

浅谈 SIM 卡虚拟化及云服务的发展趋势

作者： 龚智辉（优克云联 CTO）

来源： 黑马汇 https://www.sohu.com/a/368011397_574724

记得 1997 年我刚参加工作得到第一部摩托罗拉手机的时候，第一件事情就是到移动营业厅去开一张 SIM 卡，有了这张卡才可以打电话、发短信。一张 SIM 卡可以使用好多好多年，感觉只要不丢就可以用到天荒地老；换手机的时候只需要把 SIM 卡拔出来放入新手机，就可以继续使用原来的电话号码。还能通过 SIM 卡存储或转存通讯录，最初的时候为了方便查找联系人，中文姓名前还会加上首字母，尽管已过去了 20 多年，一些老朋友在我的手机通讯录里至今还是以这样的形式出现。

我曾经在一个运营信息交换电子商务平台的公司工作，为券商提供证券交易的综合服务平台，其中有个功能就是支持手机炒股，我们使用了 STK 技术。手机只要换上 STK SIM 卡，就可以使用手机菜单进行股票的查询、买、卖、撤单等各种操作。现在看来就是最原始的移动互联网应用之一。

今天，手机 SIM 卡作为开启每个人移动通信服务以及连接互联网大门的钥匙，其重要性、安全性、便利性一直备受关注。

SIM 卡从 1991 年在芬兰移动网络运营商率先商用以来，到现在已经有将近三十年的历史。对于普通用户来说，最直观的感觉就是 SIM 卡越做越小——苹果公司一直在积极地推动 SIM 卡的小型化，2010 年在 iPhone 4 上首次使用微型 SIM 卡，2012 年在 iPhone 5 上开始使用纳米 SIM 卡。

其实，无论是全尺寸（Full-size, 1FF, 85.6×53.98）、迷你卡（Mini SIM, 2FF, 25×15）、微型卡（Micro-SIM, 3FF, 15×12）还是纳米卡（Nano-SIM, 4FF, 12.3×8.8），SIM 卡的物理结构都基本相同，只是封装方式上的区别。

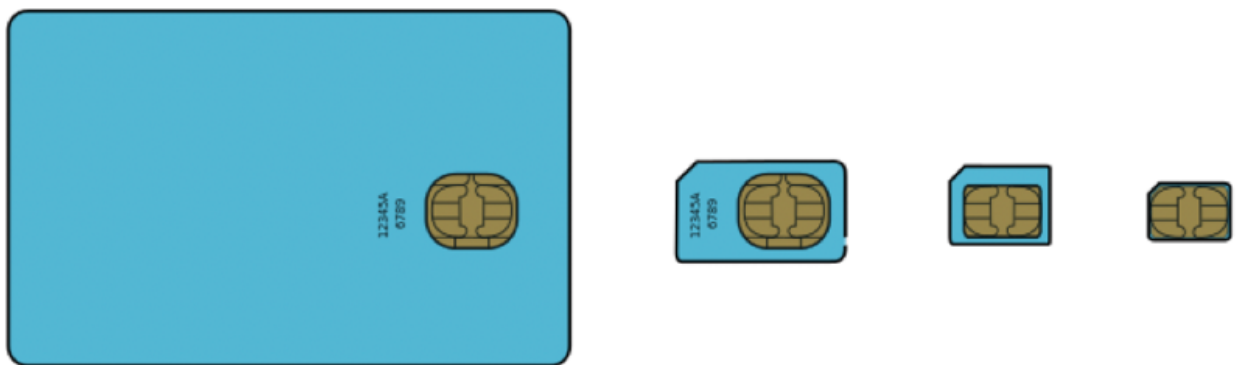


图 1 各种规格的 SIM 卡（来源：https://en.wikipedia.org/wiki/SIM_card）

随着苹果公司在 iPad Air 2 上使用 Apple SIM，软卡和 eSIM 这些名称也陆续进入大众的视野，然而这些 SIM 卡已经是只闻其名不见其形了。

未来，SIM 卡将以怎样的形态出现在我们的生活中呢？本文就试着从 SIM 的起源开始，简单探讨一下 SIM 技术的演进发展历程和 SIM 卡虚拟化及云服务的未来。

实体 SIM 卡

SIM 卡的名称来源于英文 Subscriber Identity Module 或 Subscriber Identification Module 的缩写，是为了安全地存储国际移动用户身份（IMSI，International Mobile Subscriber Identity）、用户号码及其关联密钥以及其他移动网络连接信息的一种集成电路，用于在移动通信设备（包括：移动电话、平板电脑、移动电脑等）连接移动通信网络时识别用户身份及鉴权。

SIM 卡标准最初由欧洲电信标准协会在规范中制定，编号为 TS 11.11。本规范描述了 SIM 卡的物理和逻辑行为；随着 UMTS 的发展，规范工作被部分转移到 3GPP。3GPP 现在负责诸如 SIM（TS 51.011 [4]）和 USIM（TS 31.102 [5]）和 ETSI 等应用程序的进一步开发，以便物理卡 UICC 进一步发展。

SIM 卡的物理接口使用智能卡标准接口 ISO/IEC 7816，并一直沿用至今。核心是一个集成电路芯片，使用不同大小的封装方式，形态基本保持相同（见图 2）。

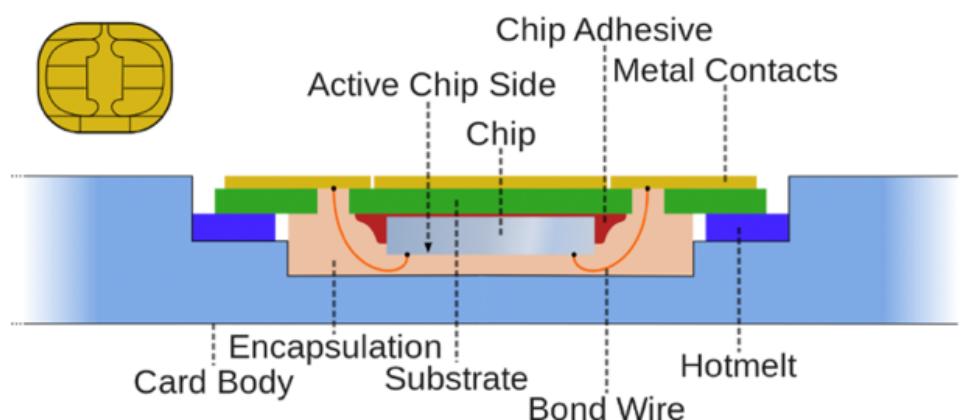


图 2 SIM卡物理结构图（来源：https://en.wikipedia.org/wiki/SIM_card）

GSM 时代，SIM 卡是软硬件一体的。随着第三代移动通信 UMTS 的出现，SIM 卡的软硬件则逐步分离。目前，SIM 的实际意义就是应用软件，而硬件部分是 UICC，也就是芯片的物理本体，集成电路芯片。软件部分对于 UMTS 来说就是引入的 USIM（通用订户身份模块）；SIM 卡中的软件包括底层操作系统和上层各种软件，包括操作系统、Java 虚拟机、Toolkit、OTA 等。3GPP 的 TS11.14 规范了 SIM 应用工具包（STK）技术，允许在 SIM 卡中加载应用。这样在 SIM 卡上进行开发和配置就更加简单方便。本文引言中提到的 2000 年左右开发的手机炒股，还有当时招商银行与中国移动合作开发的手机银行，以及影响了一代人、救活了一个伟大互联网公司的手机 QQ，都是使用了 STK 这个技术。

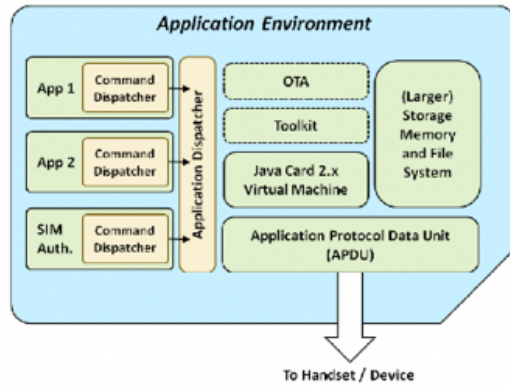


图 3 SIM卡内部软件结构

随着物联网的发展，越来越多的非通信设备也需要接入移动网络，因此对嵌入式 SIM 卡（eSIM）的需求不断增加，GSMA（全球移动通信联盟）推出了 RSP（远程 SIM 卡配置）规范，各种设备都可以预先嵌入式安装 eSIM 卡，当用户启动设备时，再按需开通和下载不同运营商的 SIM 卡用户参数和相关密钥，实现在线开通 SIM 卡。苹果公司在 iPad、iPhone 以及 Apple Watch 所使用的 AppleSIM，就是使用 eSIM 技术。

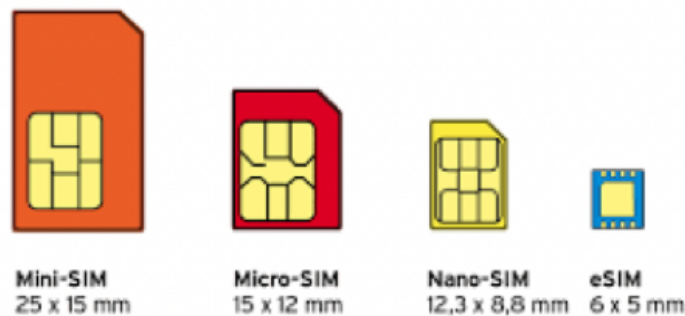


图 4 eSIM与其他SIM卡的大小比较

虚拟 SIM 卡

SIM 卡技术的引入，将通信设备的认证鉴权集中到了一个小小的 SIM 卡。不仅方便了移动设备的独立发展，也方便了 SIM 技术自身的不断发展。但是，随着人们在现实生活中对移动通信技术的越来越广泛应用，特别是移动互联网技术的发展，最终用户在各个方面的使用越来越多，SIM 卡在使用过程中的一些限制也越来越突出：

- I 机卡绑定，即移动通信设备与指定的 SIM 卡绑定，如需更换运营商，则需要连同手机一起更换。
- I 通常情况下，一张 SIM 卡只能对应一个运营商的网络，用户如需转网，原有 SIM 卡无法重用，必须重新开卡。
- I 跨国旅行时如需使用当地 SIM 卡，用户必须将原来的 SIM 卡移除，无法同时使用。即使存在多卡多待的手机，可以容纳的 SIM 卡数量也很有限，绝大多数手机仅支持双卡。

为了解决这些问题，特别是为了解决漫游地上网问题，各种突破 SIM 卡限制的技术应运而生。其中最常用的技术就是 SIM 卡虚拟化技术；其可行性来源于以下几种技术基础：

- 1) 卡规范上通过 USIM 技术，将软件部分和硬件本体分离，为 SIM 卡虚拟化提供了最基本的条件。
- 2) SAP 协议：SIM 卡访问协议（SIM Access Profile），支持远程对 SIM 卡进行操作。SAP 协议最早应用在车载蓝牙电话模块。车载模块可以通过蓝牙使用用户手机中的 SIM 使用电话功能。这样可以实现一个通信设备使用不在设备内的 SIM 卡。
- 3) 虚拟机技术：SIM 的软件部分本身就是操作系统和其中的软件及相关模块，使用虚拟机技术，非常容易在虚拟机管理系统中虚拟出一个 SIM 卡的软件系统来。
- 4) RSP 规范：RSP 是 eSIM 的供卡规范，支持 M2M 方式和 Consumer 方式。其中 Consumer 方式，是通过一般网络连接，通过安全通信协议，将 SIM 订户信息及相关安全认证信息下载到 eSIM 中，实现 SIM 卡的下载。

下面简单介绍一下几种常见的 SIM 卡虚拟化技术：

1. 接口延伸法

将 SIM 卡的接口通过物理电路延伸到另外一个模块。在新的模块中，承接原有的 SIM 卡，同时支持插入其他 SIM 卡，或者通过软件模块，获得从其他地方下载的 SIM 卡。扩展出来的模块可以自主开发，进一步扩展其他功能。



图 5 通过卡槽使用电路扩展的 SIM 卡模块
(来源：百度图片)

2. 贴片扩展法

在 SIM 卡上，重新贴上一个很薄的芯片，实现原来 SIM 卡的二次扩展。由于通过另外的电路嵌入到已有的 SIM 卡系统中，所以，可以在贴片上额外增加其他功能，比如电子钱包。

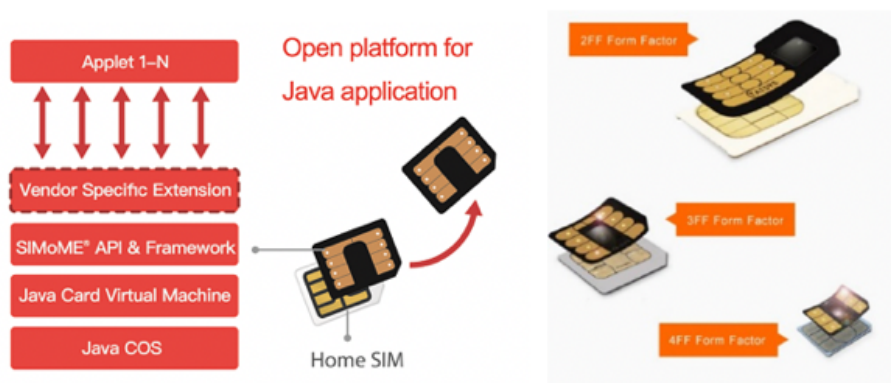


图 6 薄膜SIM卡 (来源: <http://www.taisys.com>)

3. 近距离无线延展法

通过蓝牙本地连接, 利用 SAP 协议, 或其他特有协议, 通信设备可以非常方便地使用扩展设备所提供的 SIM 卡。SAP 协议 (SIM Access Profile) 由国际蓝牙组织 (Bluetooth.org) 2000 年开始制定, 2005 年出 1.0 正式版本, 2008 年出 1.1 正式版本, 这个协议是移动设备与 SIM 卡分离的关键。因为, 既然可以本地无线, 也就可以通过移动网和互联网无限延伸了。而且, 这个通过蓝牙供卡的设备, 还可以通过其他通信手段从网络上获得其他的 SIM 卡。



图 7 使用蓝牙连接的SIM卡适配器

(来源: <https://www.dhgate.com/product/skyroam-gmate-adaptor-dual-sim-bluetooth/150100632.html>)

4. 网络远程延展法

通过互联网, 连接部署在远程的 SIM 卡, 非常方便地使用位于全球网络可以触达的任何地方的 SIM 卡。这个技术来源于远程 SIM 技术, 在 2000 年代中期, 大量应用在移动通信公司的漫游 SIM 的远程拨测设备 (RTU) (参考 2007 年 11 月期《广东科技》的“SIM 卡池及异地调度技术的实现与应用”)。但这种技术在普通用户的移动设备上应用则是 2011 年以后, 优克联、斯凯荣、iQsim、Aicent 都利用这个技术来解决用户移动漫游问题, 将 SIM 卡异地调度技术应用到普通的终端设备上, 通过远程连接来使用云端卡池中的 SIM 卡。

5. 虚拟机扩展法

前面几种方法都是将 SIM 卡在物理空间上的延伸, 使用远程或另外的 SIM 卡来替换通信设备中的 SIM 卡。但实际的使用过程中从实用性考虑, 还是需要本地有一个 SIM 卡比较好。

而本方法在通信终端中不需要 SIM 卡的物理本体，直接将 SIM 软件使用虚拟机进行仿真模拟，具备 SIM 所有的接口功能，通过软件接口（比如 SAP 协议）提供物理卡的所有功能。只有在需要使用到只有物理卡中才有的信息（比如密钥）时，才调用远程 SIM 卡。这是一种更加高效实用的方法。

我们知道，SIM 卡识别身份最重要的就是 SIM 卡硬件中的密钥。尽管密钥是一串数字，但 SIM 卡在制作的时候，将这个密钥和软件捆绑在一起，确保更高的安全级别。其实，软件运行在 SIM 卡上和运行在任何计算机模拟的计算空间都是一样的，关键还是在密钥。

按照密钥所存放位置的不同，又衍生出来以下三种技术：

1) eSIM 技术：GSMA 推荐技术，基本维持了物理实体 SIM 卡所具备的安全级别，通过 RSP 协议，将所有 SIM 信息安全地从远端下载存储到 eSIM 这个物理设备中。也就是将以前在 SIM 卡工厂写卡的一些动作，推迟到用户按需订购后再写卡。

2) 软卡技术：这个技术就是将 SIM 卡中所有的配置以及密钥，都以软件的形式在设备的操作系统中模拟出一个虚拟的 SIM 卡。

3) 远程虚拟卡技术：这个技术是将卡在用户设备端使用虚拟机的方式进行模式，当需要使用 SIM 卡的时候，需要使用 SAP 或其他相似技术，远程访问部署在远端的物理 SIM 来完成鉴权。这个技术与软卡的不同点在验证密钥还在物理卡中。

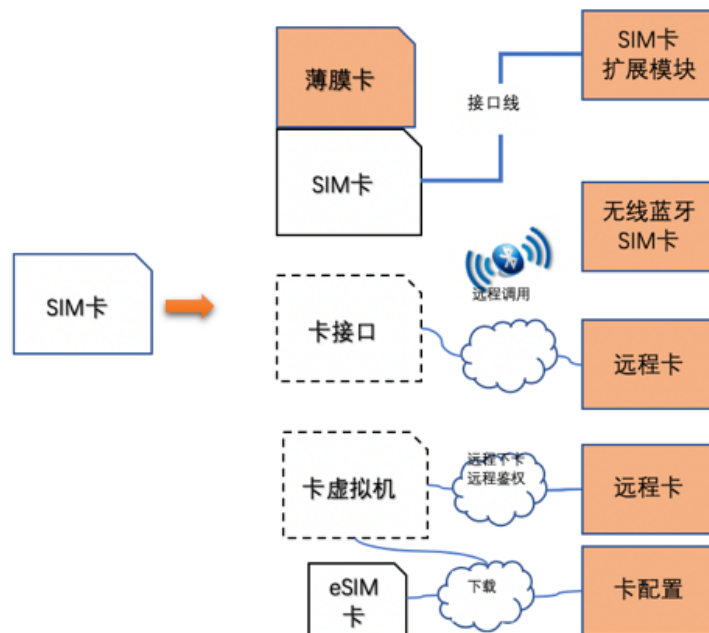


图 8 SIM 卡的多种虚拟化方式

基于虚拟 SIM 卡技术衍生的漫游解决方案

大部分技术的发展都是为了解决实际应用场景中的问题而产生的，前面所描述的 SIM 技术的不断突破，很多都是受用户漫游问题所驱动的。

为了解决漫游地高额话费以及漫游地通信不方便的问题，移动电话用户一直在期望有更好的办法解决移动漫游问题，方便出行时连接互联网。特别是 2005 年以来移动互联网的发展，更加促进了异地使用非漫游的本地卡上网的

需要。

实际生活中，用户解决漫游问题常常使用以下几种方法：

I 购买目的地 SIM 卡使用：到达目的地后购买并更换 SIM 卡使用，或者插入到双卡手机，总之需要占用一个卡槽；

I 插卡 MiFi（随身无线路由器）：使用可以插卡的上网设备（俗称插卡猫），购买目的地的 SIM 卡，并插入到设备中使用。设备提供 Wifi 热点信号，供移动设备连接使用。设备连接的网络和具备的连接能力，依赖于所购买的 SIM 卡。

I 免插卡 MiFi：无需插卡，只要购买所需的流量包，就可以使用上网功能。流量包可能是全球多个国家通用的，使用方便，且价格上普遍比插卡 MiFi 更便宜。

I eSIM 技术：通过其他网络（如 WiFi）在线购买目的地运营商提供的 eSIM 卡进行上网。但目前该技术并不受大多数运营商欢迎，因此在市场上普遍供应不足。从苹果公司的 Apple SIM 推进情况就可以得到印证。Apple Watch 开通上网卡在中国一波三折，更别说其他品牌的移动电话了。所以说，eSIM 技术的推广运营商的供应是关键。

I 软卡技术：这也是目前市面上比较常用的技术，如华为天际通、红茶移动都是使用这一技术。

I 手机内嵌全球上网技术：使用云端卡池，用户根据自身需要选择购买对应流量套餐并激活使用。优克联在 2018 年巴塞罗那移动大会上推出世界手机 S1 就是使用了这个技术，通过 GlocalMe Inside 方案将远程虚拟卡技术整合到手机的基带中。目前小米部分型号手机支持该功能，估计未来还会有更多品牌和型号的手机陆续支持。

从以上分析可以看出：

I eSIM 技术是官方推出的技术，但运营商不热心，叫好不叫座也没有办法。

I 软卡技术，由于存在安全风险，GSMA 不建议使用，运营商及相关厂商投鼠忌器，不敢大规模推广。

I 免插卡 MiFi 是相对性能优异且安全的技术，但需要携带额外的设备，造成了一定负担。一些免插卡 MiFi 兼顾充电宝功能，用户接受度更高。

I 直接将免插卡 MiFi 的技术植入手机，是更符合用户期望的方式，不影响用户原有 SIM 卡的使用，性能和安全性也最有保障。

SIM 卡云服务解决方案

移动通信的特点使得不同运营商提供的服务必然是存在差异的，以中国为例，三大运营商的覆盖就各有特点，例如：中国移动基站数量最多，大部分区域的信号覆盖就最好；但是中国移动的用户数量也最多，在高峰期网络拥塞的情况也最严重，用户即使处于良好的覆盖条件下也难以获得满意的网速，联通和电信在这时候却有更好的体验；另外，价格也是用户考虑的一个重要指标，特别是在出国漫游使用时。因此，如果用户只能使用手机中原有的一张 SIM 卡，那么就很可能遭遇到：有时候覆盖信号差；有时候网络拥塞上网速度慢；有时候需要支付高额的漫游费用；有时候套餐流量用尽只能到处蹭免费 Wi-Fi.....

应对这些问题，最根本的解决方案是：允许用户更方便的更换 SIM 卡，从而令用户可以根据自己的需求，随时随地自由选择提供服务的运营商，以及所需的网络服务套餐。

而实现这一解决方案，上述软卡、eSIM、远程 SIM 卡等技术都是可行的，但是考虑到提供全球范围上百个国家的网络服务，SIM 卡供应的问题也必须通盘考虑。

针对 SIM 卡的供应来源，我们针对上述虚拟 SIM 卡技术展开逐一分析。

I 软卡：由于密钥可以随着软件拷贝，在安全上存在着使用方面的风险，完全依赖于对卡的使用方的信任。

I eSIM 卡：可以解决软卡的安全上的担忧，但是，由于运营商在商业上希望对用户锁定来进行自我保护，不想把用户选择的权利下放到手机，目前 eSIM 的供应量有限，因此，目前 eSIM 的应用主要集中在物联网领域。

I 远程 SIM 卡：由于使用普通的物理卡，SIM 卡来源不存在特殊性，因此可以在全球范围内获得充足的供卡。

从安全性和 SIM 卡供应两方面来看，远程 SIM 卡技术是比较好的，另外，对便利性、实施成本、流量成本等其他方面一并考虑后，下表是对这三种技术的对比分析。

项目	远程SIM卡	eSIM卡	软(SIM)卡
形态	物理的，各种变体，从1FF、2FF(Mini SIM)、3FF(Micro SIM)到4FF(Nano SIM)。	物理的，形态上可以是物理卡、芯片和芯片内置模块等	软件形态，包括重建卡操作系统 (COS) 所需的所有软件要素，一般通过虚拟COS的形态存在。
密钥存放位置	卡内	卡内，通过卡供应协议安全传递	软件内，通过卡供应协议安全传递，可移动
实例化	维持物理卡的实体，不进行修改	在eSIM卡中进行物理实例化	在软件模块中进行软件实例化
安全等级	最高	其次	最差
可获得性	最普遍	运营商刚刚开始接受	GSMA不鼓励，少数运营商提供，一般大运营商不提供
实施成本	鉴权需要额外通道，成本稍贵	需要通过专门的认证，有进入成本，而且涉及到多方协议	实施最简单
采购成本	低	较高	最高

从以上分析来看，目前远程 SIM 卡还是最合适的供卡方式，其次是软卡，最后是 eSIM 卡。随着物联网的普及，在物联网领域 eSIM 会有比较好的期望，但还是需要观望。

各种虚拟卡的比较

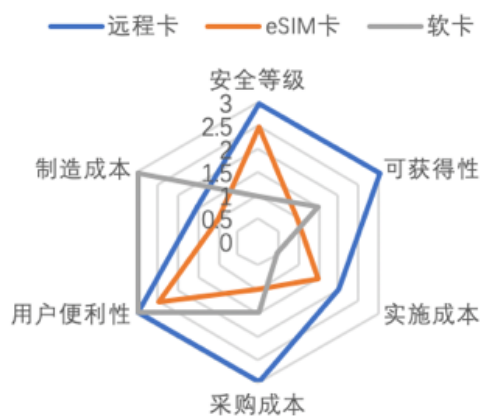


图9 虚拟卡技术比较雷达图

显然，普通用户并不会关心使用具体什么技术，用户所需要的只是一个自己满意的漫游及本地上网解决方案——无论何时何地，购买了设备及服务套餐就可以上网。而作为对应的服务提供商，则要求解决方案具备以下特点：

- l 具有连接全球移动网络所覆盖的所有区域的 SIM 卡卡池（覆盖能力）
- l 具有动态感知移动终端所在区域的网络并动态换卡的能力（联网能力）
- l 具有为用户提供连接服务的按需服务的能力（可自由选择）
- l 具有根据用户使用需求动态扩充性能的能力（容量扩充能力）
- l 具有灵活的计费能力，支撑用户的购买需求和透明消费的需求（可计费）
- l 具有优质的网络连接服务质量（最佳连接）

这些特点正好反映了云计算的弹性服务、资源池化、按需服务、服务可计费、泛在接入的五大特点，因此我们将满足以上特点的解决方案称为 SIM 卡云服务解决方案，简称云卡。通过将各种 SIM 卡资源池化，然后将连接资源的能力虚拟化之后，实现用户根据需要弹性购买。随着 5G 技术的发展，连接能力的虚拟化会更加多维度，给用户更多的选择空间。云卡正好借鉴现代云计算技术来实现 SIM 卡所提供的连接服务的云化。

云卡云服务系统包括以下基本要素：

1) 云卡终端：

- l 同时支持各种虚拟卡技术，包括 eSIM 卡、远程物理卡、软卡，并具备良好的扩展能力，支持未来各种各样的 SIM 卡；
- l 具备根据网络环境动态换卡的能力；
- l 具有高度安全的 SIM 卡保护机制，确保云卡在网络连接安全性、计费准确性；

I 具有良好的质量监控与保障机制；

2) 云卡平台

I 具有容纳全球各种各样 SIM 卡的管理能力，为云卡终端按需分配 SIM 卡资源；

I 对云卡终端连接情况进行监控与分析，保证连接质量，可按用户等级提供服务；

I 服务可量化，可计费。

I 不限于原始运营商提供的服务能力，为用户提供更方便、灵活、个性化、场景化的贴心移动连接服务。

云卡云服务的现状与展望

从前面分析来看，SIM 卡云服务就是移动用户最终所希望使用的技术。实际上，业界在该领域已经有很多厂商在辛勤耕耘，并正在为广大用户提供服务。

I 华为天际通：华为的多款手机已支持使用软 SIM 技术的天际通功能，从其官网介绍来看，已支持全球 80 + 国家的精品网络覆盖。然而，可惜的是中国却不在覆盖范围内。从这点来看说，还不是很令人完全满意的云卡平台。

(来源：<https://consumer.huawei.com/cn/mobileservices/skytone/>)

I 环球漫游：16 年出入境通信服务，全球出行移动连接服务提供商，网络覆盖超过 210 个国家，通过随身 WiFi 提供服务，并为全球商户提供广告投放服务。

(来源：<https://www.vipwifi.com/>)

I 优克联：覆盖全球 140 + 国家地区。提供漫游超人租赁服务（免插卡 MiFi）和 GlocalMe 终端产品（免插卡 MiFi 和自带流量世界手机）；并提供 GlocalMe Inside 手机嵌入方案，通过云服务平台为合作伙伴提供 PaaS 和 SaaS 云卡方案。

(来源：<https://www.ucloudlink.com/html/service-local-mobile-data/>)

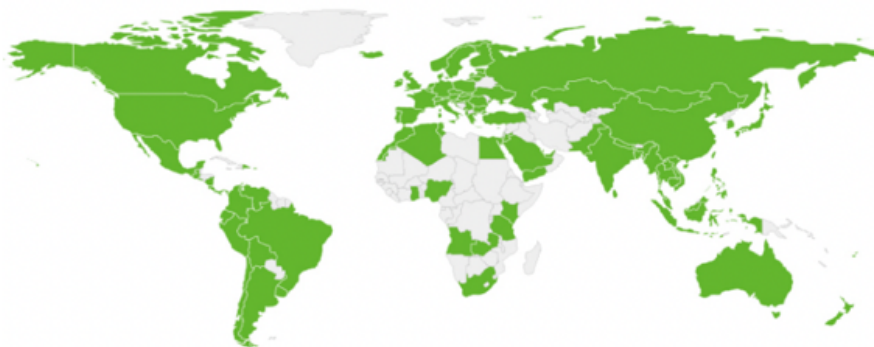


图 10 优克联云卡全球覆盖图

I 漫游宝 (Skyroam) : 提供无需插卡的随身 WiFi, 覆盖全球 130 + 国家, 并提供 VPN 服务, 覆盖 16 个国家。

(来源: <https://www.skyroam.com/wifi-pricing>)

I 小米全球上网: 通过第三方提供全球上网服务, 有的手机通过红茶移动提供, 有的通过优克联的 GlocalMe Inside 技术提供, 使用方式与华为天际通相同, 网络覆盖与技术提供商有关。

I 红茶移动: 使用 eSIM 技术, 提供 CaaS 服务平台, 采用 eSIM 技术, 为主要手机品牌提供 SIM 卡服务, 无自主终端, 网络覆盖 100 + 国家和地区。

(来源: <https://www.redteamobile.com/>)

目前看来, 华为、小米等厂商主要业务在手机, 上网也主要为手机服务, 云卡服务平台不是其主要业务方向。环球漫游、漫游宝通过自身 MiFi 产品提供上网服务, 以自主运营、直销服务的方式对外, 无法形成服务全球的云卡服务平台。红茶移动基于 eSIM 技术, 通过 CaaS 提供基础卡服务, 在 eSIM 还没有供应量和承接终端的情况下, 多数情况下采用软卡技术提供, 服务比较专注, 对最终用户的体验和触达还不够。尽管通过手机厂商, 网上公布有 2.5 亿以上的装机, 但实际使用人数不多。优克联提供的云卡平台, 广泛支持远程物理卡、eSIM 卡和软卡, 自营的漫游超人 Mifi 租赁业务在国内占有率最大, 以 PaaS 服务和 SaaS 服务方式, 面向最终用户和合作伙伴, 构建全生态链的云卡服务, 是值得期待的为移动用户提供贴心管家式云卡服务平台的公司。

云卡云服务平台的未来会怎么样? 互联网的游戏规则就是用脚投票, 最终用户说了算, 谁能将用户服务好, 谁就是赢到最后的玩家。但无论如何, 云卡云服务平台就是最终用户最喜欢的平台, 有用户需求在, 云卡云服务平台一起会发展起来的。(署名: 龚智辉)
