国民技术
nationz technologies

Nationz Technologies

VeriCard®产品手册

2016.02

国民技术股份有限公司
Nationz Technologies Inc.

声明

国民技术股份有限公司（以下简称国民技术）保有在不事先通知而修改这份文档的权利。国民技术认为提供的信息是准确可信的。尽管这样，国民技术对文档中可能出现的错误不承担任何责任。在购买前请联系国民技术获取该文档说明的最新版本。对于使用该文档引起的专利纠纷及第三方侵权国民技术不承担任何责任。另外，国民技术的产品不建议应用于生命相关的设备和系统，在使用卡片中因为设备或系统运转失灵而导致的损失国民技术不承担任何责任。国民技术对本手册拥有版权等知识产权，受法律保护。未经国民技术许可，任何单位及个人不得以任何方式或理由对本手册进行使用、复制、修改、抄录、传播等。

目 录

概述

VeriCard®作为国民技术全新推出的个人数字安全服务解决方案，是集蓝牙 BLE 通信、基础电信功能和安全芯片功能于一体的新一代智能 SIM 卡产品。

VeriCard®提供了基于蓝牙 BLE 的手机 APP 与 SIM 卡之间的通道，为更高安全的应用提供了平台：

- 提供了手机对 SIM 卡访问的高速通道，摆脱了基带芯片和操作系统对 SIM 卡访问的限制；
- 内置 Java 虚拟机，可同时承载多种安全应用业务，提供安全应用动态加载及应用安全区隔离功能；
- 提供支持 PKI/CA 应用的卡片 Applet、国密算法包，支持卡片应用的快速开发与市场化；
- 提供开发者平台和开发套件 ,支持用户快速将卡片功能集成至自有 APP；
- 支持基于 TSM 平台的应用安全下载和更新服务，使用户能够快速部署自己的安全产品业务。

VeriCard®是具备中国完全自主知识产权的个人数字安全服务的最佳载体，为最终用户提供安全、便捷的认证和其它各种应用服务。

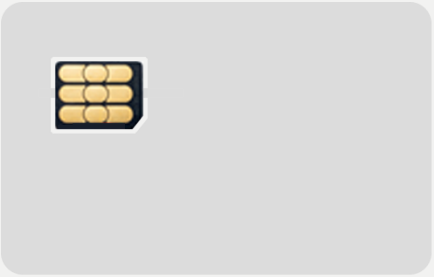

图 1 VeriCard®卡片产品

应用场景如下所示：

图 2 业务应用示意图

硬件架构

VeriCard®卡片硬件结构框图如下，主要包含一颗金融级安全芯片（集成金融支付、认证和电信等应用功能），一颗蓝牙射频芯片。所包含芯片均为国民技术自主研发，拥有完全自主的知识产权。

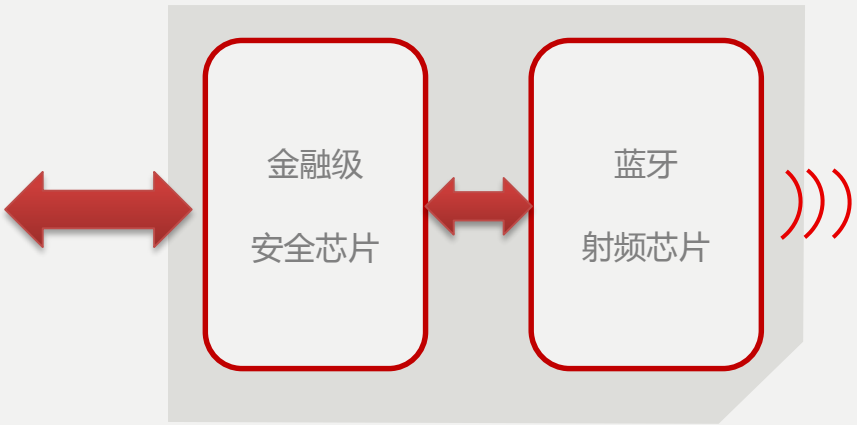

图 3 VeriCard®卡片硬件结构框图

软件架构

VeriCard®提供了包括 Java 虚拟机平台、基础卡片应用 Applet、手机 APP / SDK 和 TSM 平台管理应用等软件系统：

- 提供 Java 虚拟机平台；
- 国密算法支撑软件包；
- 商业化的 UICC Applet、典型 Java 应用开发示例程序；
- 提供手机端 APP 开发 SDK 中间件和应用 APP 开发示例程序；
- 提供 TSM 平台，帮助开发者开展应用部署、下载、删除等调试工作。

VeriCard®软件架构如下：

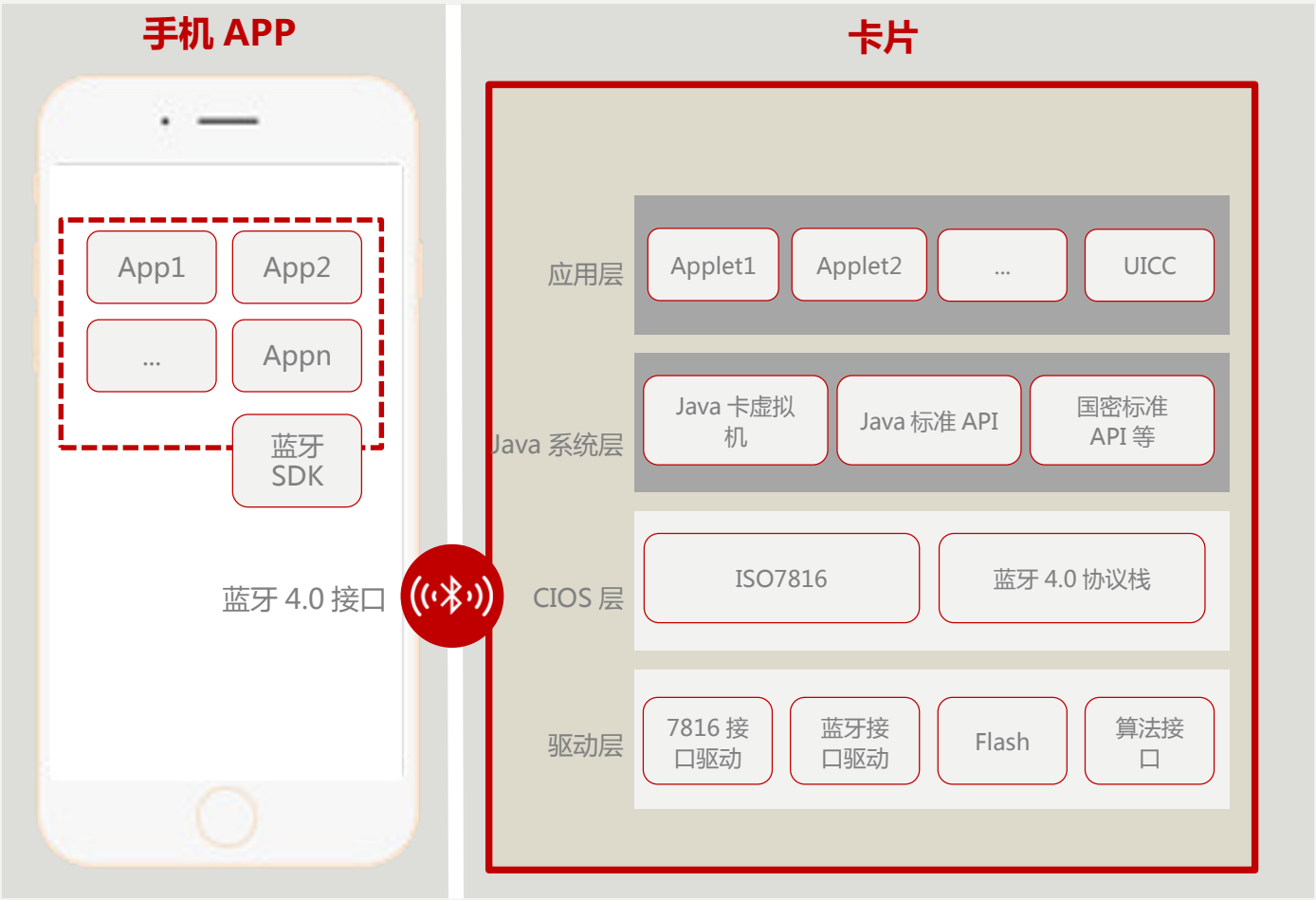

图 4 VeriCard®软件结构框图

VeriCard®卡片端：

- **驱动层：**硬件驱动层，封装了芯片底层硬件接口驱动和算法库。
- **CIOS 层：**中间件层，封装了 ISO7816、蓝牙 4.0 等通讯协议，并为不同接口提供并发处理控制。
- **Java 系统层：**符合 Java Card™ V3.0.2 和 GP V2.2.1 规范要求，为用户 Applet 开发提供 Java 平台。
  - 此部分默认为 VeriCard®产品自带，如果用户需要自行开发，可参照 VeriCard® Java 系统层用户开发接口文档进行 Java 虚拟机的移植。
  - 提供支持 SM1/2/3/4/7/SSF33(可配)等国密算法的 Java API 接口。
- **应用层：**提供了应用 Applet 示例程序供用户参考，同时提供可商用的接触式 UICC Applet 程序、预个人化及个人化指令，开发者可通过提供的指令进行 VeriCard®卡电信功能发卡。

VeriCard®手机 APP 端：

- **蓝牙 SDK：**中间件层，封装了与卡片安全蓝牙连接的接口协议，向 APP 应用提供蓝牙连接管理和数据收发接口。
- **APP：**应用层，调用蓝牙 SDK 实现 APP 与 VeriCard®卡片端的蓝牙通信和应用数据交互，完成应用业务逻辑处理。VeriCard®集成开发包中提供集成了实现典型 PKI 应用的 APP 示例程序，帮助用户实现产品快速开发和部署。

VeriCard®产品特性

协议标准

- 卡片物理尺寸符合 ETSI TS 102.221[11]要求；
- 7816 通信接口遵循 ISO7816-2/3 标准；
- 蓝牙接口协议遵循 Bluetooth® V4.0 Low Energy 标准；
- 内置 Java 平台，支持 Java Card™ V3.0.2 和 GP V2.2.1 标准；

存储特性

Flash	用户应用空间	>330KB
	擦写次数	>10 万次@25°C
	数据保持时间	>10 年@室温
	读时间	50ns
	擦除时间	<1ms
	编程时间	<4μs
RAM	用户应用空间	>8KB

卡片电气特性

工作电压	2.7V~3.6V
待机功耗	<500μA
最大工作电流	<28mA（射频工作）

ESD	8KV（HBM 模式）

蓝牙特性

- 传输速率 16Kbps(手机到卡),32Kbps(卡到手机),视不同手机稍有差异；
- 连接建立时间 ＜ 3s；
- 与蓝牙 4.0 手机通信兼容率 100%；
- 蓝牙维持连接状态下卡片模块对待机功耗的影响 ＜ 5%；

7816 接口特性

- 遵循 ISO7816-2/3 标准；
- 自适应手机终端要求，PPS 支持（96、95、94、11、00）;
- 7816 接口输入时钟频率范围：1~5MHz；

多通道并发

- 支持 7816 接触式通信接口与蓝牙接口并发处理；

安全特性

VeriCard®所采用的安全芯片在安全特性上进行了加强设计，包括：

- 光照异常 / 电压异常 / 频率异常检测，Active Shield Removed 检测；
- 防止 DPA / SPA 攻击；
- 安全应用存储区域加密；
- 时钟和复位信号脉冲过滤；

- 总线加扰；
- 每个芯片唯一序列号；

产品所支持的安全算法、获取的资质如下所示：

非对称算法	RSA（密钥长度最大 2048bit）
	SM2（密钥长度最大 256bit）
对称算法	DES，3DES，AES
	SM1，SM4，SM7，SSF33（可配）
单向散列算法	SHA-1/224/256
	SM3
随机数发生器	真随机数发生器， 符合 NIST SP800-22 标准
CRC 校验	ISO/IEC 3309 标准
芯片资质	EAL4+（中国信息安全认证中心）
	国密二级（国家密码管理局）
	金融移动支付芯片安全测试(银行卡检测中心)

应用开发

- VeriCard®提供可商用的卡片端 UICC，PBOC3.0 和 PKI 应用 Applet，应用 Applet 开发示例程序；
- VeriCard®针对手机 APP 提供蓝牙 SDK 及典型 PKI 应用示例程序。