ICS 35.040
L 80
备案号:44638—2014

GM

中华人民共和国密码行业标准

GM/T 0035.3—2014

射频识别系统密码应用技术要求
第3部分:读写器密码应用技术要求

Specifications of cryptographic application for RFID systems—Part 3:Specification of cryptographic application for RFID reader

2014-02-13 发布　　2014-02-13 实施

国家密码管理局　　发布

中华人民共和国密码
行业标准
射频识别系统密码应用技术要求
第3部分:读写器密码应用技术要求
GM/T 0035.3—2014
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)64275323 发行中心:(010)51780235
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1.25 字数 26 千字
2014年4月第一版 2014年4月第一次印刷
*
书号:155066·2-27013 定价 23.00 元

GM/T 0035.3-2014

目　　次

前　言

GM/T 0035《射频识别系统密码应用技术要求》分为五个部分：

——第1部分：密码安全保护框架及安全级别；

——第2部分：电子标签芯片密码应用技术要求；

——第3部分：读写器密码应用技术要求；

——第4部分：电子标签与读写器通信密码应用技术要求；

——第5部分：密钥管理技术要求。

本部分为GM/T 0035的第3部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分由密码行业标准化技术委员会提出并归口。

本部分起草单位：北京中电华大电子设计有限责任公司、上海华申智能卡应用系统有限公司、航天信息股份有限公司、上海复旦微电子集团股份有限公司、兴唐通信科技有限公司、复旦大学、北京同方微电子有限公司、上海华虹集成电路有限责任公司、北京华大智宝电子系统有限公司。

本部分主要起草人：董浩然、周建锁、王云松、徐树民、陈跃、顾震、俞军、吴行军、王俊峰、谢文录、梁少峰、范楠迪、王俊宇、柳逊、王会波。

射频识别系统密码应用技术要求
第3部分:读写器密码应用技术要求

1 范围

GM/T 0035的本部分规定了采用密码技术的读写器的安全认证、数据存储和通信安全等安全要求,规定了射频识别系统不同安全级别对读写器密码安全的技术要求。附录A给出了一种读写器密码安全应用示例。

本部分适用于采用密码技术的读写器的设计开发、生产制造和应用。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GM/T 0035.1—2014 射频识别系统密码应用技术要求 第1部分:密码安全保护框架及安全级别

GM/T 0035.2—2014 射频识别系统密码应用技术要求 第2部分:电子标签芯片密码应用技术要求

GM/T 0035.4—2014 射频识别系统密码应用技术要求 第4部分:电子标签与读写器通信密码应用技术要求

GM/T 0035.5—2014 射频识别系统密码应用技术规范 第5部分:密钥管理技术要求

3 术语和定义

GM/T 0035.1—2014界定的术语和定义适用于本文件。

4 符号和缩略语

GM/T 0035.1—2014界定的符号和缩略语适用于本文件。

5 读写器基本结构

读写器的基本结构包括通信模块、安全存取模块(SAM)、处理器模块和射频模块。读写器结构框图如图1所示。

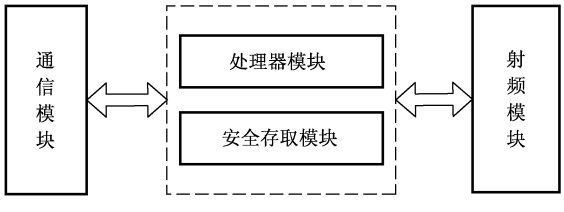

图1 读写器基本结构

通信模块是读写器与系统之间的通信接口；射频模块是读写器与电子标签之间的物理接口；安全存取模块负责读写器的安全保护；处理器模块负责对来自于电子标签或系统的指令解析、数据处理和数据转发。

6 密码安全要素

6.1 机密性

6.1.1 存储信息的机密性

读写器对存储在读写器内的敏感信息采用密码算法进行加密保护，使得读写器的任何部分损坏或失效，以及非授权访问等都不会导致敏感信息的泄露，以保证读写器数据存储的机密性。

存储信息的机密性保护应采用密码算法加密完成。

采用对称密码算法分组加密方式时，用 L_D 表示明文数据的长度，在明文数据前加上 L_D 产生新的数据块，并将该数据块按照密码算法分组长度要求进行分组，如果最后一组数据长度小于密码算法分组长度，则应进行填充补齐。填充方式为在最后一组数据后填充一个字节十六进制‘80’，如果仍小于密码算法分组长度，则填充‘00’至分组长度。在数据分组完成后，采用密码算法和加密密钥对该数据逐组加密后存储。在读取该数据时，对于存储的密文数据，采用同样的密码算法和加密密钥对其进行解密，并根据明文数据长度 L_D 截取得到完整的明文数据。

6.1.2 传输信息的机密性

读写器与电子标签通信时，读写器对传输的敏感信息采用密码算法进行加密保护，保证该传输数据在被截获后无法得到明文数据，达到传输信息的机密性要求。

传输信息机密性保护须通过对传输的明文数据进行加密完成，采用流加密或分组加密的方式进行。

传输信息机密性的实现过程见 GM/T 0035.4—2014。

6.2 完整性

6.2.1 存储信息的完整性

读写器采用密码算法对存储在读写器内的敏感信息进行校验计算，以发现数据被篡改、删除和插入等情况，确保存储信息的完整性。

存储信息完整性保护应采用密码算法，通过对存储的数据加校验码的方式进行。具体方式是在存储数据的同时存储该数据相关的校验码。

采用对称密码算法或密码杂凑函数计算检验码时，计算过程见 GM/T 0035.4—2014 中 7.2.1 和 7.2.2 规定的方法。

采用非对称密码算法产生的数字签名可用于数据完整性校验。

6.2.2 传输信息的完整性

读写器与电子标签通信时，读写器采用密码算法对传输的信息进行校验计算，以发现数据被篡改、删除和插入等情况，达到传输过程中的信息完整性要求。

传输信息的完整性实现方式见 GM/T 0035.4—2014。

6.3 抗抵赖

6.3.1 抗电子标签原发抵赖

抗电子标签原发抵赖是指标签信息的原发者（读写器或第三方）采用密码算法对写入电子标签内的

数据进行数字签名操作，确保产生该数字签名的原发者不能成功地否认曾经生成过该数据。

当读写器作为信息的原发者时，读写器采用密码算法对电子标签数据（含电子标签的身份特征）产生数字签名，将签名后的数据传输到电子标签芯片，电子标签存储该签名数据，以支持电子标签具有抗电子标签原发抵赖的功能。

当读写器作为电子标签签名信息的验证主体时，读写器能够验证电子标签存储的签名数据，以鉴别签名信息原发者的真实性。

6.3.2 抗电子标签抵赖

读写器具有抗电子标签抵赖功能时，读写器应能够对电子标签产生的数字签名进行验证，达到抗电子标签抵赖的要求。

6.3.3 抗读写器抵赖

支持抗读写器抵赖时，读写器应具有产生数字签名功能。

6.4 身份鉴别

6.4.1 唯一标识符鉴别

唯一标识符鉴别采用与电子标签唯一标识符相关的验证码鉴别方式。

唯一标识符鉴别的实现方式见 GM/T 0035.4—2014。

6.4.2 读写器对电子标签的挑战响应身份鉴别

读写器对电子标签的挑战响应鉴别的实现方式见 GM/T 0035.4—2014。

读写器应设定不成功鉴别的尝试次数，当达到或超过规定的次数时，读写器应停止再次尝试挑战响应鉴别操作。

6.4.3 电子标签对读写器的挑战响应身份鉴别

电子标签对读写器的挑战响应鉴别的实现方式见 GM/T 0035.4—2014。

6.5 访问控制

读写器数据访问控制采用密码算法对敏感数据读写、密钥存储、密钥更新等操作设置控制权限。对不同的权限应设置不同的密钥进行访问控制，阻止非授权的访问。

对读写器的访问只能按照读写器发行时所设置的访问控制权限对读写器进行相关操作。对读写器进行访问的主体可能是中间件、后台信息系统等。

6.6 审计记录

读写器对涉及应用系统安全的数据及相关操作（潜在的安全侵害）进行记录并存储，记录内容至少包括使用主体、使用时间、执行的操作等，用于应用系统审计所记录数据和操作的安全性。

对于敏感数据的记录，如果不能在 SAM 内存储，需要由 SAM 产生信息校验码进行完整性保护后存储。

6.7 密码配置

6.7.1 密码算法

读写器的密码算法配用要求见 GM/T 0035.1—2014。

6.7.2 密钥管理

读写器密钥管理涉及密钥注入、密钥存储、密钥分散和密钥使用等，密钥应存储在读写器安全存取模块(SAM)内。相关要求见 GM/T 0035.5—2014。

6.8 其他安全措施

读写器内部各处理模块之间(如 SAM 和处理器模块之间)传输敏感数据时，应采取措施保证敏感数据的安全，如打开读写器外壳时销毁密钥的防护措施，防止发生敏感数据泄漏、篡改或丢失。

在满足本标准规定的读写器密码安全技术要求之外，读写器也应根据系统安全需求决定是否支持与中间件或后台信息系统之间的通信安全和安全认证等安全机制，比如具有传输信息的机密性和完整性、挑战响应身份鉴别、抗抵赖、访问控制、审计记录等安全功能。

7 密码安全技术要求

射频识别系统不同安全级别对读写器密码安全技术的要求不同，读写器密码安全技术要求应符合表 1 的规定。

表 1 密码安全技术要求

密码安全要素			射频识别系统密码安全级别			
			1 级	2 级	3 级	4 级
机密性	存储信息的机密性			√	√	√
	传输信息的机密性				√	√
完整性	存储信息的完整性			√	√	√
	传输信息的完整性				√	√
抗抵赖	抗电子标签原发抵赖				√	√
	抗电子标签抵赖					√
	抗读写器抵赖				√	√
身份鉴别	唯一标识符身份鉴别		√			
	读写器对电子标签的挑战响应身份鉴别			√	√	√
	电子标签对读写器的挑战响应身份鉴别				√	√
访问控制				√	√	√
审计记录					√	√
密码配置	密码算法	对称算法	√	√	√	√
		非对称算法			√	√
		密码杂凑函数			√	√
	密钥管理	密钥注入	√	√	√	√
		密钥存储	√	√	√	√
		密钥分散	√	√	√	√
		密钥使用	√	√	√	√

注 1：“√”表示不同安全级别的射频识别系统中采用的读写器应具备的密码安全要素。

注 2：表中规定的是射频识别系统各安全级别对读写器的最低安全要求。

附 录 A
（资料性附录）
读写器密码安全应用实例

A.1 读写器安全需求

A.1.1 系统描述

图 A.1 给出了用于某大型赛事电子门票的射频识别系统框图。

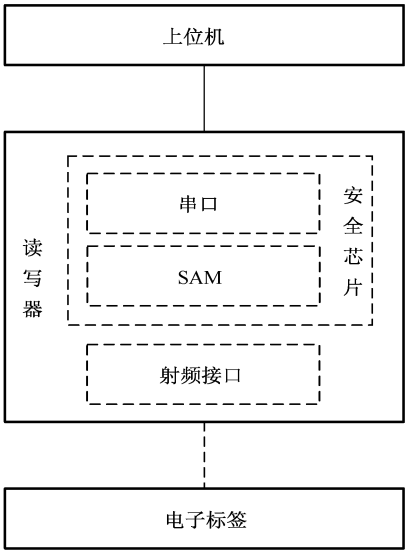

图 A.1 电子门票射频识别系统框图

电子门票系统由电子标签、读写器和上位机构成。其中，读写器采用射频接口芯片和安全芯片来实现。

采用的安全芯片具有如下特性：

- CPU：32 位 RISC 处理器
- 32KB EEPROM：用于数据和程序的存储
- 256KB FLASH：用于程序、函数库和数据的存储
- MMU：存储器管理单元，支持四种工作模式
- 随机数发生器
- 安全探测：高低频率检测、高低电压检测
- UART 接口
- 支持 SM1/SM4、SM2、SM3、SM7 密码算法

A.1.2 安全级别

射频识别系统的安全级别为第二级。

电子标签功能与 GM/T 0035.2—2014 附录 A 相同，支持国产 SM7 密码算法。

A.1.3 读写器密码安全需求

根据系统的安全需求，读写器支持如下安全要素：

a) 存储信息的机密性；

b) 存储信息的完整性；

c) 与电子标签传输信息的机密性；

d) 抗电子标签原发抵赖；

e) 读写器与电子标签双向挑战响应身份鉴别；

f) 访问控制。

此外，读写器应支持与上位机之间的传输信息的机密性和完整性、身份鉴别、访问控制、抗抵赖等安全要素。

A.2 SAM 命令集

SAM 支持的命令集说明如表 A.1 所示。

表 A.1 SAM 命令集说明

编号	命 令	功 能 描 述
1	READ BINARY	读透明文件
2	READ RECORD	读记录
3	UPDATE BINARY	修改透明文件内容
4	UPDATE RECORD	修改记录
5	APPEND RECORD	添加记录
6	VERIFY PIN	验证个人密码
7	EXTERNAL AUTHENTICATE	外部认证
8	GET CHALLENGE	取随机数
9	INTERNAL AUTHENTICATE	内部认证
10	SELECT FILE	选择文件或应用
11	GET RESPONSE	取响应
12	CREATE FILE	建立文件
13	RELOAD PIN	重装个人密码
14	CHANGE PIN	修改个人密码
15	PIN CHANGE/UNBLOCK	更改/解锁个人密码
16	WRITE KEY	重装/解锁密钥
17	CARD BLOCK	环境锁定
18	APPLICATION BLOCK	应用锁定

表 A.1（续）

编号	命　令	功 能 描 述
19	APPLICATION UNBLOCK	应用解锁
20	FREEZE MF	冻结 MF
21	GET INFO	取卡的特征信息
22	CLEAR DF	清除 DF 文件体
23	GENERATE SM2 KEY	产生 SM2 密钥对
24	STORE SM2 KEY	安装 SM2 密钥
25	GET SM2 KEY	读出 SM2 密钥
26	SM2 SIGNATURE	SM2 签名
27	SIGNATURE VERIFY	SM2 签名认证
28	SM2 ENCRYPT	SM2 加密
29	SM2 DECRYPT	SM2 解密
30	GENERATE ENVELOP	产生数字信封
31	OPEN ENVELOP	打开数字信封
32	SM3 COMPRESS	安全哈希算法压缩数据
33	DECRYPT/ENCRYPT	对称算法加解密
34	DELIVERY KEY	密钥分散
35	CIPHER DATA	对称算法加解密，计算 MAC

A.3　密钥管理

A.3.1　密码算法配用

读写器配用 SM1/SM4、SM2、SM3、SM7 密码算法，功能如下：

a）　对称密码算法 SM7：用于读写器与电子标签之间的挑战响应身份鉴别和数据传输加密；

b）　对称密码算法 SM1/SM4：用于密钥分散、读写器数据存储加密，以及与上位机的身份鉴别；

c）　非对称密码算法 SM2：用于产生电子标签内受保护数据的数字签名，以及对数字签名进行验证；

d）　密码杂凑函数 SM3：用于产生摘要信息。

A.3.2　密钥

系统中用到的密钥如表 A.2 所示。

表 A.2　系统中用到的密钥

密钥	算法	用途	产生	保存	生命周期	备份
KA	SM1/SM4	分散出密钥 KE	密码机	密码机	整个赛事	密码机
KB	SM1/SM4	分散出密钥 KF	密码机	密码机、验票读写器	整个赛事	密码机
KC	SM1/SM4	外部认证密钥	密码机	密码机、验票读写器	整个赛事	密码机
KD	SM2	签名和验证签名	密码机	私钥：密码机； 公钥：密码机和验票读写器	整个赛事	密码机
KE	SM7	门票的主密钥	由密钥 KA 分散出	门票	发票时：分散得到并写入门票 门票中：整个赛事	不备份
KF	SM7	门票的验票密钥	由密钥 KB 分散出	门票	发票时：分散得到并写入门票 验票读写器中：分散得到一值到验证密钥结束 门票中：整个赛事	不备份
注：密码机是指在密钥生成、门票签发，以及上位机与读写器通信安全保护时上位机中采用的密码设备。						

A.3.3　密钥注入

读写器密钥的分发和注入在密钥管理中心进行，根据读写器的不同应用，向读写器内注入不同的密钥，本应用中向验票读写器中注入 3 个密钥，包括用于分散得到验票密钥的 SM1/SM4 密钥 KB、用于与上位机身份鉴别用的 SM1/SM4 密钥 KC 和 SM2 密钥 KD 的公钥。

密钥的完整性检验利用 SM3 算法，在密钥分发前计算密钥的验证码，并将验证码随密钥一同分发，读写器在接收到密钥后要对验证码进行验证。

A.3.4　密钥存储

私钥：SAM 模块不提供能够导出保存在其中的非对称密钥对中私钥的接口，也就是说一旦使用 SAM 模块产生了密钥对并保存起来，那么只有 SAM 自身拥有私钥。

SM1/SM4 密钥：SM1/SM4 分组密码算法的密钥不能通过任何接口读出，只能在满足安全条件下参与运算或被修改。

SM7 密钥：在读写器 SAM 内通过密钥分散产生，用于与电子标签的身份鉴别和访问控制，在 SAM 内不存储。

A.3.5　密钥分散

密钥分散方法如图 A.2 所示，密钥长度及密钥分散因子长度均为 16 字节。将密钥分散因子作为输入数据，用 SM1/SM4 算法做加密运算，产生的 16 字节数据作为子密钥。

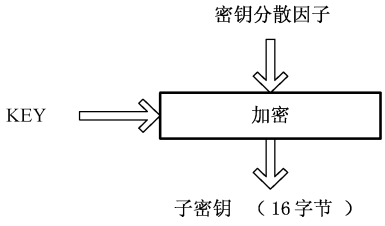

图 A.2 密钥分散计算方法

A.3.6 密钥使用

读写器内的 SM1/SM4 密钥 KB 用于分散出 SM7 算法使用的验票密钥。

读写器内的 SM1/SM4 密钥 KC 用于读写器与上位机之间的身份鉴别，以及 SAM 内敏感信息加密。

读写器内的 SM2 密钥对 KD 中的公钥用于验证数字签名。

SM7 密钥由 KB 分散得到，其参与的加解密操作在 SAM 模块内部完成，用于读写器与电子标签挑战响应身份鉴别，以及传输加密的密钥协商。

A.4 访问控制

A.4.1 文件系统

所有密钥和其他数据都存储在文件系统中，安全的文件系统是 SAM 模块的安全基础。读写器 SAM 文件系统结构及权限说明如表 A.3 所示。

表 A.3 SAM 文件结构及权限说明

文件名称	标识符	权限	密钥	说明
根目录 MF	3F00	全局权限	主控密钥 KC，标识为 0000 的外部认证密钥	成功认证后可获得主控密钥权限，可建立文件、目录等相应权限操作
环境目录 DDF	除 0000、3F00、FFFF 外其他值	全局权限	主控密钥 KC	成功认证后可获得主控密钥权限，可建立文件、目录等相应权限操作
应用目录 ADF	除 0000、3F00、FFFF 外其他值	局部权限	主控密钥 KC	成功认证后可获得主控密钥权限，可建立文件等相应权限操作
透明文件	除 0000、3F00、FFFF 外其他值	读写权限设置，可设置 1～15 级权限	主控密钥 KC 或传输密钥	读写该文件时，若需要计算密文和校验码，则使用读/写密钥短标识对应的密钥值进行计算
记录文件	除 0000、3F00、FFFF 外其他值	读写权限设置，可设置 1～15 级权限	主控密钥 KC 或传输密钥	读写该文件时，若需要计算密文和校验码，则使用读/写密钥短标识对应的密钥值进行计算

表 A.3（续）

文件名称	标识符	权限	密钥	说明
安全文件	取值范围 0001～00FF	只能写入或修改，不能从 SAM 中读出。更新密钥可设置 1～15 级权限；密钥使用可设置 1～15 级权限	主控密钥 KC 或传输密钥	存放 SM1 密钥 KA 和 KB。在更新密钥时，若需要计算密文和校验码，则使用更新密钥短标识对应的密钥值进行计算
SM2 公钥文件	除 0000、3F00、FFFF 外其他值	公钥使用可设置 1～15 级权限，以保护加密和验证签名操作；公钥读写可设置 1～15 级权限，以保护导入/导出	主控密钥 KC 或传输密钥	存放 SM2 公钥数据。在导出/导入公钥时，若需要计算密文和校验码，则使用读/写密钥标识对应的密钥值进行计算
SM2 私钥文件	除 0000、3F00、FFFF 外其他值	私钥使用可设置 1～15 级权限，以保护解密和签名操作；私钥写可设置 1～15 级权限，以保护私钥导入	主控密钥 KC 或传输密钥	存放 SM2 私钥数据。在导入私钥时，若需要计算密文和校验码，则使用写密钥标识对应的密钥值进行计算
注：标识符为 0000 的 SM1 密钥 KC 特指为主控密钥。一个目录(MF/DDF/ADF)下只能有一个主控密钥。主控密钥的建立是随目录一起建立的，可通过 WRITE KEY 命令更新主控密钥值。				

A.4.2 访问控制策略

安全管理系统支持为特定文件设定访问权限。应用必须通过外部认证等方式取得相应权限后才能访问特定文件。

访问权限用 2 个字节表示，高字节对应全局权限，低字节对应局部权限。每个字节的高 4 位表示权限的下限，每个字节的低 4 位表示权限的上限。假设权限的高字节为‘XY’，若‘X’≤‘Y’表示文件的全局权限在‘X’至‘Y’内；若‘X’＞‘Y’，表示文件被禁止访问；若为‘0Y’，表示没有权限限制。权限的低字节说明与高字节相同。

A.5 读写器与电子标签的双向身份鉴别

采用双向挑战响应身份鉴别方式，鉴别流程如图 A.3 所示。

电子标签芯片被读写器选中后(REQA、ANTI、SELECT 指令操作)，必须进行双向挑战响应身份鉴别，通过身份鉴别后，才能对认证密钥对应的块进行相应控制权限的访问。

认证前的准备：

a) 电子标签和读写器使用相同的密码算法 SM7。

b) 电子标签和读写器使用相同的密钥。

c) 电子标签和读写器使用各自的随机数发生器。

认证过程：

a) 读写器发送鉴别指令以及指令参数(密钥块地址)。

b) 电子标签接收指令后发送由随机数发生器产生的 32 位 Rb。

c) 读写器收到 Rb 后，由随机数发生器产生 32 位随机数 Ra，并以 128 位 KEY 为密钥进行加密，

加密的明文为 Ra(左半部分)Rb(右半部分)。加密结束,发送 64 位密文 Token1 (低位先发)。

d) 电子标签接收到 Token1 之后对其进行解密,解密后得到的明文右半部分 Rb′与之前产生的 Rb 比较。

e) 电子标签比较 Rb′正确后,加密生成 Token2,加密的明文为电子标签新产生的 32 位随机数 Rb″(左半部分,Rb″用于密钥协商)和解密 Token1 得到的 Ra′(右半部分),得到的 64 位密文为 Token2。如果 Rb′与 Rb 不同,则电子标签无响应并返回到空闲/挂起状态。

f) 电子标签加密完成后,发送 Token2(低位先发)。在发送完信息后,电子标签等待读写器发送的后续命令。

g) 读写器接收到 Token2 后,解密并比较所得到的 Ra′与原先发送的 Ra,如果 Ra′比较正确,鉴别通过,否则鉴别失败。

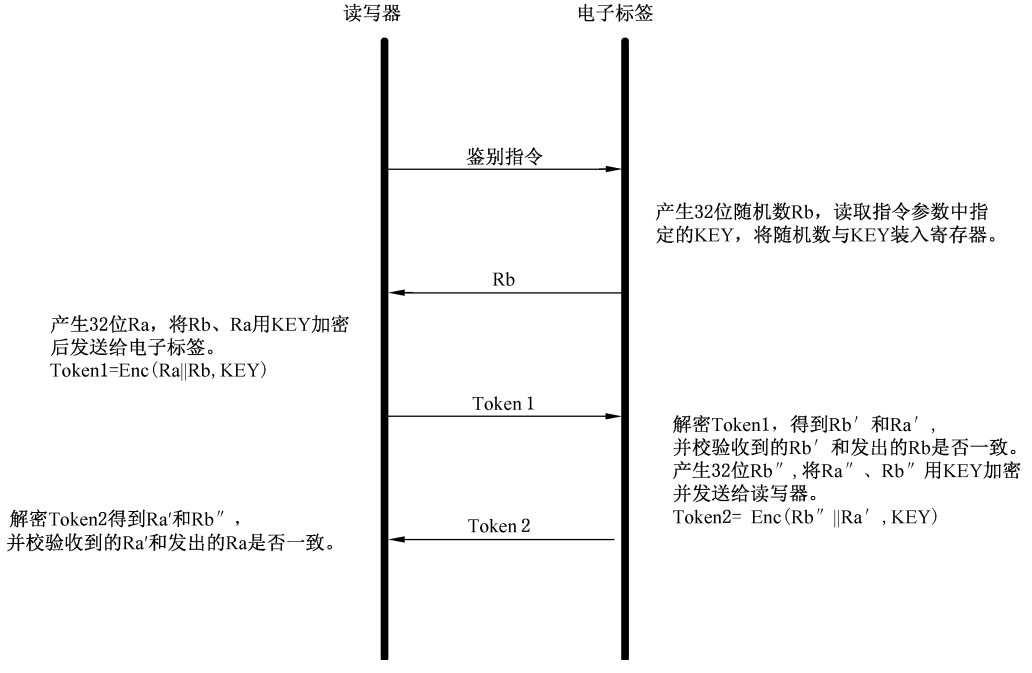

图 A.3　双向鉴别流程

某一密钥的鉴别通过后,所有该密钥对应的访问权限全部打开。

A.6　机密性和完整性

A.6.1　存储信息的机密性和完整性

读写器 SAM 内存储的敏感信息经过 SM1/SM4 密码算法加密后存储,保证存储信息的机密性。

读写器 SAM 内存储的敏感信息经过 SM3 密码杂凑函数计算产生摘要信息,并存储摘要信息,用于完整性校验。

A.6.2　与电子标签传输信息的机密性

对通信数据的加密采用基于 SM7 算法的流加密方式,数据发送端通过 OFB 模式循环产生密码流,并将通信明文数据与密码流异或后发出;数据接收端通过相同方法产生相同的密码流,将接收到的加密数据与密码流异或后得到数据明文。

在图 A.3 描述的双向身份鉴别过程结束后,电子标签与读写器都继续使用当次身份鉴别过程所使

用的密钥 KEY，将身份鉴别过程中产生的 Token2 作为初始向量，通过 SM7 算法的 OFB 模式运算，所产生的加密结果用作流加密的密码流，与通信数据明文（密文）异或后得到通信数据密文（明文）。

A.7 抗抵赖

读写器抗电子标签原发抵赖的操作过程说明如下。

电子标签发行阶段：

a） 读写器通过杂凑算法 SM3 将电子标签需要签名的数据原文生成数字摘要。

b） 读写器用私钥对数字摘要进行数字签名。

c） 读写器将签名数据原文、数字签名、公钥证书一起进行封装，形成签名结果发送给电子标签，并存储在电子标签存储器内。

应用阶段：

a） 读写器读取电子标签内存储的签名数据原文、数字签名和公钥证书。

b） 读写器通过密码杂凑函数 SM3 将电子标签的签名数据原文生成数字摘要。

c） 读写器验证从电子标签内读取的公钥证书，获得电子标签信息原发者的公钥，利用该公钥对从电子标签内读取的数字签名进行解密，获得电子标签信息原发者生成的数字摘要。

d） 读写器将两个摘要信息进行比较，结果一致则电子标签的真实性验证成功。

A.8 读写器与上位机通信安全

采用 SM1/SM4 密码算法实现读写器与上位机的双向身份鉴别。

采用 SM1/SM4 密码算法对数据加密并计算校验值（CBC-MAC），以实现读写器与上位机之间传输信息的机密性和完整性。