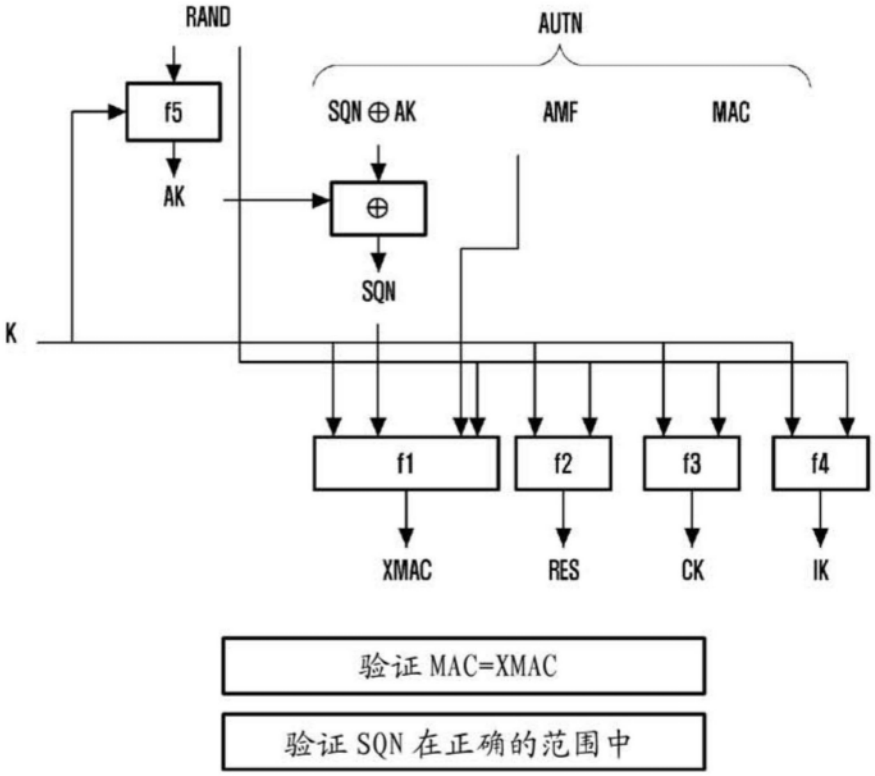

RAND
AUTN
f5
SQN ⊕ AK
AMF
MAC
AK
⊕
SQN
K
f1
f2
f3
f4
XMAC
RES
CK
IK
验证 MAC=XMAC
验证 SQN 在正确的范围中

图9

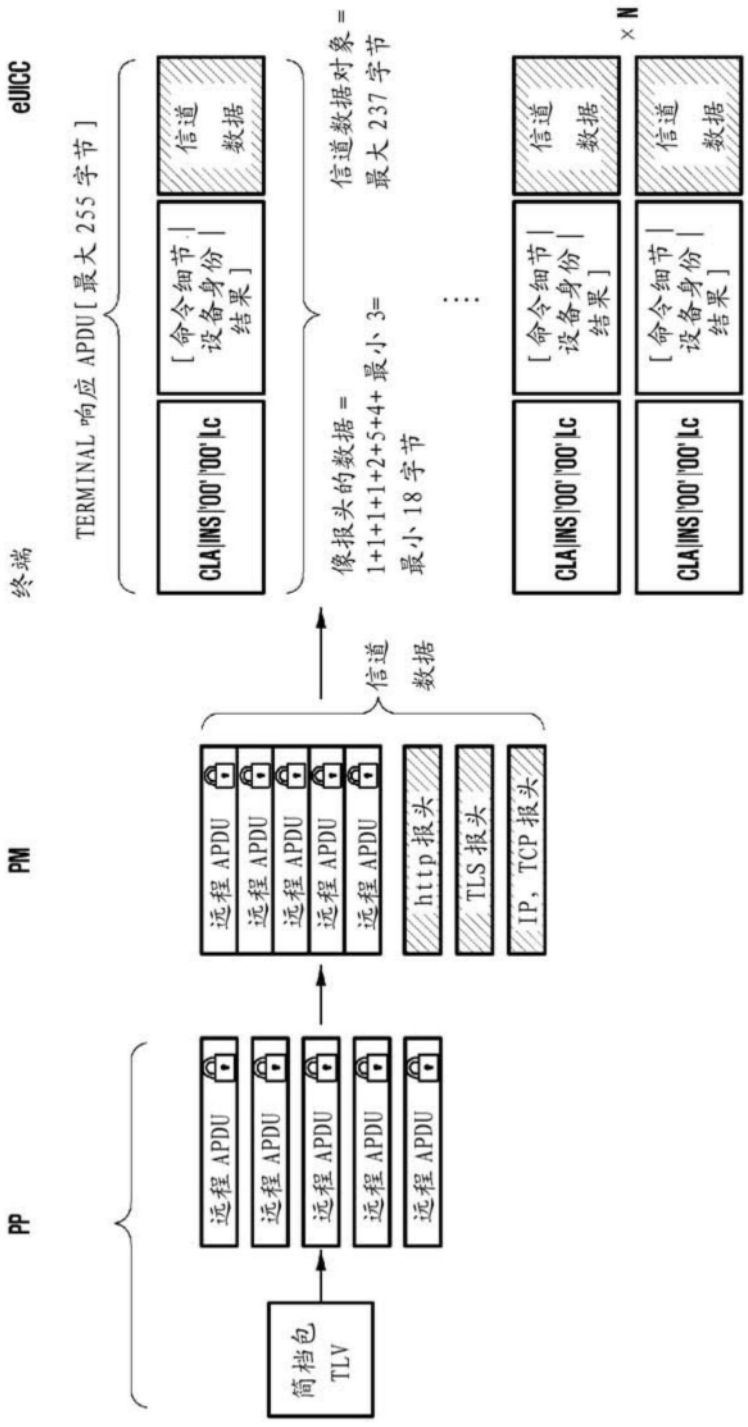

PP
PM
终端
eUICC
简档包
TLV
远程 APDU
远程 APDU
远程 APDU
远程 APDU
远程 APDU
远程 APDU
远程 APDU
远程 APDU
远程 APDU
远程 APDU
http报头
TLS报头
IP，TCP报头
信道
数据
像报头的数据 =
1+1+1+2+5+4+ 最小 3=
最小 18 字节
信道数据对象 =
最大 237 字节
TERMINAL 响应 APDU [最大 255 字节]
CLA|INS|'00'|'00'|Lc
[命令细节 | 设备身份 | 结果]
信道 数据
× N

图10

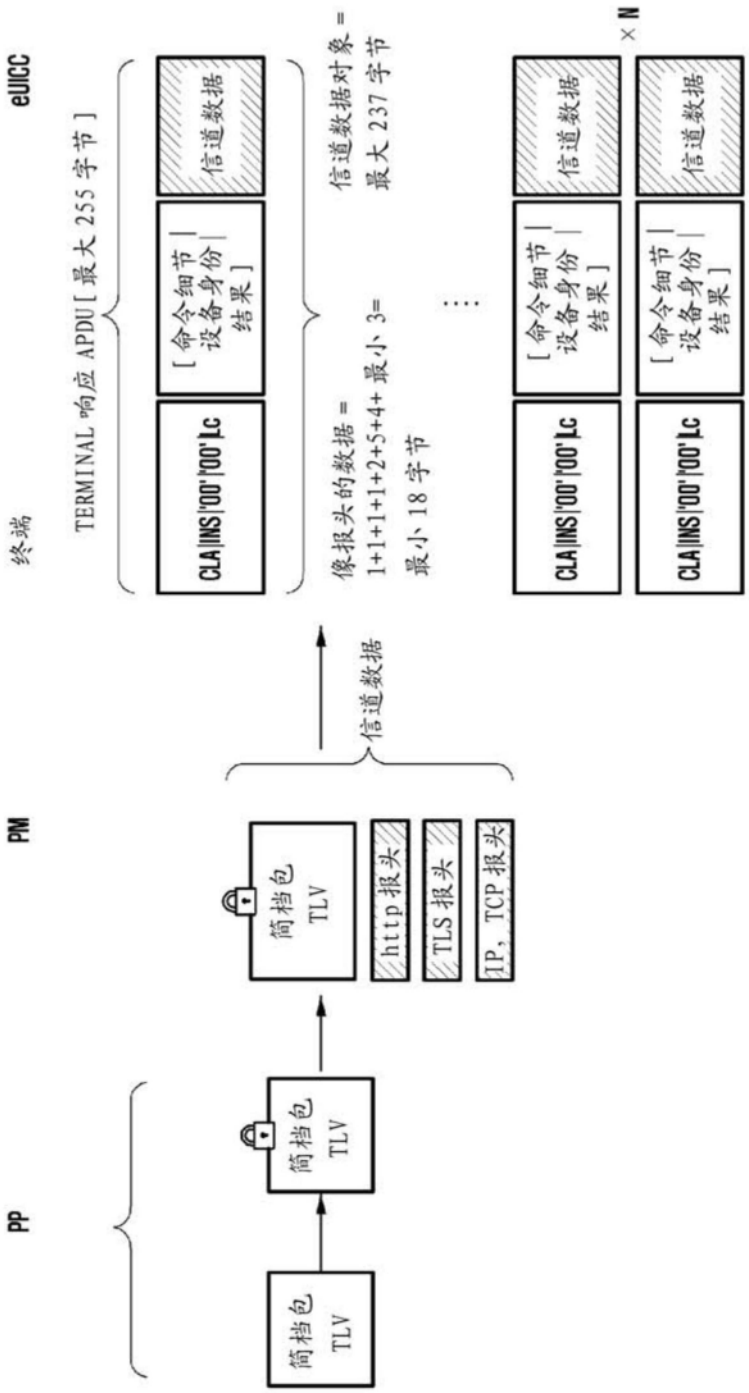

PP
PM
eUICC
终端
简档包 TLV
简档包 TLV
简档包 TLV
http报头
TLS报头
IP，TCP报头
信道数据
TERMINAL 响应 APDU[最大 255 字节]
CLA|INS|'00'|'00'|Lc
[命令细节 | 设备身份 | 结果]
信道数据
像报头的数据 = 1+1+1+1+2+5+4+ 最小 3= 最小 18 字节
信道数据对象 = 最大 237 字节
× N

图11

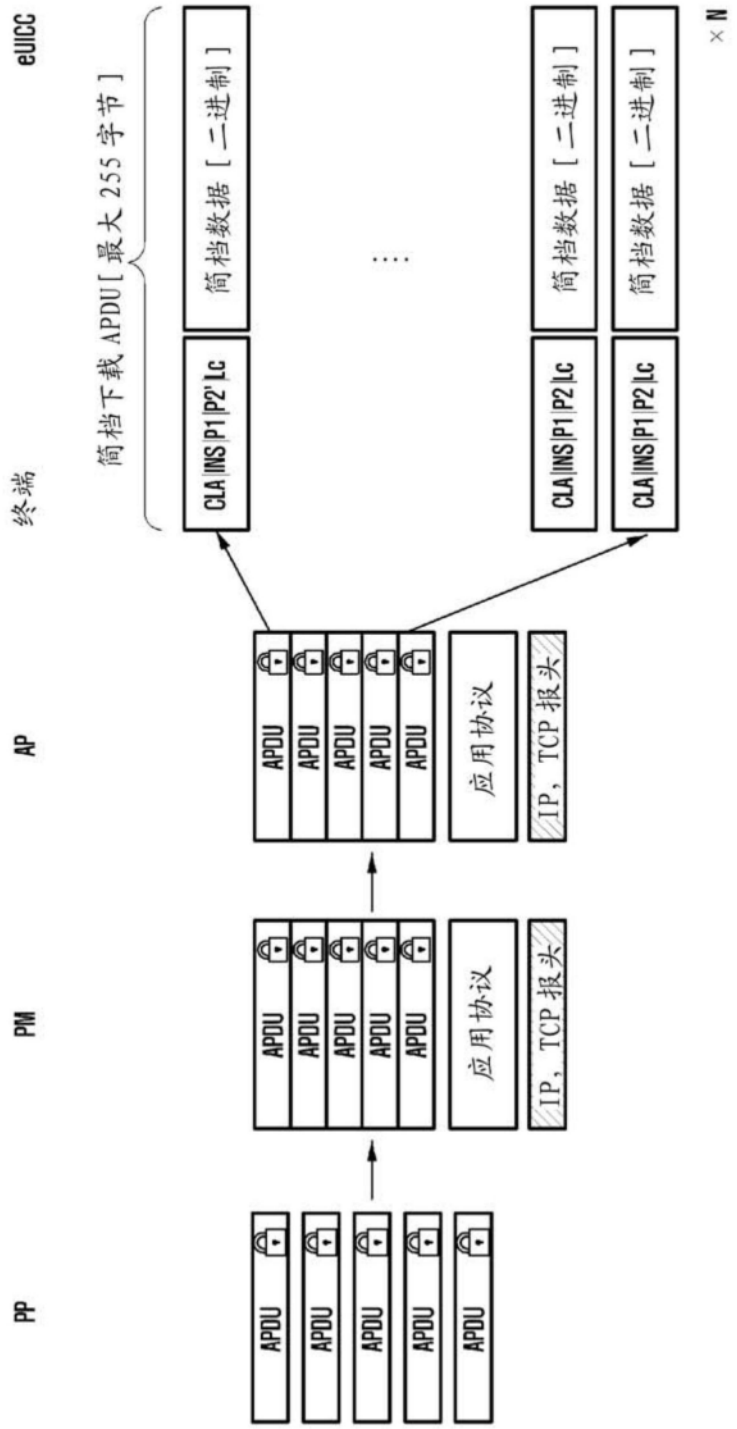

PP
PM
AP
终端
eUICC
APDU
应用协议
IP，TCP 报头
简档下载 APDU[最大 255 字节]
CLA|INS|P1|P2|Lc
简档数据 [二进制]
× N

图12

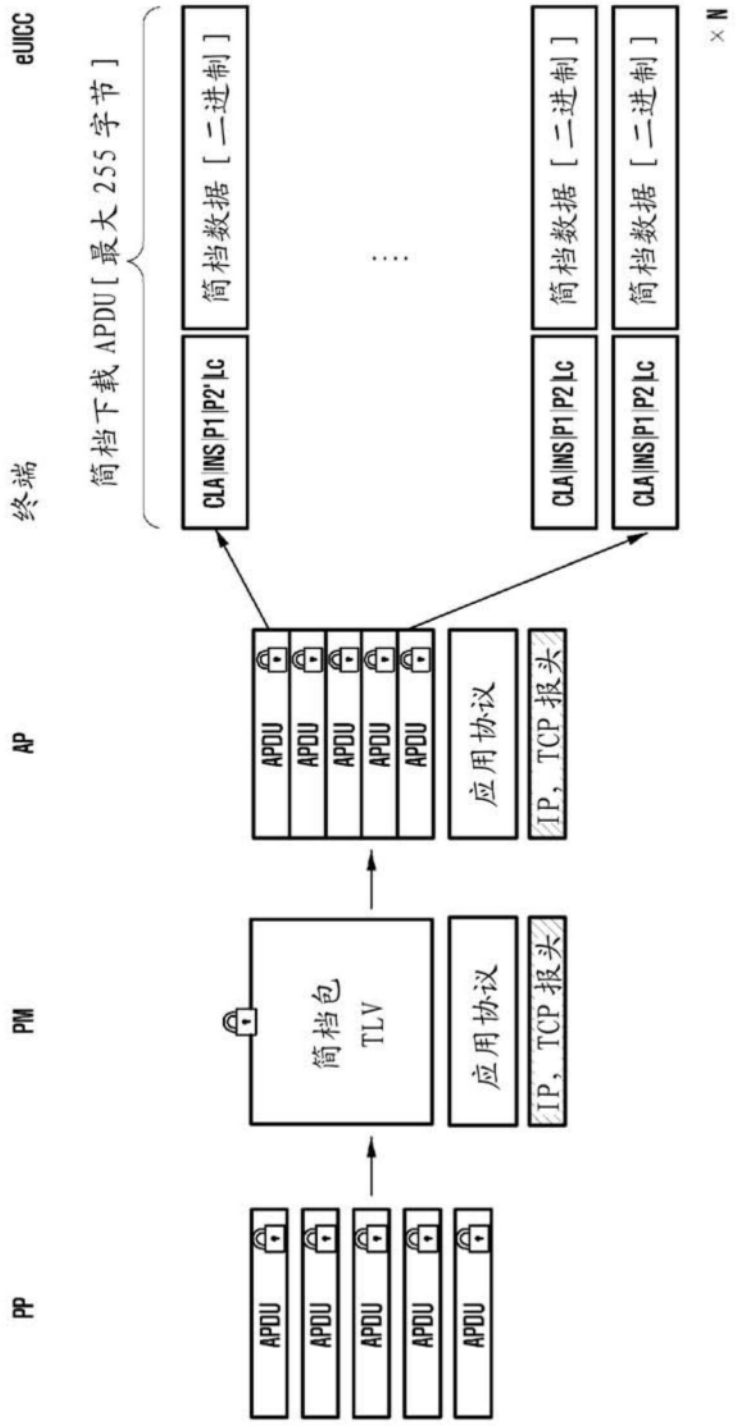

PP
PM
AP
终端
eUICC
APDU
简档包
TLV
应用协议
IP，TCP 报头
简档下载 APDU[最大 255 字节]
CLA|INS|P1|P2'|Lc
简档数据 [二进制]
CLA|INS|P1|P2|Lc
× N

图13

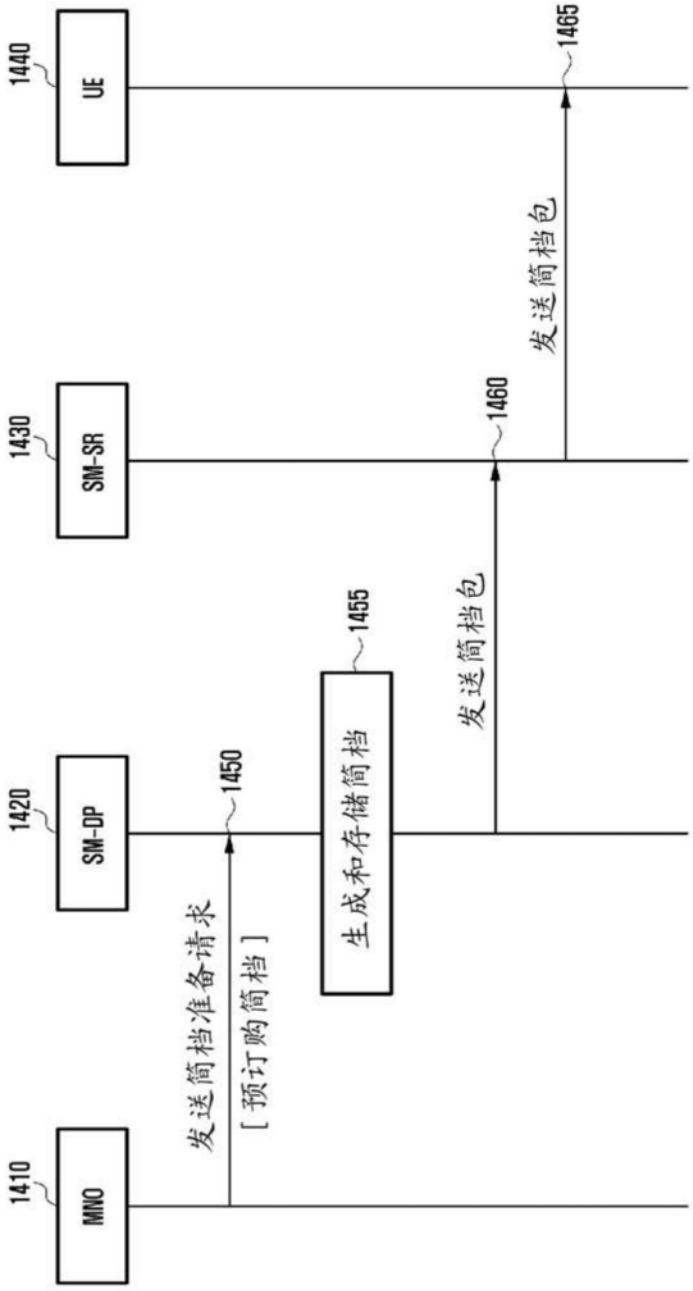

1440
UE
1465
发送简档包
1430
SM-SR
1460
发送简档包
1455
生成和存储简档
1420
SM-DP
1450
发送简档准备请求
[预订购简档]
1410
MNO

图14

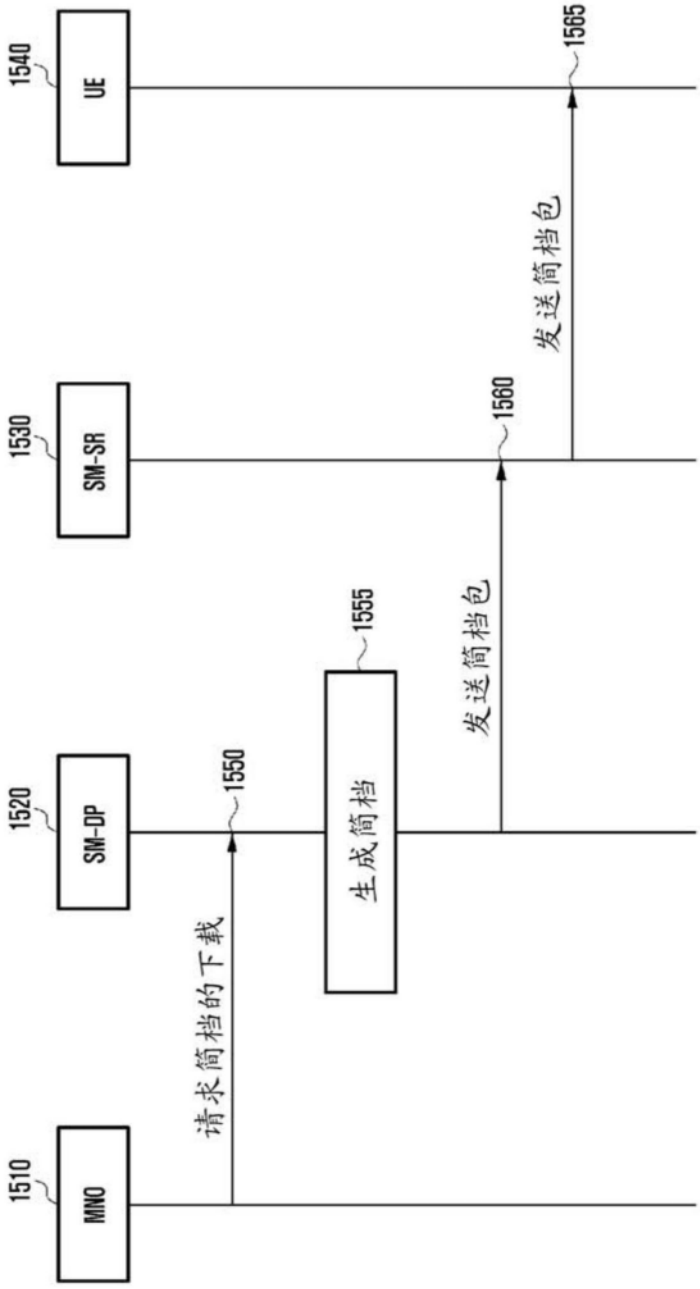

1540
UE
1565
发送简档包
1530
SM-SR
1560
发送简档包
1555
1520
SM-DP
1550
生成简档
请求简档的下载
1510
MNO

图15

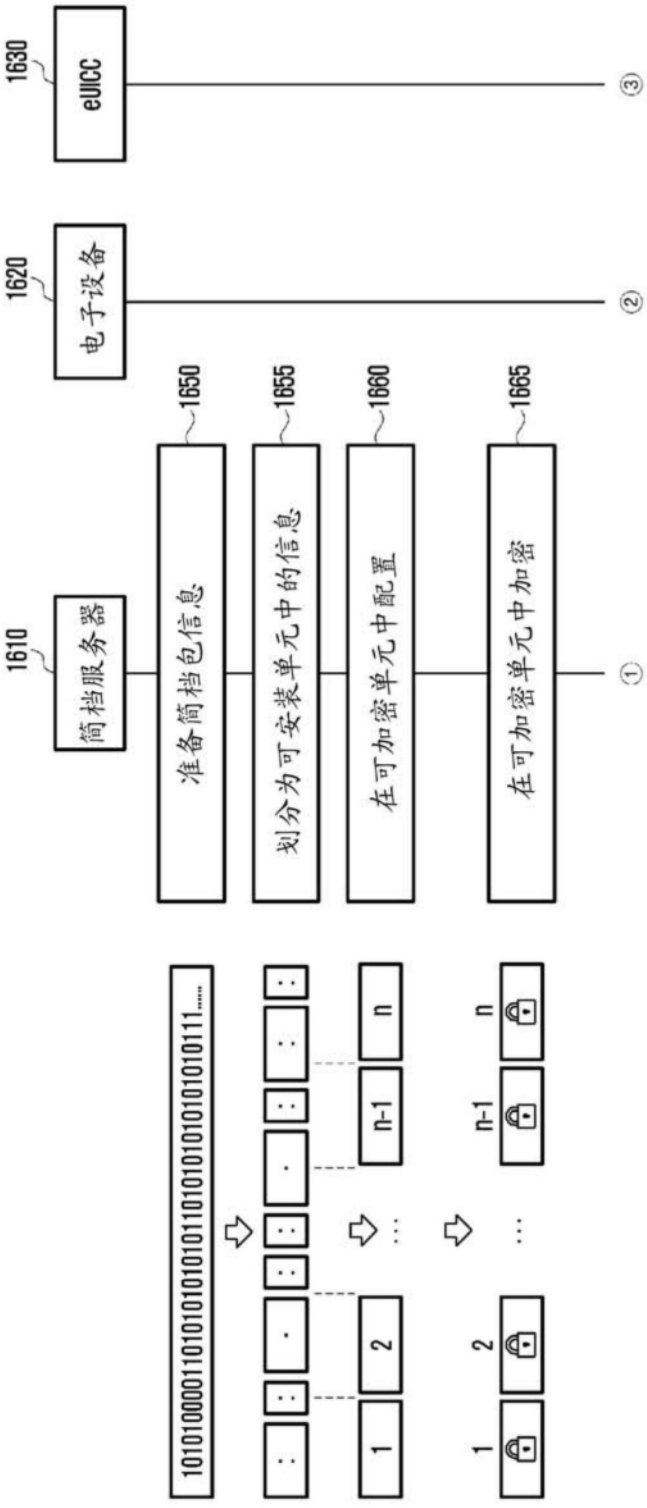

1630
eUICC
③
1620
电子设备
②
1610
简档服务器
1650
准备简档包信息
1655
划分为可安装单元中的信息
1660
在可加密单元中配置
1665
在可加密单元中加密
①
1010100001101010101010110101010101010111.....
1
2
n-1
n

图16a

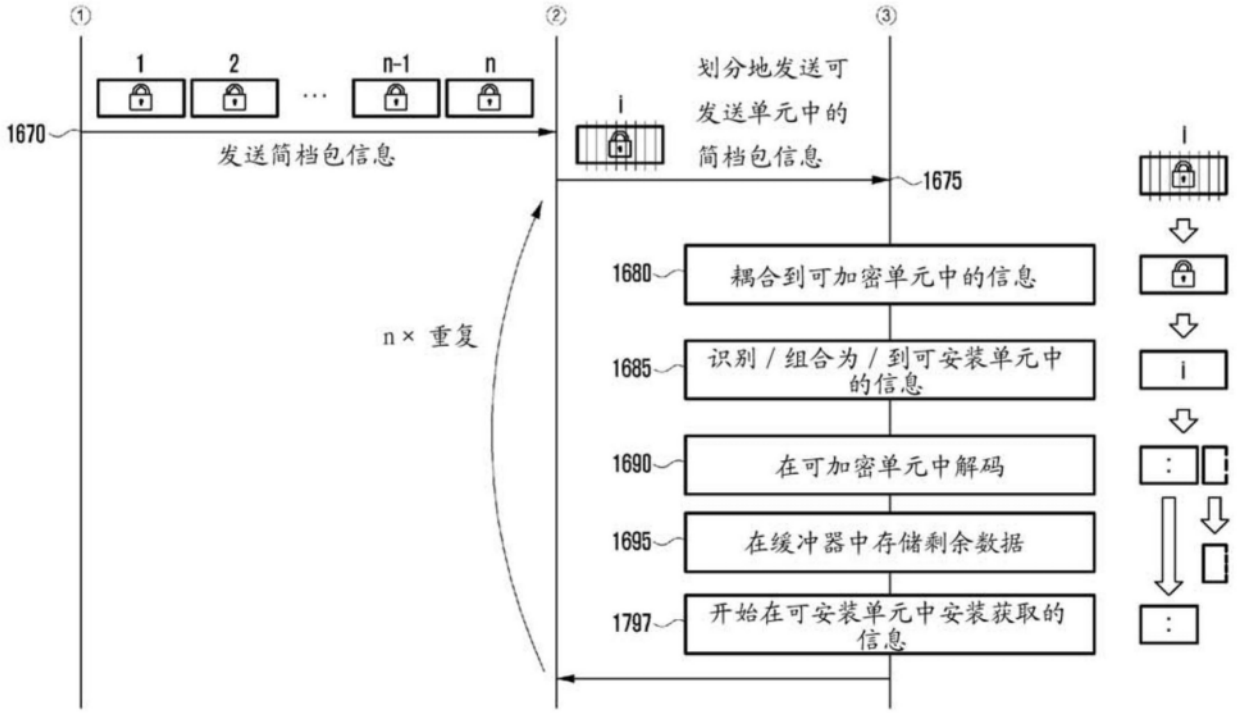

①
②
③
1
2
n-1
n
i
1670
发送简档包信息
划分地发送可
发送单元中的
简档包信息
1675
n× 重复
1680
耦合到可加密单元中的信息
1685
识别 / 组合为 / 到可安装单元中的信息
1690
在可加密单元中解码
1695
在缓冲器中存储剩余数据
1797
开始在可安装单元中安装获取的信息

图16b

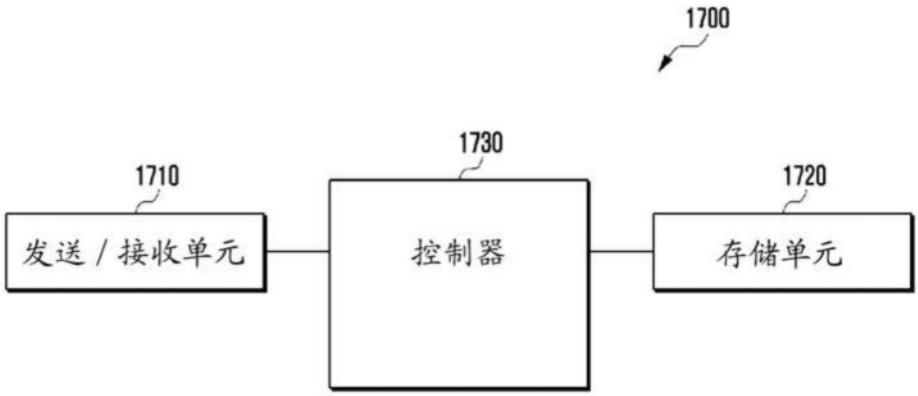

1700
1730
1710
1720
发送 / 接收单元
控制器
存储单元

图17

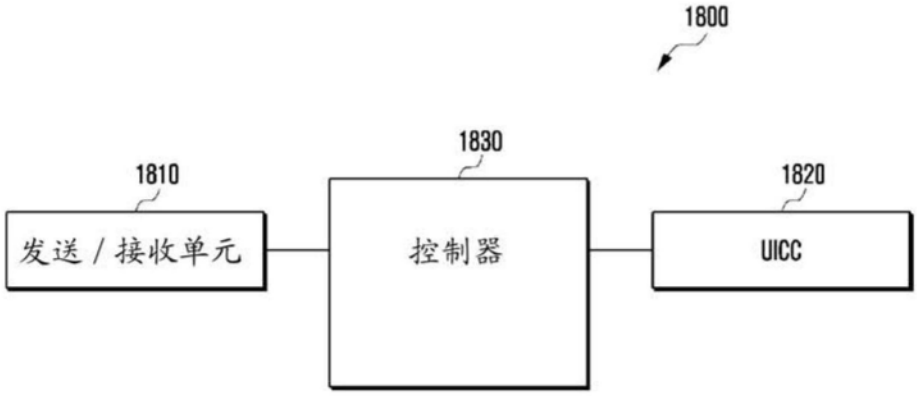


图18