CPU 卡详解

目　录

随着非接触 IC 卡技术在国内的逐步推广，非接触应用以其快捷方便的操作方式，日益深入人心，并逐渐成为公共交通、城市通卡建设的首选技术。

早期投入应用的非接触 IC 卡技术多为逻辑加密卡，比如最为著名的 Philips 公司（现 NXP）的 Mifare 1 卡片。非接触逻辑加密卡技术以其低廉的成本，简明的交易流程，较简单的系统架构，迅速得到了用户的青睐，并得到了快速的应用和发展。据不完全统计，截至去年年底，国内各领域非接触逻辑加密卡的发卡量已经达到数亿张。

随着非接触逻辑加密卡不断应用的过程，非接触逻辑加密卡技术的不足之处也日益暴露，难以满足更高的安全性和更复杂的多应用的需求。因此，非接触 CPU 卡技术正成为一种技术上更新换代的选择。

一、 CPU 卡的读写原理

一般来说，对存储卡和逻辑加密卡操作，使用接触式 IC 卡通用读写器；对 CPU 卡使用 CPU 卡读写器。所谓“通用读卡器”是指它可以对大多数流行的存储卡和逻辑加密卡操作。而 CPU 卡由于有 ISO/IEC 7816.3/4 的规范，其通讯协议、命令格式都是兼容的，被看作是一种卡。当然，也有将“通用读卡器”与 CPU 读卡器二合一的真正的接触式通用读卡器。

PC 端 IC 卡应用软件编程，要点是了解卡的数据结构和调用读

卡器函数。在这方面，非 CPU 卡与 CPU 卡有不小差别。

a) **CPU 卡的结构：**

首先，非 CPU 卡，你必须熟悉卡的存储结构，哪里是制造商区，哪里是密码区，哪里是数据控制区，哪里是数据区（应用区）……；而 CPU 卡，你不必关心数据的地址，却要关注文件系统的结构：主文件（MF，相当于 DOS 文件系统的根目录）、专用文件（DF，相当于 DOS 文件系统的目录，可以有多层）、基本文件（EF，相当于 DOS 文件系统的文件）。

CPU 卡的基本文件类型虽然只有透明（二进制）文件、（定长与不定长）线性记录文件和循环记录文件三类，但由于 COS 内部控制的需要，派生出一些特定的“变种”——复位应答文件、口令文件、密钥文件、DIR 文件、SFI 文件……。这些都需要熟悉。

纯粹的存储卡是可以自由读取的；非 CPU 逻辑加密卡的访问控制，需要掌握特定的卡的口令控制、认证控制、特定的数据控制标志字节和卡的熔丝（一种卡上这些控制不一定都有）。而 CPU 卡的访问控制，是在建立文件时定义的，读、写、更改分别是否需要认证，用哪个密钥，是否需要口令，是否需要 MAC 验证等等。需要说明的是，创建文件命令的格式是随 COS 而不同的。所以，你必须熟读他的 COS 手册。

b) **CPU 卡的操作：**

非 CPU 卡的访问一般是通过调用函数直接完成的，大不了需要熟悉一下调用参数。而 CPU 卡除了设备命令（测卡、上下电、

选卡座等）和卡的复位命令以外，所有卡命令都是通过一个通用的命令函数执行的，所以你需要熟悉 COS 手册的命令。

COS 的卡操作命令有统一的格式：CLA（命令类别 Class）、INS（命令指令 Instruction）、P1（参数 1）、P2（参数 2）、Lc（命令数据域 Data 长度）、Data 和 Le（应答数据域长度）。命令域中除了 Data，都是 1 字节十六进制数。数据域则是十六进制数串，可以是二进制数、BCD 码或文字的 ASCII 码等等。这有点像汇编语言。调用命令函数时，把命令串代入对应参数即可。

二、 CPU 卡加密系统与 M1 加密系统比较

a) **非接触 CPU 卡与逻辑加密卡介绍**

i. **逻辑加密存储卡：**

在非加密存储卡的基础上增加了加密逻辑电路，加密逻辑电路通过校验密码方式来保护卡内的数据对于外部访问是否开放，但只是低层次的安全保护，无法防范恶意性的攻击。

早期投入应用的非接触 IC 卡技术多为逻辑加密卡，比如最为著名的 Philips 公司（现 NXP）的 Mifare 1 卡片。非接触逻辑加密卡技术以其低廉的成本，简明的交易流程，较简单的系统架构，迅速得到了用户的青睐，并得到了快速的应用和发展。据不完全统计，截至去年年底，国内各领域非接触逻辑加密卡的发卡量已经达到数亿张。

随着非接触逻辑加密卡不断应用的过程，非接触逻辑加密卡技术的不足之处也日益暴露，难以满足更高的安全性和更复杂的多

应用的需求。特别是 2008 年 10 月，互联网上公布了破解 MIFARE CLASSIC IC 芯片（以下简称 M1 芯片）密码的方法，不法分子利用这种方法可以很低的经济成本对采用该芯片的各类“一卡通”、门禁卡进行非法充值或复制，带来很大的社会安全隐患。因此，非接触 CPU 卡智能卡技术正成为一种技术上更新换代的选择。

ii. 非接触 CPU 卡：

又称智能卡，卡内的集成电路中带有微处理器 CPU、存储单元（包括随机存储器 RAM、程序存储器 ROM（FLASH）、用户数据存储器 EEPROM）以及芯片操作系统 COS。装有 COS 的 CPU 卡相当于一台微型计算机，不仅具有数据存储功能，同时具有命令处理和数据安全保护等功能。

（1） 非接触 CPU 卡的特点（与存储器卡相比较）芯片和 COS 的安全技术为 CPU 卡提供了双重的安全保证自带操作系统的 CPU 卡对计算机网络系统要求较低，可实现脱机操作；可实现真正意义上的一卡多应用，每个应用之间相互独立，并受控于各自的密钥管理系统。存储容量大，可提供 1K-64K 字节的数据存储。

（2） 独立的保密模块，使用相应的实体 SAM 卡密钥实现加密、解密以及交易处理，从而完成与用户卡之间的安全认证。

b) 非接触 CPU 卡安全系统与逻辑加密系统的比较

i. 非接触逻辑加密卡

密钥管理系统（Key Management System），也简称 KMS，是 IC 项目安全的核心。如何进行密钥的安全管理，贯穿着 IC 卡应用的整个生命周期。

非接触逻辑加密卡的安全认证依赖于每个扇区独立的 KEYA 和 KEYB 的校验，可以通过扇区控制字对 KEYA 和 KEYB 的不同安全组合，实现扇区数据的读写安全控制。非接触逻辑加密卡的个人化也比较简单，主要包括数据和各扇区 KEYA、KEYB 的更新，在期间所有敏感数据包括 KEYA 和 KEYB 都是直接以明文的形式更新。

由于 KEYA 和 KEYB 的校验机制，只能解决卡片对终端的认证，而无法解决终端对卡片的认证，即我们俗称的“伪卡”的风险。

非接触逻辑加密卡，即密钥就是一个预先设定的固定密码，无论用什么方法计算密钥，最后就一定要和原先写入的固定密码一致，就可以对被保护的数据进行读写操作。因此无论是一卡一密的系统还是统一密码的系统，经过破解就可以实现对非接触逻辑加密卡的解密。很多人认为只要是采用了一卡一密、实时在线系统或非接触逻辑加密卡的 ID 号就能避免密钥被解密，其实，非接触逻辑加密卡被解密就意味着 M1 卡可以被复制，使用在线系统尽可以避免被非法充值，但是不能保证非法消费，即复制一张一样 ID 号的 M1 卡，就可以进行非法消费。现在的技术使用 FPGA 就可以完全复制。基于这个原理，M1 的门禁卡也是不安全的。目前国内 80%的门禁产品均是采用原始 IC 卡的 UID 号或 ID 卡的 ID 号去做门禁卡，根本没有去进行加密认证或开发专用的密钥，其安全隐患远远比 Mifare 卡的破解更危险，

非法破解的人士只需采用的是专业的技术手段就可以完成破解过程，导致目前国内大多数门禁产品都不具备安全性原因之一，是因为早期门禁产品的设计理论是从国外引进过来的，国内大部分厂家长期以来延用国外做法，采用 ID 和 IC 卡的只读特性进行身份识别使用，很少关注卡与机具间的加密认证，缺少钥匙体系的设计；而 ID 卡是很容易可复制的载体，导致所有的门禁很容易几乎可以在瞬间被破解复制；这才是我们国内安防市场最大的灾难。

ii. 非接触 CPU 智能卡

非接触 CPU 卡智能卡与非接触逻辑加密卡相比，拥有独立的 CPU 处理器和芯片操作系统，所以可以更灵活的支持各种不同的应用需求，更安全的设计交易流程。但同时，与非接触逻辑加密卡系统相比，非接触 CPU 卡智能卡的系统显得更为复杂，需要进行更多的系统改造，比如密钥管理、交易流程、PSAM 卡以及卡片个人化等。密钥通常分为充值密钥（ISAM 卡），减值密钥（PSAM 卡），身份认证密钥（SAM 卡）。

非接触 CPU 卡智能卡可以通过内外部认证的机制，例如像建设部定义的电子钱包的交易流程，高可靠的满足不同的业务流程对安全和密钥管理的需求。对电子钱包圈存可以使用圈存密钥，消费可以使用消费密钥，清算可以使用 TAC 密钥，更新数据可以使用卡片应用维护密钥，卡片个人化过程中可以使用卡片传输密钥、卡片主控密钥、应用主控密钥等，真正做到一钥一用。

非接触 CPU 卡加密算法和随机数发生器与安装在读写设备中的

密钥认证卡(SAM 卡)相互发送认证的随机数，可以实现以下功能：

(1) 通过终端设备上 SAM 卡实现对卡的认证。

(2) 非接触 CPU 卡与终端设备上的 SAM 卡的相互认证，实现对卡终端的认证。

(3) 通过 ISAM 卡对非接触 CPU 卡进行充值操作，实现安全的储值。

(4) 通过 PSAM 卡对非接触 CPU 卡进行减值操作，实现安全的扣款。

(5) 在终端设备与非接触 CPU 卡中传输的数据是加密传输。

(6) 通过对非接触 CPU 卡发送给 SAM 卡的随机数 MAC1，SAM 卡发送给非接触 CPU 的随机数 MAC2 和由非接触 CPU 卡返回的随机数 TAC，可以实现数据传输验证的计算。而 MAC1、MAC2 和 TAC 就是同一张非接触 CPU 卡每次传输的过程中都是不同的，因此无法使用空中接收的办法来破解非接触 CPU 卡的密钥。

非接触 CPU 卡智能卡，可以使用密钥版本的机制，即对于不同批次的用户卡，使用不同版本的密钥在系统中并存使用，达到密钥到期自然淘汰过渡的目的，逐步更替系统中所使用的密钥，防止系统长期使用带来的安全风险。

非接触 CPU 卡智能卡，还可以使用密钥索引的机制，即对于发行的用户卡，同时支持多组索引的密钥，假如当前使用的密钥被泄漏或存在安全隐患的时候，系统可以紧急激活另一组索引的密钥，而不用回收和更换用户手上的卡片。

非接触 CPU 卡智能卡系统中，PSAM 卡通常用来计算和校验消费交易过程中出现的 MAC 码，同时在计算的过程中，交易时间、交易金额、交易类型等交易信息也都参与运算，使得交易更安全更可靠。某些情况下，非接触 CPU 卡智能卡系统中的 PSAM 卡还可以用来支持安全报文更新数据时 MAC 的计算，以及交易 TAC 的验证。因此，与非接触逻辑加密卡系统相比，非接触 CPU 卡智能卡系统中的 PSAM 卡支持更广泛的功能，也更为灵活、安全和复杂。通常非接触 CPU 卡智能卡系统的 PSAM 卡还支持不同的密钥版本。

而非接触 CPU 卡智能卡的个人化通常可以分为卡片洗卡和卡片个人化两个独立的流程，前者创建卡片文件结构，后者更新个人化数据，并注入相应的密钥。在信息更新和密钥注入的过程中，通常都采用安全报文的方式，保证数据和密钥更新的正确性和安全性。而且密钥注入的次序和相互保护的依存关系，也充分体现了密钥的安全设计，比如卡片主控密钥通常被用来保护导入应用主控密钥，应用主控密钥通常被用来保护导入其他应用密钥，比如消费密钥等。

非接触 CPU 卡的密钥实现方式：

（1） 硬密钥：即在终端机具中安装 SAM 卡座，所有的认证都是由安装在 SAM 卡座中的 SAM 卡进行运算的，这样在终端机具维修时，只要取出 SAM 卡座中的 SAM 卡，这台终端机具就是空的了。所以所有的银行设备都采用 SAM 卡的认证模式。

（2） 软密钥：终端机具中没有 SAM 卡座，这个密钥的运算实

际上是由终端机具完成的，这样客户的密钥就等于存在终端机具中，厂家拿回终端机具维修时，极易造成密钥流失。

总结以上所述，M1 卡即逻辑加密卡采用的是固定密码，而采用非接触 CPU 卡智能卡采用的是动态密码，并且是一用一密即同一张非接触 CPU 卡智能卡，每刷一次卡的认证密码都不相同，这种智能化的认证方式使得系统的安全性得到提高，特别是当交易双方在完成交易之后，收单方有可能擅自修改或伪造交易流水来达到获利目的，为了防止终端伪造交易流水，系统要求卡片能够产生由交易要素生成的交易验证码，在后台清算时来对交易的有效性进行验证。非接触式 CPU 卡则可以在交易结束时产生个交易验证码 TAC，用来防止伪造交易。逻辑加密卡由于不具有运算能力，就不可能产生交易的验证码。

所以，从安全性的角度来看， 从 IC 卡逻辑加密卡升级到 CPU 卡是一种必然的选择。

三、 如何成功实施 CPU 卡工程项目

a) **系统架构的变化改造**

非接触 CPU 卡与非接触逻辑加密卡相比，拥有独立的 CPU 处理器和芯片操作系统，所以可以更灵活的支持各种不同的应用需求，更安全的设计交易流程。但同时，与非接触逻辑加密卡系统相比，非接触 CPU 卡的系统显得更为复杂，需要进行更多的系统改造，比如密钥管理、交易流程、PSAM 卡以及卡片个人化等。

i. **密钥管理和认证机制**

众所周知，密钥管理系统（Key Management System），也简称KMS，是IC项目安全的核心。如何进行密钥的安全管理，贯穿着IC卡应用的整个生命周期。非接触逻辑加密卡的安全认证依赖于每个扇区独立的KEYA和KEYB的校验，可以通过扇区控制字对KEYA和KEYB的不同安全组合，实现扇区数据的读写安全控制。

Access bits			Access condition for						Remark
			KEYA		Access bits		KEYB		
C1	C2	C3	read	write	read	write	read	write	
0	0	0	never	key A	key A	never	key A	key A	Key B may be read
0	1	0	never	never	key A	never	key A	never	Key B may be read
1	0	0	never	key B	key A|B	never	never	key B	
1	1	0	never	never	key A|B	never	never	never	
0	0	1	never	key A	key A	key A	key A	key A	Key B may be read, transport configuration
0	1	1	never	key B	key A|B	key B	never	key B	
1	0	1	never	never	key A|B	key B	never	never	
1	1	1	never	never	key A|B	never	never	never	

图 1-1 MIFARE I 卡片扇区访问控制

由于KEYA和KEYB的校验机制，只能解决卡片对终端的认证，而无法解决终端对卡片的认证，即我们俗称的“伪卡”的风险，所以通常在采用非接触逻辑加密卡的时候，还会使用卡片认证码的机制。

而非接触CPU卡可以通过内外部认证的机制，以及像建设部定义的电子钱包的交易流程，高可靠的满足不同的业务流程对安全和密钥管理的需求。对电子钱包圈存可以使用圈存密钥，消费可以使用消费密钥，清算可以使用TAC密钥，更新数据可以使用卡片应用维护密钥，

卡片个人化过程中可以使用卡片传输密钥、卡片主控密钥、应用主控密钥等，真正做到一钥一用。

实施非接触 CPU 卡项目，可以使用密钥版本的机制，即对于不同批次的用户卡，使用不同版本的密钥在系统中并存使用，达到密钥到期自然淘汰过渡的目的，逐步更替系统中所使用的密钥，防止系统长期使用带来的安全风险。

实施非接触 CPU 卡项目，还可以使用密钥索引的机制，即对于发行的用户卡，同时支持多组索引的密钥，假如当前使用的密钥被泄漏或存在安全隐患的时候，系统可以紧急激活另一组索引的密钥，而不用回收和更换用户手上的卡片。

因此，要成功实施非接触 CPU 卡项目，需要一个完善的密钥管理系统，能支持多种不同用途的密钥，并支持密钥版本和密钥索引的机制。

ii. 交易流程

非接触逻辑加密卡的交易流程比较简单，通过认证 KEYA 或者 KEYB，达到操作的安全权限，然后就直接进行交易操作，增加或者减少钱包金额。

非接触 CPU 卡的交易分为圈存交易和消费交易等，不同的交易类型，拥有不同的交易流程和安全机制。在非接触 CPU 卡的交易中，交

易数据与交易过程中的相互认证紧紧结合在了一起，使得交易更加安全和严谨。同时，非接触 CPU 卡也通过卡内自增的交易流水号以及卡片计算的交易 TAC 码保证了交易的唯一性和可追踪性。

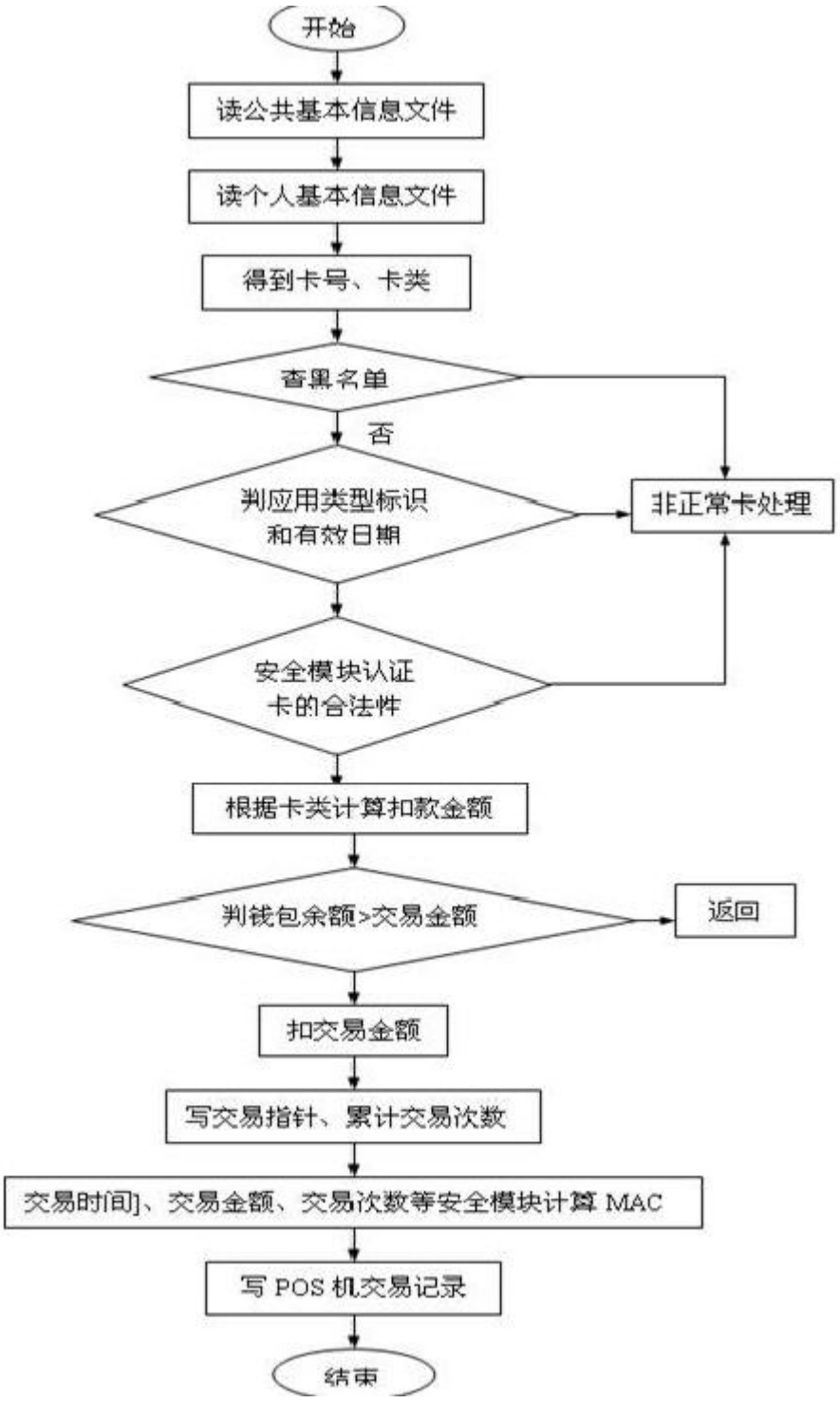

图 1-2 非接触 CPU 卡消费交易流程示例

iii. PSAM 卡

在非接触逻辑加密卡的系统中，PSAM 卡主要使用卡片认证密钥和各扇区的 KEYA、KEYB 密钥来产生非接触逻辑加密卡操作所需要的各扇区的 KEYA 和 KEYB 认证码，交易信息不直接参与运算。

而在非接触 CPU 卡系统中，PSAM 卡通常用来计算和校验消费交易过程中出现的 MAC 码，同时在计算的过程中，交易时间、交易金额、交易类型等交易信息也都参与运算，使得交易更安全更可靠。某些情况下，非接触 CPU 卡系统中的 PSAM 卡还可以用来支持安全报文更新数据时 MAC 的计算，以及交易 TAC 的验证。因此，与非接触逻辑加密卡系统相比，非接触 CPU 卡系统中的 PSAM 卡支持更广泛的功能，也更为灵活、安全和复杂。通常非接触 CPU 卡系统的 PSAM 卡还支持不同的密钥版本。

CLA	INS	P1	P2	Lc	Data	Le
80	70	00	00	14h+8xN	Data	08

LC

Lc = 14h + 8xN

N=1：只有应用序列号 APP_NR

N=2：只有应用序列号 APP_NR 和银行标识符 BANK_ID

N=3：有应用序列号 APP_NR、银行标识符 BANK_ID 以及城市标识符 CITY_ID。

Data

数据域=用户卡随机数 R_icc(4bytes) || 用户卡脱机交易序列号 NT_OFF_XX(2 bytes) || 交易金额 M_P(4bytes) || 交易类型标识 NT_IND(1byte) || 终端交易日期 DATE_TERM(4bytes) || 终端交易时间 TIME_TERM(3bytes) || 消费密钥版本号 VK(1byte) || 消费密钥算法标识 ALGK(1byte) || 应用序列号 APP_NR (8bytes) || 银行标识符 BANK_ID(8 bytes) || 城市标识符 CITY_ID(8 bytes)

图 1-3 建设部 PSAM 卡 MAC1 计算初始化指令

iv. 卡片个人化

非接触逻辑加密卡的个人化比较简单，主要包括数据和各扇区 KEYA、KEYB 的更新，在期间所有敏感数据包括 KEYA 和 KEYB 都是直接以明文的形式更新。

而非接触 CPU 卡的个人化通常可以分为卡片洗卡和卡片个人化两个独立的流程，前者创建卡片文件结构，后者更新个人化数据，并注入相应的密钥。在信息更新和密钥注入的过程中，通常都采用安全报文的方式，保证数据和密钥更新的正确性和安全性。而且密钥注入的次序和相互保护的依存关系，也充分体现了密钥的安全设计，比如卡

片主控密钥通常被用来保护导入应用主控密钥，应用主控密钥通常被用来保护导入其他应用密钥，比如消费密钥等

因此，要成功实施非接触 CPU 卡项目，必须和密钥管理系统配合，建立一套安全和完善的卡片个人化系统，并配备相应的 HSM 硬件加密机或者密钥母卡，来实现个人化流程中密钥的安全存储和运算。

b) 项目实施中注意事项

在非接触 CPU 卡的推广过程中，也发现了一些需要特别注意和着重解决的问题。

i. 卡片与机具的兼容性测试

首当其冲的是卡片与机具的兼容性问题。虽然 ISO 和众多规范已经定义了非接触 CPU 卡和机具终端之间的电气特性和数据协议，但是到目前为止国内众多的非接触 CPU 卡项目的实施经验，无不显示出卡片与机具的兼容性是一个不容忽视的问题。同一种机具，可能会无法支持不同的卡商的卡片；同一个卡商的卡片，可能在这个机具上能正常交易，在另一个机具上就无法使用。甚至，同一张卡片，和同一个机具，做某一种交易能成功，做另一种交易就失败。究其原因，这里面有不同的卡片和机具提供商对规范的不同理解，也有一些是属于项目实施过程中的历史技术原因。

因此，要成功实施非接触 CPU 卡项目，大量的深入的全面的现场测试，是克服卡片和机具兼容性问题的不二法门。

ii. 多应用扩展和开放平台

采用非接触 CPU 卡的一个很重要的原因就是非接触 CPU 卡可以很好的支持多应用扩展，自定义不同的应用交易流程。在多应用扩展的设计阶段，如何尽量符合已有的规范，更开放的适应不同供应商，是非接触 CPU 卡项目能否长期顺利的推广的重要保障。封闭式的系统，历史已经证明，都往往是短命的，不成功的，无法大范围推广的失败者，这里面即涉及未来供应商的非充分竞争，也影响了供应商对相应产品开发和投入的长期信心。

iii. 安全性与交易速度的权衡

安全性和交易速度，是非接触 CPU 卡项目中老生常谈的两个问题，也几乎是每个非接触 CPU 卡项目不得不面对的问题。快捷的交易速度，是采用非接触 IC 卡技术的一个重要原因。但是，片面追求交易速度，甚至以牺牲安全性为代价，又是一个得不偿失的做法。因为，没有可靠的安全性，也就失去了采用 IC 卡技术尤其是非接触 CPU 卡技术的意义。而同时，安全性往往又必然要消耗一定的交易时间，降低了交易的速度。因此，对于安全性和交易速度这一对矛盾体，需要系统的设计者，根据实际的业务需要，好好的权衡和把握，找到两者的平衡点。

在考虑安全性和交易速度的同时，尤其在进行交易速度优化之后，特别需要进行全面的流程测试和异常交易测试，确保交易速度优化不会造成不同交易各个阶段的影响，甚至产生安全漏洞。这方面的教训，是有很多的。

结论：

因此，要实施非接触 CPU **卡项目，多方面的考虑系统的实际需求和各种因素，充分做好系统改造的技术认证和规划设计，切实研究实施过程中的诸多技术问题，是项目成功的重要前提和保障。**