



eSIM在物联网安全中的应用探索

roam2free

2017.10

市场现状

模组厂商	模组	NB-IoT芯片
上海移远通信技术有限公司	BC95-B20/B8/B5/B28	华为海思 Boudica
深圳中微电子有限公司	SARA-N201	华为海思 Boudica
利尔达科技有限公司	LN805-01	华为海思 Boudica
深圳中微电子有限公司	BC95	高通 MDM9206
上海移远通信技术有限公司	L700	高通 MDM9206
芯讯通无线科技(上海)有限公司	SIM7000C	高通 MDM9206
龙尚科技(上海)有限公司	A9500	高通 MDM9206

随着窄带物联网的兴起，大量的NB/eMTC模组进入市场，承担着万物互联的连接基础硬件角色。

在传统模式下，模组仍需配合实体SIM实现运营商网络的鉴权与通信。



市场需求

窄带物联网所面对的市场，对于产品成本、体积、功耗、运营期限有着极端的需求（低成本、小型化，低功耗，服务期限长）；而通过eSIM取代实体SIM可以完好地满足以上需求。同时，由于窄带物联网的设备规模动辄千万量级，因此实体SIM在供应链管理及运维管理上也面临极大挑战。

因此，市场非常渴求eSIM。

市场对于eSIM的需求强烈，将会成为物联网领域的基础组件

物联网的应用特点，使得基于eSIM拥有巨大市场



传统SIM

eSIM

成本

硬件成本+产线工位，预计单颗模组成本增加8-10元，占模组成本的20%-30%

成本降低80%

体积

传统SIM需卡槽，体积巨大。焊接式SIM卡体积也达到3*3，较难满足MEMO类应用场景

体积减小90%~100%

性能

防水性差；需额外读卡电压，产生额外功耗

完全集成于半导体芯片内，各项物理性能得到加强，更适用于运行环境恶劣且服务周期长的物联网场景

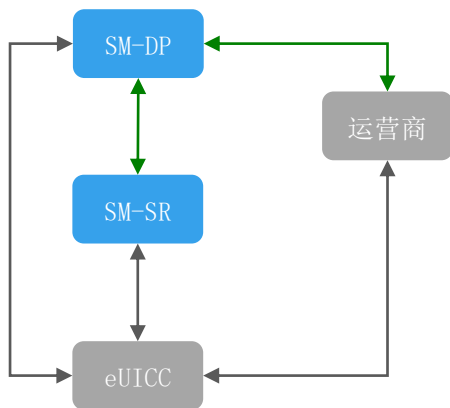
从多方面的市场诉求来看，eSIM模组更契合市场，拥有广阔的应用前景。

目前，中国电信联合果通科技与龙尚科技推出了基于eSIM的9500模组，支持NB/eMTC网络，成为全球首款eSIM模组



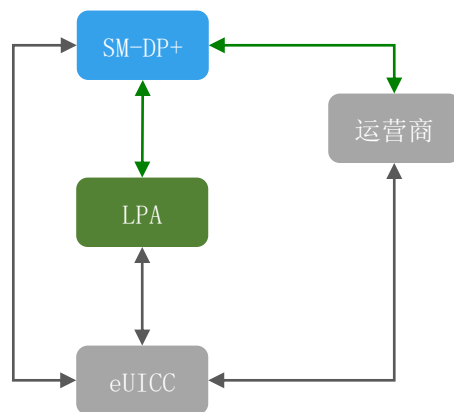
eSIM (eUICC) 是由GSMA (全球运营商联盟) 主导制定的eUICC (eSIM的一种应用方案) 规范按照行业应用场景的不同, 主要分为了M2M和消费电子两大规范, 方案如下:

M2M版本



M2M版本下, 明确由运营商主导控制SIM卡密通路: 初始SM-SR (运营商签约管理数据) 在生产阶段被预置 (初始运营商A), 未来需更换运营商B时, 需在运营商A同意的情况下, 双方配合更换SM-SR才能实现。

消费电子版本



消费电子版本的规范下, 用户可以通过LPA选择归属运营商或漫游运营商

eUICC

- 现有GSMA标准技术
- 安全级别较高EAL4+
- 目前主要应用于智能可穿戴领域，并逐步受到终端商的注意，是eSIM未来主要技术路径之一

iUICC

- 在通用功能芯片内集成安全模块单元，模拟实现SIM功能
- 安全级别未知

eSE SIM

- 基于硬件集成安全芯片技术
- 带NFC支付的终端均支持
- 应用于安全支付，金融行业认可
- 安全级别最高EAL6+

TEE SIM

- 基于ARM Trustzone技术
- 应用于指纹比对，安全支付等
- 果通正在进行EAL4+检测

eSIM是登入网络的安全凭证



eSIM是设备访问的安全入口



1

提供身份认证

作为用户设备身份认证和鉴权模块，提供用户设备接入移动网络的身份标识，完成网络接入的安全认证。

2

提供应用支撑

装载部分用户设备应用，满足物联网业务监控、定位指挥调度、数据采集和测量等方面的业务要求。

3

安全机制保证

利用智能卡安全保障能力，为用户网络接入、业务访问、数据传输、信息存储等功能提供安全机制等。

4

优化供应链管理

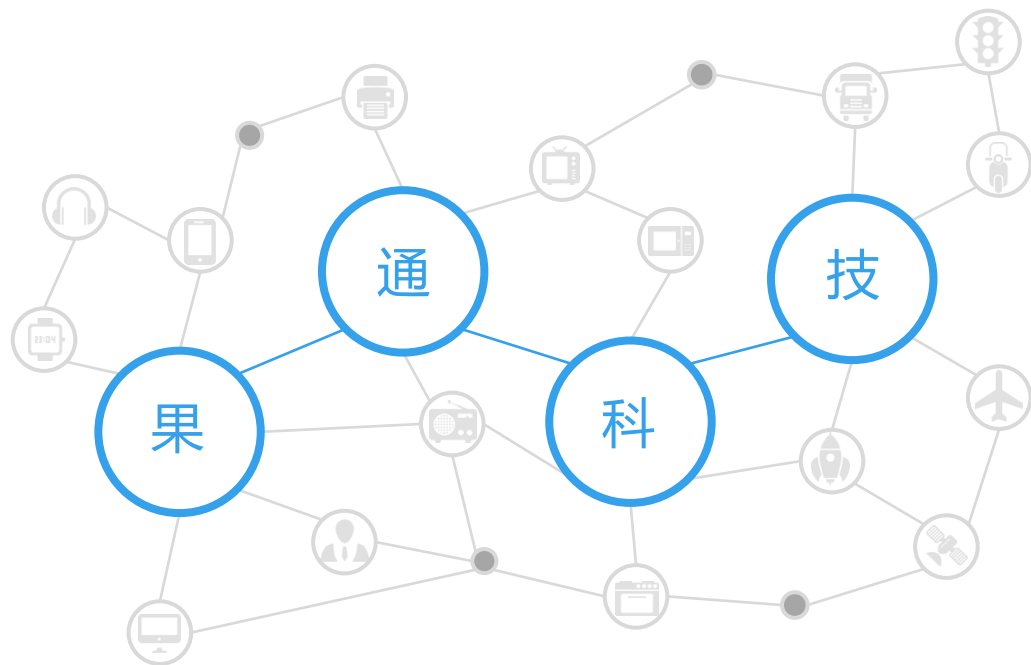
使用eSE SIM与TEE SIM，无需采购额外芯片，不存在供货周期问题，特别是针对车企，因供卡问题而导致的停产危机将得到解决

5

简化制造工艺

由于eSE SIM与TEE SIM是在固有硬件上进行软件模拟，因此无需额外工序进行芯片的安装

关于果通



Thank You

roam2free

2017.3