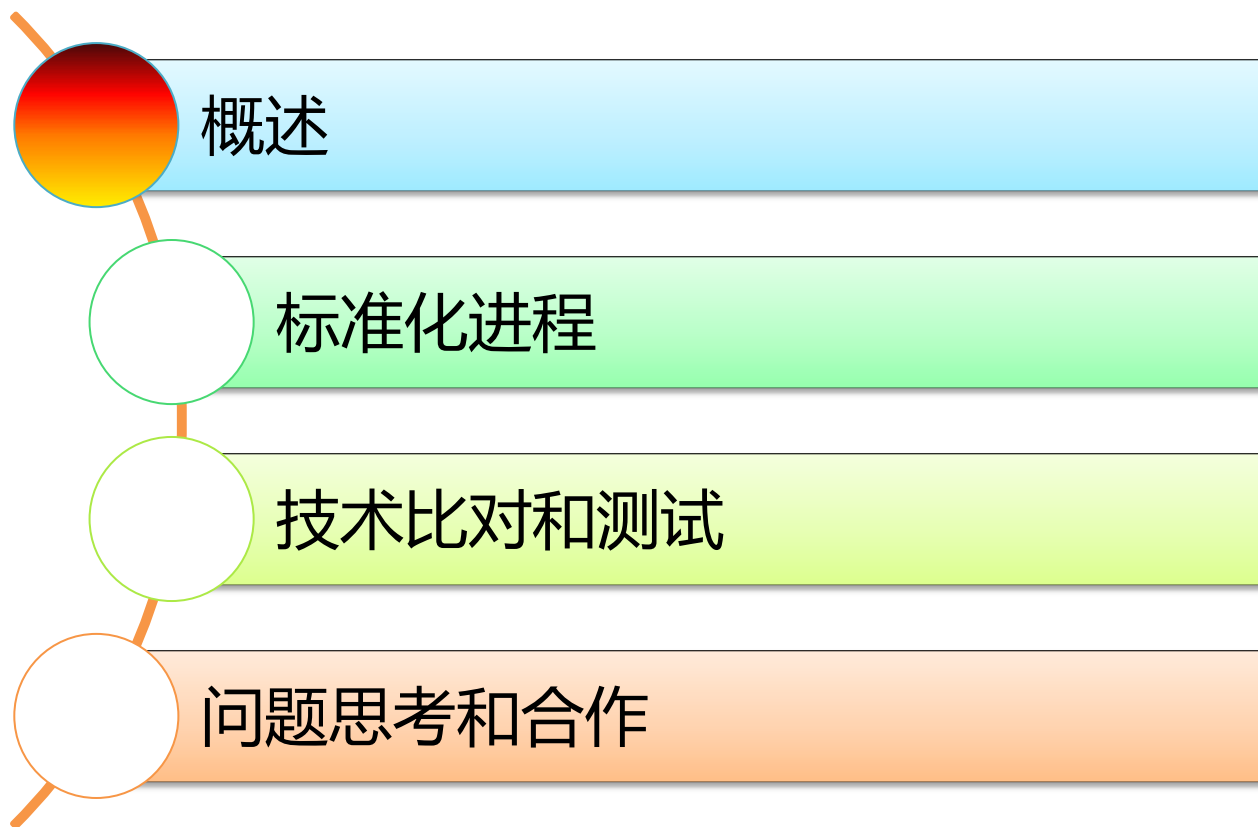


# eSIM技术及测试研究

中国信息通信研究院泰尔终端实验室  
移动终端性能部



# 卡片演进

小型化、高集成化趋势

1FF尺寸

12345A  
6789



2FF尺寸



3FF尺寸



4FF尺寸



# eSIM由来

## 源起物联网场景

- 使用环境严酷
- 使用场景成本
- 产品尺寸、工艺设计要求

## ETSI-eUICC

ETSI TS 102 671

ETSI TS 103 383

ETSI TS 103 384

MFF1/MFF2

even smaller

可包括贴片式  
(SMD)、直接封装  
于通信模块式 (SIP)

物理  
特性

## 用户市场需求丰富

- 用户签约便捷化需求
- 远程数据管理需求
- 通信业务资费市场化

## GSMA-eSIM

提出卡文件空中下载  
及可自由切换运营商

由M2M向消费电子市  
场、传统市场（手机  
/PAD）发展

软件  
特性

# eSIM特性

根据GSMA的定义，eSIM的特性可归纳为以下三点，

从目前的国内市场来看，eSIM是按照其3个特性，呈现阶段性、递进式的发展。



早前Apple SIM技术在其国外发售产品上的运用，引起了大众市场对eSIM的关注，“类eSIM”。

# eSIM技术实现方案

按照eSIM数据在终端上存储和调用激活的不同，目

前eSIM主要有两种技术实现方案：

- 所用的eUICC安全芯片通常由SIM卡商提供
- 存在独立物理硬件
- 安全性上，相对于划分通用安全存储区的方案要更受认可

通过终端内置独立SE  
芯片存储和使用



- 利用非卡商提供的通用芯片安全存储区来封装eSIM数据，通过相应的控制程序来调用
- 可用于存储eSIM文件外，还可用于移动支付、移动办公、数字版权保护等数据和密钥存储
- 应用领域较灵活，通常厂家可在进网后通过软件升级提供更多的服务。

终端CPU划分通用安全  
存储区存储和使用

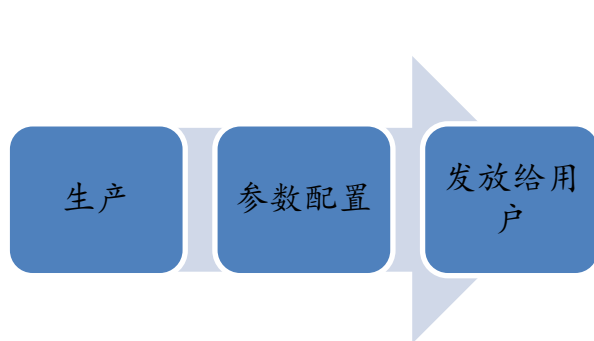
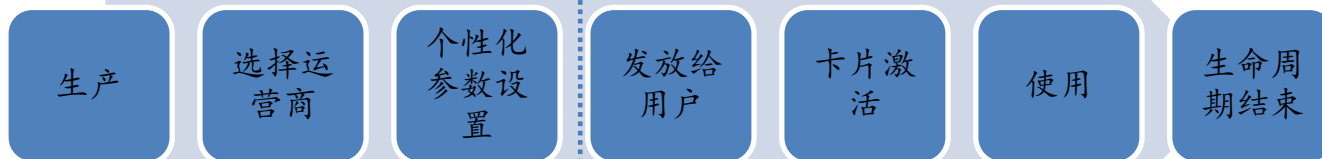


# eSIM与传统电信卡对比—生命周期

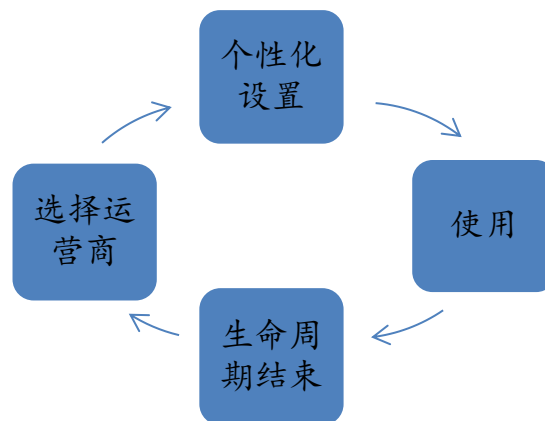
发行前

发行后

传统电信卡



eSIM



# eSIM与传统电信卡对比—业务模式

下图为早期我们分析的eSIM可能带来的几种业务运营模式的可能，但目前来看，既有尝试方案仍然均是由运营商负责eSIM卡的运营和管理。

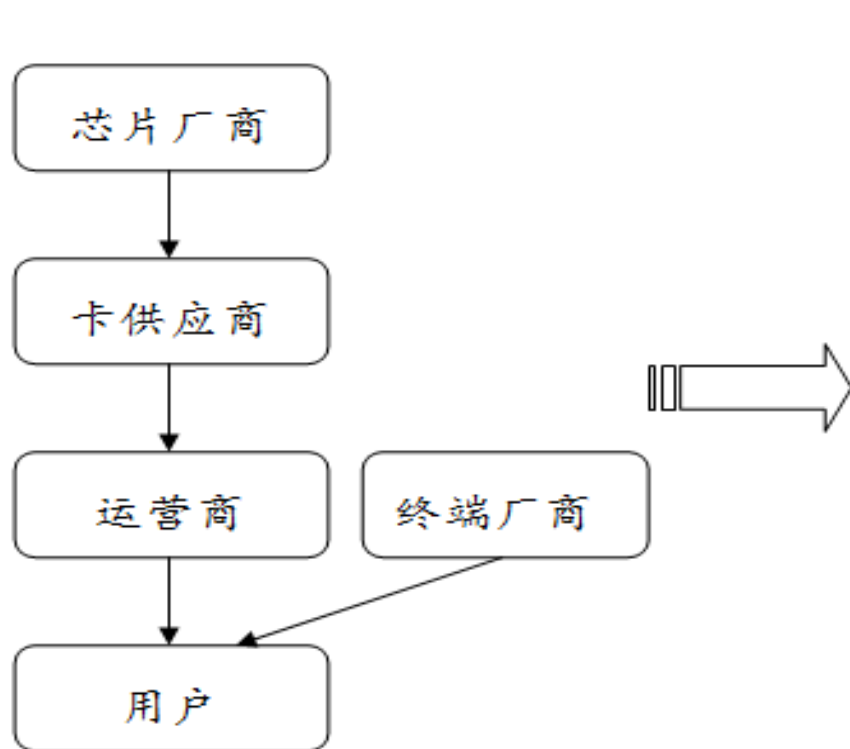


图 1：传统 SIM 业务模式

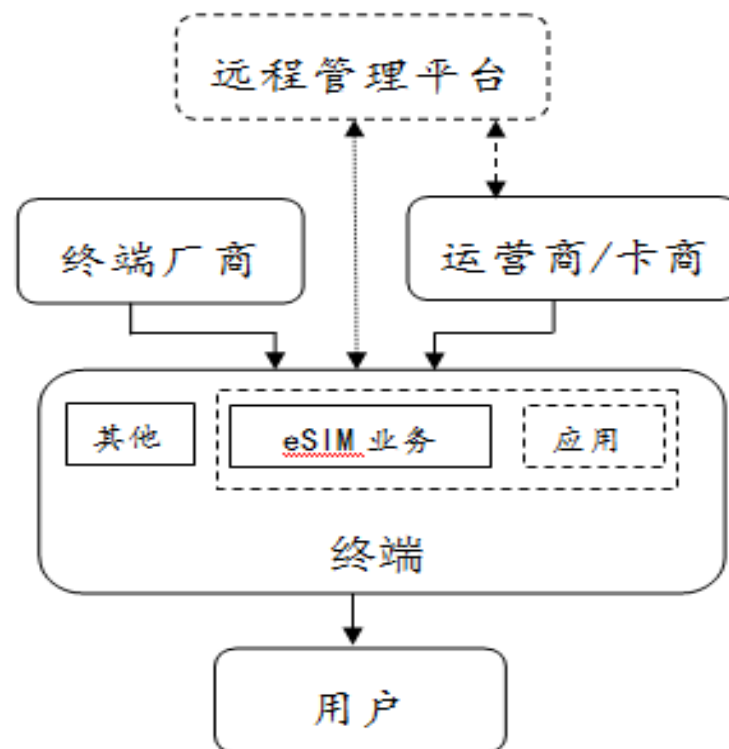
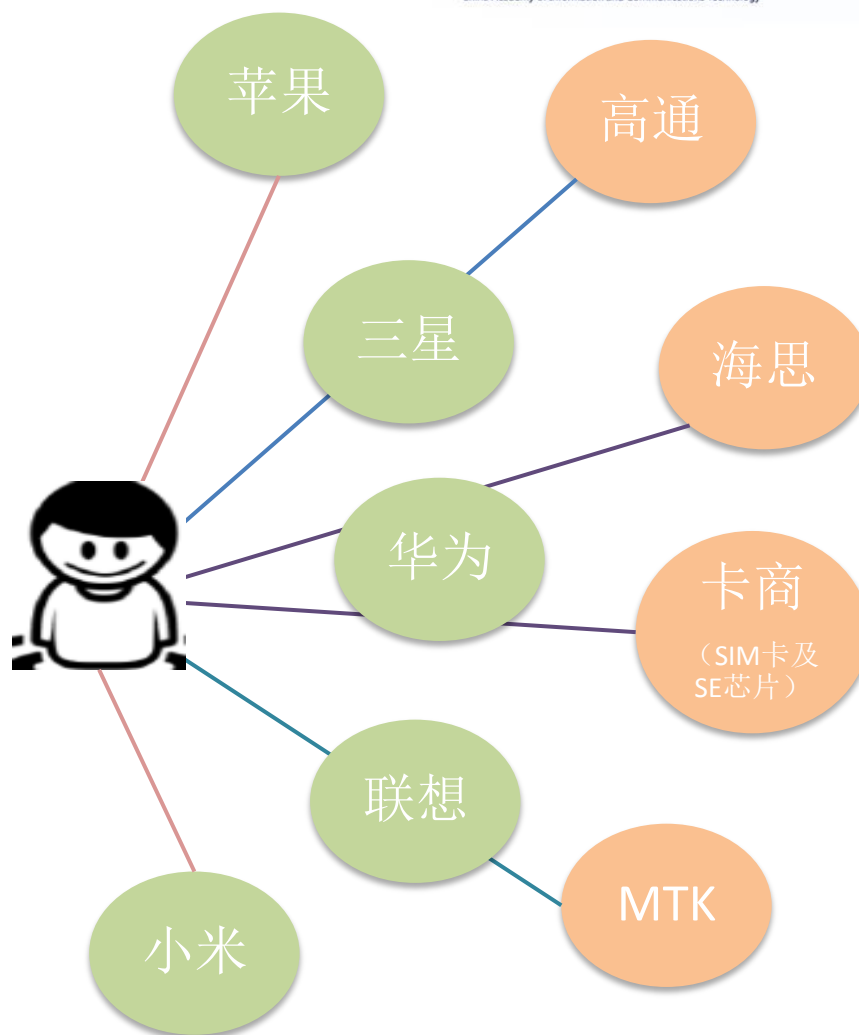
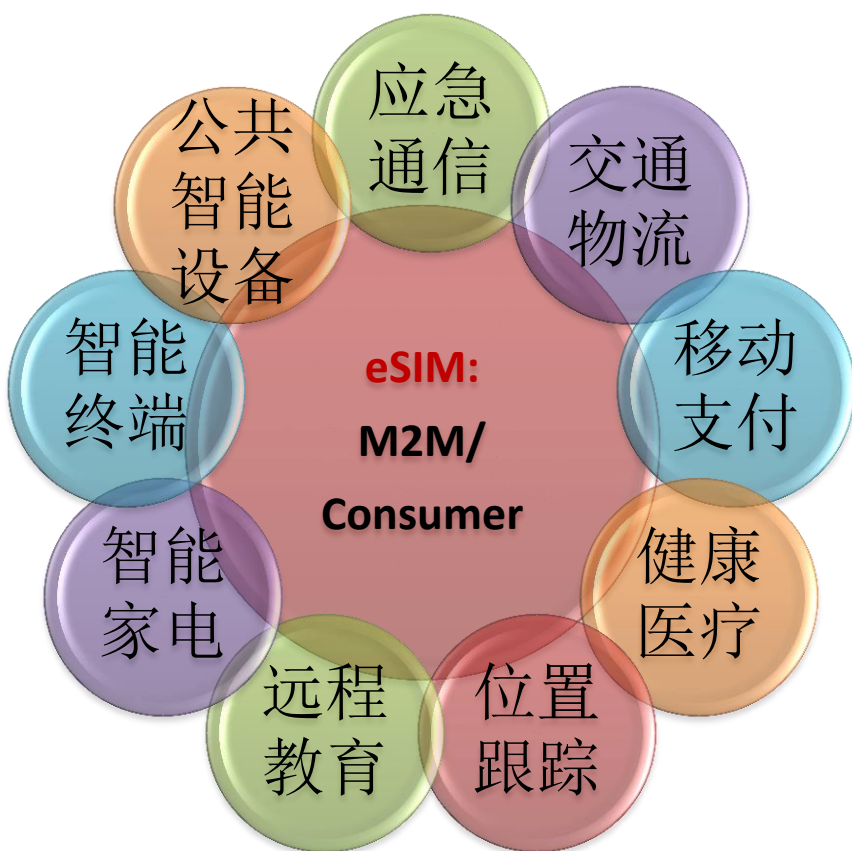


图 2：eSIM 业务模式

# 应用示例





# eSIM标准化组织



# GSMA标准最新进展

## GSMA Standards for eSIM Version&Date

|          | Architecture             | Technical Specification | Test Specification      |
|----------|--------------------------|-------------------------|-------------------------|
| M2M      | SGP.01<br>V1.12-20140130 | SGP.02<br>V3.1-20160527 | SGP.11<br>V3.1-20160531 |
| Consumer | SGP.21<br>V2.0-20160823  | SGP.22<br>V2.0-20161014 | TBD                     |

考虑融合，时间点预计2017年？

# CCSA标准最新进展

CCSA的eSIM标准主要是参考了GSMA的规范：

## CCSA Standards for eSIM-M2M

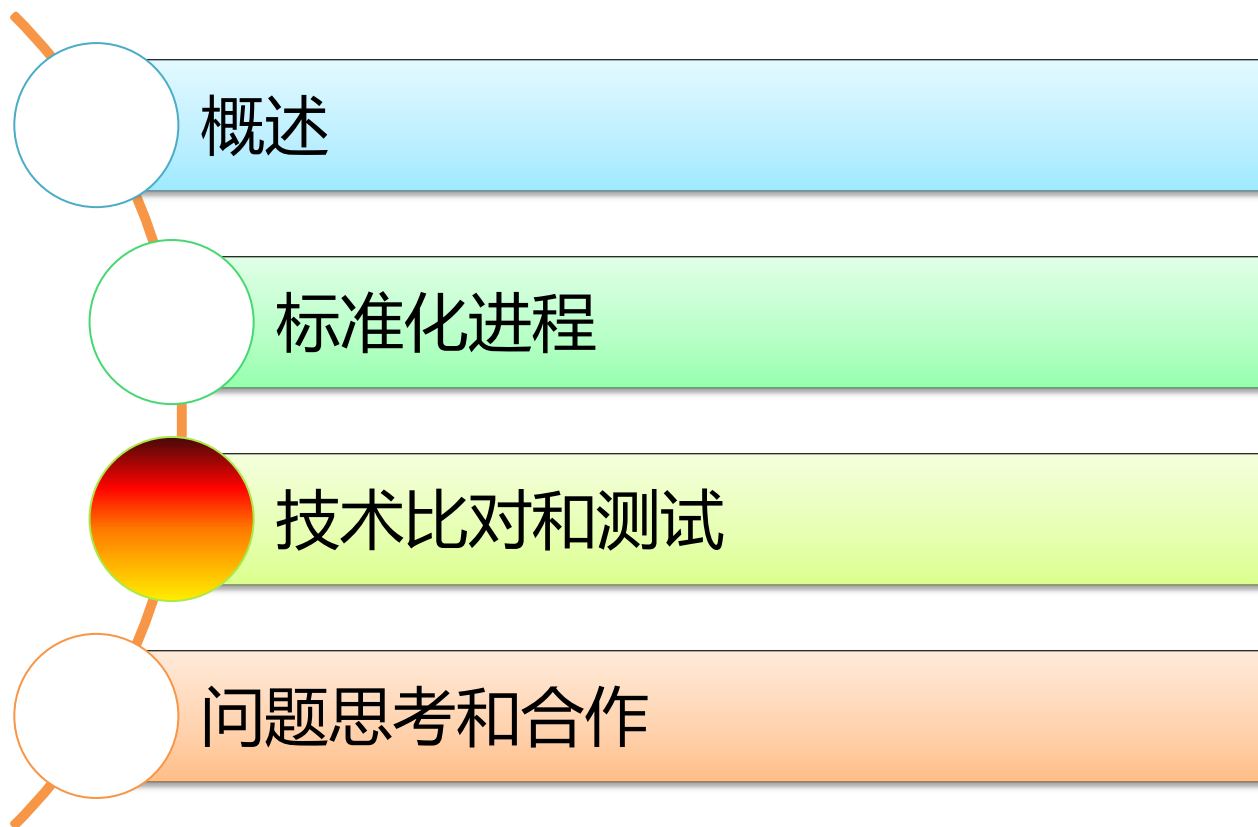
| 标准组/ 类型       | 标准名称                                                | 标准状态                                          |
|---------------|-----------------------------------------------------|-----------------------------------------------|
| TC8WG2<br>行标  | YD/T 2845-2015<br>嵌入式通用集成电路卡(eUICC)及其远程管理的安全技术要求    | 已发布                                           |
| TC10WG4<br>行标 | YD/T 2926-2015<br>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） | 2015版已发布，20160825申请按照SGP.02-V3.1新版本修订，修订稿讨论状态 |
| TC10WG4<br>行标 | 嵌入式通用集成电路卡(eUICC)远程管理平台测试方法（第一阶段）                   | 与YD/T 2926-2015配套使用版本在报批状态，但此标准同样需要修订         |
| TC10WG4<br>行标 | 支持远程管理的嵌入式通用集成电路卡(eUICC)技术要求                        | 已报批                                           |
| TC10WG4<br>行标 | 支持远程管理的嵌入式通用集成电路卡(eUICC)测试方法（第一阶段）                  | 在研，201608提交第一次草案稿                             |

# CCSA标准最新进展

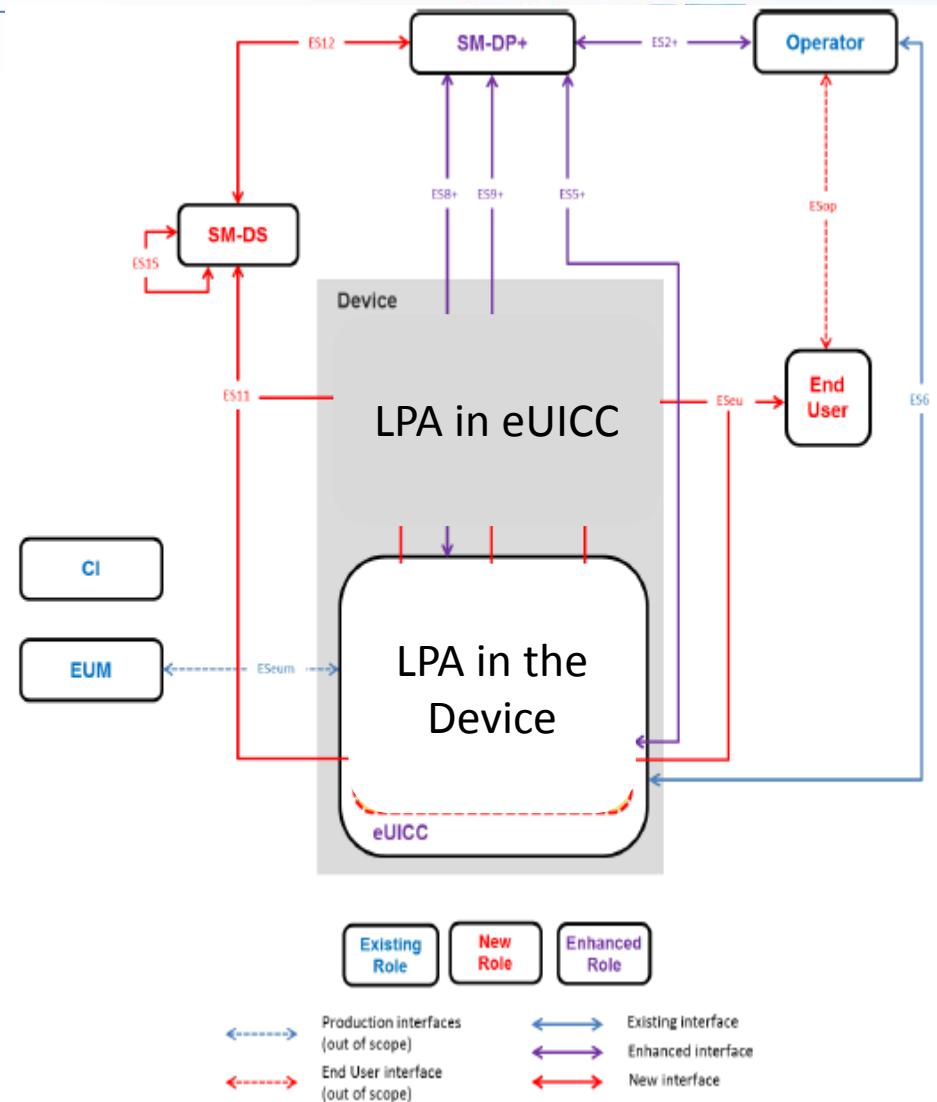
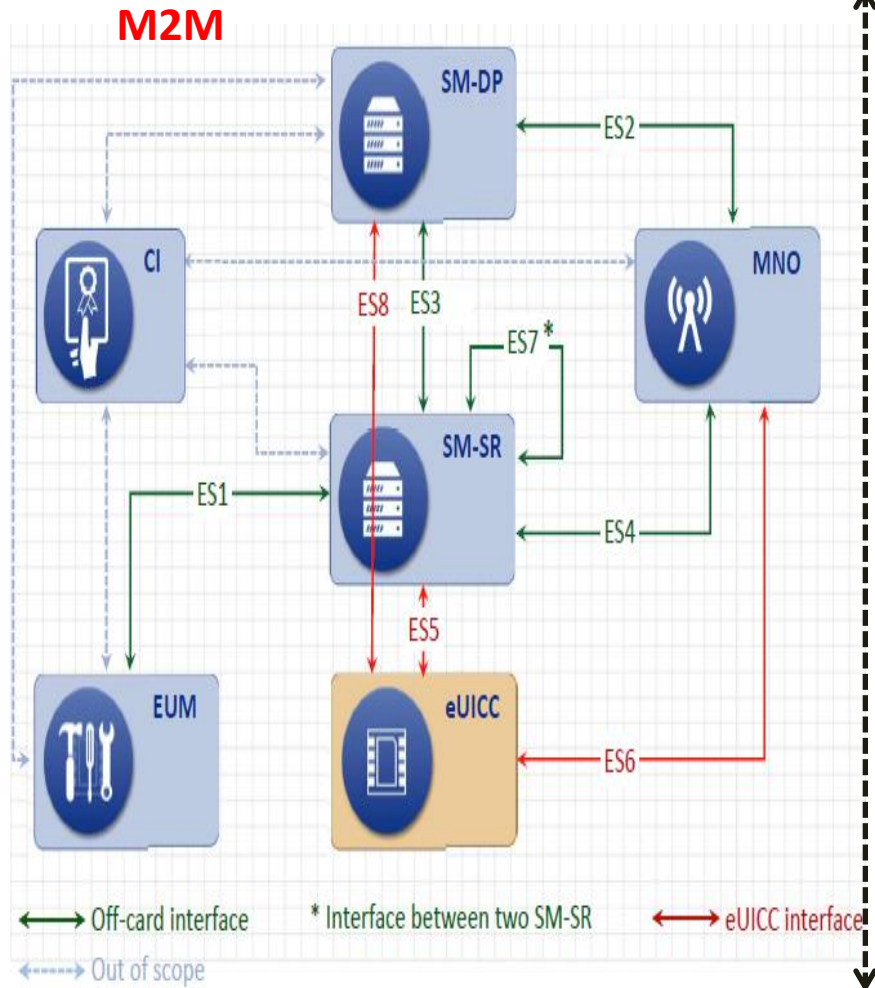
CCSA的eSIM标准主要是参考了GSMA的规范：

## CCSA Standards for eSIM-Consumer

| 标准组/ 类型        | 标准名称                 | 标准状态                      |
|----------------|----------------------|---------------------------|
| TC5WG9<br>研究课题 | 消费电子终端eSIM远程配置架构研究   | 201609已结题                 |
| TC11WG3<br>行标  | 可远程配置的物联网eSIM卡技术要求   | 201606新立项，将面向消费电子领域，名字需改变 |
| TC11WG1<br>行标  | 物联网eSIM远程配置平台技术要求    | 201606新立项，将面向消费电子领域，名字需改变 |
| TC11WG3<br>行标  | 支持远程SIM配置的消费电子终端技术要求 | 201609新立项，需和卡技术要求标准协调编制   |



# M2M VS Consumer-RSP架构



**Consumer**

# M2M VS Consumer-RSP架构实体单元

| M2M   | Consumer         | Description                             |
|-------|------------------|-----------------------------------------|
| eUCC  | eUICC            | Embedded UICC                           |
| MNO   | Operator         | Embedded UICC                           |
| SM-DP |                  | Subscription Manager Data Preparation   |
|       | SM-DP+           | Subscription Manager Data Preparation + |
| SM-SR |                  | Subscription Manager Secure Routing     |
|       | Device           | User equipment                          |
|       | LPA(LDS/LPD/LUI) | Local Profile Assistant Unit            |
|       | SM-DS            | Subscription Manager Discovery Service  |
| EUM   | EUM              | eUICC Manufacturer                      |
|       | End-user         | End User                                |
| CI    | CI               | Certificate Issuer                      |

# M2M VS Consumer-已定义接口

| M2M | Consumer                 | Description                            |
|-----|--------------------------|----------------------------------------|
| ES1 |                          | EUM – SM-SR Interface                  |
| ES2 |                          | MNO – SM-DP Interface                  |
|     | ES2+                     | Operator – SM-DP+ Interface            |
| ES3 |                          | SM-DP to SM-SR Link Establishment      |
| ES4 |                          | MNO – SM-SR Interface                  |
| ES5 |                          | SM-SR – eUICC(ISD-R) Communication     |
|     | ES5+ (LPA in the eUICC)  | SM-DP+ – LPA Interface                 |
| ES6 | ES6                      | MNO/Operator – eUICC(MNO-SD) Interface |
| ES7 |                          | SM-SR – SM-SR Interface                |
| ES8 |                          | SM-DP – eUICC(ISD-P) Interface         |
|     | ES8+                     | SM-DP+ – eUICC Interface               |
|     | ES9+ (LPA in the Device) | LPA (LPD)– SM-DP+ Interface            |
|     | ES10(a/b/c)              | LDS/LPD/LUI)– LPA Services Interface   |
|     | ES11                     | LDS – SM-DS Interface                  |
|     | ES12                     | SM-DP+ – SM-DS Interface               |
|     | ES15                     | SM-DS – SM-DS Interface                |

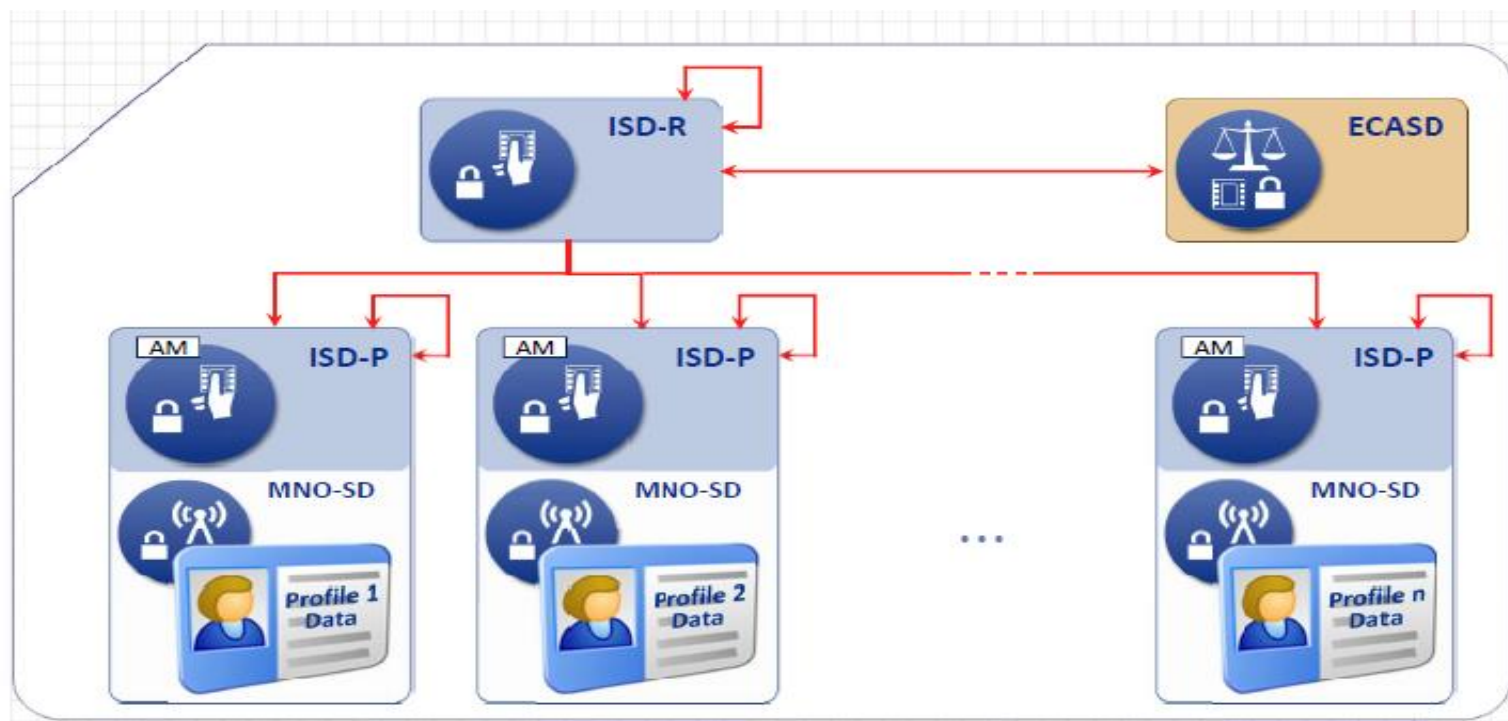
# M2M VS Consumer-未定义接口

从完整性出发，RSP架构中还有GSMA标准中未定义的接口：

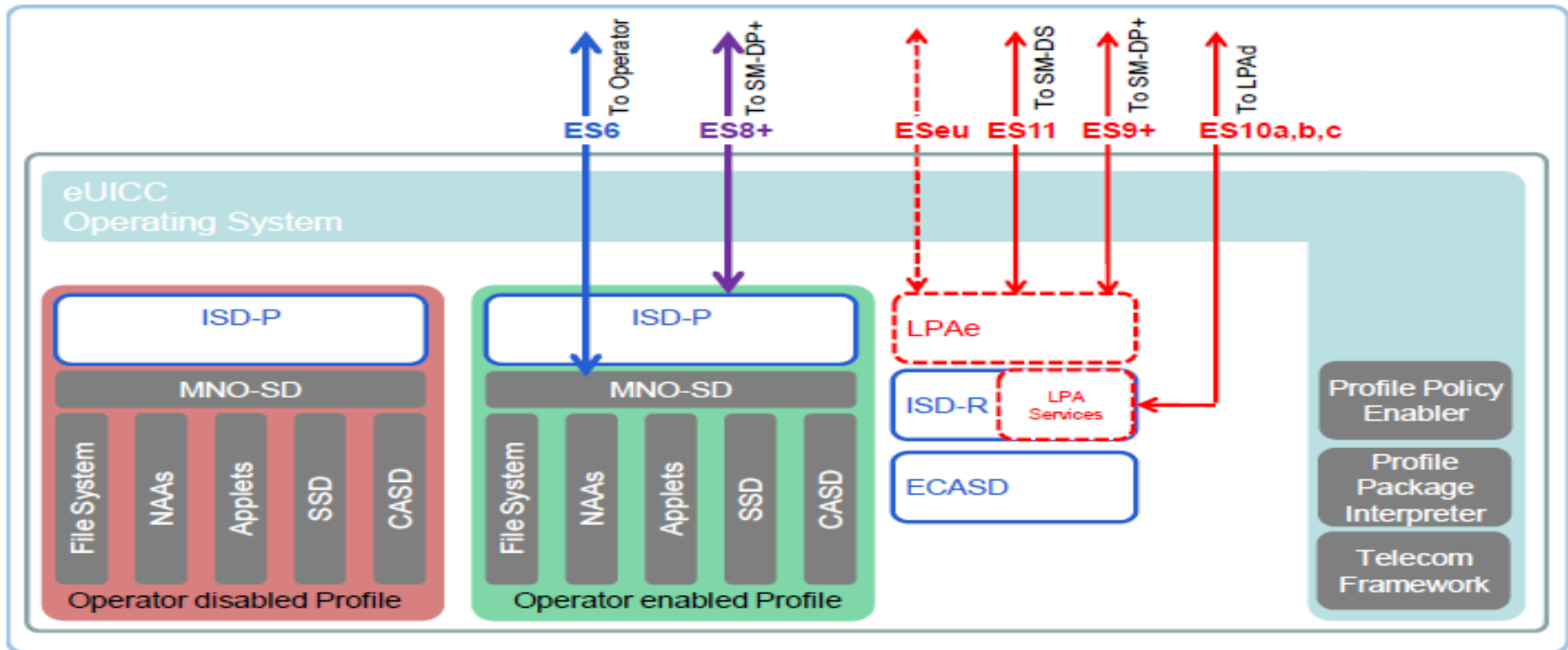
| M2M | Consumer | Description                   |
|-----|----------|-------------------------------|
| ND  |          | EUM – SM-DP Interface         |
| ND  |          | CI – SM-DP Interface          |
| ND  |          | CI – SM-SR Interface          |
| ND  |          | CI –MNO Interface             |
| ND  |          | CI – EUM Interface            |
|     | ESop     | Operator – End User Interface |
|     | ESeu     | End User - LUI Interface      |
|     | ESeum    | EUM – eUICC Interface         |

# M2M VS Consumer-eUICC架构

## M2M



# M2M VS Consumer-eUICC架构



Consumer

# M2M VS Consumer-eUICC实体单元

| M2M    | Consumer                    | Description                                                                     |
|--------|-----------------------------|---------------------------------------------------------------------------------|
| ISD-R  | ISD-R                       | Issuer Security Domain Root                                                     |
|        | LPA Services                | LPA (ISD-R) services on the eUICC                                               |
| ECASD  | ECASD                       | eUICC Controlling Authority Security Domain                                     |
| ISD-P  | ISD-P                       | Issuer Security Domain Profile                                                  |
| MNO-SD | MNO-SD                      | Mobile Network Operator Security Domain                                         |
|        | Profile Policy Enabler      | Verification the authentication by RAT and enforcement of the PPRs of a Profile |
|        | Profile Package Interpreter | Profile Package Interpreter as part of the eUICC OS                             |
|        | Telecom Framework           | Telecom Framework as part of the eUICC OS                                       |

# 测试

- ✓ 安全性 网元实体 接口 数据
- ✓ 终端 能力要求 标准一致性 功能应用 兼容性
- ✓ 卡 接口一致性、卡行为 平台系统行为

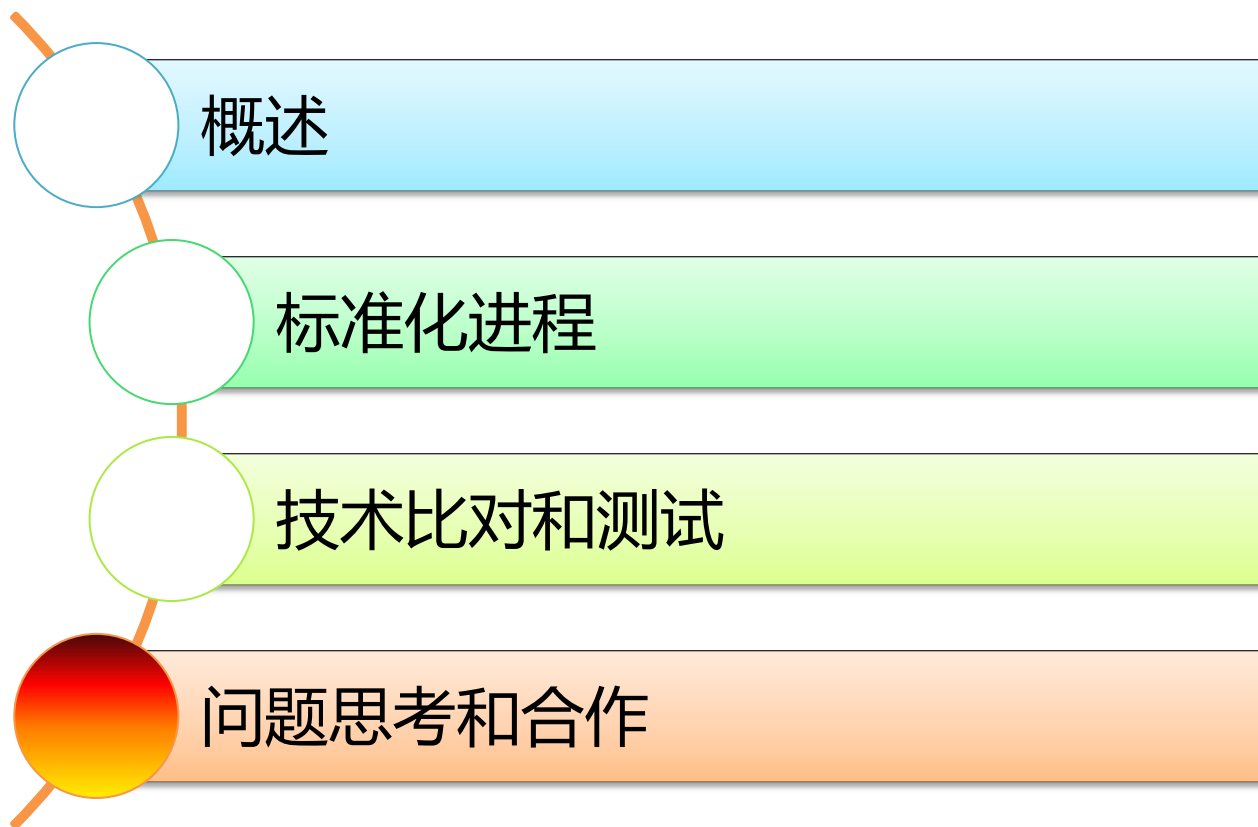


GP测试eUICC架构

- 当前套件开发依据限为M2M规范；
- 测试套件开发依据GSMA规范；
- 仪表厂商依据GP要求开发测试工具并申请GP认证。

# 进网设备目录

---



# 思考和建议

## 技术安全保证

1. 数据传输安全
2. 数据存储安全
3. eUICC\终端\RSP平台实体安全

## 符合国内法律法规

1. 落实实名制要求
2. 关注码号管理应法规要求，如“同一用户在同一家电信企业办理电话卡不超过5张”

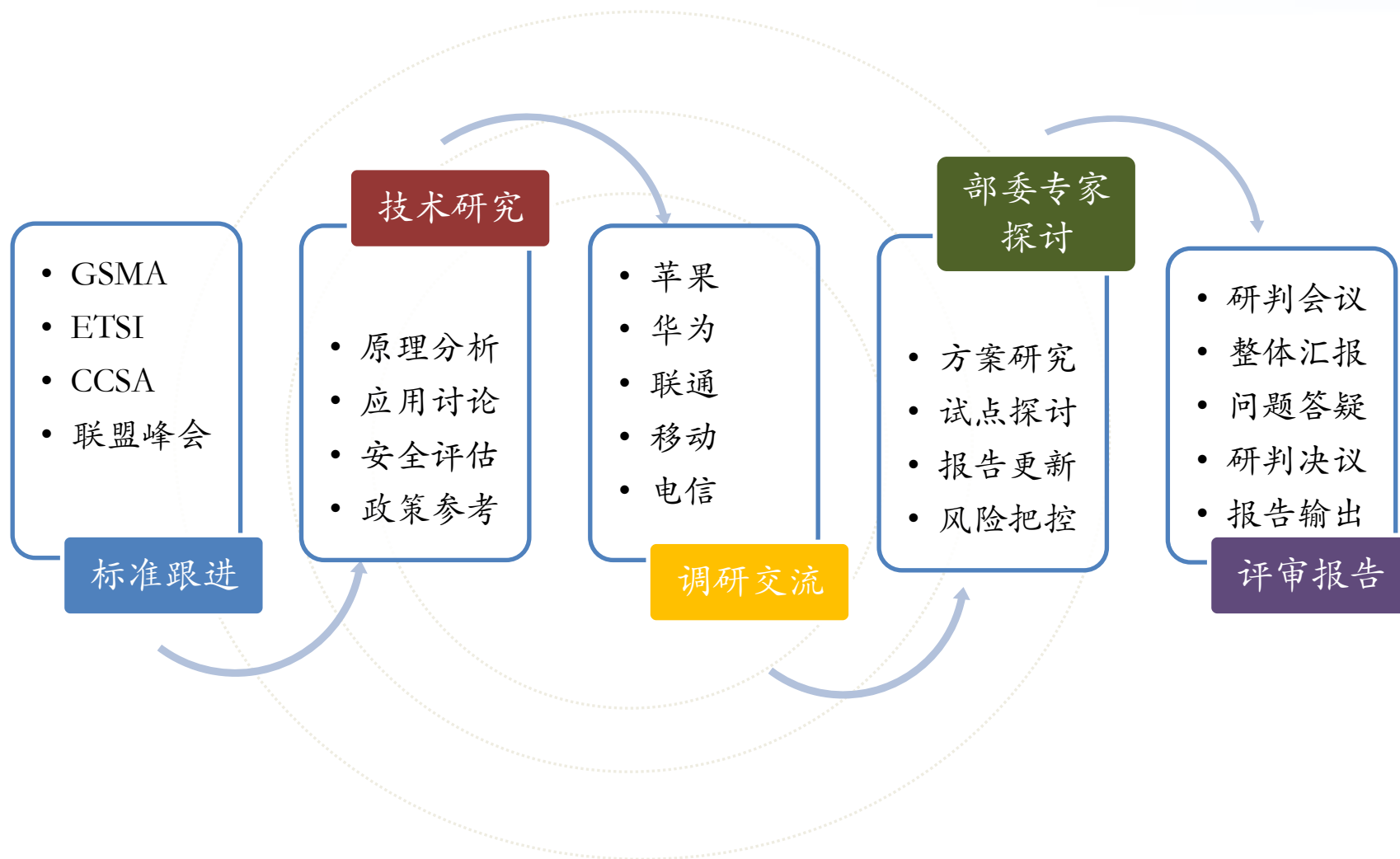
## 兼容性

1. 考虑平台对不同终端的兼容性
2. 考虑终端对不同卡商/CI的兼容性
3. 合理设计通信方案，厘清网络信令流程，谨防电信诈骗

## 兼顾其他安全需求

1. 考虑对特殊通信的影响，考虑终端和位置信息的可溯源
2. 对于当前不太可控的业务支持能力需多加考虑，如漫游功能

# 我们的工作



# 期待您的加入



# 敬请批评指正！

郑海霞 [zhenghaixia@caict.ac.cn](mailto:zhenghaixia@caict.ac.cn)