(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 108028758 B
(45)授权公告日 2021.06.25

(21)申请号 201680052315.8
(22)申请日 2016.08.31
(65)同一申请的已公布的文献号
申请公布号 CN 108028758 A
(43)申请公布日 2018.05.11
(30)优先权数据
62/212,387 2015.08.31 US
(85)PCT国际申请进入国家阶段日
2018.03.09
(86)PCT国际申请的申请数据
PCT/KR2016/009725 2016.08.31
(87)PCT国际申请的公布数据
WO2017/039320 KO 2017.03.09

(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 李慧远 李祥洙
(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 李琳

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/08(2006.01)
审查员 提启恒

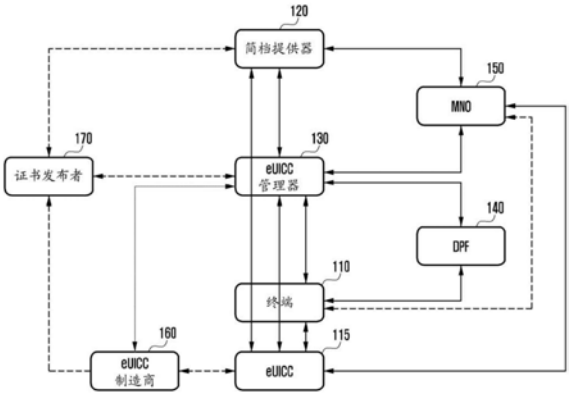
权利要求书3页 说明书38页 附图14页

(54)发明名称

在通信系统中下载简档的方法和装置

(57)摘要

本发明涉及一种在通信系统中通过在终端中下载和安装通信服务进行通信连接的方法和设备，并且根据本发明的一个实施例，一种终端的通信方法可以包括步骤：向简档提供服务器发送第一消息，该第一消息包括关于要接收的简档的信息；从简档提供服务器接收第二消息，该第二消息包括第一修改的口令码和用于指示是否需要用户的口令码输入的信息；如果第一修改的口令码的认证成功，则生成第二修改的口令码；向简档提供服务器发送第三消息，该第三消息包括第二修改的口令码和用于请求下载简档的信息；以及从简档提供服务器接收第四消息，该第四消息包括关于简档的信息。



CN 108028758 B

1.一种终端执行的方法,所述方法包括:

向简档提供服务器发送第一消息,第一消息包括用于简档提供服务器认证的第一质询值;

作为对第一消息的响应,从简档提供服务器接收第二消息,第二消息包括第一数据和在第一数据上计算的第一签名值,其中,第一数据包括第一质询值和用于终端的认证的第二质询值;

向简档提供服务器发送在第一签名值被验证之后生成的第三消息,第三消息包括第二数据和在第二数据上计算的第二签名值,其中,第二数据包括第二质询值和简档映射信息;

作为对第三消息的响应,从简档提供服务器接收第四消息,第四消息包括未加密的与简档相关的信息和指示简档是否需要确认码的信息;

在信息指示需要确认码的情况下,经由用户界面接收确认码;

向简档提供服务器发送用于请求简档数据的第五消息,第五消息包括基于确认码计算的散列确认码;以及

作为对第五消息的响应,从简档提供服务器接收包括加密的简档数据的第六消息。

2.如权利要求1所述的方法,其中,第五消息包括第三数据和在第三数据上计算的第三签名值,并且

其中,第三数据包括散列确认码。

3.如权利要求1所述的方法,其中,接收第四消息包括:

从简档提供服务器接收第四消息,第四消息包括未加密的与简档有关的信息、第四数据和在第四数据和第二签名值上计算的第四签名值,其中,第四数据包括指示是否需要确认码的信息。

4.如权利要求1所述的方法,其中,接收确认码还包括:

显示请求用户输入确认码的信息和包含在未加密的与简档有关的信息中的简档信息,并且

其中,所述方法还包括:

经由用户界面接收指示用户拒绝简档下载的信息;以及

向简档提供服务器发送指示用户拒绝简档下载的信息。

5.一种简档提供服务器执行的方法,所述方法包括:

从终端接收第一消息,第一消息包括用于简档提供服务器认证的第一质询值;

生成包括第一质询值和用于与终端相关联的认证的第二质询值的第一数据,并且在第一数据上计算第一签名值;

作为对第一消息的响应,向终端发送第二消息,第二消息包括第一数据和第一签名值;

从终端接收第三消息,第三消息包括第二数据和在第二数据上计算的第二签名值,其中,第二数据包括第二质询值和简档映射信息;

验证第二签名值;

确定由简档映射信息验证的简档是否需要确认码;

作为对第三消息的响应,向终端发送第四消息,第四消息包括未加密的与简档有关的信息和指示简档是否需要确认码的信息;

在信息指示需要确认码的情况下,从终端接收请求简档数据的第五消息,第五消息包

括基于确认码计算的散列确认码;以及

作为对第五消息的响应,向终端发送第六消息,第六消息包括加密的简档数据。

6.如权利要求5所述的方法,其中,接收第五消息包括:

从终端接收第五消息,第五消息包括第三数据和在第三数据上计算的第三签名值,其中,第三数据包括基于确认码计算的散列确认码;

使用源散列确认码计算预期散列值;

验证接收的散列确认码与预期散列值匹配;以及

在接收的散列确认码与预期散列值匹配的情况下,生成包括加密的简档数据的第六消息。

7.如权利要求5所述的方法,其中,发送第四消息包括:

向终端发送第四消息,第四消息包括未加密的与简档有关的信息、第四数据和在第四数据和第二签名值上计算的第四签名值,其中,第四数据包括指示是否需要确认码的信息。

8.如权利要求5所述的方法,其中,还包括:

从终端接收指示用户拒绝简档下载的信息。

9.一种终端,包括:

收发器;以及

控制器,被配置为:

经由收发器向简档提供服务器发送第一消息,第一消息包括用于简档提供服务器认证的第一质询值,

作为对第一消息的响应,经由收发器从简档提供服务器接收第二消息,第二消息包括第一数据和在第一数据上计算的第一签名值,其中,第一数据包括第一质询值和用于与终端相关联的认证的第二质询值,

经由收发器向简档提供服务器发送在第一签名值被验证之后生成的第三消息,第三消息包括第二数据和在第二数据上计算的第二签名值,其中,第二数据包括第二质询值和简档映射信息,

作为对第三消息的响应,经由收发器从简档提供服务器接收第四消息,第四消息包括未加密的与简档相关的信息和指示简档是否需要确认码的信息,

在信息指示需要确认码的情况下,经由用户界面接收确认码,

经由收发器向简档提供服务器发送用于请求简档数据的第五消息,第五消息包括基于确认码计算的散列确认码,以及

作为对第五消息的响应,经由收发器从简档提供服务器接收包括加密的简档数据的第六消息。

10.如权利要求9所述的终端,其中,第五消息包括第三数据和在第三数据上计算的第三签名值,并且

其中,第三数据包括散列确认码。

11.如权利要求9所述的终端,其中,所述控制器还被配置为:

经由收发器从简档提供服务器接收第四消息,第四消息包括未加密的与简档有关的信息、第四数据和在第四数据和第二签名值上计算的第四签名值,其中,第四数据包括指示是否需要确认码的信息。

12.如权利要求9所述的终端,其中,所述控制器还被配置为:

显示请求用户输入确认码的信息和包含在未加密的与简档有关的信息中的简档信息,并且

其中,所述控制器还被配置为:

经由用户界面接收指示用户拒绝简档下载的信息,并且

经由收发器向简档提供服务器发送指示用户拒绝简档下载的信息。

13.一种简档提供服务器,包括:

收发器;以及

控制器,被配置为:

经由收发器从终端接收第一消息,第一消息包括用于简档提供服务器认证的第一质询值,

生成包括第一质询值和用于与终端相关联的认证的第二质询值的第一数据,并且在第一数据上计算第一签名值,

作为对第一消息的响应,经由收发器向终端发送第二消息,第二消息包括第一数据和第一签名值,

经由收发器从终端接收第三消息,第三消息包括第二数据和在第二数据上计算的第二签名值,其中,第二数据包括第二质询值和简档映射信息,

验证第二签名值,

确定由简档映射信息验证的简档是否需要确认码,

作为对第三消息的响应,经由收发器向终端发送第四消息,第四消息包括未加密的与简档有关的信息和指示简档是否需要确认码的信息,

在信息指示需要确认码的情况下,经由收发器从终端接收请求简档数据的第五消息,第五消息包括基于确认码计算的散列确认码,并且

作为对第五消息的响应,经由收发器向终端发送第六消息,第六消息包括加密的简档数据。

14.如权利要求13所述的简档提供服务器,其中,所述控制器还被配置为:

经由收发器从终端接收第五消息,第五消息包括第三数据和在第三数据上计算的第三签名值,其中,第三数据包括基于确认码计算的散列确认码,

使用源散列确认码计算预期散列值;

验证接收的散列确认码与预期散列值匹配,并且

在接收的散列确认码与预期散列值匹配的情况下,生成包括加密的简档数据的第六消息。

15.如权利要求13所述的简档提供服务器,其中,所述控制器还被配置为:

经由收发器向终端发送第四消息,第四消息包括未加密的与简档有关的信息、第四数据和在第四数据和第二签名值上计算的第四签名值,其中,第四数据包括指示是否需要确认码的信息,并且

其中,所述控制器还被配置为:

经由收发器从终端接收指示用户拒绝简档下载的信息。

在通信系统中下载简档的方法和装置

技术领域

[0001] 本发明涉及通信系统，并且具体地，涉及终端的简档(profile)下载方法和装置，以便终端在通信系统中实时下载和安装简档。

背景技术

[0002] 自从4G通信系统的商用化以来，为了满足对无线数据通讯量日益增长的需求，开发重点集中于第5代(5G)或前5G通信系统。为此，5G或前5G通信系统被称为超4G网络通信系统或后长期演进(LTE)系统。为了实现高数据速率，正在考虑在毫米波(mm Wave)频带(例如，60GHz频带)上实现5G通信系统。为了减轻传播损耗并增加传播距离，5G通信系统可能考虑到各种技术，诸如波束成形、大规模MIMO、全维度MIMO(FD-MIMO)、阵列天线、模拟波束成形、以及大型天线。而且，为了使5G通信系统的吞吐量提高，正在对各种技术进行研究，诸如小小区(small cell)、先进小小区、云无线接入网(云RAN)、超密集网络、设备到设备通信(D2D)、无线回程、移动网络(moving network)、协作通信、协调多点(CoMP)、以及干扰消除。此外，正在进行的研究包括使用作为先进编码调制(ACM)的混合FSK与QAM调制和滑动窗口叠加编码(SWSC)、滤波器组多载波(FBMC)、非正交多址(NOMA)和稀疏代码多址(SCMA)。

[0003] 同时，互联网(Internet)正在从以人为中心的通信网络(其中由人生成并消费信息)发展为分布的事物或组件交换并处理信息的物联网(Internet of Things，IoT)。基于云服务器的大数据处理技术与IoT的组合导致万物互联技术。为了保证实现IoT所需的感测技术、有线/无线通信和网络基础设施、服务接口技术和安全技术，近来的研究集中于传感器网络、机器对机器(M2M)和机器型通信(MTC)技术。在IoT环境中，可以提供智能互联网技术(IT)，其能够收集和分析从连接的事物生成的数据，以为人们的生活添加新的价值。通过遗留(legacy)信息技术(IT)技术和各种行业的融合，IoT可以应用于诸如智能家居、智能建筑、智能城市、智能汽车或联网汽车、智能电网、医疗保健、智能电器和智能医疗服务的各个领域。

[0004] 因此，进行各种尝试以将IoT应用于5G通信系统。例如，通过诸如波束成形、MIMO和阵列天线的5G通信技术来实现传感器网络、机器对机器(M2M)和机器型通信(MTC)技术。上述将云RAN应用为大数据处理技术是5G和IoT技术之间的融合示例。

[0005] 同时，通用集成电路卡(UICC)是在移动终端中使用的智能卡。UICC可以包括用于接入移动通信运营商网络的接入控制模块。接入控制模块的示例包括订户身份模块(SIM)、通用SIM(USIM)和互联网协议(IP)多媒体服务身份模块(ISIM)。包含USIM的UICC被称为USIM卡。同样地，包含SIM的UICC被称为SIM卡。在以下描述中，在涵盖UICC卡、USIM卡和包含ISIM的UICC的意义上使用术语“SIM卡”。也就是说，提出的技术可以适用于全部SIM、USIM、ISIM和其他类型的UICC。

[0006] SIM卡存储移动通信订户信息，其用于订户认证和通讯安全密钥生成以便接入移动通信网络，用于保证移动通信的安全。

[0007] 通常，根据移动通信运营商的要求以运营商特定的方式制造SIM卡。因此，在包括

用于接入相应的运营商的网络的认证信息(例如,USIM应用、IMSI、K值和OPc值)的状态下交付SIM卡。移动通信运营商将制造商供应的SIM卡交付给订户。此后,移动通信运营商可以按照使用空中(Over The Air,OTA)技术在UICC中安装、更新和删除应用的方式管理信息。订户可以将UICC插入订户的移动通信终端,用于使用相应的移动通信运营商的网络和应用服务;并且即使在订户将旧的移动通信终端更换为新的移动通信终端时,UICC也可以使订户使用存储在UICC中的认证信息、联系人信息和电话簿。

[0008] 然而,这样的SIM卡的不便之处在于,移动通信终端用户不能使用其他移动通信运营商的服务。这意味着,为了使用由特定移动通信运营商提供的服务,用户必须具有由相应的移动通信运营商供应的SIM卡。例如,为了使出境旅行的用户使用由本地移动通信运营商提供的服务,用户必须购买本地SIM卡。虽然可以通过订阅漫游服务减轻这种不便,但是由于昂贵的漫游服务费,漫游服务是受限制的,甚至在网络运营商之间没有漫游协议。

[0009] 如果可以在UICC中下载SIM并安装SIM,则可以解决上述问题。在这种情况下,用户可以在任意时间将与用户感兴趣的移动通信服务对应的SIM下载到UICC。可以将多个下载SIM安装在UICC中,并且选择性地使用它们中的一个。UICC可以是固定的或可拆卸的。具体地,固定在终端中的UICC被称为嵌入式UICC(eUICC),并且eUICC可以被配置为远程下载多个SIM以用于选择性使用多个SIM。在以下描述中,能够安装远程下载的多个SIM的UICC通常被称为eUICC。也就是说,能够安装远程下载的SIM的、固定到终端或从终端可拆卸的所有类型的UICC通常被称为eUICC。而且,下载的SIM信息被称为简档或eUICC简档。

发明内容

[0010] 技术问题

[0011] 本发明旨在提供一种用于在通信系统中使用通信服务的终端的通信信道建立方法和装置。而且,本发明旨在提供一种用于在通信系统中建立通信信道的终端的实时简档下载方法和装置。而且,本发明旨在提供一种在通信系统中为终端提供简档的方法和装置。

[0012] 而且,本发明旨在提供一种用于防止非法移动网络运营商(MNO)进行非法简档下载的方法。

[0013] 而且,本发明旨在提供一种根证书信息更新方法,用于允许终端对用于下载简档的服务进行认证。

[0014] 而且,本发明旨在提供一种用于简档服务器认证终端的方法,该终端向简档信息传输服务器查问(inquire)简档信息。

[0015] 而且,本发明旨在提供一种以下述方式增强终端的隐私信息安全的方法,该方式使得当终端向简档信息传输服务器查问信息时,即使简档信息传输服务器没有终端信息,简档信息传输服务器也处理查问。

[0016] 而且,本发明旨在提供一种用于确定加密参数的方法,该加密参数在终端从简档提供服务器或简档管理服务器下载简档时用于认证和加密。

[0017] 本发明的目的不限于上述内容,本领域技术人员从下面的描述中将清楚地理解本文未描述的其他目的。

[0018] 解决方案

[0019] 根据本发明的一个方面,提供了一种终端的通信方法。该通信方法包括:发送第一

消息，该第一消息包括关于要从简档提供服务器接收的简档的信息；接收第二消息，该第二消息包括指示是否需要加密码(encryption code)输入的信息和第一修改的加密码(modified encryption code)；当第一修改的加密码被成功认证时，生成第二修改的加密码；向简档提供服务器发送第三消息，该第三消息包括第二修改的加密码和请求简档下载的信息；以及从简档提供服务器接收第四消息，该第四消息包括关于简档的信息。

[0020] 优选地，生成第二修改的加密码包括：接收用户输入的加密码，并通过用预定的随机值对加密码执行散列运算来生成第二修改的加密码。

[0021] 优选地，生成第二修改的加密码包括：接收用户输入的加密码，通过用预定的随机值对加密码执行散列运算来生成第三修改的加密码，并通过比较第一修改的加密码与第三修改的加密码来认证第一修改的加密码。

[0022] 优选地，第二消息包括未加密的简档信息，并且第四消息包括加密的简档信息。

[0023] 根据本发明的另一方面，提供了一种简档提供服务器的通信方法。该通信方法包括：接收第一消息，所述第一消息包括关于由终端请求的简档的信息；生成第一修改的加密码以供终端在认证简档提供服务器时使用；向终端发送第二消息，该第二消息包括指示是否需要加密码输入的信息和第一修改的加密码；从终端接收第三消息，该第三消息包括第二修改的加密码和请求简档下载的信息；以及当第二修改的加密码被成功认证时，向终端发送包括关于简档的信息的第四消息。

[0024] 优选地，生成第一修改的加密码包括：从运营商接收加密码，并通过用预定的随机值对加密码执行散列运算来生成第一修改的加密码。

[0025] 优选地，发送第四消息包括：从运营商接收加密码，通过用预定的随机值对加密码执行散列运算来生成第三修改的加密码，以及通过比较第二修改的加密码与第三修改的加密码来认证第二修改的加密码。

[0026] 根据本发明的另一方面，提供了一种终端。该终端包括：收发器，用于与网络实体进行通信；以及控制单元，该控制单元控制：发送包括关于要从简档提供服务器接收的简档的信息的第一消息；接收第二消息，该第二消息包括指示是否需要加密码输入的信息和第一修改的加密码；当第一修改的加密码被成功认证时，生成第二修改的加密码；向简档提供服务器发送第三消息，该第三消息包括第二修改的加密码和请求简档下载的信息；以及从简档提供服务器接收包括关于简档的信息的第四消息。

[0027] 根据本发明的又一方面，提供一种简档提供服务器。该简档提供服务器包括：收发器，与网络实体进行通信；以及控制单元，该控制单元控制：接收第一消息，所述第一消息包括关于由终端请求的简档的信息；生成第一修改的加密码以供终端在认证简档提供服务器时使用；向终端发送第二消息，该第二消息包括指示是否需要加密码输入的信息和第一修改的加密码；从终端接收第三消息，该第三消息包括第二修改的加密码和请求简档下载的信息；以及当第二修改的加密码被成功认证时，向终端发送包括关于简档的信息的第四消息。

[0028] 发明效果

[0029] 根据本发明的实施例，本发明的通信系统在减少存储在简档中的诸如简档和IMSI的资源数量的浪费方面是有利的，这是通过下述操作进行的：按照下述方式阻止将不会使用的不想要的简档或未加密的简档的下载，该方式使得在终端中下载和安装简档的过程中

在将加密的简档发送到终端之前发送未加密的简档信息以便用户确定是否使用简档。

[0030] 本发明的通信系统在防止简档被异常安装以及减少存储在简档中的诸如简档和IMSI的资源数量的浪费方面是有利的，这是通过下述操作进行的：按照下述方式阻止将不会使用的不想要的简档或未加密的简档的下载，该方式使得在终端中下载和安装简档的过程中在将加密的简档发送到终端之前运营商询问用户以单独的方式发送的确认码，以及仅当用户输入的确认码被验证时向终端发送加密的简档。

[0031] 本发明的优点不限于上述内容，并且本领域技术人员从下面的描述中将清楚地理解本文未描述的其他优点。

附图说明

[0032] 图1是示出根据本发明的实施例的简档安装和管理机制的图；

[0033] 图2是示出根据本发明的实施例的终端的简档下载方法的信号流程图；

[0034] 图3是示出根据本发明的实施例的终端的简档下载方法的信号流程图；

[0035] 图4是示出根据本发明的另一实施例的终端的简档下载方法的信号流程图；

[0036] 图5是示出根据本发明的另一实施例的简档下载方法的信号流程图；

[0037] 图6a至图6c是示出根据本发明的实施例的本发明的简档下载方法的信号流程图；

[0038] 图7a和图7b是示出根据本发明的实施例的在eUICC中下载简档的过程的信号流程图；

[0039] 图8a和图8b是示出根据本发明的实施例的网络初始化过程的信号流程图；

[0040] 图9是示出根据本发明的实施例的终端的配置的框图；

[0041] 图10是示出根据本发明的实施例的SM-DP+的配置的框图；

[0042] 图11是示出根据本发明的实施例的SM-SR+的配置的框图；以及

[0043] 图12是示出根据本发明的实施例的SM-DS的配置的框图。

具体实施方式

[0044] 参考附图详细描述本发明的示例性实施例。

[0045] 可以省略在此并入的公知功能和结构的详细描述，以避免模糊本发明的主题。这旨在省略不必要的描述，以使本发明的主题清楚。

[0046] 将理解，当元件被称为“连接到”或“耦合到”另一元件或层时，它可以直接连接或耦合到另一元件，或者可以存在介入元件。将理解，术语“包括(comprises)”、“包括(comprising)”、“包含(includes)”和/或“包含(including)”在本文中使用时指定所陈述的特征、整体、步骤、操作、元件和/或组件的存在，但是它们不排除存在或添加一个或多个其他特征、步骤、操作、元件、组件和/或其组合。

[0047] 尽管组件被分开描绘以指示不同的特征，但是这并不意味着这些组件被配置为单独的硬件或软件单元。也就是说，仅为了方便说明，分开列举了这些组件，但是这些组件中的至少两个可以被实现为单个组件，或一个组件可以被分割为负责相应功能的多个组件。在不脱离本发明的精神的情况下，集成和分割的组件的实施例包括在本发明的范围内。

[0048] 组件中的一些可能不是本发明的必不可少的功能的必要组件，但是它们可以是仅用于性能提高的可选组件。可以仅用实现本发明的主题所需的必要组件，而将用于性能提

高的可选组件除外，来实现本发明，并且将可选组件除外的仅具有必要组件的这种配置可以包括在本发明的权利要求中。

[0049] 可以省略在此并入的公知功能和结构的详细描述，以避免模糊本发明的主题。参考附图详细描述本发明的示例性实施例。此外，考虑到本发明中的功能来定义以下术语，并且以下术语可以根据用户或操作者的意图、使用等而变化。因此，应在本说明书的整体内容的基础上进行定义。

[0050] 将理解，流程图示图和/或框图的每个框、以及流程图示图和/或框图中的框的组合可以通过计算机程序指令来实现。这些计算机程序指令可以被提供给通用计算机、专用计算机或其他可编程数据处理装置的处理器以产生机器，使得经由计算机或其他可编程数据处理装置的处理器运行的指令创建用于实现流程图和/或框图的一个或多个框中指定的功能/动作的装置。这些计算机程序指令还可以被存储在非暂态计算机可读存储器中，该非暂态计算机可读存储器可以指导计算机或其他可编程数据处理装置以特定方式运行，使得存储在非暂态计算机可读存储器中的指令产生包括实现流程图和/或框图的一个或多个框中指定的功能/动作的指令装置的制品。计算机程序指令也可以被加载到计算机或其他可编程数据处理装置上，以使得在计算机或其他可编程装置上执行一系列操作步骤以产生计算机实现的过程，使得在计算机或其他可编程装置上运行的指令提供用于实现在流程图和/或框图的一个或多个框中指定的功能/动作的步骤。

[0051] 根据本发明的实施例的术语“模块”意指但不限于执行特定任务的软件或硬件组件，诸如现场可编程门阵列(FPGA)或专用集成电路(ASIC)。模块可以有利地被配置为驻留在可寻址存储介质上，并被配置为在一个或多个处理器上运行。因此，作为示例，模块可以包括组件(诸如，软件组件、面向对象的软件组件、类组件和任务组件)、进程、功能、属性、过程、子例程、程序代码段、驱动程序(drivers)、固件、微代码、电路、数据、数据库、数据结构、表格、数组和变量。在组件和模块中提供的功能可以组合成更少的组件和模块，或者进一步分成附加的组件和模块。另外，组件和模块可以被实现为使得它们运行设备或安全多媒体卡中的一个或多个CPU。

[0052] 提供以下描述中使用的术语以帮助理解本发明，并且可以在不脱离本发明的精神的情况下将其修改为不同的形式。

[0053] 首先，定义在本发明中使用的术语。

[0054] 图1是示出根据本发明的实施例的简档安装和管理机制的图。

[0055] 在本发明中，通用集成电路卡(UICC)115是被形成为可附接到移动通信终端110并具有能够存储个人信息(诸如，订户的网络接入认证信息、电话簿和短消息服务(SMS)信息)的芯片的智能卡。UICC 115用于在接入移动通信网络(诸如，全球移动通信系统(GSM)、宽带码分多址(WCDMA)和长期演进(LTE)网络)的过程中的订户认证和通讯安全密钥创建，以保证移动通信安全。向UICC 115提供特定于网络的身份应用(诸如，订户身份模块(SIM)、通用SIM(USIM)和互联网协议多媒体服务身份模块(ISIM))，并且UICC 115提供更高级别的安全功能以支持各种应用(诸如，电子钱包、电子开票和电子护照)。

[0056] UICC 115是嵌入式UICC，其以芯片形式固定到终端110，以便不可附接到终端110或从终端110拆卸。eUICC 115可以通过空中(OTA)技术以简档(profile)形式下载，然后安装在终端110中。在本发明中，eUICC 115表示能够下载和安装简档的所有类型的UICC。在以

下描述中，能够远程下载和安装SIM的、固定到终端110且可附接到终端110/从终端110可拆卸的所有类型的UICC被称为eUICC。而且，下载的SIM信息可互换地称为eUICC简档或简档。

[0057] 根据本发明的实施例的通过OTA技术下载简档并将简档安装在eUICC115中的方法可以应用于使用可附接到终端110/从终端110可拆卸的UICC的情况。也就是说，根据本发明的实施例，可以使用OTA技术下载简档并将下载的简档安装在UICC 115中。

[0058] 在以下描述中，术语“UICC”与“SIM”可互换地使用，并且术语“eUICC”与“eSIM”可互换地使用。

[0059] 在以下描述中，术语“简档(profile)”可以指按照处于UICC中的形式由应用、文件系统和认证密钥组成的软件包。

[0060] 在以下描述中，术语“USIM简档(SIM简档)”与具有相同含义的“简档”可互换地使用，或可以表示包含存储在简档的USIM应用中的信息的软件包。

[0061] 在以下描述中，简档提供服务器120可以可互换地称为订阅管理器数据准备(SM-DP)、SM-DP加(SM-DP+)、简档域的无卡实体(off-card entity)、简档加密服务器、简档创建服务器、简档供应者(profile provisioner,PP)、简档提供者(profile provider)、以及简档提供凭证(PPC)持有者。

[0062] 在以下描述中，简档信息递送服务器140可以可互换地称为发现和推送功能(DPF)和订阅管理器发现服务(SM-DS)。

[0063] 在以下描述中，简档管理服务器130可以可互换地称为订阅管理器安全路由(SM-SR)、SM-SR加(SM-SR+)、eUICC简档管理器的无卡(off-card)实体、PMC持有者、以及eUICC管理器(EM)。

[0064] 在以下描述中，简档提供服务器120可以集成简档管理服务器130的功能。根据本发明的各种实施例，简档提供服务器120的操作可以由简档管理服务器130执行。同样地，简档管理服务器或SM-SR 130的操作可以由简档提供服务器120执行。

[0065] 在以下描述中，终端110可以可互换地称为“终端”、“移动通信终端”、“移动台(MS)”、“用户设备(UE)”、“用户终端(UT)”、“无线终端”、“接入终端(AT)”、“订户单元”、“订户站(SS)”、“无线设备”、“无线通信设备”、“无线发射/接收单元(WTRU)”、“移动节点”等。终端110的示例可以包括蜂窝电话、启用无线通信的智能电话、启用无线通信的个人数字助理(PDA)、无线调制解调器、启用无线通信的便携式计算机、启用无线通信的数字相机、启用无线通信的游戏设备、启用无线通信的音乐存储和播放电器、启用无线互联网接入和浏览的电器、以及集成上述设备的部分的功能的其他单元和终端。终端可以包括，但不限于，机器对机器(M2M)终端和机器型通信(MTC)终端/设备。在以下描述中，终端可以可互换地称为电子设备。

[0066] 在本发明中，电子设备可以包括能够在其中安装下载的简档的UICC115。如果UICC 115未嵌入在电子设备中，则可拆卸的UICC可以物理上连接到电子设备。例如，UICC 115可以以卡的形式来设计以便插入电子设备中。例如，电子设备可以是终端110，并且在这种情况下，终端110可以具有用于在其中安装下载的简档的UICC 115。UICC 115可以嵌入终端110中，并且如果未嵌入，则UICC 115可以附接到终端110或从终端110拆卸，以建立或解除电气连接。能够在其中安装下载的简档的UICC 115可以称为eUICC 115。

[0067] 在本发明中，简档标识符可以可互换地称为“简档ID”、“集成电路卡ID(ICCID)”、

“ISD-P”和“因素匹配简档域(PD)”。简档ID可以是每个简档的唯一标识符。

[0068] 在本发明中,eUICC ID可以被称为“EID”,作为嵌入在终端中的eUICC115的唯一标识符。在提供简档(provisioning profile)被嵌入在eUICC 115中的情况下,eUICC ID可以是提供简档的标识符。根据本发明的实施例,eUICC 115被固定到终端110,并且在这种情况下,eUICC ID可以是终端ID。eUICC ID可以可互换地称为eUICC 115的特定安全域。

[0069] 在本发明中,简档容器可以称为简档域。简档容器可以是安全域。

[0070] 在本发明中,应用协议数据单元(APDU)可以是用于终端110与eUICC115协作的消息。APDU可以是用于PP 120或PM 130与eUICC 115协作的消息。

[0071] 在本发明中,简档提供凭证(PPC)可以是PP 120与eUICC 115之间进行相互认证、简档加密和签名的手段。PPC可以包括以下各项中的至少一个:对称密钥、Rivest-Shamir-Adleman(RSA)证书与私钥的对、椭圆曲线加密(ECC)证书与私钥的对、以及根证书发布机构(certification authority,CA)与证书链的对。在存在多个PP的情况下,eUICC 115可以存储并使用特定于PP的PPC。

[0072] 在本发明中,简档管理凭证(PMC)可以是用于在PM 130与eUICC 115之间进行相互认证、传输数据加密和签名的手段。PMC可以包括以下各项中的至少一个:对称密钥、RSA证书与私钥的对、ECC证书与私钥的对、以及根CA与证书链的对。

[0073] 在本发明中,AID可以是应用标识符。这个值可以用作用于在eUICC 115中的应用之间进行区分的标识符。

[0074] 在本发明中,简档包TLV可以可互换地称为简档TLV。简档包TLV可以是表示以标签、长度和值(TLV)的形式构成简档的信息的数据集合。

[0075] 在本发明中,AKA是作为用于接入3GPP和3GPP 2网络的认证算法的认证和密钥协议(Authentication and Key Agreement)的缩写。

[0076] 在本发明中,K表示存储在eUICC 115中的用于在AKA认证算法中使用的加密密钥值。

[0077] 在本发明中,OPc表示存储在eUICC 115中的用于在AKA认证算法中使用的参数。

[0078] 在本发明中,NAA是网络接入应用(Network Access Application)的缩写,其是存储在UICC 115中的用于在接入网络时使用的应用,诸如USIM和ISIM。也就是说,NAA是网络接入模块。

[0079] 同时,UICC 115可以被设计为插入到终端110中。在这种情况下,UICC115可以可附接到终端110/从终端110可拆卸,或嵌入终端110中。UICC 110的简档可以包括用于在接入特定运营商的网络时使用的“接入信息”。接入信息可以包括用于与作为订户标识符的IMSI一起在网络中进行认证的K或Ki值。

[0080] 然后,终端110可以使用UICC 115与移动运营商的认证处理系统(例如,归属位置寄存器(Home Location Register,HLR))或AuC一起执行认证。认证过程可以是AKA过程。如果认证成功,则终端110能够使用诸如移动电话的移动通信服务、以及使用移动通信系统的网络的移动数据服务。

[0081] 可以省略在此并入的公知功能和结构的详细描述,以避免模糊对本发明的主题的理解。

[0082] 如上所述,eUICC 115可以以嵌入终端110中或可附接到终端110/从终端110可拆

卸的UICC卡或芯片的形式来实现。eUICC 115可以是具有各种尺寸之一以及被实现为遗留形式因子(诸如,2FF、3FF、4FF、MFF1和MFF2)之一的UICC。eUICC 115可以嵌入终端110中,或集成到终端110的通信芯片(例如,基带调制解调器)中。

[0083] 简档提供服务器120可以具有生成简档并加密简档的功能,并且可以被称为SM-DP+。

[0084] 简档管理服务器130可以被称为EM或SM-SR+,并负责将从SM-DP+120接收的简档中继到终端110的本地简档助理(LPA)或管理简档。此时,SM-SR+130可以控制SM-DP+120与终端110的LPA之间的简档下载和简档管理操作。

[0085] 简档信息递送服务器140可以被称为SM-DS或DPF,并且可以将从SM-SR+130接收的SM-SR+服务器地址和事件标识符中继到终端110的LPA。

[0086] 根据本发明的实施例,SM-DP+120和SM-SR+130可以被实现为可称为SM-DP+或订阅管理器加(SM+)的单个服务器。

[0087] eUICC制造商(EUM)160可以制造eUICC 115并将制造的eUICC 115提供给移动通信运营商或终端制造商。移动网络运营商(MNO)150可以是用于向终端提供移动通信服务的移动通信网络运营商。证书发布者(CI)170可以认证简档提供服务器120、简档管理服务器130、简档信息递送服务器140和EUM 160。根据本发明的一个实施例,终端110可以包括:收发器,用于从SM-DP+120或SM-SR+130接收加密的简档或未加密的简档;显示单元,用于显示未加密的简档信息;用户界面(UI)单元,用于请求(asking)用户对接收到简档进行确认,在简档下载过程期间在接收到加密的简档之前执行显示和确认输入过程;以及控制单元,用于基于用户输入来确定是继续还是停止简档下载过程。

[0088] 在根据本发明的实施例的无线通信系统中,SM-DP+120可以在简档下载过程期间生成原始简档信息和加密的简档,并且仅当在发送原始(raw)简档信息之后从终端110接收到正常简档下载请求消息时向控制单元和收发器发送加密简单信息。

[0089] 在根据本发明的实施例的无线通信系统中,终端110可以包括:收发器,用于从SM-DP+120或SM-SR+130接收加密的简档和未加密的原始简档信息;显示单元,用于显示原始简档信息;控制单元,用于基于作为在简档下载过程期间从SM-DP+120接收的信息的一部分的、指示是否需要用户的确认码的指示符,来确定是否请求用户输入确认码;以及UI单元,用于与显示原始简档信息分开地或同时地向用户请求确认码,控制单元对用户输入的确认码和在简档接收过程期间从SM-DP+120或SM-SR+130接收的随机值执行散列运算,以及控制以在简档接收过程期间将运算结果值发送到SM-DP+120或SM-SR+130。

[0090] 在根据本发明的实施例的无线通信系统中,SM-DP+120可以包括:存储单元,用于存储指示是否需要确认码以下载特定简档的信息和确认码信息;收发器;以及控制单元,其控制收发器向终端110发送指示是否需要确认码用于下载特定简档的信息,当需要确认码时,其将从终端110接收到的散列运算值与由SM-DP+120使用存储在SM-DP+120中的确认码和从终端110接收的随机值计算的散列运算值进行比较,并且当散列值不匹配时,其控制收发器不将加密的简档发送到终端110。

[0091] 下文中描述本发明的优选实施例。

[0092] 图2是示出根据本发明的实施例的终端的简档下载方法的信号流程图。

[0093] 参考图2,在步骤210处,终端110可以生成用于验证服务器的服务器验证信息。此

时,服务器验证信息可以是随机值,例如,质询值(challenge value)。该质询值可以是由终端110的控制单元或连接到终端110的eUICC115生成的值,并且可以被称为eUICC质询值。终端110可以向简档提供服务器120发送包括用于验证服务器的信息的消息。该消息可以是初始认证请求(IniAuthRequest)消息。简档提供服务器120可以是SM-DP+。终端110可以包括可执行终端110的一部分操作的eUICC 115。

[0094] 在步骤215处,SM-DP+120可以生成用于验证终端110的终端验证信息。此时,终端验证信息可以是随机值,例如,由SM-DP+120的控制单元生成的SM-DP+质询值。SM-DP+120可以针对包括在步骤210处接收的eUICC质询值和由SM-DP+120生成的SM-DP+质询值的数据计算SM-DP+签名。计算出的SM-DP+签名值可以是SM-DP+signature1(签名1)。SM-DP+signature1是使用SM-DP+私钥计算的。SM-DP+120可以向终端110发送包括SM-DP+signature1和SM-DP+质询值的响应消息。

[0095] 终端110可以验证SM-DP+signature1,并且在验证成功的情况下继续后续过程,或者在验证失败的情况下可以不继续后续过程。

[0096] 如果在步骤220处SM-DP+120被成功验证,则终端110可以在步骤225处针对包括SM-DP+质询的数据生成eUICC签名。eUICC签名可以是eUICC signature1。eUICC signature1可以是使用eUICC 115的私钥创建的签名。终端110可以向SM-DP+120发送包括eUICC signature1和简档信息的消息。该消息可以是认证请求消息(例如,AuthClientRequest(客户端认证请求))。简档信息可以包括用于由SM-DP+120在识别简档或简档的类型时使用的简档映射信息。此时,简档信息可以包括如下简档映射信息:

[0097] -eUICC标识符或EID

[0098] -eUICC证书

[0099] -EventID(事件ID)

[0100] -MatchingID(匹配ID)

[0101] -ActivationToken(激活令牌)

[0102] -NotificationID(通知ID)

[0103] 在步骤230处,SM-DP+120可以从简档映射信息检查对应于特定简档或简档类型的简档信息。

[0104] 在步骤235处,SM-DP+120可以针对包括在步骤230处检查的简档信息的数据计算签名值(SM-DP+signature2(签名2))。SM-DP+120可以向终端110发送签名值(SM-DP+signature2)和简档信息。简档信息可以是未加密的原始简档信息。

[0105] 然后,终端110可以在显示单元上显示在步骤235处接收的简档信息的部分或全部或者映射到简档信息的部分或全部的信息。映射的信息可以是预先存储在终端110中的值或从外部服务器接收的值。用于在映射过程中使用的简档信息的部分或全部如下:

[0106] -IMSI

[0107] -包括MCC或MNC的信息

[0108] -包括MCC和MNC的信息

[0109] -运营商名称

[0110] -构成ICCID信息的一部分的信息

[0111] -运营商代码

[0112] 在步骤245处,终端110可以接收用于简档下载确认的用户输入。也就是说,终端110可以接收用于确认简档下载的用户输入。

[0113] 简档下载确认输入可以如下进行。

[0114] -在使用用户界面(UI)的输入设备(例如,触摸板和按钮)在显示单元上显示“是”项和“否”项的状态下,在对应于“是”项的位置上简单地做出输入动作

[0115] -使用诸如指纹认证和虹膜认证的生物特征认证进行输入

[0116] 终端110可以在步骤250处确定用户是否在用户确认步骤245处确认了简档下载。

[0117] 如果在步骤250处确定用户已确认简档下载,则终端110可以在步骤260处向SM-DP+120请求简档下载。此时,终端110可以响应于简档下载请求信息而生成eUICC签名值(eUICC signature2)。终端110可以向SM-DP+120发送包括eUICC签名值(eUICC signature2)和简档下载请求信息的消息(例如,GetBoundProfilePackage(取得绑定简档包))。

[0118] 在步骤270处,SM-DP+120可以根据在步骤260处接收的简档下载请求信息向终端110发送加密的简档。

[0119] 然后,终端110可以在步骤280处解码加密的简档并安装简档。简档解码可以在终端110的eUICC 115中执行。

[0120] 如果在步骤250处确定用户没有确认简档下载,则终端110可以在步骤290处向SM-DP+120发送简档下载拒绝报告和/或确认结果。然后,终端110可以停止简档下载过程。

[0121] 如果接收到简档下载拒绝报告,则SM-DP+120可以在步骤295处停止简档下载过程。在这种情况下,SM-DP+120可以响应于简档下载拒绝报告而向终端110发送确认(ACK)消息。

[0122] 对于本领域技术人员明显的是,上述简档下载过程可以应用于其他类型的通信系统。

[0123] 图3是示出根据本发明的实施例的终端的简档下载方法的信号流程图。

[0124] 参考图3,在步骤310处,终端110可以生成用于验证服务器的服务器验证信息。服务器验证信息可以是随机值,例如,质询值。质询值可以由终端110的控制单元或连接到终端110的eUICC 115来生成,并且可以被称为eUICC质询值。终端110可以向简档提供服务器120发送包括服务器验证信息的消息。该消息可以是初始认证请求消息(例如,IniAuthRequest)。简档提供服务器120可以是SM-DP+。终端110可以包括负责终端110的一部分操作的eUICC 115。

[0125] 在步骤315处,SM-DP+120可以生成用于验证终端110的终端验证信息。终端验证信息可以是随机值,例如,可以由SM-DP+120的控制单元生成的SM-DP+质询值。SM-DP+120可以针对包括在步骤310处接收的eUICC质询值和由SM-DP+120生成的SM-DP+质询值的数据计算签名值。此时,SM-DP+签名值可以是SM-DP+signature1。SM-DP+signature1可以是使用SM-DP+私钥计算的值。SM-DP+120可以向终端110发送包括SM-DP+signature1和SM-DP+质询值的响应消息。

[0126] 终端110可以在步骤320处验证SM-DP+signature1,并且在SM-DP+验证成功的情况下继续该过程,或者在SM-DP+验证失败的情况下可以停止该过程。

[0127] 如果在步骤320处SM-DP+验证成功,则终端110可以在步骤325处针对包括SM-DP+

质询的数据生成eUICC签名。eUICC签名可以是eUICC signature1。eUICC signature1可以是使用eUICC 115的私钥生成的签名。终端110可以向SM-DP+120发送包括eUICC signature1和简档信息的消息。该消息可以是认证请求消息(例如,AuthClientRequest)。简档信息可以包括用于由SM-DP+120在识别简档或简档的特定类型时使用的简档映射信息。简档信息可以包括如下简档映射信息:

[0128] -eUICC标识符或EID

[0129] -eUICC证书

[0130] -EventID

[0131] -MatchingID

[0132] -ActivationToken

[0133] -NotificationID

[0134] 在步骤330处,SM-DP+120可以从简档映射信息检查对应于特定简档或简档类型的简档信息。

[0135] SM-DP+120可以确定是否需要用户的确认码输入来下载相应的简档。如果SM-DP+120具有指示是否需要用户的确认码输入的信息,则它可以检查相应的信息。

[0136] 在步骤335处,SM-DP+120可以针对包括在步骤330处检查的简档信息的数据计算签名值(SM-DP+signature2)。SM-DP+120可以发送签名值(SM-DP+signature2)、未加密的简档信息、以及指示是否需要确认码输入的信息(ConformationCodeRequired(需要确认码))。例如,指示是否需要确认码输入的信息可以是1位信号,对于不需要确认码输入的情况,该1位信号被设置为0,或者对于需要确认码输入的情况,该1位信号被设置为1。简档信息可以是未加密的简档信息。

[0137] 在步骤340处,终端110可以在显示单元上显示在步骤335处接收的简档信息的部分或全部或者映射到简档信息的部分或全部的信息。映射的信息可以是预先存储的值或从外部服务器接收的值。用于在映射过程中使用的简档信息的部分或全部可以包括如下信息:

[0138] -IMSI

[0139] -包括MCC或MNC的信息

[0140] -包括MCC和MNC的信息

[0141] -运营商名称

[0142] -构成ICCID信息的一部分的信息

[0143] -运营商代码

[0144] 在步骤345处,终端110可以接收用户对简档下载的确认。也就是说,用户可以对终端110做出用于确认简档下载的输入。

[0145] 简档下载确认输入可以如下进行。

[0146] -在使用用户界面(UI)的输入设备(例如,触摸板和按钮)在显示单元上显示“是”项和“否”项的状态下,仅做出到对应于“是”项的位置的输入动作

[0147] -使用诸如指纹认证和虹膜认证的生物特征认证进行输入

[0148] 与用户的确认过程同时或分开地、或者在没有用户的确认过程的情况下,终端110可以通过检查从SM-DP+120接收的相应信息来确定是否需要确认码。如果接收到指示是否

需要确认码输入的信息，则终端110可以通过UI向用户询问确认码并接收确认码输入。然后，终端110可以对由用户输入的确认码和在步骤315处接收的SM-DP+质询信息执行散列运算。终端110可以通过散列运算生成修改的确认码(或散列确认码(散列的确认码))。散列运算可以被执行一次或多次以隐藏确认码。也可以使用SM-DP+质询值进行运算，使得每次生成唯一的散列结果值。该运算可以由终端110的一个或多个CPU来执行。例如，可以通过具有负责运算的一部分的应用处理器(AP)和负责运算的其余部分的调制解调器或eUICC 115来改进安全性。

[0149] 在步骤350处，终端110可以确定用户是否已确认在步骤345处的简档下载。

[0150] 如果在步骤350处确定用户已确认简档下载，则终端110可以在步骤360处向SM-DP+120请求简档下载。此时，终端110可以针对简档下载请求信息而生成eUICC签名值(eUICC signature2)。终端110可以向SM-DP+120发送包括eUICC签名值(eUICC signature2)和简档下载请求信息的请求消息(例如，GetBoundProfilePackage)。

[0151] 请求消息可以包括散列的确认码。

[0152] 在步骤365处，SM-DP+120可以验证散列的确认码。

[0153] SM-DP+120可以确定在步骤360处接收的请求消息是否包括散列的确认码。如果在步骤350处接收的请求消息不包括散列的确认码，则SM-DP+120可以执行步骤375。

[0154] 如果在步骤360处接收的请求消息包括散列的确认码，则SM-DP+120可以自己计算散列的确认码。SM-DP+120可以确定计算出的散列的确认码与接收到的散列的确认码是否匹配。

[0155] 如果这两个码匹配，则SM-DP+120可以执行步骤370。

[0156] 否则，如果这两个码不匹配，则SM-DP+120可以向终端110发送包括指示简档下载失败的信息的消息并结束该过程。

[0157] 在步骤370处，SM-DP+120可以根据在步骤360处接收的简档下载请求信息向终端110发送加密的简档。

[0158] 然后，终端110可以在步骤380处解码加密的简档并安装简档。简档解码可以在终端110的eUICC 115中执行。

[0159] 如果在步骤350处确定用户没有确认简档下载，则终端110可以在步骤390处向SM-DP+发送简档下载拒绝报告和/或确认结果。然后，终端110可以结束简档下载过程。

[0160] 如果接收到简档下载拒绝报告，则SM-DP+120可以在步骤395处结束简档下载过程。此时，SM-DP+120可以响应于简档下载拒绝报告而向终端110发送确认(ACK)消息。

[0161] 对于本领域技术人员明显的是，上述简档下载过程可以应用于其他类型的通信系统。

[0162] 图4是示出根据本发明的另一实施例的终端的简档下载方法的信号流程图。

[0163] 参考图4，在步骤410处，终端110可以生成用于验证服务器的服务器验证信息。服务器验证信息可以是随机值，例如，质询值。质询值可以由终端110的控制单元或连接到终端110的eUICC 115来生成，并且可以被称为eUICC质询值。终端110可以向简档提供服务器120发送包括服务器验证信息的消息。该消息可以是初始认证请求消息(例如，IniAuthRequest)。简档提供服务器120可以是SM-DP+。终端110可以包括负责终端110的一部分操作的eUICC 115。

[0164] 在步骤415处,SM-DP+120可以生成用于验证终端110的终端验证信息。终端验证信息可以是随机值,例如,可以由SM-DP+120的控制单元生成的SM-DP+质询值。SM-DP+120可以针对包括在步骤410处接收的eUICC质询值和由SM-DP+120生成的SM-DP+质询值的数据计算签名值。此时,SM-DP+签名值可以是SM-DP+signature1。SM-DP+signature1可以是使用SM-DP+私钥计算的值。SM-DP+120可以向终端110发送包括SM-DP+signature1和SM-DP+质询值的响应消息。

[0165] 终端110可以在步骤420处验证SM-DP+signature1,并且在SM-DP+验证成功的情况下继续该过程,或者在SM-DP+验证失败的情况下可以停止该过程。

[0166] 如果在步骤420处SM-DP+验证成功,则终端110可以在步骤425处针对包括SM-DP+质询的数据生成eUICC签名。eUICC签名可以是eUICC signature1。eUICC signature1可以是使用eUICC 115的私钥生成的签名。终端110可以向SM-DP+120发送包括eUICC signature1和简档信息的消息。该消息可以是认证请求消息(例如,AuthClientRequest)。简档信息可以包括用于由SM-DP+120在识别简档或简档的特定类型时使用的简档映射信息。简档信息可以包括如下简档映射信息:

[0167] -eUICC标识符或EID

[0168] -eUICC证书

[0169] -EventID

[0170] -MatchingID

[0171] -ActivationToken

[0172] -NotificationID

[0173] 在步骤430处,SM-DP+120可以从简档映射信息检查对应于特定简档或简档类型的简档信息。

[0174] SM-DP+120可以确定是否需要用户的确认码输入来下载相应的简档。如果SM-DP+120具有指示是否需要用户的确认码输入的信息,则它可以检查相应的信息。

[0175] 如果用户需要输入确认码,则SM-DP+120可以生成第一修改的确认码(或第一散列确认码(散列的确认码1))以保护终端110免受恶意运营商或服务器的影响。此时,可以如下计算散列的确认码1:

[0176] 散列的确认码1=散列函数(确认码,随机数A)

[0177] 此时,可以从运营商接收确认码,并且随机数A可以是终端110已经知道或将知道的任意随机值。例如,随机数A可以是eUICC质询或SM-DP+质询。

[0178] 散列函数可以是用于对确认码和随机数A的输入因子执行一个或多个散列运算的函数。可以如下计算散列的确认码1:

[0179] 散列的确认码1=SHA256(确认码|SM-DP+质询)

[0180] 如果SM-DP+120将散列的确认码1发送给终端110,则终端110可以基于用户在步骤445处输入的确认码来计算散列的确认码1。通过比较计算的散列的确认码1与接收到的散列的确认码1,可以防止终端110从未知的恶意运营商或SM-DP+120下载简档。

[0181] 在步骤435处,SM-DP+120可以针对包括在步骤430处获取的简档信息的数据计算签名值(SM-DP+signature2)。SM-DP+120可以向终端110发送签名值(SM-DP+signature2)、未加密的简档信息、指示是否需要确认码输入的信息(ConformationCodeRequired)、以及

散列的确认码1。例如，指示是否需要确认码输入的信息可以是1位信号，对于不需要确认码输入的情况，该1位信号被设置为0，或者对于需要确认码输入的情况，该1位信号被设置为1。简档信息可以是未加密的简档信息。

[0182] 在步骤440处，终端110可以在显示单元上显示在步骤435处接收的简档信息的部分或全部或者映射到简档信息的部分或全部的信息。映射的信息可以是预先存储的值或从外部服务器接收的值。用于在映射过程中使用的简档信息的部分或全部可以包括如下信息：

[0183] -IMSI

[0184] -包括MCC或MNC的信息

[0185] -包括MCC和MNC的信息

[0186] -运营商名称

[0187] -构成ICCID信息的一部分的信息

[0188] -运营商代码

[0189] 在步骤445处，终端110可以接收用户对简档下载的确认。也就是说，用户可以对终端110做出用于确认简档下载的输入。

[0190] 简档下载确认输入可以如下进行。

[0191] -在使用用户界面(UI)的输入设备(例如，触摸板和按钮)在显示单元上显示“是”项和“否”项的状态下，仅做出到对应于“是”项的位置的输入动作

[0192] -使用诸如指纹认证和虹膜认证的生物特征认证进行输入

[0193] 与用户的确认过程同时或分开地、或者在没有用户的确认过程的情况下，终端110可以通过检查从SM-DP+120接收的相应信息来确定是否需要确认码。如果接收到指示是否需要确认码输入的信息，则终端110可以通过UI向用户询问确认码并接收确认码输入。

[0194] 终端110可以使用用户输入的确认码和在步骤415处接收的SM-DP+质询信息来验证由SM-DP+120在步骤435处发送的散列的确认码1。也就是说，终端110可以使用用户输入的确认码和在步骤415处接收的SM-DP+质询信息自己计算散列的确认码1。然后，终端110可以确定计算出的散列的确认码1是否与从SM-DP+120接收到的散列的确认码1相同。

[0195] 终端110可以计算第二修改的确认码(或第二散列确认(散列的确认码2))。散列运算可以被执行一次或多次以隐藏确认码。也可以使用SM-DP+质询值进行运算，使得每次生成唯一的散列结果值。可以利用不同于散列的确认码1的公式来计算散列的确认码2。此运算可以由终端110的一个或多个CPU来执行。例如，可以通过具有负责运算的一部分的应用处理器(AP)和负责运算的其余部分的调制解调器或eUICC 115来改进安全性。

[0196] 在步骤450处，终端110可以确定用户是否已确认在步骤445处的简档下载。

[0197] 如果在步骤450处确定用户已确认简档下载，则终端110可以在步骤455处确定散列的确认码1是否被成功验证。

[0198] 如果用户在步骤450处已确认简档下载并且如果在步骤435处从SM-DP+120接收到的散列的确认码1与在步骤445处由终端110计算出的散列的确认码1匹配，则终端110可以在步骤460处向SM-DP+120请求简档下载。此时，终端110可以针对简档下载请求信息生成eUICC签名值(eUICC signature2)。终端110可以向SM-DP+120发送包括eUICC签名值(eUICC signature2)和简档下载请求信息的请求消息(例如，GetBoundProfilePackage)。

[0199] 请求消息可以包括散列的确认码2。

[0200] 在步骤465处,SM-DP+120可以验证散列的确认码2。

[0201] SM-DP+120可以确定在步骤460处从终端110接收的请求消息是否包括散列的确认码2。如果请求消息不包括散列的确认码2,则SM-DP+120可以执行步骤475。

[0202] 如果在步骤460处接收的请求消息包括散列的确认码2,则SM-DP+120可以自己计算散列的确认码2。然后,SM-DP+120可以确定计算出的散列的确认码2和接收到的散列的确认码2是否匹配。

[0203] 如果这两个码值匹配,则SM-DP+120可以执行步骤470。

[0204] 如果这两个码值不匹配,则SM-DP+120可以向终端110发送包括指示简档下载失败的信息的消息并结束该过程。

[0205] 在步骤470处,SM-DP+120可以根据在步骤460处接收的简档下载请求信息向终端110发送加密的简档。

[0206] 然后,在步骤480处,终端110可以解码加密的简档并安装简档。简档解码可以在终端110内的eUICC 115中执行。

[0207] 如果用户在步骤450处拒绝简档下载或在步骤455处散列的确认码不匹配,则终端110可以在步骤490处向SM-DP+120发送简档下载拒绝报告和/或确认结果和/或确认码不匹配结果。然后,终端110结束简档下载过程。

[0208] 根据本发明的一个实施例,当散列的确认码1值不匹配时,终端110可以向用户询问确认码,将输入的确认码与散列的确认码1进行比较,并且根据比较结果执行步骤460。

[0209] 如果接收到简档下载拒绝报告,则SM-DP+120可以在步骤495处结束简档下载过程。此时,SM-DP+120可以响应于简档下载拒绝报告向终端110发送ACK消息。

[0210] 对于本领域技术人员明显的是,上述简档下载过程可以应用于其他类型的通信系统。

[0211] 图5是示出根据本发明的另一实施例的简档下载方法的信号流程图。在本实施例中,终端和SM-DP+在简档下载过程期间交换用于正常签名和加密处理的签名和加密参数。

[0212] 参考图5,在步骤510处,终端110可以生成用于验证服务器的服务器验证信息。服务器验证信息可以是随机值,例如质询值。质询值可以由终端110的控制单元或连接到终端110的eUICC 115生成,并且可以被称为eUICC质询值。终端110可以向简档提供服务器120发送包括服务器验证信息、eUICC签名和加密参数的消息。该消息可以是初始认证请求消息(InitAuthRequest)。简档提供服务器120可以是SM-DP+。eUICC签名和加密参数可以被包括在向SM-DP+120发送的eUICC信息(eUICC Info)中。此时,eUICC质询可以是签名创建算法,并且eUICC签名可以是签名验证算法。

[0213] 可以将签名创建算法、签名验证算法和加密参数间接地通知给SM-DP+120,而不是如图5的图中所示直接发送。例如,可以在终端110与SM-DP+120之间定义参考识别信息。在这种情况下,如果终端110根据参考识别信息值向SM-DP+120发送预定值,则SM-DP+120可以根据接收到的参考识别信息值检查签名创建算法、签名验证算法和加密参数。例如,如果参考识别信息被设置为1,则终端110和SM-DP+120采用A的签名创建算法、B的签名验证算法和C的加密参数。此时,如果终端110向SM-DP+120发送被设置为1的参考识别信息,则SM-DP+120可以检查签名创建算法、签名验证算法和加密参数。

[0214] 如果终端110(或eUICC 115)确定使用特定信息,则SM-DP+120可以基于特定信息来检查签名创建算法、签名验证算法和加密参数。例如,当终端110确定使用特定参数时,在终端110与SM-DP+120之间可以存在假定使用预定的签名创建算法、签名验证算法和加密参数的协议。此时,如果终端110通知SM-DP+120使用特定参数,则SM-DP+120可以基于该通知来检查签名创建算法、签名验证算法和加密参数。例如,如果终端110确定使用某个证书发布者(CI),则SM-DP+120可以根据CI信息(CIInfo)检查签名创建算法、签名验证算法和加密参数。

[0215] 在步骤515处,SM-DP+120可以生成用于验证终端110的终端验证信息。此时,终端验证信息可以是随机值,例如,由SM-DP+120的控制单元生成的SM-DP+质询值。SM-DP+120可以针对包括在步骤510处接收到的eUICC质询值和由SM-DP+120生成的SM-DP+质询值的数据计算SM-DP+签名。此时,SM-DP+签名可以是SM-DP+signature1。

[0216] 同时,SM-DP+120可以基于在步骤510处接收的eUICC签名和加密参数来选择最佳签名和加密参数。SM-DP+120可以选择要被eUICC 115使用的签名和加密参数,并将它们发送到终端110(或eUICC 115)。如果在从eUICC115接收的信息中没有可支持的参数,则SM-DP+120可以拒绝来自eUICC115的请求,并向终端110发送拒绝消息。

[0217] 可以使用SM-DP+私钥来计算SM-DP+signature1。SM-DP+120可以向终端110发送包括SM-DP+signature1和SM-DP+质询值的响应消息。响应消息可以包括签名和加密参数以供eUICC 115使用。

[0218] 步骤520至595类似于图4的步骤420至495;因此,在此省略其详细描述。

[0219] 图6a至图6c是示出根据本发明的实施例的本发明的简档下载方法的信号流程图。

[0220] 参考图6a至图6c,终端110向SM-DP+140询问信息而不暴露终端标识符(例如,EID)以便在简档下载期间保证私有信息安全。

[0221] 如下有条件地执行图6a至6c的过程610至630。

[0222] 当LPA(即,终端110)具有eUICC证书(CERTS_eUICC)、通过使EID散列而获得的受保护的EID、以及eUICC信息时,可以省略过程610。同时,终端110包括LPA,并且在此实施例中,LPA执行终端110的操作。

[0223] 当简档管理服务器(SM-SR+130)或简档提供服务器(SM-DP+120)向MNO 150请求用与SM-DS 140相关联的简档的指示进行简档下载时,可以执行过程620。

[0224] 当终端110(LPA)已经接收到eventType(事件类型)、dpToken1和srToken1信息时,可以省略过程630。

[0225] 下文中详细描述各个步骤。

[0226] 终端110可以通过步骤611和612从eUICC 115读取CERTS_eUICC。CERTS_eUICC可以包括eUICC证书和EUM证书。详细地,终端110可以在步骤611处向eUICC 115发送包括CERTS_eUICC请求信息(GetCert(获得证书))的LocalManagementRequest(本地管理请求)消息,并且在步骤612处从eUICC 115接收包括CERTS_eUICC的LocalManagementResponse(本地管理响应)消息。

[0227] 终端110可以通过步骤613和614从eUICC 115读取受保护的EID值。受保护的EID可以包括以下信息项中的至少一个:

[0228] 时间信息,

[0229] EID或散列的EID值，

[0230] EID的签名值。

[0231] 可以利用时间信息计算散列的EID值或EID的签名值。为了实现这一点，终端110可以向eUICC 115发送包括受保护的EID值请求信息(GetEID(获得EID))的LocalManagementRequest消息，并且从eUICC 115接收包括受保护的EID值的LocalManagementResponse消息。

[0232] 终端110可以通过步骤615和616从eUICC 115获取eUICCInfo(eUICC信息)。

[0233] eUICCInfo可以包括如下信息：

[0234] eUICC的签名和用于加密的椭圆曲线参数，

[0235] eUICC的剩余存储容量(memory size)。

[0236] 详细地，终端110可以在步骤615处向eUICC 115发送包括eUICCInfo请求信息(GetEUICCInfo(获得EUICCInfo))的LocalManagementRequest消息，并且在步骤616处从eUICC 115接收包括eUICCInfo的LocalManagementResponse消息。

[0237] 在eUICCManagementRequest(eUICC管理请求)、简档下载请求或简档管理请求消息包括指示利用SM-DS 140的简档下载处理或简档管理的指示信息的情况下，SM-SR+130或SM-DP+120可以通过步骤621和622向SM-DS140请求事件注册。详细地，SM-SR+130可以在步骤621处向SM-DS 140发送包括简档映射信息(EventID)、EID和服务器ID(SRID)的RegisterEventRequest(注册事件请求)消息，并且在步骤622处从SM-DS 140接收包括结果码(ResultCode)的RegisterEventResponse(注册事件响应)消息。

[0238] 在步骤623处，SM-DS 140可以经由推送服务器向终端110发送推送通知。

[0239] 在步骤624处，终端110可以向SM-DS 140发送包括受保护的EID的EventID(简档映射信息)请求消息(EventIDRequest)。然后，SM-DS 140可以验证受保护的EID。具体地，如果包括在受保护的EID中的时间点与接收到EventID请求消息的时间点之间的时间间隔大于预定范围，则SM-DS 140验证受保护的EID失败。验证过程还可以包括验证散列值或签名值的有效性。如果任何验证失败，则SM-DS 140可以不回复，或可以向终端110发送包括与拒绝原因对应的响应码的响应消息。

[0240] 在步骤625处，SM-DS 140可以向终端110发送EventID和服务器信息(SRID)的一个或多个信息对。服务器地址(SRID)包括用于处理相应的EventID的服务器的地址，并且相应的服务器可以是SM-DS 140、SM-DP+120或SM-SR+130。根据本发明的实施例，如果没有EventID，则SM-DS 140可以不发送EventID信息。为了便于说明，在步骤631处假定服务器地址是SM-DP+120或SM-SR+130的地址。

[0241] 如果终端110通过先前的步骤获取EventID和服务器地址，则终端110可以向SM-SR+130或SM-DP+120请求EventID处理过程。EventID处理过程可以是下述各项之一：下载简档、远程管理简档、远程管理eUICC以及返回其他EventID和服务器地址。此时，终端110可以向SM-SR+130或SM-DP+120请求利用终端信息(terminal Info)或eUICC信息(eUICC Info)处理相应的EventID。在终端110向SM-SR+130发出请求的情况下，SM-DP+120可以向该请求添加或从该请求删除。终端信息可以包括终端的IMEI或其一部分。

[0242] 在SM-SR+130或SM-DP+120检查终端信息或eUICC信息的情况下，如果至少一项信息不被SM-SR+130或SM-DP+120支持，则SM-SR+130或SM-DP+120可以拒绝相应的请求并结束

过程。例如，如果SM-SR+130或SM-DP+120不支持包括在eUICC信息中的ECC签名参数或加密参数，则它可以拒绝该请求。如果SM-SR+130或SM-DP+120支持包括在eUICC信息中的ECC签名参数和加密参数之一或两者，则它可以选择用于在签名验证、签名创建和加密时使用的可支持参数。

[0243] 如果SM-DP+120接收到来自SM-SR+130的请求，则SM-DP+120可以在步骤633处验证包括在EventID中的SM-SR+标识符与包括在SM-SR+130的证书中的SM-SR+标识符是否匹配。此时，SM-SR+130的证书可以是用于ECDSA签名的证书。

[0244] 在步骤634处，SM-DP+120可以创建用于简档加密的非对称密钥对(ECKA临时密钥对)。

[0245] 在步骤635处，SM-DP+120可以创建DPToken1。此时，DPToken1可以包括如下信息项中的至少一个：

[0246] profileRecordPart1(简档记录部分1，包括简档明文信息的一部分)

[0247] ePK_DP_ECKA(临时非对称密钥对的公钥)

[0248] sign_DP1(SM-DP+signature1)

[0249] cert_DP_ECDSA(用于签名的SM-DP+证书)

[0250] cert_DP_ECKA(用于加密的SM-DP+证书)

[0251] confirmType(用户确认类型)

[0252] confirmMessage(获取用户确认时的消息)

[0253] confirmCodeHash1(确认码散列值1)

[0254] 具体地，如果confirmType包括需要用户的确认码输入的值，则SM-DP+120可以生成确认码散列值1。

[0255] 如果从已经向用户发出确认码的运营商正常接收到确认码的SM-DP+120向终端110发送正常确认码散列值1，则终端110可以基于用户输入的确认码验证SM-DP+120以验证简档不是从异常服务器下载的。

[0256] 即使对于特定简档确认码是固定的，SM-DP+120也可以每次生成唯一的确认码散列值1。例如，SM-DP+120可以如下生成确认码散列值1：

[0257] 由SM-DP+120生成的confirmCodeHash1＝SHA256(ePK_DP_ECKA|确认码)

[0258] 此时，确认码可以是SM-DP+120从运营商接收的值。

[0259] 以这种方式生成的确认码散列值1被发送到终端110;因此，如果用户输入的确认码与SM-DP+120发送的信息不匹配，则在终端110处阻止简档下载。此时，终端110可以将接收到的确认码散列值1与其自己计算出的确认码散列值1进行比较。根据本发明的实施例，终端110计算出的确认码散列值可以是利用用户输入的确认码和从SM-DP+120接收的ePK_DP_ECKA值的SHA256(ePK_DP_ECKA|确认码)公式的结果值。

[0260] SM-DP+120和终端110也可以使用另一个公式生成confirmCodeHash1值，但是即使在这种情况下，确认码和每次唯一生成的值也被用作因子。例如，可以使用以下等式生成confirmCodeHash1(确认码散列值1)：

[0261] confirmCodeHash1＝SHA256(ePK_DP_ECKA|SHA256(确认码))。

[0262] 在步骤636处，SM-DP+120可以向SM-SR+130发送包括DPToken1的响应消息。此时，响应消息可以是ES3_DownloadProfileResponse(ES3_下载简档响应)。

[0263] 在步骤637处,SM-SR+130可以生成SRToken1。

[0264] 此时,SRToken1可以包括以下信息项中的至少一个:

[0265] SM-SR+证书

[0266] 一次性随机值

[0267] SM-SR+签名值

[0268] 此时,可以使用一次性随机值来保护终端110免受通过重新使用签名值而进行的回放攻击。之后,SM-SR+130可以使用一次性随机值来验证终端110的签名以认证终端110。

[0269] 在步骤638处,SM-SR+130可以向终端110发送响应消息。此时,响应消息可以是ES9_EventResponse(ES9_事件响应)。

[0270] ES9_EventResponse可以包括以下信息项中的至少一个:

[0271] resultCode

[0272] eventType

[0273] srToken1

[0274] dpToken1

[0275] eventType表示关于下载简档(downloadProfile)的信息,并且根据本发明的实施例包括DPToken1。

[0276] 如果在步骤631处接收的ES9_EventRequest中包括的EventID无效,则SM-SR+130可以向终端110发送包括包含错误信息的resultCode的ES9_EventResponse。在步骤675处,SM-SR+130可以向SM-DS 140发送包括EventID的ES12_DeleteEventRequest(ES12_删除事件请求)。

[0277] 在步骤639处,终端110可以向eUICC115发送认证数据请求消息。认证数据请求消息可以是ES10_GetAuthDataRequest(ES10_获得认证数据请求)。

[0278]

ES10_GetAuthDataRequest 可以包括以下信息项中的至少一个:

eventID

eventType

srToken1

dpToken1

terminalType(终端类型)

provisioningType(提供类型)

terminalType 信息可以包括如下的终端身份信息:

```
TerminalType ::= ENUMERATED {
   without_UI (0),
   with_UI (1)
}
```

[0279] provisioningType信息可以包括指示在简档下载过程中是否涉及SM-DS140的信

息。

[0280]
```
ProvisioningType ::= ENUMERATED {
   without_SM-DS (0),
   with_SM-DS (1)
}
```

[0281] 如果eventType被设置为“downloadProfile”,则ES10_GetAuthDataRequest消息可以包括dpToken1、terminalType和provisioningType。

[0282] eUICC 115可以在步骤641处验证srToken1。

[0283] 此时,验证过程可以如下进行。eUICC 115可以使用PK_CI_ECDSA来验证CERT_SR_ECDSA。eUICC 115可以从CERT_SR_ECDSA中提取PK_SR_ECDSA,并且用PK_SR_ECDSA和NONCE_SR验证SIGN_SR1。eUICC 115可以将PK_SR_ECDSA和NONCE_SR与eventID一起存储以供稍后在步骤659处使用。

[0284] 如果eventType被设置为“downloadProfile”,则eUICC 115可以创建并识别用于存储简档的安全域。

[0285] 之后,eUICC 115可以验证dpToken1。

[0286] 验证过程可以如下进行。eUICC 115可以使用PK_CI_ECDSA来验证CERT_DP_ECDSA。eUICC 115可以从CERT_DP_ECDSA中提取PK_DP_ECDSA,并用PK_DP_ECDSA和ePK_DP_ECKA验证SIGN_DP1。eUICC 115可以使用PK_CI_ECDSA来验证CERT_DP_ECKA。eUICC 115可以从CERT_DP_ECKA中提取PK_DP_ECKA。之后,eUICC 115可以存储PK_DP_ECDSA、PK_DP_ECKA和ePK_DP_ECKA以供稍后在步骤659处使用。eUICC 115还可以存储profileRecordPart1以供稍后在步骤662处使用。

[0287] 如果任何验证失败,则eUICC 115可以向终端110发送错误消息。

[0288] 如果srToken1和dpToken1被成功验证,则在步骤642处,eUICC 115可以具有验证的信息,诸如SRID、DPID、EventID、EventType、TargetEID(目标EID)、ProfileType(简档类型)、ProfileDescription(简档描述)、MNO的PLMNID、TerminalType、ConfirmType和ProvisioningType。

[0289] 利用这样的信息,eUICC 115可以如下确定是否继续简档下载过程:

[0290] -eUICC 115可以根据eUICC的配置验证是否允许包括在CERT_RR_ECDSA中的SRID。

[0291] -eUICC 115可以根据eUICC的配置验证是否允许包括在CERT_DP_ECDSA中的DPID。

[0292] -eUICC 115可以根据eUICC的配置验证是否允许PLMNID。

[0293] -如果TerminalType被设置为“without_UI”,则eUICC 115可以验证ConfirmType是否是“yesOrNo(是或否)”。

[0294] -如果TerminalType被设置为“with_UI”,ConfirmType被设置为“yesOrNo”,并且ProvisioningType被设置为“with_SM-DS”,则eUICC 115可以根据eUICC的配置验证是否允许PLMNID。

[0295] 如果全部验证成功,则eUICC 115可以继续简档下载过程。

[0296] 如果任何验证失败,则eUICC 115可以拒绝该事件并发送包括拒绝原因的响应消息。

[0297] eUICC 115可以创建临时公钥(ePK_eUICC_ECKA)和临时私钥(eSK_eUICC_ECKA)的对。

[0298] eUICC 115可以将ePK_eUICC_ECKA、eSK_eUICC_ECKA、PK_SR_ECDSA、PK_DP_ECDSA和NONCE_SR与EventID一起存储。

[0299] eUICC 115可以在步骤644处创建eUICC令牌(EUICCToken)。

[0300] 此时,EUICCToken可以包括如下信息中的至少部分:

[0301] eventID

[0302] sign_eUICC(由eUICC创建的签名)

[0303] nonce_eUICC(由eUICC生成的一次性随机值)

[0304] ePK_eUICC_ECKA(由eUICC生成的临时非对称密钥对的公钥)

[0305] eUICCInfo EUICCInfo

[0306] 可以用SK_eUICC_ECDSA来计算eUICC签名(sign_eUICC)。

[0307] 在计算中包括NONCE_SR,用于SM-SR+130认证eUICC 115,并且在计算中包括ePK_DP_ECKA,用于SM-DP+120认证eUICC 115。

[0308] eUICC 115可以生成并存储会话密钥以供稍后在步骤660处使用。此时,可以与会话密钥一起生成收据(Receipt)。收据可以用作第一个SCP03t CommandTLV(SCP03t命令TLV)的初始MAC链接值。

[0309] 在步骤645处,eUICC 115可以向终端110发送ES10_GetAuthDataResponse(ES10_获得认证数据响应)消息。

[0310] ES10_GetAuthDataResponse消息可以包括以下信息项中的至少一个:

[0311] resultCode结果码

[0312] eUICCToken

[0313] 如果在步骤645处接收的ES10_GetAuthDataResponse消息中包括的resultCode被设置为“拒绝”,则终端110可以在步骤670处向SM-SR+130发送ES9_NotifyResultRequest(ES9_通知结果请求)消息。发送到SM-SR+130的ES9_NotifyResultRequest消息可以包括与ES10_GetAuthDataResponse消息(包括在步骤670的消息中的EventResult(事件结果)信息)相同的结果码。否则,如果在步骤645处接收的ES10_GetAuthDataResponse消息中包括的resultCode被设置为“成功”,则在步骤646处终端110可以向用户询问确认码。

[0314] -如果dpToken1.confirmType被设置为“yesOrNo”,则终端110可以向用户呈现诸如eventType和profileRecordPart1的必要信息以要求明确同意执行eUICC管理事件。

[0315] -如果dpToken1.confirmType被设置为“codeInput(码输入)”,则终端110可以在订阅过程期间向用户询问从MNO 150接收的确认码。终端110可以使用以下公式验证接收到的dpToken1.confirmCodeHash1是否正确:

[0316] SHA256(dpToken1.ePK_DP_ECKA|用户输入的确认码)

[0317] 如果验证成功,则SM-DP+120可以向SM-SR+130发送错误消息。

[0318] -如果ES9_EventResponse消息包括dpToken1.confirmMessage,则终端110可以在请求确认时向用户呈现上述消息。

[0319] -例外地,如果终端110是没有UI的M2M设备并且confirmType被设置为“yesOrNo”,则终端110可以省略用户确认过程。

[0320] 如果用户接受简档下载,则终端110可以在步骤647处向SM-SR+130发送ES9_eUICCManagementRequest(ES9_eUICC管理请求)消息。

[0321] ES9_eUICCManagementRequest消息可以包括如下信息的至少部分:

[0322] eUICCToken

[0323] confirmCodeHash2由终端计算出的确认散列码值2

[0324] certs_eUICC CERTS_eUICC

[0325] 此时,可以由终端110如下计算confirmCodeHash2。

[0326] SHA256(ePK_eUICC_ECKA|ePK_DP_ECKA|用户输入的确认码)

[0327] 否则,如果用户拒绝简档下载,则终端110可以在步骤670处向SM-SR+130发送ES9_NotifyResultRequest消息。此时,ES9_NotifyResultRequest消息可以包括设置为“用户拒绝”的resultCode和相应的eventID。

[0328] 在步骤648处,SM-SR+130可以验证eUICCToken和CERTS_eUICC。

[0329] 验证过程可以如下进行。SM-SR+130可以使用存储在SM-SR+130中的CERT_CI_ECDSA和以CERTS_eUICC传送的CERT_EUM_ECDSA来验证CERT_eUICC_ECDSA。

[0330] SM-SR+130从CERT_eUICC_ECDSA中提取PK_eUICC_ECDSA,并使用PK_eUICC_ECDSA、ePK_DP_ECKA和NONCE_SR验证sign_eUICC。SM-SR+130可以使用与eventID一起存储的ePK_DP_ECKA和NONCE_SR值。

[0331] 如果任何验证失败,则SM-SR+130可以向终端110和SM-DP+120发送错误值。

[0332] 如果全部验证成功,则这可以意味着SM-SR+130成功认证eUICC 115。

[0333] 在步骤649处,SM-SR+130可以向SM-DP+120发送ProfileRequest(简档请求)消息。

[0334] ES3_ProfileRequest消息可以包括如下信息中的至少部分:

[0335] eUICCToken

[0336] nonce_SR

[0337] confirmCodeHash2

[0338] certs_eUICC

[0339] SM-DP+120可以在步骤651处验证eUICCToken和CERTS_eUICC。

[0340] 验证过程可以如下进行。SM-DP+120可以使用存储在SM-DP+120中的CERT_CI_ECDSA和以CERTS_eUICC传送的CERT_EUM_ECDSA来验证CERT_eUICC_ECDSA和CERT_eUICC_ECKA。

[0341] SM-DP+120可以从CERT_eUICC_ECDSA中提取PK_eUICC_ECDSA,并使用PK_eUICC_ECDSA、ePK_DP_ECKA和ONCE_SR验证sign_eUICC。在步骤649处,SM-DP+120可以使用与从SM-SR+130接收的eventID和NONCE_SR一起存储的ePK_DP_ECKA。

[0342] 接下来,SM-DP+120可以从CERT_eUICC_ECKA中提取PK_eUICC_ECKA。

[0343] 如果event.userConfirmation.confirmType被设置为“codeInput”,则SM-DP+120可以使用以下公式验证接收到的ES3_ProfileRequest.confirmCodeHash2是否正确:

[0344] SHA256(eUICCToken.ePK_eUICC_ECKA|ePK_DP_ECKA|event.userConfirmation.confirmCode)

[0345] 如果任何验证失败,则SM-DP+120可以向SM-SR+130发送错误值。

[0346] 如果全部验证成功,则这可以意味着SM-DP+120成功认证eUICC 115。

[0347] 在步骤652处,SM-DP+120可以从PK_eUICC_ECKA、SK_DP_ECKA、ePK_eUICC_ECKA和eSK_DP_ECKA导出SCP03t AES会话密钥。

[0348] SCP03tSessionKey(SCP03t会话密钥)可以包括如下信息中的至少部分:

[0349] sENC用于加密出站信息的加密密钥

[0350] sMAC用于出站信息的完整性保护密钥

[0351] sRMAC用于入站信息的完整性保护密钥

[0352] 在步骤653处,SM-DP+120可以生成ProfileInstallPackage(简档安装包)。

[0353] ProfileInstallPackage可以包括如下信息中的至少部分:

[0354] dpToken2DPToken2,

[0355] profileProtectionKey(简档保护密钥)加密密钥修改密钥

[0356] securedProfilePackage(安全简档包)加密的简档

[0357] DPToken2可以包括以下信息:

[0358] sign_DP2SIGN_ECDSA

[0359] sign_DP2是由SM-DP+120生成的签名。

[0360] profileProtectionKey是包括预先生成的SCP03t AES密钥的可选的SCP03tCommand TLV。预先生成的SCP03t AES密钥可以用于保证SecuredProfilePackage安全。TLV可以用在步骤652处接收的SCP03t会话密钥来保护。

[0361] 在步骤654处,SM-DP+120可以向SM-SR+130发送ES3_ProfileResponse(ES3_简档响应)消息。

[0362] ES3_ProfileResponse消息可以包括以下信息:

[0363] resultCode ResultCode,

[0364] profileInstallPackage ProfileInstallPackage

[0365] 在步骤655处,SM-SR+130可以生成srToken2。

[0366] srToken2可以包括以下信息:

[0367] sign_SR2SIGN_ECDSA

[0368] 可以用SK_eUICC_ECDSA来计算签名sign_SR2。

[0369] 在步骤656处,SM-SR+130可以向终端110发送ES9_eUICCManagementResponse(ES9_eUICC管理响应)消息。

[0370] ES9_eUICCManagementResponse消息可以包括以下信息:

[0371] resultCode ResultCode,

[0372] profileInstallPackage ProfileInstallPackage OPTIONAL,

[0373] srToken2SRToken2

[0374] 在步骤657处,终端110可以向eUICC 115发送ES10_EstablishSecureChannelRequest(ES10_建立安全信道请求)消息。

[0375] 如果eUICC 115接收到ES10_EstablishSecureChannelRequest,则其可以在步骤658处首先验证srToken2。

[0376] 验证过程可以如下进行。eUICC 115可以用PK_SR_ECDSA验证sign_SR2。

[0377] 如果验证失败,则eUICC 115可以向终端110发送错误值。

[0378] 如果在步骤685处验证成功,则在步骤659处,eUICC 115可以验证dpToken2。

[0379] 验证过程可以如下进行。eUICC 115可以用PK_DP_ECDSA验证sign_DP2。

[0380] 在步骤641处,eUICC 115可以使用与EventID一起存储的ePK_eUICC_ECKA、NONCE_SR和PK_DP_ECDSA值来验证SIGN_DP2。

[0381] eUICC 115可以用其中存储的PK_CI_ECDSA验证CERT_DP_ECKA。

[0382] 接下来,eUICC 115可以从CERT_DP_ECKA中提取PK_DP_ECKA。

[0383] eUICC 115可以检查存储在CERT_DP_ECKA中的DPID是否与存储在CERT_DP_ECDSA中的DPID相同。

[0384] 如果任何验证失败,则eUICC 115可以向终端110发送错误消息。

[0385] 如果全部验证成功,则这可以意味着SM-DP+120和SM-SR+130成功验证eUICC 115。

[0386] 如果在步骤659处验证失败,则eUICC 115可以在步骤660处使用在步骤644处生成的SCP03t会话密钥打开安全信道(即,在此步骤之后eUICC 115可以解密SCP03tCommandTLV)。

[0387] 在生成会话密钥之后,eUICC 115可以在步骤661处向终端110发送ES10_EstablishSecureChannelResponse(ES10_建立安全信道响应)TLV。

[0388] 在步骤662处,终端110可以向eUICC 115发送ES10_InstallProfileRecordRequest(ES10_安装简档记录请求)消息。

[0389] eUICC 115可以用profileRecordPart2(简档记录部分2)解密securedProfileRecordPart2(安全简档记录部分2)。eUICC 115可以组合从步骤641处的DPToken1获取的profileRecordPart1和profileRecordPart2,以在ProfileRegistry(简档注册处)中生成ProfileRecord。

[0390] 在步骤663处,eUICC 115可以向终端110返回ES10_InstallProfileRecordResponse(ES10_安装简档记录响应)消息。

[0391] 步骤664是可选(optional)步骤,其中如果包括profileProtectionKey TLV的ProfileInstallPackage消息从SM-SR+130/SM-DP+120被递送,则终端110可以向eUICC 115发送携载profileProtectionKey的ES10_UpdateSessionKeyRequest(ES10_更新会话密钥请求)消息。

[0392] 如果eUICC 115接收到ES10_UpdateSessionKeyRequest消息,则eUICC115可以用SCP03tSessionKey(SCP03t会话密钥)来解密profileProtectionKey,并用解密的SCP03tSessionKey替换SCP03t会话密钥。更新后的SCP03t会话密钥可以用于通过建立的安全信道来保护随后的SCP03tCommandTLV。

[0393] 如果会话密钥由ES10_UpdateSessionKeyRequest消息更新,则第一个后续SCP03tCommandTLV可以包括C-MAC。可以用“MAC链接值”来计算C-MAC,以便将其设置为16字节“0x00”。

[0394] 步骤665是可选步骤,其中eUICC 115可以在步骤664之后向终端110返回ES10_UpdateSessionKeyResponse(ES10_更新会话密钥响应)消息。

[0395] 在步骤666处,终端110可以向eUICC 115发送ES10_InstallProfilePackageBlockRequest(ES10_安装简档包块请求)消息。

[0396] 在步骤667处,eUICC 115可以利用会话密钥来解密securedProfilePackageBlock(安全简档包块)。解密的ProfilePackageBlock(简档包块)可以包括一个或多个简档元素

(PE)和/或PE的部分。PE的部分可以与PE的先前存储的部分组合以形成单个完整的PE。如果解密和可能的组合导致一个或多个完整的PE,则eUICC 115可以按顺序安装PE。剩余的和/或不完整的PE可以被存储在eUICC 115中以供将来使用。

[0397] 在处理ProfilePackageBlock之后,在步骤668处,eUICC 115可以向终端110发送ES10_InstallProfilePackageBlockResponse(ES10_安装简档包块响应)消息。

[0398] 可以重复步骤666至668,直到最后的ProfilePackageBlock被发送。如果ES10_InstallProfilePackageBlockRequest消息包括设置为lastPB(1)的lastPBIndicator(最后PB指示符)并且所有PE被成功安装,则eUICC 115生成包括eventResult以及ProfileRegistry中的简档的resultCode和ProfileRecord的ES10_InstallProfilePackageBlockResponse消息。

[0399] 如果从eUICC 115接收到包括eventResult的ES10_InstallProfilePackageBlockResponse消息,则终端110可以在步骤670处向SM-SR+130发送包括由eUICC 115生成的eventResult的ES9_NotifyResultRequest消息。如果从eUICC 115与eventResult一起接收到ES10_InstallProfilePackageBlockResponse消息,则终端110可以向SM-SR+130发送包括由eUICC 115生成的eventResult的ES9_NotifyResultRequest消息。

[0400] ES9_NotifyResultRequest消息可以包括如下信息:

[0401] eventResult(eUICC的处理结果)

[0402] cert_EUM_ECDSA(EUM证书)

[0403] resultCode(结果码)

[0404] EventResult可以包括如下信息:

[0405] resultCode

[0406] eID

[0407] eventID

[0408] profileID简档标识符

[0409] sign_Result由eUICC生成的处理结果签名值

[0410] SM-SR+130可以用下面的TLV进行响应。如果SM-SR+130不知道终端110发送的eventResult中的eventID,则SM-SR+130可以向终端110发送错误消息连同相应的resultCode。

[0411] ES9_NotifyResultResponse(ES9_通知结果响应)消息可以包括如下信息:

[0412] resultCode ResultCode

[0413] 如果从终端110接收到结果通知,则SM-SR+130可以将结果发送到MNO 150和/或SM-DP+120(参见步骤680、681、683、684、685和686)。如果结果通知被设置为“成功”,则SM-SR+130可以从其数据库删除EventID以便不重复处理相同的事件。如果事件在SM-DS 140中没有被成功删除,则当终端向SM-SR+130请求相同的事件时,终端110可以再次取回该事件。

[0414] 建议当EventID成功完成时,eUICC 115存储并保持EventID。结果,eUICC115可以控制这样的情况,其中从SM-DS 140和SM-SR+130的数据库没有成功删除完成的事件,并且因此向eUICC 115发起相同的事件(参见步骤690和691)。eUICC 115可以识别到这种情形并返回失败。

[0415] 如果不再需要建立的安全信道,则终端110可以在步骤672处向eUICC115发送

ES10_ReleaseSecureChannelRequest(ES10_释放安全信道请求)消息。ES10_ReleaseSecureChannelRequest消息可以包括指示安全信道和相关的会话密钥的释放的信息。

[0416] 如果ES10_ReleaseSecureChannelRequest消息被发送,则eUICC 115可以在步骤673处释放安全信道和相关的会话密钥,然后向终端110发送ES10_ReleaseSecureChannelResponse(ES10_释放安全信道响应)消息作为答复。

[0417] 在安全信道被释放的情况下,当接收到SCP03tCommandTLV而没有任何指示重新建立新的安全信道的信息时,eUICC 115可以发送错误消息。

[0418] 步骤674是可选步骤,其中终端110可以要求用户启用安装的简档。如果用户接受启用简档,则终端110可以执行本地简档启用过程。

[0419] 如果由终端110发送的ES9_NotifyResultRequest消息指示简档的成功安装,则在步骤675处,SM-SR+130可以向SM-DS 140发送包括下载简档事件的EventID的ES12_DeleteEventRequest消息。SM-DS 140可以从其数据库删除在步骤620处存储的EventID和相关参数。

[0420] ES12_DeleteEventRequest消息可以包括如下信息:

[0421] eventID eventID

[0422] 在步骤676处,SM-DS 140可以响应下一个TLV。如果SM-DS 140不知道ES12_DeleteEventRequest消息中的eventID,则SM-DS 140可以向SM-SR+130发送包括resultCode的失败消息。

[0423] 从SM-DS 140发送到SM-SR+130的响应消息可以是ES12_DeleteEventResponse(ES12_删除事件响应),其可以包括如下信息:

[0424] resultCode ResultCode

[0425] 在步骤677处,SM-SR+130可以向SM-DP+120发送ES3_NotifyResultRequest消息。ES3_NotifyResultRequest消息可以包括由eUICC 115生成的eventResult。ES3_NotifyResultRequest消息可以向SM-DP+120通知SM-DP+120发送的ProfilePackage的下载和安装结果。

[0426] ES3_NotifyResultRequest消息可以包括如下信息:

[0427] eventResult EventResult OPTIONAL,/*条件,如果ES9_NotifyResultRequest

[0428] 包含eventResult*/

[0429] resultCode ResultCode OPTIONAL--否则

[0430] 在步骤678处,SM-DP+120可以响应下一个TLV。如果SM-DP+120不知道eventResult中的eventID,则SM-DP+120可以向SM-SR+130发送包括resultCode的失败消息。

[0431] 从SM-DP+120发送到SM-SR+130的响应消息可以是ES3_NotifyResultResponse消息,其可以包括如下信息:

[0432] resultCode ResultCode

[0433] 如果终端110或SM-DP+120经由MNO 150请求简档下载,则在步骤680处,SM-DP+120可以向MNO 150发送ES2_NotifyResultRequest消息。替选地,如果终端110或MNO 150经由SM-SR+130请求简档下载,则SM-SR+130可以在步骤683处向MNO 150发送ES4_NotifyResultRequest消息。ES2或ES4的NotifyResultRequest消息接口可以包括由eUICC

115生成的eventResult。

[0434] ES2_NotifyResultRequest消息可以包括以下信息项中的至少一个：

[0435] eventResult，

[0436] resultCode

[0437] ES4_NotifyResultRequest消息可以包括如下信息的至少一部分：

[0438] eventResult

[0439] cert_eUICC_ECDSA

[0440] cert_EUM_ECDSA

[0441] resultCode

[0442] MNO 150可以在步骤681或684处发送下一个TLV。

[0443] 在步骤681处发送的ES2_NotifyResultResponse消息可以包括如下信息：

[0444] resultCode ResultCode

[0445] 在步骤684处发送的ES4_NotifyResultResponse消息可以包括如下信息：

[0446] resultCode(结果码)

[0447] 步骤690是可选步骤，其中终端110可以向SM-DS 140发送包括在下载的简档事件中包括的ProtectedEID(受保护的EID)和EventID的ES11_DeleteEventRequest消息。

[0448] ES11_DeleteEventRequest消息可以包括如下信息的至少一部分：

[0449] protectedEID或EID

[0450] eventID

[0451] 在步骤691处，SM-DS 140可以验证protectedEID和eventID。如果protectedEID.sign_eID有效并且针对eUICC 115发出eventID，则SM-DS 140可以从数据库删除相应的事件。SM-DS 150可以向终端110发送ES11_DeleteEventResponse消息的处理结果。

[0452] ES11_DeleteEventResponse消息可以包括如下信息：

[0453] resultCode

[0454] 如果SM-SR+130无意地省略了该步骤和/或删除该事件失败，则终端110可以避免不必要地接收已处理的事件的通知。

[0455] 通过图6a至图6c的实施例的步骤，相比于在特定步骤处生成或在特定步骤之前预先生成并存储参数和消息，可以更高效地生成上述参数和消息。

[0456] 图7a和图7b是示出根据本发明的实施例的在eUICC中下载简档的过程的信号流程图。

[0457] 参考图7a和图7b，SM-DP+120可以使用基于公共IP的HTTPS直接与LPA(即，终端110)通信，而不涉及SM-SR+130。

[0458] SM-DP+120可以将签名证书(CERT.DP.ECDSA)和私钥(SK.DP.ECDSA)存储在内部存储装置中。SM-DP+120可以将用于HTTPS的TLS服务器证书(CERT.DP.TLS)和私钥(SK.DP.TLS)存储在内部存储装置中。用于存储CERT.DP.ECDSA、SK.DP.ECDSA和CERT.DP.TLS、SK.DP.TLS的存储装置可以在物理上彼此相同或不同。

[0459] eUICC 115可以将其签名证书(CERT.EUICC.ECDSA)和私钥(SK.eUICC.ECDSA)存储在内部存储装置中。简档下载过程可以如下进行。

[0460] 在步骤710处,终端110可以向eUICC 115请求eUICC证书。然后,eUICC115可以在步骤713处向终端110发送eUICC证书(CERT.eUICC.ECDSA)和EUM证书(CERT.EUM.ECDSA)。

[0461] 此时,如果终端110具有证书,则可以省略步骤710和713。

[0462] 如果需要将eUICC 115的证书值发送到服务器(SM-DP+120),则终端110可以在步骤715处请求eUICC 115生成证书值。签名所需的因素可以是递送到终端110的值,并且包括如下信息的至少一部分:

[0463] -EventID(用于识别特定简档下载事件的标识符)

[0464] -NotificationID(类似于EventID)

[0465] -MatchingID(类似于EventID)

[0466] -激活码令牌(类似于EventID)

[0467] -由终端生成的随机值

[0468] 如果不需要eUICC 115的签名值,则终端110可以向eUICC 115请求除eUICC 115的签名值之外的eUICC信息(UICC信息)。

[0469] eUICC 115可以在步骤717处使用SK.eUICC.ECDSA生成其签名值。

[0470] 在步骤719处,eUICC115可以向终端110发送eUICC签名值。如果不需要eUICC签名值,则eUICC 115可以仅将eUICC_Info返回给终端110。eUICC_Info可以包括eUICC 115的版本信息。

[0471] 在步骤720处,终端110可以向SM-DP+120发送ES9+.InitiateDownload(ES9+.启动下载)消息。此时,可以在终端110与SM-DP+120之间建立HTTPS会话,以发送ES9+.InitiateDownload消息。HTTPS会话可以与用于整个简档下载过程的会话相同或分开。

[0472] ES9+.InitiateDownload消息可以是ES9.InitiateAuthentication(ES9.启动认证)消息或ES9.EventRequest消息。

[0473] ES9+.InitiateDownload消息可以包括eUICC_Info以及另外还包括eUICC质询。如果包括eUICC签名值,则也可以包括eUICC证书和EUM证书。

[0474] 如果SM-DP+120在步骤720处接收到eUICC证书和签名值,则SM-DP+120可以使用CI证书或CI证书公钥(PK.CI.ECDSA)来验证EUM证书,使用EUM证书来验证eUICC证书,并使用eUICC证书来验证eUICC签名值。根据本发明的实施例,可以省略证书和签名验证。

[0475] SM-DP+120可以基于eUICC_Info来检查eUICC 115的资格(eligibility)。此时,可以使用eUICC_Info的eUICC版本信息。

[0476] SM-DP+120可以生成DP质询。DP质询可以是由SM-DP+120生成的供将来认证eUICC 115的值。

[0477] SM-DP+120可以生成TransactionID(交易ID)。TransactionID是用于识别特定简档下载会话的标识符,以便能够同时处理多个终端请求。如果未由TransactionID识别,则SM-DP+120可以一次下载一个终端的简档;因此,当某个终端110延迟响应SM-DP+120时,其他终端也不能下载简档。为了解决这个问题,SM-DP+120可以配置会话的使用期以便在相应的时间段期满之后释放会话,但是这种方法可能导致SM-DP+120的性能问题。

[0478] 如果SM-DP+120可以从终端接收到MatchingID或EID,则SM-DP+120可以检查是否存在与MatchingID或EID对应的任何可下载简档。

[0479] SM-DP+120可以针对包括eUICC_Challenge(eUICC_质询)、DP质询和

TransactionID值的数据使用SK.DP.ECDSA来计算EP签名值。

[0480] DP签名值可以是用于eUICC 115认证SM-DP+120的签名值。

[0481] 在步骤727处,SM-DP+120可以响应在步骤720处接收的消息向终端110发送SM-DP+120的签名证书(CERT.DP.ECDSA)、DP质询、TransactionID、DP签名、简档信息和确认码输入要求指示符(ConfirmationCodeRequired标识符)。

[0482] 在这种情况下,在步骤729处,终端110可以显示简档信息并接收用户的确认或确认码输入。

[0483] 如果在步骤727处接收到上述信息项,则终端110可以在步骤730处向eUICC 115发送ES10b.PrepareDownload(ES10b.准备下载)消息。ES10b.PrepareDownload消息可以是ES10.GetAuthDataRequest消息。

[0484] ES10b.PrepareDownload消息可以包括CERT.DP.ECDSA、DP质询、TransactionID和DP签名。

[0485] 在步骤735处,eUICC 115可以使用存储在其中的CI证书或CI公钥来验证DP证书(CERT.DP.ECDSA)。

[0486] 如果证书验证成功,则eUICC 115可以验证SM-DP+签名值(DP-Signature)。

[0487] 此时,利用从终端110接收的DP质询和TransactionID、从eUICC 115发送给终端110的eUICC质询、以及包括在CERT.DP.ECDSA中的SM-DP+公钥(PK.DP.ECDSA)来进行SM-DP+签名验证。

[0488] 如果验证成功,则eUICC 115可以生成一次性非对称密钥对。

[0489] eUICC 115可以在如下情况下加载并使用先前生成的一次性非对称密钥对:

[0490] -当由特定SM-DP+120进行请求时

[0491] -当由终端110用单独的Indicator(指示符)进行请求时

[0492] 一次性非对称密钥对可以用于生成SM-DP+120与eUICC 115之间的加密密钥连同服务器120的一次性非对称密钥对。加密密钥可以如下生成:

[0493] -SM-DP+120通过组合SM-DP+120的一次性私钥和eUICC 115的一次性私钥来生成加密密钥。

[0494] -eUICC通过组合eUICC 115的私钥和SM-DP+120的公钥来生成加密密钥。

[0495] 生成加密密钥另外需要的因素可以经由终端110从SM-DP+120发送到eUICC 115。

[0496] eUICC 115可以针对包括所生成的一次性非对称密钥对的一次性公钥(otPK.eUICC.ECKA)和DP质询的数据使用eUICC 115的用于签名的私钥(SK.eUCIC.ECDSA)来计算eUICC签名值(eUICC_Sign2)。由于在计算eUICC签名值时使用由SM-DP+120生成的DP质询值,所以SM-DP+120可以在随后的步骤中使用eUICC签名值来认证eUICC 115。eUICC_Sign2使得eUICC 115能够将所生成的otPK.eUICC.ECKA值无任何修改地发送到SM-DP+120。

[0497] 在步骤737处,eUICC 115可以向终端110发送eUICC 115的一次性公钥和eUICC签名值。

[0498] 在步骤740处,终端110可以向SM-DP+120发送ES9+GetBoundProfilePackage消息。ES9+GetBoundProfilePackage消息可以是eUICCManagementRequest或ProfileRequest消息。

[0499] ES9+GetBoundProfilePackage消息可以包括一次性eUICC公钥和eUICC签名值。另

外,ES9+GetBoundProfilePackage消息可以包括用于验证eUICC签名值的eUICC签名证书(CERT.eUICC.ECDSA)和用于验证eUICC签名证书的EUM证书(CERT.eUICC.ECDSA)。

[0500] 另外,ES9+GetBoundProfilePackage消息可以包括如下信息,用于在下载特定简档时用作映射标识符。

[0501] -EventID

[0502] -MatchingID

[0503] -NotificationID

[0504] -激活码令牌

[0505] 如果映射标识符已经在之前的步骤(例如,步骤720)处被发送,则可以省略发送映射标识符。

[0506] 终端110可以向SM-DP+120发送散列确认码。

[0507] 在步骤745处,SM-DP+120可以验证EUM证书和eUICC证书,如结合步骤725所描述的。

[0508] SM-DP+120可以使用在步骤740处从终端110接收到的eUICC一次性公钥、在步骤727处发送到终端110的DP质询值、以及包括在eUICC证书中的公钥,来验证eUICC签名(eUICC Sign2)。如果验证成功,则这意味着SM-DP+120已认证eUICC 115。如果验证失败,则SM-DP+120可以停止相应的会话并向终端110返回错误消息。

[0509] SM-DP+120可以使用在步骤740处接收到的EventID(或NotificationID、MatchingID或激活码令牌)值来映射要下载的简档。如果不存在要下载的简档,则SM-DP+120可以向终端110返回错误消息并结束相应的会话。

[0510] SM-DP+120可以生成一次性非对称密钥对。一次性非对称密钥对可以用于生成eUICC 115与SM-DP+120之间的认证密钥。

[0511] -SM-DP+120通过组合SM-DP+120的一次性私钥和eUICC 115的一次性私钥来生成加密密钥。

[0512] -eUICC 115通过组合eUICC 115的一次性私钥和SM-DP+120的一次性公钥来生成加密密钥。

[0513] SM-DP+120可以计算SM-DP+签名值(DP签名2)。SM-DP+签名值可以是使用CRT、SM-DP+120的一次性公钥、eUICC 115的一次性公钥和SM-DP+签名公钥(SK.DP.ECDSA)来计算的。CRT可以用作生成认证密钥的因素。

[0514] SM-DP+120可以生成与特定eUICC 115组合的简档包(绑定简档包(Bound Profile Package)或BPP)。BPP可以包括CRT、SM-DP+120的一次性公钥和DP Signature2。

[0515] BPP可以包括用加密密钥加密的ProfileInfo(简档信息)(或MetaData(元数据))。

[0516] BPP可以包括通过用加密密钥加密简档保护密钥而生成的加密的PPK。

[0517] BPP可以包括用加密密钥或PPK加密的简档包块(PPB)。加密的PPB可以通过以可安装的单元(简档元素(Profile Element)或PE)划分整个简档数据并加密由可加密单元分割的PPD来生成。加密可以使用SCP03t协议来执行。

[0518] 之后,响应于在步骤740处接收的消息,SM-DP+120可以在步骤747处向终端110发送BPP消息。

[0519] 终端110可以在步骤750处向eUICC 115多次发送

ES10b.LoadBoundProfilePackage(ES10b.加载绑定简档包)消息,以将包括在BPP中的ES8_InitializeSecureChannel(ES8_初始化安全信道)信息递送给eUICC 115。ES8_InitializeSecureChannel信息可以包括CRT、SM-DP+120的一次性公钥和DP signature2。ES8_InitializeSecureChannel可以是EstablishSecureChannel(建立安全信道)消息。ES10b.LoadBoundProfilePackage消息可以携载StoreData(存储数据)命令。

[0520] 在步骤753处,eUICC 115可以使用在步骤730处接收到的DP签名证书(CERT.DP.ECDSA)的公钥(PK.DP.ECDSA)、在步骤750处接收到的CRT、SM-DP+的一次性公钥和在步骤737处从终端110接收到的eUICC的一次性公钥,来验证DP签名(DP signature2)。

[0521] 如果验证失败,则eUICC 115可以在步骤755处向终端110返回错误消息并结束该过程。

[0522] 如果验证成功,则eUICC 115可以在步骤755处使用CRT、eUICC 115的一次性私钥和SM-DP+120的一次性公钥来生成加密密钥,并向终端110发送加密密钥。

[0523] 在步骤757处,终端110可以多次发送ES10b.LoadBoundProfilePackage消息,以将包括在BPP中的ES8+SetProfileInfo(ES8+设定简档信息)递送给eUICC 115。ES8+SetProfileInfo可以被称为ES8+.存储元数据)或InstallProfileRecord(安装简档记录)。ES8+SetProfileInfo可以包括ProfileInfo(或Metadata或ProfileRecord)。在步骤759处,eUICC 115可以向终端110发送响应消息。

[0524] 在步骤760处,如果BPP包括ES8+ReplaceSessionKey(ES8+替换会话密钥),则终端110可以多次发送ES10b.LoadBoundProfilePackage消息以将包括在BPP中的ES8+ReplaceSessionKey信息递送给eUICC 115。ES8+ReplaceSessionKey可以被称为UpdateSessionKeyRequest消息。

[0525] ES8+ReplaceSessionKey可以包括用步骤745的加密密钥加密的ProfileProtectionKey(PPK)。

[0526] 在步骤763处,eUICC 115可以向终端110发送对在步骤760处接收到的消息作出答复的响应消息。

[0527] 之后,终端110可以多次发送ES10b.LoadBoundProfilePackage消息以递送包括在BPP中的加密的简档包块(PPB)或简档段。

[0528] eUICC 115可以使用加密密钥或PPK来串行解密Profile段。

[0529] 在处理所有简档段之后,eUICC 115可以计算eUICC签名值,并在步骤767处将签名值发送到终端110。终端110可以在步骤770处向SM-DP+120发送相应的eUICC签名值以通知简档安装结果。在步骤775处,SM-DP+120可以向终端110发送响应消息。

[0530] 示例性地,从SM-DP+120发送到终端110的指示是否需要用户的确认的信息可以如下进行格式化。

[0531] UserConfirmation::=SEQUENCE{

[0532] confirmType ConfirmType,

[0533] confirmMessage ConfirmMessage OPTIONAL

[0534] }

[0535] ConfirmType::=ENUMERATED{yesOrNo(0),codeInput(1)}

[0536] ConfirmMessage::=UTF8String

[0537] 在上面的示例中,可以将UserConfirmation(用户确认)数据连同或不连同其他数据一起从SM-DP+120发送到终端110。包括在UserConfirmation中的confirmType(确认类型)可以具有如下值:

[0538] 如果confirmType被设置为指示yesOrNo的0,则终端110可以选择确认或不确认简档下载,如参考图2至5和图6a至6c所述的。

[0539] 如果confirmType被设置为1,这意味着需要代码输入(code input);因此,终端110要求输入确认码。

[0540] 确认消息可以是终端110呈现给用户的补充信息,并且该消息可以取决于运营商而被不同地格式化。

[0541] 图8a和图8b是示出根据本发明的实施例的网络初始化过程的信号流程图。

[0542] 如果由MNO 150发送的eUICCManagementRequest消息中包括的eventType未被设置为“profileDownload”,则可以在ES5安全中执行无线管理(远程管理),而不涉及ES8。下文中进行其详细描述。

[0543] 在步骤810处,LPA(即,终端110)可以从eUICC 115读取CERTS_eUICC。CERTS_eUICC可以是包括eUICC证书和EUM证书的信息。为了实现这个,在步骤810处,终端110可以向eUICC 115发送包括请求CERTS_eUICC的信息(GetCert)的LocalManagementRequest消息,并且在步骤813处从eUICC115接收包括CERTS_eUICC的LocalManagementResponse消息。如果终端110已经具有CERTS_eUICC,则可以省略步骤810和813。由于这些步骤与图6a至图6c的步骤611和612相同,所以这里省略其详细描述。

[0544] 在步骤820处,MNO 150可以向SM-SR+130发送ES4_eUICCManagementRequest消息。

[0545] ES4_eUICCManagementRequest消息可以包括如下信息:

[0546] event Event,

[0547] dsInfo DSInfo

[0548] 已经在图6a至6c的实施例中描述了Event(事件)。ES4_eUICCManagementRequest消息的EventID可以被设置为NULL(空)。

[0549] 在步骤823处,SM-SR+130可以针对管理事件生成全局唯一的EventID。

[0550] 在步骤825处,SM-SR+130可以向MNO 150发送eUICCManagementResponse消息。eUICCManagementResponse消息可以包括如下信息:

[0551] resultCode ResultCode,

[0552] eventID EventID

[0553] OPTIONAL--条件为如果resultCode指示成功

[0554] SM-SR+130可以使用步骤830和833的ES12_RegisterEventRequest和ES12_RegisterEventResponse消息向SM-DS 140注册Event。ES12_RegisterEventRequest和ES12_RegisterEventResponse消息可以与关于图6a至图6c的步骤621和图622描述的相同;因此,这里省略其详细描述。

[0555] SM-DS 140可以经由推送服务器向终端110发送推送通知消息。

[0556] 终端110可以通过步骤840和843从eUICC 115读取ProtectedEID值。稍后可以在步骤845处使用ProtectedEID。如果终端110知道ProtectedEID值,则可以省略步骤840和843。终端110可以在步骤810和813之前执行这些步骤。由于这些步骤与图6a至图6c的实施例中

描述的步骤613和614相同，所以这里省略其详细描述。

[0557] 在步骤845处，终端110可以向SM-DS 140发送EventIDRequest消息。

[0558] EventIDRequest消息可以包括如下信息：

[0559] protectedEID ProtectedEID

[0560] 然后，SM-DS 140可以验证ProtectedEID。如果受保护的EID中包括的时间点与接收到EventID请求消息的时间点之间的时间间隔大于预定范围，则SM-DS 140可能验证受保护的EID失败。由于该步骤与图6a至图6c的实施例中描述的步骤624相同，所以这里省略其详细描述。

[0561] 接下来，SM-DS 140可以向终端110发送ES11_EventIDResponse(ES11_事件ID响应)消息。

[0562] ES11_EventIDResponse消息可以包括如下信息：

[0563] resultCode ResultCode，

[0564] eventIDList SEQUENCE OF PendingEvent(待决事件的序列)--条件为如果resultCode指示成功

[0565] PendingEvent(待决事件)可以包括如下信息：

[0566] eventID EventID，

[0567] SRID SRID

[0568] 当终端110向SM-DS 140请求EventID时，SM-DS 140可能具有至少一个PendingEvent。在这种情况下，eventIDList(事件ID列表)可以包括一个或多个PendingEventID(待决事件ID)。然后，终端110可以按照eventIDList中排列的顺序逐个处理PendingEvent。

[0569] 终端110可以通过步骤850和853从eUICC 115接收eUICCInfo。稍后可以在步骤855处使用eUICCInfo。如果终端110已经具有eUICCInfo，则可以省略步骤850和853。终端110可以在步骤810和813或步骤840或843之前执行这些步骤。由于这些步骤与图6a至图6c的实施例中描述的步骤615和616相同，所以这里省略其详细描述。

[0570] 如果接收到包括至少一个PendingEvent的EventIDResponse消息，则终端110可以在步骤855处向SM-SR+130发送EventRequest(事件请求)消息。

[0571] EventRequest消息可以包括如下信息：

[0572] eventID EventID，

[0573] terminalInfo TerminalInfo，

[0574] eUICCInfo EUICCInfo

[0575] 如果SM-SR+130不支持所接收的eUICCInfo.ECCParameter(eUICC信息.ECC参数)，则它可以向终端110发送失败消息。

[0576] 在步骤857处，SM-SR+130可以生成SRToken1。

[0577] 此时，SRToken1可以包括如下信息：

[0578] cert_SR_ECDSA CERT_ECDSA，

[0579] nonce_SR NONCE_SR，

[0580] sign_SR1SIGN_ECDSA

[0581] cert_SR_ECDSA可以遵从在步骤855处接收到的ECC参数。

[0582] sign_SR1可以是由SM-SR+130使用SK_SR_ECDSA生成的签名。

[0583] SM-SR+130可以将NONCE_SR与eventID一起存储，并且稍后在步骤873处使用NONCE_SR来认证eUICC115。

[0584] 在步骤859处，SM-SR+130可以向终端110发送EventResponse消息。

[0585] EventResponse消息可以包括如下信息：

[0586] resultCode ResultCode，

[0587] eventType EventType，

[0588] srToken1SRToken1

[0589] 在步骤860处，终端110可以向eUICC 115发送ES10_GetAuthDataRequest消息。由于该步骤与图6a至6c的实施例中描述的步骤639相同，所以省略其详细描述。

[0590] 在步骤861处，eUICC 115可以验证srToken1。

[0591] 此时，验证过程可以如下进行。eUICC 115可以使用PK_CI_ECDSA来验证CERT_SR_ECDSA。eUICC 115可以从CERT_SR_ECDSA中提取PK_SR_ECDSA，并利用PK_SR_ECDSA验证sign_SR1。eUICC 115可以存储PK_SR_ECDSA以供稍后使用。

[0592] eUICC 115可以验证包括在CERT_SR_ECDSA中的SRID是否依照EPRServerAccessControl(EPR服务器访问控制)来执行。

[0593] 如果eventType被设置为enableProfile(启用简档)(1)、disableProfile(禁用简档)(2)、deleteProfile(删除简档)(3)、getProfileRegistry(获得简档注册)(4)或updateProfileRegistry(更新简档注册)(5)，则eUICC 115可以验证包括在CERT_SR_ECDSA中的SRID是否包括在简档的ProfileRecord的authorizedSR(授权的SR)中。

[0594] 如果eventType被设置为getEPR(获得EPR)(6)或updateEPR(更新EPR)(7)，则eUICC 115可以验证包括在CERT_SR_ECDSA中的SRID是否包括在EPR的授权的SR中。

[0595] 如果eventType被设置为getDSInfo(获得DS信息)(8)或updateDSIfo(更新DS信息)(9)，则eUICC 115可以验证包括在CERT_SR_ECDSA中的SRID是否包括在DSINfoStatic(静态DS信息)的authorizedSR中。

[0596] 如果eventType被设置为getCIInfo(获得CI信息)(10)或updateCIInfo(更新CI信息)(11)，则eUICC 115可以验证包括在CERT_SR_ECDSA中的SRIC是否包括在CIInfo(CI信息)的authorizedSR中。

[0597] 如果eventType被设置为getFirmwareInfo(获得固件信息)(12)或updateFirmwareInfo(更新固件信息)(13)，则eUICC 115可以验证包括在CERT_SR_ECDSA中的SRID是否包括在FirmwareInfo(固件信息)的authorizedSR中。

[0598] eUICC 115可以在步骤863处生成eUICCToken。

[0599] eUICCToken可以包括如下信息：

[0600] eventID EventID，

[0601] sign_eUICC SIGN_ECDSA，

[0602] nonce_eUICC NONCE_eUICC

[0603] OPTIOANL

[0604] eUICC签名sign_eUICC可以用SK_eUICC_ECDSA来计算。由于该步骤与图6a至图6c的实施例中描述的步骤644相同，所以这里省略其详细描述。

[0605] 在步骤865处,eUICC 115可以向终端110发送ES10_GetAuthDataResponse消息。

[0606] ES10_GetAuthDataResponse消息可以包括如下信息:

[0607] resultCode ResultCode,

[0608] eUICCToken EUICCToken

[0609] 步骤867是可选步骤,其中终端110可以向请求用户同意。

[0610] 如果用户同意该事件或者不需要用户的同意,则在步骤869处,终端110可以向SM-SR+130发送ES9_eUICCManagementRequest消息。

[0611] 此时,ES9_eUICCManagementRequest消息可以包括如下信息:

[0612] eUICCToken EUICCToken,

[0613] certs_eUICC CERTS_eUICC

[0614] 否则,如果用户拒绝该事件,则终端110可以在步骤871处向SM-SR+130发送ES9_NotifyResultRequest消息。ES9_NotifyResultRequest消息可以包括与“3200User_Rejected(用户拒绝)”的resultCode对应的eventID。由于该步骤与图6a至图6c的实施例中描述的步骤670相同,所以省略其详细描述。

[0615] SM-SR+130可以在步骤873处验证eUICCToken。

[0616] 验证过程可以如下进行:

[0617] SM-SR+130可以利用存储在SM-SR+130中的CERT_CI_ECDSA和从终端110接收到的CERT_EUM_ECDSA来验证CERT_eUICC_ECDSA。

[0618] 之后,SM-SR+130可以从CERT_eUICC_ECDSA中提取PK_eUICC_ECDSA,并且利用PK_eUICC_ECDSA验证sign_eUICC。由于该步骤与图6a至图6c的实施例中描述的步骤648相同,所以省略其详细描述。

[0619] 在步骤857处,SM-SR+130可以使用与eventID一起存储的NONCE_SR来验证sign_eUICC。

[0620] 如果任何验证失败,则SM-SR+130可以向终端110和/或MNO 150返回错误消息。

[0621] 如果全部验证成功,则这可以意味着SM-SR+130已成功认证eUICC115。

[0622] SM-SR+130可以在步骤875处生成srToken2。

[0623] 此时,srToken2可以包括如下信息:

[0624] sign_SR2SIGN_ECDSA

[0625] 签名sign_SR2可以用SK_SR_ECDSA来计算。由于该步骤与图6a至图6c的实施例中描述的步骤655相同,所以这里省略其详细描述。

[0626] 在步骤877处,SM-SR+130可以向终端110发送ES9_eUICCManagementResponse消息。

[0627] ES9_eUICCManagementResponse消息可以包括如下信息:

[0628] event Event OPTIONAL,/*条件为如果eventType!=downloadProfile(0)*/

[0629] profileInstallPackage ProfileInstallPackage OPTIONAL,/*条件为如果eventType=downloadProfile(0)*/

[0630] srToken2SRToken2

[0631] 在步骤879处,终端110可以向eUICC115发送eUICCManagementRequest消息。eUICCManagementRequest消息可以包括事件信息和srToken2。

[0632] 在步骤881处,eUICC 115可以验证srToKen2。

[0633] 验证过程可以如下执行:eUICC 115可以利用PK_SR_ECDSA验证sign_SR2。由于该步骤与图6的实施例中描述的步骤658相同,所以省略其详细描述。

[0634] eUICC 115可以使用在步骤861和863处与eventID一起存储的PK_SR_ECDSA和NONCE_eUICC值来验证sign_SR2。

[0635] 如果eventType被设置为“updateCIInfo(11)”并且CIInfo包括新的CI证书,则eUICC 115可以利用包含在证书中的PK_CI_ECDSA检查相同证书的签名以验证CI证书。

[0636] 如果eventType被设置为“updateFirmwareInfo(13)”,则eUICC 115可以验证FirmwareInfo中的sign_EUM。

[0637] 如果任何验证失败,则eUICC 115可以向终端110返回错误消息。

[0638] 如果所有验证成功,则这可以意味着eUICC 115已成功认证SM-SR+130。

[0639] 如果srToken1被成功验证,则eUICC 115可以获取一些有价值的验证信息,例如用于EventType的SRID、目标EID、EventID、EventType和其他参数。

[0640] 使用这样的信息,eUICC 115可以参考eUICC策略规则(例如,服务器访问控制和补贴锁(subsidy lock))、简档策略规则以及其他必要的规则。eUICC可以检查该事件是否满足eUICC 115中配置的所有规则。

[0641] 如果事件不满足上述规则,则eUICC 115可以拒绝该事件并发送拒绝原因。

[0642] 如果步骤881的验证成功,则eUICC 115可以执行借助事件指示的eUICC管理。eUICC 115可以根据事件的eventType执行eUICC管理。

[0643] 例如,eventType可以是更新CIInfo。

[0644] 网络可以启动存储在eUICC 115中的CIInfo(证书发布者信息)的更新。

[0645] eUICC 115可以更新其CIList(证书发布者列表)。如果ES10_eUICCManagementRequest.event.eventType设置为“updateCIInfo(11)”,则eUICC可以根据ES10_eUICCManagementRequest.event.CIInfo更新在CIInfo中定义的允许的SM-SR+信息。允许的SM-SR+信息可以包括关于能够更新eUICC 115的服务器(SM-SR+)的信息,以便允许特定的授权服务器更新eUICC 115。eUICC 115可以保留允许的SM-SR+信息以将该信息与被接收的服务器身份信息进行比较,以便仅当它们匹配时允许更新eUICC的简档。

[0646] 如果SM-SR+130的SRID不包括在eUICC 115的CIInfo.authorizedSR中,则eUICC 115可以省略更新CIInfo并返回包括指示“SRID_Not_Allowed(SRID_不允许)”的信息的错误消息。

[0647] 之后,在步骤885处,eUICC 115可以向终端110发送ES10_eUICCManagementResponse消息。ES10_eUICCManagementResponse消息可以包括事件结果信息。

[0648] 在步骤887处,终端110可以向SM-SR+130发送ES9_NotifyResultRequest消息,并且SM-SR+130可以向终端110发送ES9_NotifyResultResponse消息作为该消息的回复。由于这些步骤与图6a至图6c的实施例中描述的步骤670和671相同,所以这里省略其详细描述。

[0649] 步骤892是可选步骤,其中如果entType被设置为“enableProfile(1)”或“disableProfile(2)”,则eUICC 115可以向终端110发送终端刷新(Terminal REFRESH)消息(UICC重置)。

[0650] 如果eventType被设置为“enableProfile(1)”，并且ES10_eUICCManagementResponse消息指示简档已成功启用，则终端110可以执行REFRESH(UICC重置)操作以与当前网络断开连接并使用启用简档重新连接到新的MNO网络。(终端110可以向SM-SR+130成功发送结果通知，并自己执行REFRESH操作，而无需从eUICC 115接收到REFRESH主动命令。因此，eUICC 115甚至可以在启用简档后不向终端110发送REFRESH命令)。

[0651] 在步骤890处，SM-SR+130可以向MNO 150发送ES4_NotifyResultRequest消息。ES4_NotifyResultRequest可以包括由eUICC115生成的eventResult，并且在步骤820处，eventResult可以指示由eUICC 115发起的管理事件的结果。EUM证书和与eventResult一起发送的CERT_EUM_ECDSA可以是链接到由MNO 150存储的CI证书的证书，以供在验证eUICC签名时由MNO 150使用。由于ES4_NotifyResultRequest消息是关于图6的步骤670和683描述的，所以这里省略其详细描述。

[0652] 之后，在步骤891处，MNO 150可以回复下一个TLV。如果MNO 150不知道eventResult中的eventID，则MNO 150可以向SM-SR+130发送包括resultCode的失败消息。

[0653] 从MNO 150发送到SM-SR+130的ES4_NotifyResultResponse消息可以包括如下信息：

[0654] resultCode ResultCode

[0655] 如果终端110发送的ES9_NotifyResultRequest消息指示事件成功完成，则SM-SR+130可以向SM-DS 140发送包括EventID的ES12_DeleteEventRequest消息。然后，SM-DS 140可以从其数据库删除在步骤830处存储的EventID和相关参数。

[0656] ES12_DeleteEventRequest消息可以包括如下信息：

[0657] eventID EventID

[0658] 接下来，在步骤895处，SM-DS 140可以回复下一个TLV。如果SM-DS140不知道包括在ES12_DeleteEventRequest消息中的eventID，则SM-DS 140可以向SM-SR+130发送包括resultCode的失败消息。

[0659] 同时，作为从SM-DS 140发送到SM-SR+130的响应消息的ES12_DeleteEventResponse消息可以包括如下信息：

[0660] resultCode ResultCode

[0661] 图9是示出根据本发明的实施例的终端的配置的框图。

[0662] 参考图9，根据本发明的实施例的终端110可以包括收发器920和用于控制终端110的整体操作的控制单元910。终端110还可以包括eUICC 115。eUICC 115可以包括在控制单元910中，如图中所描绘的，或实现为与控制单元910分开的组件。eUICC 115可以被实现为与终端110分开的网络实体。

[0663] 控制单元910控制终端110执行上述实施例中的一个的操作。例如，控制单元910可以控制终端110：发送包括关于要从简档提供服务器120接收的简档的信息的第一消息；从简档提供服务器120接收第二消息，第二消息包括指示是否需要用户的加密码输入的信息和第一修改的加密码；当第一修改的加密码被成功认证时，生成第二修改的加密码；向简档提供服务器120发送第三消息，第三消息包括第二修改的加密码和请求简档下载的信息；以及从简档提供服务器120接收包括关于简档的信息的第四消息。

[0664] 终端110的收发器920可以根据上述实施例中的一个的操作来发送/接收信号。例如，终端110的收发器920可以向服务器120发送包括关于简档的信息的第一消息。收发器920还可以从简档提供服务器120接收包括关于简档的信息的第四消息。

[0665] 图10是示出根据本发明的实施例的SM-DP+的配置的框图。

[0666] 参考图10，根据本发明的实施例的SM-DP+120可以包括收发器1020和用于控制SM-DP+120的整体操作的控制单元1010。

[0667] 控制单元1010控制SM-DP+120执行上述实施例中的一个的操作。例如，SM-DP+120的控制单元1010可以控制SM-DP+120：从终端110接收包括关于要接收的简档的信息的第一消息；生成用于认证简档提供服务器的第一修改的加密码；发送第二消息，该第二消息包括指示是否需要用户的加密码输入的信息和第一修改的加密码；从终端110接收第三消息，该第三消息包括第二修改的加密码和请求简档下载的信息；以及当第二修改的加密码被成功认证时，发送包括关于简档的信息的第四消息。

[0668] SM-DP+120的收发器1020可以根据上述实施例中的一个的操作来发送/接收信号。例如，SM-DP+120的收发器1020可以从终端110接收包括关于要由终端110接收的简档的信息的消息，并且向终端110提供相应的简档。

[0669] 图11是示出根据本发明的实施例的SM-SR+的配置的框图。

[0670] 参考图11，根据本发明的实施例的SM-SR+130可以包括收发器1120和用于控制SM-SR+130的整体操作的控制单元1110。

[0671] 控制单元1110控制SM-SR+130执行上述实施例中的一个的操作。例如，控制单元1110可以控制SM-SR+130发送包括请求简档下载或简档管理的信息的消息。

[0672] SM-SR+130的收发器1120可以根据上述实施例中的一个的操作来发送/接收信号。例如，收发器1120可以发送包括请求简档下载或简档管理的信息的消息。

[0673] 图12是示出根据本发明的实施例的SM-DS的配置的框图。

[0674] 参考图12，根据本发明的实施例的SM-DS 140可以包括收发器1220和用于控制SM-DS 140的整体操作的控制单元1210。

[0675] 控制单元1210控制SM-DS 140执行根据上述实施例中的一个的操作。例如，控制单元1210可以控制SM-DS 140从SM-SR+130接收包括请求简档下载或简档管理的信息的消息。

[0676] SM-DS 140的收发器1220可以根据上述实施例中的一个的操作来发送/接收信号。例如，收发器1220可以从SM-SR+130接收包括请求简档下载或简档管理的信息的消息。

[0677] 尽管已经使用特定术语描述了本发明的各种实施例，但是说明书和附图被认为是说明性的而不是限制性以帮助理解本发明。对于本领域技术人员而言明显的是，在不脱离本发明的更广泛的精神和范围的情况下，可以对其进行各种修改和变化。

[0678] 尽管已经使用特定术语描述了本发明的各种实施例，但是说明书和附图被认为是说明性的而不是限制性以帮助理解本发明。对于本领域技术人员而言明显的是，在不脱离本发明的更广泛的精神和范围的情况下，可以对其进行各种修改和变化。

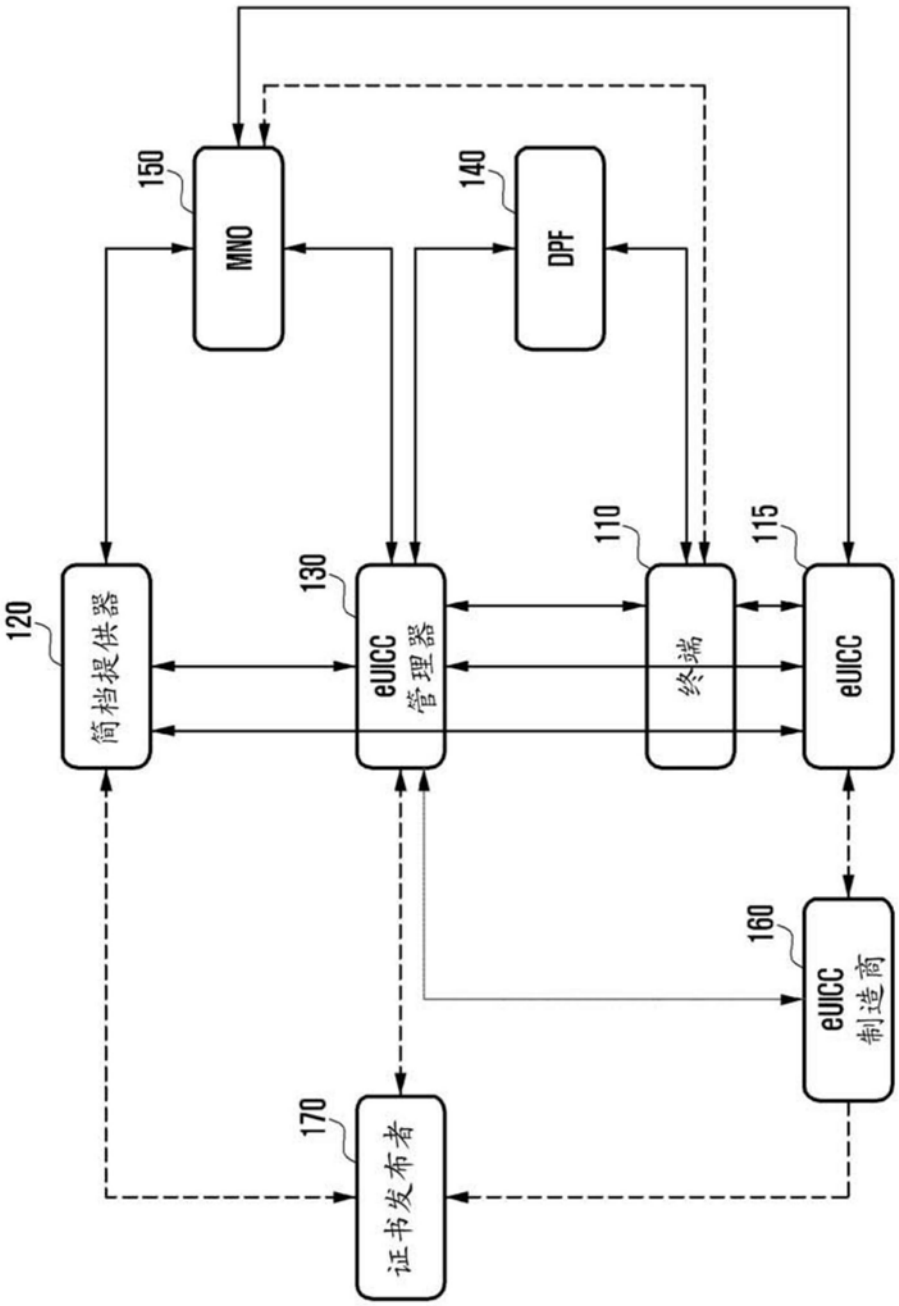

150
MNO
140
DPF
110
115
120
130
简档提供器
eUICC
管理器
终端
eUICC
160
eUICC
制造商
170
证书发布者

图1

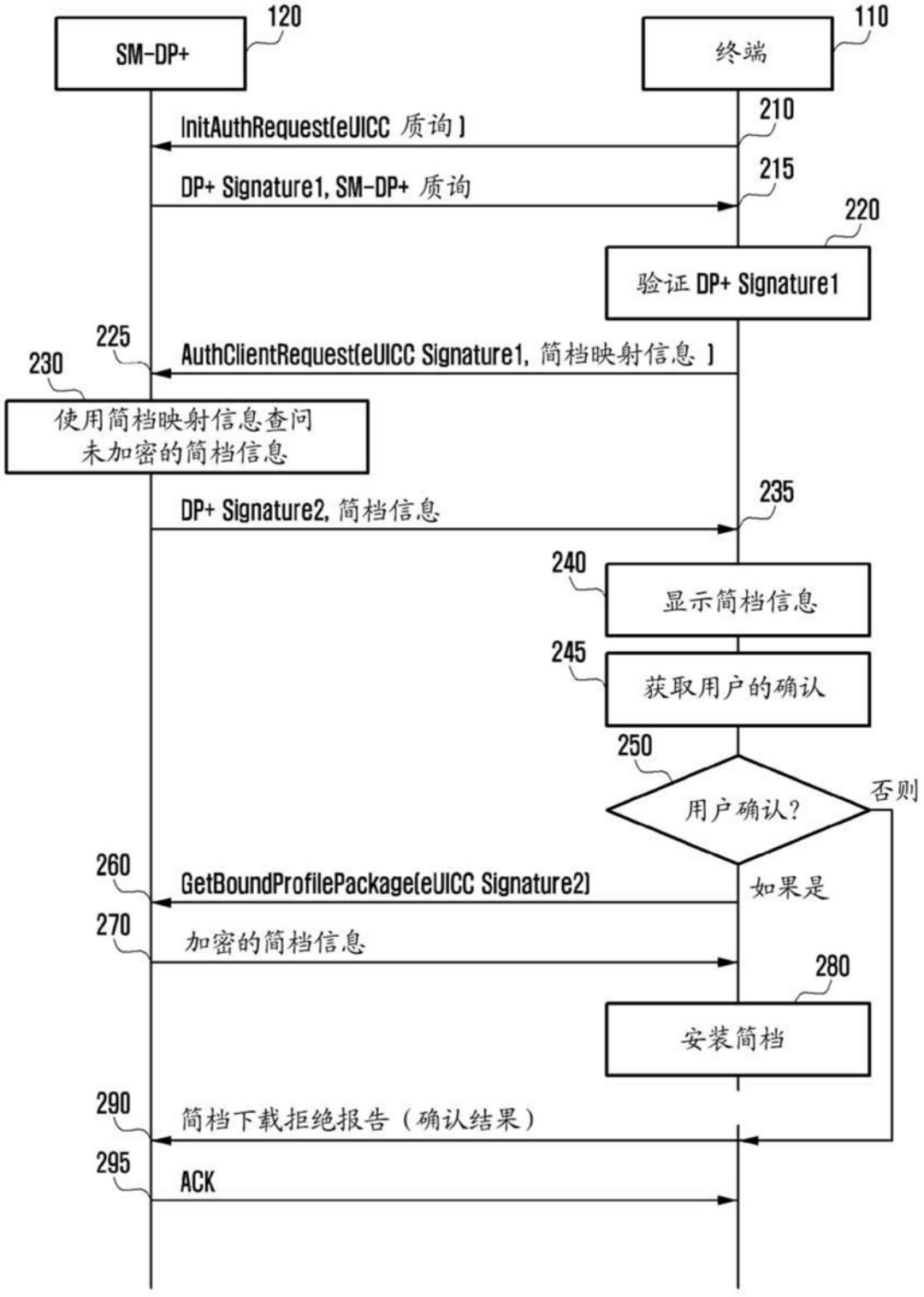

SM-DP+
120
终端
110
210
InitAuthRequest(eUICC 质询)
215
DP+ Signature1, SM-DP+ 质询
220
验证 DP+ Signature1
225
230
AuthClientRequest(eUICC Signature1, 简档映射信息)
使用简档映射信息查问
未加密的简档信息
235
DP+ Signature2, 简档信息
240
显示简档信息
245
获取用户的确认
250
用户确认?
否则
如果是
260
GetBoundProfilePackage(eUICC Signature2)
270
加密的简档信息
280
安装简档
290
简档下载拒绝报告（确认结果）
295
ACK

图2

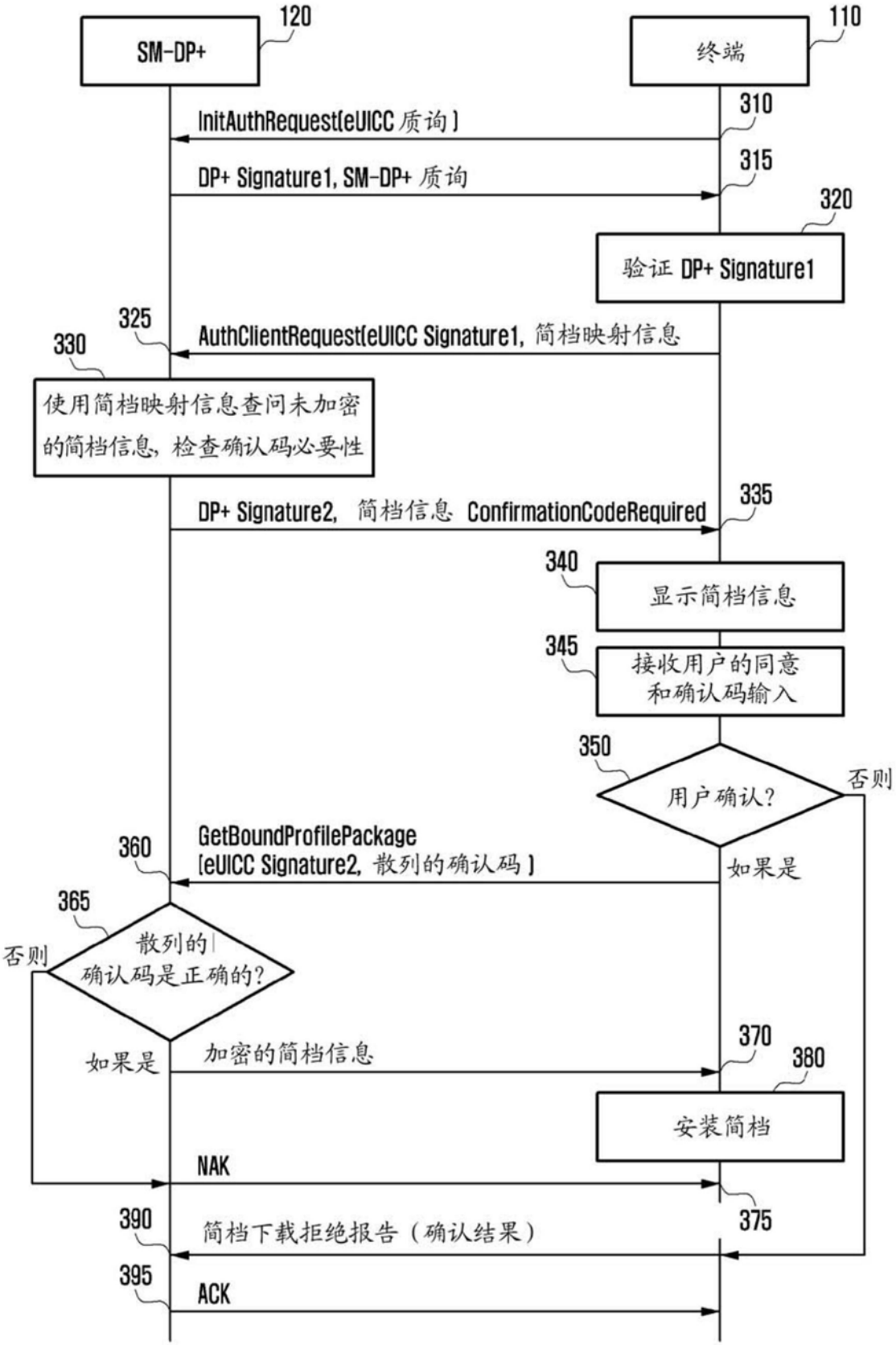

SM-DP+
120
终端
110
310
InitAuthRequest(eUICC 质询)
315
DP+ Signature1, SM-DP+ 质询
320
验证 DP+ Signature1
325
AuthClientRequest(eUICC Signature1, 简档映射信息
330
使用简档映射信息查问未加密的简档信息，检查确认码必要性
335
DP+ Signature2, 简档信息 ConfirmationCodeRequired
340
显示简档信息
345
接收用户的同意和确认码输入
350
用户确认?
否则
如果是
360
GetBoundProfilePackage
(eUICC Signature2, 散列的确认码)
365
散列的确认码是正确的?
否则
如果是
370
加密的简档信息
380
安装简档
NAK
375
390
简档下载拒绝报告（确认结果）
395
ACK

图3

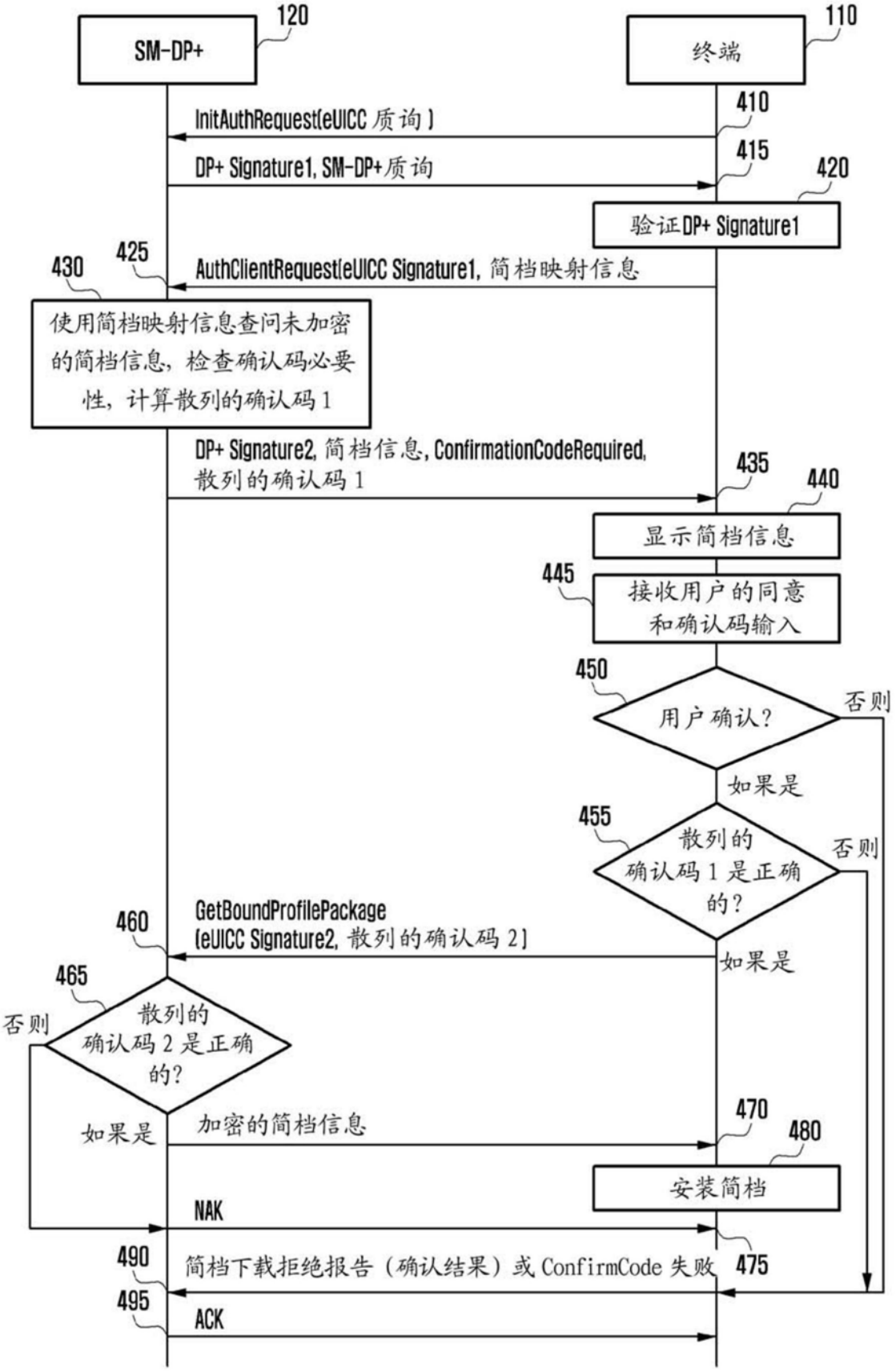

SM-DP+
120
终端
110
410
InitAuthRequest(eUICC 质询)
415
DP+ Signature1, SM-DP+质询
420
验证DP+ Signature1
425
430
AuthClientRequest(eUICC Signature1, 简档映射信息
使用简档映射信息查问未加密的简档信息，检查确认码必要性，计算散列的确认码 1
DP+ Signature2, 简档信息, ConfirmationCodeRequired, 散列的确认码 1
435
440
显示简档信息
445
接收用户的同意和确认码输入
450
用户确认?
否则
如果是
455
散列的确认码 1 是正确的?
否则
460
GetBoundProfilePackage (eUICC Signature2, 散列的确认码 2)
如果是
465
否则
散列的确认码 2 是正确的?
如果是
470
加密的简档信息
480
安装简档
NAK
475
490
简档下载拒绝报告（确认结果）或 ConfirmCode 失败
495
ACK

图4

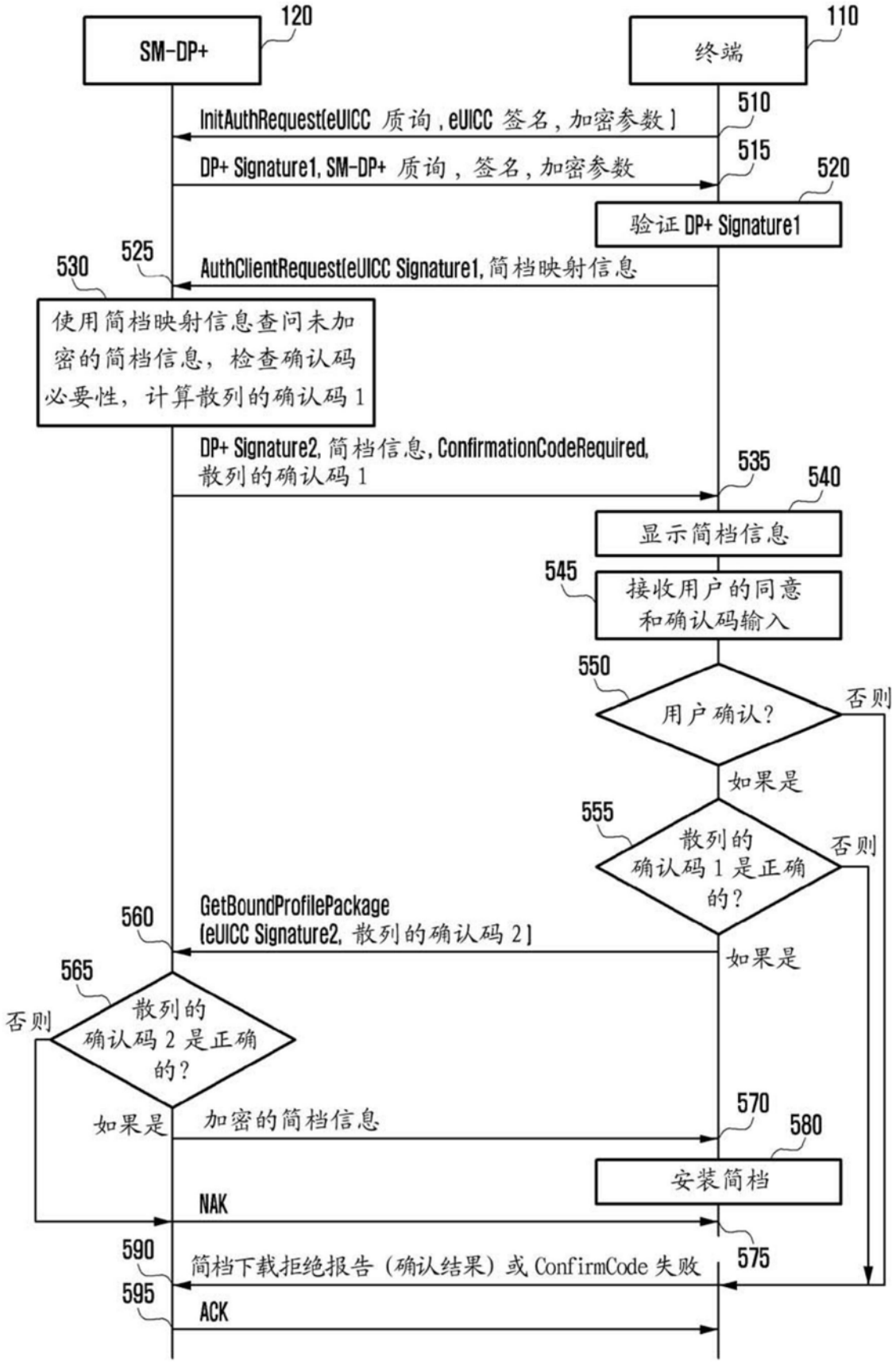

SM-DP+
120
终端
110
InitAuthRequest(eUICC 质询，eUICC 签名，加密参数)
510
DP+ Signature1, SM-DP+ 质询，签名，加密参数
515
520
验证 DP+ Signature1
525
530
AuthClientRequest(eUICC Signature1, 简档映射信息
使用简档映射信息查问未加密的简档信息，检查确认码必要性，计算散列的确认码 1
DP+ Signature2, 简档信息, ConfirmationCodeRequired, 散列的确认码 1
535
540
显示简档信息
545
接收用户的同意和确认码输入
550
用户确认?
否则
如果是
555
散列的确认码 1 是正确的?
否则
560
GetBoundProfilePackage (eUICC Signature2, 散列的确认码 2)
如果是
565
散列的确认码 2 是正确的?
否则
如果是
加密的简档信息
570
580
安装简档
NAK
575
590
简档下载拒绝报告（确认结果）或 ConfirmCode 失败
595
ACK

图5

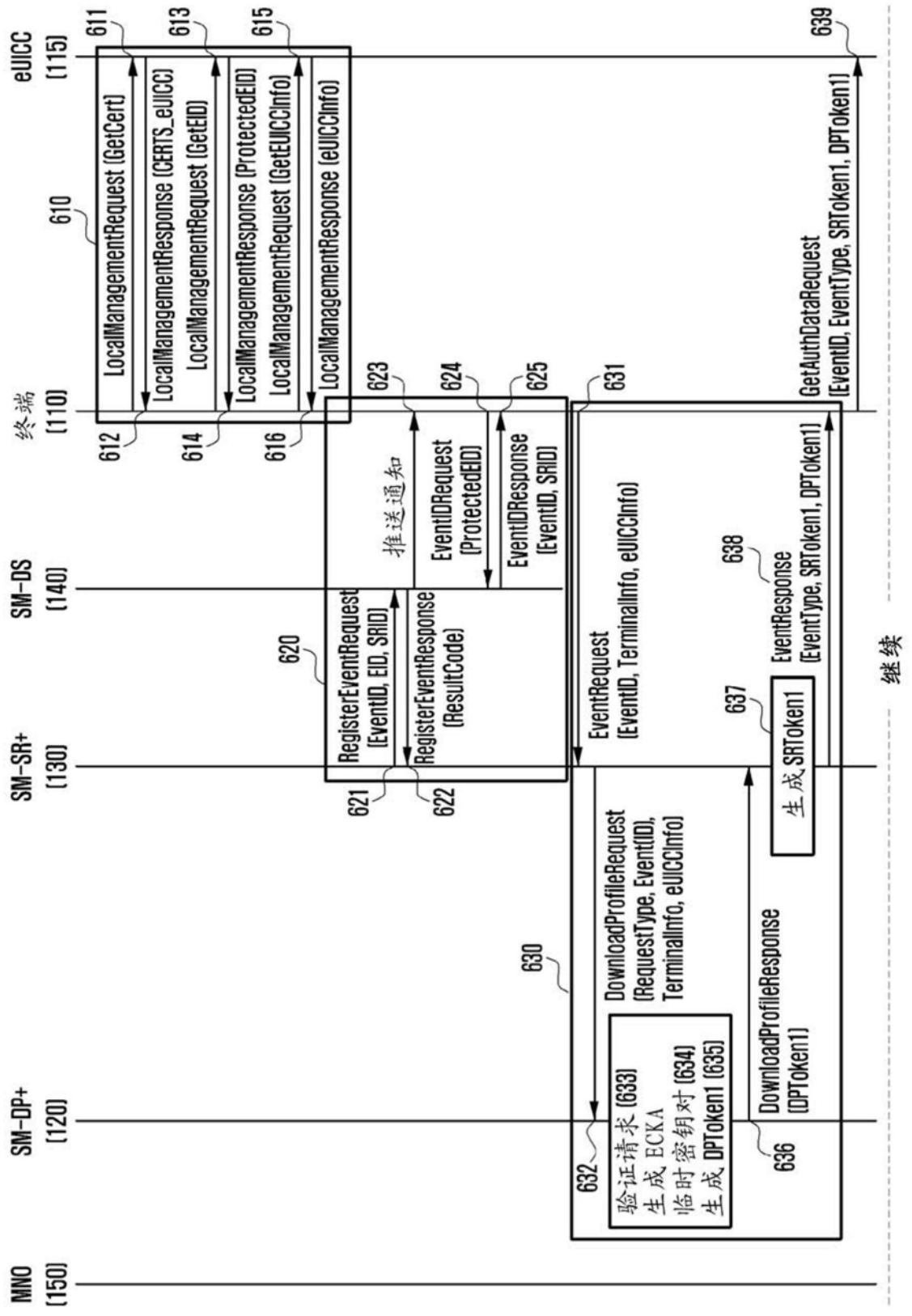

eUICC (115)
终端 (110)
SM-DS (140)
SM-SR+ (130)
SM-DP+ (120)
MNO (150)
611
610
612
LocalManagementRequest (GetCert)
613
LocalManagementResponse (CERTS_eUICC)
614
LocalManagementRequest (GetEID)
615
LocalManagementResponse (ProtectedEID)
616
LocalManagementRequest (GetEUICCInfo)
LocalManagementResponse (eUICCInfo)
620
RegisterEventRequest (EventID, EID, SRID)
621
RegisterEventResponse (ResultCode)
622
推送通知
623
EventIDRequest (ProtectedEID)
624
EventIDResponse (EventID, SRID)
625
630
631
EventRequest (EventID, TerminalInfo, eUICCInfo)
632
验证请求 (633)
生成 ECKA
临时密钥对 (634)
生成 DPToken1 (635)
DownloadProfileRequest (RequestType, EventID, TerminalInfo, eUICCInfo)
636
DownloadProfileResponse (DPToken1)
637
生成 SRToken1
638
EventResponse (EventType, SRToken1, DPToken1)
639
GetAuthDataRequest (EventID, EventType, SRToken1, DPToken1)
继续

图6a

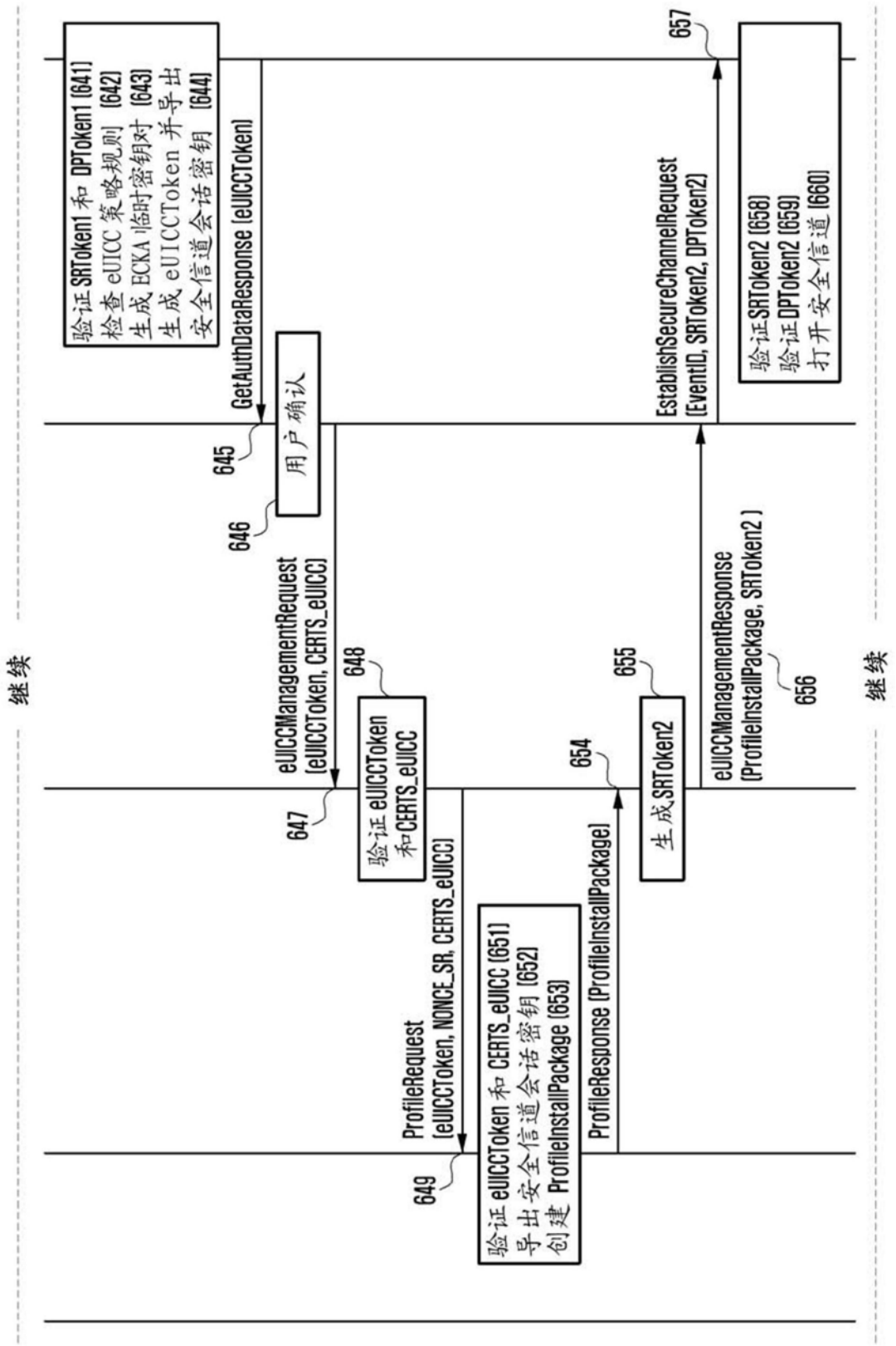

继续
验证SRToken1和DPToken1 [641]
检查eUICC策略规则 [642]
生成ECKA临时密钥对 [643]
生成eUICCToken并导出
安全信道会话密钥 [644]
GetAuthDataResponse (eUICCToken)
645
用户确认
646
eUICCManagementRequest
(eUICCToken, CERTS_eUICC)
647
验证eUICCToken
和CERTS_eUICC
648
ProfileRequest
(eUICCToken, NONCE_SR, CERTS_eUICC)
649
验证eUICCToken和CERTS_eUICC (651)
导出安全信道会话密钥 [652]
创建ProfileInstallPackage (653)
ProfileResponse (ProfileInstallPackage)
654
生成SRToken2
655
eUICCManagementResponse
(ProfileInstallPackage, SRToken2)
656
EstablishSecureChannelRequest
(EventID, SRToken2, DPToken2)
657
验证SRToken2 [658]
验证DPToken2 [659]
打开安全信道 [660]
继续

图6b

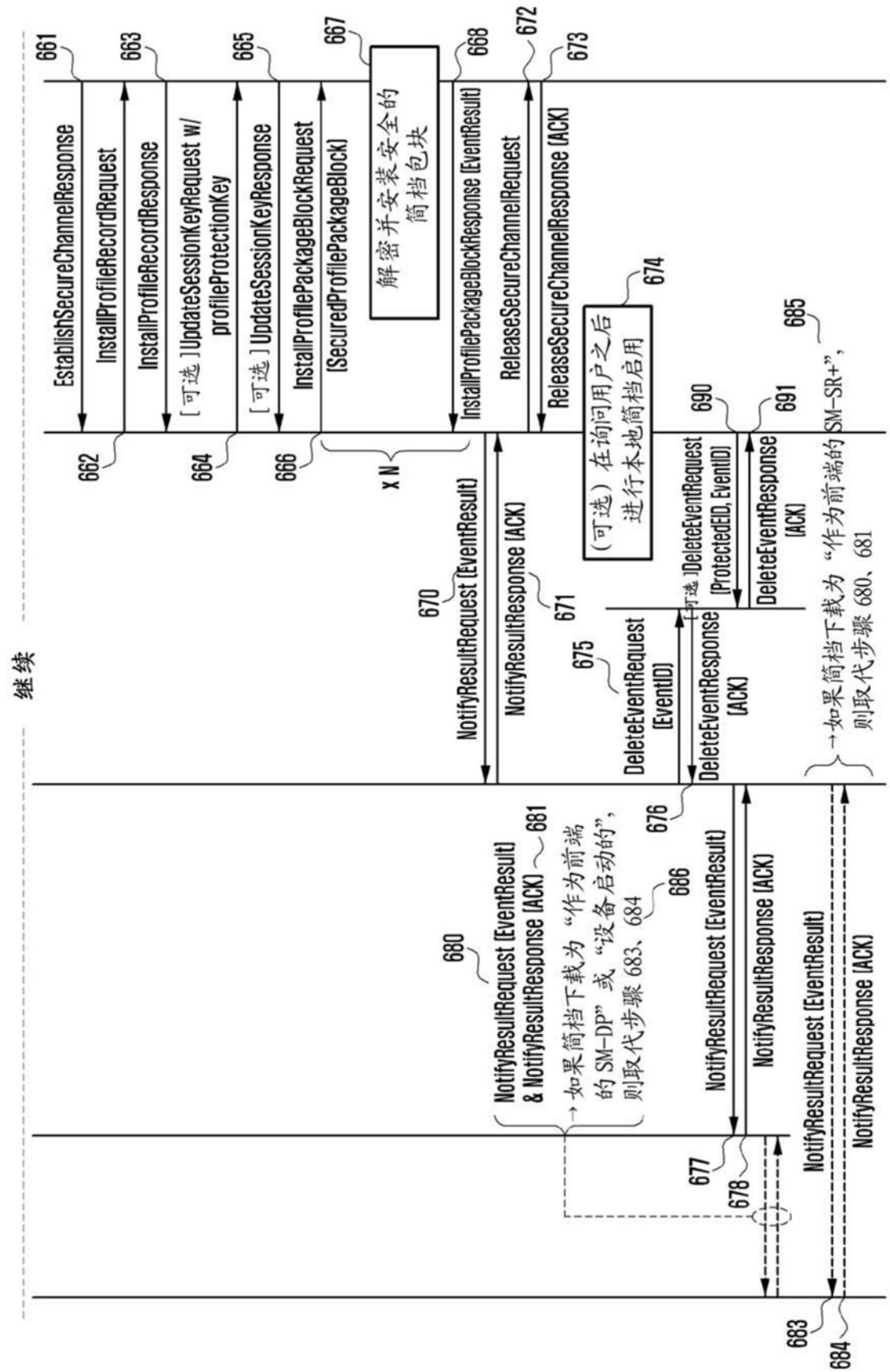

661
EstablishSecureChannelResponse
662
663
InstallProfileRecordRequest
664
InstallProfileRecordResponse
665
[可选]UpdateSessionKeyRequest w/ profileProtectionKey
666
[可选]UpdateSessionKeyResponse
667
InstallProfilePackageBlockRequest
[SecuredProfilePackageBlock]
解密并安装安全的简档包块
668
InstallProfilePackageBlockResponse [EventResult]
672
ReleaseSecureChannelRequest
673
ReleaseSecureChannelResponse [ACK]
674
(可选)在询问用户之后进行本地简档启用
685
→如果简档下载为“作为前端的SM-SR+”，则取代步骤680、681
690
[可选]DeleteEventRequest [ProtectedEID, EventID]
691
DeleteEventResponse [ACK]
X N
670
NotifyResultRequest [EventResult]
671
NotifyResultResponse [ACK]
675
DeleteEventRequest [EventID]
676
DeleteEventResponse [ACK]
680
NotifyResultRequest [EventResult] & NotifyResultResponse [ACK]
681
→如果简档下载为“作为前端的SM-DP”或“设备启动的”，则取代步骤683、684
686
NotifyResultRequest [EventResult]
677
NotifyResultResponse [ACK]
678
NotifyResultRequest [EventResult]
683
NotifyResultResponse [ACK]
684
继续

图6c

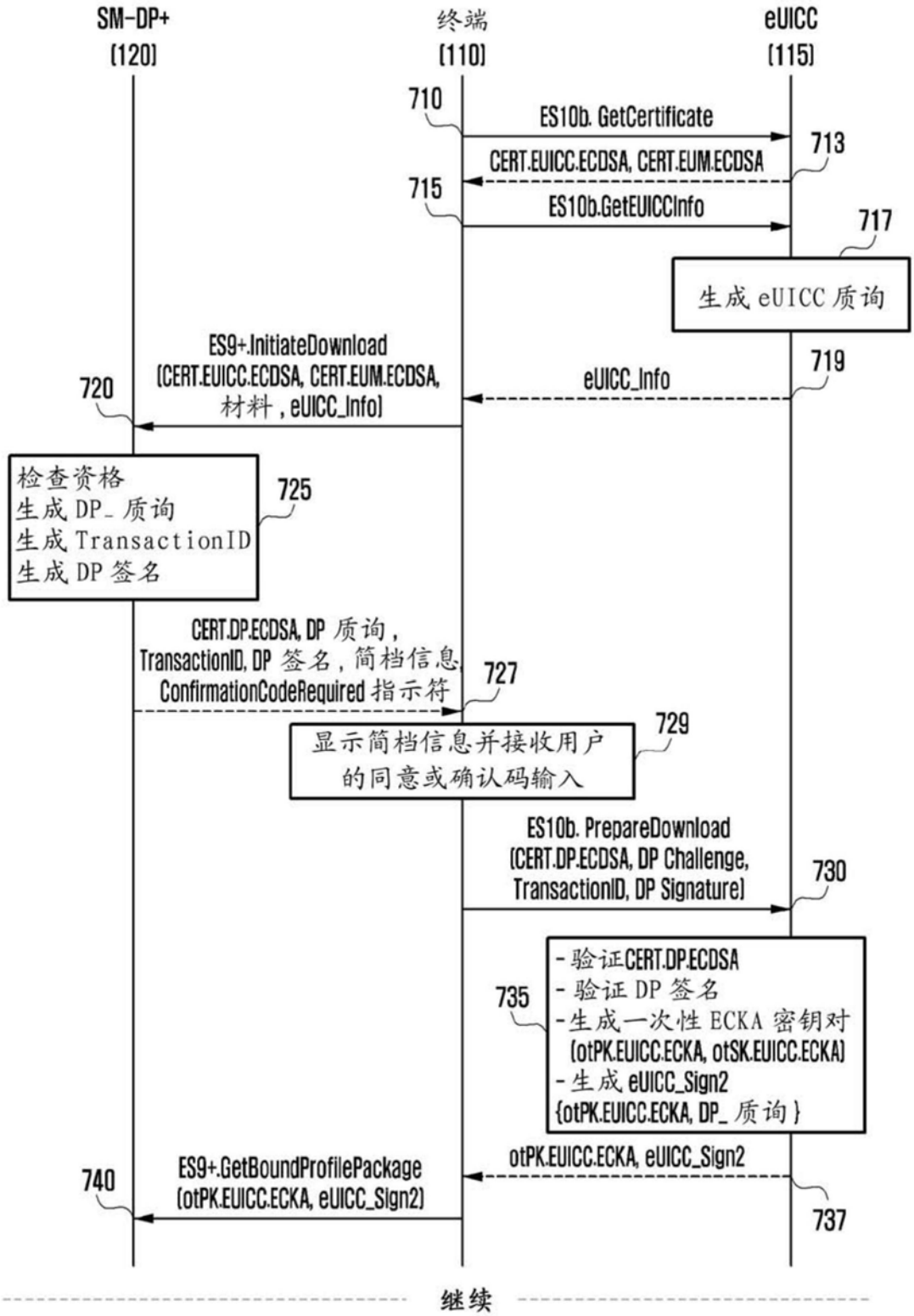

SM-DP+
(120)
终端
(110)
eUICC
(115)
710
ES10b. GetCertificate
713
CERT.EUICC.ECDSA, CERT.EUM.ECDSA
715
ES10b.GetEUICCInfo
717
生成 eUICC 质询
ES9+.InitiateDownload
(CERT.EUICC.ECDSA, CERT.EUM.ECDSA,
材料, eUICC_Info)
720
eUICC_Info
719
检查资格
生成 DP_ 质询
生成 TransactionID
生成 DP 签名
725
CERT.DP.ECDSA, DP 质询,
TransactionID, DP 签名, 简档信息,
ConfirmationCodeRequired 指示符
727
显示简档信息并接收用户
的同意或确认码输入
729
ES10b. PrepareDownload
(CERT.DP.ECDSA, DP Challenge,
TransactionID, DP Signature)
730
- 验证CERT.DP.ECDSA
- 验证 DP 签名
- 生成一次性 ECKA 密钥对
(otPK.EUICC.ECKA, otSK.EUICC.ECKA)
- 生成 eUICC_Sign2
{otPK.EUICC.ECKA, DP_ 质询}
735
otPK.EUICC.ECKA, eUICC_Sign2
737
ES9+.GetBoundProfilePackage
(otPK.EUICC.ECKA, eUICC_Sign2)
740
继续

图7a

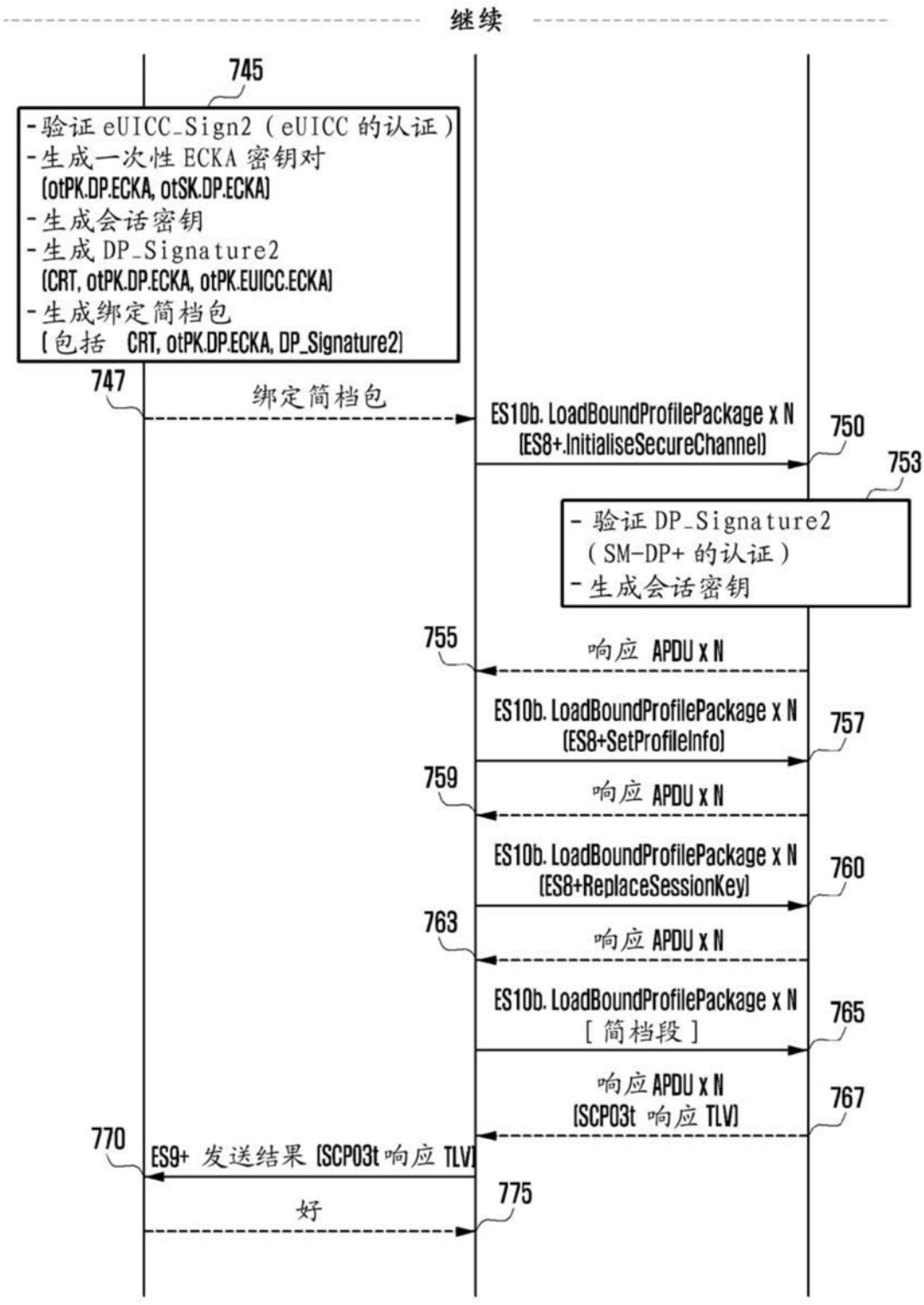

继续
745
-验证 eUICC_Sign2 (eUICC 的认证)
-生成一次性 ECKA 密钥对
(otPK.DP.ECKA, otSK.DP.ECKA)
-生成会话密钥
-生成 DP_Signature2
(CRT, otPK.DP.ECKA, otPK.EUICC.ECKA)
-生成绑定简档包
(包括 CRT, otPK.DP.ECKA, DP_Signature2)
747
绑定简档包
ES10b. LoadBoundProfilePackage x N
(ES8+.InitialiseSecureChannel)
750
753
- 验证 DP_Signature2
(SM-DP+ 的认证)
- 生成会话密钥
755
响应 APDU x N
ES10b. LoadBoundProfilePackage x N
(ES8+SetProfileInfo)
757
759
响应 APDU x N
ES10b. LoadBoundProfilePackage x N
(ES8+ReplaceSessionKey)
760
763
响应 APDU x N
ES10b. LoadBoundProfilePackage x N
[简档段]
765
响应 APDU x N
(SCP03t 响应 TLV)
767
770
ES9+ 发送结果 (SCP03t 响应 TLV)
775
好

图7b

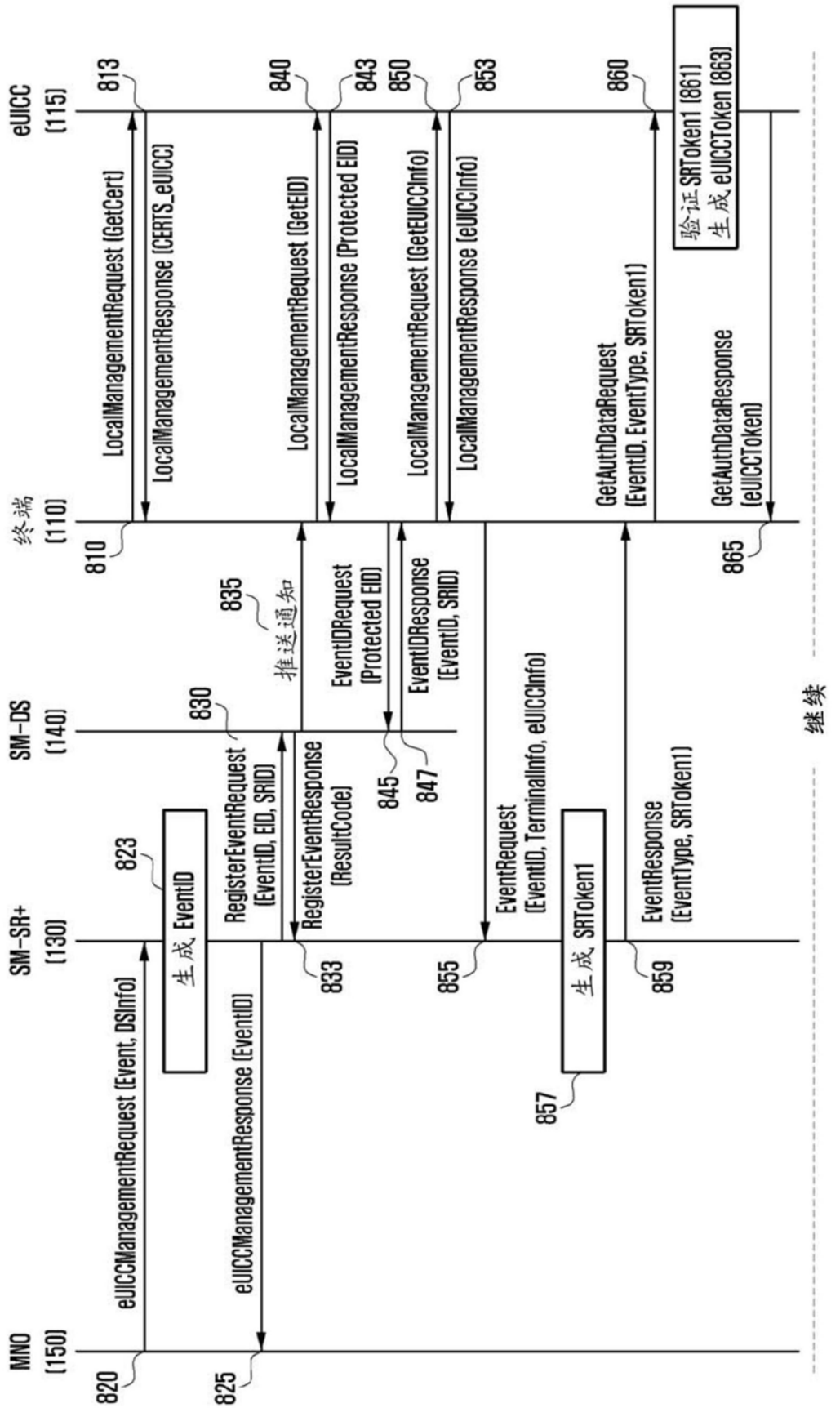

MNO
(150)
SM-SR+
(130)
SM-DS
(140)
终端
(110)
eUICC
(115)
820
825
823
生成 EventID
eUICCManagementRequest (Event, DSInfo)
eUICCManagementResponse (EventID)
830
RegisterEventRequest
(EventID, EID, SRID)
RegisterEventResponse
(ResultCode)
833
835
推送通知
845
EventIDRequest
(Protected EID)
847
EventIDResponse
(EventID, SRID)
855
EventRequest
(EventID, TerminalInfo, eUICCInfo)
857
生成 SRToken1
859
EventResponse
(EventType, SRToken1)
865
GetAuthDataResponse
(eUICCToken)
810
813
LocalManagementRequest (GetCert)
LocalManagementResponse (CERTS_eUICC)
840
LocalManagementRequest (GetEID)
843
LocalManagementResponse (Protected EID)
850
LocalManagementRequest (GetEUICCInfo)
853
LocalManagementResponse (eUICCInfo)
860
GetAuthDataRequest
(EventID, EventType, SRToken1)
验证 SRToken1 (861)
生成 eUICCToken (863)
继续

图8a

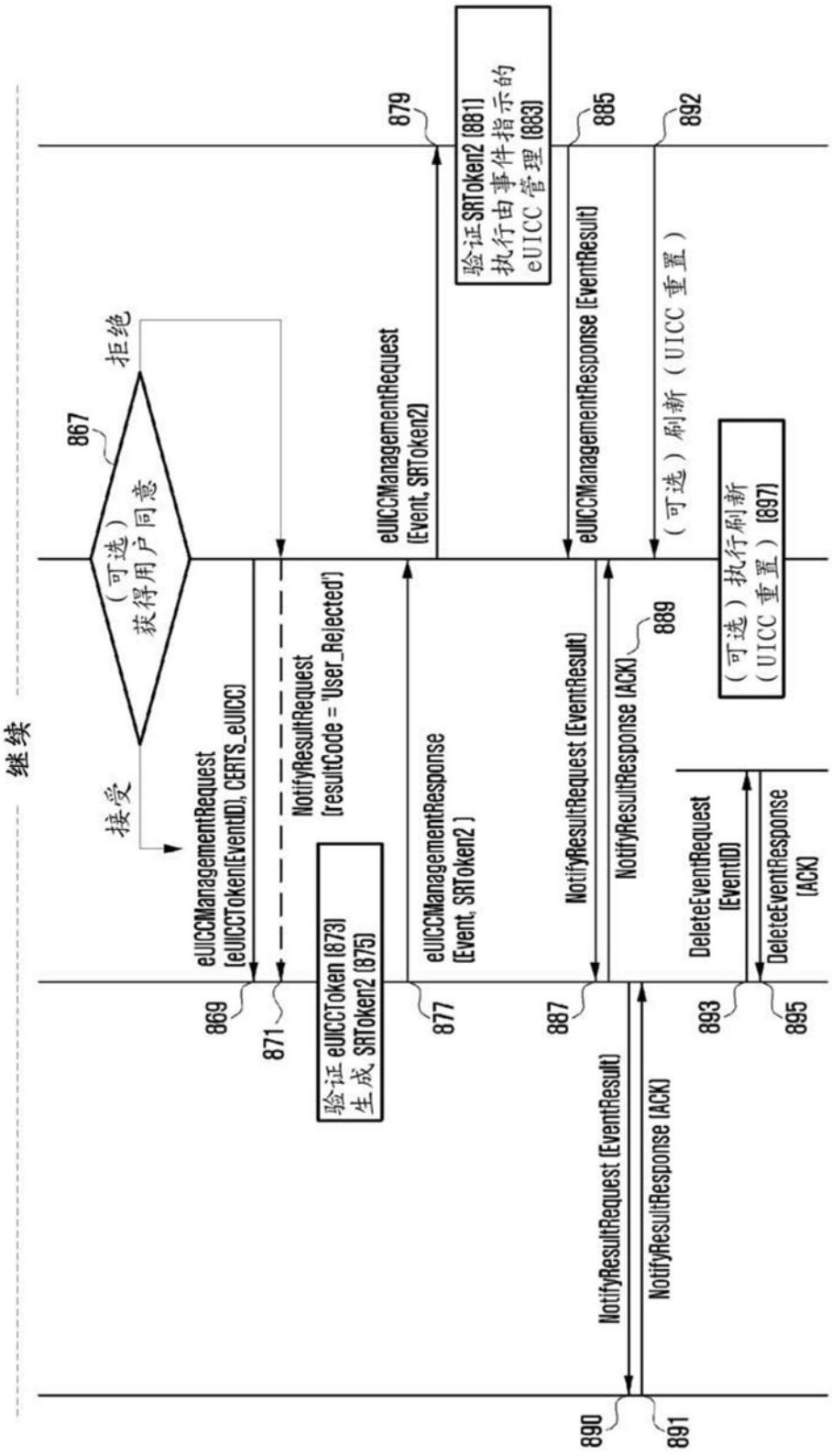

继续
(可选)
获得用户同意
867
拒绝
接受
eUICCManagementRequest
[eUICCToken(EventID), CERTS_eUICC]
869
NotifyResultRequest
[resultCode = 'User_Rejected']
871
验证 eUICCToken [873]
生成 SRToken2 [875]
eUICCManagementResponse
[Event, SRToken2]
877
eUICCManagementRequest
[Event, SRToken2]
879
验证SRToken2 [881]
执行由事件指示的
eUICC 管理 [883]
885
eUICCManagementResponse [EventResult]
887
NotifyResultRequest [EventResult]
889
NotifyResultResponse [ACK]
(可选)刷新(UICC 重置) 892
(可选)执行刷新
(UICC 重置) [897]
DeleteEventRequest
[EventID]
893
DeleteEventResponse
[ACK]
895
NotifyResultRequest [EventResult]
890
NotifyResultResponse [ACK]
891

图8b

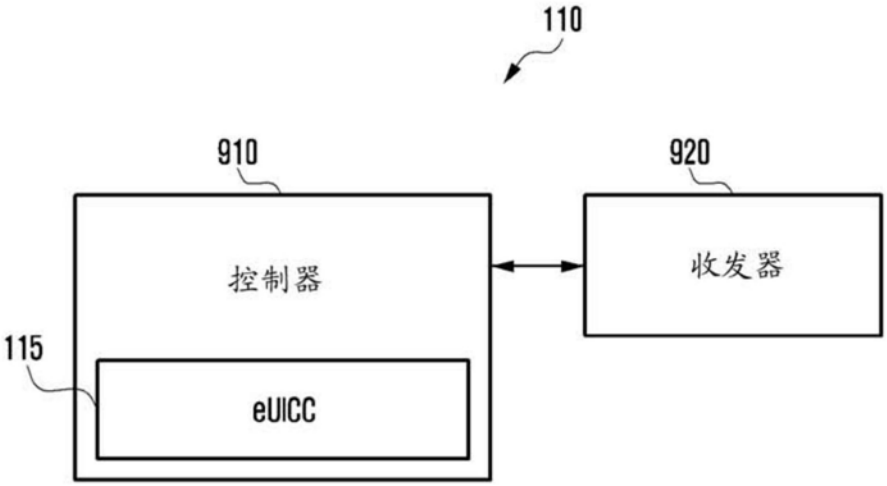

110
910
920
控制器
收发器
115
eUICC

图9

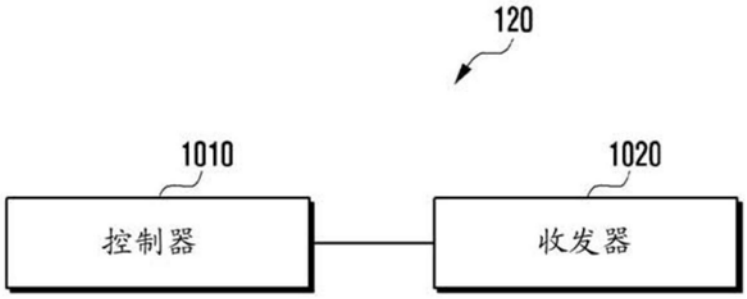

120
1010
1020
控制器
收发器

图10

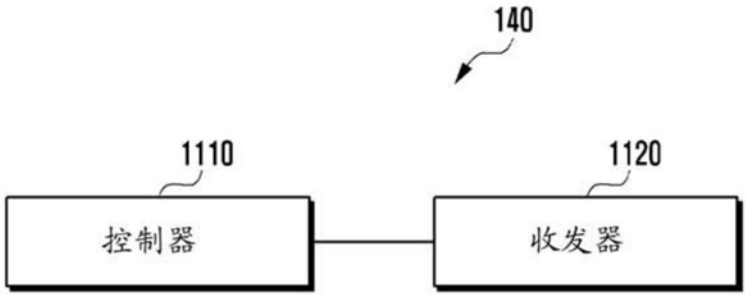

140
1110
1120
控制器
收发器

图11

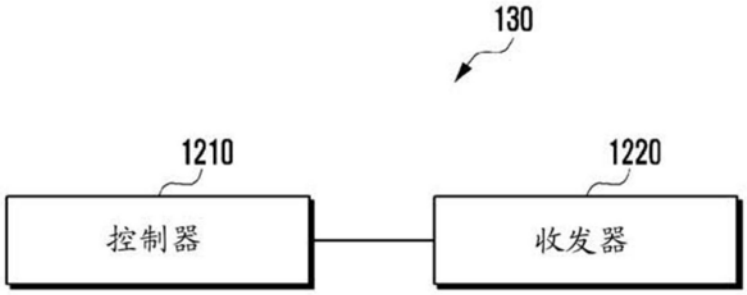


图12