ICS 35.040
L 80
备案号:44640—2014

GM

中华人民共和国密码行业标准

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

Specifications of cryptographic application for RFID systems—Part 5:Specification for key management

2014-02-13 发布　　2014-02-13 实施

国家密码管理局　　发布

GM/T 0035.5—2014

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5部分:密钥管理技术要求
GM/T 0035.5—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 18 千字
2014年4月第一版　2014年4月第一次印刷
*
书号:155066·2-27015　定价 18.00 元

GM/T 0035.5-2014

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地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。

目　次

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 和信息区 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唯一标识的厂商 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唯一性。

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

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 5 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：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、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、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。

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。