ICS 35.040
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0096—2020

射频识别防伪系统密码应用指南

Guide for RFID anti-counterfeiting cipher application

2020-12-28 发布　　2021-07-01 实施

国家密码管理局　　发布

中华人民共和国密码
行业标准
射频识别防伪系统密码应用指南
GM/T 0096—2020
*
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)68533533　发行中心:(010)51780238
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 2　字数 60 千字
2021年4月第一版　2021年4月第一次印刷
*
书号:155066·2-35975　定价 36.00 元

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：北京中电华大电子设计有限责任公司、安徽云盾信息技术有限公司、上海复旦微电子集团股份有限公司、上海华申智能卡应用系统有限公司、复旦大学、兴唐通信科技有限公司、紫光同芯微电子有限公司、华大半导体有限公司、北京华大智宝电子系统有限公司、上海坤锐电子科技有限公司、成都卫士通信息产业股份有限公司、北京三未信安科技发展有限公司、中国电力科学研究院有限公司、中国电子技术标准化研究院。

本文件主要起草人：周建锁、董浩然、沈宁、柳逊、顾震、陈波涛、费渡、孙孝年、王政、王俊宇、王俊峰、吕永其、盛敬刚、李静进、李强、刘晓东、赵兵、陈跃、沈磊。

射频识别防伪系统密码应用指南

1 范围

本文件规定了射频识别防伪应用的安全类别、系统规划与实施。

本文件适用于射频识别防伪应用中密码安全方案设计、密码产品选用与系统实施。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 28925 信息技术 射频识别 2.45 GHz 空中接口协议

GB/T 29768 信息技术 射频识别 800/900 MHz 空中接口协议

GB/T 32915 信息安全技术 二元序列随机性检测方法

GB/T 37033.1—2018 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

GB/T 37033.2—2018 信息安全技术 射频识别系统密码应用技术要求 第 2 部分：电子标签与读写器及其通信密码应用技术要求

GB/T 37033.3—2018 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

GB/T 37092 信息安全技术 密码模块安全要求

GM/T 0008 安全芯片密码检测准则

GM/T 0014 数字证书认证系统密码协议规范

GM/T 0030 服务器密码机技术规范

GM/T 0039 密码模块安全检测要求

GM/T 0040—2015 射频识别标签模块密码检测准则

GM/Z 4001—2013 密码术语

SB/T 10768—2012 基于射频识别的瓶装酒追溯与防伪标签技术要求

3 术语和定义

GB/T 37033.1—2018 和 GM/Z 4001—2013 界定的以及下列术语和定义适用于本文件。

3.1

安全存取模块 secure access module

嵌入在电子标签读写器内的密码模块，为读写器提供安全服务。

3.2

单向鉴别 unidirectional authentication

由读写器发起对标签的身份鉴别。

3.3

对称密码算法　symmetric cryptographic algorithm

加密和解密使用相同密钥的密码算法。

3.4

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

加密和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。

3.5

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。

3.6

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。

3.7

双向鉴别　bidirectional authentication

读写器和标签之间进行的相互身份鉴别。

3.8

密码边界　cryptographic boundary

明确定义的连续边线,该边线建立了密码模块的物理和/或逻辑边界,并包括了密码模块的所有硬件、软件、和/或固件部分。

3.9

密码机　cryptographic machine

能够独立运行的,实现密码运算、密钥管理等功能,提供密码服务的设备。

3.10

密码模块　cryptographic module

实现了安全功能的硬件、软件和/或固件的集合,并且被包含在密码边界内。

4　缩略语

下列缩略语适用于本文件。

CA:数字证书认证机构(Certificate Authority)

KGC:密钥生成中心(Key Generation Center)

NFC:近场通信(Near Field Communication)

RFID:射频识别(Radio Frequency IDentification)

SAM:安全存取模块(Secure Access Module)

TF:TF 卡(Trans-flash Card)

UID:唯一标识符(Unique IDentifier)

5　概述

基于射频识别防伪系统的密码应用框架如图 1 所示,由标签发行、防伪验证、中间件、信息处理系

统、网关、密钥管理系统和 CA 组成。其中，CA 和中间件作为可选部分，根据应用需求选用。

防伪验证由读写器和电子标签实现，当读写器作为信息透明传输通道使用时，标签通过中间件或信息处理系统实现防伪验证，对读写器无密码安全要求。

标签发行由读写器和电子标签实现，当读写器作为信息透明传输通道使用时，标签通过中间件或信息处理系统完成发行，对读写器无密码安全要求。

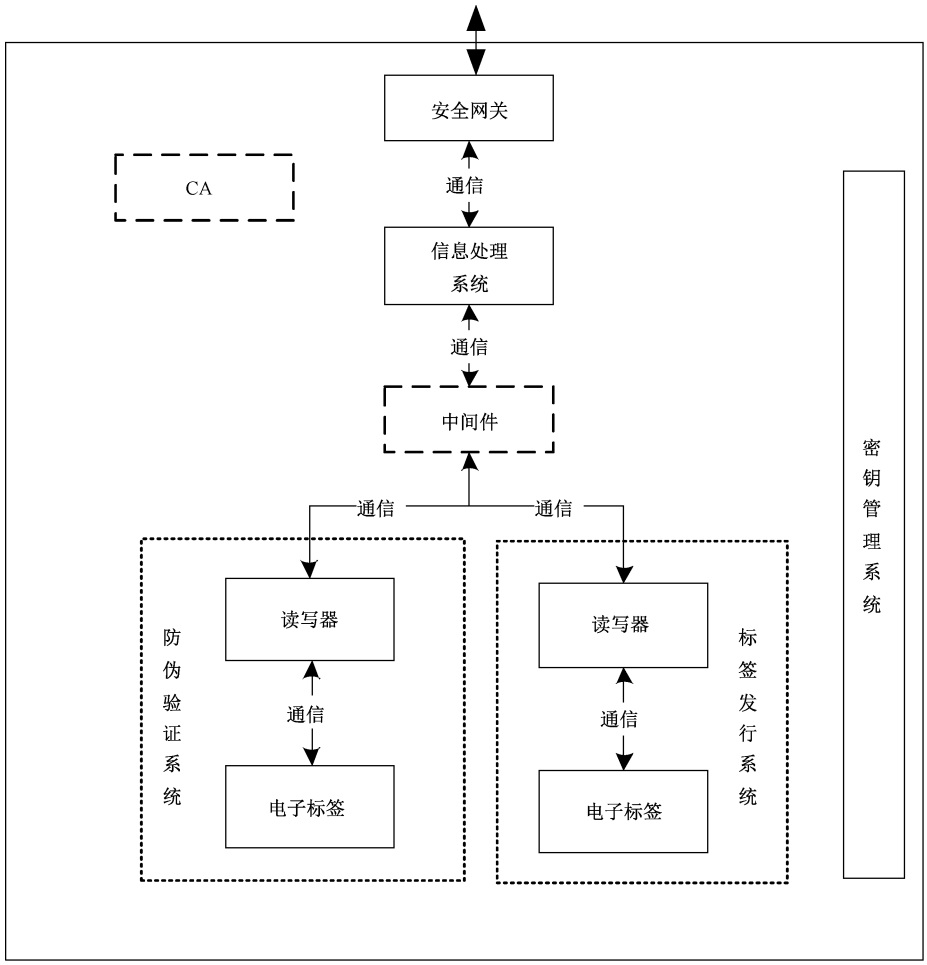

图 1　射频识别防伪系统密码应用框架

6　安全类别

6.1　安全级别

根据射频识别防伪系统对密码安全技术的要求不同，可将防伪系统安全级别分为两类，即 A 类和 B 类。

6.2　A 类系统

A 类防伪密码安全级别的系统（以下简称 A 类系统）应符合 GB/T 37033.1—2018 中 6.2.2 规定的二级安全级别要求。系统中的随机数应符合 GB/T 32915 的要求。

6.3 B类系统

B类防伪密码安全级别的系统(以下简称B类系统)符合GB/T 37033.1—2018中6.2.4规定的四级安全级别要求。系统中的随机数应符合GB/T 32915的要求。

7 A类系统规划与实施

7.1 系统规划

7.1.1 系统架构

A类系统,采用对称密码算法,通过读写器对电子标签的身份鉴别,或读写器与电子标签之间的双向身份鉴别,提高射频识别标签的安全防伪能力。双向身份鉴别见附录A。A类系统提供一种数字化的安全防伪方案,方便消费者使用NFC智能终端,通过移动互联网,对贴有RFID防伪标签的商品进行验伪查询。

A类系统的系统架构参考设计如图2所示。

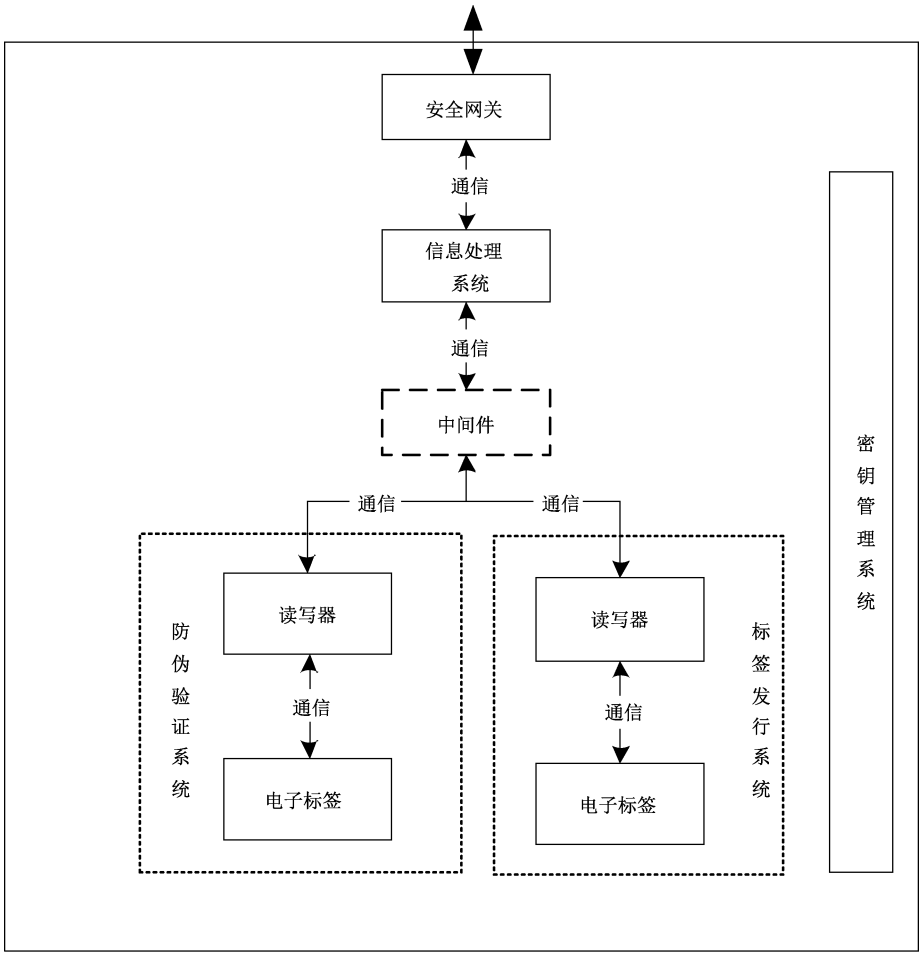

图2 A类防伪密码安全级别系统架构示意图

7.1.2 标签发行系统

对防伪标签进行密钥发行，并在发行完成后，将商品溯源相关信息与防伪标签 UID 进行关联，存入信息处理系统中，便于消费者进行商品溯源防伪。

7.1.3 防伪验证系统

防伪验证系统提供对防伪标签的验证查询服务，以及防伪数据信息（产品生产、销售、验证查询等数据）的下载等。

7.1.4 信息处理系统

包括商品生产、仓储、运输、销售等多类信息的处理系统。

7.1.5 密钥管理系统

负责整个系统中密钥的生成、分散、存储等密钥管理功能，是整个系统中安全核心；为保证该系统的安全性，密钥管理系统部署在独立的密钥管理中心，与商品溯源防伪应用系统的其他部分（包括信息处理系统、防伪验证系统、标签发行系统）物理隔离。密钥管理系统生成的密钥，通过密钥卡等安全措施，分发到商品防伪溯源应用系统的其他部分。

7.2 产品选择

7.2.1 射频电子标签

7.2.1.1 密码安全要求

A 类系统中使用的射频电子标签满足以下密码安全要求。

a) 符合 GM/T 0040—2015 中规定的Ⅰ类或Ⅱ类检测要求。

b) 身份鉴别：应支持读写器对电子标签的身份鉴别。读写器对电子标签的身份鉴别实现方式见 GB/T 37033.2—2018 中的 8.3.2.2。

c) 访问控制：支持访问控制功能，保障存储信息在受控权限下进行访问。电子标签的访问控制实现方式见 GB/T 37033.2—2018 中 6.1.5。电子标签的访问控制检测见 GM/T 0040—2015 中 6.5。

d) 密码算法：应采用国家密码管理部门核准的密码算法。

e) 宜选用国家密码管理部门核准的密码产品。

7.2.1.2 可选密码安全要求

A 类系统中使用的射频电子标签根据应用需求，可选择支持以下密码安全要求。

a) 存储信息机密性保护：可选择支持对电子标签内存储信息机密性保护，电子标签存储信息的机密性实现方式见 GB/T 37033.2—2018 中 6.1.1.1。电子标签存储信息的机密性检测见 GM/T 0040—2015 中 6.3.3。

b) 传输信息机密性保护：可选择支持对电子标签传输信息保护功能。电子标签传输信息的机密性实现方式见 GB/T 37033.2—2018 中 6.1.1.2。电子标签传输信息的机密性检测见 GM/T 0040—2015 中 6.3.2。

c) 存储信息完整性保护：可选择支持对电子标签存储信息完整性保护功能。电子标签存储信息的完整性实现方式见 GB/T 37033.2—2018 中 6.1.2.1。电子标签存储信息的完整性检测见 GM/T 0040—2015 中 6.3.5。

d) 传输信息完整性保护:可选择支持对电子标签传输信息的完整性保护功能。电子标签传输信息的完整性实现方式见 GB/T 37033.2—2018 中 6.1.2.2。电子标签传输信息的完整性检测见 GM/T 0040—2015 中 6.3.4。

e) 身份鉴别:可选择支持电子标签对读写器的身份鉴别。电子标签对读写器的身份鉴别实现方式见 GB/T 37033.2—2018 中的 8.3.2.1。电子标签对读写器的身份鉴别应通过 GM/T 0040—2015 中 6.2 和 6.3 的检测。读写器与电子标签之间的双向身份鉴别的实现方式见 GB/T 37033.2—2018 中 8.3.3.1。读写器与电子标签之间的双向身份鉴别应通过 GM/T 0040—2015 中 6.2 和 6.3 的检测。

f) 抗电子标签原发抵赖:可选择支持抗电子标签原发抵赖功能。抗电子标签原发抵赖的实现方式见 GB/T 37033.2—2018 中 6.1.3.1。抗电子标签原发抵赖检测见 GM/T 0040—2015 中 6.6.1。

7.2.2 射频读写器

7.2.2.1 密码安全要求

A 类系统中使用的密码安全功能射频读写器可满足以下密码安全要求。

a) 读写器使用的 SAM 芯片应符合 GM/T 0008 规定的不低于二级的检测要求。

b) 身份鉴别:应支持读写器对电子标签的身份鉴别。读写器对电子标签的身份鉴别实现方式见 GB/T 37033.2—2018 中 8.3.2.2。

c) 应支持访问控制功能。读写器访问控制实现方式见 GB/T 37033.2—2018 中 6.2.5。

d) 密码算法:应采用与电子标签中密码算法相适应的国家密码管理部门核准的密码算法。

e) 宜选用国家密码管理部门核准的密码产品。

7.2.2.2 可选密码安全要求

A 类系统中使用的密码安全功能射频读写器根据应用需求,可选择支持以下密码安全要求。

a) 存储信息的机密性:可选择支持对读写器内存储信息的机密性保护。读写器存储信息的机密性实现方式见 GB/T 37033.2—2018 中 6.2.1.1。

b) 传输信息的机密性:可选择支持对读写器传输信息保护功能。读写器传输信息的机密性实现方式见 GB/T 37033.2—2018 中 6.2.1.2。

c) 存储信息的完整性:A 类安全级别读写器可选择支持对读写器存储信息完整性保护功能。读写器存储信息的完整性实现方式见 GB/T 37033.2—2018 中 6.2.2.1。

d) 传输信息的完整性:可选择支持对读写器传输信息完整性保护功能。读写器传输信息的完整性实现方式见 GB/T 37033.2—2018 中 6.2.2.2。

e) 身份鉴别:可选择支持电子标签对读写器的身份鉴别。电子标签对读写器的身份鉴别实现方式见 GB/T 37033.2—2018 中的 8.3.2.1。电子标签对读写器的身份鉴别应通过GM/T 0040—2015 中 6.2 和 6.3 的检测。读写器与电子标签之间的双向身份鉴别的实现方式见 GB/T 37033.2—2018 中 8.3.3.1。读写器与电子标签之间的身份鉴别应通过 GM/T 0040—2015 中 6.2 和 6.3 的检测。

f) 抗电子标签原发抵赖:可选择支持抗电子标签原发抵赖功能。抗电子标签原发抵赖实现方式见 GB/T 37033.2—2018 中 6.2.3.1。抗电子标签原发抵赖检测见 GM/T 0040—2015 中6.6.1。

g) 可选择支持审计功能。读写器的审计记录实现方式见 GB/T 37033.2—2018 中 6.2.6。

h) 密码算法:可选择采用国家密码管理部门核准的密码算法。

7.2.3 安全网关

宜选用国家密码管理部门核准的密码产品。

7.2.4 密码机

符合 GM/T 0030 要求，宜选用国家密码管理部门核准的密码产品。

7.3 实施建议

7.3.1 信息处理系统

使用安全网络及网关产品保障信息处理系统传输安全性；保障信息处理系统存储和访问安全性，见 GB/T 37092 和 GM/T 0039。

7.3.2 中间件

使用安全网络及网关产品保障中间件传输安全性；保障中间件存储和访问安全性，见 GB/T 37092 和 GM/T 0039。

7.3.3 密钥管理系统

电子标签的密钥管理见 GB/T 37033.3—2018。

针对电子标签密钥管理的检测见 GM/T 0040—2015 中 6.9。

读写器的密钥管理见 GB/T 37033.3—2018。密码机密钥管理系统提供防伪标签发行系统、防伪验证系统、信息处理系统的密钥产生和管理，密钥进行分级控制和管理。

密钥应至少为三级，并逐级进行散列。厂商设立密钥管理机构并产生根密钥，根密钥通过一级分散因子散列出鉴别主密钥；鉴别主密钥通过二级分散因子散列出防伪标签鉴别密钥。密钥散列如图 3 所示。

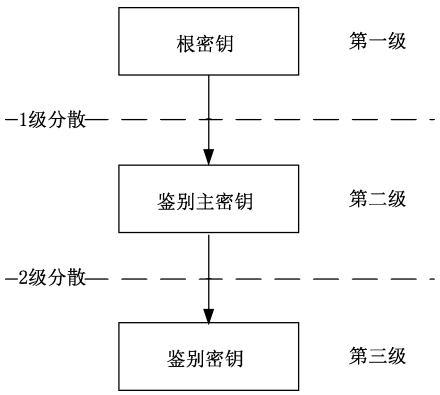

图 3 密钥分级管理示意图

注 1：1 级分散因子，厂商代码或商品类别代码。

注 2：级分散因子，防伪标签 UID。

7.3.4 透明传输通道读写器要求

射频识别标签发行、防伪验证过程中，如读写器作为信息透明传输通道使用时，标签通过中间件或信息处理系统实现防伪验证，对读写器无密码安全要求。

7.4 应用方案

A 类射频识别防伪密码应用方案见附录 B。

8 B 类系统规划与实施

8.1 系统规划

8.1.1 系统架构

B 类系统采用非对称密钥体制。

B 类系统，采用非对称加密方法进行身份鉴别和权限控制，防止商品生产、流通、销售各个环节数据伪造，实现商品全流程跟踪。支持离线认证、独立认证；支持商品全流程各阶段数据记录，满足商品的个性化需求和收藏性需求的信息写入，满足商品渠道管理的需求。

B 类系统的系统架构参考设计如图 4 所示。

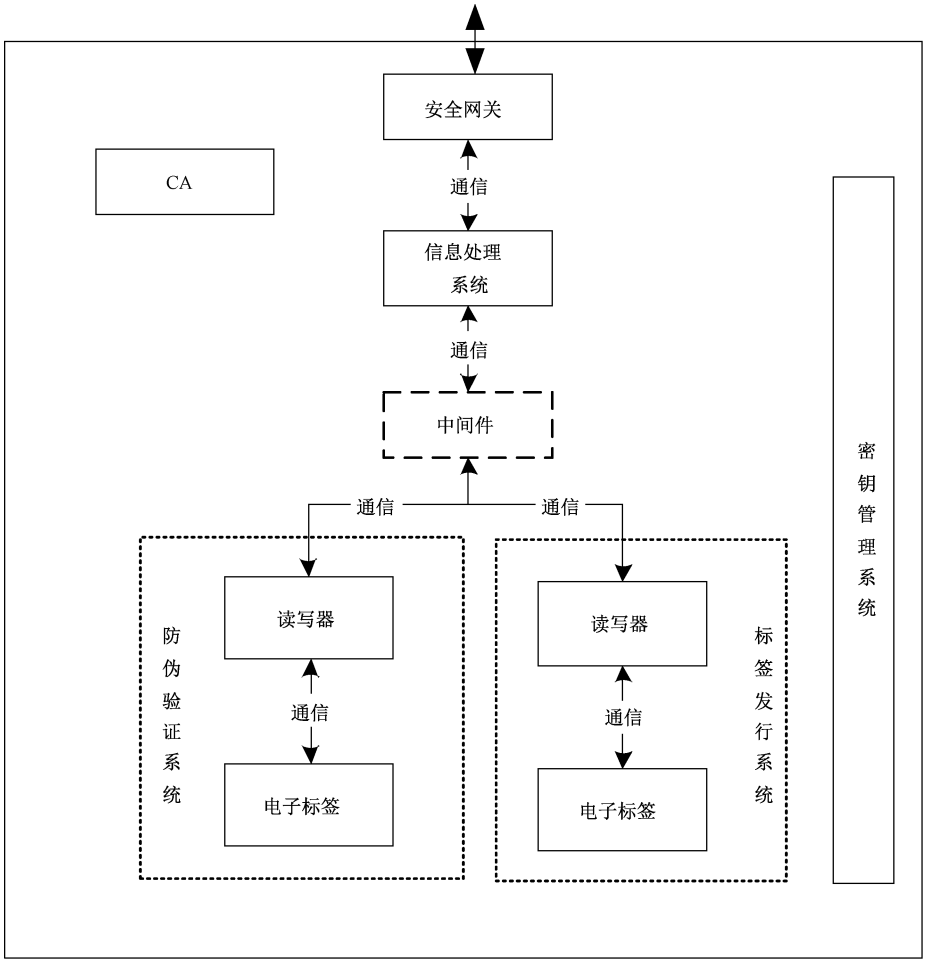

图 4 B 类防伪密码安全级别系统架构示意图

8.1.2 标签发行系统

对防伪标签进行密钥发行，并在发行完成后，将商品溯源相关信息与防伪标签 UID 进行关联，存入

信息处理系统中，便于消费者进行商品溯源防伪。

8.1.3 防伪验证系统

防伪验证系统提供对防伪标签的验证查询服务，以及防伪数据信息（产品生产、销售、验证查询等数据）的下载等。

8.1.4 信息处理系统

包括商品生产、仓储、运输、销售等多类信息的处理系统。

8.1.5 密钥管理系统

负责整个系统中密钥的生成、分散、存储等密钥管理功能，是整个系统中安全核心；为保证该系统的安全性，密钥管理系统部署在独立的密钥管理中心，与商品溯源防伪应用系统的其他部分（包括信息处理系统、防伪验证系统、标签发行系统）物理隔离。密钥管理系统生成的密钥，通过密钥卡等安全措施，分发到商品防伪溯源应用系统的其他部分。

8.1.6 证书签发与身份鉴别系统

电子标签和防伪系统各个环节的设备中集成密码模块，由企业向 CA 申请企业根证书，用根证书签发二级证书，二级证书签发三级证书的方式建立证书链，作为电子标签和业务系统、业务系统和业务系统之间身份鉴别的依据。身份鉴别应按以下要求进行。

a) 业务系统和业务系统之间通信时，采用非对称算法实现身份鉴别。
b) 业务系统和电子标签进行通信时，采用非对称算法进行身份鉴别。
c) 业务系统读写器向电子标签写入信息时，业务系统和读写器进行双向身份鉴别，双向鉴别通过后，写入信息。双向身份鉴别见附录 A。
d) 业务系统读写器从电子标签读取信息时，对读写器进行单向身份鉴别，鉴别通过后，读取信息。
e) 读写器和电子标签内写入的信息用写入方的私钥签名，保证信息的完整性和抗抵赖。

8.2 产品选择

8.2.1 射频电子标签

8.2.1.1 密码安全要求

B 类系统中使用的射频电子标签满足以下密码安全要求。

a) 射频电子标签应符合 GM/T 0040—2015 中规定的Ⅱ类检测要求，射频电子标签所采用的芯片应符合 GM/T 0008 规定的不低于二级的检测要求。
b) 存储信息的机密性：应支持对电子标签内存储信息机密性保护。电子标签存储信息的机密性实现方式见 GB/T 37033.2—2018 中 6.1.1.1。电子标签存储信息的机密性检测见 GM/T 0040—2015 中 6.3.3。
c) 传输信息的机密性：应支持对电子标签传输信息保护功能。电子标签传输信息的机密性实现方式见 GB/T 37033.2—2018 中 6.1.1.2。电子标签传输信息的机密性检测见 GM/T 0040—2015 中 6.3.2。
d) 存储信息的完整性：应支持对电子标签存储信息完整性保护功能。电子标签存储信息的完整性实现方式见 GB/T 37033.2—2018 中 6.1.2.1。电子标签存储信息的完整性检测见 GM/T 0040—2015 中 6.3.5。
e) 传输信息的完整性：应支持对电子标签传输信息完整性保护功能。电子标签传输信息的完整

性实现方式见 GB/T 37033.2—2018 中 6.1.2.2。电子标签传输信息的完整性检测见 GM/T 0040—2015 中 6.3.4。

f) 身份鉴别：在对电子标签信息写入时应支持读写器与电子标签之间的双向身份鉴别；在对电子标签信息读取时，应支持读写器对电子标签的身份鉴别。读写器对电子标签的身份鉴别实现方式见 GB/T 37033.2—2018 中的 8.3.2.2。读写器与电子标签之间的双向身份鉴别的实现方式见 GB/T 37033.2—2018 中的 8.3.3.2。读写器与电子标签之间的身份鉴别应通过 GM/T 0040—2015 中 6.2 和 6.3 的检测。

g) 抗读写器抵赖：应支持抗读写器抵赖功能。抗读写器抵赖实现方式见 GB/T 37033.2—2018 中的 6.1.3.3。

h) 访问控制：应支持访问控制功能，保障存储信息在受控权限下进行访问。电子标签的访问控制实现方式见 GB/T 37033.2—2018 中 6.1.5。电子标签的访问控制检测见 GM/T 0040—2015 中 6.5。

i) 审计：应支持审计功能。电子标签的审计实现方式见 GB/T 37033.2—2018 中 6.1.6。电子标签的审计检测应满足 GM/T 0040—2015 中 6.8 审计功能检测。

j) 密码算法：应采用国家密码管理部门核准的密码算法。

k) 宜选用国家密码管理部门核准的密码产品。

8.2.1.2 可选密码安全要求

B 类系统中使用的射频电子标签根据应用需求，可选择支持以下密码安全要求：

抗电子标签原发抵赖：抗电子标签原发抵赖的实现方式见 GB/T 37033.2—2018 中 6.2.3。抗电子标签原发抵赖检测见 GM/T 0040—2015 中 6.6.1。

8.2.2 射频读写器

8.2.2.1 密码安全要求

B 类系统中使用的密码安全功能射频读写器满足以下密码安全要求。

a) 存储信息的机密性：应支持对读写器内存储信息的机密性保护。读写器存储信息的机密性实现方式见 GB/T 37033.2—2018 中 6.2.1.1。

b) 传输信息的机密性：应支持对读写器传输信息保护功能。读写器传输信息的机密性实现方式见 GB/T 37033.2—2018 中 6.2.1.2。

c) 存储信息的完整性：应支持对读写器存储信息完整性保护功能。读写器存储信息的完整性实现方式见 GB/T 37033.2—2018 中 6.2.2.1。

d) 传输信息的完整性：应支持对读写器传输信息完整性保护功能。读写器传输信息的完整性实现方式见 GB/T 37033.2—2018 中 6.2.2.2。

e) 身份鉴别：B 类安全级别读写器在信息写入时，应支持电子标签对读写器的身份鉴别，在信息读取时可选择支持电子标签对读写器的身份鉴别。电子标签对读写器的身份鉴别实现方式见 GB/T 37033.2—2018 中的 8.3.2.1。电子标签对读写器的身份鉴别应通过 GM/T 0040—2015 中 6.2 和 6.3 的检测。

f) 抗电子标签原发抵赖：应支持抗电子标签原发抵赖功能。抗电子标签原发抵赖实现方式见 GB/T 37033.2—2018 中 6.2.3.1。抗电子标签原发抵赖检测见 GM/T 0040—2015 中 6.6.1。

g) 抗读写器抵赖：应支持电子标签抗读写器抵赖功能。电子标签抗读写器抵赖的实现方式见 GB/T 37033.2—2018 中 6.2.3.3。

h) 访问控制：应支持访问控制功能。读写器访问控制实现方式见 GB/T 37033.2—2018 中 6.2.5。

i) 审计：应支持审计功能。读写器的审计记录实现方式见 GB/T 37033.2—2018 中 6.2.6。

j) 密码算法：应采用与电子标签中密码算法相适应的国家密码管理部门核准的密码算法。

k) 宜选用国家密码管理部门核准的密码产品。

8.2.3 安全网关

宜选用国家密码管理部门核准的密码产品。

8.2.4 密码机

符合 GM/T 0030 要求，宜选用国家密码管理部门核准的密码产品。

8.3 实施建议

8.3.1 信息处理系统

使用安全网络及网关产品保障信息处理系统传输安全性；保障信息处理系统存储和访问安全性，见 GB/T 37092 和 GM/T 0039。

8.3.2 中间件

使用安全网络及网关产品保障中间件传输安全性；保障中间件存储和访问安全性，见 GB/T 37092 和 GM/T 0039。

8.3.3 CA 和密钥管理系统

8.3.3.1 CA 和密钥管理系统安全要求

CA 和密钥管理系统应有两个证书管理发行系统，分别为企业证书系统和销售管理证书系统。两个证书管理发行系统应由第三方电子认证服务机构实施。

所有系统均采用密码模块保证对应证书的密钥安全，保证私钥不被导出、不被复制。同时工作流程中，操作员配备密码模块(如智能密码钥匙)，操作流程被数字签名，保证操作流程可控，并且被审计和追责。

数字认证系统的密码协议应符合 GM/T 0014 规定的要求。

8.3.3.2 CA 中心发放企业根证书

企业发证中心的安全模块，随机生成非对称密钥，作为签名密钥对。

企业将本企业信息、签名公钥提交到 CA 中心，CA 中心核实企业身份后为企业发放由 CA 私钥签名的数字证书。

数字证书包含企业基本信息、企业公钥、发放机构、使用期限等。

8.3.3.3 企业证书系统发放应用证书

本系统发放的证书均用于企业内部的生产和管理。生产管理系统、发行系统、生产系统、商品管理系统的密码模块生成公私密钥对，公钥由企业根私钥签名，分别发放证书。生产管理证书、发行证书、生产证书、销售管理证书作为与其他系统交互过程中的身份识别。

可将密码模块以智能密码钥匙或 TF 卡形式封装，发放集成到对应的系统中。

8.3.3.4 销售管理证书系统发放销售管理证书

本系统发放的证书均用于企业外部的渠道、销售、售后。对应管理防伪标签中的渠道管理信息、个

性化信息、销售日期、售后维护记录等非核心防伪信息。

销售系统、售后系统的密码模块生成公私密钥对，公钥由销售管理系统私钥签名，分别发放证书。销售证书、售后证书作为与其他系统交互过程中的身份识别。

考虑到商品的销售点和售后点的流动性大，随时会增加网点，为了控制企业发证系统根盾的使用频次，保护根盾安全，由销售管理系统为销售点和售后点发放三级证书。

可将密码模块以智能密码钥匙或 TF 卡形式封装，发放集成到对应的系统中。

8.3.4 透明传输通道读写器要求

射频识别标签发行、防伪验证过程中，如读写器作为信息透明传输通道使用时，标签通过中间件或信息处理系统实现防伪验证，对读写器无密码安全要求。

8.4 应用方案

B 类射频识别防伪密码应用方案见附录 C。

附 录 A
（资料性）
双向身份鉴别实现方式

对称分组密码算法的双向身份鉴别与流加密可见 GB/T 37033.2—2018 中附录 C。

采用非对称密码算法的双向身份鉴别和密码协议可见 GB/T 37033.2—2018 中附录 D。

针对不同的应用领域，存在不同的双向鉴别协议实现方式。如 SB/T 10768—2012 中附录 A 规定了酒类防伪双向鉴别协议实现方式。GB/T 28925 和 GB/T 29768 规定了国标安全鉴别协议和安全通信协议。各行业可依据本行业应用环境，采用相应的鉴别协议实现方式，保障防伪应用的安全性。

附 录 B
（资料性）
A 类射频识别防伪密码应用方案

B.1 概述

该方案符合本文件规定的 A 类要求。可应用于酒类、药品、食品等商品溯源防伪。

该方案电子标签采用 SM7 密码算法，读写器采用 SM1 和 SM7 密码算法，SM1 用于密钥分散；支持读写器和电子标签之间的双向身份鉴别机制和读写器对电子标签的单向身份鉴别机制。

该方案具有如下特点。

a） 一芯一密

标签的鉴别密钥，采用 SM1 安全算法对标签 UID 进行分散后生成，保证一芯一密。

b） 提前验伪

在购买行为发生之前，可以完成商品防伪，真正保护消费者及商家利益。

c） 交钥匙

本方案的验伪关键（鉴别密钥）掌握在厂商手里，即使防伪方案厂商也无法复制。

d） 网络验证、大众防伪

采用移动互联网技术，结合日益普及的 NFC 智能移动通信终端，实现大众防伪。

该方案贯穿了产品生产、销售流通、验伪查询与信息处理等环节的全过程，如图 B.1 所示。

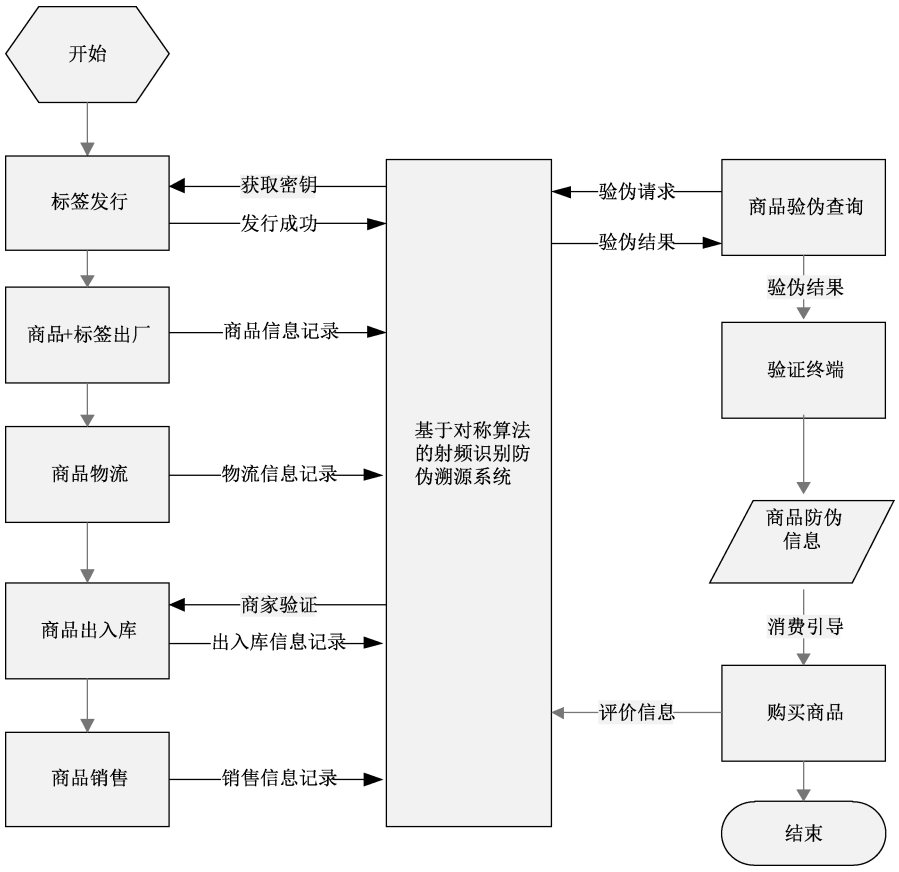

图 B.1 A 类射频识别防伪密码应用方案示意图

B.2 系统架构

本方案的系统架构如图 B.2 所示。

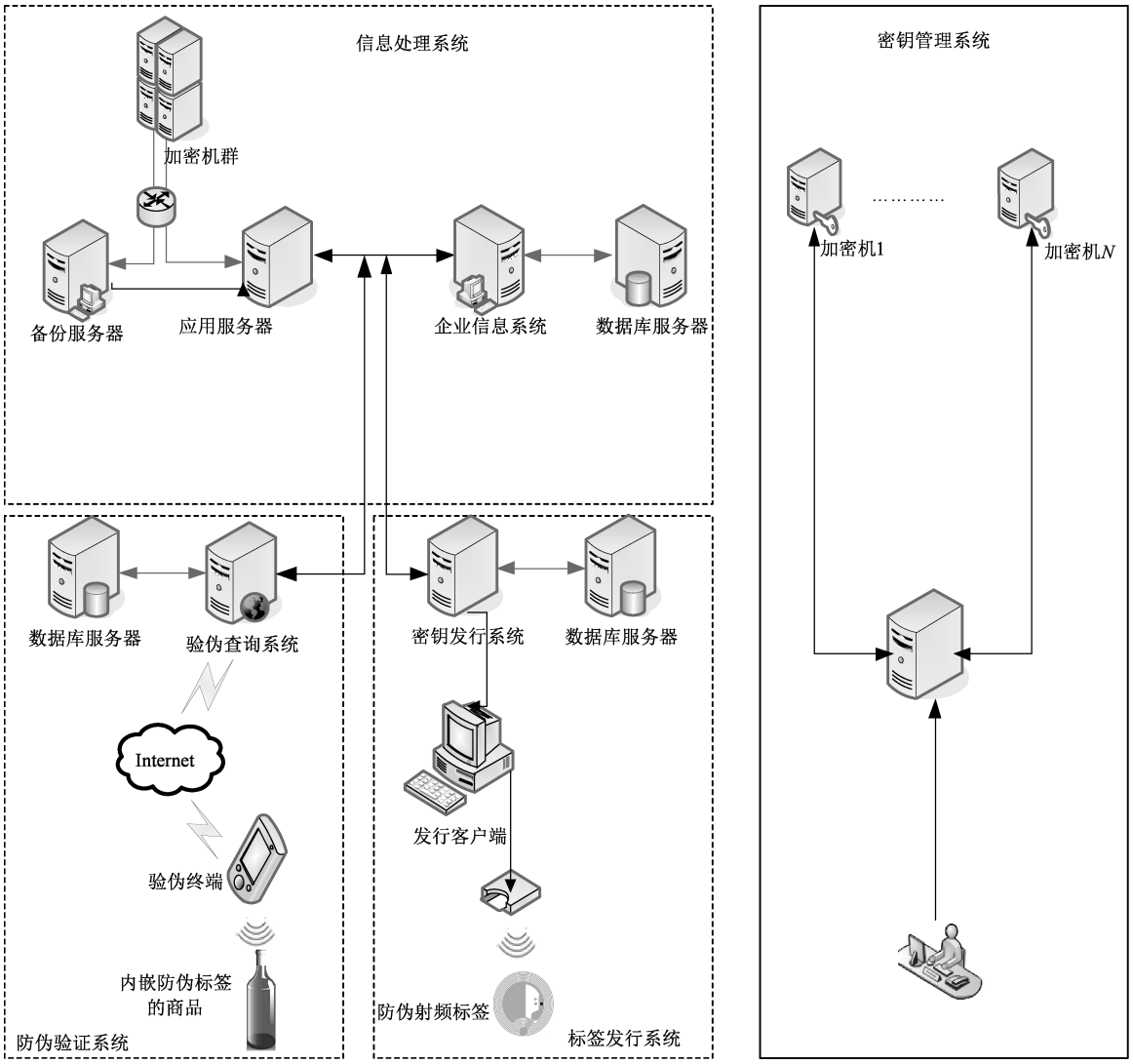

图 B.2 A 类系统架构示意图

标签发行系统：对防伪标签进行密钥发行，并在发行完成后，将商品溯源相关信息与防伪标签 UID 进行关联，存入信息处理系统中，便于消费者进行商品溯源防伪。

防伪验证系统：验伪系统提供对防伪标签的验证查询服务，以及防伪数据信息（产品生产、销售、验证查询等数据）的下载等。

信息处理系统：包括商品生产、仓储、运输、销售等多类信息处理系统。

密钥管理系统：负责整个系统中密钥的生成、分散、存储等密钥管理功能，是整个系统中安全核心；为保证该系统的安全性，密钥管理系统部署在独立的密钥管理中心，与商品溯源防伪应用系统的其他部分（包括信息处理系统、防伪验证系统、标签发行系统）物理隔离。密钥管理系统生成的密钥，通过密钥卡，分发到商品防伪溯源应用系统的其他部分。

B.3 应用系统设计

B.3.1 防伪标签发行系统

防伪标签发行系统主要包括由密钥管理服务器、密钥发行服务器和发行读写器组成，如图 B.3 所示。

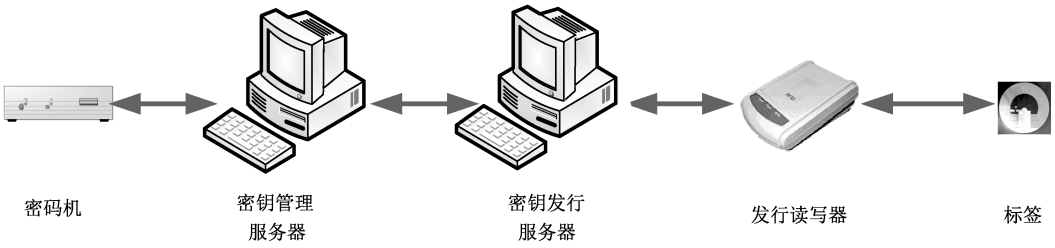

图 B.3 防伪标签发行系统结构图

防伪标签发行系统中所采用的读写器应为受控防伪读写器，只能通过受控渠道获取。

具体的防伪标签发行流程如图 B.4 所示。

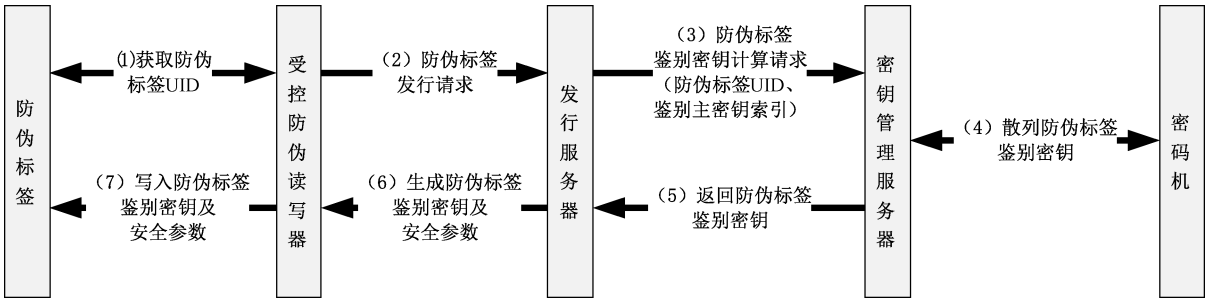

图 B.4 防伪标签发行流程示意图

B.3.2 防伪验证系统

B.3.2.1 系统概述

防伪验证系统是防伪体系中提供验证服务的系统，由数据库服务器、验伪管理服务器和验伪终端组成。为消费者、零售商、专卖店及经销商提供验伪查询服务，如图 B.5 所示。

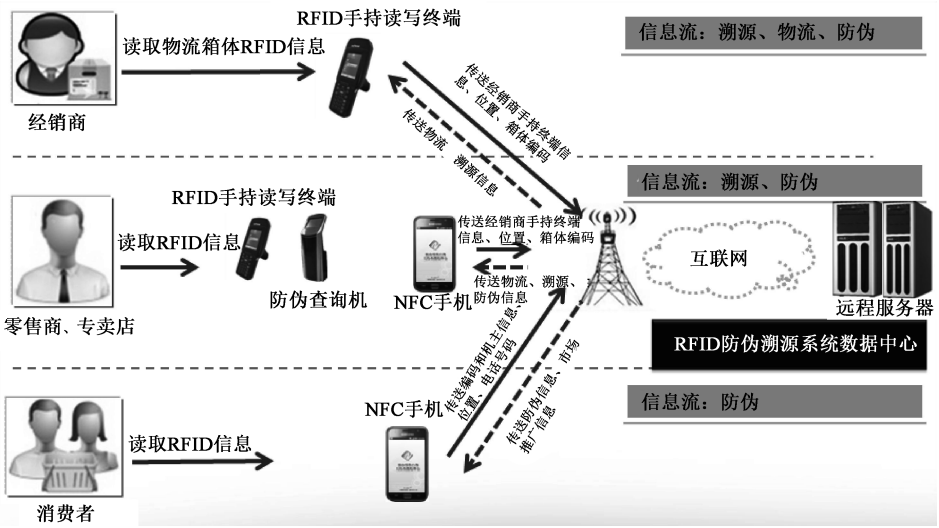

图 B.5　验伪查询示意图

通常消费者、零售商、专卖店及经销商只能进行验伪查询，不能在未授权的情况下对标签写入信息。

B.3.2.2　防伪标签安全机制

该方案电子标签采用 SM7 密码算法，读写器采用 SM1 和 SM7 密码算法；支持读写器和电子标签之间的双向身份鉴别机制和读写器对电子标签的单向身份鉴别机制。

该方案中使用的防伪标签具备安全存储区，读写器欲访问控制安全存储区数据，需首先通过读写器与防伪标签的双向身份鉴别，并采用加密通信的方式进行后续的访问控制。

B.3.2.3　验伪查询流程

B.3.2.3.1　验伪终端分类

该方案中的验伪终端，可分为两类：

a）　集成 NFC 功能的移动通信终端，主要面向大众消费防伪应用；

b）　集成 SAM 专用终端设备，主要面向厂商进行打假、防串货等管理应用。

防伪查询系统与验伪终端之间，建立安全通信通道，对传输信息进行安全保护。以下将对基于两类验伪终端的验伪查询进行详细说明。

B.3.2.3.2　基于 NFC 移动终端的验伪查询流程

防伪查询系统，通过 NFC 移动通信终端提供的信息传输通道，对防伪标签进行单向鉴别，判别真伪，给消费者提供快捷、可信的防伪查询服务。如图 B.6 所示。

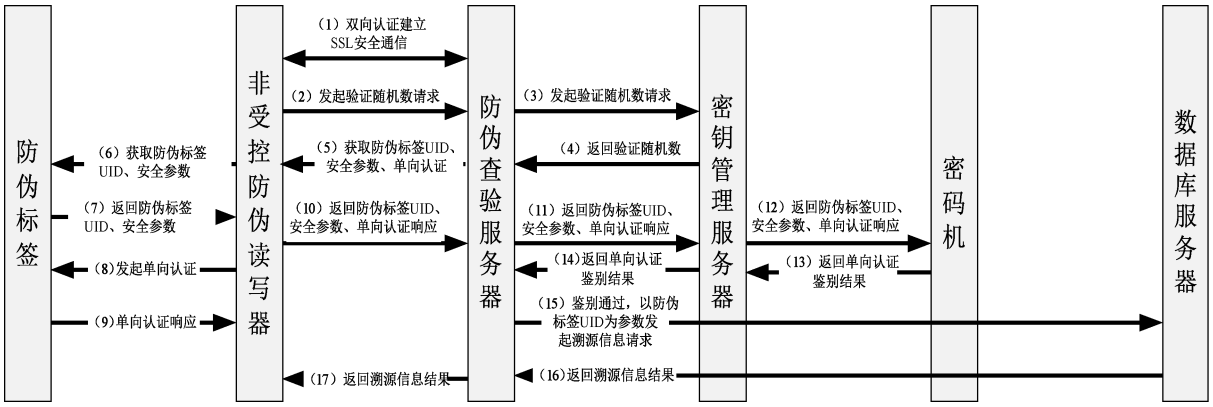

图 B.6　基于 NFC 移动通信终端的验伪查询流程

B.3.2.3.3　基于集成 SAM 专用终端设备的验伪流程

集成 SAM 专用终端设备，具备密码运算能力，从防伪查询系统获取防伪标签鉴别密钥、完成与防伪标签的双向鉴别，判别真伪。此外，在通过双向鉴别后，可以加密通讯方式访问控制防伪标签安全存储区数据，完成其他管理应用。

基于集成 SAM 专用终端设备的验伪流程如图 B.7 所示。

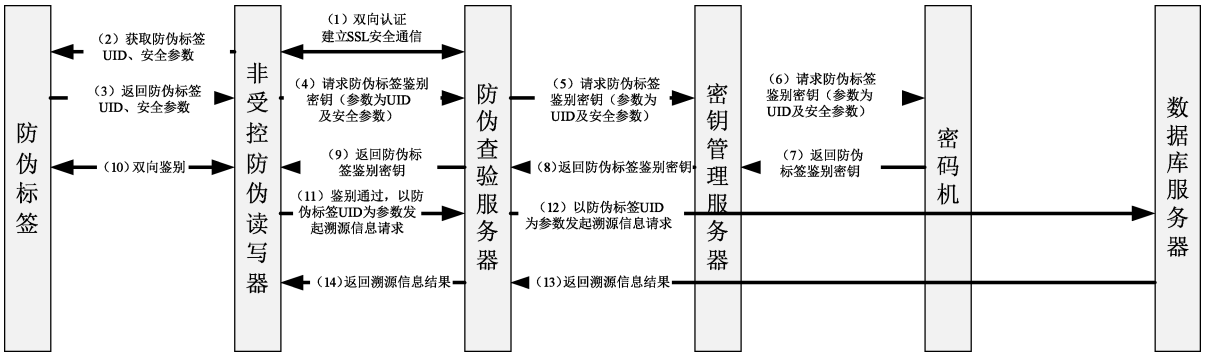

图 B.7　基于集成 SAM 专用终端的验伪查询流程

B.3.3　信息处理系统

信息处理系统：包括商品生产、仓储、运输、销售等多类信息处理系统。信息处理系统为防伪标签发行系统、防伪验证系统提供溯源防伪信息。

信息处理系统与防伪标签发行系统之间建立安全通信通道。

信息处理系统与防伪验证系统之间建立安全通信通道。

B.3.4　密钥管理系统

B.3.4.1　系统概述

密钥管理系统结构如图 B.8 所示，由密钥管理服务器、密码机、密钥管理数据库以及密钥卡组成。

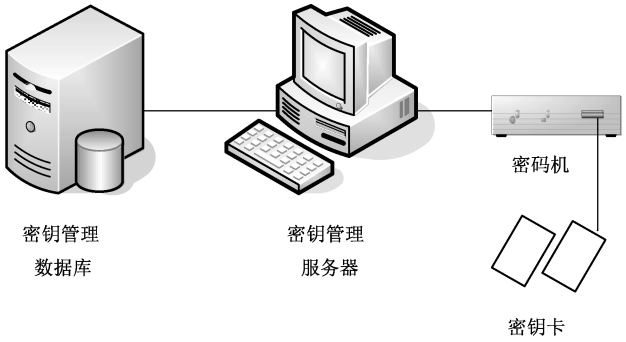

图 B.8　密钥管理系统结构图

密钥管理中心需要产生的密钥卡如表 B.1 所示。

表 B.1　密钥管理中心密钥卡

密钥卡名称	保存密钥	用途
控制卡	传输密钥	密钥备份和恢复注入其他子系统密码机，保护主密钥导入过程
根密钥卡	根密钥	密钥备份和恢复
主密钥卡	防伪标签鉴别主密钥	导出密钥，注入其他子系统密码机

B.3.4.2　密钥生成与管理

B.3.4.2.1　密钥分级管理

密钥管理系统提供防伪标签发行系统、防伪验证系统、信息处理系统的密钥产生和管理，密钥进行分级控制和管理。

密钥应至少为 3 级，并逐级进行散列。厂商设立密钥管理机构并产生根密钥；根密钥通过 1 级分散因子散列出鉴别主密钥；鉴别主密钥通过 2 级分散因子散列出防伪标签鉴别密钥。密钥散列如图 B.9 所示。

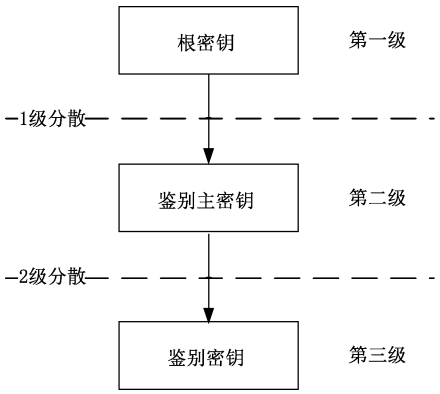

图 B.9　密钥分级管理示意图

注 1：1 级分散因子，厂商代码或商品类别代码。

注 2：2 级分散因子，防伪标签 UID。

B.3.4.2.2 根密钥生成与管理

根密钥的生成与管理分为根密钥的产生、备份/恢复、更新。

a) 根密钥产生：由 3 或 5 名(奇数)管理员分别使用硬件 IC 卡或者智能密码钥匙随机产生密钥种子，然后通过 IC 卡或者智能密码钥匙将这 3 个或 5 个密钥种子一起输入到密码机。

b) 根密钥备份/恢复：根密钥除在密码机中安全保存外，还以密钥卡的形式进行备份，备份密钥卡由机要安全部门代为保管。若通过备份密钥卡不能完成恢复卡片根密钥，则通过密钥种子进行卡片根密钥的恢复。

c) 根密钥更新：重新执行产生、备份过程。原有根密钥的处理根据管理中心管理条例进行。重新产生根密钥后，应重新执行所有的流程。

附 录 C
（资料性）
B类射频识别防伪密码应用方案

C.1 概述

该方案符合本文件规定的B类要求。

电子标签采用SM2、SM3和SM4密码算法，读写器采用SM2、SM3和SM4密码算法；支持读写器和电子标签之间的双向身份鉴别机制和读写器对电子标签的单向身份鉴别机制。电子标签芯片通过了GM/T 0008规定的二级检测要求，电子标签通过了GM/T 0040—2015中规定的Ⅱ类B档检测要求。

本方案通过非对称加密方法进行身份鉴别和权限控制，防止各个环节数据伪造，实现商品的生产、流动渠道、销售终端的跟踪。本方案支持离线认证、独立认证；支持数据的各阶段写入，满足商品的个性化需求和收藏性需求的信息写入，满足商品渠道管理的需求。

方案包括防伪标签发行系统、防伪验证系统、信息处理系统、CA和密钥管理系统。

密码模块含有密码算法、安全功能，是可实现密钥管理机制的相对独立硬件。

C.2 系统架构

本方案的系统架构如图C.1所示。

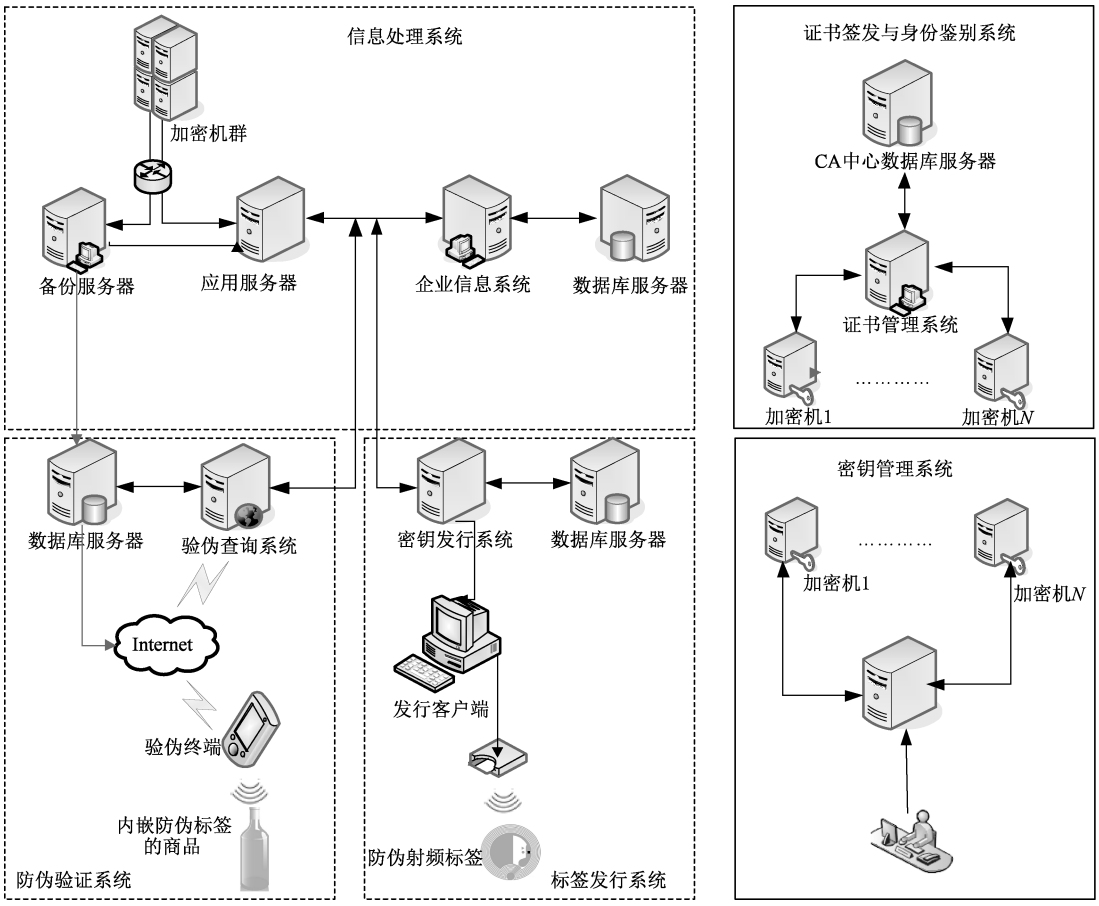

图 C.1 B类系统架构示意图

本方案在电子标签和防伪系统各个环节的设备中集成密码模块，由企业向 CA 申请企业根证书，用根证书签发二级证书，二级证书签发三级证书的方式建立证书链，作为电子标签和业务系统，业务系统和业务系统之间识别的依据。

业务系统和业务系统之间通信时，采用非对称算法实现身份鉴别。

业务系统和电子标签进行通信时，采用非对称算法进行身份鉴别。

业务系统读写器向电子标签写入信息时，业务系统和读写器进行双向身份鉴别，双向鉴别通过后，写入信息。

业务系统读写器从电子标签读取信息时，对读写器进行单向身份鉴别，鉴别通过后，读取信息。读写器和电子标签内写入的信息用写入方的私钥签名，保证信息的完整性、抗抵赖。

C.3 应用系统设计

C.3.1 防伪标签发行系统

C.3.1.1 标签发行系统示意图

非对称射频识别防伪标签发行系统示意图如图 C.2 所示。

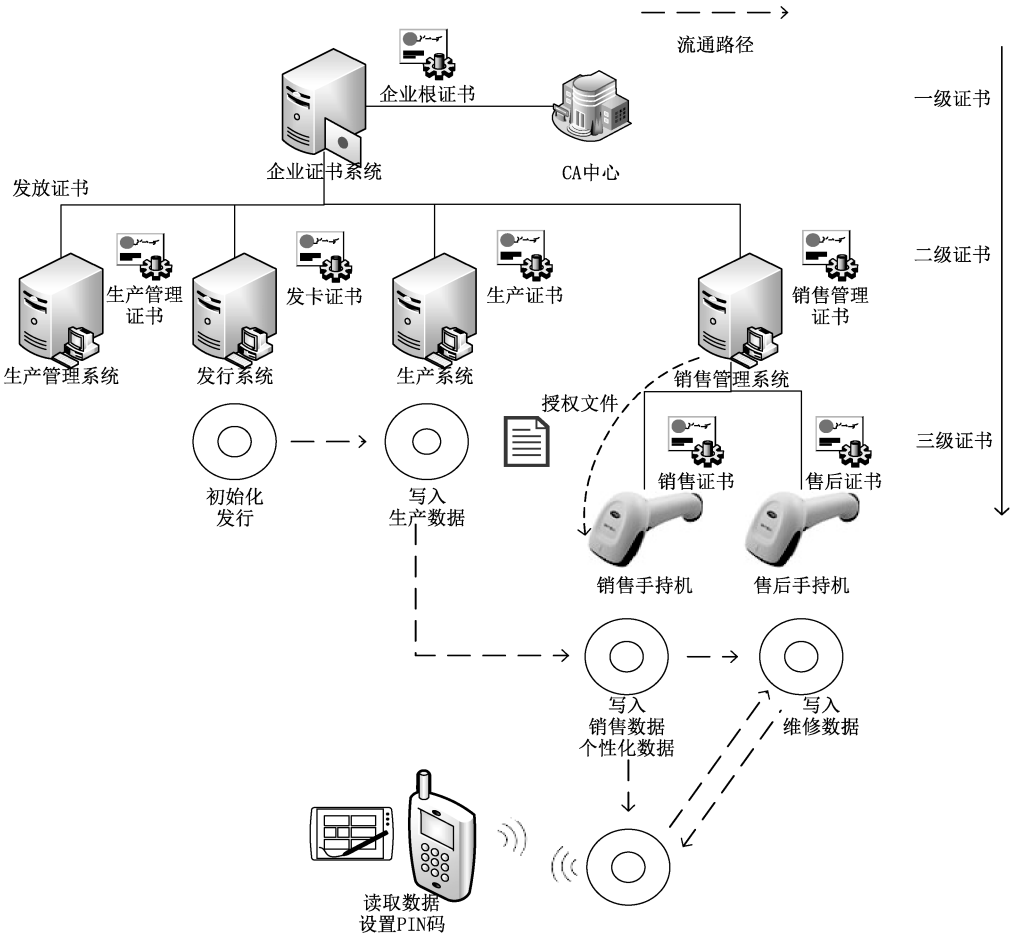

图 C.2 非对称射频识别防伪标签发行系统示意图

C.3.1.2 标签初始化

空白电子标签在发行系统进行初始化。对每张电子标签进行独立的数字证书发放。初始化后，电

子标签中数据内容如表 C.1 所示。

表 C.1　电子标签数据内容

企业根证书
发行证书
电子标签证书
……

C.3.1.3　写入生产数据

电子标签初始化后根据要嵌入的商品定制成不同的形状，嵌入商品。

生产线上放置读写器，读写器中集成生产密码模块。

写入生产数据时：

a）　生产系统获得生产管理系统的授权，该授权基于数字签名实现；

b）　生产系统读写器和电子标签进行双向身份鉴别；

c）　双向身份鉴别通过后，生产系统读写器将生产数据包括但不限于品名、型号、产品序号、生产日期等信息写入电子标签，并使用生产证书对信息进行数字签名。

写入生成数据后，电子标签中数据内容如表 C.2 所示。

表 C.2　电子标签数据内容

企业根证书
发行证书
电子标签证书
生产(产品)信息
生产信息数字签名
生产设备数字证书
……

C.3.1.4　写入销售数据

写入销售数据时：

a）　商品销售时，首先销售机具验证电子标签的真伪，同时根据厂家的销售授权文件(含数字签名)判别写入权限；

b）　完成鉴权后，销售机具写入销售信息(销售网点、销售日期等)和个性化信息(例如生日祝贺)，并对信息用销售网点机具的证书对信息进行数字签名。

写入销售数据后，电子标签中数据内容如表 C.3 所示。

表 C.3　电子标签数据内容

企业根证书
发行证书

表 C.3　电子标签数据内容（续）

电子标签证书
生产(产品)信息
生产信息数字签名
生产设备数字证书
销售信息
销售信息数字签名
个性化信息
个性化信息数字签名
销售机具证书
……

C.3.1.5　写入售后维修数据

写入售后维修数据时：

a)　商品进行售后服务时，售后机具验证电子标签的真伪，并获取商品信息，从而进行对应售后服务；

b)　写入服务记录，完成售后服务后，售后机具将服务记录写入电子标签并签名。

写入售后维修数据后，电子标签中数据内容如表 C.4 所示。

表 C.4　电子标签数据内容

企业根证书
发行证书
电子标签证书
生产(产品)信息
生产信息数字签名
生产设备数字证书
销售信息
销售信息数字签名
个性化信息
个性化信息数字签名
销售机具证书
售后服务记录 1
售后服务记录数字签名 1
售后服务机具数字证书 1
售后服务记录 2
售后服务记录数字签名 2
售后服务机具数字证书 2

C.3.2 防伪验证系统

C.3.2.1 专业设备辨别商品真伪

专业设备，内置密码模块，内部固化企业根证书。

专业设备通过企业根证书，首先验证电子标签中的一系列书的合法性，并且通过双向身份鉴别电子标签的数字证书合法性，验证通过后，读取相关的信息，并采用对应证书对相关信息的数字签名进行信息的可靠性和完整性进行验证，验证通过后显示相关信息。

C.3.2.2 消费者辨别商品真伪

消费者终端，如手机、PAD 等具备 NFC 的移动设备内安装防伪 APP，APP 内存储 CA 的根证书或者国家根证书。

APP 软件通过国家根证书或者 CA 根证书，首先验证电子标签中的一系列证书的合法性，并且通过双向身份鉴别电子标签的数字证书合法性，验证通过后，读取相关的信息，并采用对应证书对相关信息的数字签名进行信息的可靠性和完整性进行验证，验证通过后显示相关信息。

C.3.3 信息处理系统

C.3.3.1 系统概述

本方案包括两个管理系统，生产管理系统和销售管理系统。

C.3.3.2 生产管理系统

生产管理系统管理发行系统和生产系统的写入信息、授权等，分别将发行信息/生产信息签名写入或导入发行读写器/生产读写器。

发行读写器/生产读写器接收信息后，使用企业根证书验证生产管理证书合法性，验证合法后，验签信息。从而确认信息是否来自合法生产管理系统，并校验信息完整性。

每一次使用信息前，读写器都要对信息进行完整性校验。

C.3.3.3 销售授权管理

商品发往各个销售点前，销售管理系统将商品电子标签和销售点进行绑定，采用数字签名方式生成授权文件，保证只有经授权的销售点才可以销售商品。

销售管理系统中有各个销售点的证书、商品电子标签的证书。将销售点证书、电子标签证书、授权命令，进行签名生成授权文件，和商品管理证书通过网络、移动存储设备等传输给销售点，导入到系统中。

销售点导入授权信息时，用验证签名证书，判断证书合法性，证书合法，验签信息。

销售管理系统向电子标签写入销售数据时，找到授权信息，传输给电子标签，电子标签验证销售点是否为商品管理系统授权的合法销售点，验证通过，接受销售网点写入的信息。

C.3.4 CA 和密钥管理系统

C.3.4.1 系统概述

为确保系统高安全性和使用的便利性，根据安全实施的需求，系统设计了两个证书管理发行系统，分别为企业证书系统和销售管理证书系统。

所有系统均采用密码模块确保对应证书的密钥安全，确保私钥不能被导出、不能被复制。同时在所有工作人员参与的工作流程中，所有的人员都配备密码模块（智能密码钥匙），所有的过程均被数字签名，确保整个过程是可控的，并且可以被审计和追责。

C.3.4.2 企业从CA中心获得企业根证书

企业发证中心的密码模块，随机生成非对称密钥，作为根密钥对。

企业将本企业信息、根公钥提交到CA中心，CA中心核实企业身份后为企业发放由CA私钥签名的数字证书。

数字证书包含企业基本信息、企业公钥、发放机构、使用期限等。

C.3.4.3 企业证书系统发放证书

本系统发放的证书均用于企业内部的生产和管理，对应管理防伪标签中的核心防伪信息包括但不限于品名、型号、生产日期、收藏信息、限量版信息等。

生产管理系统、发行系统、生产系统、商品管理系统的密码模块生成公私密钥对，公钥由企业根私钥签名，分别发放证书。生产管理证书、发行证书、生产证书、销售管理证书，作为与其他系统交互过程中的身份识别。

将密码模块以智能密码钥匙或TF卡形式封装，发放集成到对应的系统中。

C.3.4.4 销售管理证书系统发放证书

本系统发放的证书均用于企业外部的渠道、销售、售后。对应管理防伪标签中的渠道管理信息、个性化信息、销售日期、售后维护记录等非核心防伪信息。

销售系统、售后系统的密码模块生成公私密钥对，公钥由销售管理系统私钥签名，分别发放证书。销售证书、售后证书，作为与其他系统交互过程中的身份识别。

本方案考虑到商品的销售点和售后点的流动性大，随时会增加网点，为了控制企业发证系统根盾的使用频次，保护根盾安全，由销售管理系统为销售点和售后点发放三级证书。

将密码模块以智能密码钥匙或TF卡形式封装，发放集成到对应的系统中。

GM/T 0096-2020

码上扫一扫 正版服务到

*

书号：155066·2-35975

定价： 36.00 元