RFID 与移动终端相结合的 SMAP 技术

石亦欣 复旦大学专用集成电路与系统国家重点实验室

李蔚 王元彪 上海复旦微电子股份有限公司

摘要：

移动通讯技术和 RFID 技术近年来发展非常迅速，在 NFC（近场通讯）的概念提出之后，移动通讯和 RFID 技术的相互融合趋势逐渐加快，但作为一机多用，其发展的困难和障碍是巨大的。本文提出和阐述了一种的平衡渐进发展的智能移动应用平台 SMAP（Smart Mobile Application Platform）解决方案，适合于 RFID 与移动终端应用相互融合及发展。

关键词： RFID（电子标签） SMAP（智能移动应用平台） NFC（近场通讯）

1. 概述

IC 卡特别是非接触 IC 卡/RFID（以下将非接触 IC 卡及 RFID 统称为 RFID）经过十多年的发展，已深入现代生活的各个角落，被广泛应用于公交、门禁、小额电子支付等领域。近年来，在轨道交通、物流管理、物品防伪、身份识别等需求推动下，RFID 技术的不断进步，应用越来越普及，迫切需要各类 RFID 识别设备。与此同时，移动通讯终端经历 20 多年的迅速发展，已经几乎成为居民人手俱备的随身装置，普及率非常高，并且有向移动终端集成更多功能的趋势。

如果说 80－90 年代推动半导体行业发展的杀手级应用是 PC，90－2000 年代推动半导体行业发展的杀手级应用是手机的话，那么在最近十多年可能成为新杀手级应用的将是结合移动终端与 RFID 技术的一机（卡）多用。特别是在 3G 时代，具有无线连接功能无处不在的 RFID 读写器与非接触式应用的 RFID 将是重点中的重点。目前业界主要有两套基于非接触技术的解决方案：Combi SIM 卡方案和 NFC（Near Field Communication）方案。

Combi SIM（又称 Dual Interface 双界面）卡方案指通过更换手机内部 SIM，取代以 Combi SIM 卡，在保留原接触界面的 SIM 卡功能基础上增加非接触 IC 卡应用界面。Combi SIM 卡方案在手机中增加了非接触 IC 卡的功能，但没有实现读写器和双工通讯功能。

NFC(Near Field Communication 近场通讯)是这几年飞速发展的一种新兴技术，由 Sony、Philips 和 Nokia 提出，它使得两个电子设备直接可以进行短程的通讯，工作在 13.56MHz 频段，工作距离几个厘米。NFC 技术目标是电子设备之间的近距离通讯，在实际推广过程中面临诸多困难，目前将其主要应用领域集中在近距离支付应用方面，并正在寻求 NFC 技术与

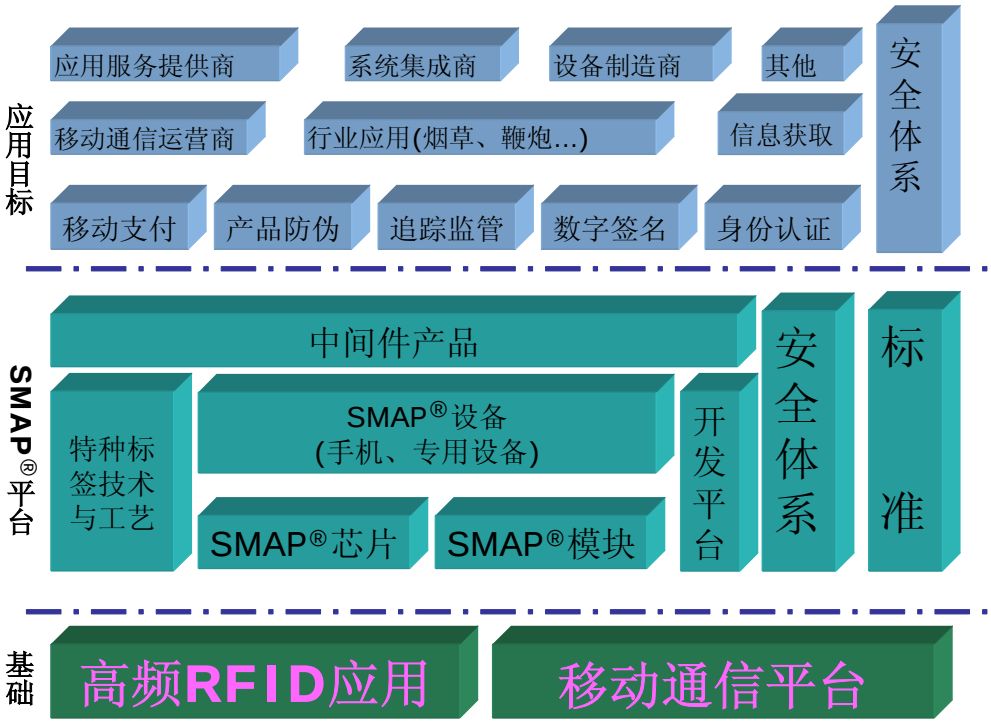
SIM 的关联方案。

上述两种方案尽管技术上都可行，但对于一机（卡）多用来说，核心是如何理顺移动设备制造商、移动服务运营商和应用服务运营商之间的关系，在这股跨行业的新应用整合中，需要一种平衡的、兼顾各方利用的渐进式方案。本文提出的 SMAP（智能移动应用平台）解决方案，可以适用于移动支付、产品防伪、追踪监管、数字签名、身份认证和信息获取等多类应用，是移动终端与 RFID 结合的一种平衡演进之路。

2. SMAP 平台及其应用的体系结构

2.1. SMAP 平台的体系结构

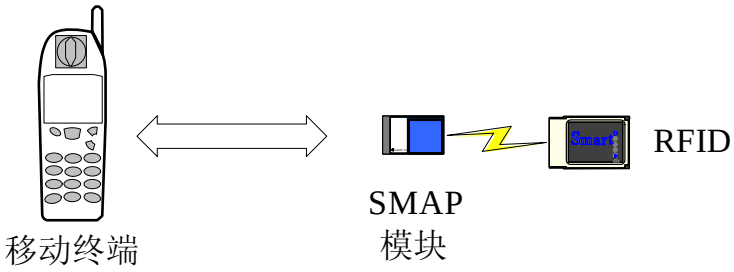
SMAP 平台构建在现有的非接触式 IC 卡应用和移动通信应用的基础上，进一步集成各种应用环境和安全体系，形成更小型的、更安全的、价格更低廉的和更便捷的高频 RFID 应用环境，SMAP 平台的结构框图如下：



在 SMAP 平台的体系结构中，SMAP 模块(芯片)、安全体系和中间件产品构成了其核心内容，这里定义 SMAP 模块(芯片)为具有安全体系的、可以进行应用导入的、对外通过中间件提供服务的高频 RFID 应用产品。

2.2. SMAP 平台的架构

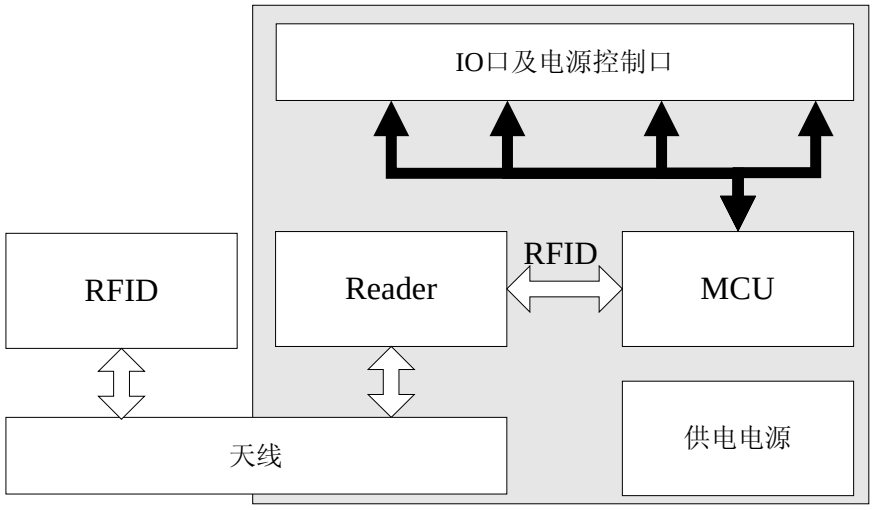
如前所述，SMAP 平台是针对移动终端与 RFID 应用结合的解决方案，其基本的架构为移动通信终端＋SMAP 模块＋RFID，如下图所示：



SMAP 模块通过接口电路与移动通信终端集成在一起，RFID 也被集成在移动终端上，其中 RFID 可以是单列的独立部分，也可以与 SMAP 模块集成在一起。单列的独立 RFID 可以接受 SMAP 模块的射频操作，这样做的目的是能很好地兼顾现状。正如前面所述，以非接触 IC 卡为技术核心的一卡通技术在我国得到了广泛的应用，典型和成熟的应用行业如公交一卡通、校园一卡通等，刷卡消费作为一种小额消费在这些行业广为接收，并且已经形成了事实上的利益关系。另一方面，在我国的现行制度规定下，除了银行及其相关单位之外，其他单位要发行带金卡具有很大的制度上的障碍。因此，在移动支付业务中，RFID 作为一种独立的方式出现，既能够保证移动支付业务的实施，又能够兼顾已发卡方的利益关系，同时针对新发卡还可以直接采用银行卡，以规避政策风险。

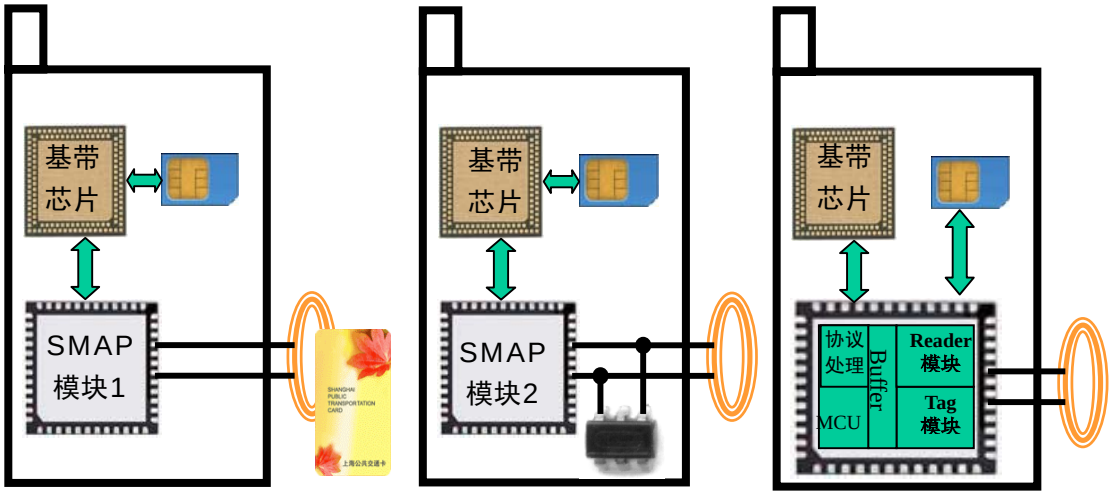
2.3. SMAP 模块的发展路线

在上述应用的体系结构中，其核心是 SMAP 模块，目前状态下，SMAP 模块是内置安全特性和应用流程的多芯片模块，该模块的结构如下图所示：



其中，SMAP 模块由 3 块芯片及若干分立元件组成，核心芯片为主控 MCU，包含 IO 接口及电源管理控制接口；Reader 为通用 RFID 读写器，支持访问 13.56MHz 频段下的 ISO14443 type A，type B 标准及 ISO15693 标准的产品；RFID 为独立的电子标签模块，其可以独立封装天线，通过射频耦合与 Reader 通讯，也可以与模块集成在一起，共享一副天线。

如前所述，对于一机（卡）多用来说，核心是如何理顺移动设备制造商、移动服务运营商和应用服务运营商之间的关系。，跨行业的应用整合，需要采用一种平衡的、渐进的、兼顾各方利用的方案逐步演进。下图演示了 SMAP 方案的发展路线。



RFID 分立的 SMAP 方案　　天线共享 SMAP 方案　　单芯片 SMAP 方案

第一种方案是采用独立 RFID 的 SMAP 模块方案，该方案优点是独立 RFID 可以低障碍地引入现有的非接触应用运营商，发行和应用模式几乎保持不变，支持非接触的掉电应用模式，该方案适用于该类新应用初期概念的试点期；第二种方案是 RFID 与 SMAP 模块集成在一起，共用一副天线，方案二与方案一实现的功能相同，优点是减小独立 RFID 标签尺寸对手持移动终端的外观设计影响，但需要应用运营商与移动运营商、手机制造商之间的配合，该方案适合于一机多用的推广期；第三种方案则真正将 SMAP 模块集成为一颗单芯片，支持 ISO18092 标准，并将 SMAP 应用与 SIM 进行关联，是在前两种方案试运行后根据市场的反馈而推出的真正大规模推广的解决方案。

3. 安全体系

在 SMAP 的应用过程中，安全性是最基本也是最重要的要求。特别是移动支付应用，根据 PBOC2.0 的要求，在支付过程中，应该根据不同的交易类型，实现联机或脱机的交易认证。对于其他种类的 SMAP 应用，例如产品防伪、追踪监管等，就其安全体系来说，事实上就是一个数据加解密的过程。

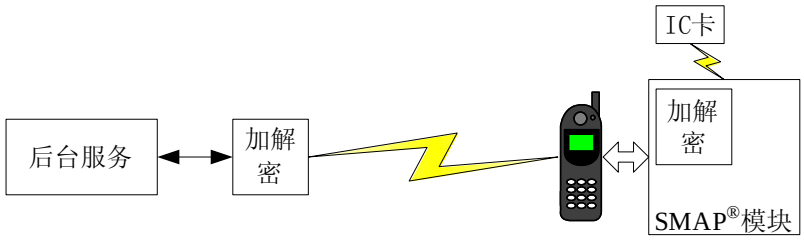
在 SMAP 不同的应用中，IC 卡(RFID)主要有两种不同的产品：一般的逻辑加密卡或者 CPU 卡。一般来说，对于 CPU 卡，终端只是在用户卡与后台或 PSAM 卡之间传递认证数据，无须获得用户卡的密钥。密钥存储在后台或 PSAM 卡中，在交易过程中通过分散算法计算出用户卡的密钥，并进一步计算出相关的交易认证数据输出或对输入进行验证，系统的安全体系与终端是不相关的。在目前的非接触逻辑加密卡的应用中，由于卡片没有运算能力，终

端必须通过对读写模块加载密钥才能实现对卡片的读写，因此如何保证密钥在传输过程中的安全性，是保证卡片安全交易的关键。

SMAP 应用的安全体系支持三种模式：

1. 第一种模式：后台密钥支持体系

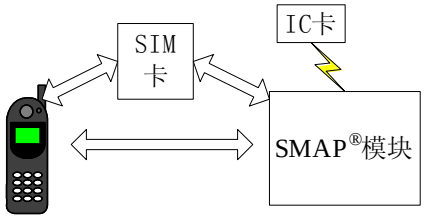
此种方式下，所有的密钥被放置在应用服务提供商的后台服务器上，由后台服务器向前端应用提供实时的密钥服务，其基本的过程如下图所示：



在每次交易时，终端向后台申请分散后的卡片密钥密文，传送给 SMAP 模块，由模块解密后使用。一般来说，应用服务提供商比较倾向于这种模式。应用开始之前，用户需要向应用服务提供商提出应用申请，由应用服务提供商完成对用户终端的初始化(如应用程序导入)工作，在每次的应用中，后台服务和用户终端之间还有一个相互认证的过程，以确定后台服务和用户终端对于对方来说都是合法的。

2. 第二种模式：采用本地 SIM 卡作为 SAM 卡的安全体系

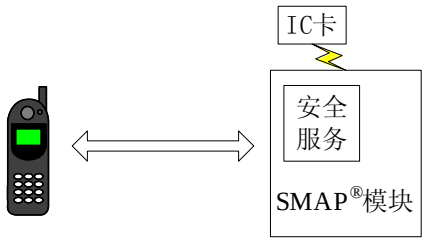
此种方式下，密钥被放置在移动终端的 SIM 卡中，SMAP 模块在需要时，向 SIM 卡申请密钥服务。此种方式的基本结构和过程如下图所示：



此种方案的应用初始化工作由移动通信运营商负责提供，其初始化的过程就是在 SIM 卡中增加应用所需要的密钥以及在 SMAP 模块中导入应用程序。

3. 第三种模式：内部模拟 SAM 卡的安全体系

此种方式下，密钥被放置在 SMAP 模块的内部，SMAP 模块在需要时，由内置的安全服务计算出访问 IC 卡的密钥。此种方式的基本结构和过程如下图所示：



此种方案的应用初始化工作由应用服务提供商负责提供，其初始化的过程主要是在SMAP 模块中导入密钥及应用程序。

三种模式的优缺点比较如下：

比较的内容	模式一	模式二	模式三
优点	易于为运营商所接受	利用 SIM 卡，成本低，移动通信运营商愿意大力推广	成本低，速度快
缺点	速度慢，有通信费用	需要说服其他应用服务提供商接受	需要得到运营商的认可

4. SIM 卡与 SMAP 应用的关联

在 IC 应用领域中，一卡多用的推广是十分困难的，而 SMAP 应用领域更是涉及包括移动运营商、终端设备制造商在内的各类 RFID 应用运营商，为了更好的推广 SMAP 应用，需要一个相对独立的运营商负责 RFID 应用的发行管理。移动运营商的地位相对超脱，对一机多用的推广起着举足轻重的作用，需要给移动运营商一定的手段将 SIM 卡与 SMAP 应用关联起来。

在 NFC 技术解决方案中，目前讨论的焦点是单线协议 SWP（Single Wire Protocol）。SWP 利用 SIM 卡 7816 接口中的 C6（原 VPP 高压编程脚，现已失去作用）引进，利用电压和电流的变化实现 SIM 卡与 NFC 射频模块的通讯，从而将 SIM 卡与 NFC 应用关联。由于 SWP 协议标准仍在制定过程中，暂时没有现成产品。并且 SWP 要求 SIM 卡芯片和 NFC 芯片都要改动设计，涉及面比较广。

SMAP 解决方案中，在 SMAP 模块中保留了完整的符合 ISO14443 标准的非接触式 CPU 卡芯片，因此不需要像 NFC 方案那样要求上位机提供 RFID 的模拟波形，自己可以独立完成非接触标签应用。而 RFID 的应用是和安全认证联系在一起的，因此 SIM 卡可以利用认证密钥来关联 RFID 应用。SMAP 模块中的非接触 CPU 的 COS 在开机后首先要与 SIM 之间进行安全认证，通过后在进入常规的 RFID 应用，SIM 卡可以在 SMAP 模块上创建、锁住及删除新应用。SMAP 模块可以通过移动终端的主控芯片（如基带芯片）与 SIM 卡通讯在 SMAP

单芯片解决方案中，还将支持双 7816 接口， SMAP 芯片和 SIM 卡直接通过 7816 接口通讯，在 SIM 卡的内嵌 MCU 具有一定处理能力的条件下，可以直接产生 106K 波特率的非接触应用数据，由 SMAP 芯片翻译成 ISO14443 协议实现卡片模拟功能。SMAP 的方案可以通过 COS 升级的方式使用现有的 SIM 卡芯片产品，降低应用的整体进入门槛。

5. SMAP 平台的应用

和 NFC 应用一样，SMAP 平台的应用主要包括三类：RFID 读写器应用、卡片模拟应用及点对点通讯应用。从应用角度看，SMAP 方案可以适用于移动支付、产品防伪、追踪监管、数字签名、身份认证和信息获取等多类应用。

目前实现的典型应用包括公交一卡通应用、小额金融消费及积分应用、银行卡磁道信息非接触应用、产品防伪与溯源应用、车辆监管应用等。其中公交一卡通应用是目前非接触支付应用最成熟的系统，是和普通用户关系最密切的应用，SMAP 方案可以完成公交一卡通的发行、充值、消费与查询功能，给用户带来新的应用体验，是 SMAP 应用推广的关键领域。

下图是已开发完成的 SMAP 终端的样品。

6. 总结

针对移动通讯与 RFID 应用相互融合的趋势，本文提出并介绍了智能移动应用平台 SMAP 的解决方案，相较与 NFC、双界面 SIM 卡等解决方案，SMAP 平台是一种平衡、渐进的，更符合实际应用需求的方案。