ICS 35.030
CCS L 80

中华人民共和国密码行业标准

GM/T 0040—2024
代替 GM/T 0040—2015

射频识别标签模块密码检测规范

Cipher test specification of radio frequency identification tag module

2024-12-27 发布　　2025-07-01 实施

国家密码管理局　　发布

目　　次

前　言

本文按照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。

本文件代替GM/T 0040—2015《射频识别标签模块密码检测准则》，与GM/T 0040—2015相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 更改了标签模块分类，把标签模块新划分为4大类，其中Ⅰ类被分为Ⅰ-A类和Ⅰ-B类，保留原Ⅱ-A和Ⅱ-B的分类，增加了Ⅲ类和Ⅳ类（见第5章，2015年版的第5章）；

b) 更改了“检测要求和判定准则”，增加了Ⅲ类和Ⅳ类标签模块的检测项，更改了Ⅱ类标签模块的随机数测试内容（见第6章，2015年版的第6章）；

c) 更改了“随机数测试”中的“检测项目要求”和“检测条件要求”，并删除了相应的表1和表3，表2和表4（见2015年版的6.2.2.2和6.2.2.3），直接引用标准GM/T 0005—2021附录A中A.1 20 000比特样本检测设置和A.2 1 000 000比特样本检测设置（见6.2.2）；

d) 增加了“审计记录”，并按照GM/T 0035.2—2014的要求来判定，且只有第Ⅳ类标签才需要符合审计要求（见6.9）；

e) 更改了“密钥管理”中各检测项的要求，不要求符合“GM/T 0008—2012”，删除了对“GM/T 0008—2012”的引用（见6.10，2015年版的6.9）；

f) 删除“开发环境保障”的内容（见2015年版的6.10）；

g) 更改了“标签模块分类及检测项”的内容（见附录A，2015年版的附录A）。

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：华大恒芯科技有限公司、商用密码检测认证中心、苏州安超微电子有限公司、紫光同芯微电子有限公司、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、国民技术股份有限公司、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责任公司。

本文件主要起草人：张建平、周建锁、雷银花、毛颖颖、陈小庆、杨贤伟、邵波、柳逊、孙磊、董浩然、罗鹏、兰天、费渡、莫凡、邓开勇、顾震、刘颖、岳超。

本文件及其所替代文件的历次版本发布情况为：

——2015年首次发布为GM/T 0040—2015；

——本次为第一次修订。

射频识别标签模块密码检测规范

1 范围

本文件规定了采用密码技术的射频识别标签模块产品的分类和密码检测的检测内容、检测要求以及判定准则。

本文件适用于包括高频，超高频，微波等频段的射频识别标签模块的密码及安全功能检测。

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—2012 信息技术 射频识别 2.45 GHz 空中接口协议

GB/T 29768—2013 信息技术 射频识别 800/900 MHz 空中接口协议

GM/T 0005—2021 随机性检测规范

GM/T 0035—2014(所有部分) 射频识别系统密码应用技术要求

GM/Z 4001 密码术语

3 术语和定义

GM/Z 4001 界定的以及下列术语和定义适用于本文件。

3.1

单向鉴别 unidirectional authentication

由读写器发起对标签的身份鉴别。

3.2

数据源鉴别 data origin authentication

确认接收到的数据的来源与其声明的一致。

3.3

灭活 kill

对标签模块的一种操作指令，成功执行后，标签模块不再响应任何命令。

3.4

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。

3.5

射频识别标签模块 RFID tag module

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。

注：每个射频识别标签模块(以下简称“标签模块”)具有唯一的电子编码，可由单芯片或多芯片组成。

3.6

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。

3.7

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

唯一标识符　unique identifier

由电子标签芯片制造商固化在电子标签芯片内的唯一标识符。

注：包含芯片生产序列号、经注册的厂商代码等唯一性信息。

4　缩略语

下列缩略语适用于本文件。

RFID：射频识别（radio frequency identification）

UID：唯一标识符（unique identifier）

5　射频识别标签模块分类

5.1　Ⅰ类标签模块

Ⅰ类标签模块划分为两个子类：Ⅰ-A 类和Ⅰ-B 类，Ⅰ-A 类仅规定了标签唯一标识符鉴别能力。Ⅰ-B 类规定了标签模块应具备与读写器间的单向鉴别能力，适用于仅需要认证标签模块身份真实性的应用环境。

5.2　Ⅱ类标签模块

Ⅱ类标签模块规定了标签模块应具备与读写器间的双向鉴别能力和支持数据传输的机密性，适用于需要对标签模块与读写器进行相互认证身份真实性和传输机密性的应用环境。该类标签模块根据认证真实性和传输机密性的要求高低不同划分为两个子类：Ⅱ-A 类和Ⅱ-B 类，其中Ⅱ-A 类标签模块随机数只需要通过 GM/T 0005—2021 附录 A，A.1 的 12 项检测，Ⅱ-B 类标签模块随机数需要通过 GM/T 0005—2021 附录 A，A.2 的全部 15 项检测。

5.3　Ⅲ类标签模块

除具备Ⅱ-B 类标签模块的所有功能外，Ⅲ类标签模块还需要支持存储的机密性和完整性校验，还应支持数据源鉴别中的电子标签原发数据源鉴别，使其能确保电子标签信息原发者不能成功地否认曾经生成过该信息，接收电子标签信息的主体能获得证明电子标签信息原发者的证据，而且该证据可由该主体或第三方验证。

5.4　Ⅳ类标签模块

除具备Ⅲ类标签模块的所有功能外，Ⅳ类标签模块还需要支持数据源鉴别中的电子标签数据源鉴别和读写器数据源鉴别，支持非对称算法和密码杂凑算法，支持审计记录。

6 检测要求和判定准则

6.1 一般要求

本文件一般性检测要求如下。

a) 标签模块的检测按照 GM/T 0035—2014(所有部分)及本文件内容开展,本文件定义了标签模块的密码检测。

b) 标签模块的密码算法应为国家密码管理主管部门认可的密码算法。

c) 标签模块应明确声明产品类型及密码功能,产品各项密码功能应正确有效。

标签模块检测项见附录 A。

6.2 密码算法

6.2.1 算法实现正确性测试

6.2.1.1 Ⅰ-A 类标签模块

Ⅰ-A 类标签无要求。

6.2.1.2 Ⅰ-B 类标签模块

Ⅰ-B 类标签需要支持对称算法,模块算法实现正确性测试方式如下。

a) 检测要求

按照标签模块提供的密码算法功能进行算法调用正确性检测;

使用读写器发起操作指令,分别测试标签模块支持的各类密码算法及其工作模式,标签模块返回的响应数据应正确有效。

b) 判定准则

标签模块能正确实现各类密码算法功能。

6.2.1.3 Ⅱ类标签模块

同Ⅰ-B 类标签模块。

6.2.1.4 Ⅲ类标签模块

同Ⅰ-B 类标签模块。

6.2.1.5 Ⅳ类标签模块

Ⅳ类标签模块还需要支持非对称算法和密码杂凑函数,模块算法实现正确性测试同Ⅰ-B 类标签。

6.2.2 随机数测试

6.2.2.1 Ⅰ类标签模块

无要求。

6.2.2.2 Ⅱ-A 类标签模块

Ⅱ-A 类标签模块随机数测试方式如下。

a） 检测要求

1） 显著性水平

应符合 GM/T 0005—2021 的要求；

2） 样本数量

随机数样本数量为 1 000 组；

3） 样本长度

应符合 GM/T 0005—2021 的要求；

4） 检测项目

检测项目定义见 GM/T 0005—2021 的 A.1；

5） 检测参数

检测参数定义见 GM/T 0005—2021 的 A.1。

b） 判定准则

如果随机数通过 GM/T 0005—2021 中 A.1 规定的所有检测项目，则随机数通过本文件检测，否则，未通过本文件检测。

6.2.2.3 Ⅱ-B 类标签模块

Ⅱ-B 类标签模块随机数测试方式如下。

a） 检测要求

1） 显著性水平

应符合 GM/T 0005—2021 的要求；

2） 样本数量

随机数样本数量为 1 000 组；

3） 样本长度

应符合 GM/T 0005—2021 中 A.2 的要求；

4） 检测项目

检测项目定义见 GM/T 0005—2021 的 A.2；

5） 检测参数

检测参数定义见 GM/T 0005—2021 的 A.2。

b） 判定准则

如果随机数通过 GM/T 0005—2021 中 A.2 规定的所有检测项目，则随机数通过本文件检测，否则，未通过本文件检测。

6.2.2.4 Ⅲ类标签模块

同Ⅱ-B 类标签模块。

6.2.2.5 Ⅳ类标签模块

同Ⅱ-B 类标签模块。

6.3 密码服务

6.3.1 通则

密码服务指标签模块基于算法提供的身份鉴别、机密性和完整性等安全要素。密码服务的实现与产品具有耦合性。选用 GB/T 28925—2012、GB/T 29768—2013 中的安全鉴别协议的产品应实现该标

准中规定的安全命令和机制；选用 GM/T 0035.4—2014 安全鉴别协议产品应实现该标准中规定的安全机制；选用其他安全标准或自定义安全鉴别协议的产品应实现相应的安全机制。

6.3.2 身份鉴别测试

6.3.2.1 Ⅰ-A 类标签模块

Ⅰ-A 类标签模块身份鉴别测试方式如下。

a) 检测要求

采用唯一标识符鉴别。见 GM/T 0035.2—2014 的 5.4.1，使用读写器根据标签模块的 UID 及相关应用信息采用密码算法计算产生验证码(MAC')，比对 MAC'与标签模块存储的验证码(MAC)的一致性。

b) 判定准则

标签唯一标识鉴别有效。

6.3.2.2 Ⅰ-B 类标签模块

Ⅰ-B 类标签模块身份鉴别测试方式如下。

a) 检测要求

采用单向鉴别方式，单向鉴别过程应使用密码，其密码功能应正确有效。鉴别过程应符合 GM/T 0035.4—2014 中 7.3.2.2。测试环境需设计有效类和无效类测试用例，标签模块应对读写器发出的认证请求做出相应的正确应答。

b) 判定准则

标签模块单向鉴别机制有效。

6.3.2.3 Ⅱ类标签模块

Ⅱ类标签模块身份鉴别测试方式如下。

a) 检测要求

采用双向鉴别方式，双向鉴别过程应使用密码，其密码功能应正确有效，鉴别过程应符合 GM/T 0035.4—2014 中 7.3.3.1；

测试环境需设计有效类和无效类测试用例，标签模块应对与读写器之间的双向鉴别做出相应的正确应答。

b) 判定准则

标签模块双向鉴别机制有效。

6.3.2.4 Ⅲ类标签模块

同Ⅱ类标签模块。

6.3.2.5 Ⅳ类标签模块

同Ⅱ类标签模块。采用非对称算法时，鉴别过程应符合 GM/T 0035.4—2014 中 7.3.3.2 的要求。

6.3.3 数据传输机密性测试

6.3.3.1 Ⅰ类标签模块

无要求。

6.3.3.2 Ⅱ-A 类标签模块

Ⅱ-A 类标签模块数据传输机密性测试方式如下。

a) 检测要求

标签模块能够根据需要，为允许传输的敏感信息提供正确有效的机密性传输服务；

标签模块与读写器通信时，采用流加密或分组加密的方式对传输的敏感信息进行加密保护，其数据传输机密性服务应正确有效；传输密钥的生成方式符合 GM/T 0035.4—2014 的 7.1.1 a)，加密实现方式符合 GM/T 0035.4—2014 的 7.1.2。

b) 判定准则

信道传输的数据在传输过程中能够采用密码算法进行机密性保护。

6.3.3.3 Ⅱ-B 类标签模块

同Ⅱ-A 类标签模块。

6.3.3.4 Ⅲ类标签模块

同Ⅱ-A 类标签模块。

6.3.3.5 Ⅳ类标签模块

同Ⅱ-A 类标签模块。采用非对称算法时，传输密钥的生成方式应符合 GM/T 0035.4—2014 中 7.1.1 b)的要求。

6.3.4 数据存储机密性测试

6.3.4.1 Ⅰ类标签模块

无要求。

6.3.4.2 Ⅱ类标签模块

无要求。

6.3.4.3 Ⅲ类标签模块

Ⅲ类标签模块数据存储机密性测试方式如下。

a) 检测要求

标签模块能够根据需要，为存储的敏感信息提供正确有效的数据存储机密性服务；

标签模块对存储在标签模块内的敏感信息采用密码算法进行加密保护，确保除合法读写器外，其余任何读写器不能获得该数据；采用对称密码算法分组加密方式时，符合 GM/T 0035.2—2014 的 5.1.1，存储加密密钥的产生、使用和存储，符合 GM/T 0035.5—2014 的 8.3.1。

b) 判定准则

标签模块能够采用密码算法对存储的敏感信息数据进行机密性保护。

6.3.4.4 Ⅳ类标签模块

同Ⅲ类标签模块。

6.3.5 数据传输完整性测试

6.3.5.1 Ⅰ类标签模块

无要求。

6.3.5.2 Ⅱ类标签模块

无要求。

6.3.5.3 Ⅲ类标签模块

Ⅲ类标签模块数据传输完整性测试方式如下。

a) 检测要求

标签模块能够根据需要，为允许传输的敏感信息提供正确有效的数据传输完整性服务；

标签模块与读写器通信时，标签模块采用密码算法对传输的数据进行校验计算，以发现数据被篡改、删除和插入等情况，达到传输过程中的数据完整性要求。

b) 判定准则

信道传输的数据在传输过程中能够采用密码算法进行完整性保护。

6.3.5.4 Ⅳ类标签模块

同Ⅲ类标签模块。

6.3.6 数据存储完整性测试

6.3.6.1 Ⅰ类标签模块

无要求。

6.3.6.2 Ⅱ类标签模块

无要求。

6.3.6.3 Ⅲ类标签模块

Ⅲ类标签模块数据存储完整性测试方式如下。

a) 检测要求

标签模块能够根据需要，为存储的敏感信息提供正确有效的数据存储完整性服务；

标签模块采用密码算法对存储在标签模块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。

b) 判定准则

标签模块能够采用密码算法对存储的敏感信息数据进行完整性保护。

6.3.6.4 Ⅳ类标签模块

同Ⅲ类标签模块。

6.4 密码性能

6.4.1 鉴别性能测试

6.4.1.1 Ⅰ类标签模块

Ⅰ-A 类标签模块无要求。

Ⅰ-B类标签模块鉴别性能测试方式如下。

a） 检测要求

测试标签模块认证流程时长。

b） 判定准则

标签模块能够达到认证过程的时长要求。

6.4.1.2 Ⅱ类标签模块

同Ⅰ-B类标签模块。

6.4.1.3 Ⅲ类标签模块

同Ⅰ-B类标签模块。

6.4.1.4 Ⅳ类标签模块

同Ⅰ-B类标签模块。

6.4.2 数据交互性能测试

6.4.2.1 Ⅰ类标签模块

Ⅰ-A类标签模块无要求。

Ⅰ-B类标签模块数据交互性能测试方式如下。

a） 检测要求

测试标签模块数据交互(数据传输、数据处理及读写)的速率。

b） 判定准则

标签模块能够达到数据交互的速率要求。

6.4.2.2 Ⅱ类标签模块

同Ⅰ-B类标签模块。

6.4.2.3 Ⅲ类标签模块

同Ⅰ-B类标签模块。

6.4.2.4 Ⅳ类标签模块

同Ⅰ-B类标签模块。

6.5 敏感信息保护

6.5.1 口令保护测试

6.5.1.1 Ⅰ类标签模块

Ⅰ-A类标签模块无要求。

Ⅰ-B类标签模块口令保护测试方式如下。

a） 检测要求

标签模块采用口令保护方式对数据的读、写以及数据的更新等操作设置控制权限,阻止非授权的访问;

在用户应用时，读写器只能按照标签模块发行时所设置的口令权限对标签模块进行相关操作；标签模块能够根据需要正确、有效地操作敏感信息。

b） 判定准则

标签模块数据读、写及更新权限有效。

6.5.1.2 Ⅱ类标签模块

同Ⅰ-B类标签模块。

6.5.1.3 Ⅲ类标签模块

同Ⅰ-B类标签模块。

6.5.1.4 Ⅳ类标签模块

同Ⅰ-B类标签模块。

6.5.2 敏感信息保护测试

6.5.2.1 Ⅰ类标签模块

Ⅰ-A类标签模块无要求。

Ⅰ-B类标签模块敏感信息保护测试方式如下。

a） 检测要求

测试标签模块对敏感信息的防非法访问功能。

b） 判定准则

1） 标签模块具有防止存储数据被非法访问的功能；

2） 标签模块的关键参数和其他敏感信息不能通过物理或逻辑接口非法访问。

6.5.2.2 Ⅱ类标签模块

同Ⅰ-B类标签模块。

6.5.2.3 Ⅲ类标签模块

同Ⅰ-B类标签模块。

6.5.2.4 Ⅳ类标签模块

同Ⅰ-B类标签模块。

6.6 数据源鉴别

6.6.1 概述

电子标签原发数据源鉴别功能，使其能确保电子标签信息原发者不能成功地否认曾经生成过该信息，接收电子标签信息的主体能获得证明电子标签信息原发者的证据，而且该证据可由该主体或第三方验证。

电子标签数据源鉴别功能，即电子标签能对其生成的信息产生数字签名，确保电子标签不能成功地否认曾经生成过该信息，接收电子标签信息的主体能获得证明电子标签信息原发的证据，而且该证据可由该主体或第三方验证。

读写器数据源鉴别功能，使其能确保读写器不能成功地否认曾经生成过该信息，接收读写器信息的

主体能获得证明读写器信息原发的证据，而且该证据可由该主体或第三方等其他主体验证。

6.6.2 电子标签原发数据源鉴别测试

6.6.2.1 Ⅰ类标签模块

无要求。

6.6.2.2 Ⅱ类标签模块

无要求。

6.6.2.3 Ⅲ类标签模块

Ⅲ类标签模块电子标签原发数据源鉴别测试方式如下。

a) 检测要求

读取标签模块内存储的签名数据原文、数字签名和公钥证书，验证数字签名的合法性。

b) 判定准则

应符合 GM/T 0035.2—2014 中 5.3.1 的要求。

6.6.2.4 Ⅳ类标签模块

同Ⅲ类标签。

6.6.3 电子标签数据源鉴别测试

6.6.3.1 Ⅰ类标签模块

无要求。

6.6.3.2 Ⅱ类标签模块

无要求。

6.6.3.3 Ⅲ类标签模块

无要求。

6.6.3.4 Ⅳ类标签模块

Ⅳ类标签模块电子标签数据源鉴别测试方式如下。

a) 检测要求

读取标签模块内的签名数据原文、数字签名和公钥证书，验证数字签名的合法性。

b) 判定准则

应符合 GM/T 0035.2—2014 中 5.3.2 的要求。

6.6.4 读写器数据源鉴别测试

6.6.4.1 Ⅰ类标签模块

无要求。

6.6.4.2 Ⅱ类标签模块

无要求。

6.6.4.3 Ⅲ类标签模块

无要求。

6.6.4.4 Ⅳ类标签模块

Ⅳ类标签模块读写器数据源鉴别测试方式如下。

a) 检测要求

标签模块使用读写器的公钥证书、数字签名和签名数据原文，来验证读写器数字签名的合法性。

b) 判定准则

应符合 GM/T 0035.2—2014 中 5.3.3 的要求。

6.7 生命周期安全

6.7.1 标签模块灭活测试

6.7.1.1 Ⅰ类标签模块

Ⅰ类标签模块灭活测试方式如下。

a) 检测要求

测试标签模块灭活功能的有效性。

b) 判定准则

灭活后，被测标签模块不应有任何应答。

6.7.1.2 Ⅱ类标签模块

同Ⅰ类标签模块。

6.7.1.3 Ⅲ类标签模块

同Ⅰ类标签模块。

6.7.1.4 Ⅳ类标签模块

同Ⅰ类标签模块。

6.7.2 防非法指令测试

6.7.2.1 Ⅰ类标签模块

Ⅰ类标签模块防非法指令测试方式如下。

a) 检测要求

使用产品未定义或错误的指令，测试标签模块防非法指令的功能。

b) 判定准则

向被测标签模块发送产品未定义或错误的指令，标签模块应报错或不产生响应。

6.7.2.2 Ⅱ类标签模块

同Ⅰ类标签模块。

6.7.2.3 Ⅲ类标签模块

同Ⅰ类标签模块。

6.7.2.4 Ⅳ类标签模块

同Ⅰ类标签模块。

6.7.3 防初始使用权欺骗测试

6.7.3.1 Ⅰ类标签模块

Ⅰ类标签模块防初始使用权欺骗测试方式如下。

a) 检测要求

标签模块不提供初始化权限,对被测标签模块执行初始化操作,测试标签模块是否具备防初始化功能。

b) 判定准则

不能对被测标签模块执行初始化操作。

6.7.3.2 Ⅱ类标签模块

同Ⅰ类标签模块。

6.7.3.3 Ⅲ类标签模块

同Ⅰ类标签模块。

6.7.3.4 Ⅳ类标签模块

同Ⅰ类标签模块。

6.7.4 防生命周期越界测试

6.7.4.1 Ⅰ类标签模块

Ⅰ类标签模块防生命周期越界测试方式如下。

a) 检测要求

使用非当前生命周期阶段的指令,测试标签模块防生命周期越界功能。

b) 判定准则

向被测标签模块发送非当前生命周期阶段指令,标签模块应报错或不产生响应。

6.7.4.2 Ⅱ类标签模块

同Ⅰ类标签模块。

6.7.4.3 Ⅲ类标签模块

同Ⅰ类标签模块。

6.7.4.4 Ⅳ类标签模块

同Ⅰ类标签模块。

6.8 标签唯一性

6.8.1 Ⅰ类标签模块

Ⅰ类标签模块标签唯一性检测方式如下。

a) 检测要求

测试标签模块标识的唯一性，不同标签其标识不同，其标识唯一不可更改。

b) 判定准则

被测标签模块标识应与该标签模块提供的唯一标识一致。

6.8.2 Ⅱ类标签模块

同Ⅰ类标签模块。

6.8.3 Ⅲ类标签模块

同Ⅰ类标签模块。

6.8.4 Ⅳ类标签模块

同Ⅰ类标签模块。

6.9 审计记录

6.9.1 Ⅰ类标签模块

无要求。

6.9.2 Ⅱ类标签模块

无要求。

6.9.3 Ⅲ类标签模块

无要求。

6.9.4 Ⅳ类标签模块

Ⅳ类标签模块审计测试方式如下。

a) 检测要求

读取标签模块内存储的使用主体，使用时间，执行的操作等其他记录。

b) 判定准则

应符合 GM/T 0035.2—2014 中 5.6 的要求。

6.10 密钥管理

6.10.1 密钥生成

6.10.1.1 Ⅰ类标签模块

Ⅰ-A 类标签模块无要求。

Ⅰ-B 类标签模块使用的密钥数据应经由商用密码检测认证的密码设备随机生成。

6.10.1.2 Ⅱ类标签模块

同Ⅰ-B类标签模块。

6.10.1.3 Ⅲ类标签模块

同Ⅰ-B类标签模块。

6.10.1.4 Ⅳ类标签模块

同Ⅰ-B类标签模块。

6.10.2 密钥存储

6.10.2.1 Ⅰ类标签模块

Ⅰ-A类标签模块无要求。

Ⅰ-B类应能够正确、有效地存储密钥。

6.10.2.2 Ⅱ类标签模块

同Ⅰ-B类标签模块。

6.10.2.3 Ⅲ类标签模块

同Ⅰ-B类标签模块。

6.10.2.4 Ⅳ类标签模块

同Ⅰ-B类标签模块。

6.10.3 密钥使用

6.10.3.1 Ⅰ类标签模块

Ⅰ-A类标签模块无要求。

Ⅰ-B类应能够根据密钥的类型和使用场景等情况正确、有效地使用密钥。

6.10.3.2 Ⅱ类标签模块

同Ⅰ-B类标签模块。

6.10.3.3 Ⅲ类标签模块

同Ⅰ-B类标签模块。

6.10.3.4 Ⅳ类标签模块

同Ⅰ-B类标签模块。

6.10.4 密钥更新

6.10.4.1 Ⅰ类标签模块

Ⅰ-A类标签模块无要求。

对Ⅰ-B类标签模块，如果标签模块具备密钥更新功能，则应能够正确、有效地更新密钥。

6.10.4.2 Ⅱ类标签模块

同Ⅰ-B类标签模块。

6.10.4.3 Ⅲ类标签模块

同Ⅰ-B类标签模块。

6.10.4.4 Ⅳ类标签模块

同Ⅰ-B类标签模块。

6.10.5 密钥导入

6.10.5.1 Ⅰ类标签模块

Ⅰ-A类标签模块无要求。

Ⅰ-B类标签模块应能够正确、有效地导入密钥。

6.10.5.2 Ⅱ类标签模块

同Ⅰ-B类标签模块。

6.10.5.3 Ⅲ类标签模块

同Ⅰ-B类标签模块。

6.10.5.4 Ⅳ类标签模块

同Ⅰ-B类标签模块。

6.10.6 密钥清除

6.10.6.1 Ⅰ类标签模块

Ⅰ-A类标签模块无要求。

对Ⅰ-B类标签模块，如果标签模块具备密钥清除功能，则应能够根据需要正确、有效地清除存储的密钥。

6.10.6.2 Ⅱ类标签模块

同Ⅰ-B类标签模块。

6.10.6.3 Ⅲ类标签模块

同Ⅰ-B类标签模块。

6.10.6.4 Ⅳ类标签模块

同Ⅰ-B类标签模块。

附 录 A
（规范性）
射频识别标签模块密码检测项

射频识别标签模块密码检测项见表 A.1。

表 A.1 射频识别标签模块密码检测项

标签模块检测项			标签模块分类					
			Ⅰ类		Ⅱ类		Ⅲ类	Ⅳ类
			Ⅰ-A 类	Ⅰ-B 类	Ⅱ-A 类	Ⅱ-B 类		
密码算法	对称算法测试			√	√	√	√	√
	非对称算法测试							√
	密码杂凑函数测试							√
	算法实现正确性测试			√	√	√	√	√
	随机数测试	符合 GM/T 0005—2021 附录 A 中 A.1			√			
		符合 GM/T 0005—2021 附录 A 中 A.2				√	√	√
密码服务	身份鉴别测试	唯一标识符鉴别	√					
		单向鉴别测试		√				
		双向鉴别测试			√	√	√	√
	数据传输机密性测试				√	√	√	√
	数据存储机密性测试						√	√
	数据传输完整性测试						√	√
	数据存储完整性测试						√	√
密码性能	鉴别性能测试			√	√	√	√	√
	数据交互性能测试			√	√	√	√	√
敏感信息保护	口令保护测试			√注	√注	√注	√注	√注
	敏感信息保护测试			√	√	√	√	√
数据源鉴别	电子标签原发数据源鉴别测试						√	√
	电子标签数据源鉴别测试							√
	读写器数据源鉴别测试							√
生命周期安全	标签模块灭活测试		√	√	√	√	√	√
	防非法指令测试			√	√	√	√	√
	防初始使用权欺骗测试			√	√	√	√	√
	防生命周期越界测试		√	√	√	√	√	√

表 A.1　射频识别标签模块密码检测项（续）

标签模块检测项		标签模块分类					
		Ⅰ类		Ⅱ类		Ⅲ类	Ⅳ类
		Ⅰ-A类	Ⅰ-B类	Ⅱ-A类	Ⅱ-B类		
标签唯一性	唯一标识测试	√	√	√	√	√	√
审计记录							√
密钥管理			√	√	√	√	√

说明：“√”表示不同类别的射频识别标签模块中具备的密码检测项。

注：检测项可选。

中华人民共和国密码
行业标准
射频识别标签模块密码检测规范
GM/T 0040—2024
*
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)
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 1.5　字数 38 千字
2025年6月第1版　2025年6月第1次印刷
*
书号:155066·2-39087　定价 43.00 元

GM/T 0040-2024