



eSIM 及其远程配置技术与应用

黄海昆

(中国电信股份有限公司上海研究院,上海 200122)

摘要: 由于恶劣环境的影响,车载设备越来越多地使用嵌入式 SIM 卡,同时对其远程配置也提出了一定的要求。从 eSIM 的业务需求和技术发展进行分析,并对使用移动通信网络的车载通信设备应用 eSIM 及其远程配置的技术架构和商务模式进行探讨。

关键词: eSIM;车联网;空中写号

中图分类号: TN929.53

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2016245

Technology and business of remote provisioning for embedded SIM

HUANG Haikun

Shanghai Research Institute of China Telecom Co., Ltd., Shanghai 200122, China

Abstract: Due to the harsh usage environment, embedded SIM (eSIM) card are required, and its remote provisioning is needed correspondingly. Business requirements and technological development of eSIM were analyzed. The technical architecture and business mode of remote provisioning for eSIM were also discussed.

Key words: eSIM, internet of vehicles network, OTA

1 引言

大部分物联网应用终端都使用移动通信网进行数据通信,特别是汽车等高速移动的载体,更依赖高带宽、低时延的移动网络。被各运营商普遍使用的 SIM 卡作为移动通信的用户鉴权信息载体,是移动通信终端的必备组件,然而传统的插入式(plug-in)SIM 卡难以满足经常工作在极限温度和剧烈震动环境中的车载设备需求,嵌入式 SIM 卡得到了越来越多的应用。eSIM(embedded SIM)是将移动运营商的客户识别信息写入嵌入式通用集成电路卡(embedded universal integrated circuit card,eUICC),并固定在嵌入终端设备上,不能随便拔出和替换,用户无法直接进行更换,

需要后期远程对码号资源进行管理,从而在车辆跨地域销售或行驶时能够切换不同运营商的移动通信网络。

很多 eSIM 卡的制卡商制定了基于 eSIM 的远程码号管理系统,为了能在全球更多的运营商之间建立兼容性更强的远程写号系统,国际标准也在陆续制定,目前这方面的标准主要有:M2M 智能卡(物理和逻辑特征)^[1]、eUICC 卡的使用场景及需求^[2]、嵌入式 UICC 远程配置技术规范^[3]、SIM 卡远程配置技术规范^[4]。

2 eSIM 概念及发展演进

eSIM 卡和普通 SIM 卡最显著的不同是外形和封装形式。普通的 SIM 卡主要用于手机或平板设备,用于支持移

动通信基础业务和增值业务,使用环境对 SIM 的封装工艺和软硬件没有特殊要求,采用插入式封装。普通 SIM 卡在恶劣环境下的适应性较差,无法满足很多物联网应用场景对于环境特性的需求。随着物联网技术的普及驱动,越来越多的传统商品(如汽车、智能表具、监控设备等)被嵌入传感器和通信模块,成为物联网终端^[9]。物联网终端的工作环境比传统移动终端更加复杂和恶劣,终端可能部署在偏远无人地区,温湿度极低或者极高,可能需要频繁变更工作区域,还面临行驶过程中高频率震动的影响。为了保证移动通信的稳定性和设备自身的物理安全性,物联网终端往往采用 eSIM 卡取代传统插拔式 SIM 卡,即将 eUICC 芯片直接焊接在终端电路板(SMD 方式)或直接封装入通信模块(SIP 方式)。

针对车联网特殊的应用场景和复杂的应用环境,SIM 卡的需求目前主要集中在以下 3 个方面。

(1)封装特性

插拔式 UICC 易造成接触问题,无法满足震动环境的使用。MFF(M2M form factor)UICC 以更小的尺寸与通信模块焊接在一起,采用贴片封装工艺,在防震动和防盗用方面有明显改善。

(2)硬件特性

SIM 卡需要达到工业级的环境特性要求。尤其是汽车厂商往往要求其前装车载终端内使用的 SIM 卡达到车规级要求。

(3)管理模式

物联网应用中,很多设备在生产时就预装了 eSIM 卡的

终端。这些设备往往在某一地生产,在全球销售和使用;生产后可能长时间后才被启用,并且在业务签约到期时,很多设备需要重新订购,甚至转换运营商,而给 M2M 终端换卡的方式则影响正常的业务运营;此外,物联网设备的活动范围大,国际漫游的情况下存在切换到运营商以降低成本的需求。因此不同于传统的面向手机使用的 SIM 卡发行管理体制,出现了二次发行和运营商签约关系转移等新问题。

ETSI TS102.671^[10]定义了 M2M UICC 在普通 SIM 卡基础上添加了适应宽幅环境温度、震动、防腐蚀等物理指标;同时大幅提高嵌入式 SIM 卡的存储器数据的保存时间和数据更新次数等参数,以保证在车载等需长时间保存数据的场合中应用。为适应各种大小不同的设备,规范定义了 M2M UICC 可以是传统的插入式和新型的 MFF 两种外形(MFF1 和 MFF2)之一。TS103.383^[12]标准定义了 eUICC 的使用场景及需求,尚在制定中的 ETSI TS103.384 标准将进一步规定 eUICC 的物理、逻辑、电器特性,eUICC 的架构及 profile(用户签约参数集)的定义、远程管理、安全特性。

eSIM 本质上是一种可编程 SIM 卡,profile 出厂后可编辑,它支持通过 OTA 对 SIM 卡进行远程配置,实现 profile 的下载、安装、激活、去激活及删除,能够应用于 M2M 终端出厂后批量业务开通、业务到期后续约、改变签约以及在漫游时变更运营商等场景。其内部逻辑结构与传统单一运营商签约数据方式不同,如图 1 所示。

eSIM 可以满足物联网业务的一系列特征和需求:能够提升芯片性能,满足更宽的温度范围,并且提高数据保

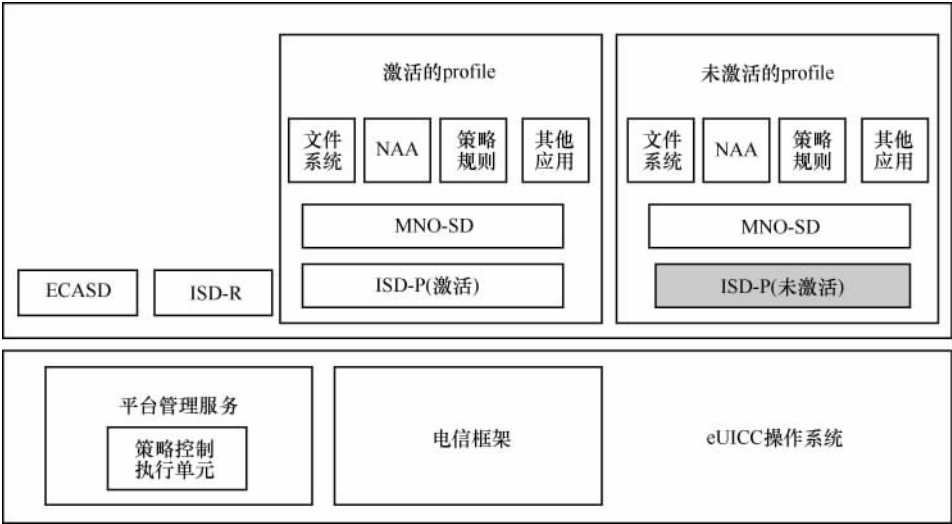


图 1 eSIM 卡逻辑结构



存时间和擦写次数,避免了可插拔 SIM 卡存在的被盗风险,并且有效减小终端尺寸,在 M2M 终端部署后,可以远程开展业务订购及用户信息配置,按需分配码号并及时回收,通过 OTA 方式可以灵活实现业务订购、运营商及网络的选择切换。

根据 GSMA Intelligence 在 2015 年 3 月发布的白皮书《Understanding SIM evolution》,从中远期来看,嵌入式 SIM 卡以及远程业务配置能力将广泛应用于物联网以及消费电子领域,GSMA 提供的 SIM 发展路径包括以下 4 个阶段。

(1) 传统方案

SIM 卡可从设备上插拔,每张 SIM 卡保存一个运营商的 profile,当用户转换运营商时需要更换 SIM 卡。

(2) 近期演进

SIM 卡嵌入物联网终端并可保存多个运营商的 profile。

(3) 中期演进

eSIM 首先应用于汽车行业,并逐渐扩展到物联网其他领域,包括可穿戴设备。

(4) 远期演进

eSIM 及远程业务配置能力将应用到包括手机在内的所有设备上。

3 eSIM 远程配置技术

eSIM 发行后,为了实现对卡片上的文件和参数集进行配置管理,需要设计一套 eSIM 卡远程配置(remote SIM provisioning, RSP)管理系统。该系统能在一套安全的机制下实现对运营商 profile 的整个生命周期管理,包括 profile 的下载、安装、激活、去激活和删除。

一个典型的 eSIM 远程写卡系统的架构如图 2 所示。

其中,eSIM 远程配置平台是整个系统的核心网元。eSIM 卡中用户签约数据须经由远程配置平台生成完整的运营商数据文件,才能通过空中写卡等方式下载到 eSIM 卡中。eSIM 卡上 profile 的整个生命周期管理都是由远程配置平台实现。eSIM 远程配置平台包括签约数据准备和签约数据分组管理两个主要功能模块。

(1) 签约数据准备

签约数据准备主要负责在可靠的环境下生成包含签约信息的 profile 数据分组,并且与签约数据分组管理模块配合实现 profile 安全下载到 eSIM 卡中。在 profile 数据分组生成过程中,签约数据准备模块先从 eSIM 卡制造商处获取不包含个性化签约信息的 profile 数据文件,再从运营商卡管理平台获取个性化签约信息,包括 IMSI、密钥、ICCID、目标 eSIM 卡编号等,最终生成完整的个性化签约数据分组。该数据分组用签约数据准备模块的公钥加密并带上自己的签名后传递给签约数据分组管理模块。

(2) 签约数据分组管理

签约数据分组管理主要负责将加密的 profile 数据分组通过可靠安全的传输信道传递到目标 eSIM 卡中,并对 eSIM 卡中 profile 后续的生命周期进行管理。签约数据分组管理模块拥有可信证书发行方授予的 eSIM 卡传输证书,通过该证书才能与 eSIM 卡建立安全通信通道,通过安全通信通道,可以将签约数据分组传至 eSIM 卡并向 eSIM 卡传递 profile 状态切换等生命周期管理的命令。

可信证书发行方负责 eSIM 卡制造商,eSIM 卡远程配置平台和运营商卡管平台这几个网元的安全证书发放和

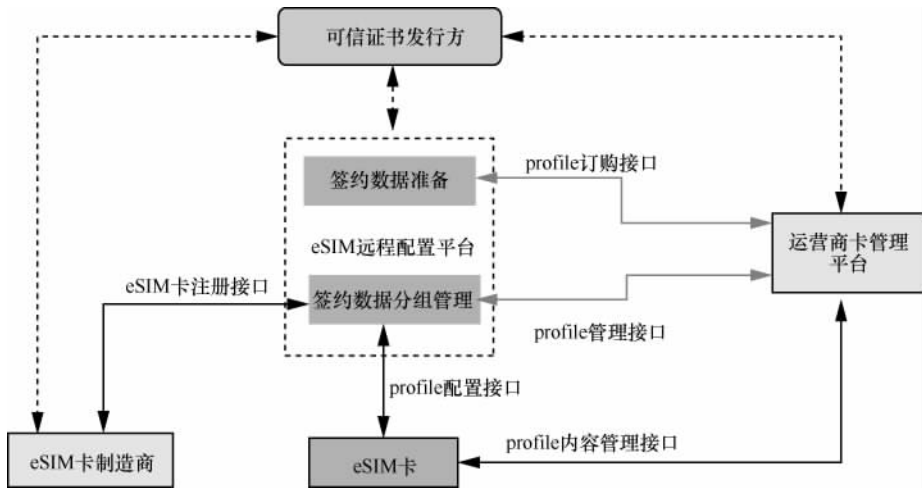


图 2 典型远程写卡系统架构及接口

公钥发布,只有符合整个系统安全认证规范的网元才能获取认证证书。

eSIM 卡远程配置管理系统各个网元之间的接口必须是执行设备双向认证的安全接口,远程配置平台与 eUICC 之间、运营商卡管平台与 eUICC 之间采用 GP 的 SCP 80 或者 81 协议传输数据。该平台主要接口功能如下所示。

(1)eSIM 卡注册接口

eSIM 卡制造商将新生产的 eSIM 卡信息、卡管理和 profile 管理的信任状态安全传递至远程配置平台。

(2)profile 订购接口

卡管理平台向远程配置平台发起 profile 预订请求,平台按照卡管理平台提供的输入生成个性化的 profile 数据分组。

卡管理平台提供的输入是为有效用户生成一组信任状态的信息请求、和 NAA 相关的算法和参数、profile 中的其他数据和应用、策略规则。

(3)profile 管理接口

平台接收卡管理平台发送的信息是 profile 管理命令/指令、策略控制和执行的命令/指令。

平台向卡管理平台提供的信息是配置 profile 的目标 eSIM 卡信息、对 profile 管理命令的接收响应、对策略控制和执行命令/指令的接收响应。

(4)profile 配置接口

负责对 eSIM 卡上 profile 的下载和安装、激活、去激

活、删除等操作。

2016 年 6 月,GSMA 发布 SGP02 (remote provisioning architecture for embedded UICC technical specification)v3.1^[4] 版本,制定了物联网 eSIM 远程配置的架构,如图 3 所示。

该系统架构包括了 eSIM 卡制造商(EUM)、证书发行方(CI)、SM-DP、SM-SR 等功能网元。其中,CI 作为可信的第三方,负责为 eUICC 远程配置系统和网元实体发行证书,通过认证鉴权保证网元之间交互的安全。SM-DP 负责签约数据的准备,创建 profile 数据分组并进行安全加密,通过 SM-SR 把 profile 安全下载和安装到 eSIM 中。SM-SR 提供安全路由,根据 SM-DP 的请求,把数据分组从 SM-DP 下载到 eUICC 上,并且支持对 eSIM 上 profile 的激活、去激活以及删除等操作。

eSIM 技术最早应用在物联网领域,但是,近期苹果、三星等设备商已经把 eSIM 技术应用到消费电子设备上,如 iPad、智能手机、智能手表等。为了应对消费电子领域出现的这种趋势,GSMA 组织制定了消费电子领域以及物联网领域统一的架构和标准,可同时应用于物联网以及消费电子领域,为 M2M 设备以及消费电子设备提供远程配置管理的能力。该融合 RSP 架构于 2016 年 6 月底完成统一架构 1.1 版^[4],如图 4 所示。

融合 RSP 方案是在 GSMA M2M 方案的基础上进行扩展,新增 LPA,并且弱化/取消原架构中的 SM-SR,其功能

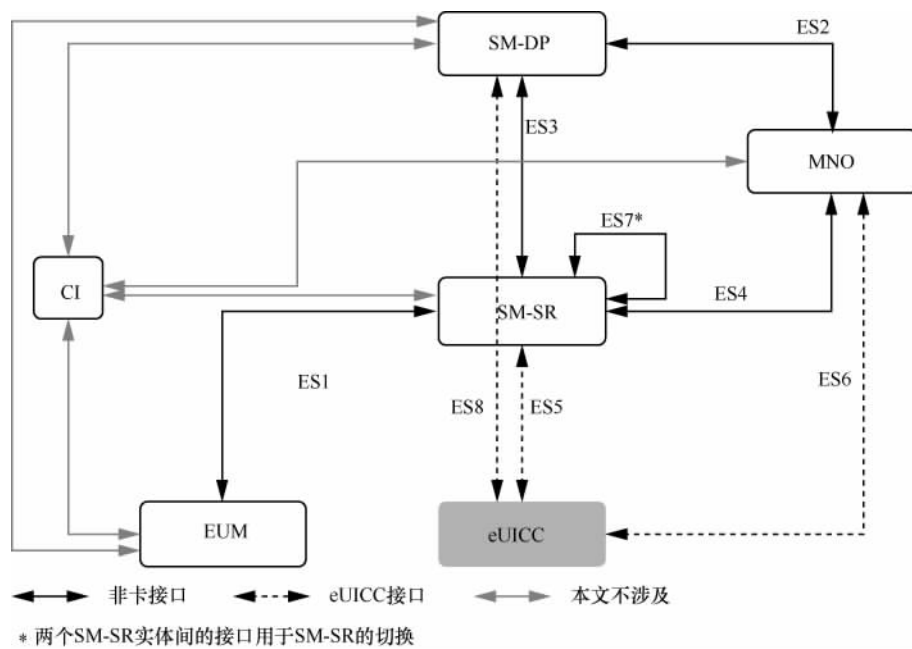


图 3 GSMA eSIM 远程业务配置架构

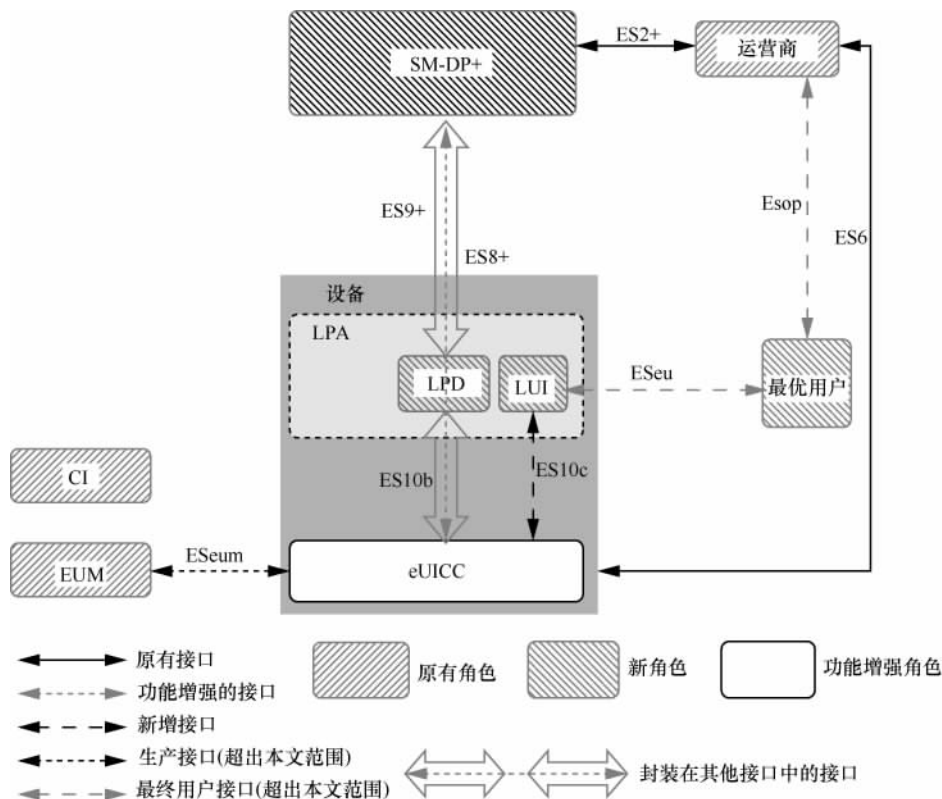


图4 GSMA eSIM RSP融合架构

由 SM-DP+以及 LPA 来实现。LPA 是终端设备上的本地 profile 代理，其功能包括 profile 下载（local profile download），作为 eUICC 与 SM-DP+之间的代理，从 SM-DP+ 获取 profile 数据分组，再转移到 eUICC 中；本地用户接口（local user interface）面向用户提供 profile 管理的功能，包括 profile 的激活、去激活、删除等。SM-DS 负责为终端设备提供目标 SM-DP+的地址，使终端设备可以找到该 SM-DP+并下载所需的 profile 包。

4 eSIM 在车联网业务中的应用

eSIM 当前主要应用于物联网领域，重点集中在车联网，典型应用场景如下。

(1) 一点制造，全球销售

大多数汽车巨头的关键零部件均采用全球采购的方式来统一标准、降低成本。随着车联网业务的发展和普及，车企对其车载终端供应商提出同样的要求，希望汽车从生产开始就具备通信能力以便于测试，运输到销售地区后切换到当地运营商提供通信服务。车载终端的制造地和销售地的不同造成了码号切换的业务需求。在车机生产和调试期间，使用制造地运营商的码号；待整车总装调试时切换

到车辆生产地的运营商，销售到客户所在地后切换为当地运营商，从而在不同国家使用当地的移动通信服务，达到降低使用成本、提高通信服务的目的。

(2) 跨域漫游

车辆的活动范围相对一般的物联网终端要大得多，很多车辆会经常在不同地域漫游，为获取良好的通信服务和降低使用成本，车厂希望可适时切换不同运营商的码号，在不同国家使用当地的移动通信服务。

(3) 国内运营商切换

随着全制式通信模块的推出，车厂希望车载终端能够同时支持接入多个运营商，并能够根据最终用户需求，选择某家运营商接入。当车厂向车辆所有者提供的免费期到期后，允许车辆所有者变更运营商；车厂和原运营商合约到期，允许将 TCU 批量切换为新运营商。

(4) 运营商远程管理自身码号资源的需求

由于车载终端从制造到最终销售的周期比较长，在正式使用前后会有一段沉默期，相对于正式激活期，该段沉默期时间较长，运营商一般会提供特殊号段，采用低资费，并在计算 ARPU 值考核时予以特殊考虑。用 eSIM 远程配置技术，可以实现上述沉默期到激活期的互相转换。终端

出厂后码号进入沉默期,待终端正式测试后转换为激活期号段。终端激活后码号进入激活期,当最终客户和车厂的合约到期后,为避免销号后车载终端无法重新激活的情况,可以让该号码进入沉默期。

(5)移动业务用户变更

大部分车厂为客户提供部分业务或一定期限的免费服务,如车辆监控和安防服务。车内娱乐、多媒体、Wi-Fi等服务在免费期后由客户自己付费。发生付费签约主体变化的码号要进行相应的切换,新用户可以选择自己喜欢的运营商及相应的套餐。

5 结束语

eSIM 在车联网的使用已经是大势所趋,越来越多的车厂对 eSIM 的远程配置提出了明确的需求。但是,跨运营商的码号切换带来的潜在用户黏性降低是运营商不愿意看到的。从运营商的角度而言,在全球范围内提供码号远程配置和切换能力是运营商提高自身竞争力、扩大服务范围的机遇。

参考文献:

[1] Smart cards machine to machine UICC physical and logical

characteristics(release 9): ETSI TS 102.671[S/OL]. (2011-09-01)[2016-08-20]. <http://www.freestd.us/soft3/955827.htm>.

[2] Smart cards embedded UICC requirements specification (release 13): ETSI TS 103.383[S/OL]. (2013-09-01)[2016-08-20]. <http://www.etsi.org/index.php/technologies-clusters/technologies/smart-cards>.

[3] Remote provisioning architecture for embedded UICC technical specification version 3.1: GSMA. SGP.02[S/OL]. (2016-05-27)[2016-08-20]. <http://www.gsma.com/newsroom/all-documents/sgp-02-v3-1-remote-provisioning-architecture-for-embedded-uicc-technical-specification/>.

[4] RSP technical specification version 1.1: GSMA. SGP.22[S/OL]. (2016-07-09) [2016-08-26]. <http://www.gsma.com/newsroom/all-documents/sgp-22-technical-specification-v1-1/>.

[5] Understanding SIM evolution: GSMA [EB/OL]. (2015-03-03)[2016-08-20]. <https://www.gsmainelligence.com/research/2015/03/understanding-sim-evolution/499/>.

[作者简介]



黄海昆(1973-),男,中国电信股份有限公司上海研究院高级工程师,主要研究方向为物联网相关技术。