ICS 35.040
L 80
备案号:44639—2014

GM

中华人民共和国密码行业标准

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

Specifications of cryptographic application for RFID systems—Part 4:Specification of cryptographic application for communication between RFID tag and reader

2014-02-13 发布　　2014-02-13 实施

国家密码管理局　发布

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4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。

本部分主要起草单位：北京同方微电子有限公司、兴唐通信科技有限公司、北京中电华大电子设计有限责任公司、上海复旦微电子集团股份有限公司、航天信息股份有限公司、上海华申智能卡应用系统有限公司、复旦大学、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：吴行军、董浩然、王俊峰、周建锁、陈跃、俞军、梁少峰、谢文录、王云松、徐树民、顾震、王俊宇、柳逊、王会波。

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

1 范围

GM/T 0035的本部分规定了电子标签与读写器之间的身份鉴别、传输信息的机密性和完整性等安全要求及实现方式。

本部分适用于射频识别系统中电子标签与读写器间通信的安全设计、实现和应用。

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 0035.5—2014 射频识别系统密码应用技术要求 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 密码安全要素

5.1 传输信息的机密性

电子标签与读写器通信时，电子标签和读写器对相互之间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。

传输信息的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方式见7.1。

5.2 传输信息的完整性

电子标签与读写器通信时，电子标签和读写器对相互之间传输的信息采用密码算法进行校验计算，以发现信息被篡改、删除和插入等情况，达到传输过程中的信息完整性要求。

传输信息完整性校验的实现方式见7.2。

5.3 身份鉴别

5.3.1 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 7.3.1。

5.3.2 读写器对电子标签的挑战响应鉴别

读写器采用挑战响应鉴别方式对电子标签身份的真实性进行鉴别。

读写器对电子标签的挑战响应鉴别的实现方式见 7.3.2.2 和 7.3.3。

5.3.3 电子标签对读写器的挑战响应鉴别

电子标签采用挑战响应鉴别方式对读写器身份的真实性进行鉴别。

电子标签对读写器的挑战响应鉴别的实现方式见 7.3.2.1 和 7.3.3。

6 密码安全技术要求

射频识别系统不同安全级别对电子标签与读写器通信的密码安全技术要求不同，电子标签与读写器通信密码安全技术要求应符合表 1 的规定。

表 1 电子标签与读写器通信密码安全技术要求

密码安全要素		射频识别系统安全级别			
		1 级	2 级	3 级	4 级
机密性	传输信息的机密性			√	√
完整性	传输信息的完整性			√	√
身份鉴别	唯一标识符鉴别	√			
	读写器对电子标签的挑战响应鉴别		√	√	√
	电子标签对读写器的挑战响应鉴别			√	√
注 1：“√”表示不同安全级别的射频识别系统中采用的电子标签与读写器通信密码安全要素。 注 2：表中规定的是射频识别系统各安全级别对电子标签与读写器通信的最低安全要求。					

7 通信密码安全实现方式

7.1 传输信息的机密性

7.1.1 传输密钥

7.1.1.1 协商密钥模式

a) 采用分组密码算法的密钥协商

读写器和电子标签之间进行数据加密传输之前，先采用分组密码算法进行密钥协商。

电子标签产生随机数 R_T（长度与密码算法分组长度一样），用个性化密钥 K1 加密得到工作密钥 $K_{TR}=Enc(R_T,K1)$，电子标签将 R_T 发送给读写器，并保证传输过程中 R_T 的完整性。

读写器用电子标签个性化密钥 K1 加密 R_T 得到 $K_{TR}=Enc(R_T,K1)$，并将 K_{TR} 作为协商出的工作密钥。

b) 采用非对称算法的密钥协商

读写器和电子标签之间进行数据加密传输之前，先采用非对称密码算法进行密钥协商。

读写器产生随机数(长度与密码算法密钥长度一样)，作为协商的工作密钥 K_{TR}，用电子标签的公钥加密得到 K_{TR}'，将 K_{TR}' 发送给电子标签，并保证传输过程中 K_{TR}' 的完整性。

电子标签用自己的私钥解密 K_{TR}' 得到 K_{TR}，作为协商出的工作密钥。

7.1.1.2 固定密钥加密模式

电子标签内存储传输密钥 K_{TR}。读写器与电子标签之间进行数据加密传输前，读写器读取电子标签的 UID，使用该 UID 进行密钥分散得到传输密钥 K_{TR}，作为读写器与电子标签数据加密传输的工作密钥。

7.1.2 实现方法

读写器和电子标签双方交换数据时均使用对称密码算法加密。

采用分组加密方式时，发送方先采用得到的电子标签的传输密钥 K_{TR} 和对称密码算法对待传输数据 M 进行加密运算得到密文数据 $C=Enc(M,K_{TR})$，然后将密文 C 发送给对方。对方接收到密文 C 后，采用电子标签的传输密钥 K_{TR} 和对称密码算法对 C 进行解密运算恢复明文数据 $M=Dec(C,K_{TR})$。

采用流加密方式时，数据发送方和接收方具有共同的密码流产生器，该密码流产生器应由传输加密密钥 K_{TR}、双方产生的随机数 R_R 和 R_T 等初始化。采用 OFB 模式产生密码流，且顺序使用密码流，不作丢弃。发送方采用密码流对明文数据逐位进行线性操作(如位异或操作)，产生传输的密文数据。接收方在接收到该密文数据后，采用与发送方相同的线性操作逐位还原出原始明文数据。

7.2 传输信息的完整性

7.2.1 采用 CBC-MAC 的完整性校验方法

电子标签和读写器通信过程中，发送方发送敏感信息前，读写器读取电子标签的 UID，使用该 UID 对根密钥进行分散得到电子标签个性化密钥 K1。双方通信过程中，使用 MAC 方式进行完整性校验，具体过程如下：

a) 发送方用个性化密钥 K1 计算待发送信息 M 的 MAC 值：MAC1=MAC(M,K1)，并将 MAC1 附加至信息 M 后，将 Token1=(M ‖ MAC1)发送给接收方。

b) 接收方收到 Token1 后，用个性化密钥 K1 计算收到的信息 M 的 MAC 值：MAC2=MAC (M,K1)，比较 MAC1 和 MAC2，如相等则通过完整性校验。

MAC 的计算过程如下：

a) 将信息 M 分成长度为 n 比特的数据分组 M1,M2,…,Mj。若 Mj 的长度不够，在后面补足，补足方式由具体应用规定；若 Mj 的长度刚好为 n 比特，则在其后补一个数据分组。

b) 计算 C1=Enc(M1,K1)。

c) 当 $j>1$ 时，计算 Ci=Enc(Mi⊕Ci−1,K1)，其中 $i=2,3,\cdots,j$。

d) MAC=Cj。

7.2.2 采用 HMAC 的完整性校验方法

电子标签和读写器通信过程中，发送方发送敏感信息前，读写器读取电子标签的 UID，使用该 UID 对根密钥进行分散得到电子标签个性化密钥 K1。双方通信过程中，使用 HMAC 的方式进行完整性校验。

选择一个密码杂凑函数 H，其输入数据块的字节长度为 B（$B=64$），输出数据块字节长度为 L（L 为所选密码杂凑算法的输出长度）。鉴别密钥 K1 的长度应是小于或等于 B，但大于或等于 L 的任何正整数值。

定义两个固定且不同的字符串 ipad 和 opad：

ipad = 字节'0x36'重复 B 次

opad = 字节'0x5C'重复 B 次

计算信息 M 的 HMAC：

$$HMAC(M)= H((K1\oplus opad),H((K1\oplus ipad),M))$$

具体计算过程说明如下：

a) 若密钥 K1 长度小于 B，在密钥 K1 后面添加 0 来创建一个字长为 B 的字符串 K。（例如，如果 K1 的字长是 20 字节，$B=64$ 字节，则 K1 后会加入 44 个字节 0x00）

b) 计算 $S_i=K\oplus ipad$。

c) 将输入信息 M 附加在 S_i 之后。使用密码杂凑函数 $H(S_i,M)$ 计算其杂凑值。

d) 计算 $S_o=K\oplus opad$。

e) 将 c)得到的 $H(S_i,M)$ 附加在 S_o 后面，并用密码杂凑函数 $H(S_o,H(S_i,M))$ 计算其杂凑值。

f) 以上 e)得到密码杂凑函数的输出即为最终的 HMAC 值。

7.3 身份鉴别

7.3.1 唯一标识符鉴别

唯一标识符鉴别需要在电子标签中存储 UID 以及验证码（MAC），该 MAC 是由 UID 与相关应用信息关联后采用密码算法计算产生，并在发行电子标签时写入。鉴别时，读写器获取电子标签的 UID、应用信息和 MAC，并根据相应的密码算法重新计算产生验证码（MAC′），通过比对 MAC 与 MAC′是否一致来鉴别电子标签的身份。

7.3.2 单向身份鉴别

7.3.2.1 电子标签对读写器的挑战响应鉴别

电子标签对读写器身份的真实性进行鉴别。

鉴别前，读写器读取电子标签的 UID，使用该 UID（或其他具有唯一性的参数）对根密钥分散得到与该电子标签存储的个性化密钥一致的分散密钥 K1。分散密钥的产生过程见 GM/T 0035.5—2014。

鉴别过程如下：

a) 读写器发送“身份鉴别”的命令给电子标签，电子标签中产生一随机数 R_T，并发送给读写器。电子标签使用密钥 K1 对随机数 R_T 进行加密，计算出 $R_T'=Enc(R_T,K1)$。

b) 读写器使用密钥 K1 对随机数 R_T 进行加密，计算出 $R_T''=Enc(R_T,K1)$，并将 R_T''发送给电子标签。

c) 电子标签将收到的 R_T''与 R_T'进行比较。如果 $R_T'=R_T''$，则通过对读写器的鉴别。

7.3.2.2 读写器对电子标签的挑战响应鉴别

读写器对电子标签身份的真实性进行鉴别。

鉴别前，读写器读取电子标签的 UID，使用该 UID（或其他具有唯一性的参数）对根密钥分散得到与该电子标签存储的个性化密钥一致的分散密钥 K1。分散密钥的产生过程见 GM/T 0035.5—2014。

鉴别过程如下：

a) 读写器生成随机数 R_R，发送给电子标签。读写器采用密钥 K1 对 R_R 进行加密，计算出 $R_R'=Enc(R_R,K1)$。

b) 电子标签使用密钥 K1 对 R_R 进行加密，计算出 $R_R''=Enc(R_R,K1)$，并将 R_R'' 发送给读写器。

c) 读写器比较 R_R' 和 R_R''。若 $R_R''=R_R'$，则通过对电子标签的鉴别。

7.3.3 双向身份鉴别

7.3.3.1 对称密码算法鉴别

采用分组密码算法实现双向身份鉴别。

双向鉴别前，读写器读取电子标签的 UID，使用该 UID(或其他具有唯一性的参数)对根密钥分散得到与该电子标签存储的个性化密钥一致的分散密钥 K1。分散密钥的产生过程见 GM/T 0035.5—2014。

鉴别过程如图 1 所示。

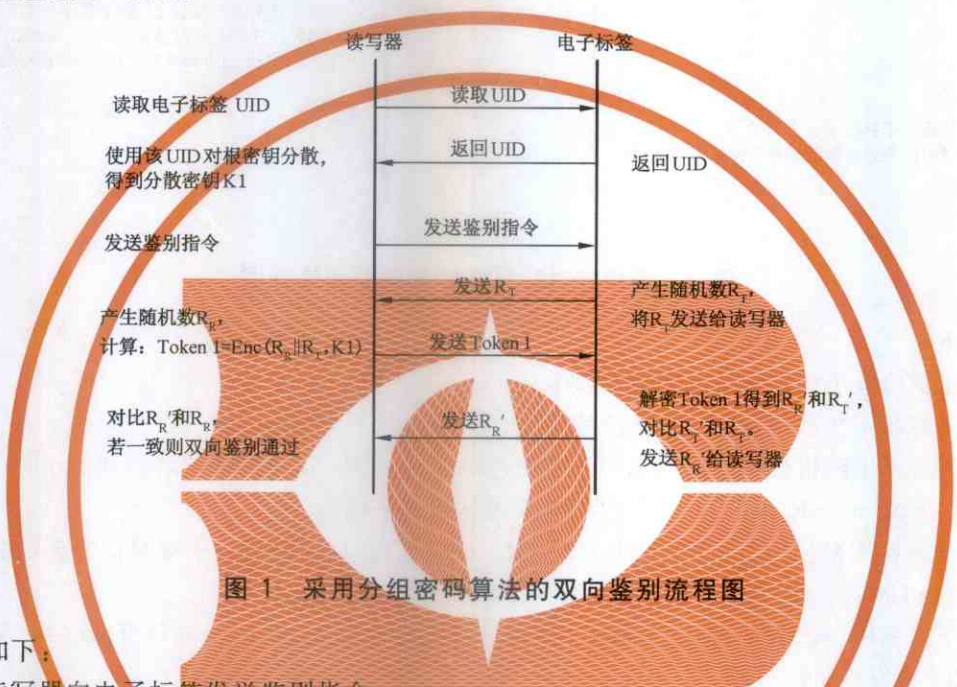

图 1 采用分组密码算法的双向鉴别流程图

描述如下：

a) 读写器向电子标签发送鉴别指令。

b) 电子标签接收到鉴别指令后，产生随机数 R_T(随机数长度为密码算法分组长度的一半)，发送给读写器。

c) 读写器产生随机数 R_R(随机数长度为密码算法分组长度的一半)，用电子标签的个性化密钥 K1 对 R_R 和 R_T 进行加密得到 $Token1=Enc(R_R \| R_T,K1)$；读写器将 Token1 发送给电子标签。

d) 电子标签用个性化密钥 K1 解密 Token1 得到 R_R' 和 R_T'。比较 R_T' 和 R_T，若 $R_T'=R_T$，则电子标签将 R_R' 发送给读写器。

e) 读写器比较 R_R' 和 R_R，若 $R_R'=R_R$，则双向鉴别通过。

也可对上述鉴别过程进行适当变化，如附录 A 所示。

7.3.3.2 非对称密码算法鉴别

采用非对称密码算法实现双向身份鉴别。

电子标签初始化或发行时，存储根公钥 Pu、电子标签的私钥 Pr_T 和用根私钥签发的证书 CER_T。读写器存储根公钥 Pu、读写器的私钥 Pr_R 和用根私钥签发的证书 CER_R。

鉴别过程如图 2 所示。

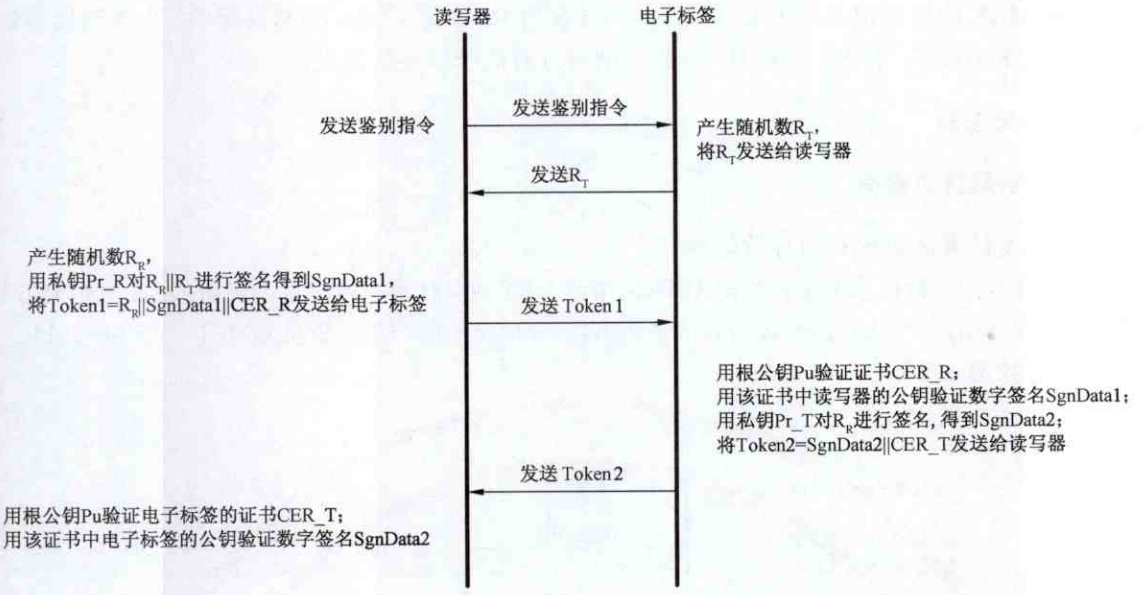

图 2　采用非对称算法的双向鉴别流程图

描述如下：

a) 读写器向电子标签发送鉴别请求命令。

b) 电子标签产生随机数 R_T，发送给读写器。

c) 读写器产生随机数 R_R，用自己的私钥 Pr_R 对 $R_R \| R_T$ 直接进行签名得到 SgnData1，并将数据块 Token1 = $R_R \| SgnData1 \| CER\_R$ 发送给电子标签。

d) 电子标签用根公钥 Pu 验证证书 CER_R。如验证通过，用该证书中读写器的公钥验证数字签名 SgnData1。如果验证通过，则完成对读写器的身份鉴别。

e) 电子标签用自己的私钥 Pr_T 对 R_R 直接进行签名得到 SgnData2，并将 Token2 = SgnData2 ‖ CER_T 发送给读写器。

f) 读写器用根公钥 Pu 验证电子标签的证书 CER_T。如果验证通过，用该证书中电子标签的公钥验证数字签名 SgnData2，如果验证通过，则完成对电子标签的身份鉴别，双向鉴别通过。

也可对上述鉴别过程进行适当变化，如附录 B 所示。

附 录 A
（资料性附录）
采用 SM7 对称分组密码算法的双向身份鉴别与流加密应用

A.1 概述

本附录给出了一种采用 SM7 对称分组密码算法的双向身份鉴别方式，双向身份鉴别过程中产生用于流加密密码流生成的初始向量。

A.2 采用 SM7 对称分组密码算法的双向身份鉴别

进行双向身份鉴别前，读写器读取电子标签的 UID，使用该 UID 对根密钥分散得到电子标签个性化密钥 KEY。

双向身份鉴别和密钥协商过程如下：

a) 读写器发送鉴别指令。

b) 电子标签接收指令后发送由随机数发生器产生的 32 位 R_T。

c) 读写器收到 R_T 后，由随机数发生器产生 32 位随机数 R_R，并以 128 位 KEY 为密钥进行加密，加密的明文为 R_R（左半部分）和 R_T（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 R_T' 与之前产生的 R_T 比较。

e) 电子标签比较 R_T' 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 R_T''（左半部分，R_T'' 用于密钥协商）和解密 Token1 得到的 R_R'（右半部分），得到的 64 位密文为 Token2。如果 R_T' 与 R_T 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 R_R' 与原先发送的 R_R，如果 R_R' 比较正确，鉴别通过，否则鉴别失败。

双向身份鉴别过程见图 A.1。

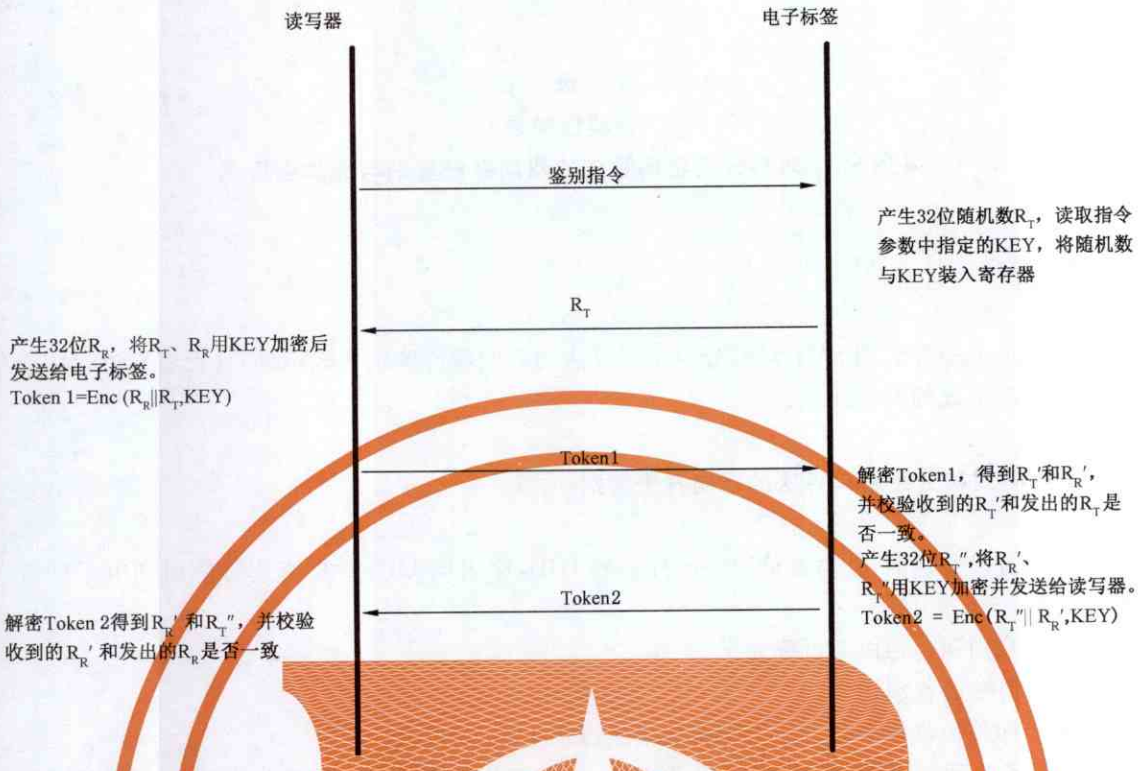

图 A.1 基于 SM7 对称密码算法的双向身份鉴别

A.3 流加密应用

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.1 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）。

附 录 B
（资料性附录）
采用非对称密码算法的双向身份鉴别和密钥协商

采用非对称密码算法实现双向身份鉴别和密钥协商，即在身份鉴别的同时协商出工作密钥。

电子标签初始化或发行时，存储根公钥 Pu、电子标签的私钥 Pr_T 和用根私钥签发的证书 CER_T。读写器存储根公钥 Pu、读写器的私钥 Pr_R 和用根私钥签发的证书 CER_R。双向身份鉴别和密钥协商过程如下：

a) 读写器向电子标签发送密钥协商请求命令。

b) 电子标签产生随机数 R_T，并将 $R_T \| CER\_T$ 发送给读写器。

c) 读写器用根公钥 Pu 验证电子标签的证书 CER_T。读写器产生随机数 R_R，用自己的私钥 Pr_T 对 $R_R \| R_T$ 进行签名得到 SgnData1。读写器生成密钥 K_{TR}，并用证书 CER_T 中的电子标签公钥对 K_{TR} 进行加密得到 K_{TR}'，并将 $Token1 = R_R \| SgnData1 \| CER\_R \| K_{TR}'$ 发送给电子标签。

d) 电子标签用根公钥 Pu 验证读写器的证书 CER_R。如 CER_R 验证通过，用读写器公钥验证数字签名 SgnData1。如 SgnData1 验证通过，用自己的私钥 Pr_T 解密 K_{TR}' 得到 K_{TR}。

e) 电子标签用自己的私钥 Pr_T 对 R_R 进行签名得到 SgnData2，用证书 CER_R 中的读写器公钥对 K_{TR} 加密得到 K_{TR}''，并将 $Token2 = SgnData2 \| K_{TR}''$ 发送给读写器。

读写器用 CER_T 中的公钥验证数字签名 SgnData2。如验证通过，读写器用自己的私钥 Pr_R 解密 K_{TR}''，并将结果与 K_{TR} 比较，如 $K_{TR}'' = K_{TR}$，则 K_{TR} 为本次协商的工作密钥。

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4部分：电子标签与读写器通信密码
应用技术要求
GM/T 0035.4—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　字数 20 千字
2014年4月第一版　2014年4月第一次印刷
*
书号：155066·2-27014　定价 18.00 元

GM/T 0035.4-2014