ICS 35.040

L 80

中 华 人 民 共 和 国 国 家 标 准

GB/T XXXX.3—XXXX

信息安全技术
射频识别系统密码应用技术要求
第3部分：密钥管理技术要求

Information security technology-Specifications of cryptographic application for RFID systems-Part 3: specification for key management

（征求意见稿）

××××-××-××发布　　××××-××-××实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前 言

GB/T XXXX《信息安全技术 射频识别系统密码应用技术要求》分为三个部分：

——第1部分：密码安全保护框架及安全级别

——第2部分：电子标签与读写器及其通信密码应用技术要求

——第3部分：密钥管理技术要求

本部分为GB/T XXXX的第3部分。

本部分按照 GB/T 1.1—2009给出的规则起草。

本部分由国家密码管理局提出。

本部分由全国信息安全标准化技术委员会归口。

本部分中的附录A为资料性附录。

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

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

信息安全技术　射频识别系统密码应用技术要求
第3部分：密钥管理技术要求

1　范围

本部分规定了射频识别系统在采用密码机制时电子标签、读写器及其通信相关的密钥管理要求。

本部分适用于指导射频识别系统密钥管理的设计、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。

GB/T 25069-2010　信息安全技术 术语

GB/T XXXX.1-XXXX　信息安全技术 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

3　术语和定义

GB/T 25069-2010中界定的以及下列术语和定义适用于本部分。

3.1

安全存取模块 secure access module

嵌入在读写器内的密码模块，为读写器提供安全服务。

3.2

电子标签 RFID tag

一种用于射频识别，载有与预期应用相关的电子识别信息的载体，每个标签具有惟一的电子编码。通常由耦合元件及芯片组成，包括非接触CPU卡和非接触存储卡。

3.3

读写器 reader

与电子标签进行数据通信并对标签进行读、写操作的设备。

3.4

对称密码算法 symmetric cryptographic algorithm

加解密使用相同密钥的密码算法。

3.5

非对称密码算法/公钥密码算法 asymmetric cryptographic algorithm/public key cryptographic algorithm

加解密使用不同密钥的密码算法。其中一个密钥（公钥）可以公开，另一个密钥（私钥）必须保密，且由公钥求解私钥是计算不可行的。

3.6

分散密钥 derived key

由根密钥和非保密可变数据生成的对称密钥。

3.7

根密钥 derivation key

用来生成分散密钥的密钥。

3.8

公钥 public key

非对称密码算法中可以公开的密钥。

3.9

公钥证书 public key certificate

一种数字证书，由认证机构签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及一些扩展信息的数字文件。

3.10

机密性 confidentiality

保证信息不被泄露给非授权的个人、进程等实体的性质。

3.11

加密 encipherment /encryption

对数据进行密码变换以产生密文的过程。

3.12

鉴别 authentication

确认一个实体所声称的身份或信息的真实性。

3.13

解密 decipherment /decryption

加密过程对应的逆过程。

3.14

抗抵赖 non-repudiation

也称不可否认，证明一个操作或事件已经发生且无法否认的机制。

3.15

密码模块 cryptographic module

实现密码运算功能的、相对独立的软件、硬件、固件或其组合。

3.16

密码算法 cryptographic algorithm

描述密码处理过程的运算规则。

3.17

密码杂凑函数 cryptographic hash function

又称密码散列函数或密码哈希函数，将一个任意长的比特串映射到一个固定长的比特串的函数，且满足下列三个特性：

（1）为一个给定的输出找出能映射到该输出的一个输入是计算上困难的；

（2）为一个给定的输入找出能映射到同一个输出的另一个输入是计算上困难的；

（3）要发现不同的输入映射到同一输出是计算上困难的。

3.18

密钥管理 key management

根据安全策略，对密钥的产生、分发、存储、更新、归档、撤销、备份、恢复和销毁等密钥全生命周期的管理。

3.19

密钥协商 key agreement

两个或多个实体通过相互传送一些消息来共同建立一个共享的秘密密钥的协议，且各个实体无法预先确定这个秘密密钥的值。

3.20

射频识别 radio frequency identification

利用射频信号通过空间耦合(交变磁场或电磁场)实现信息的无接触传递，并通过所传递的信息达到识别目的。

3.21

审计 audit

对信息系统记录与活动进行的独立观察和考核。

3.22

数据完整性 data integrity

数据没有遭受以非授权方式所作的篡改或破坏的性质。

3.23

数字签名 digital signature

签名者使用私钥对待签名数据的杂凑值做密码运算得到的结果，该结果只能用签名者的公钥进行验证，用于确认待签名数据的完整性、签名者身份的真实性和签名行为的抗抵赖性。

3.24

私钥 private key

非对称密码算法中只能由拥有者使用的不公开密钥。

3.25

SM1 算法 SM1 algorithm

一种分组密码算法，分组长度为 128 比特，密钥长度为 128 比特。

3.26

SM2 算法 SM2 algorithm

由 GB/T 32918《信息安全技术 SM2 椭圆曲线公钥密码算法》定义的一种算法。

3.27

SM3 算法 SM3 algorithm

由 GB/T 32905《信息安全技术 SM3 密码杂凑算法》定义的一种算法。

3.28

SM4 算法 SM4 algorithm

由 GB/T 32907《 SM4 分组密码算法》定义的一种算法。

3.29

SM7 算法 SM7 algorithm

一种分组密码算法，分组长度为 128 比特，密钥长度为 128 比特。

3.30

随机数 random number

一种数据序列，其产生不可预测，其序列没有周期性。

3.31

消息鉴别码 message authentication code

又称消息认证码，是消息鉴别算法的输出。

3.32

惟一标识符 unique identifier

由电子标签芯片制造商固化在电子标签芯片内的惟一标识符，包含芯片生产序列号、经注册的厂商代码等惟一性信息。

4 符号和缩略语

下列符号和缩略语适用于本文件。

Dec(X,K) 解密运算符，用密钥 K 对 X 进行解密运算

Enc(X,K) 加密运算符，用密钥 K 对 X 进行加密运算

RFID 射频识别（Radio Frequency IDentification）

UID 惟一标识符（Unique IDentifier）

5 密钥体制

5.1 对称密钥体制

适用于电子标签与读写器之间的身份鉴别、访问控制、机密性及完整性的安全保护。按照射频识别系统中对称密钥产生方式的要求不同，可以将对称密钥分为根密钥、分散密钥和传输保护密钥等，密钥类别及产生方式见表 1。

表 1 密钥类别与产生方式

密钥类别	产生方式
根密钥	由密钥生成系统通过随机数发生器生成
分散密钥	由根密钥经密钥分散因子分散产生
传输保护密钥	在电子标签与读写器进行信息传输前临时协商产生，用于信息传输的加密保护

其中，分散密钥由根密钥和 16 字节的密钥分散因子经符合国家密码管理部门指定的密码算法运算产生，应保证分散密钥被泄露不会导致根密钥和其他分散密钥的泄露。

分散密钥产生过程见图 1。

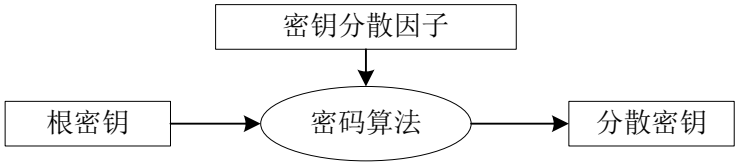

图 1 分散密钥产生过程

密钥可以进行多级分散，每一级分散所选择的密钥分散因子应采用能够惟一标识该级内应用对象（如厂商编号等）的信息获得。该信息的长度应不大于 16 字节、且不小于 4 字节；信息长度不足 16 字节时，应在右边填 0x00 补齐。

电子标签内仅存储最后一级的分散密钥，在进行最后一级密钥分散时，应以能够标识电子标签惟一性的信息（如 UID）作为密钥分散因子。

密钥应按用途使用。在同一级内，不同用途的密钥应由上一级不同的密钥分散产生。

读写机具根据应用需要存储根密钥或某一级的分散密钥，但不应存储最后一级的分散密钥。

5.2 非对称密钥体制

非对称密钥体制适用于电子标签和读写器之间业务行为涉及的抗抵赖、身份鉴别、访问控制、机密性及完整性的安全保护。

非对称密钥管理的技术要求参见国家密码管理主管部门的相关要求。

6 对称密钥管理模型

在射频识别系统中，对称密钥管理模型如图 2 所示。

射频识别系统对称密钥管理模型包含了密钥生命周期中的密钥生成、密钥分发、密钥使用和密钥销毁/注销的四个主要过程。

按照 GB/T XXXX.1-XXXX 中所规定的标准适用范围，射频识别系统对称密钥管理模型包括了电子标签和读写器等密码设备的密钥管理。

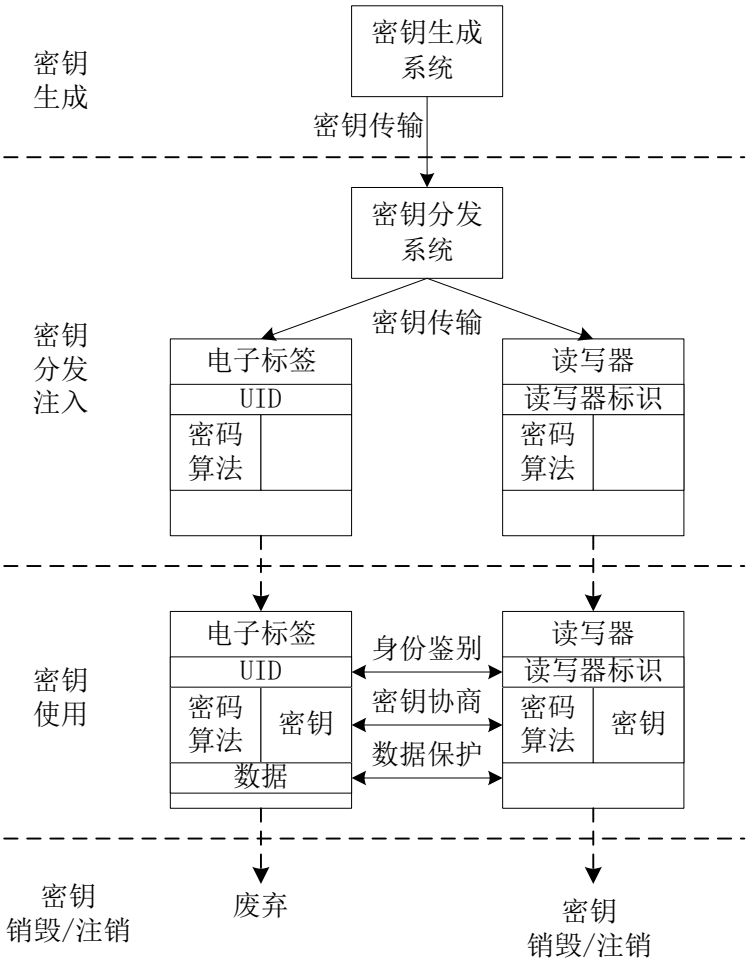

图 2 射频识别系统对称密钥管理模型

图 2 中，密钥生成系统完成射频识别系统中密钥的生成和密钥的分散，密钥分发系统完成对电子标签和读写器的密钥分发与注入；密钥在安全密码设备中使用，安全密码设备包括读写器内安全存取模块和电子标签。

7 对称密钥管理通用要求

在系统中应有必要的安全保护措施，以达到保障密钥安全的要求。

存储在电子标签内的对称密钥，不能被读出。

存储在读写器内的对称密钥，应存储在安全存取模块内，且不能被读出。

在密钥管理中的密钥生成、存储、分散、分发、注入、备份、恢复、验证、使用、更新、归档、注

销和销毁等内容应符合国家密码管理部门的相关要求。

8 对称密钥使用要求

8.1 身份鉴别

8.1.1 惟一标识符鉴别

电子标签需存储由电子标签惟一标识符以及与相关应用信息结合建立的验证码，读写器需存储产生这一验证码的密钥。

8.1.2 挑战响应鉴别

用于挑战响应鉴别的密钥必须具有惟一性。

电子标签存储的用于挑战响应鉴别的密钥应由相应根密钥与电子标签 UID 分散产生。

读写器应存储用于挑战响应鉴别的根密钥，并应能够通过读取电子标签 UID 分散产生与该电子标签内存储的用于挑战响应鉴别的密钥一致的密钥。

8.2 访问控制

用于访问控制的密钥必须具有惟一性。

电子标签存储的用于访问控制的密钥应由相应根密钥与电子标签 UID 分散产生；对具有多个存储区，且对存储区具有不同访问权限（读/写）控制的电子标签，应在电子标签内存储多个密钥分别用于不同权限的访问控制，即不同的权限采用不同的密钥进行控制。

根据对电子标签的访问权限，读写器应只存储用于相应权限访问控制的根密钥，并应能够通过读取电子标签 UID 分散产生与该电子标签内存储的与访问权限相对应的密钥一致的密钥。

8.3 机密性

8.3.1 存储加密

信息的存储加密应设置存储加密密钥，对自身存储数据的加密密钥应由随机数发生器产生，并在密码设备内安全存储，不能导出。

8.3.2 传输加密

传输加密密钥用于电子标签与读写器之间进行数据传输时的加密保护。

用于传输保护的加密密钥，可以是存储在电子标签和读写器内的固定密钥；也可以由电子标签与读写器在进行数据传输前临时协商产生，在通信完成后，废弃该密钥。

8.4 完整性

用于存储完整性保护的密钥的使用要求同 8.3.1 中的存储加密要求。

用于传输完整性保护的密钥的使用要求同 8.3.2 中的传输加密要求。

附录 A
（资料性附录）
射频识别系统的密钥管理示例

本附录描述了一个密钥管理示例，该示例适用于安全级别为三级的射频识别系统。

A.1 系统的应用要求

此应用的密钥管理要求基于以下基本条件：

a) 系统涉及多个电子标签发行者（指电子标签信息的原发者），每个发行者有一个惟一编码以示区别(厂商 ID)；
b) 每个电子标签出厂时都具有惟一标识符（芯片 UID）；
c) 对电子标签中划分的两个信息存储区（用标签信息区 1 和标签信息区 2 加以区别）进行安全访问控制，每个信息存储区需要有独立的访问控制权限，并对读写加以区分；
d) 电子标签具有专用的密钥存储区，对密钥存储区一次性写入且不能改写；
e) 电子标签的信息存储区中保存的数据使用专用密钥进行加密；
f) 读写器中的算法有：
   i) 对称密码算法 SM7，用于与电子标签进行双向身份鉴别、访问控制及传输过程中的信息加密；
   ii) 对称密码算法 SM1/SM4，用于信息存储加密和密钥分散；
   iii) 非对称密码算法 SM2，用于产生信息的数字签名及对签名进行验证；
   iv) 密码杂凑函数 SM3，用于产生信息摘要。
g) 标签中的算法是对称密码算法 SM7，用于与读写器进行双向身份鉴别、访问控制及传输过程中的信息加密；
h) 读写器可生成自己的公私钥对；
i) 仅电子标签的发行者具有对电子标签信息的写入权限，且具有写权限的发行者应具有读取权限；
j) 电子标签的使用者只具有对电子标签信息区 1 和信息区 2 的读取权限，不具有写入权限。并可以根据电子标签使用目的限定使用者对电子标签信息区的读取权限（如只允许读取电子标签信息区 1 或只允许读取电子标签信息区 2）；
k) 读写器与电子标签之间传输的信息需要进行加密保护；
l) 读写器具有抗电子标签原发抵赖功能。

A.2 密钥管理设计实现

A.2.1 密钥生成

需针对该应用系统建立密钥管理中心，除各读写器的公私钥对外，系统其他密钥在密钥管理中心的密钥生成设备中产生，要保证密钥管理中心的物理环境安全，在密钥生成、存储时不会泄露密钥，且生成过程需记录审计信息。

在密钥管理中心生成的密钥包括：

a) 电子标签信息区 1 的读取根密钥 K_{R1}；
b) 电子标签信息区 1 的写入根密钥 K_{W1}；
c) 电子标签信息区 2 的读取根密钥 K_{R2}；
d) 电子标签信息区 2 的写入根密钥 K_{W2}；
e) 电子标签数据存储加密根密钥 K_D；
f) 根公私密钥对，根公钥以证书（PubCert）的形式存储。

在读写器中生成的密钥包括：读写器自身的公私钥对（PKi 和 SKi）。此密钥对在读写器中生成，生成后私钥在读写器中安全存储，公钥上传给密钥管理中心的密码设备，由根私钥签名得到其公钥证书，再注入到读写器中，即读写器的公钥以证书（PubCerti）的形式存储。

A.2.2 密钥分散

采用密钥分散方法产生注入电子标签中的全部密钥和注入读写器中的部分密钥（具有写权限的密钥）。

由于 K_{W1} 和 K_{W2} 分别具有对电子标签信息区 1 和 2 的写入权限，且对于写入权限的使用仅限于各标签的发行者，因此需要对这两个密钥进行两级分散。第一级分散在密钥管理中心进行，利用厂商 ID 对根密钥进行分散，并将分散后的密钥派发给各电子标签发行者。第二级分散在各标签发行者向电子标签内写入密钥时进行，利用芯片 UID 对第一级分散后的密钥再次分散产生电子标签的个性化密钥，并写入电子标签的密钥区。

由于使用者可以读取任意标签发行者所发行电子标签的信息，因此，对于 K_{R1} 、K_{R2} 和 K_D 可以只利用芯片 UID 对根密钥进行一次分散即可。

采用 SM1/SM4 密码算法进行密钥分散。

一次分散的方法如下：

K_{W1}' = Enc（厂商 ID，K_{W1}）；

K_{W2}' = Enc（厂商 ID，K_{W2}）；

K_{R1}' = Enc（标签 UID，K_{R1}）；

K_{R2}' = Enc（标签 UID，K_{R2}）；

K_D' = Enc（标签 UID，K_D）。

对 K_{W1}' 和 K_{W2}' 还需进行二次分散，方法如下：

K_{W1}'' =Enc（标签 UID，K_{W1}'）；

K_{W2}'' = Enc（标签 UID，K_{W2}'）。

其中，用以区分各发行厂商或芯片的惟一标识的厂商 ID 或芯片 UID 作为分散因子，长度固定为 16 字节。对长度不足或超过 16 字节的厂商 ID 或芯片 UID，应采用以下方式进行处理：

a) 长度不足 16 字节时，通过在右边填充 0x00 补齐到 16 字节；

b) 长度超过 16 字节时，截取其中变化率最大的 16 字节作为分散因子，所截取部分应能够保证惟一性。

A.2.3 密钥分发和注入

密钥的分发和注入包括对读写器的密钥分发注入和对电子标签的密钥分发注入。

在分发和注入前应先检验密钥的完整性，在确保密钥未被篡改后，直接从安全密码设备中将密钥注入到读写器和电子标签中。

a) 读写器的密钥分发与注入

读写器密钥的分发和注入在密钥管理中心进行。首先读写器生成自身的公私钥对，私钥安全存储在读写器中，公钥上传给密钥管理中心的密码设备，由密钥管理中心的密码设备使用根私钥为其签名，得到读写器的公钥证书，然后根据读写器的不同应用，向读写器内注入不同的对称密钥、根公钥证书和读写器的公钥证书。密钥的完整性检验利用 SM3 算法，在密钥分发前计算对所有要注入的密钥一并计算验证码，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。

依据读写器的使用功能，各读写器使用的密钥见表 A.1。

表 A.1 不同功能读写器的密钥列表

密钥 / 读写器	K_{W1}'	K_{W2}'	K_{R1}	K_{R2}	K_D	PubCert	PubCerti	SKi
具有电子标签密钥写入功能	△	△	√	√	√			
具有电子标签信息写入功能	△	△			√	√	*	*
具有电子标签信息区 1 读功能			√		√	√	√	
具有电子标签信息区 2 读功能				√	√	√	√	

注：“√”表示在该功能的读写器内注入此密钥

“△”表示各电子标签发行者所使用的读写器内只注入各自的写密钥

“*”表示此密钥的公私钥对由读写器自己产生，私钥由该读写器安全存储，读写器的公钥证书由密钥管理中心签发。

b) 电子标签的密钥分发与注入

对于电子标签，先由密钥管理中心将密钥分发给用于密钥写入的读写器，再由读写器根据芯片 UID 对密钥进行分散后注入到电子标签内。

对注入电子标签的密钥的正确性验证，采用已经注入的密钥逐一进行身份鉴别的方式进行。如果身份鉴别通过，则对应的密钥注入正确。

注入到标签中的密钥有：K_{W1}'' 、K_{R1}' 、K_{W2}'' 、K_{R2}' 。

A.2.4 密钥存储

密钥管理中心的密钥采用加密的密钥组件的方式保存，使用密钥分割技术把密钥分割成至少两个部分。每一部分采用不同的密钥加密密钥进行加密，密钥加密密钥由不同的人保存。应在两人同时操作的情况下才能解密得到密钥明文，并且该明文只能出现在安全密码设备中，断电即消失。

读写器中的对称密钥和读写器的私钥安全存储在读写器的安全存取模块内，并确保不能以任何方式导出，根公钥和读写器公钥均以证书的形式存储。

电子标签上安全存储经电子标签 UID 分散后的密钥，并确保不能以任何方式导出。

A.2.5 根密钥备份

密钥管理中心生成的根密钥的副本采用以下两种方式之一脱机保存：

a) 加密保存在光盘、IC 卡或磁带上，密钥密文和其密钥加密密钥由两个人员分别保存，实现双重控制；

b) 采用密钥分割的方式，将密钥分成几个部分，每个有关人员保管一个部分，缺少任何一部分都不能正确恢复出密钥。

A.2.6 密钥验证

存储和备份的密钥定期检验。不管是采用了加密存储或密钥组件存储，每个密钥或组件都需要有验证码同时存储。每次检验时，应通过检查此验证码校验密钥完整性。

A.2.7 密钥更新与销毁

如果根密钥被泄露，重新生成新的根密钥，并将所有读写器的密钥更新，此后发行的电子标签也应注入更新后的密钥。

对于只具有读功能的读写器，需保留原有的读根密钥，以便支持对更新前的电子标签进行操作。

密钥更新后，旧的密钥应被归档，以备必要时验证以前交易的合法性。

A.2.8 密钥的使用

在读写器与电子标签采用对称密钥进行身份鉴别、访问控制等操作时，读写器应先采用 SM1/SM4 密码算法，根据读取的电子标签的 UID 对相应操作权限的根密钥（如 K_{R1}）进行分散，以获得与电子标签共享的对称密钥。

采用抗读写器抵赖功能时，先由读写器利用自己的私钥对写入电子标签的信息进行签名，并将电子标签信息、数字签名连同产生签名的读写器的信息一同写入电子标签。在读取验证时，验证的读写器先利用根公钥验证产生签名的读写器的公钥证书，再用产生签名的读写器的公钥验证数字签名。

其中，验证读写器在密钥管理中心下载密钥时已经下载了根公钥证书，对产生签名的读写器的公钥证书的获取，根据系统的具体应用情况，可以采用以下的方式：

a) 若读写器可实时与后台管理系统连接，可以根据从电子标签内读取的产生签名的读写器信息从后台系统实时的获得相应读写器的公钥证书；
b) 若读写器不能实时与后台管理系统连接，根据系统规模大小，可在读写器内存储系统内所有公钥证书（必要时可定期更新）；
c) 若电子标签存储空间允许，可以将产生数字签名的读写器的公钥证书在写入数字签名的同时一同写入电子标签，当需要进行数字签名验证时，可直接由读写器从电子标签内读取获得该公钥证书。