ICS 35.240.15
CCS L 64
备案号 92458-2024

LD

中华人民共和国劳动和劳动安全行业标准

LD/T 6001.5—2023

社会保障卡检测规范
第5部分：读写终端接口检测

Test specifications for social security card—
Part5: Test of read-write terminal interface

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5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、西藏自治区人力资源社会保障厅信息中心、甘肃省人力资源社会保障厅综合信息办公室、青海省金保工程管理办公室、新疆维吾尔自治区社会保障卡管理中心、新疆生产建设兵团社会保障卡服务中心、北京惟望科技发展有限公司、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：徐钰伟、魏丽丽、李晨星、李娜、于斌、王智飞、高琦、宋京燕、谭军、陈耀江、任秀玲、周鹏、杨明、靳朝晖、高燕、张文杰、任小晢、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5部分：读写终端接口检测

1 范围

本文件规定了社会保障卡读写终端接口检测环境要求，以及基于PSAM卡社会保障卡读写终端接口检测方法、基于加密机社会保障卡读写终端接口检测方法和数字证书接口检测方法。

本文件适用于社会保障卡应用相关的各类读写终端接口的检测。

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 02.5 人力资源社会保障电子认证体系规范 第5部分：数字证书载体规范

LD/T 32.2 社会保障卡规范 第2部分：机电特性、逻辑接口与传输协议

LD/T 32.3 社会保障卡规范 第3部分：文件系统和应用选择

LD/T 32.4 社会保障卡规范 第4部分：安全机制

LD/T 32.5 社会保障卡规范 第5部分：命令

LD/T 32.6 社会保障卡规范 第6部分：应用数据结构

LD/T 32.7 社会保障卡规范 第7部分：应用流程

LD/T 33 社会保障卡读写终端规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

终端 terminal

为处理卡业务而在服务网点安装的设备，用于同卡的连接，包括接口设备、其他部件和接口。

注：终端可包括接口设备、其他部件和接口。

3.2

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。

3.3

交易 transaction

持卡人和业务、管理部门之间根据卡所支持的应用接受、提供服务的行为。

4 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。

本文件中有关读写终端接口的其他要求，按照LD/T 32.2、LD/T 33的规定执行；有关证书逻辑的其他要求，按照LD/T 02.5的规定执行。

5 基于PSAM卡社会保障卡读写终端接口测试

5.1 “读基本信息”函数 long iReadCardBas （int iType, char* pOutInfo）

“读基本信息”函数的测试方法如下。

a) 测试目的：根据所需读取的信息进行认证后读出卡内基本文件的文件信息。
b) 测试条件：
   1) 默认环境条件；
   2) 待测产品上电；
   3) 测试卡；
   4) PSAM 卡。
c) 测试流程：输入参数 int iType 值，取值范围 1～4。
d) 通过标准：选择社会保障系统环境成功，确定算法环境正确，执行内部认证通过，若规范版本为 3.0 的卡，外部认证通过。当函数执行成功时，读取出的信息与卡内基本文件信息一致，其格式为：发卡地区行政区划代码（卡识别码前 6 位）、社会保障号码、卡号、卡识别码、姓名、卡复位信息（仅取历史字节）、规范版本、发卡日期、卡有效期、终端机编号、终端设备号，各数据项之间以“|”分割，且最后一个数据项以“|”结尾。

5.2 “通用读卡”函数 long iReadCard （int iType, int iAuthType, char* pCardInfo, char* pFileAddr, char* pOutInfo）

“通用读卡”函数的测试方法如下。

a) 测试目的：根据所需读取的信息进行认证后读出卡内指定文件信息。
b) 测试条件：
   1) 默认环境条件；
   2) 待测产品上电；
   3) 测试卡；
   4) PSAM 卡。
c) 测试流程：
   1) 输入参数 int iType 值，取值范围 1～4；
   2) 输入参数 int iAuthType，取值范围 1～2，根据输入值指定读控制认证方式，1-PIN 校验，2-RK 密钥认证；
   3) 输入参数 char* pCardInfo，传入卡的基本信息，依次为：卡识别码、卡号，各数据项之间以“|”分割，且最后一个数据项以“|”结尾；
   4) 输入参数 char* pFileAddr，指定需要读出的文件和文件下的数据项。
d) 通过标准：选择社会保障系统环境成功，确定算法环境正确，执行内部认证通过，若规范版本为 3.0 的卡，外部认证通过。卡的基本信息比对通过，所要读取的信息所在的文件读取权限认证通过。当函数执行成功时，读取出的信息与卡内指定文件信息一致，其格式与输入参数 char* pFileAddr 严格对应且分隔符完全一致。

5.3 “通用写卡”函数 long iWriteCard （int iType, char* pCardInfo, char* pFileAddr, char* pWriteData, char* pOutInfo）

“通用写卡”函数的测试方法如下。

a) 测试目的：根据所需写入的信息，先做外部认证，认证通过后写入指定文件。
b) 测试条件：
   1) 默认环境条件；
   2) 待测产品上电；
   3) 测试卡；
   4) PSAM 卡。
c) 测试流程：
   1) 输入参数 int iType 值，取值范围 1～4；
   2) 输入参数 char* pCardInfo，传入卡的基本信息，依次为：卡识别码、卡号。各数据项之间以“|”分割，且最后一个数据项以“|”结尾；

3) 输入参数 char* pFileAddr；
4) 本函数只允许对一个文件进行操作。若传入多个文件则只对第一个文件进行操作，后续内容将被忽略。
5) 输入参数 char* pWriteData，传入拟写入的数据项信息。

d) 通过标准：选择社会保障系统环境成功，确定算法环境正确，执行内部认证通过，若规范版本为 3.0 的卡，外部认证通过。卡的基本信息比对通过，所要写入的信息所在的文件写入权限认证通过。当函数执行成功时，读取出的指定写入文件信息与需要写入的文件信息一致。

5.4 “PIN 校验”函数 Long iVerifyPIN （int iType, char* pOutInfo）

“PIN校验”函数的测试方法如下。

a) 测试目的：校验 PIN。
b) 测试条件：
   1) 默认环境条件；
   2) 待测产品上电；
   3) 测试卡；
   4) PSAM 卡。
c) 测试流程：输入参数 int iType 值，取值范围 1～4。
d) 通过标准：选择社会保障系统环境成功，执行内部认证通过，启动密码键盘成功，获取 PIN 成功。当函数执行成功时，当前 PIN 校验成功。

5.5 “PIN 修改”函数 long iChangePIN （int iType, char* pOutInfo）

“PIN修改”函数的测试方法如下。

a) 测试目的：修改 PIN。
b) 测试条件：
   1) 默认环境条件；
   2) 待测产品上电；
   3) 测试卡；
   4) PSAM 卡。
c) 测试流程：输入参数 int iType 值，取值范围 1～4。
d) 通过标准：选择社会保障系统环境成功，执行内部认证通过，启动密码键盘成功，获取当前 PIN、新 PIN 成功。当函数执行成功时，当前 PIN 修改成功，校验新 PIN 通过。

5.6 “PIN 重置”函数 long iReloadPIN （int iType, char* pCardInfo, char* pOutInfo）

“PIN重置”函数的测试方法如下。

a) 测试目的：重置 PIN。
b) 测试条件：
   1) 默认环境条件；
   2) 待测产品上电；
   3) 测试卡；
   4) PSAM 卡。
c) 测试流程：
   1) 输入参数 int iType 值，取值范围 1～4；
   2) 输入参数 char* pCardInfo，传入卡的基本信息。
d) 通过标准：选择社会保障系统环境成功，确定算法环境正确，执行内部认证通过，若规范版本为 3.0 的卡，外部认证通过，卡的基本信息比对通过，启动密码键盘成功，获取新 PIN 成功。当函数执行成功时，当前 PIN 重置成功，校验新 PIN 通过。

5.7 “PIN 解锁”函数 long iUnblockPIN （int iType, char* pCardInfo, char* pOutInfo）

“PIN解锁”函数的测试方法如下：

a) 测试目的：解锁 PIN。

b) 测试条件：
   1) 默认环境条件；
   2) 待测产品上电；
   3) 测试卡；
   4) PSAM 卡。
c) 测试流程：
   1) 输入参数 int iType 值，取值范围 1～4；
   2) 输入参数 char* pCardInfo，传入卡的基本信息。
d) 通过标准：选择社会保障系统环境成功，确定算法环境正确，执行内部认证通过，若规范版本为 3.0 的卡，外部认证通过，卡的基本信息比对通过。当函数执行成功时，当前 PIN 解锁成功，校验原 PIN 通过。

5.8 “消费交易”函数 long iDoDebit （int iType, char* pCardInfo, char* pPayInfo, char* pOutInfo）

“消费交易”函数的测试方法如下：

a) 测试目的：执行社保卡消费交易并写入消费记录。
b) 测试条件：
   1) 默认环境条件；
   2) 待测产品上电；
   3) 测试卡；
   4) PSAM 卡。
c) 测试流程：
   1) 输入参数 int iType 值，取值范围 1～4；
   2) 输入参数 char* pCardInfo，传入卡的基本信息；
   3) 输入参数 char* pPayInfo，传入消费相关信息，依次为：本次消费总金额(小于 42949672.95 的小数，小数点后保留两位)、个人账户交易金额和统筹基金支付金额相加的总金额（小于 42949672.95 的小数，小数点后保留两位）、交易时间（格式为 YYYYMMDDHHMMSS），各数据项之间以“|”分割，且最后一个数据项以“|”结尾。
d) 通过标准：选择社会保障系统环境成功，确定算法环境正确，执行内部认证通过，若规范版本为 3.0 的卡，外部认证通过，卡的基本信息比对通过，PIN 校验通过，执行医疗初始化命令通过，进行消费交易操作。当函数执行成功时，其格式为：算法标识、密钥地址、交易金额（转换成十六进制向卡片发送命令时的后两个金额拼接组成）、交易类型、终端机编号、终端交易序号、交易时间（格式为 YYYYMMDDHHMMSS）、交易验证码（TAC），各数据项之间以“|”分割，且最后一个数据项以“|”结尾。

5.9 “读消费交易记录”函数 long iReadDebitRecord （int iType, char* pOutInfo）

“读消费交易记录”函数的测试方法如下。

a) 测试目的：读取消费交易记录。
b) 测试条件：
   1) 默认环境条件；
   2) 待测产品上电；
   3) 测试卡；
   4) PSAM 卡。
c) 测试流程：输入参数 int iType 值，取值范围 1～4。
d) 通过标准：选择社会保障系统环境成功，执行内部认证通过，PIN 校验通过。当函数执行成功时，读取出的信息与卡内消费交易记录一致，每条记录由交易序号、终端机编号、交易时间（格式为 YYYYMMDDHHMMSS）、本次消费总金额、个人账户交易金额和统筹基金支付金额相加的总金额组成，每条记录之间以“|”分隔，每条记录里面的数据项之间以“^”分隔，最后一个数据项以“^”结尾，最后一条记录以“|”结尾。

6 基于加密机社会保障卡读写终端接口测试

6.1 “读基本信息”函数

6.1.1 “基于加密机的读基本信息(步骤一)”函数 longiReadCardBas_HSM_Step1 （int iType, char* pOutInfo）

“基于加密机的读基本信息（步骤一）”函数的测试方法如下。

a) 测试目的：选择社会保障系统环境后，返回内部认证和外部认证所需信息。

b) 测试条件：

1) 默认环境条件；

2) 待测产品上电；

3) 测试卡；

4) PSAM 卡。

c) 测试流程：输入参数 int iType 值，取值范围 1～4。

d) 通过标准：选择社会保障系统环境成功，确定算法环境正确，从卡内取 2 个随机数作为内部认证过程因子和内部认证鉴别所需的原始信息，当规范版本为 3.0 的卡，再从卡片取 2 个随机数作为外部认证过程因子和外部认证鉴别所需的原始信息。当函数执行成功时，输出为社保卡内部认证和外部认证的计算数据，其格式为：发卡地区行政区划代码（卡识别码前 6 位）、卡复位信息（仅取历史字节）、算法标识、卡识别码、内部认证过程因子、内部认证鉴别所需的原始信息、外部认证过程因子、外部认证鉴别所需的原始信息，其中外部认证相关数据项全部不为空或全部为空，各数据项之间以“|”分割，且最后一个数据项以“|”结尾。

6.1.2 “基于加密机的读基本信息（步骤二）”函数 long iReadCardBas_HSM_Step2 （char *pKey, char* pOutInfo）

“基于加密机的读基本信息（步骤二）”函数的测试方法如下。

a) 测试目的：根据加密机返回的内部认证和外部认证结果数据对社保卡进行内部认证和外部认证，通过后将卡内的基本信息读出返回。

b) 测试条件：

1) 默认环境条件；

2) 待测产品上电；

3) 测试卡；

4) PSAM 卡。

c) 测试流程：输入参数 char *pKey，加密机返回的内部认证和外部认证结果数据，依次为：内部认证结果数据（内部认证鉴别数据（16 位）和内部认证鉴别所需的原始信息（16 位）拼接组成）、外部认证结果数据（外部认证鉴别数据（16 位）和外部认证鉴别所需的原始信息（16 位）拼接组成），各数据项之间以“|”分割，且最后一个数据项以“|”结尾。

d) 通过标准：比对卡片和加密机返回的内部认证鉴别数据正确。当规范版本为 3.0 的卡，同时比对外部认证鉴别数据正确。当函数执行成功时，读取出的信息与卡内基本文件信息一致，其格式为：发卡地区行政区划代码（卡识别码前 6 位）、社会保障号码、卡号、卡识别码、姓名、卡复位信息（仅取历史字节）、规范版本、发卡日期、卡有效期、终端机编号、终端设备号，各数据项之间以“|”分割，且最后一个数据项以“|”结尾。

6.2 “通用读卡”函数

6.2.1 “基于加密机的通用读卡（步骤一）”函数 long iReadCard_HSM_Step1 （int iType, char* pCardInfo, char* pFileAddr, char* pOutInfo）

“基于加密机的通用读卡（步骤一）”函数的测试方法如下。

a) 测试目的：根据所需读取的信息确定需要认证的密钥，并返回认证所需信息。

b) 测试条件：

1) 默认环境条件；

2） 待测产品上电；
3） 测试卡；
4） PSAM 卡。

c） 测试流程：
1） 输入参数 int iType 值，取值范围 1～4；
2） 输入参数 char* pCardInfo，传入卡的基本信息，依次为：卡识别码、卡号，各数据项之间以“|”分割，且最后一个数据项以“|”结尾；
3） 输入参数 char* pFileAddr，指定需要读出的文件和文件下的数据项，根据不同的卡内规范版本选择对应的文件结构。

d） 通过标准：选择社会保障系统环境成功，确定算法环境正确，执行内部认证通过，若规范版本为 3.0 的卡，外部认证通过，卡的基本信息比对通过，从卡片取 2 个随机数作为外部认证过程因子和外部认证鉴别所需的原始信息。当函数执行成功时，其格式为：算法标识、外部认证密钥地址、外部认证过程因子（从卡片获得的随机数）、外部认证鉴别所需的原始信息（从卡片获得的随机数），各数据项之间以“|”分割，且最后一个数据项以“|”结尾。

6.2.2 “基于加密机的通用读卡（步骤二）”函数 long iReadCard_HSM_Step2 （char* pKey, char* pOutInfo）

“基于加密机的通用读卡（步骤二）”函数的测试方法如下。

a） 测试目的：根据加密机返回的结果数据对社保卡进行外部认证，通过后读出卡内指定文件的信息。

b） 测试条件：
1） 默认环境条件；
2） 待测产品上电；
3） 测试卡；
4） PSAM 卡。

c） 测试流程：输入参数 char* pKey，传入由加密机返回的结果数据，由鉴别数据（过程因子分散后加密原始信息的密文）和鉴别所需的原始信息拼接组成，总长度为 32 位。

d） 通过标准：外部认证通过。当函数执行成功时，且读取出的信息与卡内指定文件信息一致，其格式与输入参数 char* pFileAddr 严格对应且分隔符完全一致。

6.3 “通用写卡”函数

6.3.1 “基于加密机的通用写卡（步骤一）”函数 long iWriteCard_HSM_Step1 （int iType, char* pCardInfo, char* pFileAddr, char* pOutInfo）

“基于加密机的通用写卡（步骤一）”函数测试方法如下。

a） 测试目的：根据所需写入的信息确定需要认证的密钥，并返回认证所需信息。

b） 测试条件：
1） 默认环境条件；
2） 待测产品上电；
3） 测试卡；
4） PSAM 卡。

c） 测试流程：
1） 输入参数 int iType 值，取值范围 1～4；
2） 输入参数 char* pCardInfo，传入卡的基本信息，依次为：卡识别码、卡号，各数据项之间以“|”分割，且最后一个数据项以“|”结尾；
3） 输入参数 char* pFileAddr，用于指定需要读出的文件和文件下的数据项，根据不同的卡内规范版本选择对应的文件结构。

d） 通过标准：选择社会保障系统环境成功，确定算法环境正确，执行内部认证通过，若规范版本为 3.0 的卡，外部认证通过，卡的基本信息比对通过，从卡片取 2 个随机数作为外部认证过程因子和外部认证鉴别所需的原始信息。当函数执行成功时，其格式为：算法标识、外部认证密

钥地址、外部认证过程因子（从卡片获得的随机数）、外部认证鉴别所需的原始信息（从卡片获得的随机数），各数据项之间以“|”分割，且最后一个数据项以“|”结尾。

6.3.2 “基于加密机的通用写卡（步骤二）”函数 long iWriteCard_HSM_Step2 （char* pKey, char* pWriteData, char* pOutInfo）

“基于加密机的通用写卡（步骤二）”函数测试方法如下。

a) 测试目的：根据加密机返回的结果数据对社保卡进行外部认证，通过后写入卡内指定文件。
b) 测试条件：
   1) 默认环境条件；
   2) 待测产品上电；
   3) 测试卡；
   4) PSAM 卡。
c) 测试流程：
   1) 输入参数 char* pKey，传入由加密机返回的结果数据，由鉴别数据（过程因子分散后加密原始信息的密文）和鉴别所需的原始信息拼接组成，总长度为 32 位；
   2) 输入参数 char* pWriteData，传入要写入的数据项信息。
d) 通过标准：外部认证通过。当函数执行成功时，读取出的指定写入文件信息与需要写入的文件信息一致。

6.4 “PIN 重置”函数

6.4.1 “基于加密机的 PIN 重置（步骤一）”函数 long iReloadPIN_HSM_Step1 （int iType, char* pCardInfo, char* pOutInfo）

“基于加密机的PIN重置（步骤一）”函数测试方法如下。

a) 测试目的：获取新 PIN，返回所需的认证信息。
b) 测试条件：
   1) 默认环境条件；
   2) 待测产品上电；
   3) 测试卡；
   4) PSAM 卡。
c) 测试流程：
   1) 输入参数 int iType 值，取值范围 1～4；
   2) 输入参数 char* pCardInfo，传入卡的基本信息，依次为：卡识别码、卡号，各数据项之间以“|”分割，且最后一个数据项以“|”结尾。
d) 通过标准：选择社会保障系统环境成功，确定算法环境正确，执行内部认证通过，若规范版本为 3.0 的卡，外部认证通过，卡的基本信息比对通过，从卡片取 2 个随机数作为外部认证过程因子和外部认证鉴别所需的原始信息。当函数执行成功时，其格式为：算法标识、外部认证密钥地址、外部认证过程因子（从卡片获得的随机数）、外部认证鉴别所需的原始信息（从卡片获得的随机数），各数据项之间以“|”分割，且最后一个数据项以“|”结尾。

6.4.2 “基于加密机的 PIN 重置（步骤二）”函数 long iReloadPIN_HSM_Step2 （char* pKey, char* pOutInfo）

“基于加密机的PIN重置（步骤二）”函数的测试方法如下。

a) 测试目的：进行外部认证，返回安全报文计算数据。
b) 测试条件：
   1) 默认环境条件；
   2) 待测产品上电；
   3) 测试卡；
   4) PSAM 卡。

c) 测试流程：输入参数 char* pKey，传入由加密机返回的结果数据，由鉴别数据（过程因子分散后加密原始信息的密文）和鉴别所需的原始信息拼接组成，总长度为 32 位。
d) 通过标准：外部认证通过，启动密码键盘成功，获取新 PIN 成功，产生安全报文计算数据。当函数执行成功时，其格式为：算法标识、安全报文计算密钥地址、安全报文计算过程因子（从卡片获得的随机数）、APDU 命令头、APDU 命令明文数据（新 PIN），各数据项之间以“|”分割，且最后一个数据项以“|”结尾。

6.4.3 “基于加密机的 PIN 重置（步骤三）”函数 long iReloadPIN_HSM_Step3 （char* pKey, char* pOutInfo）

“基于加密机的PIN重置（步骤三）”函数的测试方法如下。

a) 测试目的：完成 PIN 重置。
b) 测试条件：
   1) 默认环境条件；
   2) 待测产品上电；
   3) 测试卡；
   4) PSAM 卡。
c) 测试流程：输入参数 char* pKey，传入由加密机计算的安全报文数据，由命令头、加密数据和 MAC 拼接组成，总长度为 34 位或 50 位。
d) 通过标准：当函数执行成功时，当前 PIN 重置成功，校验新 PIN 通过。

6.5 “PIN 解锁”函数

6.5.1 “基于加密机的 PIN 解锁（步骤一）”函数 long iUnblockPIN_HSM_Step1 （int iType, char* pCardInfo, char* pOutInfo）

“基于加密机的PIN解锁（步骤一）”函数的测试方法如下。

a) 测试目的：获得所需的认证信息。
b) 测试条件：
   1) 默认环境条件；
   2) 待测产品上电；
   3) 测试卡；
   4) PSAM 卡。
c) 测试流程：
   1) 输入参数 int iType 值，取值范围 1～4；
   2) 输入参数 char* pCardInfo，传入卡的基本信息，依次为：卡识别码、卡号，各数据项之间以“|”分割，且最后一个数据项以“|”结尾。
d) 通过标准：选择社会保障系统环境成功，确定算法环境正确，执行内部认证通过，若规范版本为 3.0 的卡，外部认证通过，卡的基本信息比对通过，从卡片取 2 个随机数作为外部认证过程因子和外部认证鉴别所需的原始信息。当函数执行成功时，其格式为：算法标识、外部认证密钥地址、外部认证过程因子（从卡片获得的随机数）、外部认证鉴别所需的原始信息（从卡片获得的随机数），各数据项之间以“|”分割，且最后一个数据项以“|”结尾。

6.5.2 “基于加密机的 PIN 解锁（步骤二）”函数 long iUnblockPIN_HSM_Step2 （char* pKey, char* pOutInfo）

“基于加密机的PIN解锁（步骤二）”函数的测试方法如下。

a) 测试目的：进行外部认证，返回安全报文计算数据。
b) 测试条件：
   1) 默认环境条件；
   2) 待测产品上电；
   3) 测试卡；
   4) PSAM 卡。

c) 测试流程：输入参数 char* pKey，传入由加密机返回的结果数据，由鉴别数据（过程因子分散后加密原始信息的密文）和鉴别所需的原始信息拼接组成，总长度为 32 位。
d) 通过标准：外部认证通过，产生安全报文计算数据。当函数执行成功时，其格式为：算法标识、安全报文计算密钥地址、安全报文计算过程因子（从卡片获得的随机数）、APDU 命令头、APDU 命令明文数据（空字符串），各数据项之间以“|”分割，且最后一个数据项以“|”结尾。

6.5.3 “基于加密机的 PIN 解锁（步骤三）”函数 long iUnblockPIN_HSM_Step3 (char* pKey, char* pOutInfo)

“基于加密机的PIN解锁（步骤三）”函数的测试方法如下。

a) 测试目的：完成 PIN 解锁。
b) 测试条件：
   1) 默认环境条件；
   2) 待测产品上电；
   3) 测试卡；
   4) PSAM 卡。
c) 测试流程：输入参数 char* pKey，传入由加密机计算的安全报文数据，由命令头和 MAC 拼接组成，总长度为 18 位。
d) 通过标准：当函数执行成功时，当前 PIN 解锁成功，校验原 PIN 通过。

6.6 “消费交易”函数

6.6.1 “基于加密机的消费交易（步骤一）”函数 long iDoDebit_HSM_Step1 (int iType, char* pCardInfo, char* pPayInfo, char* pOutInfo)

“基于加密机的消费交易（步骤一）”函数的测试方法如下。

a) 测试目的：执行社保卡消费交易初始化命令并返回交易认证相关数据。
b) 测试条件：
   1) 默认环境条件；
   2) 待测产品上电；
   3) 测试卡；
   4) PSAM 卡。
c) 测试流程：
   1) 输入参数 int iType 值，取值范围 1～4；
   2) 输入参数 char* pCardInfo，传入卡的基本信息，依次为：卡识别码、卡号，各数据项之间以“|”分割，且最后一个数据项以“|”结尾；
   3) 输入参数 char* pPayInfo，传入消费相关信息，依次为：本次消费总金额(小于 42949672.95 的小数，小数点后保留两位)、个人账户交易金额和统筹基金支付金额相加的总金额（小于 42949672.95 的小数，小数点后保留两位）、交易时间（格式为 YYYYMMDDHHMMSS），各数据项之间以“|”分割，且最后一个数据项以“|”结尾。
d) 通过标准：选择社会保障系统环境成功，确定算法环境正确，执行内部认证通过，若规范版本为 3.0 的卡，外部认证通过，卡的基本信息比对通过，PIN 校验通过，执行医疗初始化命令通过，返回用于计算 MAC1 的相关交易认证数据。当函数执行成功时，其格式为：算法标识、密钥地址、伪随机数、医疗消费交易序号、交易金额（转换成十六进制向卡片发送命令时的后两个金额拼接组成）、交易类型、终端机编号、交易时间（格式为 YYYYMMDDHHMMSS），各数据项之间以“|”分割，且最后一个数据项以“|”结尾。

6.6.2 “基于加密机的消费交易（步骤二）”函数 long iDoDebit_ HSM_Step2 (char* pKey, char* pOutInfo)

“基于加密机的消费交易（步骤二）”函数的测试方法如下。

a) 测试目的：完成消费交易写入消费记录。
b) 测试条件：

1) 默认环境条件；
2) 待测产品上电；
3) 测试卡；
4) PSAM 卡。

c) 测试流程：输入参数 char* pKey，传入由加密机计算的交易认证数据，依次为：终端交易序号、交易时间、MAC1，各数据项之间以“|”分割，且最后一个数据项以“|”结尾。

d) 通过标准：进行消费交易操作。当函数执行成功时，其格式为：MAC2、算法标识、密钥地址、交易金额（转换成十六进制向卡片发送命令时的后两个金额拼接组成）、交易类型、终端机编号、终端交易序号、交易时间（格式为 YYYYMMDDHHMMSS）、交易验证码（TAC），各数据项之间以“|”分割，且最后一个数据项以“|”结尾。

7 数字证书接口函数测试

7.1 “签名”函数 long stdcall PKI_SignData （char* pUserPin，char* pInData，int iType，char*pOutInfo）

“签名”函数的测试方法如下。

a) 测试目的：对输入数据进行数字签名，签名前必须先校验私钥保护口令。

b) 测试条件：
1) 默认环境条件；
2) 待测产品上电；
3) 测试卡；
4) PSAM 卡。

c) 测试流程：
1) 输入参数 char* pUserPin，用户 PIN，传入 NULL，将启动密码键盘输入；
2) 输入参数 char* pInData，待签名数据；
3) 输入参数 int iType，签名值类型，取值：0-1。

d) 通过标准：选择非对称认证系统环境成功，选择社会保障证书应用成功，用户 PIN 认证通过。当函数执行成功时，数据签名成功。

7.2 “验证签名”函数 long stdcall PKI_VerifySign （char* pUserPin，char* pCert，char* pClearText，char* pSignature，int iType，char*pOutInfo）

“验证签名”函数的测试方法如下。

a) 测试目的：对输入数据进行数字签名的验证，此过程不验证证书。

b) 测试条件：
1) 默认环境条件；
2) 待测产品上电；
3) 测试卡；
4) PSAM 卡。

c) 测试流程：
1) 输入参数 char* pUserPin，用户 PIN，传入 NULL，将启动密码键盘输入；
2) 输入参数 char* pCert，验证所使用的经 Base64 编码后的签名证书；
3) 输入参数 char* pClearText，签名的原文数据；
4) 输入参数 char* pSignature，经 Base64 编码后的待验证的签名数据；
5) 输入参数 int iType，签名值类型，取值：0-1。

d) 通过标准：选择非对称认证系统环境成功，选择社会保障证书应用成功，解析签名证书公钥成功，导入卡内临时公钥文件成功。当函数执行成功时，数据验签成功。

7.3 “数字信封加密”函数 long stdcall PKI_SealEnvelope （char* pUserPin，char* pCert，char* pInData，char* pOutInfo）

“数字信封加密”函数测试的方法如下：

a) 测试目的：加密所使用的经 Base64 编码后的数字证书。
b) 测试条件：
   1) 默认环境条件；
   2) 待测产品上电；
   3) 测试卡；
   4) PSAM 卡。
c) 测试流程：
   1) 输入参数 char* pUserPin，用户 PIN，传入 NULL，将启动密码键盘输入；
   2) 输入参数 char* pCert，用来加密对称密钥的加密证书；
   3) 输入参数 char* pInData，原文信息，必须为 16 字节倍数。
d) 通过标准：选择非对称认证系统环境成功，选择社会保障证书应用成功，解析签名证书公钥成功，导入卡内临时公钥文件成功。当函数执行成功时，输出加密后的密文数据。

7.4 “解析数字信封”函数 Long stdcall PKI_OpenEnvelope （char*pUserPin，char*pInData，char*pOutInfo）

“解析数字信封”函数测试的方法如下。

a) 测试目的：解析数字信封，解密之前必须先校验私钥保护口令。
b) 测试条件：
   1) 默认环境条件；
   2) 待测产品上电；
   3) 测试卡；
   4) PSAM 卡。
c) 测试流程：
   1) 输入参数 char* pUserPin，用户 PIN，传入 NULL，将启动密码键盘输入；
   2) 输入参数 char*pInData，Base64 编码的信封密文数据。
d) 通过标准：选择非对称认证系统环境成功，选择社会保障证书应用成功，用户 PIN 认证通过。当函数执行成功时，输出为解密后的原文数据。

7.5 “哈希”函数 long stdcall PKI_HashData （char*pInData，char*pOutInfo）

“哈希”函数测试的方法如下。

a) 测试目的：对输入数据进行哈希运算。
b) 测试条件：
   1) 默认环境条件；
   2) 待测产品上电；
   3) 测试卡；
   4) PSAM 卡。
c) 测试流程：输入参数 char*pInData，待计算的原文数据。
d) 通过标准:选择非对称认证系统环境成功。当函数执行成功时,输出 Base64 编码后的 hash 值。

7.6 “读证书接口”函数 long stdcall PKI_GetCert （int iType，char* pOutInfo）

“读证书接口”函数测试的方法如下。

a) 测试目的：获取用户证书。
b) 测试条件：
   1) 默认环境条件；
   2) 待测产品上电；
   3) 测试卡；
   4) PSAM 卡。
c) 测试流程：输入参数 int iType 值，取值范围 1 或者 2，1 表示加密证书，2 表示签名证书。

d) 通过标准：选择非对称认证系统环境成功，选择证书应用文件成功。当函数执行成功时，输出Base64编码后的证书数据。

7.7 “修改PIN”函数 long stdcall PKI_ChangePIN （int iType, char* pOldPin, char* pNewPin, char* pOutInfo）

“修改PIN”函数测试的方法如下。

a) 测试目的：修改证书PIN。
b) 测试条件：
   1) 默认环境条件；
   2) 待测产品上电；
   3) 测试卡；
   4) PSAM卡。
c) 测试流程：
   1) 输入参数int iType值，取值范围1～2，1-管理员，2-普通用户；
   2) 输入参数char* pOldPin，原证书PIN；
   3) 输入参数char* pNewPin，待修改的新证书PIN。
d) 通过标准：选择非对称认证系统环境成功，选择证书应用文件成功，启动密码键盘成功，获取当前PIN和新PIN成功。当函数执行成功时，当前PIN修改成功，新PIN检验成功。

7.8 “解锁用户PIN”函数 long stdcall PKI_UnblockPIN （char* pAdminPIN, char* pNewUserPIN, char* pOutInfo）

“解锁用户PIN”函数测试的方法如下。

a) 测试目的：解锁用户原证书PIN，解锁后用户原证书PIN设置为新证书PIN。
b) 测试条件：
   1) 默认环境条件；
   2) 待测产品上电；
   3) 测试卡；
   4) PSAM卡。
c) 测试流程：
   1) 输入参数char* pAdminPIN，证书管理员PIN；
   2) 输入参数char* pNewUserPIN，用户新证书PIN。
d) 通过标准：选择非对称认证系统环境成功，选择证书应用文件成功，启动密码键盘成功，获取新PIN成功。当函数执行成功时，当前解锁用户PIN成功。

7.9 “签名公私钥对”函数 long stdcallPKI_GetPublicKey （char* pUserPin, int iType, char* pOutInfo）

“签名公私钥对”函数测试的方法如下。

a) 测试目的：产生签名公私钥对，并输出编码后的公钥数据。
b) 测试条件：
   1) 默认环境条件；
   2) 待测产品上电；
   3) 测试卡；
   4) PSAM卡。
c) 测试流程：
   1) 输入参数char* pUserPin，用户证书PIN；
   2) 输入参数int iType，取值范围0～1，0-直接导出签名公私钥，1-重新生成签名公私钥。
d) 通过标准：选择非对称认证系统环境成功，选择社会保障证书应用成功，PIN认证通过，重新生成签名公私钥对成功。当函数执行成功时，输出Base64编码后的公钥数据。

7.10 “证书初始化”函数 long stdcall PKI_CardPersonInit（char* pUserPin,char* pPrivateKey, char* pEnCert, char* pSignCert, char* pOldDevKey, char* pNewDevKey, char* pOutInfo）

“证书初始化”函数测试的方法如下。

a) 测试目的：写入数字证书。

b) 测试条件：

1) 默认环境条件；
2) 待测产品上电；
3) 测试卡；
4) PSAM 卡。

c) 测试流程：

1) 输入参数 char* pUserPin，用户证书 PIN；
2) 输入参数 char* pPrivateKey，经 Base64 编码的私钥文件数据；
3) 输入参数 char* pEnCert，经 Base64 编码的加密证书文件数据；
4) 输入参数 char* pSignCert，经 Base64 编码的签名证书文件数据；
5) 输入参数 char* pOldDevKey，旧的主控密钥（需要约定初始值！）；
6) 输入参数 char* pNewDevKey，新的主控密钥。

d) 通过标准：选择非对称认证系统环境成功，选择社会保障证书应用成功，PIN 认证通过。当函数执行成功时，证书初始化成功。

参 考 文 献

[1] LD/T 02.1—2022 人力资源社会保障电子认证体系规范 第1部分：框架规范
[2] LD/T 02.2—2022 人力资源社会保障电子认证体系规范 第2部分：电子认证系统技术规范
[3] LD/T 02.3—2022 人力资源社会保障电子认证体系规范 第3部分：数字证书格式规范
[4] LD/T 02.4—2022 人力资源社会保障电子认证体系规范 第4部分：数字证书应用接口规范
[5] 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）
[6] 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）
[7] 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）
[8] 关于印发社会保障卡读写终端接口规范的通知（人社信息函〔2016〕38号）
[9] 关于印发社会保障卡读写终端接口规范补充说明的通知（人社信息函〔2016〕59号）
[10] 关于印发第三代社会保障卡相关技术规范的通知（人社信息函〔2018〕1号）
[11] 社会保障卡规范 第9部分：非对称认证应用技术要求（人社信息函〔2016〕38号）
[12] 关于印发社会保障卡读写终端接口规范的通知（人社信息函〔2016〕38号）
[13] 关于印发社会保障卡读写终端接口规范补充说明的通知（人社信息函〔2016〕59号）