ICS 35.240.15
CCS L 64
备案号 92456-2024

LD

中华人民共和国劳动和劳动安全行业标准

LD/T 6001.3—2023

社会保障卡检测规范 第3部分：卡内数据结构及密钥装载检测（通用性检测）

Test specifications for social security card—
Part 3: Test of the universality of data structure and key loading

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3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、北京惟望科技发展有限公司、福建省人力资源社会保障信息中心、江西省社会保障卡服务中心、河南省社会保障卡服务中心、湖北省人力资源社会保障信息中心、山东省东营市人力资源社会保障局、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：徐钰伟、魏丽丽、王智飞、李晨星、李娜、于斌、高琦、宋京燕、吴数园、丁志强、彭慧、汤隽、杨爽、燕习勤、靳朝晖、高燕、张文杰、任小晢、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3部分：卡内数据结构及密钥装载检测（通用性检测）

1 范围

本文件规定了社会保障卡记录规范性、读写安全性、密钥多版本和非对称应用等检测的检测方法。
本文件适用于社会保障卡发卡前卡内数据结构和密钥装载的正确性检测。

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 32.6 社会保障卡规范 第6部分：应用数据结构

3 术语和定义

本文件没有需要界定的术语和定义。

4 符号和缩略语

下列符号和缩略语适用于本文件。

ACSE：非对称认证系统环境（asymmetric authentication system environment）
ATR：复位应答（answer to reset）
EF：基本文件（elementary file）
PIN：个人密码（personal identification number）
SSSE：社会保障系统环境（social security system environment）

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。
默认测试卡片为符合社会保障卡规范要求的社会保障卡。
默认测试终端为符合社会保障卡规范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 基本测试

6.1 CHANGE PIN命令

CHANGE PIN命令的测试方法如下。
a) 测试目的：CHANGE PIN命令允许持卡人将当前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。

d) 通过标准：执行 CHANGE PIN 命令能够实现持卡人将当前 PIN 修改为新 PIN。

6.2 复位应答

复位应答的测试方法如下。

a) 测试目的：检查复位应答信息中 T1-T7 是否满足要求。
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) 检查复位应答信息中 T1-T7 是否满足要求。
d) 通过标准：复位应答返回的 T1-T7 真实有效。

7 记录规范性测试

7.1 SSSE_RECORD

SSSE_RECORD的测试方法如下。

a) 测试目的：检查 SSSE 下的所有 EF 文件下的所有数据项是否满足规范 LD/T 32.6 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) 读取 SSSE 下所有 EF 文件下的所有数据项；
3) 检查所有数据项是否满足规范 LD/T 32.6 要求。
d) 通过标准：能够顺利读取所有文件和数据项，所有数据项的格式满足规范 LD/T 32.6 要求。

7.2 DF01_RECORD

DF01_RECORD的测试方法如下。

a) 测试目的：检查 DF01 下的所有 EF 文件下的所有数据项是否满足规范 LD/T 32.6 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) 读取 DF01 下所有 EF 文件下的所有数据项；
3) 检查所有数据项是否满足规范 LD/T 32.6 要求。
d) 通过标准：能够顺利读取所有文件和数据项，所有数据项的格式满足规范 LD/T 32.6 要求。

7.3 DF02_RECORD

DF02_RECORD的测试方法如下。

a) 测试目的：检查 DF02 下的所有 EF 文件下的所有数据项是否满足规范 LD/T 32.6 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) 读取 DF02 下所有 EF 文件下的所有数据项；
3) 检查所有数据项是否满足规范 LD/T 32.6 要求。
d) 通过标准：能够顺利读取所有文件和数据项，所有数据项的格式满足规范 LD/T 32.6 要求。

7.4 DF03_RECORD

DF03_RECORD的测试方法如下。

a) 测试目的：检查 DF03 下的所有 EF 文件下的所有数据项是否满足规范 LD/T 32.6 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) 读取 DF03 下所有 EF 文件下的所有数据项；
   3) 检查所有数据项是否满足规范 LD/T 32.6 要求。
d) 通过标准：能够顺利读取所有文件和数据项，所有数据项的格式满足规范 LD/T 32.6 要求。

7.5 DF04_RECORD

DF04_RECORD的测试方法如下。
a) 测试目的：检查 DF04 下的所有 EF 文件下的所有数据项是否满足规范 LD/T 32.6 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) 读取 DF04 下所有 EF 文件下的所有数据项；
   3) 检查所有数据项是否满足规范 LD/T 32.6 要求。
d) 通过标准：能够顺利读取所有文件和数据项，所有数据项的格式满足规范 LD/T 32.6 要求。

7.6 DF05_RECORD

DF05_RECORD的测试方法如下。
a) 测试目的：检查 DF05 下的所有 EF 文件下的所有数据项是否满足规范 LD/T 32.6 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) 读取 DF05 下所有 EF 文件下的所有数据项；
   3) 检查所有数据项是否满足规范 LD/T 32.6 要求。
d) 通过标准：能够顺利读取所有文件和数据项，所有数据项的格式满足规范 LD/T 32.6 要求。

7.7 DF07_RECORD

DF07_RECORD的测试方法如下。
a) 测试目的：检查 DF07 下的所有 EF 文件下的所有数据项是否满足规范 LD/T 32.6 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) 读取 DF07 下所有 EF 文件下的所有数据项；
   3) 检查所有数据项是否满足规范 LD/T 32.6 要求。
d) 通过标准：能够顺利读取所有文件和数据项，所有数据项的格式满足规范 LD/T 32.6 要求。

8 读写安全性测试

8.1 SSSE_SAFETY

SSSE_SAFETY的测试方法如下。
a) 测试目的：检查 SSSE 下的所有 EF 文件的读写权限是否满足规范 LD/T 32.6 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) 检查 SSSE 下所有 EF 文件的读权限；
   3) 检查 SSSE 下所有 EF 文件的写权限。
d) 通过标准：SSSE 下的所有 EF 文件的读权限和写权限满足规范 LD/T 32.6 要求。

8.2 DF01_SAFETY

DF01_SAFETY的测试方法如下。

a) 测试目的：检查DF01下的所有EF文件的读写权限是否满足规范LD/T 32.6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) 检查DF01下所有EF文件的读权限；
   3) 检查DF01下所有EF文件的写权限。
d) 通过标准：DF01下的所有EF文件的读权限和写权限满足规范LD/T 32.6要求。

8.3 DF02_SAFETY

DF02_SAFETY的测试方法如下。

a) 测试目的：检查DF02下的所有EF文件的读写权限是否满足规范LD/T 32.6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) 检查DF02下所有EF文件的读权限；
   3) 检查DF02下所有EF文件的写权限。
d) 通过标准：DF02下的所有EF文件的读权限和写权限满足规范LD/T 32.6要求。

8.4 DF03_SAFETY

DF03_SAFETY的测试方法如下。

a) 测试目的：检查DF03下的所有EF文件的读写权限是否满足规范LD/T 32.6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) 检查DF03下所有EF文件的读权限；
   3) 检查DF03下所有EF文件的写权限。
d) 通过标准：DF03下的所有EF文件的读权限和写权限满足规范LD/T 32.6要求。

8.5 DF04_SAFETY

DF04_SAFETY的测试方法如下。

a) 测试目的：检查DF04下的所有EF文件的读写权限是否满足规范LD/T 32.6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) 检查DF04下所有EF文件的读权限；
   3) 检查DF04下所有EF文件的写权限。
d) 通过标准：DF04下的所有EF文件的读权限和写权限满足规范LD/T 32.6要求。

8.6 DF05_SAFETY

DF05_SAFETY的测试方法如下。

a) 测试目的：检查DF05下的所有EF文件的读写权限是否满足规范LD/T 32.6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) 检查DF05下所有EF文件的读权限；
   3) 检查DF05下所有EF文件的写权限。
d) 通过标准：DF05下的所有EF文件的读权限和写权限满足规范LD/T 32.6要求。

8.7 DF07_SAFETY

DF07_SAFETY的测试方法如下。

a) 测试目的：检查 DF07 下的所有 EF 文件的读写权限是否满足规范 LD/T 32.6 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) 检查 DF07 下所有 EF 文件的读权限；
   3) 检查 DF07 下所有 EF 文件的写权限。
d) 通过标准：DF07 下的所有 EF 文件的读权限和写权限满足规范 LD/T 32.6 要求。

9 密钥多版本测试

9.1 KEY_VER_1

KEY_VER_1的测试方法如下。

a) 测试目的：检查 SSSE 下第一组密钥中所有国家级密钥是否认证通过、内部认证是否通过。
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) SSSE 下第一组密钥中所有国家级密钥进行外部认证；
   3) 进行内部认证。
d) 通过标准：SSSE 下第一组密钥中所有国家级密钥认证通过、内部认证通过。

9.2 KEY_VER_2

KEY_VER_2的测试方法如下。

a) 测试目的：检查 SSSE 下第二组密钥中所有国家级密钥是否认证通过、内部认证是否通过。
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) SSSE 下第二组密钥中所有国家级密钥进行外部认证；
   3) 进行内部认证。
d) 通过标准：SSSE 下第二组密钥中所有国家级密钥认证通过、内部认证通过。

9.3 KEY_VER_3

KEY_VER_3的测试方法如下。

a) 测试目的：检查 SSSE 下第三组密钥中所有国家级密钥是否认证通过、内部认证是否通过。
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) SSSE 下第三组密钥中所有国家级密钥进行外部认证；
   3) 进行内部认证。
d) 通过标准：SSSE 下第三组密钥中所有国家级密钥认证通过、内部认证通过。

10 非对称认证应用测试

10.1 ACSE_RECORD

ACSE_RECORD的测试方法如下。

a) 测试目的：检查 ACSE 下的所有文件的数据项是否满足规范要求。
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) 读取 ACSE 下的所有文件的数据项；
3) 检查数据项是否满足规范要求。

d) 通过标准：ACSE 下的所有文件的数据项满足规范要求。

10.2 ACSE_SAFETY

ACSE_SAFETY的测试方法如下。

a) 测试目的：检查 ACSE 下的所有文件的读写权限是否满足规范要求。
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) 检查 ACSE 下的所有文件的读权限；
3) 检查 ACSE 下的所有文件的写权限。
d) 通过标准：ACSE 下的所有文件的读写权限满足规范要求。

10.3 CHECK_CERT

CHECK_CERT的测试方法如下。

a) 测试目的：检查证书签名和验签是否正常。
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) 用证书进行签名；
3) 用证书进行验签。
d) 通过标准：证书签名和验签正常。

11 测试项目的划分

11.1 社会保障卡 1.0 版本和 2.0 版本

包括上述5、6、7、8章节的测试内容，且仅有接触部分的测试项目。

11.2 社会保障卡 3.0 版本

包括上述5、6、7、8、9章节的测试内容，接触部分和非接触部分均需进行全部项目的测试。

参 考 文 献

[1] GB/T 2260—2007 中华人民共和国行政区划代码
[2] GB/T 2261.1—2003 个人基本信息分类与代码第1部分：人的性别代码
[3] GB/T 6864—2003 中华人民共和国学位代码
[4] GB/T 7408—2005 数据元和交换格式信息交换日期和时间表示法
[5] GB/T 8561—2001 专业技术职务代码
[6] GB/T 8563.2—2005 奖励、纪律处分信息分类与代码第2部分：荣誉称号和荣誉奖章代码
[7] GB 11643—1999 公民身份号码
[8] GB 11714—1997 全国组织机构代码编制规则
[9] GB/T 16649.4—2010 识别卡 集成电路卡 第4部分：用于交换的结构、安全和命令
[10] GB/T 16835—1997 高等学校本科、专科专业名称代码
[11] JR/T 0025—2018 中国金融集成电路（IC）卡规范
[12] LD/T 92—2013 社会保险管理信息系统指标集与代码
[13] 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）
[14] 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）
[15] 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）
[16] 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）