ICS 35.240.15
CCS L 64
备案号 92455-2024

LD

中华人民共和国劳动和劳动安全行业标准

LD/T 6001.2—2023

社会保障卡检测规范
第2部分：卡内COS检测

Test specifications for social security card—
Part 2: Test of card operation system

2023-11-24 发布　　2023-12-01 实施

中华人民共和国人力资源和社会保障部　　发布

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。

本文件是LD/T 6001《社会保障卡检测规范》的第2部分。LD/T 6001已经发布了以下部分。

——第 1 部分：卡片质量物理特性检测；

——第 2 部分：卡内 COS 检测；

——第 3 部分：卡内数据结构及密钥装载检测（通用性检测）；

——第 4 部分：读写终端检测；

——第 5 部分：读写终端接口检测。

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。

本文件由人力资源社会保障部提出并归口。

本文件起草单位：人力资源社会保障部信息中心、上海市社会保障卡服务中心、江苏省人力资源社会保障信息中心、浙江省人力资源社会保障信息中心、安徽省人力资源社会保障信息中心、北京惟望科技发展有限公司、北京中电华大电子设计有限责任公司、楚天龙股份有限公司、深圳市德卡科技股份有限公司、深圳市明泰智能技术有限公司。

本文件主要起草人：魏丽丽、徐钰伟、李娜、于斌、王智飞、李晨星、高琦、宋京燕、邢勤、任鹏、肖可、潘明俊、郑斌、靳朝晖、高燕、张文杰、任小晢、盖树天、熊园、蒋东、段凯智。

引　言

社会保障卡全称为“中华人民共和国社会保障卡”，由人力资源社会保障部统一规划，各级人力资源社会保障部门联合服务银行面向社会公众发行，是持卡人享受人力资源社会保障权益及其他政府公共服务权益的服务载体。

制定LD/T 6001旨在规范社会保障卡检测工作，健全社会保障卡质量保障机制，提高社会保障卡制作、发行、应用的技术支撑水平，提升社会保障卡安全、通用、便民服务能力，实现“一卡多用、全国通用”，建立以社会保障卡为载体的居民服务“一卡通”。

LD/T 6001由五部分组成。

——第1部分：卡片质量物理特性检测。规范社会保障卡卡片物理特性检测方法和流程，保障社会保障卡卡片的物理质量水平符合规范性要求。

——第2部分：卡内COS检测。规范社会保障卡卡内操作系统的检测方法和流程，保障社会保障卡卡内操作系统的设计及安全机制符合规范性要求。

——第3部分：卡内数据结构及密钥装载检测（通用性检测）。规范社会保障卡卡内数据结构、读写数据安全性等检测方法和流程，保障社会保障卡卡内数据读写安全符合规范性要求。

——第4部分：读写终端检测。规范社会保障卡读写终端的检测方法和流程，保障社会保障卡应用相关的读写终端符合规范性要求。

——第5部分：读写终端接口检测。规范社会保障卡读写终端接口的检测方法和流程，保障社会保障卡应用相关的读写终端接口符合规范性要求。

社会保障卡检测规范
第2部分：卡内COS检测

1 范围

本文件规定了社会保障卡的命令功能、命令参数、防火墙和防拔的检测方法。

本文件适用于社会保障卡卡内命令设置、防火墙设置、医疗消费交易、数字证书应用设置以及社会保障卡终端的兼容性检测。

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。

LD/T 32.2 社会保障卡规范 第2部分：机电特性、逻辑接口和传输协议

LD/T 32.5 社会保障卡规范 第5部分：命令

LD/T 32.7 社会保障卡规范 第7部分：应用流程

3 术语和定义

下列术语和定义适用于本文件。

3.1

命令 command

终端向卡发出的一条信息，该信息启动一个操作或请求一个应答。

3.2

响应 response

卡处理完成收到的命令报文后，返回给终端的报文。

3.3

功能 function

由一个或多个命令实现，用于完成全部或部分交易的处理过程。

3.4

报文 message

由终端向卡或卡向终端发出的，不含传输控制字符的字节串。

4 符号和缩略语

下列符号和缩略语适用于本文件。

APDU：应用协议数据单元（application protocol data unit）

ATR：复位应答（answer to reset）

CLA：命令报文的类别字节（class byte of the command message）

COS：卡内操作系统（Chip Operating System）

INS：命令报文的指令字节（instruction byte of command message）

Lc：终端发出的命令数据的实际长度（exact length of data sent by the TAL in a case 3 or 4 command）

Le：响应数据的最大期望长度（maximum length of data expected by the TAL in response to a case 2 or 4 command）

P1：参数1（parameter 1）

P2：参数2（parameter 2）

5 测试环境条件

默认测试环境条件若无特殊说明，均在正常大气条件下进行，即：
——温度：15℃～35℃；
——相对湿度：45%～75%；
——大气压：86 kPa～106 kPa。
默认测试卡片已完成初始化。
默认测试终端为符合社会保障卡规范LD/T 32要求的社会保障卡终端。
本文件中有关传输协议的其他要求，按照LD/T 32.2的规定执行；有关命令的其他要求，按照LD/T 32.5的规定执行；有关应用流程的其他要求，按照LD/T 32.7的规定执行。

6 命令功能测试

6.1 APPLICATION BLOCK 命令

APPLICATION BLOCK命令的测试方法如下。
a) 测试目的：APPLICATION BLOCK 命令能够使当前选择的应用失效。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行 APPLICATION BLOCK 命令流程；
   3) 检验当前应用是否失效。
d) 通过标准：正确执行 APPLICATION BLOCK 命令后当前应用失效。

6.2 CARD BLOCK 命令

CARD BLOCK命令的测试方法如下。
a) 测试目的：CARD BLOCK 命令能够使社会保障系统环境中所有应用永久失效。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行 CARD BLOCK 命令流程；
   3) 检验社会保障系统环境中所有应用是否失效。
d) 通过标准：正确执行 CARD BLOCK 命令后社会保障系统环境中所有应用永久失效。

6.3 CHANGE PIN 命令

CHANGE PIN命令的测试方法如下。
a) 测试目的：CHANGE PIN 命令能够将当前 PIN 修改为新 PIN。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行 CHANGE PIN 命令流程；
   3) 检验当前 PIN 是否修改为新 PIN；
   4) 密码尝试计数器复位至密码尝试次数的上限；
   5) 检查 PIN 的有效格式。
d) 通过标准：正确执行 CHANGE PIN 命令后当前 PIN 修改为新 PIN，密码尝试计数器复位至密码尝试次数的上限。

6.4 EXTERNAL AUTHENTICATION 命令

EXTERNAL AUTHENTICATION命令的测试方法如下。

a) 测试目的：EXTERNAL AUTHENTICATION 命令能够使接口设备获得相应的授权。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行 EXTERNAL AUTHENTICATION 命令流程；
   3) 检验 EXTERNAL AUTHENTICATION 命令的授权是否正确。
d) 通过标准：正确执行 EXTERNAL AUTHENTICATION 命令后获得相应的授权且授权正确。

6.5 GET CHALLENGE 命令

GET CHALLENGE命令的测试方法如下。
a) 测试目的：GET CHALLENGE 命令能够获取到相应的随机数并保证该随机数在当前应用下只能使用一次。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行 GET CHALLENGE 命令流程；
   3) 检验随机数是否可以正确获得；
   4) 检验随机数在当前应用下是否仅能使用一次。
d) 通过标准：正确执行 GET CHALLENGE 命令后获取到相应的随机数并保证该随机数在当前应用下只能使用一次。

6.6 GET RESPONSE 命令

GET RESPONSE命令的测试方法如下。
a) 测试目的：GET RESPONSE 命令能够返回 APDU 的一部分。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行 GET RESPONSE 命令流程；
   3) 检验 GET RESPONSE 命令返回的数据是否为 APDU 的一部分。
d) 通过标准：正确执行 GET RESPONSE 命令后返回对应数据。

6.7 INTERNAL AUTHENTICATION 命令

INTERNAL AUTHENTICATION命令的测试方法如下。
a) 测试目的：INTERNAL AUTHENTICATION 命令能够实现 SSSE 层和 DF 层的数据鉴别功能。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行 INTERNAL AUTHENTICATION 命令流程；
   3) 检验 INTERNAL AUTHENTICATION 命令分别在 SSSE 层和 DF 层的特定鉴别作用。
d) 通过标准：正确执行 INTERNAL AUTHENTICATION 命令后在 SSSE 层和 DF 层实现数据鉴别的功能。

6.8 PIN CHANGE/UNBLOCK 命令

PIN CHANGE/UNBLOCK命令的测试方法如下。
a) 测试目的：PIN CHANGE/UNBLOCK 命令能够实现重置 PIN 或解锁 PIN。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行 PIN CHANGE/UNBLOCK 命令流程；
   3) 检验 PIN CHANGE/UNBLOCK 命令是否能够正确实现重置 PIN 或解锁 PIN。

d) 通过标准：正确执行 PIN CHANGE/UNBLOCK 命令后实现重置 PIN 或解锁 PIN，密码尝试计数器复位至密码尝试次数的上限。

6.9 READ BINARY 命令

READ BINARY命令的测试方法如下。

a) 测试目的：READ BINARY 命令能够用于读取透明文件的内容（或部分内容）。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行 READ BINARY 命令流程；
   3) 检验 READ BINARY 命令是否能够用于读取透明文件的内容（或部分内容）。
d) 通过标准：正确执行 READ BINARY 命令后实现读取透明文件的内容（或部分内容）。

6.10 READ RECORD 命令

READ RECORD命令的测试方法如下。

a) 测试目的：READ RECORD 命令能够读取记录结构的基本文件中一些指定的记录或一个记录起始部分的数据。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行 READ RECORD 命令流程；
   3) 检验 READ RECORD 命令是否能够读取记录结构的基本文件中一些指定的记录或一个记录起始部分的数据。
d) 通过标准：正确执行 READ RECORD 命令后实现读取记录结构的基本文件中一些指定的记录或一个记录起始部分的数据。

6.11 SELECT 命令

SELECT命令的测试方法如下。

a) 测试目的：SELECT 命令能够通过文件名或 AID、文件标识符来选择卡中的 SSSE、DDF 或 ADF，通过文件标识符来选择 ADF 中的 AEF；SELECT 命令执行成功后，SSSE、DDF 或 ADF、AEF 的路径被设定；SELECT 命令除选择 AEF 外，卡的响应报文应由回送的 FCI 组成；SELECT 命令执行后，在当前 ADF 未被 SELECT 命令改变或重新设定时，该 ADF 下的所有安全状态应被保持。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行 SELECT 命令流程；
   3) 检验 SELECT 命令是否能够通过文件名或 AID、文件标识符来选择卡中的 SSSE、DDF 或 ADF，通过文件标识符来选择 ADF 中的 AEF；
   4) 检验 SELECT 命令执行成功后，SSSE、DDF 或 ADF、AEF 的路径是否被设定；
   5) 检验 SELECT 命令执行后，返回的 FCI 是否正确；
   6) 检验 SELECT 命令执行后，在当前 ADF 未被 SELECT 命令改变或重新设定时，该 ADF 下的所有安全状态是否被保持。
d) 通过标准：
   1) 正确执行 SELECT 命令后通过文件名或 AID、文件标识符来选择卡中的 SSSE、DDF 或 ADF，通过文件标识符来选择 ADF 中的 AEF；
   2) SELECT 命令执行成功后，SSSE、DDF 或 ADF、AEF 的路径被设定；
   3) SELECT 命令执行后，返回的 FCI 正确；
   4) SELECT 命令执行后，在当前 ADF 未被 SELECT 命令改变或重新设定时，该 ADF 下的所有安全状态被保持。

6.12 UPDATE BINARY 命令

UPDATE BINARY命令的测试方法如下。

a) 测试目的：UPDATE BINARY 命令能够用于写入或修改透明结构的基本文件的全部或部分数据。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行 UPDATE BINARY 命令流程；
   3) 检验 UPDATE BINARY 命令是否能够写入或修改透明结构的基本文件的全部或部分数据。
d) 通过标准：正确执行 UPDATE BINARY 命令后实现写入或修改透明结构的基本文件的全部或部分数据。

6.13 UPDATE RECORD 命令

UPDATE RECORD命令的测试方法如下。

a) 测试目的：UPDATE RECORD 命令能够用于添加新的记录或修改指定记录。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行 UPDATE RECORD 命令流程；
   3) 检验 UPDATE RECORD 命令是否能够添加新的记录或修改指定记录。
d) 通过标准：
   1) 正确执行 UPDATE RECORD 命令后实现添加新的记录或修改指定记录；
   2) 对线性结构文件来说，当指定的记录号不存在时，可按记录号顺序添加新的记录。按记录标识符访问的记录不存在时，也应视为添加新的记录；
   3) 对循环结构文件来说，当使用“P1 指定标识符的上一个实例”命令选项时应视为添加新的记录；
   4) 在使用当前记录地址时，该命令将在修改记录成功后重新设定记录指针。

6.14 VERIFY 命令

VERIFY命令的测试方法如下。

a) 测试目的：VERIFY 命令能够用于校验命令数据域中的 PIN 的正确性。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行 VERIFY 命令流程；
   3) 检验 VERIFY 命令是否能够校验命令数据域中的 PIN 的正确性。
d) 通过标准：正确执行 VERIFY 命令后实现校验命令数据域中的 PIN 的正确性。

6.15 CREDIT FOR LOAD 命令

CREDIT FOR LOAD命令的测试方法如下。

a) 测试目的：CREDIT FOR LOAD 命令能够用于账户划入。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行 CREDIT FOR LOAD 命令流程；
   3) 检验 CREDIT FOR LOAD 命令是否实现正常账户划入。
d) 通过标准：正确执行 CREDIT FOR LOAD 命令后实现正常账户划入。

6.16 DEBIT FOR PURCHASE 命令

DEBIT FOR PURCHASE命令的测试方法如下：

a) 测试目的：DEBIT FOR PURCHASE 命令能够实现医疗费用结算。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行 DEBIT FOR PURCHASE 命令流程；
   3) 检验 DEBIT FOR PURCHASE 命令是否实现医疗费用结算。
d) 通过标准：正确执行 DEBIT FOR PURCHASE 命令后实现医疗费用结算。

6.17 GET BALANCE 命令

GET BALANCE命令的测试方法如下。
a) 测试目的：GET BALANCE 命令能够用于读取 CIA 余额/年度 SPIP 金额/年度 SPFP 金额。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行 GET BALANCE 命令流程；
   3) 检验 GET BALANCE 命令是否能够读取 CIA 余额/年度 SPIP 金额/年度 SPFP 金额。
d) 通过标准：正确执行 GET BALANCE 命令后实现正确读取 CIA 余额/年度 SPIP 金额/年度 SPFP 金额。

6.18 GET TRANSACTION PROOF 命令

GET TRANSACTION PROOF命令的测试方法如下。
a) 测试目的：GET TRANSACTION PROOF 命令能够用于取回 TAC 和 MAC。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行 GET TRANSACTION PROOF 命令流程；
   3) 检验 GET TRANSACTION PROOF 命令是否能够正确取回 TAC 和 MAC。
d) 通过标准：正确执行 GET TRANSACTION PROOF 命令后实现正确取回 TAC 和 MAC。

6.19 INITIALIZE FOR LOAD 命令

INITIALIZE FOR LOAD命令的测试方法如下。
a) 测试目的：INITIALIZE FOR LOAD 命令能够用于账户划入的初始化。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行 INITIALIZE FOR LOAD 命令流程；
   3) 检验 INITIALIZE FOR LOAD 命令是否能够实现账户划入的初始化。
d) 通过标准：正确执行 INITIALIZE FOR LOAD 命令后实现账户划入的初始化。

6.20 INITIALIZE FOR PURCHASE 命令

INITIALIZE FOR PURCHASE命令的测试方法如下。
a) 测试目的：INITIALIZE FOR PURCHASE 命令能够用于医疗费用结算的初始化。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行 INITIALIZE FOR PURCHASE 命令流程；
   3) 检验 INITIALIZE FOR PURCHASE 命令是否能够实现医疗费用结算的初始化。
d) 通过标准：正确执行 INITIALIZE FOR PURCHASE 命令后实现医疗费用结算的初始化。

6.21 UPDATE STARTING DAY 命令

UPDATE STARTING DAY命令的测试方法如下。

a) 测试目的：UPDATE STARTING DAY 命令能够用于修改医疗保险账户中的“年度起始日期”数据元。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行 UPDATE STARTING DAY 命令流程；
   3) 检验 UPDATE STARTING DAY 命令是否能够实现修改医疗保险账户中的“年度起始日期”数据元。
d) 通过标准：正确执行 UPDATE STARTING DAY 命令后实现修改医疗保险账户中的“年度起始日期”数据元。

6.22 GET STARTING DAY 命令

GET STARTING DAY命令的测试方法如下。

a) 测试目的：GET STARTING DAY 命令能够用于读取医疗保险账户中的“年度起始日期”数据元。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行 GET STARTING DAY 命令流程；
   3) 检验 GET STARTING DAY 命令是否能够读取医疗保险账户中的“年度起始日期”数据元。
d) 通过标准：正确执行 GET STARTING DAY 命令后实现读取医疗保险账户中的“年度起始日期”数据元。

6.23 CHANGE DEV KEY 命令

CHANGE DEV KEY 命令的测试方法如下。

a) 测试目的：CHANGE DEV KEY 命令能够用于修改 DF 的主控密钥。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行 CHANGE DEV KEY 命令流程；
   3) 检验 CHANGE DEV KEY 命令是否能够修改 DF 的主控密钥。
d) 通过标准：正确执行 CHANGE DEV KEY 命令后实现修改 DF 的主控密钥。

6.24 GENERATE KEY PAIR 命令

GENERATE KEY PAIR 命令的测试方法如下。

a) 测试目的：GENERATE KEY PAIR 命令能够用于产生 SM2 密钥对，同时将私钥和公钥分别存放在指定文件中。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行 GENERATE KEY PAIR 命令流程；
   3) 检验 GENERATE KEY PAIR 命令是否能够产生密钥对，同时将私钥和公钥分别存放在指定文件中。
d) 通过标准：正确执行 GENERATE KEY PAIR 命令后产生密钥对，同时将私钥和公钥分别存放在指定文件中。

6.25 GET PUBLIC KEY 命令

GET PUBLIC KEY 命令的测试方法如下。

a) 测试目的：GET PUBLIC KEY 命令能够用于导出指定公钥。
b) 测试条件：默认测试环境条件。

c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行 GET PUBLIC KEY 命令流程；
   3) 检验 GET PUBLIC KEY 命令是否能够导出指定公钥，该公钥受指定的私钥保护。
d) 通过标准：正确执行 GET PUBLIC KEY 命令后导出指定公钥，该公钥受指定的私钥保护。

6.26 STORE PKI KEY 命令

STORE PKI KEY命令的测试方法如下。
a) 测试目的：STORE PKI KEY 命令能够用于导入公钥到指定文件中。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行 STORE PKI KEY 命令流程；
   3) 检验 STORE PKI KEY 命令是否能够导入公钥，并能支持使用卡内对称会话密钥加密方式导入。
d) 通过标准：正确执行 STORE PKI KEY 命令后导入公钥，并能支持使用卡内对称会话密钥加密方式导入。

6.27 PUBLIC KEY OPERATION 命令

PUBLIC KEY OPERATION命令的测试方法如下。
a) 测试目的：PUBLIC KEY OPERATION 命令能够用于使用公钥进行加密/验签计算。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行 PUBLIC KEY OPERATION 命令流程；
   3) 检验 PUBLIC KEY OPERATION 命令是否能够使用公钥进行加密/验签计算。
d) 通过标准：正确执行 PUBLIC KEY OPERATION 命令后实现公钥加密/验签计算。

6.28 PRIVATE KEY OPERATION 命令

PRIVATE KEY OPERATION命令的测试方法如下。
a) 测试目的：PRIVATE KEY OPERATION 命令能够用于使用私钥进行加密/验签计算。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行 PRIVATE KEY OPERATION 命令流程；
   3) 检验 PRIVATE KEY OPERATION 命令是否能够使用私钥进行加密/验签计算。
d) 通过标准：正确执行 PRIVATE KEY OPERATION 命令后实现私钥加密/验签计算。

6.29 GENERATE ENVELOP 命令

GENERATE ENVELOP命令的测试方法如下。
a) 测试目的：GENERATE ENVELOP 命令能够用于内部生成加解密用对称会话密钥保存到 RAM 中并导出。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行 GENERATE ENVELOP 命令流程；
   3) 检验 GENERATE ENVELOP 命令是否能够用于内部生成加解密用对称会话密钥保存到 RAM 中并导出。
d) 通过标准：正确执行 GENERATE ENVELOP 命令后实现内部生成加解密用对称会话密钥保存到 RAM 中并导出。

6.30 OPEN ENVELOP 命令

OPEN ENVELOP命令的测试方法如下。

a) 测试目的：OPEN ENVELOP 命令能够使用明文或密文方式导入对称会话密钥。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行 OPEN ENVELOP 命令流程；
   3) 检验 OPEN ENVELOP 命令是否能够使用明文或密文方式导入对称会话密钥,该会话密钥保存在卡内易失性存储器中（卡内最多同时保存 5 条会话密钥），卡片掉电后自动失效。密钥在应用目录重新选择后继续有效，也可以删除指定会话密钥。
d) 通过标准：正确执行 OPEN ENVELOP 命令后实现用明文或密文方式导入对称会话密钥、可以同时保存 5 条、卡片掉电后自动失效。密钥在应用目录重新选择后继续有效，可以删除指定会话密钥。

6.31 CIPHER DATA 命令

CIPHER DATA命令的测试方法如下。

a) 测试目的：CIPHER DATA 命令能够使用对称会话密钥对数据进行加解密。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行 CIPHER DATA 命令流程；
   3) 检验 CIPHER DATA 命令是否能够使用对称会话密钥对数据进行加解密。
d) 通过标准：正确执行 CIPHER DATA 命令后实现用对称会话密钥对数据进行加解密。

6.32 HASH OPERATION 命令

HASH OPERATION命令的测试方法如下。

a) 测试目的：HASH OPERATION 命令能够用安全散列算法将数据压缩为固定长度字节。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行 HASH OPERATION 命令流程；
   3) 检验 HASH OPERATION 命令是否能够用安全散列算法将数据压缩为固定长度字节。
d) 通过标准：正确执行 HASH OPERATION 命令后实现用安全散列算法将数据压缩为固定长度字节。

7 命令参数测试

7.1 APPLICATION BLOCK 命令

APPLICATION BLOCK命令的测试方法如下。

a) 测试目的：APPLICATION BLOCK 命令中 CLA、INS、P1、P2、Lc、Data 参数全部符合要求。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行完整的 APPLICATION BLOCK 命令参数检索流程。
d) 通过标准：APPLICATION BLOCK 命令中 CLA、INS、P1、P2、Lc、Data 参数全部符合要求。

7.2 CARD BLOCK 命令

CARD BLOCK命令的测试方法如下。

a) 测试目的：CARD BLOCK 命令中 CLA、INS、P1、P2、Lc、Le 参数全部符合要求。
b) 测试条件：默认测试环境条件。

c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行完整的 CARD BLOCK 命令参数检索流程。
d) 通过标准：CARD BLOCK 命令中 CLA、INS、P1、P2、Lc、Le 参数全部符合要求。

7.3 CHANGE PIN 命令

CHANGE PIN命令的测试方法如下。

a) 测试目的：CHANGE PIN 命令中 CLA、INS、P1、P2、Lc、Data 参数全部符合要求。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行完整的 CHANGE PIN 命令参数检索流程。
d) 通过标准：CHANGE PIN 命令中 CLA、INS、P1、P2、Lc、Data 参数全部符合要求。

7.4 EXTERNAL AUTHENTICATION 命令

EXTERNAL AUTHENTICATION命令的测试方法如下。

a) 测试目的：EXTERNAL AUTHENTICATION 命令中 CLA、INS、P1、P2、Lc、Data 参数全部符合要求。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行完整的 EXTERNAL AUTHENTICATION 命令参数检索流程。
d) 通过标准：EXTERNAL AUTHENTICATION 命令中 CLA、INS、P1、P2、Lc、Data 参数全部符合要求。

7.5 GET CHALLENGE 命令

GET CHALLENGE命令的测试方法如下。

a) 测试目的：GET CHALLENGE 命令中 CLA、INS、P1、P2、Data、Le 参数全部符合要求。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行完整的 GET CHALLENGE 命令参数检索流程。
d) 通过标准：GET CHALLENGE 命令中 CLA、INS、P1、P2、Data、Le 参数全部符合要求。

7.6 GET RESPONSE 命令

GET RESPONSE命令的测试方法如下。

a) 测试目的：GET RESPONSE 命令中 CLA、INS、P1、P2、Data、Le 参数全部符合要求。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行完整的 GET RESPONSE 命令参数检索流程。
d) 通过标准：GET RESPONSE 命令中 CLA、INS、P1、P2、Data、Le 参数全部符合要求。

7.7 INTERNAL AUTHENTICATION 命令

INTERNAL AUTHENTICATION命令的测试方法如下。

a) 测试目的：INTERNAL AUTHENTICATION 命令中 CLA、INS、P1、P2、Lc、Data、Le 参数全部符合要求。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；

2) 执行完整的 INTERNAL AUTHENTICATION 命令参数检索流程。

d) 通过标准：INTERNAL AUTHENTICATION 命令中 CLA、INS、P1、P2、Lc、Data、Le 参数全部符合要求。

7.8 PIN CHANGE/UNBLOCK 命令

PIN CHANGE/UNBLOCK命令的测试方法如下。

a) 测试目的：PIN CHANGE/UNBLOCK 命令中 CLA、INS、P1、P2、Lc、Data 参数全部符合要求。

b) 测试条件：默认测试环境条件。

c) 测试流程：

1) 发起冷复位并接收冷复位 ATR；

2) 执行完整的 PIN CHANGE/UNBLOCK 命令参数检索流程。

d) 通过标准：PIN CHANGE/UNBLOCK 命令中 CLA、INS、P1、P2、Lc、Data 参数全部符合要求。

7.9 READ BINARY 命令

READ BINARY命令的测试方法如下。

a) 测试目的：READ BINARY 命令中 CLA、INS、P1、P2、Data、Le 参数全部符合要求。

b) 测试条件：默认测试环境条件。

c) 测试流程：

1) 发起冷复位并接收冷复位 ATR；

2) 执行完整的 READ BINARY 命令参数检索流程。

d) 通过标准：READ BINARY 命令中 CLA、INS、P1、P2、Data、Le 参数全部符合要求。

7.10 READ RECORD 命令

READ RECORD命令的测试方法如下。

a) 测试目的：READ RECORD 命令中 CLA、INS、P1、P2、Data、Le 参数全部符合要求。

b) 测试条件：默认测试环境条件。

c) 测试流程：

1) 发起冷复位并接收冷复位 ATR；

2) 执行完整的 READ RECORD 命令参数检索流程。

d) 通过标准：READ RECORD 命令中 CLA、INS、P1、P2、Data、Le 参数全部符合要求。

7.11 SELECT 命令

SELECT命令的测试方法如下。

a) 测试目的：SELECT 命令中 CLA、INS、P1、P2、Lc、Data、Le 参数全部符合要求。

b) 测试条件：默认测试环境条件。

c) 测试流程：

1) 发起冷复位并接收冷复位 ATR；

2) 执行完整的 SELECT 命令参数检索流程。

d) 通过标准：SELECT 命令中 CLA、INS、P1、P2、Lc、Data、Le 参数全部符合要求。

7.12 UPDATE BINARY 命令

UPDATE BINARY命令的测试方法如下。

a) 测试目的：UPDATE BINARY 命令中 CLA、INS、P1、P2、Lc、Data 参数全部符合要求。

b) 测试条件：默认测试环境条件。

c) 测试流程：

1) 发起冷复位并接收冷复位 ATR；

2) 执行完整的 UPDATE BINARY 命令参数检索流程。

d) 通过标准：UPDATE BINARY 命令中 CLA、INS、P1、P2、Lc、Data 参数全部符合要求。

7.13 UPDATE RECORD 命令

UPDATE RECORD命令的测试方法如下。

a) 测试目的：UPDATE RECORD 命令中 CLA、INS、P1、P2、Lc、Data 参数全部符合要求。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行完整的 UPDATE RECORD 命令参数检索流程。
d) 通过标准：UPDATE RECORD 命令中 CLA、INS、P1、P2、Lc、Data 参数全部符合要求。

7.14 VERIFY 命令

VERIFY命令的测试方法如下。

a) 测试目的：VERIFY 命令中 CLA、INS、P1、P2、Lc、Data 参数全部符合要求。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行完整的 VERIFY 命令参数检索流程。
d) 通过标准：VERIFY 命令中 CLA、INS、P1、P2、Lc、Data 参数全部符合要求。

7.15 CREDIT FOR LOAD 命令

CREDIT FOR LOAD命令的测试方法如下。

a) 测试目的：CREDIT FOR LOAD 命令中 CLA、INS、P1、P2、Lc、Data、Le 参数全部符合要求。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行完整的 CREDIT FOR LOAD 命令参数检索流程。
d) 通过标准：CREDIT FOR LOAD 命令中 CLA、INS、P1、P2、Lc、Data、Le 参数全部符合要求。

7.16 DEBIT FOR PURCHASE 命令

DEBIT FOR PURCHASE命令的测试方法如下。

a) 测试目的：DEBIT FOR PURCHASE 命令中 CLA、INS、P1、P2、Lc、Data、Le 参数全部符合要求。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行完整的 DEBIT FOR PURCHASE 命令参数检索流程。
d) 通过标准：DEBIT FOR PURCHASE 命令中 CLA、INS、P1、P2、Lc、Data、Le 参数全部符合要求。

7.17 GET BALANCE 命令

GET BALANCE命令的测试方法如下。

a) 测试目的：GET BALANCE 命令中 CLA、INS、P1、P2、Data、Le 参数全部符合要求。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行完整的 GET BALANCE 命令参数检索流程。
d) 通过标准：GET BALANCE 命令中 CLA、INS、P1、P2、Data、Le 参数全部符合要求。

7.18 GET TRANSACTION PROOF 命令

GET TRANSACTION PROOF命令的测试方法如下。

a) 测试目的：GET TRANSACTION PROOF 命令中 CLA、INS、P1、P2、Lc、Data、Le 参数全部符合要求。
b) 测试条件：默认测试环境条件。
c) 测试流程：

1) 发起冷复位并接收冷复位 ATR；
2) 执行完整的 GET TRANSACTION PROOF 命令参数检索流程。

d) 通过标准：GET TRANSACTION PROOF 命令中 CLA、INS、P1、P2、Lc、Data、Le 参数全部符合要求。

7.19 INITIALIZE FOR LOAD 命令

INITIALIZE FOR LOAD命令的测试方法如下。

a) 测试目的：INITIALIZE FOR LOAD 命令中 CLA、INS、P1、P2、Lc、Data、Le 参数全部符合要求。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行完整的 INITIALIZE FOR LOAD 命令参数检索流程。
d) 通过标准：INITIALIZE FOR LOAD 命令中 CLA、INS、P1、P2、Lc、Data、Le 参数全部符合要求。

7.20 INITIALIZE FOR PURCHASE 命令

INITIALIZE FOR PURCHASE命令的测试方法如下。

a) 测试目的：INITIALIZE FOR PURCHASE 命令中 CLA、INS、P1、P2、Lc、Data、Le 参数全部符合要求。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行完整的 INITIALIZE FOR PURCHASE 命令参数检索流程。
d) 通过标准：INITIALIZE FOR PURCHASE 命令中 CLA、INS、P1、P2、Lc、Data、Le 参数全部符合要求。

7.21 UPDATE STARTING DAY 命令

UPDATE STARTING DAY命令的测试方法如下。

a) 测试目的：UPDATE STARTING DAY 命令中 CLA、INS、P1、P2、Lc、Data 参数全部符合要求。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行完整的 UPDATE STARTING DAY 命令参数检索流程。
d) 通过标准：UPDATE STARTING DAY 命令中 CLA、INS、P1、P2、Lc、Data 参数全部符合要求。

7.22 GET STARTING DAY 命令

GET STARTING DAY命令的测试方法如下。

a) 测试目的：GET STARTING DAY 命令中 CLA、INS、P1、P2、Data、Le 参数全部符合要求。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行完整的 GET STARTING DAY 命令参数检索流程。
d) 通过标准：GET STARTING DAY 命令中 CLA、INS、P1、P2、Data、Le 参数全部符合要求。

7.23 CHANGE DEV KEY 命令

CHANGE DEV KEY命令的测试方法如下。

a) 测试目的：CHANGE DEV KEY 命令中 CLA、INS、P1、P2、Lc、Data 参数全部符合要求。
b) 测试条件：默认测试环境条件。
c) 测试流程：

1) 发起冷复位并接收冷复位 ATR；
2) 执行完整的 CHANGE DEV KEY 命令参数检索流程。

d) 通过标准：CHANGE DEV KEY 命令中 CLA、INS、P1、P2、Lc、Data 参数全部符合要求。

7.24 GENERATE KEY PAIR 命令

GENERATE KEY PAIR命令的测试方法如下。

a) 测试目的：GENERATE KEY PAIR 命令中 CLA、INS、P1、P2、Lc、Data 参数全部符合要求。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行完整的 GENERATE KEY PAIR 命令参数检索流程。
d) 通过标准：GENERATE KEY PAIR 命令中 CLA、INS、P1、P2、Lc、Data 参数全部符合要求。

7.25 GET PUBLIC KEY 命令

GET PUBLIC KEY命令的测试方法如下。

a) 测试目的：GET PUBLIC KEY 命令中 CLA、INS、P1、P2、Lc、Data、Le 参数全部符合要求。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行完整的 GET PUBLIC KEY 命令参数检索流程。
d) 通过标准：GET PUBLIC KEY 命令中 CLA、INS、P1、P2、Lc、Data、Le 参数全部符合要求。

7.26 STORE PKI KEY 命令

STORE PKI KEY命令的测试方法如下。

a) 测试目的：STORE PKI KEY 命令中 CLA、INS、P1、P2、Lc、Data 参数全部符合要求。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行完整的 STORE PKI KEY 命令参数检索流程。
d) 通过标准：STORE PKI KEY 命令中 CLA、INS、P1、P2、Lc、Data 参数全部符合要求。

7.27 PUBLIC KEY OPERATION 命令

PUBLIC KEY OPERATION命令的测试方法如下。

a) 测试目的：PUBLIC KEY OPERATION 命令中 CLA、INS、P1、P2、Lc、Data、Le 参数全部符合要求。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行完整的 PUBLIC KEY OPERATION 命令参数检索流程。
d) 通过标准：PUBLIC KEY OPERATION 命令中 CLA、INS、P1、P2、Lc、Data、Le 参数全部符合要求。

7.28 PRIVATE KEY OPERATION 命令

PRIVATE KEY OPERATION命令的测试方法如下。

a) 测试目的：PRIVATE KEY OPERATION 命令中 CLA、INS、P1、P2、Lc、Data、Le 参数全部符合要求。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行完整的 PRIVATE KEY OPERATION 命令参数检索流程。

d) 通过标准：PRIVATE KEY OPERATION 命令中 CLA、INS、P1、P2、Lc、Data、Le 参数全部符合要求。

7.29 GENERATE ENVELOP 命令

GENERATE ENVELOP命令的测试方法如下。

a) 测试目的：GENERATE ENVELOP 命令中 CLA、INS、P1、P2、Lc、Data、Le 参数全部符合要求。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行完整的 GENERATE ENVELOP 命令参数检索流程。
d) 通过标准：GENERATE ENVELOP 命令中 CLA、INS、P1、P2、Lc、Data、Le 参数全部符合要求。

7.30 OPEN ENVELOP 命令

OPEN ENVELOP命令的测试方法如下。

a) 测试目的：OPEN ENVELOP 命令中 CLA、INS、P1、P2、Lc、Data、Le 参数全部符合要求。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行完整的 OPEN ENVELOP 命令参数检索流程。
d) 通过标准：OPEN ENVELOP 命令中 CLA、INS、P1、P2、Lc、Data、Le 参数全部符合要求。

7.31 CIPHER DATA 命令

CIPHER DATA命令的测试方法如下。

a) 测试目的：CIPHER DATA 命令中 CLA、INS、P1、P2、Lc、Data、Le 参数全部符合要求。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行完整的 CIPHER DATA 命令参数检索流程。
d) 通过标准：CIPHER DATA 命令中 CLA、INS、P1、P2、Lc、Data、Le 参数全部符合要求。

7.32 HASH OPERATION 命令

HASH OPERATION命令的测试方法如下。

a) 测试目的：HASH OPERATION 命令中 CLA、INS、P1、P2、Lc、Data、Le 参数全部符合要求。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行完整的 HASH OPERATION 命令参数检索流程。
d) 通过标准：HASH OPERATION 命令中 CLA、INS、P1、P2、Lc、Data、Le 参数全部符合要求。

8 防火墙测试

防火墙测试的测试方法如下。

a) 测试目的：测试各个系统环境相互不受影响。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 建立若干个系统环境；
   3) 依次选择一个环境进行功能测试或者命令操作，检验其他环境内功能是否保持不变。
d) 通过标准：各个系统环境相互独立，互不干预。

9 防拔测试

防拔测试的测试方法如下。

a) 测试目的：COS 中的所有命令符合防拔要求。
b) 测试条件：默认测试环境条件。
c) 测试流程：
   1) 发起冷复位并接收冷复位 ATR；
   2) 执行完整命令功能和命令参数检索的防拔测试流程。
d) 通过标准：COS 中的所有命令功能和命令参数检索符合防拔机制要求。

参 考 文 献

[1] GB/T 16649.1—2006 识别卡 带触点的集成电路卡 第1部分：物理特性
[2] GB/T 16649.2—2006 识别卡 带触点的集成电路卡 第2部分：触点的尺寸和位置
[3] GB/T 16649.3—2006 识别卡 带触点的集成电路卡 第3部分：电信号和传输协议
[4] GB/T 17554.1—2006 识别卡 测试方法 第1部分：一般特性测试
[5] GB/T 17554.3—2006 识别卡 测试方法 第3部分：带触点的集成电路卡及其相关接口设备
[6] GB/T 19584—2010 银行卡磁条信息格式和使用规范
[7] JR/T 0025—2018 中国金融集成电路（IC）卡规范
[8] 中国人民银行 人力资源社会保障部关于社会保障卡银行业务应用有关事宜的通知（银发〔2010〕348号）
[9] 人力资源社会保障部、中国人民银行关于社会保障卡加载金融功能的通知（人社部发〔2011〕83号）
[10] 中国人民银行办公厅 人力资源社会保障部办公厅关于印发《具有金融功能的第三代社会保障卡技术规范》的通知（银办发〔2017〕170号）