

ICS 33.060

M 30

**YD**

# 中华人民共和国通信行业标准

YD/T 2926-2015

---

## 嵌入式通用集成电路卡 (eUICC) 远程管理平台技术要求 (第一阶段)

Technical requirements of embedded UICC  
remote management platform (phase one)

2015-07-14 发布

2015-10-01 实施

---

中华人民共和国工业和信息化部 发布





## 目 次

前 言	II
引 言	III
1 范围	1
2 规范性引用文件	1
3 术语、定义和缩略语	1
3.1 术语与定义	1
3.2 缩略语	3
4 eUICC 远程管理架构	4
4.1 概述	4
4.2 总体架构	4
4.3 角色	5
5 eUICC 技术要求	5
5.1 eUICC 物理要求	5
5.2 卡发行管理要求	6
5.3 eUICC 及其远程管理要求	6
6 eUICC 远程管理平台技术要求	6
6.1 主要功能	6
6.2 接口要求	8
6.3 业务流程	9
6.4 Profile 定义	15
6.5 策略控制 (PCF) 功能	16
7 eUICC 远程管理安全要求	17
7.1 安全等级和认证	17
7.2 安全通信	19
8 无运营商网络覆盖情况下技术要求	20
8.1 场景	20
8.2 切换类型和规则	20
8.3 技术要求	20





## 前 言

嵌入式通用集成电路卡（eUICC）远程管理平台的系列标准预计包括：

- 《嵌入式通用集成电路卡（eUICC）远程管理平台技术要求（第一阶段）》；
- 《嵌入式通用集成电路卡（eUICC）远程管理平台测试要求（第一阶段）》。

本标准按照GB/T 1.1—2009给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：中国联合网络通信集团有限公司、北京邮电大学、华为技术有限公司。

本标准主要起草人：张云勇、张 尼、姚海鹏、宫 雪、陈 豪、刘廉如、陶 冶、黄 韬、高林毅。





## 引 言

物联网被称为继计算机、互联网之后，世界信息产业的第三次浪潮，代表了下一代信息技术发展方向，美国、欧盟、中国等国纷纷出台物联网发展规划，进行相关技术和产业前瞻布局。eUICC 作为物联网终端接入运营商网络的鉴权工具，以及承载各种应用、数据的安全载体，已经成为物联网发展的关键核心技术。

应用于物联网业务的 eUICC 已不仅仅是一种新的 UICC 卡形态或用户终端设备形态，还包括为支持这种新形态设备而建立的整体系统，其中 eUICC 的设备管理、用户关系管理、远程管理、业务管理和安全管理可能都将是该系统中必不可少的功能。

其中 eUICC 远程管理的引入是为了满足海量物联网设备批量开卡，降低国际漫游成本等行业需求，eUICC 的远程管理意味着突破了传统的由运营商管控的 UICC 线性流程管理，可能导致运营商迁移，其用户关系管理前所未有的复杂和灵活并对现有安全机制产生重大影响。





# 嵌入式通用集成电路卡 (eUICC) 远程管理平台技术要求 (第一阶段)

## 1 范围

本标准规定嵌入式通用集成电路卡 (eUICC) 远程管理平台的技术要求, 包括远程管理平台架构、技术要求、功能要求、接口要求、业务流程、安全要求等内容。

本标准适用于物联网领域的嵌入式通用集成电路卡 (eUICC) 远程管理平台。

## 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件, 仅所注日期的版本适用于本文件。凡是不注日期的引用文件, 其最新版本 (包括所有的修改单) 适用于本文件。

ISO/IEC 15408 信息技术安全评估准则

ETSI TS 103.383 嵌入式 UICC 卡需求规范

GSMA 12FAST.13 GSMA 嵌入式 UICC 卡远程管理架构

全球平台智能卡技术规范 GlobalPlatform Card Specification

## 3 术语、定义和缩略语

### 3.1 术语与定义

下列术语和定义适用于本文件。

#### 3.1.1

客户 Users

付费方、法律责任人或实体。

#### 3.1.2

设备 Devices

装配期间嵌入式UICC和通信模块所嵌入的设备。例如: 智能仪表、汽车和照相机。

#### 3.1.3

嵌入式移动设备 Embedded Mobile Device

具备嵌入式3GPP网络接入能力的设备。例如照相机、车载终端和笔记本电脑。

#### 3.1.4

嵌入式通用集成电路卡 Embedded Universal Integrated Circuit Card

不容易接触或替换的UICC, 在终端中不能被删除或替换, 并可安全的进行签约变更。

#### 3.1.5

用户信息 Profile

待配置或出现在eUICC上的文件结构、数据和应用程序的集合。详细定义见6.4节。

#### 3.1.6

用户信息激活 Enabled Profile

用户信息的状态, 通过UICC-终端接口选择它的文件和/或应用程序(例如NAA)。



3.1.7

集成电路卡识别码 Integrated Circuit Card Identity

存储在UICC上的UICC硬件的唯一号码，并且刻在硬件上。该号码遵循ITU-T的E.118定义。

3.1.8

国际移动用户识别码 International Mobile Subscriber Identification Number

由移动运营商发行和拥有的SIM应用程序的唯一标识符，支持设备访问网络和使用服务。

3.1.9

移动网络运营商 Mobile Network Operator

通过移动网络基础设施给客户提供通信服务的实体。

3.1.10

网络接入应用 Network Access Application

保存在UICC上提供网络接入授权的应用程序。如USIM应用程序。

3.1.11

网络接入信任状 Network Access Credentials

ITU E.212[i.1]网络验证需要的数据。可能包括的数据如Ki/ K和存储在NAA的IMSI。

3.1.12

策略 Policy

表现为一组规则的原则，管理eUICC和/或参与eUICC远程管理的实体的行为。

3.1.13

策略控制功能 Policy Control Function

定义、更新或删除策略规则来执行策略的功能。

3.1.14

策略执行功能 Policy Enforcement Function

执行策略规则来实现策略的功能。

3.1.15

策略规则 Policy Rule

定义策略的原子操作及执行条件。

3.1.16

用户信息接入信任状 Profileaccess Credentials

存在于Profile内的数据，这样外部实体能建立安全通信，目的是为了管理Profile的结构和数据。

3.1.17

用户信息管理信任状 Profilemanagement Credentials

存在于eUICC内的数据，这样外部实体和eUICC之间能建立安全通信，目的是为了管理eUICC上Profile的加载、启用、禁用和删除。

3.1.18

角色 Role

角色是代表逻辑分组功能的实体。



## 3.1.19

远程管理平台 Subscription Management Platform

远程管理平台主要有两部分功能：数据准备和数据路由，详细功能描述见4.2。

## 3.2 缩略语

下列缩略语适用于本文件。

3G	3rd-generation	第三代移动通信技术
AuC	Authentication Center	鉴权中心
CA	Certificate Authority	证书授权中心
CRM	Customer Relationship Management	客户关系管理
EID	eUICC ID	eUICC标识
EIS	eUICC Information Set	eUICC信息集
eUICC	Embedded Universal Integrated Circuit Card	嵌入式通用集成电路卡
GPCS	GlobalPlatform Card Specification	全球平台智能卡技术规范
HLR	Home Location Register	归属位置寄存器
ID	Identity	标识
ICCID	Integrate circuit card identity	集成电路卡识别码
IMSI	International Mobile Subscriber Identity	国际移动用户识别码
M2M	Machine to Machine	机器对机器通信
MNO	Mobile Network Operator	移动网络运营商
MSISDN	Mobile Subscriber International ISDN/PSTN number	移动台识别号码
NAA	Network Access Application	网络接入应用
NAC	Network Access Control	网络准入控制
OS	Operating System	操作系统
OTA	Over The Air	空中下载技术
OTI	Over The Internet	网络下载技术
PCF	Policy Control Function	策略控制功能
PKI	Public Key Infrastructure	公钥基础设施
PIN	Personal Identification Number	个人识别密码
STK	SIM Tool Kit	SIM工具包
SIM	Subscriber Identity Module	客户识别模块
UICC	Universal Integrated Circuit Card	通用集成电路卡
USAT	USIM Application Toolkit	USIM应用工具箱
USIM	Universal Subscriber Identity Module	通用用户识别模块
VPLMN	Visited Public Land Mobile Network	访问公共陆地移动网络



## 4 eUICC 远程管理架构

### 4.1 概述

eUICC 已不仅仅是一种新的通用集成电路卡形态，其还包括为支撑这种新的卡形态而建立的一系列系统接口、平台，以及保障安全可信的业务提供和运营管理等。因此，eUICC 涉及到一种新的系统架构，在这种架构中，终端管理、用户签约关系管理、个人定制化管理、业务管理、安全管理将是该系统中不可或缺的功能。而远程签约管理是其中最基本、最关键的功能之一，其在一定程度上决定或影响着其他管理功能的实现。

eUICC 签约管理意味着突破了传统由运营商管控的 UICC 线性流程管理：传统的 SIM 卡生命周期呈现线性特征，其包括制卡，选择运营商，定制，发行，激活，使用，终止签约几个阶段，并且呈现不可逆的特性；而引入物联网智能卡后，SIM 卡的生命周期将被重新定义，包括发行前（生产、发行、选择运营商）和发行后（选择/变更运营商、定制、使用、终止签约），其中发行后仍然可以选择运营商和变更运营商。尤其由于在物联网智能卡中引入更换运营商的可能性，其用户关系管理变得更加复杂和灵活。

### 4.2 总体架构

图 1 所示描述了参与 eUICC 远程管理的三种角色：eUICC 制造商、运营商（MNO）和远程管理平台。在上述架构中，远程管理平台是 eUICC 远程管理的核心。eUICC 中涉及运营商及卡商的数据须经由远程管理平台生成完整的运营商数据文件后，才能通过空中写卡等方式下载到 eUICC 卡中。此外，运营商数据的变更、eUICC 更换运营商等过程也经由远程管理平台完成。远程管理平台功能的实现一定程度上还决定或影响着其它管理功能的实现。远程管理平台功能主要实现 eUICC 远程下载 Profile，并且通过提供授权、认证、防重放攻击、隐私保护、完整性保护等措施保证下载过程的安全性。

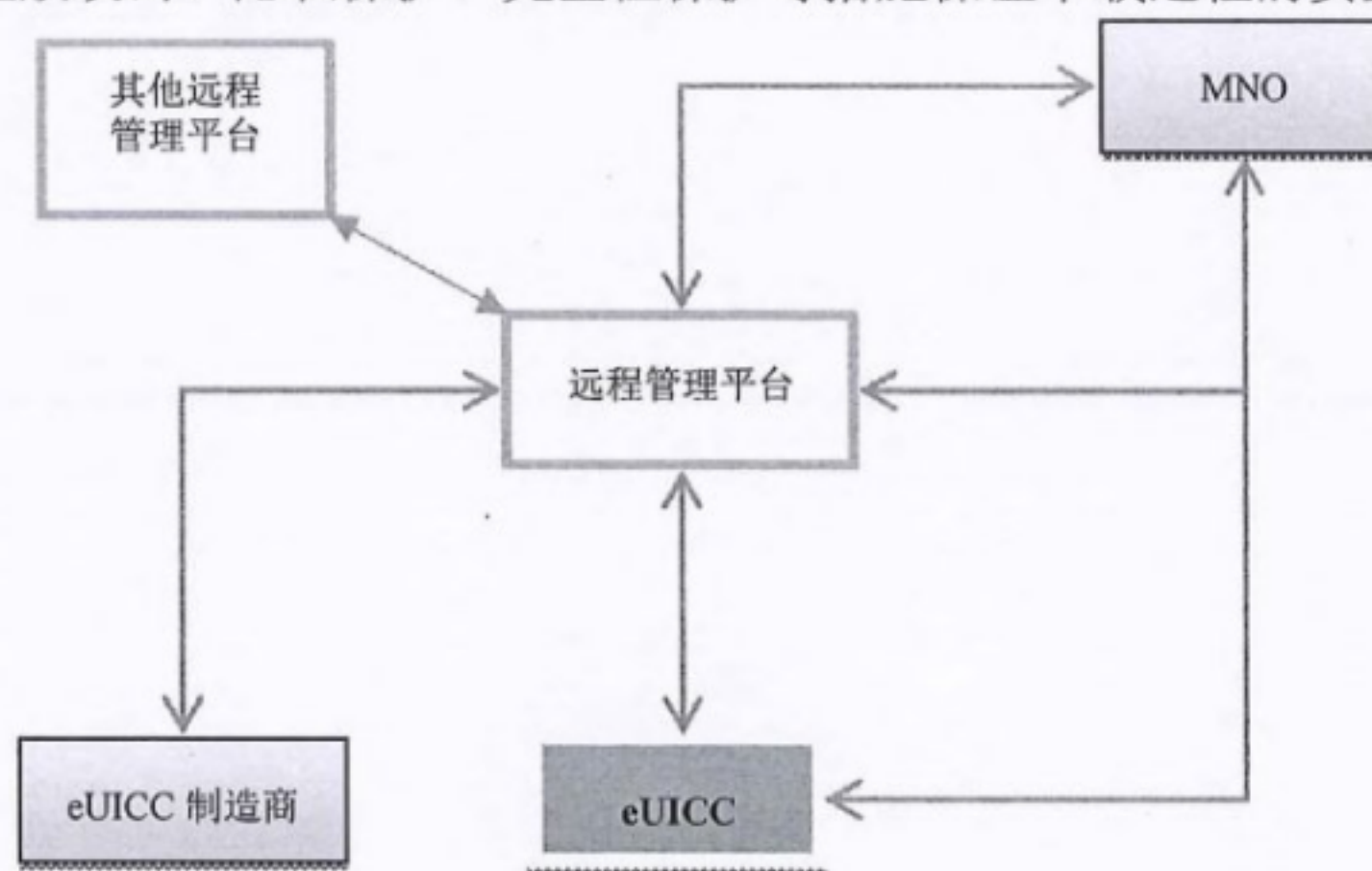


图 1 eUICC 远程管理总体架构

其中，远程管理平台处于网络架构的核心地位，远程管理平台的功能主要包括两部分：数据准备和数据路由。其中，数据准备主要负责 eUICC 卡远程配置的用户签约数据（Profile）的安全生成、存储和下载；数据路由主要负责 eUICC 卡远程配置数据的安全传输和管理。上述功能可以由一个或多个物理实体进行系统实现。

数据准备主要负责 Profile 的可靠准备和存储，数据准备功能拥有 Profile 配置信任状（Profile Provisioning Credentials）。在数据准备阶段，远程管理平台接收来自 MNO 的签约数据（如 IMSI 等），进而生成 Profile，进行加密（由于该数据由运营商证书及其他敏感数据组成，尤其是密钥 K 和 NAA 算法参数），通过数据路由功能实现 Profile 安全下载到 eUICC 中。



在 eUICC 远程管理架构中，数据路由主要负责建立到 eUICC 的安全通道，转发 eUICC 和数据准备之间的消息或数据；将数据准备生成的 Profile 可靠路由并且下载到目标 eUICC 中，并负责将 eUICC 发送的消息路由到数据准备。同时，数据路由也负责管理 eUICC 中的 Profile，如激活、去激活、删除等。数据路由拥有 Profile 管理信任状，可以与 eUICC 建立通信通道，而且数据准备与 eUICC 通信都需经过数据路由建立通信通道，通过这条通信通道，利用 eUICC 信任状可以安全的将要求的数据传至 eUICC。

4.3 角色

eUICC 远程签约管理的角色主要涉及设备制造商、智能卡提供商、电信运营商、远程管理平台商等，详细描述见表 1。

表 1 eUICC 远程签约管理角色描述

序号	角色	详细描述
1	设备供应商	提供的设备包括无线通信模块，该模块通过运营商网络实现通信
2	eUICC 供应商	提供安全的 eUICC 组件及其相关软件（例如固件和操作系统），其中，硬件、软件和生产过程应该进行相关认证以达到指定安全等级
3	物联网服务提供商	为商业客户和消费者提供 M2M 服务，其中，根据服务提供商请求，签约管理服务商在 eUICC 中配置单个或多个运营商签约信息，如配置多个运营商签约信息时，同时完成对新签约的激活
4	移动网络运营商 (MNO)	提供移动通信网络服务，当运营商不承担远程管理平台角色时，运营商应该至少和一家远程管理平台服务商实现连接
5	eUICC 远程管理服务商	远程管理平台商：一个运营商信任的，管理 eUICC 中可用配置和其它配置的实体。在 eUICC 产业链中，此角色可以由运营商承担，也可有由受信的第三方承担

5 eUICC 技术要求

5.1 eUICC 物理要求

物联网典型应用环境对 eUICC 卡的需求跟普通 UICC 卡不同，手机上使用的 UICC 卡的需求更多在于软件层面，其使用环境对卡的封装工艺和硬件等没有特殊要求。而物联网环境下，对卡增加了硬件平台、软件平台、封装工艺以及物联网情况下物与物通信的要求，包括以下五个方面：

a) 物理要求：eUICC 卡应符合适应大温差、抗震动、防腐蚀、抗静电、耐湿等物理指标，eUICC 卡的物理连接触点更加可靠和更耐磨损，可能在大幅颠簸的场景中使用。

b) 存储要求：物联网使用的 SIM 卡要求数据保存的时间更长。普通 SIM 卡在手机里的平均保存时间是 3 到 5 年左右，而在物联网某些应用场景下（如电力行业）要求嵌入式 UICC 卡具备十年、十五年甚至更高的数据保存时间。

c) 卡擦写次数要求：普通移动终端对 SIM 卡的擦写一般只在开关机或者位置更换的时候进行，而在 M2M 应用领域，在数据采集的场景下，终端对 SIM 卡的擦写将会非常频繁；针对 SIM 卡传输速率，在物联网某些对数据采集、传输的实时性要求较高的应用领域，对嵌入式 UICC 卡与终端间的接口传输速度也有更高的需求。

d) 物理安全要求：在物联网环境中，智能卡主要用在机器设备或监控设备上，很可能是无人值守的场景，易受到外部攻击，需要对智能卡上关键数据的存储安全提出更高的需求，防止非授权使用、盗用等情况的发生。



e) eUICC 上的安全算法要求: 为了防止破解, eUICC 卡算法应选用为更高安全级别的算法, 如采用 3G 网络中的 Milenage 算法。另外 eUICC 可选择多算法支持, 或者允许 OS 更新以支持新加算法的支持。

## 5.2 卡发行管理要求

物联网中的物体数量会比以往任何一个网络中终端数量高出几个数量级, 原有的标志终端的方法通常用一串码号或卡号来进行, 如果在现有的技术体制内开展物联网应用, 必须提供充足的码号资源来标志泛在网内的终端或用户, 现有码号资源会变得非常贫乏。这对现有码号长度、分配原则以及回收方法等都提出了挑战。

此外, 当前移动网络中电信智能卡根据发行地、使用地以及卡片用途不同, 发行采用网络管理区域(省、地市)方法。但在物联网应用场景下, 由于智能卡通常存在于物联网终端中或者焊接在终端模块中, 其发行地及使用地很难在物联网终端生产时确定。因此, 在此种应用场景下, 需考虑物联网智能卡的首次使用时激活、换号不换卡发卡、测试环节激活业务等。

因此, 物联网业务对智能卡发行管理提出的新的需求, 其要求物联网智能卡具备空中配号、码号激活回收、远程业务管理、漫游支持等新的特性。

## 5.3 eUICC 及其远程管理要求

eUICC 与 UICC 的最大区别在于前者不能插拔, 难以通过传统的方式对其进行操作, eUICC 需要平台对其进行远程管理, 典型的远程应用场景如签约信息的远程配置、卡的远程激活、空中更换运营商等。因此, 要求:

- eUICC 无论是在发行前还是发行后, 应能提供一种安全的机制实现将用户签约信息配置到 eUICC 上。
- 应能从 eUICC 上安全删除对运营商的签约信息, 包括 ICCID、Key、IMSI、MSISDN 等参数和相关应用。
- 在运营商的管理控制下, eUICC 能配置多个属性参数集(Profile)。
- eUICC 可以支持去活, 例如被锁定和擦除内存。
- eUICC 能至少支持登陆网络所必需的最小参数集。
- 能远程实现重配置, 即把与一个新运营商相关联的订购数据配置到 eUICC 上。
- 运营商能对 eUICC 上自己的 Profile 内属性参数进行更新。
- eUICC 能支持 STK/USAT 应用。
- 应至少与现有 UICC 有相同安全级别等。

## 6 eUICC 远程管理平台技术要求

在 eUICC 远程管理架构中, 远程管理平台是核心, 用于管理用户签约信息的生成、下载、安装、激活、更换、删除等。远程管理平台的主要功能包括 Profile 的生成、下载、安装、激活、去激活、删除等 Profile 管理操作。

### 6.1 主要功能

#### 6.1.1 Profile 订购

Profile 订购是远程管理平台根据 MNO 提供的数据生成个性化数据以及生成 Profile 的过程。MNO



向远程管理平台提供的数据可以包括但不限于：

- 生成 Profile 的数量；
- IMSI 值或者范围；
- ICCID 的值或者范围。

除此之外，MNO 也可能提供 eUICC 的相关信息，如 eUICC ID。ICCID 的值或者范围也可以由远程管理平台产生。

#### 6.1.2 个性化数据生成

这个过程包括根据 MNO 提供的数据在一个安全环境中生成信任状和密钥值，如 NAC, PINs, OTA 密钥, Profile 下载凭证等。

#### 6.1.3 Profile 生成

Profile 生成是远程管理平台根据 MNO 提供的数据以及远程管理平台产生的个性化数据，按照标准的 Profile 格式，生成 Profile 的过程。远程管理平台生成的 Profile 可以下载并安装到任何遵从本规范的 eUICC 中。

#### 6.1.4 Profile 下载

远程管理平台可以根据 MNO 或者用户请求，将其生成的 Profile 传送到 eUICC 中。由于远程管理平台和 eUICC 之间没有实际的物理接口，远程管理平台需要建立到 eUICC 的传输通道来下载 Profile。

#### 6.1.5 Profile 安装

eUICC 将下载的 Profile 安装为可执行的应用和文件系统，这一过程包括为 Profile 分配资源以及注册相关参数。

Profile 安装通常和 Profile 下载同时进行，成功安装的 Profile 进入去激活状态。

#### 6.1.6 Profile 激活

根据 MNO 或用户请求，远程管理平台将 eUICC 上当前处于去激活状态的 Profile 激活，以使 Profile 中的文件和应用可以通过终端和 eUICC 之间的接口进行选择。

#### 6.1.7 Profile 去激活

根据 MNO 或用户请求，远程管理平台将 eUICC 上当前处于激活状态的 Profile 去激活，以使 Profile 中的文件和应用不可以通过终端和 eUICC 之间的接口选择。

#### 6.1.8 Profile 删除

根据 MNO 或用户请求，远程管理平台将 eUICC 上当前处于去激活状态的 Profile 删除，释放 Profile 占用的资源。

#### 6.1.9 安全功能

对 Profile 的下载、安装、激活、去激活和删除等操作需要进行认证、授权、完整性和机密性保护。远程管理平台需要和 eUICC 进行双向认证，拥有 Profile 下载、安装、激活、去激活和删除等的授权信息，并且能和 eUICC 进行密钥协商或密钥传输，生成用于保护 Profile 管理操作和安全通信的密钥。

#### 6.1.10 策略规则设置

策略规则设置是指 MNO 和远程管理平台对特定命令的执行条件或 Profile 管理的相关操作进行设置。策略规则是定义策略执行的动作和条件。

#### 6.1.11 策略控制



策略控制是指远程管理平台根据存储的策略规则对 eUICC 的管理操作进行控制, 或验证 MNO 的策略规则是否被正确执行。

## 6.2 接口要求

### 6.2.1 接口概述

eUICC 远程管理平台的相关接口如图 2 所示。

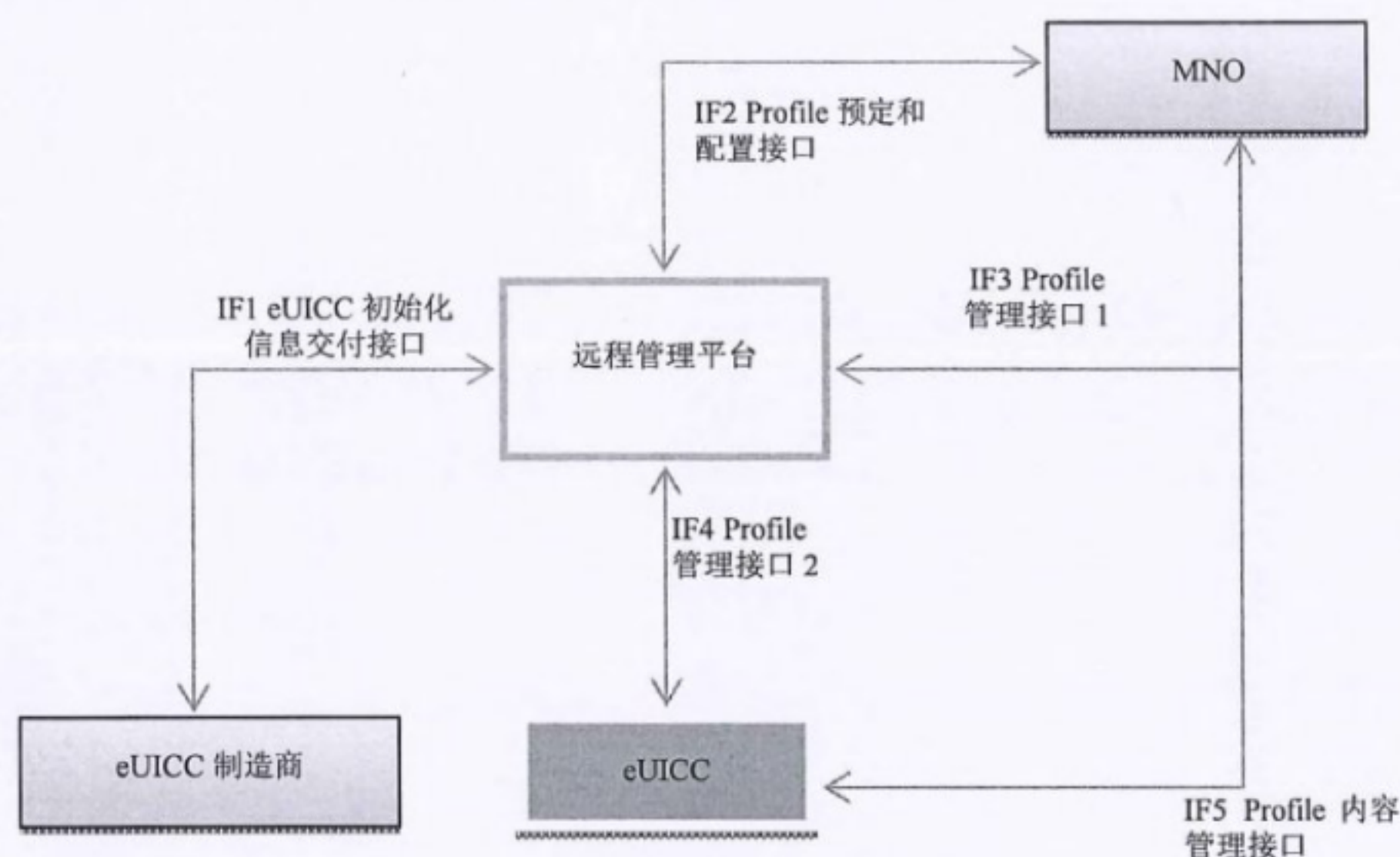


图 2 eUICC 远程管理平台接口

### 6.2.2 eUICC 初始化信息交付接口 (eUICC 制造商—远程管理平台)

该接口是 eUICC 制造商和远程管理平台之间的接口。在实际部署和应用过程中, 该接口可根据实际情况进行选择。对于新的 eUICC, 在 eUICC 预订时 eUICC 制造商已知将来的远程管理平台, eUICC 制造商将 eUICC 信息、eUICC 管理和 Profile 管理的信任状安全传递至远程管理平台; 或者对于 eUICC 管理中基于 PKI 的证书认证, 双方没有实际信息传输, 但是都需要加载共同信任的 root CA 的证书和公钥。根据预加载配置信息的需要, 远程管理平台将 Profile 安全传递至 eUICC 制造商。

### 6.2.3 Profile 预定和配置接口(MNO-远程管理平台)

该接口是 MNO 和远程管理平台之间的接口。该接口主要用于 Profile 的预定。MNO 首先向远程管理平台发起 Profile 预定请求, 远程管理平台按照 MNO 提供的输入生成并准备被预定的 Profile。

该接口主要用于交换以下信息:

- 来自于 MNO (合法的网络接入签约的发行商) 的包含为有效用户生成一组信任状的足够信息的请求;
- 和 NAA 相关的算法和参数;
- Profile 中的其他数据和应用;
- Profile 中的策略规则;
- 将要接收生成的 Profile 的远程管理平台的详细信息。

### 6.2.4 Profile 管理接口 1 (MNO—远程管理平台)

该接口是 MNO 和远程管理平台之间的接口。

远程管理平台接收 MNO 发送的以下信息:



- MNO 的 Profile 管理命令/指令；
- MNO 的策略控制和执行的命令/指令。
- 远程管理平台向 MNO 提供以下信息：
  - 准备配置 Profile 的目标 eUICC 的相关信息；
  - 来自于 MNO 的 Profile 管理命令/指令的接收/响应；
  - 来自于 MNO 的策略控制和执行命令/指令的接收/响应。

#### 6.2.5 Profile 管理接口 2（远程管理平台--eUICC）

该接口是远程管理平台和 eUICC 之间的接口。该接口用于 Profile 的下载和安装, Profile 激活, Profile 去激活, Profile 删除等。

#### 6.2.6 Profile 内容管理接口（MNO--eUICC）

该接口是 MNO 和 eUICC 之间的接口, 主要用于 MNO 对 eUICC 上的当前激活的 MNO 的 Profile 进行内容管理。

### 6.3 业务流程

#### 6.3.1 Profile 订购

在 eUICC 中, Profile 代表了现有 UICC 的一切功能性内容。与现有 UICC 类似, 仍由 MNO 负责发起 Profile 的订购。不同的是, 不会生产物理形态的 UICC 卡, 而是以 Profile 的方式保存在远程管理平台中。

注: 现有 UICC 订购的流程和接口是非标准化的, 即不同的 MNO 之间可能不同。

Profile 订购的业务流程如图 3 所示。

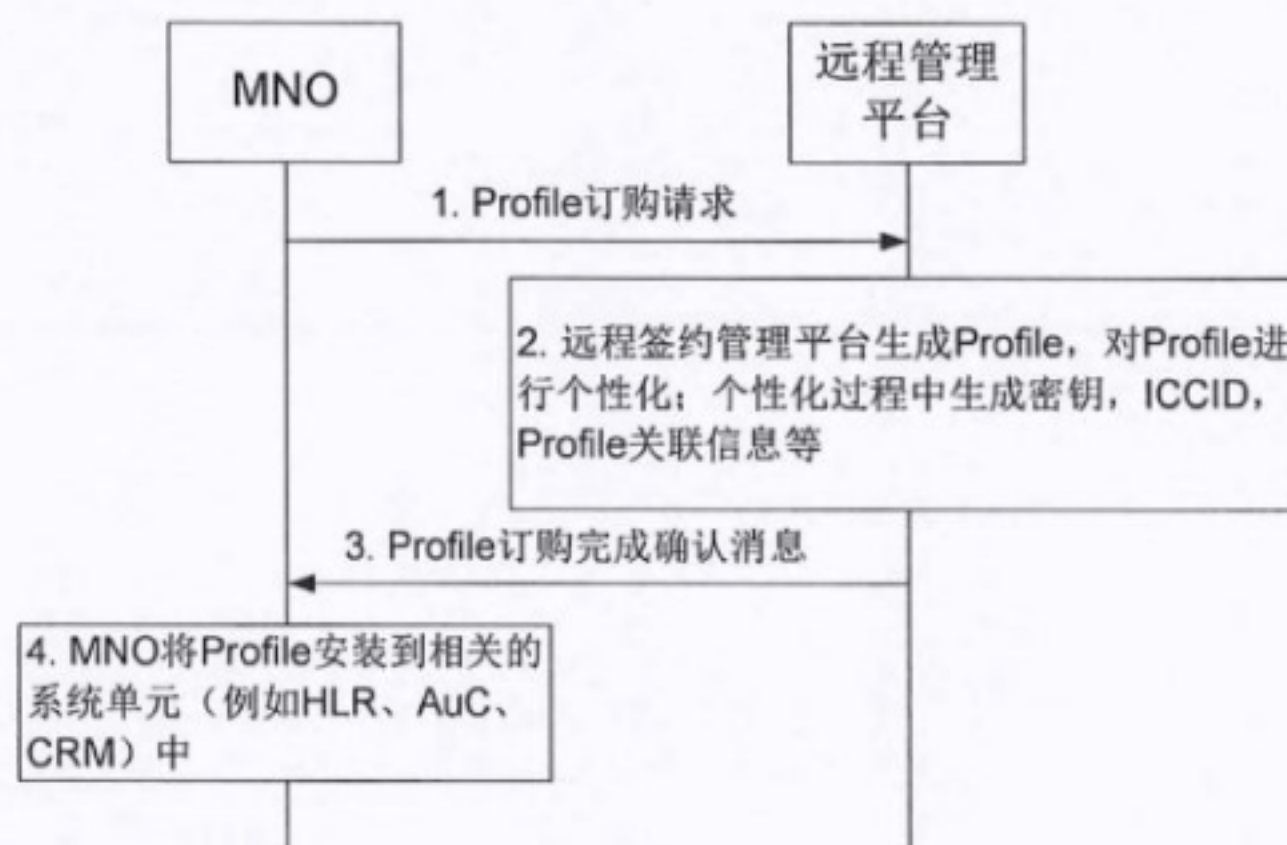


图 3 Profile 订购流程

流程执行前的准备: MNO 和远程管理平台之间针对 Profile 的定义、测试等方面达成一致, 而且 MNO 需要一定数量的可以在 eUICC 上使用的 Profile。

图 3 所示的流程步骤说明如下:

步骤1) MNO 向指定的远程管理平台发送订购请求。订单中包含生产 Profile 所需的数据, 例如该 MNO 的 Profile 规范, 订购数量, IMSI 清单 (或者起始 IMSI 和 IMSI 范围)。策略规则的内容定义或者 Profile 关联指示也可以是订单的一部分。

步骤2) 远程管理平台开始生成 Profile, 即使用从 MNO 收到的数据对 Profile 进行个性化。远程管理平台还可以在个性化过程生成其他的数据, 例如密钥或 ICCID。同时, 远程管理平台也生成并保存每个



Profile 的下载凭证（如随机产生的全球唯一的序列码等），用于授权 Profile 的下载请求。如果订单中包括 Profile 关联指示，远程管理平台需要生成 Profile 关联信息，即彼此关联的 Profile 标识。生成的 Profile 被保存在远程管理平台中。

步骤3) 远程管理平台向 MNO 发送 Profile 订购完成确认消息，其中包括所有需要在将 Profile 注册到 MNO 后台系统时用到的数据，其中可以含有 Profile 关联信息。每个 Profile 都能通过 ICCID 被唯一标识。

步骤4) MNO 将 Profile 安装到相关的系统单元中，例如 HLR、AuC、CRM。这些步骤与现有 UICC 注册没有区别。

流程执行后的状态：订单中指定数量的 Profile 准备就绪，随时可以下载。MNO 获得了相关运营商证书。

注：生成一个 Profile 的数据哪些由 MNO 提供，哪些由远程管理平台产生，需要进一步研究。

### 6.3.2 Profile 下载和安装

当远程管理平台收到 Profile 下载请求时，首先需要在 eUICC 上创建一个用于存储 Profile 的容器。然后建立远程管理平台和 eUICC 之间保护 Profile 内容所需的加密密钥，之后远程管理平台将 Profile 下载到 eUICC 中。

Profile 的下载可以由移动运营商（MNO）发起，也可以由用户（通过 eUICC）发起。Profile 的下载也可以提前在网络侧做一些离线处理操作，如 Profile 生成和加密等。Profile 在线下载和安装的具体流程如图 4 所示。

图 4 所示范的流程步骤说明如下：

步骤1) 发起者向远程管理平台发送 Profile 下载请求，请求远程管理平台将 Profile 下载到 eUICC 中，下载请求中包括 eUICC 标识（eID）、Profile 标识（ICCID）等。当发起者为订购该 Profile 的 MNO 时，下载请求中还包括远程管理平台 ID 或者远程管理平台地址等；当发起者为用户时，用户将 Profile 下载凭证以及远程管理平台 ID 或远程管理平台地址输入 eUICC，由 eUICC 向远程管理平台发送 Profile 下载请求。

步骤2) 远程管理平台验证 Profile 下载请求。当发起者为 MNO 时，远程管理平台验证该 Profile 是否为该 MNO 所有，若是则允许 Profile 下载；当发起者为用户时，远程管理平台将验证 Profile 下载请求中携带的 Profile 下载凭证是否和远程管理平台中保存的凭证一致，若一致，则根据 ICCID 获得请求下载的 Profile。

步骤3) 远程管理平台根据 eID 获取 eUICC 信息集（EIS），包括 eUICC 中已有的 Profile 信息以及 eUICC 的物理状态，如可用存储等，判断该 eUICC 是否可以下载该 ICCID 对应的 Profile，若该 eUICC 可以下载该 Profile，则远程管理平台判断是否可以在该 eUICC 中创建存储容器。

步骤4) 若验证通过，则远程管理平台数据路由和 eUICC 进行双向认证，建立到 eUICC 的安全链接，向 eUICC 发送创建存储容器请求。

步骤5) eUICC 根据请求创建存储容器。

步骤6) eUICC 向远程管理平台发送创建存储容器响应。

步骤7) 远程管理平台数据准备和 eUICC 双向认证，认证通过后在远程管理平台和 eUICC 之间建立 Profile 安全保护的密钥，密钥建立流程可以采用改进的 / 基于 GPCS（全球平台智能卡技术规范）中基于 PKI 的密钥协商机制或者密钥传输机制。



步骤8) 远程管理平台使用上述步中建立的安全密钥对需要下载的 Profile 进行加密和完整性保护。

步骤9) 远程管理平台将加密后的 Profile 发送给 eUICC。

步骤10) eUICC 验证数据的安全性后, 进行 Profile 的解密和安装。

步骤11) eUICC 向远程管理平台发送 Profile 下载完成消息, 其确认消息可以被远程管理平台的数据路由和数据准备功能分别认证, 指示 Profile 已经被成功安装到 eUICC。

步骤12) 远程管理平台更新 EIS。

步骤13) 如果发起者为 MNO, 则远程管理平台向发起者发送 Profile 下载和安装成功消息。

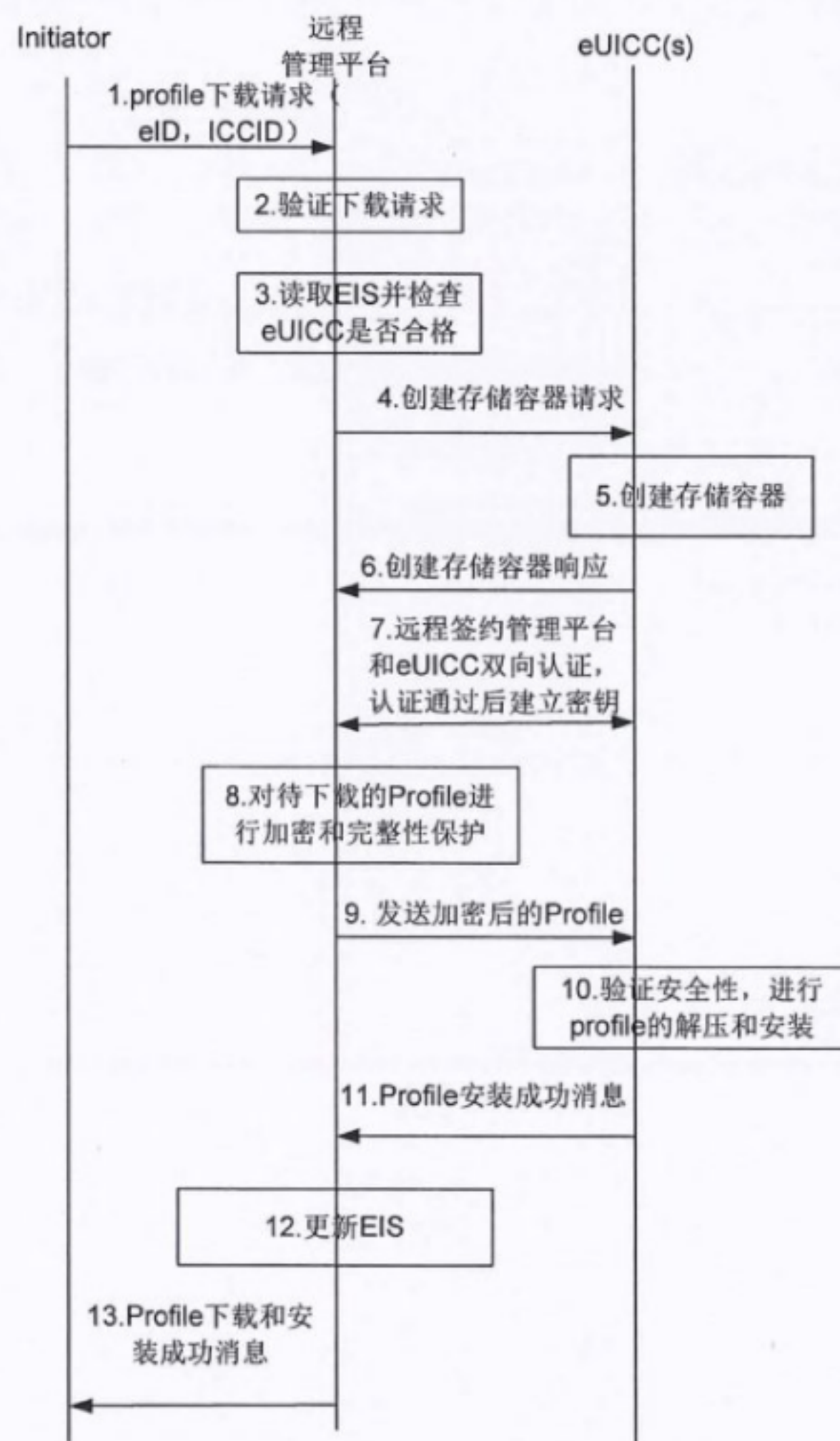


图4 Profile 下载和安装流程

### 6.3.3 Profile 激活

MNO 和远程管理平台之间的 Profile 激活流程用于激活一个之前已经下载并安装到 eUICC 上的 Profile。流程由待激活 Profile 的归属 MNO 发起, 该流程也可以由生态系统中的其他角色作为发起者。Profile 激活流程如图 5 所示。



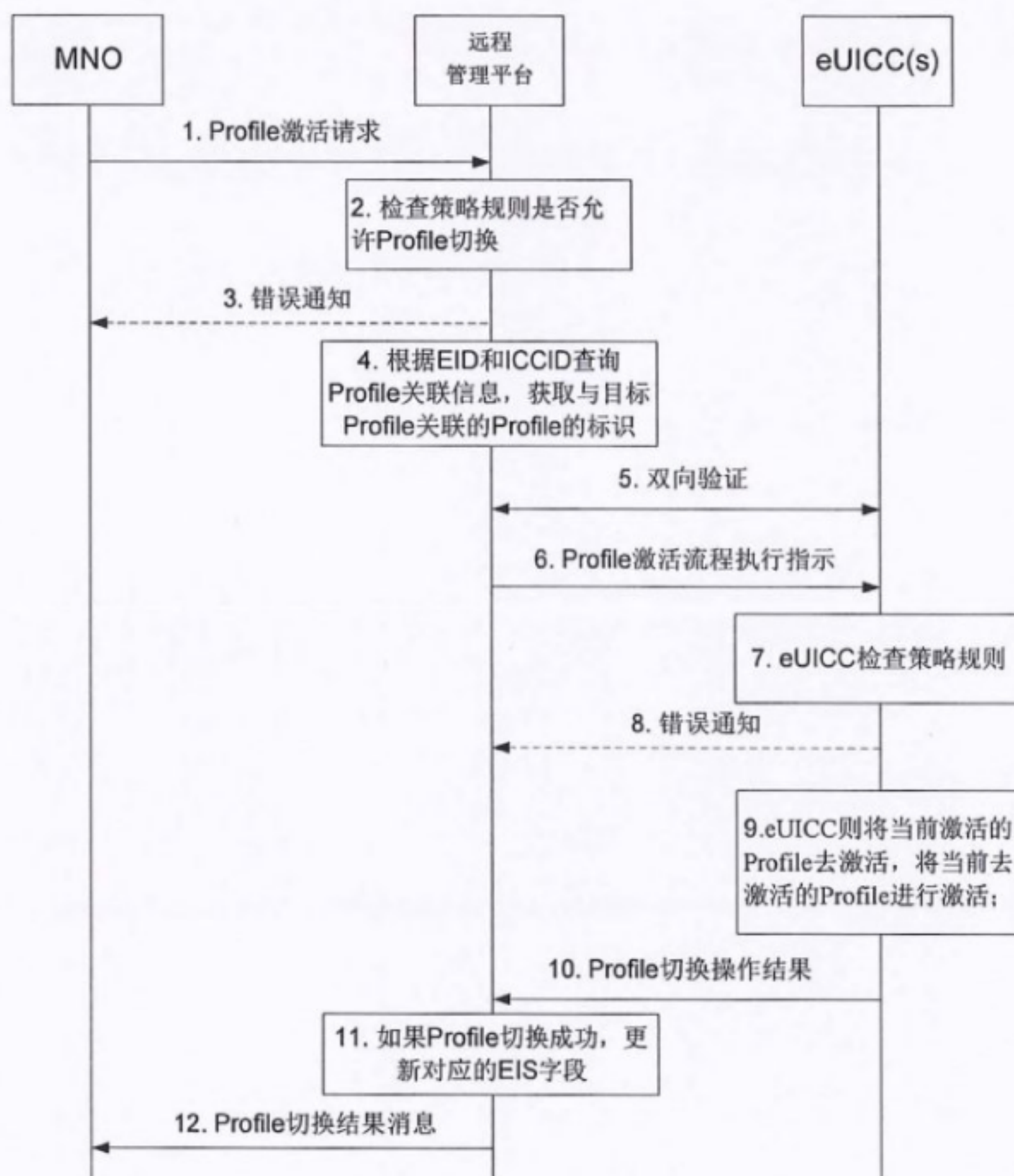


图5 Profile 激活流程

流程执行前的准备:

- a) 目标 Profile 在目标 eUICC 上处于去激活状态, 该 eUICC 上有另外一个 Profile 处于激活状态;
- b) 与目标 Profile 相关的签约已经在 MNO 网络中激活;
- c) 目标 eUICC 的 EID、负责管理目标 Profile 的远程管理平台的 ID 以及目标 Profile 的 ICCID 对 MNO 都是已知的。如发起者为生态系统中的其他角色, 发起所需要的信息可能不同。

图5所示的流程步骤说明如下:

步骤1) MNO 向远程管理平台发送 Profile 激活请求, 请求消息中携带目标 eUICC 的 EID 以及目标 Profile 的 ICCID;

步骤2) 远程管理平台检查当前与处于激活状态的 Profile 和目标 Profile 相关的策略规则是否允许进行 Profile 切换;

步骤3) 如果步骤2中的策略检测出现冲突, 远程管理平台会终止流程, 并告知相关的 MNO;

步骤4) 如果步骤2中的策略检测通过, 远程管理平台根据 EID 和 ICCID 查询对应 EIS 中的 Profile 关联信息, 获取与目标 Profile 关联的 Profile 的标识;

步骤5) 远程管理平台和 eUICC 之间进行必要的双向验证;

步骤6) 远程管理平台指示承载目标 Profile 的 eUICC 和承载与目标 Profile 关联的 Profile 的 eUICC 执行目标 Profile 及其关联的 Profile 的激活流程, 指示消息中携带目标 Profile 及其关联的 Profile 各自的



ID;

步骤7) eUICC 检查当前正在执行的所有策略规则和与目标 Profile 相关的策略规则;

步骤8) 如果步骤 7 中的策略检测出现冲突, eUICC 将终止流程并告知远程管理平台;

步骤9) 如果步骤 7 中的策略检测不出现冲突, eUICC 则将当前激活的 Profile 去激活, 将当前去激活的目标 Profile 进行激活;

步骤10) eUICC 向远程管理平台发送 Profile 切换操作结果;

步骤11) 如果 Profile 切换操作成功, 远程管理平台更新对应的 EIS 字段, 将目标 Profile 的状态更新为已激活, 将原来处于激活状态的 Profile 的状态更新为去激活;

步骤12) 远程管理平台向目标 Profile 所属 MNO 和原来处于激活状态的 Profile 的所属 MNO 返回 Profile 切换结果消息, 这些消息中包含相应 Profile 的 EID 和 ICCID。

流程执行后的状态: 目标 Profile 及其关联的 Profile 在 eUICC 上处于激活状态, 之前处于激活状态的 Profile 处于去激活状态, 远程管理平台中的 EIS 对应字段得到更新。

#### 6.3.4 Profile 去激活

Profile 去激活流程如图 6 所示。

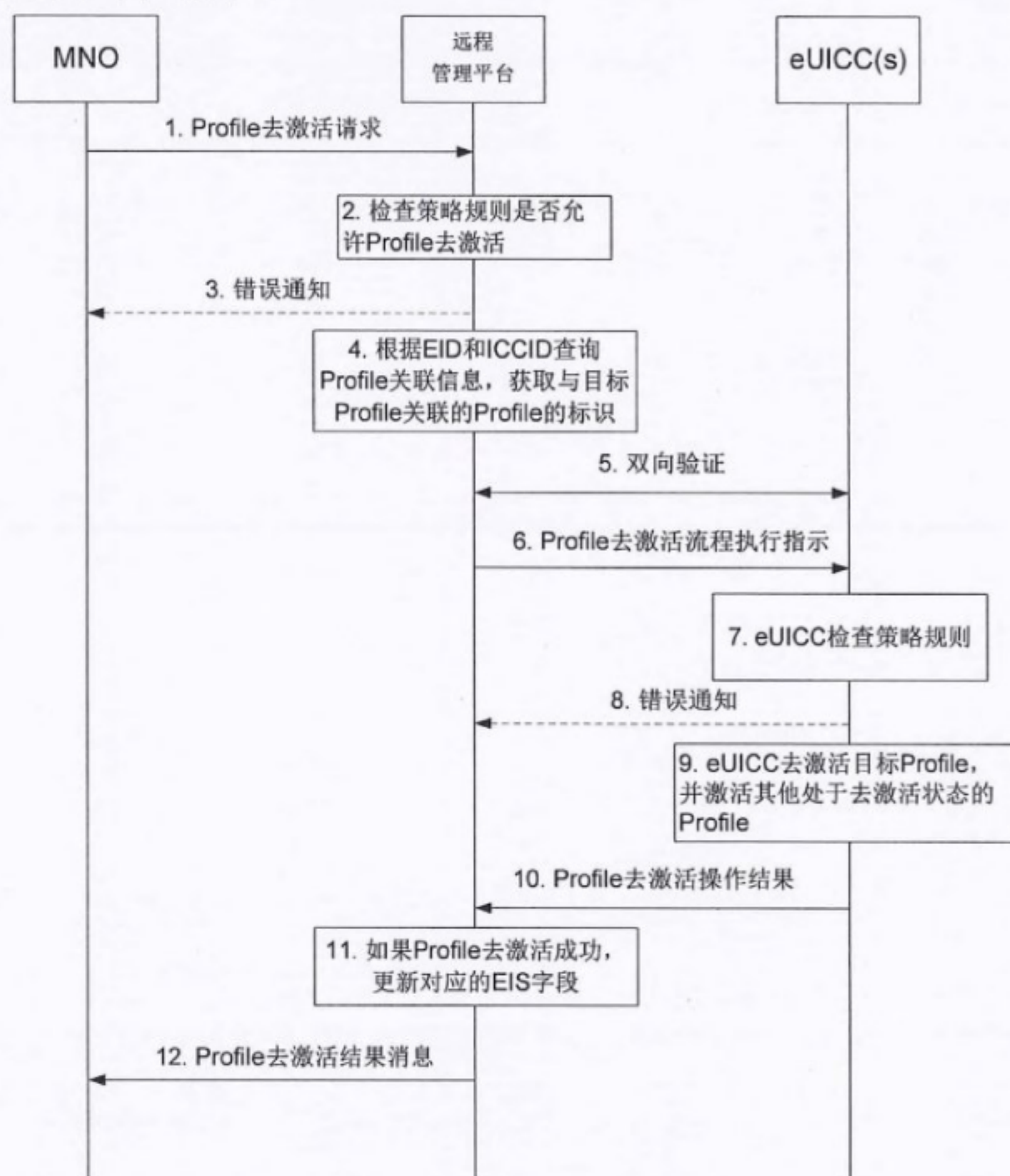


图 6 Profile 去激活流程

流程执行前的准备: 目标 Profile 在目标 eUICC 上处于激活状态。

图 6 所示的流程步骤说明如下:



步骤1) MNO 向远程管理平台发送 Profile 去激活请求,请求消息中携带目标 eUICC 的 EID 以及目标 Profile 的 ICCID;

步骤2) 远程管理平台检查与目标 Profile 相关的策略规则是否允许去激活;

步骤3) 如果步骤 3 中的策略检测出现冲突,远程管理平台将终止流程,并向相关的 MNO 发送错误消息;

步骤4) 如果步骤 3 中的策略检测通过,远程管理平台根据 EID 和 ICCID 查询对应 EIS 中的 Profile 关联信息,获取与目标 Profile 关联的 Profile 的标识;

步骤5) 远程管理平台和 eUICC 之间进行必要的双向验证;

步骤6) 远程管理平台指示承载目标 Profile 的 eUICC 和承载与目标 Profile 关联的 Profile 的 eUICC 执行目标 Profile 及其关联的 Profile 的去激活流程,并激活 eUICC 上其他处于去激活状态的 Profile;

步骤7) eUICC 检查当前处于激活状态的 Profile 的策略规则;

步骤8) 如果步骤 8 中的策略检测出现冲突,eUICC 将终止流程并告知远程管理平台;

步骤9) 如果检测通过,eUICC 将去激活目标 Profile,并激活其他处于去激活状态的 Profile;

步骤10) eUICC 向远程管理平台发送 Profile 去激活操作结果;

步骤11) 如果去激活操作成功,远程管理平台会更新对应的 EIS 字段,将目标 Profile 的状态更新为去激活;

步骤12) 远程管理平台向相关的 MNO 发送 Profile 去激活结果消息,消息中携带相应 Profile 的 EID 和 ICCID。

流程执行后的状态:目标 Profile 及其关联的 Profile 在 eUICC 上处于去激活状态,且其他 Profile 处于激活状态,远程管理平台中的 EIS 对应字段得到更新。

### 6.3.5 Profile 删除

Profile 删除流程如图 7 所示。

流程执行前的准备:MNO 决定将目标 Profile 从目标 eUICC 上永久性删除。

图 7 所示的流程步骤说明如下:

步骤1) MNO 向远程管理平台发送 Profile 删除请求,请求消息中携带目标 eUICC 的 EID 和目标 Profile 的 ICCID;

步骤2) 远程管理平台检测目标 Profile 的策略规则是否允许删除;

步骤3) 如果步骤 2 中的策略检测出现冲突,远程管理平台将终止流程并告知相关的 MNO;

步骤4) 如果目标 Profile 处于激活状态,远程管理平台发起 Profile 去激活流程,参考 6.3.4 中的流程步骤;

步骤5) 远程管理平台根据 EID 和 ICCID 查询对应 EIS 中的 Profile 关联信息,获取与目标 Profile 关联的 Profile 的标识;

步骤6) 远程管理平台和 eUICC 之间进行必要的双向验证;

步骤7) 远程管理平台指示承载目标 Profile 的 eUICC 和承载与目标 Profile 关联的 Profile 的 eUICC 执行目标 Profile 及其关联的 Profile 的删除流程,指示消息中携带目标 Profile 及其关联的 Profile 各自的 ID;

步骤8) eUICC 检查 Profile 相关的策略规则;



步骤9) 如果步骤 8 中的策略检测出现冲突, eUICC 将终止流程, 并告知远程管理平台;

步骤10) 如果步骤 8 中的策略检测通过, eUICC 将删除 Profile 以及对应的存储容器;

步骤11) eUICC 向远程管理平台返回 Profile 删除操作结果;

步骤12) 远程管理平台更新对应的 EIS 字段;

步骤13) 远程管理平台向请求发起方 MNO 返回 Profile 删除操作结果。

流程执行后的状态: 目标 Profile 及其关联的 Profile 被永久性地从 eUICC 上删除, 远程管理平台中的 EIS 相应字段得到更新。

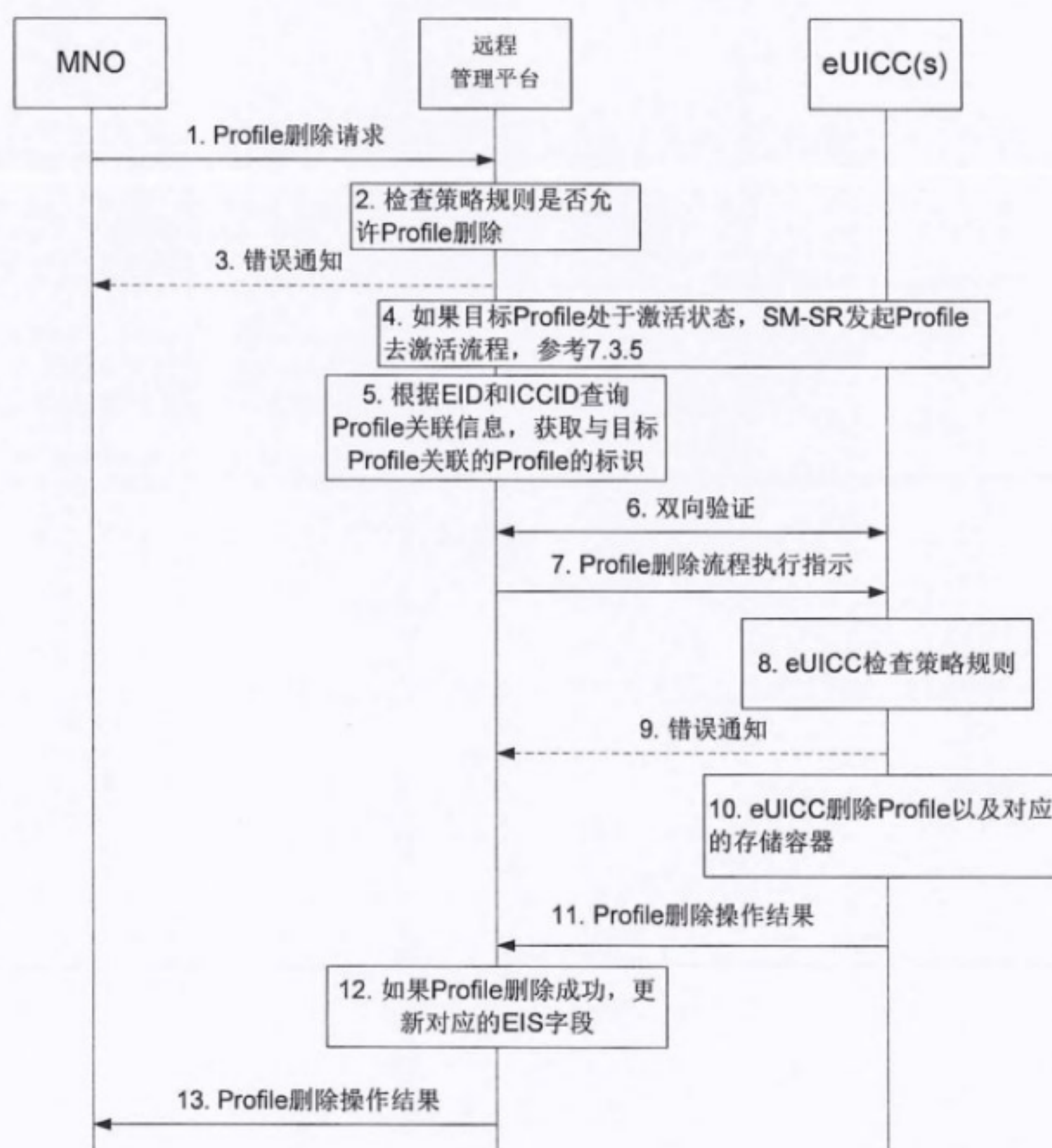


图 7 Profile 删除流程

#### 6.4 Profile 定义

Profile 是一组提供服务的应用、文件和数据, 例如 MNO 的 NAA 文件和信任状。任何合法的远程管理平台生成的 Profile 都可以以标准化的描述格式下载并安装到任何符合本规范的 eUICC 中。

成功下载和安装一个 Profile 后, 该 Profile 即进入去激活 (Disable) 状态, 之后可以进入激活 (Enable) 状态, 并可以在 Disable 状态和 Enable 状态间转换。为了 eUICC 操作稳定性, 只有 Disable 状态的 Profile 可以执行删除 (Delete) 操作。

Profile 主要包括以下几方面的数据:

- 相关技术规范中定义的应用程序和文件; (3GPP TS 31.102, 3GPP TS 31.103 和 ETSI TS 102 221)
- 网络接入应用程序 (NAA) 所需的密钥和算法参数 (例如 Milenage: Opc, K, ri, ci 等);



- OTA 远程程序管理 / 远程文件管理 (RAM/RFM) 所需的密钥和参数 (ETSI TS 102 225, ETSI TS 102 226);

- 策略规则。

## 6.5 策略控制 (PCF) 功能

### 6.5.1 策略规则管理

#### 6.5.1.1 概述

由于策略规则是与 Profile 相关的, 因此 MNO 需要通过执行自身设置的规则, 对策略进行控制。

策略控制通常由单一的 MNO 策略管控。策略也可以包括多个子策略, 每个子策略由不同的实体执行。

策略规则包括但不仅限于如下两种:

- POL1----这些规则位于 Profile 内部, 由 eUICC 负责执行;
- POL2----这些规则由远程管理平台负责保存和执行。MNO 可以将 POL2 直接发送给远程管理平台或者附加到 Profile 中, 再转发至远程管理平台。

注: 除了上述两种规则外, 还可能在 eUICC 上且 Profile 外存在策略规则, 该规则同 POL1 一起由 eUICC 负责执行。

POL1 和 POL2 代表了在不同实体上执行的通用 MNO 策略。POL1 和 POL2 共同代表了 MNO 和用户之间针对相应 Profile 的合同信息。

本条中, 所有命令均使用 Update; 在第一个示例中, 当建立一条新规则时, 视为 Update 的一种特例。

#### 6.5.1.2 远程管理平台策略规则管理工具

远程管理平台包括一个策略规则管理工具, 主要完成以下任务:

- 根据 MNO 的请求更新 POL2。远程管理平台根据 MNO 提供的 Profile 内部数据来设置 POL2。在 Profile 安装成功后, 立即执行 POL2 中的规则, 并更新对应的 EIS。远程管理平台在管理某个 eUICC 时需要执行对应的 POL2 规则;

- 根据 MNO 的请求设置 POL1, 并将 POL1 嵌入到 Profile 中;
- 来自 MNO 的“Update POL2”命令, 并将该命令发送到远程管理平台来更新 EIS;
- 设置来自 MNO 的 POL2, 并将策略规则附加到 Profile 中, 之后将该 Profile 传输到远程管理平台。

#### 6.5.1.3 eUICC 策略规则管理工具

eUICC 包括一个策略规则管理工具, 读取已安装的 Profile 内的 POL1 规则, 在 Profile 安装成功后立即执行 POL1 规则。根据 MNO 的请求读取或更新 POL1 (请求命令由 MNO 的专属 OTA 系统发送)。

#### 6.5.1.4 OTA 策略规则更新机制

MNO 通过 OTA 平台并向 eUICC 发起 POL1 更新命令。

### 6.5.2 策略控制机制

#### 6.5.2.1 概述

eUICC 中的策略控制机制包含但不限于:

- MNO 授权存储在 Profile 存储容器中的策略规则;
- 位于 eUICC 平台中负责执行策略规则的策略执行器。

#### 6.5.2.2 策略规则



在 Profile 管理操作时需要进行策略规则的检查, 这些策略规则会影响和这些策略规则相关联的 Profile 以及其他 Profile。

根据规则的种类, 策略规则可以在 eUICC 层面执行, 也可以在远程管理平台层面执行。只有 Profile 所有的 MNO 才能修改策略规则。在 eUICC 层面, 策略规则是 Profile 包的一部分, 被 eUICC 操作系统中的策略执行器执行。

MNO 可以通过 OTA 的方式更新 Profile 中的策略规则, 只有在 Profile 是激活状态的时候才能更新策略规则。

本标准定义的用于控制 eUICC 远程管理的策略执行机制应该允许公平竞争, 并符合相关监管法律。在执行策略控制功能时应该遵守以下原则:

- 参与的运营商不能滥用策略执行机制以任何方式来阻止或妨碍合理的 Profile 安装, 激活, 去激活以及删除等操作;
- 参与的运营商可以执行符合公平竞争和监管法律的策略规则。

POL1 和 POL2 的设置可以相同, 也可以不同。POL1 和 POL2 被不同的实体执行, 并被独立执行。MNO 可以选择如何设置 POL1 和 POL2, 如可以设置 POL1 为空。

#### 6.5.2.3 eUICC 策略规则执行功能

eUICC 策略规则执行器能够读取和执行 eUICC 上的所有 POL1。

#### 6.5.2.4 远程管理平台策略规则执行功能

远程管理平台策略规则执行器能够读取和执行与目标 eUICC 相关联的策略规则。

### 7 eUICC 远程管理安全要求

#### 7.1 安全等级和认证

##### 7.1.1 安全威胁

现有 UICC 卡不具备下载和转移签约关系的能力, 其没有获取或修改运营商敏感数据的安全风险, 这些数据是通过其他安全途径置入到 UICC 中。eUICC 远程管理应该包括一系列安全机制, 实现运营商签约关系和相关用户密钥的下载和转移, 可以预见该机制将面临严重的安全风险, 包括:

- 海量 M2M 设备的去激活: 木马、系统漏洞、恶意软件都可以在短时间内通过将 eUICC 状态转移为非连接状态, 从而实现海量物联网终端的去激活;
- 修改签约关系: 通过木马、恶意软件、硬件攻击实现对运营商敏感数据的修改, 计费、终端补贴、运营商优惠策略可能面临风险;
- 克隆: 通过木马、系统漏洞、恶意软件、硬件攻击等实现对运营商敏感数据的捕获或偷听, 并威胁终端用户和网络的交互;
- 隐私: 通过木马、系统漏洞、恶意软件、硬件攻击等实现对运营商敏感数据的捕获或偷听, 并威胁终端用户和网络的交互。

以上安全威胁将严重影响 eUICC 远程管理系统, 除了运营商敏感数据, M2M 设备网络连接性同样面临以上威胁, 并且可能会影响物联网关键应用。

##### 7.1.2 认证流程

eUICC 可以由通用认证评估 (Common Criteria evaluations) 实现认证。其中, Common Criteria (CC) 为



ISO标准,即ISO/IEC 15408,该标准被有认证能力、独立的实验室进行认证评估。CC认证主要由CCRA (Common Criteria Recognition Agreement) 的签约会员单位组织,CCRA包含26个国家。此外,目前SIM卡产业界已有10年以上的CC认证经验,其数百款安全模块已经经过了EAL4+以上的CC认证。此外,物联网应用可能有安全方面严格需求,CC认证可以被作为参考标准。目前关于智能抄表,智能抄表系统中网侧的保护文件其定义的目标安全级别为EAL4+。

为了保证eUICC远程管理避免木马、系统漏洞、恶意软件、硬件攻击,建议CC EAL4+为最低安全等级要求。因此对eUICC平台的认证可以符合CC EAL4+规范: EAL4的扩展版AVA\_VAN.5 及 ALC\_DVS.2 (在ISO/IEC 15408第3部分定义)。进一步, eUICC中新的保护文件 (Protection Profile, PP), 涉及到远程配置特性的部分需要定义, PP可以符合EAL4扩展版: AVA\_VAN.5 和ALC\_DVS.2。具体而言, eUICC新的PP, 其特性应该包括:

- eUICC PP 应该和现有 PP 兼容, 如 Java 卡 PP 或者 USIM PP;
- eUICC PP 需考虑运营商签约配置相关步骤和机制, 如管理初始证书 (OTA 及 OTI 证书) 涉及的步骤和机制。eUICC PP 主要涉及安全功能, 并且要考虑足够的通用性, 以便于适应于不同的技术和实施方法;
- eUICC 远程管理角色、环境应该在 eUICC PP 中描述 (角色: eUICC 卡商、设备商、签约管理者; 环境: eUICC 卡商及设备商生产地、销售者、终端用户)。在 eUICC PP 中对安全环境的需求主要针对 eUICC 卡商, 关于 eUICC R&D 及生产地点, eUICC 卡商主要负责其自己的生产、预配置、初始化阶段。其他关于安全环境、解决方案、处理流程的假设将由远程管理平台负责, eUICC 卡商负责文件的准备和下载。针对安全环境假设方法、解决方案、处理流程方法, 其主要由签约管理者及 eUICC 卡商负责文件的准备和下载。

eUICC需要保护的内容包括数据及信任状 (允许签约配置及数据配置), 相关配置数据仅在配置状态时为保护数据。当eUICC完成配置后, 其配置数据将不在eUICC 保护PP范围之内。eUICC配置数据包括:

- 配置数据: OTI 及 OTI 信任状; eUICC ID: eUICC 唯一标识, 在 eUICC 签约交换时唯一标识 eUICC; 日志及状态信息;
- 配置后信息: 运营商文件, 包括 MNO 信任状, 机密信息 (Ki, 鉴权算法, 加密参数等)。

### 7.1.3 初始个人化安全等级及流程

在 UICC 产业链中, 卡的安全主要由几个关键因素来保证:

- UICC 产品特性主要由运营商认证, 并且运营商执行针对所有产品的评估和审查;
- 一些运营商要求 UICC 产品经过一个正式的第三方安全认证, 如 CC 认证 (可选);
- 主流运营商要求 UICC 卡商涉及其数据管理的流程必须经过安全认证 (GSMA-SAS 认证)。

以上元素构成 UICC 卡商和运营商之间信任关系架构的组成部分。因此, eUICC 信任关系应建立在已有 UICC 信任关系架构上, 并扩展到 eUICC 供应链中。在此基础上, 需要一种适应于 eUICC 供应的认证机制, 其中包括引入新的参与者 (如远程管理平台) 对整体安全模型的影响。因此, eUICC 初始个人化的安全需求, 即预初始化、初始化阶段, 应该满足以下条件:

- 预初始化和初始化阶段应该在信任环境下实现;
- 信任环境的可信任性应该由一个针对 eUICC 卡商的认证, 例如扩展 SAS 认证机制认证, 其中认证应该包括数据准备流程、Key 管理、初始个性化, 并且和新的 PP 定义保持一致。



#### 7.1.4 远程配置安全等级及流程

在 eUICC 远程管理架构下，远程配置是一个关键特性，通过其可以实现 eUICC 生命周期远程管理。此外，eUICC 远程配置是针对已经完成初始配置的 eUICC。eUICC 远程配置的主要需求是要保证其至少实现和现有 UICC 配置流程相同的可靠性，现有 UICC 配置认证是由 UICC 卡商通过执行 SAS 认证实现。eUICC 远程配置应满足以下条件：

- 保证 eUICC 解决方案和现有基于 UICC 方案的兼容性；
- 保证和现有 OTA 方案兼容性；
- 尽量重用现有标准。

#### 7.1.5 实体间安全等级及认证

本条分析的安全认证适用于两个不同实体之间的接口和协议。

#### 7.1.6 远程管理平台和运营商间安全等级及认证

假设远程管理平台和运营商之间的通信安全等级至少和现有运营商和 UICC 卡商数据交换的安全等级相同。此外，远程管理平台和运营商之间的链接将由运营商通过一个可靠、私有的信道实现。其中，可靠信道将用来传送以下数据：

- 配置数据；
- 策略控制文件（PCF）。

此外，考虑到 eUICC 市场处于初步开拓阶段，远程管理平台将至少有两种商业模式：

- 运营商作为远程管理平台；
- 由第三方作为远程管理平台。

#### 7.1.7 eUICC 与 eUICC 卡商间安全等级及认证

eUICC 卡商在 eUICC 产业链中主要负责的工作有：

- eUICC 更新管理；
- eUICC 初始化；
- eUICC 首次配置；
- eUICC OS 修订；
- 运营商私有认证算法更新，这是基于 eUICC 不可移除性，以及 M2M 市场特性的需求决定的。

根据上述 eUICC 卡商工作，eUICC 与 eUICC 卡商之间应该具备如下安全机制：

- eUICC 更新完整性检测，以防止非 eUICC 卡商更新的安装；
- 机密性机制，以确保即使 eUICC 更新被第三方非法获取，也不能解密；
- 因 eUICC 数据的敏感性，要求 eUICC 卡商提供 eUICC 更新功能，并且 eUICC 和 eUICC 卡商之间通过安全算法实现端到端管理。

#### 7.1.8 远程管理平台与 eUICC 卡商间安全等级及认证

在 eUICC 远程管理架构中，远程管理平台主要负责保障运营商 PCF 策略执行，以及建立和 eUICC 之间的通信。其中，远程管理平台负责建立一条和 eUICC 之间安全的通信链路（通过使用初始信任状实现远程接入）。根据远程管理平台和运营商之间关系的不同，远程管理平台的功能也不尽相同。因此对远程管理平台及 eUICC 卡商间应实现不同的认证等级。

### 7.2 安全通信



eUICC 远程管理平台的安全通信要求主要包括:

- 在远程管理系统中应实现端到端的加密。
- eUICC 与终端间加密, 防治恶意软件伪造通信, 影响 eUICC 的工作
- eUICC 与远程管理平台间加密, 防止传输的信息被监听。
- 远程管理平台与运营商之间应加密, 保证远程管理平台不能获取用户签约信息的明文。

## 8 无运营商网络覆盖情况下技术要求

### 8.1 场景

现有的eUICC的远程管理技术中, 物联网设备的合约期满后, 可更换运营商。更换运营商实际上是用户签约信息重新配置的过程, 通常用户签约信息包括Ki, IMSI, ICCID等。并使用OTA方法重新配置新的签约信息, 即物联网设备通过当前运营商网络下载新运营商的签约信息, 然后用新的签约信息代替原有签约信息。

在已开展的工作中, 一个基本的假设是eUICC所处环境的运营商网络情况良好。但是, 因为某些特殊情况, 如基站故障、设备移动到地下车库、山区等网络覆盖较差的环境, 设备存在较大可能性失去当前运营商的网络。

eUICC远程管理系统需要相应的机制能够切换到下一个可用的运营商网络, 以保证业务的连续性。

失去当前网络覆盖的场景主要有以下两种:

- 漫游地的信号很差或者 VPLMN 无漫游协议:

对一些典型的工业场景, 漫游是常见的需求。例如, 一辆在亚洲制造的汽车, 被运往德国, 然后移动到某些无当前MNO的区域或者漫游至合作伙伴的网络。

• 当前网络故障: 由于基站的故障等, eUICC 设备失去了当前网络的信号。该场景有如下三种不同的情况:

- 由设备导致的失去网络连接, 而不是由eUICC用户发起的;
- eUICC无法使用当前的网络服务, 必须寻找其他可用的运营商网络;
- 如果先前的网络服务变得可用, eUICC一般切换回去。

### 8.2 切换类型和规则

根据运营商服务的类型和资费, 我们可以将eUICC切换分为不同的类型:

- 实时/非实时 eUICC 切换;
- 有/没有运营商补贴的 eUICC 切换。

eUICC设备失去网络连接的时候, 可参考如下的切换规则:

- 有实时性服务要求的 eUICC, 应该立即切换至其他的运营商;
- 非实时性服务要求的 eUICC, 应该参考本地的 PCF 再决定是否切换;
- 含有运营商补贴的 eUICC, 当先前的服务网络可用的时候, 应该切换回先前的网络;
- 没有运营商补贴的 eUICC, 应该参考本地的 PCF 再决定是否切换。

在任何情况下, 如果状态改变的Profile内有相关的策略描述, eUICC应该将切换上下文(如切换时间、位置、当前连接的信息等)上报至对应的远程管理平台。

### 8.3 技术要求



8.3.1 总体要求

无运营商网络覆盖情况对现有的架构和安全的影响因素见表2。

表 2 无运营商网络覆盖的影响因素

	影响因素	描述
架构	角色	eUICC 与远程管理平台进行交互来决定是否从当前网络切换到另一个服务网络
	功能	远程管理平台或 eUICC 参考 PCF 来选择候选网络并实现转换流程
	接口	设备可以使用当前已有的 eUICC 与终端的接口和终端与远程管理平台的接口来传输网络覆盖信息并上报切换信息
安全	PCF	eUICC 应该存储 PCF 规则。此外，为了避免 PCF 文件的修改，需要进行加密和完整性验证，还有的攻击者的伪装和窃听
	切换机制	应该指定两个切换机制：一个是使用配置 Profile。另一种是使用紧急呼叫服务。如果使用紧急呼叫服务，eUICC 可以使用 IMSI 或 EID 来接入网络。网络因此应该有更多的安全考虑，避免滥用紧急呼叫服务
	eUICC-终端的接口	这个接口需要用于传输信号测试结果，并且随后的终端-网络接口用于传输切换报告。应该引入新的安全机制来保证 eUICC 与 M2M 设备之间和 M2M 设备与远程管理平台之间的通信安全

8.3.2 eUICC 要求

无运营商网络覆盖情况下对 eUICC 的技术要求主要包括：

- eUICC 可以支持检测和阻止频繁攻击切换的能力；
- 应该有一种机制来执行预定义的 Profile 切换。

8.3.3 终端要求

终端设备应该将网络连接信息报告给eUICC和远程管理平台。

8.3.4 信息的真实性和完整性的要求

eUICC和远程管理平台应该核实设备产生的无网络覆盖的通信消息的真实性和完整性。

8.3.5 远程管理平台要求

无运营商网络覆盖情况下对远程管理平台的技术要求主要包括：

- 远程管理平台应该获取和分析来自 eUICC 设备的异常报告；
- 当先前的服务网络可用的时候，远程管理平台应支持 eUICC 切换回先前的网络。



中华人民共和国  
通信行业标准  
嵌入式通用集成电路卡 (eUICC)  
远程管理平台技术要求 (第一阶段)  
YD/T 2926-2015

\*

人民邮电出版社出版发行  
北京市丰台区成寿寺路 11 号邮电出版大厦  
邮政编码: 100164  
北京康利胶印厂印刷  
版权所有 不得翻印

\*

开本: 880×1230 1/16 2016 年 1 月第 1 版  
印张: 2 2016 年 1 月北京第 1 次印刷  
字数: 46 千字

15115 • 855

定价: 20 元

本书如有印装质量问题, 请与本社联系 电话: (010)81055492