文章编号:1005－0523(2003)01－0024－04

双界面智能卡操作系统的安全体系

张利华[1]，朱灿焰[1]，张其善[2]

(1.华东交通大学 电气电子工程学院,江西 南昌 330013;2.北京航空航天大学,北京 100083)

摘要:阐述了一种双界面智能卡Cashcard COS的安全体系的实现方案,包括密钥管理系统、安全认证系统和通信安全系统,并进行了具体的分析.

关 键 词:双界面智能卡;COS;密钥管理安全认证;通信安全

中图分类号:TP391 **文献标识码**:A

0 引 言

由于智能卡具有良好的人机接口、强大的读写能力、足够的安全技术、大容量的存储能力、便于携带和易于扩充功能等优点,智能卡已经在金融领域和非金融领域作为数据载体、交易媒介和安全工具得到了广泛的应用.智能卡的片内操作系统COS的主要功能是控制智能卡和外界的信息交换,管理智能卡的存储器并在卡内部完成各种命令的处理,通过特定的安全机制、文件系统的设计实现智能卡安全性和一卡多用的要求.双界面智能卡同时具有接触式和非接触式接口,和单接口的智能卡相比,能够根据不同的场合及应用的要求灵活地选择通信接口,具有更广泛的应用灵活性.但与此同时,双界面智能卡有着更为复杂的安全需求,双界面智能卡COS的安全体系一方面要提供接触式智能卡实现数据完整性和安全性的功能,同时还要实现非接触式智能卡特有的多路存取即防冲撞功能和双界面智能卡的两个接口独立通信功能.

根据应用方的要求,依据新加坡NETS规范,采用Infineon公司研制生产的双界面智能卡芯片SLE66CL160S(微处理器卡),设计并实现Cashcard COS,其安全体系由密钥管理系统、安全认证系统和通信安全系统构成.

1 密钥管理系统

1.1 密钥体制和算法

密钥体制的选择要依据硬件条件、交易时间和应用要求来综合考虑,要在较小的开销的情况下实现足够的安全.在Cashcard COS中采用对称密钥体制,使用DES、3-DES和OWF2密钥分散算法,并进行适当组合,进一步增强安全性.

Cashcard COS采用DES密码体制,使用OWF2、DES和3—DES加密算法,具体算法如下:

1) DES算法

设DES密钥Km的长度为8字节,数据Data为8字节,结果Result为8字节.加密算法如下:

$$R=DES(Km)[D] \tag{1}$$

解密算法如下:

$$D=DES^{-1}(Km)[R] \tag{2}$$

2) 3-DES算法

设密钥K的长度为16字节(Km＝(KmL||KmR)),数据Data为8字节,结果Result为8字节.

加密算法如下:

$$R=DES(Km_L)[DES^{-1}(Km_R)[DES(Km_L)[D]]] \tag{3}$$

收稿日期:2002－03－28

作者简介:张利华(1972—),男,湖北京山人,华东交通大学讲师.

解密算法如下:

$$D = DES^{-1}(Km_L)[DES(Km_R)[DES^{-1}(Km_L)[D]]] \quad (4)$$

3) OWF2 算法

设密钥 K 的长度为 16 字节($Km = (Km_L \| Km_R)$),数据 Data 为 8 字节,结果 Result 为 16 字节($R = R_L \| R_R$).

$$R_L = DES(Km_L)[DES^{-1}(Km_R)[DES(Km_L)[D]]]$$

$$R_R = DES(Km_R)[DES^{-1}(Km_L)[DES(Km_R)[D]]]$$

1.2　密钥管理及使用

Cashcard COS 主要采用"一卡一密"、"一类命令一密"、"一次一密"和安全锁定等来实现智能卡的安全.

1) 一卡一密

Cashcard COS 利用发卡中心的主控密钥对芯片号进行多过程加密生成卡中的管理密钥,然后在管理密钥的保护下导入其他密钥,单卡密钥的泄密不会影响的整个系统的运行.

2) 类命令一密

Cashcard COS 使用了五类密钥,即 Transport Key、Authentication Key、Credit/cipher、Debit Key 和 Signature Key,特定的密钥只能使用在特定的命令中,完成特定的功能,不能被其它功能所使用,也不能利用其他密钥产生或派生;在脱机和在线交易时同样使用不同的密钥,从而大大增强了智能卡的抗攻击能力.因此,在智能卡与终端通信时,命令响应序列中单个密钥的泄密不会影响整个智能卡的安全.

3) 一次一密

在交易过程中使用经过一定计算过程,利用对临时性数据如随机数、卡和终端交易计数器值加密计算产生的过程密钥进行加密.过程密钥仅使用一次.如执行 Credit 流程时,数据处理过程如下:

第一步:SK=OWF2(Ki,CTC) 其中 Ki 为指定的密钥,CTC 为卡交易计数器的值;

第二步:<CC>=3—DES(SK, Data) 其中 Data 为输入的数据;

第三步:TSK = OWF2(CreditKey, CTC) 其中 CreditKey 为命令中指定的密钥;

第四步:CC=3—DES(TSK,<cc>)

4) 安全锁定

每个密钥都规定它的使用权限、后续状态以及错误计数器.使用密钥时,要检查当前的卡片安全状态是否满足它的使用权限,只有满足时才能使用.密钥的后续状态用于 PIN 认证或外部认证时,使当前卡片的安全状态达到这一后续状态.而密钥的错误计数器则用于密钥允许外部认证或 MAC 认证失败的次数,每失败一次,错误计数器就会加一,到一定限度后,此密钥会自动锁定,不能再使用.同时,对交易次数和交易金额进行控制,达到一定限度后,智能卡自动拒绝下一步操作.

同时,为了独立地管理一张卡上不同应用的安全问题,每一个应用应该放在一个单独的 DF 中,密钥不能跨应用使用.而且,在卡的整个生存期,密钥不能被外界读取和非法修改,生存期结束,卡永久锁定,密钥停止使用.

2　安全认证系统

2.1　对持卡人的核实

对持卡人的核实是对用户的身份进行鉴别,用以确定持卡人合法性,可以采用 PIN 鉴别和生物鉴别技术.Cashcard COS 使用成熟、简单易行但安全性足够的 PIN 鉴别.为了保证安全,对不同的操作,设置了不同的 PIN,对非常重要的操作还可设置多重 PIN 认证.当多次无效尝试后,卡会自动锁定,禁止进一步的操作.

用户通过命令 Verify 输入口令,然后首先判断密码文件中指定密码的错误计数器的值是否已是最大,如否,则与密码进行比较,比较成功设置相关寄存器的值,下一步操作时需首先判断此寄存器的值.否则,错误计数器加 1,需再次输入口令比较.

2.2　卡与读写器的相互鉴别

卡与读写器的相互鉴别包括读写器对卡的鉴别、卡对读写器的鉴别,即内部认证和外部认证.认证是通过卡与读写器对同样的随机数进行加密,然后比较判断结果是否一致来实现.认证过程如下:

第一步:读写器读取卡号,利用主控密钥经过一定的运算过程得到卡的管理密钥;

第二步:卡产生随机数,读写器取卡随机数;

第三步:读写器产生随机数,读写器对送来的随机数进行一定的运算,然后将运算结果和本身的随机数送卡;

第四步:卡对本身的随机数进行与读写器同样的运算,然后进行结果比较,比较成功,即完成卡对读写器的鉴别,此时要设置安全状态寄存器的值.然后卡对运算结果和送来的随机数进行另一过程运算,等待卡取回;

第五步:读写器取回数据,进行运算比较,比较成功,完成对对卡的鉴别

2.3 文件访问权限认证

Cashcard COS 采用层次结构的文件系统,由 MF(主控文件)、DF(专有文件)和若干个 EF(基本文件)组成,其中一个 DF 对应一个应用.发行商在个人化时通过 COS 对每一个应用建立一个对应 DF 文件的方法来实现对应用的存储和管理,用户无权建立或删除,每个文件都有唯一的 ID 号.文件的安全属性受密钥、密码保护.对每一个文件的访问都需要满足该文件的安全属性,即通过执行命令 SelectFileKey、SelectPurseKey、SelectFile、Verify 来设置卡的安全状态.在做文件访问前,COS 将根据文件的安全属性检查卡的安全状态,以确定操作的可行性.文件的安全属性和文件结构一旦产生便处于 COS 的控制之下.

对文件数据的操作和管理将按照如下的规则:

1) 对某个 DF 文件做操作之前,必须先选择该文件.

2) 文件系统的两层结构,并且操作系统不支持以路径方式选择文件,所以在选择某个文件前必须先选择它的上一层文件,不允许越层选择.

3) 访问文件中的数据要受文件的安全属性的控制.

4) 对文件的建立要受该文件所属的上层文件的安全属性的控制.

3 通信安全系统

3.1 接口独立通信

双界面智能卡两个接口共用一个 CPU 和存储器,在同一过程中只能有一个接口与外界通信,而且同一次交易只能够通过一个接口访问卡中的数据.Cashcard COS 中接触式协议使用的是 ISO/IEC 7816 的 T=0 协议,非接触式协议使用是的 ISO/IEC 14443 的 Type B 协议.T=0 通信协议是异步半双工字符传输协议,数据以字符的形式按照规定的时间周期进行传输.Type B 采用 10%ASK 调制,是半双工分组传输协议.芯片中使用鉴别寄存器的方法实现接口的独立通信.当芯片检测到磁场能量时,该寄存器置 0,封锁接触式接口信道,此时进行非接触式通信;未检测到磁场能量时,该寄存器置 1,封锁非接触式接口信道,进行接触式通信.智能卡 COS 根据鉴别寄存器的值,判断使用的相应的通信接口,然后遵循对应的协议启动相应的通信过程.

3.2 防冲撞机制

在非接触式通信中,当多张智能卡同时进入读写器的有效工作区域时,读写器和智能卡要采用合适的算法实现单卡选择和通信的实现.在 Cashcard COS 中采用动态时隙法,通过一组命令,采用有限状态机来实现智能卡的防冲撞.

读写器不停地通过高频界面发出查询命令,即 REQB 命令.当有卡进入有效区域时,该卡将对 REQB 命令做出应答 ATQB,每张卡回送的应答 ATQB 都包含卡片唯一的个人识别号,如果有两张或者更多的卡同时应答,便发生了冲撞.此时开始启动防冲撞过程.防冲撞算法以时隙为基础,时隙的个数由 REQB 命令中的参数 N($1 \leqslant N \leqslant 16$)决定,所有的卡片都根据参数 N 生成随机数 R($R \leqslant N$).接着读写器发送 N−1 个 SLOTMARKER 命令,用来规定每一个时隙,只有随机数 R 与 SLOTMARKER 命令定义的时隙序号相等的卡才回送 ATQB 应答.这样,读写器就有可能在同一时隙里只收到一张卡的应答,从而与它建立起独立的通信通道,进行通信.如果在某一时隙又发生冲撞,重复以上过程,直到与所有的卡都建立独立的通信通道为止.

表 1 动态时隙法防冲撞原理

读写器传输数据	时隙 0 Request	时隙 1	时隙 2	时隙 3	时隙 4 选择智能卡 5	时隙 n Request	…
智能卡传输数据		冲撞	冲撞	ATR			…
智能卡 1		ATR					…
智能卡 2			ATR				…
智能卡 3		ATR					…
智能卡 4			ATR				…
智能卡 5				ATR			…

3.3 防拔插机制

在双界面智能卡与读写器的通信中,由于外界或人为的因素(如断电),COS 在执行相关命令对卡中的数据进行更新操作未结束时,突然中止,造成读写器与智能卡中的数据不符.Cashcard COS 中使用鉴别寄存器和特定区域备份的方法实现防拔插.在对文件中的数据进行更新前先进行备份,此时,鉴别寄存器为第一类值;进行更新成功后,鉴别寄存器置第二类值.重新上电后,读写器首先检查鉴别寄存器的值,然后根据相应的值选择进行下一步操作.

3.4 安全报文设计

安全报文传送的目的是保证通信中数据的完整性、可靠性和对发送方的认证,它包括对报文源、报文目的地和交易内容和时间(次数)的验证,为最终确认此次交易或命令是否有效提供依据.数据的可靠性通过对数据进行加密、插入校验和、数据和来实现;数据的完整性及验证通过在数据末尾附加 MAC 来实现.

在 Cashcard COS 中一共有三种模式,一种是加密模式,只是对 Data 域进行加密,将密文数据作为最终发送的数据;一种是认证模式,即对 5 个命令头和明文数据进行加密计算得到 MAC,然后在明文数据后附加 MAC,作为最终发送的数据;第三种是先对数据加密,然后和命令头一起进行加密计算得到 MAC,把密文数据附加 MAC,作为最终发送的数据.在数据中根据需要还可以插入校验和、数据和.MAC 的计算方法如下:

第一步:将'00　00　00　00　00　00　00　00',作为初始值.

第二步:按照顺序将以下数据连接在一起形成数据块:

——CLA,INS,P1,P2,Lc+3,Data

第三步:将该数据块分成 8 字节为单位的数据块,标号为 D1,D2,D3,D4 等,最后的数据块有可能是 1—8 个字节.

第四步:如果最后的数据块长度是 8 字节的话,转到第五步.如果最后的数据块长度不足 8 字节的话,在其后加入 16 进制数字'0'直到长度达到 8 字节.

第五步:将这些数据块与初始值或前一步的结果异或得到新的数据块,对新数据块逐步使用相同的密钥进行 3—DES 加密.

第六步:最终得到是从计算结果左侧取得的 3 字节长度的 MAC.

发送的命令采用何种模式是由规范来决定的.

4　结束语

智能卡的一卡多用代表了智能卡应用发展的潮流,利用一张智能卡在一个相对封闭系统内实现具有不同交易时间和安全性要求的个人身份认证、个人信息存储、考勤管理、小额消费、银行金融服务、交通服务、安全登陆管理和保安巡更等多种功能,双界面智能卡具有比单接口智能卡更强的应用适应性.相信随着芯片制造技术水平的提高,CPU 运行速度的提高和卡内存储器容量的增大,性能更好的加密算法的出现,双界面智能卡最终将得到更广泛的应用.

参考文献:

[1] The Cashcard Documentation Set [S]. Part 4 Chapter 3 Volume 7: Cashcard commands, NETS, V1.04, 2002.

[2] The Cashcard Documentation Set [S]. Part 4 Chapter 3 Volume 8: Card Mapping, NETS, V1.04, 2002, 5.

[3] The Cashcard Documentation Key Management, NETS, V1.04, 2002, 5

Security System of the Combi-smart Card′COS

ZHANG Li-hua[1], ZHU Chan-yan[1], ZHAN Qi-shan[2]

(1. East China Jiaotong Uni., Nanchang, 330013; 2. Beijing Uni. of Aeronautics and Astronautics, Beijing, 10083)

Abstract: Security system of the combi-smart card′COS is the key factor in the smart cad, which is composed of key management mechanism、authentication mechanism and communication security mechanism. A scheme is given and analysed in this paper.

Key words: combi-smart card COS; key management; authentication; communication security