ICS 35.240.15

L 64

|  |
| --- |
|  备案号： |

DB11

北京市地方标准

DB11/T 159.5—20xx

|  |
| --- |
| 代替DB11/T 159.5—2015 |

市政交通一卡通技术规范第5部分：检测

Municipal administration & communication card technology specifications——Part 5:Test

|  |
| --- |
|  |
|  |

北京市市场监督管理局   发布

20XX - XX - XX发布

20XX - XX - XX实施

目  次

前言 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 2

5 卡片检测 2

5.1 卡片检测要求 2

5.1.1 物理检测 3

5.1.2 安全检测 4

5.1.3 应用检测 5

5.2 卡片验收规则 6

6 终端检测 7

6.1 终端检测要求 7

6.1.1 硬件检测 7

6.1.1.1 终端硬件通用 7

6.1.1.2 终端硬件专用检测 8

6.1.2 安全检测 10

6.1.2.1 通用安全检测 10

6.1.2.2 交易安全检测 11

6.1.3 应用检测 12

6.1.3.1 终端通用应用检测 12

6.1.3.2 联机终端应用检测 13

6.1.3.3 脱机终端应用检测 15

6.1.3.4 互联网终端应用检测 16

6.2 终端验收 17

7 系统检测 17

7.1 安全检测要求 17

7.2 数据质量检测 21

8 移动支付检测 23

8.1 可信服务管理系统测试 23

8.2 安全单元测试 23

8.2.1 安全芯片检测 23

8.2.2 SE嵌入式软件功能测试 23

8.2.3 SE嵌入式软件安全检测 24

8.2.4 非接触电气特性和传输协议检测 24

8.2.5 SE安全和应用检测 24

8.3 客户端软件测试 24

8.3.1 功能测试 24

8.3.2 安全测试 27

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DB11/T 159《市政交通一卡通技术规范》的第5部分。DB11/T 159已经发布了以下部分：

——第1部分：总则；

——第2部分：卡片；

——第3部分：终端；

——第4部分：安全；

——第5部分：检测；

——第6部分：移动支付。

本文件代替DB11/T 159.5—2015《市政交通一卡通技术规范 第5部分：检测》，与DB11/T 159.5—2015相比，除结构调整和编辑性改动外，主要技术变化如下：

1. 增加了卡片典型交易时间的测试方法（见5.1.3）；
2. 增加了二维码摄像头的相关检测内容（见6.1.1.2）；
3. 增加了终端检测的“算法切换”测试内容描述（见6.1.3.1）；
4. 增加了移动支付检测的相关内容（见8）。

本文件由北京市交通委员会提出并归口。

本文件由北京市交通委员会组织实施。

本文件主要起草单位：北京市政交通一卡通有限公司、北京市智慧交通发展中心。

本文件主要起草人员：

本文件及其所代替文件的历次版本发布情况为：

——2015年首次发布为DB11/T 159.5—2015《市政交通一卡通技术规范 第5部分：检测》；

——本次为第一次修订。

市政交通一卡通技术规范

第5部分：检测

1. 范围

本文件规定了市政交通一卡通系统检测的技术要求，包括卡片检测、终端检测、系统检测、移动支付检测的要求。

本文件适用于市政交通一卡通卡片、终端、系统、移动支付的检测及验收工作。

1. 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，仅所注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 2423.1 环境试验 第2部分: 试验方法 试验A：低温

GB/T 2423.2 环境试验 第2部分: 试验方法 试验B：高温

GB/T 2423.3 环境试验 第2部分：试验方法 试验Cab：恒定湿热试验

GB/T 2423.5 环境试验 第2部分：试验方法 试验Ea和导则：冲击

GB/T 2423.10 环境试验 第2部分: 试验方法 试验Fc：振动(正弦)

GB 4943.1 信息技术设备的安全 第一部分：通用要求

GB 9254.2 信息技术设备、多媒体设备和接收机 电磁兼容 第2部分：抗扰度要求

GB/T 14916 识别卡 物理特性

GB/T 18239 集成电路(IC)卡读写机通用规范

GB/T 22351.1 识别卡 无触点的集成电路卡 邻近式卡 第1部分：物理特性

GB/T 22351.2 识别卡 无触点的集成电路卡 邻近式卡 第2部分：空中接口和初始化

JT/T 978.5 城市公共交通IC卡技术规范 第五部分：非接触接口通信

JT/T 1059.8交通一卡通移动支付技术规范 第8部分：检测项目

JT/T 1179 交通一卡通二维码支付技术规范

JT/T 1356 城市公共交通IC卡检测规范

DB11/T 159.1 市政交通一卡通技术规范 第1部分：总则

DB11/T 159.2 市政交通一卡通技术规范 第2部分：卡片

DB11/T 159.3 市政交通一卡通技术规范 第3部分：终端

DB11/T 159.4 市政交通一卡通技术规范 第4部分：安全

DB11/T 159.6 市政交通一卡通技术规范 第6部分：移动支付

1. 术语和定义

DB11/T 159.1界定的以及下列术语和定义适用于本文件。

* 1.

个人化 personalization

SE发行者职责的最后流程，通过该流程配置SE、装载安全参数和设置密钥。个人化流程结束后，SE就可以完全操作并可发到最终用户手中。

[来源：JT/T 1059.8—2016,3.16]

* 1.

卡片典型交易时间 currently transaction time

完成一次正常消费交易的卡片处理时间，这个时间是从终端寻卡成功，到终端接收到卡片返回的最后一条指令为止，包括卡片密钥计算、电子钱包消费、复合应用消费、读写卡片信息等与卡片交互的时间，不包括其他非卡片处理时间。

* 1.

安全域 security domain

负责对某个SE外实体（例如SE发行方、应用提供方、授权管理者）的管理、安全、通信需求进行支持的SE内实体。

[来源：JT/T 1059.1—2016,3.14]

* 1.

客户端 client

用于提供用户接口界面，与SE配合实现SE管理及应用管理功能的应用软件。

[来源：JT/T 1059.6—2016,3.1]

1. 缩略语

DB11/T 159.1界定的以及下列缩略语适用于本文件。

HALT：Type A PICC暂停命令（HLTA Command，Type A）

P1：参数1

P2：参数2

PIN：个人识别码（Personal Identification Number）

REQA：Type A的请求命令（Request Command, Type A）

RATS：Type A的选择应答请求（Request Command, Type A）

PPS：协议和参数选择

SE-TSM：SE发行方可信服务管理系统（SE Issuer Trusted Service Management）

SP-TSM：应用提供方可信服务管理平台（Service Provider Trusted Service Management）

TAC：交易验证码（Transaction Authorization Code）

TSD：交通一卡通辅助安全域（Transport Security Domain）

WUPA：Type A的PICC唤醒命令（Wake-UP Command，Type A）

1. 卡片检测
	1. 卡片检测要求
		1. 物理检测

应对卡片物理特性进行检测，卡片通用物理检测见表1。

1. 卡片通用物理检测

| 序号 | 检测项 | 检测要求 | 检测结论 |
| --- | --- | --- | --- |
|  | 动态弯曲特性 | 应符合GB/T 22351.1中的相关要求 | 通过/不通过 |
|  | 紫外线 | 应符合GB/T 22351.1中的相关要求 |
|  | 静电 | 应符合GB/T 22351.1中的相关要求 |
|  | 静磁场 | 应符合GB/T 22351.1中的相关要求 |
|  | 交变磁场 | 应符合GB/T 22351.1中的相关要求 |
|  | 交变电场 | 应符合GB/T 22351.1中的相关要求 |
|  | 卡的工作频率 | 应符合DB11/T 159.2中的相关要求 |
|  | 通讯速率 | 应符合DB11/T 159.2中的相关要求 |
|  | 负载调制 | 应符合GB/T 22351.2中的相关要求 |
|  | 温度稳定性 | 应符合GB/T 14916中的相关要求 |
|  | 湿度 | 应符合GB/T 14916中的相关要求 |
|  | 卡的翘曲 | 应符合GB/T 14916中的相关要求 |
|  | 抗弯曲强度 | 应符合GB/T 22351.1中的相关要求 |
|  | X-射线 | 应符合GB/T 22351.1中的相关要求 |

卡片专用物理检测见表2。

1. 卡片专用物理检测

| 序号 | 检测项 | 测试步骤 | 检测要求 | 检测结论 |
| --- | --- | --- | --- | --- |
|  | 读写距离 | 1. 确认样卡功能正常
2. 检查设备状态并确认状态设置正常
3. 将样卡放入测试设备中，启动设备进行检测
4. 对游标卡尺测量的读写距离进行判断、记录
 | 应符合DB11/T 159.2中的相关要求 | 通过/不通过 |
|  | 动态扭曲特性 | 1. 确认样卡功能正常
2. 检查设备状态并确认状态设置正常
3. 将样卡放入测试设备中，启动设备进行检测
4. 对输出的长边弯曲检测结果进行判断、记录
5. 对输出的宽边弯曲检测结果进行判断、记录
6. 对输出的扭曲检测结果进行判断、记录
 | 应符合DB11/T 159.2中的相关要求 | 通过/不通过 |
|  | 卡的尺寸 | 1. 确认样卡功能正常
2. 检查设备状态并确认状态设置正常
3. 将样卡放入测试设备中，启动设备进行检测
4. 对游标卡尺测量的卡片尺寸进行判断、记录
 | 应符合GB/T 14916中的相关要求 | 通过/不通过 |
|  | 表面外形 | 1. 确认样卡功能正常
2. 检查设备状态并确认状态设置正常
3. 将样卡放入测试设备中，启动设备进行检测
4. 目测卡片外形，对目测结果进行判断、记录
 | 应符合DB11/T 159.2中的相关要求 | 通过/不通过 |

* + 1. 安全检测

应对卡片安全进行检测，卡片安全检测见表3。

1. 卡片通用安全检测

| 序号 | 检测项 | 测试步骤 | 检测要求 | 检测结论 |
| --- | --- | --- | --- | --- |
| 1 | 卡片随机数检查 | 1. 确认样卡功能正常
2. 检查设备状态并确认状态设置正常
3. 将样卡放入测试设备中，启动设备进行检测
4. 对输出的4字节随机数重复频率检验结果进行判断、记录
5. 对输出的8字节随机数重复频率检验结果进行判断、记录
 | 应符合DB11/T 159.4中的相关要求 | 通过/不通过 |
| 2 | 卡片加密算法检测 | 1. 确认样卡功能正常
2. 检查设备状态并确认状态设置正常
3. 将样卡放入测试设备中，启动设备进行检测
4. 对输出的加密密文检验结果进行判断、记录
5. 对输出的解密明文检验结果进行判断、记录
6. 对输出的鉴别码检验结果进行判断、记录
7. 对输出的签名检验结果进行判断、记录
8. 对输出的摘要检验结果进行判断、记录
 | 应符合DB11/T 159.4中的相关要求 | 通过/不通过 |
| 3 | 卡片文件权限检测 | 1. 确认样卡功能正常
2. 检查设备状态并确认状态设置正常
3. 将样卡放入测试设备中，启动设备进行检测
4. 对输出的文件读取信息检测结果进行判断、记录
5. 对输出的文件不认证写信息检验结果进行判断、记录
6. 对输出的文件认证写信息检验结果进行判断、记录
 | 应符合DB11/T 159.4中的相关要求 | 通过/不通过 |
| 4 | 卡片NVM安全域检测 | 1. 确认样卡功能正常
2. 检查设备状态并确认状态设置正常
3. 将样卡放入测试设备中，启动设备进行检测
4. 对输出的NVM安全域读取检验结果进行判断、记录
5. 对输出的NVM安全域不认证写检验结果进行判断、记录
6. 对输出的NVM安全域认证写检验结果进行判断、记录
 | 应符合DB11/T 159.2中的相关要求 | 通过/不通过 |

* + 1. 应用检测

续表3 卡片通用安全检测

卡片初始化成功后，应对应用进行检测，卡片应用检测见表4。

1. 卡片应用检测

| 序号 | 检测项 | 测试步骤 | 检测要求 | 检测结论 |
| --- | --- | --- | --- | --- |
| 1 | ATQA返回值检测 | 1. 确认样卡功能正常
2. 检查设备状态并确认状态设置正常
3. 将样卡放入测试设备中，启动设备进行检测
4. 对输出的ATQA返回值检测结果进行判断、记录
 | 应符合DB11/T 159.2中的相关要求 | 通过/不通过 |
| 2 | ATQA响应时间检测 | 1. 确认样卡功能正常
2. 检查设备状态并确认状态设置正常
3. 将样卡放入测试设备中，启动设备进行检测
4. 分析抓取波形，计算REQA与ATQA之间的时间差
5. 对计算结果进行判断、记录
 | 应符合DB11/T 159.2中的相关要求 | 通过/不通过 |
| 3 | 算法切换检测 | 1. 确认样卡功能正常
2. 检查设备状态并确认状态设置正常
3. 将样卡放入测试设备中，启动设备进行检测
4. 对输出的获取当前密钥组执行结果进行判断、记录
5. 对输出的选择当前密钥组执行结果进行判断、记录
6. 对输出的设置默认密钥组执行结果进行判断、记录
7. 对输出的锁定密钥组执行结果进行判断、记录
 | 应符合DB11/T 159.2中的相关要求 | 通过/不通过 |
| 4 | 初始化及防冲撞检测 | 1. 确认样卡功能正常
2. 检查设备状态并确认状态设置正常
3. 将样卡放入测试设备中，启动设备进行检测
4. 对输出的卡片REQA、WUPA执行情况进行判断、记录
5. 对输出的卡片 Anticollision and Select 执行情况进行判断、记录
 | 应符合JT/T 978.5中的相关要求 | 通过/不通过 |
| 5 | 通信协议 | 1. 确认样卡功能正常
2. 检查设备状态并确认状态设置正常
3. 将养卡放入测试设备中，启动设备进行检查
4. 对卡片的Type A的协议激活的执行情况进行判断，记录
5. 对卡片的RATS、PPS等指令执行情况进行判断、记录
6. 对协议停活指令 HALT 执行情况进行判断、记录
 | 应符合JT/T 978.5中的相关要求 | 通过/不通过 |
| 6 | 卡片操作系统指令检测 | 1. 确认样卡功能正常
2. 检查设备状态并确认状态设置正常
3. 将样卡放入测试设备中，启动设备进行检测
4. 对输出的命令扫描结果进行判断、记录
 | 应符合DB11/T 159.2中的相关要求 | 通过/不通过 |
| 7 | 卡片操作系统命令参数检测 | 1. 确认样卡功能正常
2. 检查设备状态并确认状态设置正常
3. 将样卡放入测试设备中，启动设备进行检测
4. 对输出的P1/P2参数扫描结果进行判断、记录
 | 应符合DB11/T 159.2中的相关要求 | 通过/不通过 |
| 8 | 一般功能检测 | 1. 确认样卡功能正常
2. 检查设备状态并确认状态设置正常
3. 将样卡放入测试设备中，启动设备进行检测
4. 对输出的一般消费执行结果进行判断、记录
5. 对输出的复合应用消费执行结果进行判断、记录
6. 对输出的一般充值执行结果进行判断、记录
7. 对输出的文件读写执行结果进行判断、记录
8. 对输出的应用锁定、解锁执行结果进行判断、记录
9. 对输出的PIN码重装、修改、解锁执行结果进行判断、记录
 | 应符合DB11/T 159.2中的相关要求 | 通过/不通过 |
| 9 | 卡片容量检测 | 1. 确认样卡功能正常
2. 检查设备状态并确认状态设置正常
3. 将样卡放入测试设备中，启动设备进行检测
4. 对输出的卡片容量大小进行判断、记录
 | 应符合DB11/T 159.2中的相关要求 | 通过/不通过 |
| 10 | 卡片应用文件结构检测 | 1. 确认样卡功能正常
2. 检查设备状态并确认状态设置正常
3. 将样卡放入测试设备中，启动设备进行检测
4. 对输出的文件选择、读取结果进行判断、记录
 | 应符合DB11/T 159.2中的相关要求 | 通过/不通过 |
| 11 | 卡片典型交易时间测试 | 1. 确认样卡功能正常
2. 检查设备状态并确认状态设置正常
3. 将样卡放入测试设备中，启动设备进行检测
4. 获取波形，以发送REQA或WUPA指令波形的前沿为时间的起点，以交易结束最后一条卡片返回的指令波形的后沿为时间的终点，计算包括卡片密钥计算、电子钱包消费、复合应用消费、读写信息等与卡片交互的时间并记录
5. 获取10组波形，计算交易时间平均值，作为卡片典型交易时间
6. 对计算结果进行判断、记录
 | 应符合DB11/T 159.2中的相关要求 | 通过/不通过 |

* 1. 卡片验收规则

卡片按交货的批次不同执行分批抽检，合格判定方式如下：

1. 每批按照批次总数的1‰进行抽检，单次抽检总量不超过100张，100%通过视为合格，否则 为不合格；
2. 若一次抽样结果为不合格，则再次按照批次总数的3‰进行抽样，单次抽检总量不超过300张，100%通过视为合格，否则为不合格；
3. 若连续两次检验仍不合格，则判定该批卡为不合格。
4. 终端检测
	1. 终端检测要求
		1. 硬件检测
			1. 终端硬件通用

终端硬件通用检测见表5。

1. 终端硬件通用检测

| 序号 | 检测项 | 检测要求 | 检测结论 |
| --- | --- | --- | --- |
|  | 机械环境适应性试验 | 振动适应性 | 测试方法应符合GB/T 2423.10中的相关要求；技术指标应符合DB11/T 159.3中的相关要求 | 通过/不通过 |
|  | 冲击适应性 | 测试方法应符合GB/T 2423.5中的相关要求；技术指标应符合DB11/T 159.3中的相关要求 | 通过/不通过 |
|  | 气候环境适应性试验 | 工作温度下限检测 | 测试方法应符合GB/T 2423.1中的相关要求；技术指标应符合DB11/T 159.3中的相关要求 | 通过/不通过 |
|  | 贮存温度下限检测 | 测试方法应符合GB/T 2423.1中的相关要求；技术指标应符合DB11/T 159.3中的相关要求 | 通过/不通过 |
|  | 工作温度上限检测 | 测试方法应符合GB/T 2423.2中的相关要求；技术指标应符合DB11/T 159.3中的相关要求 | 通过/不通过 |
|  | 贮存温度上限检测 | 测试方法应符合GB/T 2423.2中的相关要求；技术指标符合DB11/T 159.3中的相关要求 | 通过/不通过 |
|  | 工作条件下的恒定湿热检测 | 测试方法应符合GB/T 2423.3中的相关要求；技术指标符合DB11/T 159.3中的相关要求 | 通过/不通过 |
|  | 贮存运输条件下的恒定湿热检测 |
|  | 电源适应能力 | 对直流样品电源适应性检测 | 应符合DB11/T 159.3中的相关要求 | 通过/不通过 |
|  | 对交流样品电源适应性检测 |
|  | 安全试验 | 对地泄露电流检测 | 应符合GB 4943.1中的相关要求 | 通过/不通过 |
|  | 抗电强度检测 | 应符合GB 4943.1中的相关要求 | 通过/不通过 |
|  | 保护接地措施检测 | 应符合GB 4943.1中的相关要求 | 通过/不通过 |
|  | 电磁兼容性试验 | 辐射骚扰检测 | 应符合GB 9254.2中的相关要求 | 通过/不通过 |
|  | 电源端子传导骚扰检测 | 应符合GB 9254.2中的相关要求 | 通过/不通过 |
|  | 静电放电抗扰度检测 | 应符合GB 9254.2中的相关要求 | 通过/不通过 |
|  | 射频电磁场辐射抗扰度检测 | 应符合GB 9254.2中的相关要求 | 通过/不通过 |
|  | 电快速瞬变脉冲群抗扰度检测 | 应符合GB 9254.2中的相关要求 | 通过/不通过 |
|  | 浪涌（冲击）抗扰度检测 | 应符合GB 9254.2中的相关要求 | 通过/不通过 |
|  | 射频场感应的传导骚扰抗扰度检测 | 应符合GB 9254.2中的相关要求 | 通过/不通过 |
|  | 工频磁场抗扰度检测 | 应符合GB 9254.2中的相关要求 | 通过/不通过 |
|  | 电压暂降、短时中断和电压变化抗扰度检测 | 应符合GB 9254.2中的相关要求 | 通过/不通过 |

* + - 1. 终端硬件专用检测

终端硬件专用检测见表6。

1. 终端硬件专用检测

| 序号 | 检测项 | 测试步骤 | 检测要求 | 检测结论 |
| --- | --- | --- | --- | --- |
|  | 外观和结构检测 | 由检测人员目测或监测仪器检测 | 应符合DB11/T 159.3中的相关要求 | 通过/不通过 |
|  | 可靠性试验 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 对显示器、SAM卡、通讯接口、非易失性存储器、电源、时钟、蜂鸣器、键盘、打印、摄像头、等进行检测，是否正常运行
4. 对正常业务刷卡进行检测，是否正常运行
 | 在每批次测试过程中，每出现一次异常，记入一次相关失效；应符合DB11/T 159.3中的相关要求 | 通过/不通过 |
|  | 非接触电气特性和通讯协议 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 设备正常开机
4. 对终端的非接触电气特性和通信协议进行测试
 | 测试方法应符合JT/T 1356.4中的相关要求；技术指标应符合DB11/T 159.3中的相关要求 | 通过/不通过 |
|  | 硬件接口检测 | 通讯接口检查 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 设备正常开机
4. 根据样机的可提供的通讯方式，进行数据交互检查，检查是否可以传输数据
 | 应符合DB11/T 159.3中的相关要求 | 通过/不通过 |
|  | 界面接口检查 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 设备正常开机
4. 采用目测和计时方式进行验证，检查界面、声音、时钟
 | 应符合DB11/T 159.3中的相关要求 | 通过/不通过 |
|  | 与SAM接口检查 | 1. 确认样机测试程序正常
2. 依次装入不同等级速率的SAM卡到样机
3. 设备正常开机，运行，记录其运行状况
 | 应符合DB11/T 159.3中的相关要求 | 通过/不通过 |
| **注**：故障判断应符合GB/T 18239中的相关要求 |

二维码摄像头性能检测要求见表7。

1. 二维码摄像头性能检测

| 序号 | 检测项 | 测试步骤 | 检测要求 | 检测结论 |
| --- | --- | --- | --- | --- |
| 1 | 识读正确率（亮度变化、容错率7%、重复码） | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 生成不同亮度、容错率为7%等情况的二维码，用二维码摄像头读取生成的二维码，查看二维码摄像头读取的结果信息。
4. 根据结果检测各种情况下均可准确识读
 | 应符合JT/T 1179中的相关要求 | 通过/不通过 |
| 2 | 运动容差 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 设置二维码显示设备与摄像头以大于等于15cm/s相对速度移动, 终端二维码摄像头识读二维码，连续识读10次
4. 根据结果，二维码摄像头在被扫描二维码移动时，应能够准确识别二维码信息，识读成功率不低于90%
 | 应符合JT/T 1179中的相关要求 | 通过/不通过 |
| 3 | 识读精度 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 使用不同型号、不同分辨率的手机生成不同精度的二维码，用二维码摄像头读取二维码信息。
4. 针对不同型号生成不同分辨率的二维码，二维码摄像头都能准确识读
 | 应符合JT/T 1179中的相关要求 | 通过/不通过 |
| 4 | 识读角度 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 设置二维码显示设备与摄像头成不同倾角（平行读头360°旋转，上下偏转±45°，左右偏转±45°，用二维码摄像头识读二维码信息
4. 针对二维码显示设备与摄像头成不同倾角，二维码摄像头都能准确识读二维码信息
 | 应符合JT/T 1179中的相关要求 | 通过/不通过 |
| 5 | 识读距离 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 设置二维码显示设备与摄像头不同距离（距离设定从1cm开始每2cm递增，递增至10cm），用二维码摄像头识读二维码信息
4. 二维码摄像头对不同距离的二维码都能准确识读。
 | 应符合JT/T 1179中的相关要求 | 通过/不通过 |

* + 1. 安全检测
			1. 通用安全检测

终端通用安全检测见表8。

1. 终端通用安全检测

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 检测项 | 测试步骤 | 检测要求 | 检测结论 |
| 1 | 数据安全检测 | 1. 确认样机工作正常
2. 检查设备状态并确认状态设置正常
3. 设备正常开机进入业务界面
4. 对设备根据实际不同卡片业务，执行单笔正常业务操作，检查交易数据的完整性，和实际业务保存数据是否一致
5. 对设备根据实际不同卡片业务，执行批量正常业务操作，检查交易数据的完整性，和实际业务保存数据（如交易时间、交易类型、交易金额、交易站点信息等）是否一致
6. 对终端在异常掉电后，检查交易数据是否可以改变或丢失
7. 对终端在下载中心系统的参数文件后，检查参数文件信息的完整性和一致性
8. 对终端的传输加密密钥的使用方式进行检测，是否可靠，在签退之后是否失效
9. 对测试结果进行判断、记录
 | 应符合DB11/T 159.4中的相关要求 | 通过/不通过 |
| 2 | 设备安全检测 | 1. 确认样机工作正常
2. 样机硬件模块拆卸后，再安装，验证其是否仍可正常工作
3. 对需要签名的终端程序，进行非签名程序的安装，验证其是否仍可正常工作
4. 对终端开机后，检查其默认的初始化数据和参数文件信息，是否被篡改，是否可以正常保留
5. 对终端的接口进行检查，是否存在正常使用程序外，可以另下载一个程序，对正常程序的数据进行篡改
6. 对密码输入数据，是否在专门设备上采集，检查终端密码输入方式
7. 对测试结果进行判断、记录
 | 应符合DB11/T 159.4中的相关要求 | 通过/不通过 |
| 3 | 数据存储安全检测 | 1. 确认样机工作正常
2. 样机硬件模块拆卸后，再安装，验证其是否仍可正常工作
3. 对终端采集或存储的关键信息进行加密存储安全的检测
4. 对终端采集的数据保护进行测试，是否存在入侵设备、安装附加物、替代或修改数据的方式修改或提取生关键信息
 | 应符合DB11/T 159.4中的相关要求 | 通过/不通过 |

* + - 1. 交易安全检测

终端交易安全检测见表9。

1. 终端交易安全检测

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 检测项 | 测试步骤 | 检测要求 | 检测结论 |
| 1 | 消费类交易检测 | 1. 确认样机工作正常
2. 检查设备状态并确认状态设置正常
3. 按照试验设备的操作规定，设备正常启动
4. 采用SAM卡，对卡片执行业务操作，完成卡片的验证，卡片内文件执行情况与实际情况对比一致
5. 对卡片交易过程中卡片合法性检查
6. 对卡片交易过程中业务参数检查
7. 对联机交易模式检查其上送的数据报文符合报文安全机制
8. 对联机交易模式检查中心计算机系统的参数，验证终端根据其反馈进行判断处理情况
9. 检查交易数据报文应包括TAC
10. 终端保持交易数据的完整性，断电不丢失
11. 对测试结果进行判断、记录
 | 应符合DB11/T 159.4中的相关要求 | 通过/不通过 |
| 2 | 充值类交易检测 | 应符合DB11/T 159.4中的相关要求 | 通过/不通过 |
| 3 | 退卡类交易检测 | 应符合DB11/T 159.4中的相关要求 | 通过/不通过 |

* + 1. 应用检测
			1. 终端通用应用检测

终端通用应用检测见表10。

1. 终端通用应用检测

| 序号 | 检测项 | 测试步骤 | 检测要求 | 检测结论 |
| --- | --- | --- | --- | --- |
| 1 | 终端防冲突检测 | 1. 确认样机工作正常
2. 检查设备状态并确认状态设置正常
3. 按照试验设备的操作规定，设备正常启动后，根据终端实际应用，在各类卡业务的交易过程中放入多张卡片（2~3张），目测是否有错误提示或可以正常做交易
4. 对测试结果进行判断、记录
 | 交易过程中感应区存在多卡，应拒绝交易 | 通过/不通过 |
| 2 | 异常中断恢复检测 | 1. 确认样机工作正常
2. 检查设备状态并确认状态设置正常
3. 按照试验设备的操作规定，设备正常启动后，在交易过程中提前移走卡片，检测终端在交易中断及恢复的情况下应能够继续交易，数据应正确无误
4. 对测试结果进行判断、记录
 | 应符合DB11/T 159.3中的相关要求 | 通过/不通过 |
| 3 | 卡片识别及读写测试 | 1. 确认样机工作正常
2. 检查设备状态并确认状态设置正常
3. 按照试验设备的操作规定，设备正常启动后，在终端上刷系统认可的各种物理及逻辑类型卡片，进行交易测试
4. 对终端识别卡类型后的各过程区及必要文件读写进行测试
5. 对测试结果进行判断、记录
 | 应符合DB11/T 159.3中的相关要求 | 通过/不通过 |
| 4 | 卡片通用合法性的检测 | 1. 确认样机工作正常
2. 检查设备状态并确认状态设置正常，并正常开机
3. 更改卡片结构信息，对不同的卡状态、黑名单卡、过期卡等，检测终端应用对卡内信息合法性检查
4. 对测试结果进行判断、记录
 | 应符合DB11/T 159.3中的相关要求 | 通过/不通过 |
| 5 | 软件代码检测 | 1. 查看源代码，检查人员对关键业务处理环节进行逻辑判断并记录
2. 根据源代码和开发平台，检查人员对程序进行编译，并记录编译结果
 | 应符合DB11/T 159.3中的相关要求 | 通过/不通过 |
| 6 | 人机界面检测 | 1. 确认样机工作正常
2. 检查设备状态并确认状态设置正常
3. 样机开机，通过目测检查其界面菜单显示和实际业务是否一致，并能够执行正常交易
4. 对测试结果（菜单项、交易过程声音提示等）进行判断、记录
 | 应符合DB11/T 159.3中的相关要求 | 通过/不通过 |
| 7 | 程序升级 | 1. 通过手工，在样机的下载软件上，执行正常软件下载，并观察程序是否可以正常运行，记录其下载结果
2. 通过远程下载系统，执行正常软件下载，并观察程序是否可以正常运行，记录其下载结果
 | 应符合DB11/T 159.3中的相关要求 | 通过/不通过 |
| 8 | 算法切换 | 1. 确认样机工作正常
2. 检查设备状态并确认状态设置正常
3. 样机开机，通过发送算法切换指令，将卡片切换到不通的密钥体系
4. 通过不通密钥体系的卡片
5. 终端使用切换后的密钥体系对卡片进行交易验证测试
6. 对测试结果进行判断、记录
 | 应符合DB11/T 159.4中的相关要求 | 通过/不通过 |

* + - 1. 联机终端应用检测

续表9 终端通用应用检测

1. 9终端通用应用检测

联机终端应用检测要求见表11。

1. 联机终端应用检测

| 序号 | 检测项 | 测试步骤 | 检测要求 | 检测结论 |
| --- | --- | --- | --- | --- |
| 1 | 终端业务配置信息 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 设备的管理功能进入设置终端业务配置信息（如商户号、终端号）
 | 在系统后台，已维护的终端业务信息可以正常作业务，未维护的不可以正常做业务 | 通过/不通过 |
| 2 | 系统管理 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 设备开机检查
4. 设备参数管理检查
5. 设备状态管理检查
 | 应符合DB11/T 159.3中的相关要求 | 通过/不通过 |
| 3 | 操作员管理 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 设备的管理功能进入操作员管理设置
 | 应符合DB11/T 159.3中的相关要求 | 通过/不通过 |
| 4 | 应用管理 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 设备正常开机，并可正常输入操作员
4. 设备进行签到并确认签到成功
5. 进入设备业务界面，执行参数查询、交易查阅、重打印等操作
6. 设备进行签退，并可正常批上送、签退
 | 应符合DB11/T 159.3中的相关要求 | 通过/不通过 |
| 5 | 管理安全要求 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 设备正常开机，并可输入非法操作员或密码，检查执行情况
4. 设备进行签到并确认签到成功，做正常业务，检查是否正常接收系统反馈数据
5. 设备进行签退，签退后检查是否仍可执行正常业务
 | 应符合DB11/T 159.3中的相关要求 | 通过/不通过 |
| 6 | 正常交易业务 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 设备正常开机，进行签到并确认签到成功
4. 设备执行正常业务，检查交易执行情况
 | 应符合DB11/T 159.3中的相关要求 | 通过/不通过 |
| 7 | 卡类型检查 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 设备正常开机，进行签到并确认签到成功
4. 设备执行业务时，检查执行卡业务参数情况
 | 应符合DB11/T 159.3中的相关要求 | 通过/不通过 |
| 8 | 卡有效期检查 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 设备正常开机，进行签到并确认签到成功
4. 设备执行业务时，检查卡有效期的合法性
 | 有效期存储格式应符合正常YYYYMMDD格式，应检查卡有效期是否过期 | 通过/不通过 |
| 9 | 黑名单标识检查 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 设备正常开机，进行签到并确认签到成功
4. 设备执行业务时，检查识别正常卡和黑名单卡情况
 | 黑名单标示为正常的卡可以做交易，标示为黑名单卡提示“黑名单卡”不可继续交易 | 通过/不通过 |
| 10 | 黑名单参数检查 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 设备正常开机，进行签到并确认签到成功
4. 设备执行卡业务时，检查黑名单参数情况
 | 在黑名单参数内的卡执行锁卡，不在黑名单参数内的卡可正常交易 | 通过/不通过 |
| 11 | 交易金额检查 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 设备正常开机，进行签到并确认签到成功
4. 设备执行卡业务时，检查交易金额
 | 应符合DB11/T 159.1中的相关要求  | 通过/不通过 |
| 12 | 卡片应用结构检查 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 设备正常开机，进行签到并确认签到成功
4. 设备执行卡业务时，检查卡内结构处理和业务要求是否一致
 | 应符合DB11/T 159.2中的相关要求 | 通过/不通过 |
| 13 | 系统后台反馈异常 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 设备正常开机，进行签到并确认签到成功
4. 设备执行卡业务时，检查对系统后台响应码处理情况
 | 系统后台响应码为不成功，提示不成功信息，业务中断；响应码为成功，业务继续 | 通过/不通过 |

* + - 1. 脱机终端应用检测

脱机终端应用检测见表12。

1. 脱机终端应用检测

| 序号 | 检测项 | 测试步骤 | 检测要求 | 检测结论 |
| --- | --- | --- | --- | --- |
| 1 | 终端业务配置信息 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 设备的管理功能进入设置终端业务配置信息（如商户号、终端号）
 | 在系统后台，已维护的终端业务信息可以正常作业务，未维护的不可以正常做业务 | 通过/不通过 |
| 2 | 系统管理 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 设备开机检查
4. 设备参数管理检查
5. 设备状态管理检查
 | 应符合DB11/T 159.3中的相关要求 | 通过/不通过 |
| 3 | 操作员管理（条件） | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 设备的管理功能进入操作员管理设置
 | 应符合DB11/T 159.3中的相关要求 | 通过/不通过 |
| 4 | 应用管理 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 设备正常开机，并可正常输入操作员
4. 进入设备业务界面，执行参数查询、交易查阅、重打印等操作
 | 应符合DB11/T 159.3中的相关要求 | 通过/不通过 |
| 5 | 管理安全要求 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 设备正常开机，并可输入非法操作员或密码，检查执行情况
 | 应符合DB11/T 159.3中的相关要求 | 通过/不通过 |
| 6 | 正常交易业务 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 设备正常开机，进入交易正常界面
4. 设备执行正常业务，检查交易执行情况
 | 应符合DB11/T 159.3中的相关要求 | 通过/不通过 |
| 7 | 卡类型检查 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 设备正常开机，进入交易正常界面
4. 设备执行业务时，检查执行卡业务参数情况
 | 应符合DB11/T 159.3中的相关要求 | 通过/不通过 |
| 8 | 卡有效期检查 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 设备正常开机，进入交易正常界面
4. 设备执行业务时，检查卡有效期的合法性
 | 有效期存储格式应符合正常YYYYMMDD格式，应检查卡有效期是否过期 | 通过/不通过 |
| 9 | 黑名单标识检查 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 设备正常开机，进入交易正常界面
4. 设备执行业务时，检查识别正常卡和黑名单卡情况
 | 黑名单标示为正常的卡可以做交易，标示为黑名单卡提示“黑名单卡”不可继续交易 | 通过/不通过 |
| 10 | 黑名单参数检查 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 设备正常开机，进入交易正常界面
4. 设备执行卡业务时，检查黑名单参数情况
 | 在黑名单参数内的卡执行锁卡，不在黑名单参数内的卡可正常交易 | 通过/不通过 |
| 11 | 交易金额检查 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 设备正常开机，进入交易正常界面
4. 设备执行卡业务时，检查交易金额
 | 应符合DB11/T 159.1中的相关要求 | 通过/不通过 |
| 12 | 卡片应用结构检查 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 设备正常开机，进入交易正常界面
4. 设备执行卡业务时，检查卡内结构处理和业务要求是否一致
 | 应符合DB11/T 159.2中的相关要求 | 通过/不通过 |

* + - 1. 互联网终端应用检测

互联网终端应用检测见表13。

1. 互联网终端应用检测

| 序号 | 检测项 | 测试步骤 | 检测要求 | 检测结论 |
| --- | --- | --- | --- | --- |
| 1 | 正常交易业务 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 设备与WEB控件驱动正常
4. 设备执行正常业务，检查交易执行情况
 | 应符合DB11/T 159.3中的相关要求 | 通过/不通过 |
| 2 | 卡片处理 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 设备与WEB控件驱动正常
4. 设备执行卡业务时，检查卡内处理和业务要求的是否一致
 | 应符合DB11/T 159.2中的相关要求 | 通过/不通过 |
| 3 | 系统后台反馈异常 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 设备与WEB控件驱动正常
4. 设备执行卡业务时，检查对系统后台响应码处理情况
 | 系统后台响应码为不成功，提示不成功信息，业务中断；响应码为成功，业务继续 | 通过/不通过 |
| 4 | 业务流程 | 1. 确认样机测试程序正常
2. 检查设备状态并确认状态设置正常
3. 设备与WEB控件驱动正常
4. 设备执行卡业务时，检查业务执行
 | 应符合DB11/T 159.3中的相关要求 | 通过/不通过 |

* 1. 终端验收

终端验收，按交货的批次不同执行分批抽检，其合格判定方式如下：

1. 出具终端的出厂检测报告、操作手册等合格证，同时出具行业主管部门认可的第三方检测报告；
2. 每批按照批次总数的1%进行抽检，单次抽检总量不超过10台，100%通过视为合格，否则为不合格；
3. 若一次抽样结果为不合格，则再次按照批次总数的3%进行抽样，单次抽检总量不超过30台，100%通过视为合格，否则为不合格；
4. 若连续两次检验仍不合格，则判定该批终端不合格。
5. 系统检测
	1. 安全检测要求

系统安全检测见表14。

1. 系统安全检测

| 序号 | 检测项 | 测试步骤 | 检测要求 | 检测结论 |
| --- | --- | --- | --- | --- |
| 1 | 鉴别检测 | 1. 对系统登录界面检测，是否存在单独的登录界面，登录过程存在身份标识和鉴别
2. 对系统登录用户，进行登录号和登录密码双重检测，两者之间完全和系统匹配才可登录系统
3. 对系统的登录用户，关键的登录身份识别信息是唯一的，是否存在重复的，对已开通的登录用户，逐一进行登录检测
4. 系统用户身份登录验证失败后，是否自动结束会话，登录重试次数是否有限制，日重试次数超过限制次后，是否仍允许登录
5. 对测试结果进行判断、记录
 | 应符合DB11/T 159.4中的相关要求 | 通过/不通过 |
| 2 | 访问控制检测 | 1. 对系统登录用户，是否设置有不同的权限级别，不同级别的登录人员可以访问的界面是可配置的
2. 是否只有系统最高级管理员才可以分配不同用户的权限
3. 同一类别的用户级别，其登录操作界面是否一致，同一级别的用户操作权限是否一致
4. 对关键业务执行是否在流程上区分不同的用户执行，以便相互监督
5. 对系统关键业务的执行，是否有双重，同级别或更高级级别用户授权后，才可执行
6. 对测试结果进行判断、记录
 | 应符合DB11/T 159.4中的相关要求 | 通过/不通过 |
| 3 | 操作审计检测 | 1. 检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统，查看当前审计范围是否覆盖到各主要服务器操作系统、重要终端操作系统和主要数据库管理系统，查看审计策略是否覆盖系统内重要的安全相关事件，例如，用户标识与鉴别、自主访问控制的所有操作记录、重要用户行为（如用超级用户命令改变用户身份，删除系统表）、系统资源的异常使用、重要系统命令的使用等
2. 检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统，查看审计记录信息是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源（如末端标识符）、事件的结果等内容
3. 检查主要服务器和重要终端操作系统，查看是否为授权用户浏览和分析审计数据提供专门的审计工具（如对审计记录进行分类、排序、查询、统计、分析和组合查询等），并能根据需要生成审计报表
4. 检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统，查看能否对特定事件指定实时报警方式（如声音、EMAIL、短信等）
5. 检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统，查看审计跟踪设置是否定义了审计跟踪极限的阈值，当存储空间被耗尽时，能否采取必要的保护措施，例如，报警并导出、丢弃未记录的审计信息、暂停审计或覆盖以前的审计记录等
6. 测试主要服务器操作系统、重要终端操作系统和主要数据库管理系统，可通过非法终止审计功能或修改其配置，验证审计功能是否受到保护
7. 测试主要服务器操作系统、重要终端操作系统和主要数据库管理系统，在系统上以某个用户试图产生一些重要的安全相关事件（如鉴别失败等），测试安全审计的覆盖情况和记录情况与要求是否一致
8. 测试主要服务器操作系统、重要终端操作系统和主要数据库管理系统，在系统上以某个系统用户试图删除、修改或覆盖审计记录，测试安全审计的保护情况与要求是否一致
9. 对测试结果进行判断、记录
 | 应符合DB11/T 159.4中的相关要求 | 通过/不通过 |
| 4 | 数据安全检测 | 1. 检查操作系统、网络设备、数据库管理系统的设计/验收文档或相关证明性材料（如证书、检验报告等）等，查看其是否能检测/验证到系统管理数据（如WINDOWS域管理、目录管理数据）、鉴别信息（如用户名和口令）和业务数据在传输过程中完整性受到破坏，是否能检测到系统管理数据、身份鉴别信息和业务数据（如防火墙的访问控制规则）在存储过程中完整性受到破坏，是否能检测到重要系统完整性受到破坏。在检测到完整性错误时应有对采取的必要恢复措施的描述，如果有相关信息，查看其配置是否正确
2. 检查主要应用系统，查看其是否配备检测/验证系统管理数据、鉴别信息和业务数据在传输过程中完整性受到破坏的功能；是否配备检测/验证系统管理数据、身份鉴别信息和业务数据在存储过程中完整性受到破坏的功能；是否配备检测/验证重要系统/模块完整性受到破坏的功能；在检测/验证到完整性错误时能采取必要的恢复措施
3. 检查主要应用系统，查看其是否配备检测系统完整性受到破坏的功能；并在检测到完整性错误时采取必要的恢复措施
4. 检查操作系统、网络设备、数据库管理系统、关键应用系统的设计/验收文档，查看其是否有关于鉴别信息、系统管理数据和业务数据采用加密或其他有效措施实现传输保密性描述，是否有采用加密或其他保护措施实现存储保密性的描述
5. 检查主要应用系统，查看其鉴别信息、系统管理数据和业务数据是否采用加密或其他有效措施实现传输保密性描述，是否采用加密或其他保护措施实现存储保密性
6. 测试主要应用系统，通过用嗅探工具获取系统传输数据包，查看其是否采用了加密或其他有效措施实现传输保密性
7. 对测试结果进行判断、记录
 | 应符合DB11/T 159.4中的相关要求 | 通过/不通过 |
| 5 | 网络与计算环境安全检测 | 网络结构安全 | 1. 检查网络拓扑图，查看其与当前运行情况是否一致
2. 检查网络设计/验收文档，查看是否有边界和主要网络设备能满足基本业务需求，网络接入及核心网络的带宽能满足业务高峰期的需要，是否不存在带宽瓶颈等方面的设计或描述
3. 检查网络设计/验收文档，查看是否有根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网和网段分配地址段的设计或描述
4. 检查边界和主要网络设备，查看是否配置路由控制策略（如使用静态路由等）建立安全的访问路径；
5. 检查边界和主要网络设备，查看重要网段是否采取了网络地址与数据链路地址绑定的措施（如对重要服务器采用IP地址和MAC地址绑定措施）
6. 检查边界和主要网络设备，查看是否有对带宽进行控制的策略（如路由、交换设备上的QOS策略配置情况，专用的带宽管理设备的配置策略等），这些策略能否保证在网络发生拥堵的时候优先保护重要业务（如重要业务的主机的优先级要高于非重要业务的主机）
7. 测试网络拓扑结构，可通过网络拓扑结构自动发现、绘制工具，验证实际的网络拓扑结构和网络拓扑结构图是否一致
8. 测试业务终端与业务服务器之间的访问路径，可通过使用路由跟踪工具（如tracert等工具），验证业务终端与业务服务器之间的访问路径是否安全（如访问路径是否固定等）
9. 测试重要网段，验证其采取的网络地址与数据链路地址绑定措施是否有效（如试图使用非绑定地址，查看是否能正常访问等）
10. 测试网络带宽分配策略，可通过使用带宽测试工具，测试网络带宽分配是否有效
11. 对测试结果进行判断、记录
 | 应符合DB11/T 159.4中的相关要求 | 通过/不通过 |
| 6 | 访问控制安全 | 1. 检查边界网络设备，查看其是否根据会话状态信息（如包括数据包的源地址、目的地址、源端口号、目的端口号、协议、出入的接口、会话序列号、发出信息的主机名等信息，并应支持地址通配符的使用）对数据流进行控制
2. 检查边界网络设备，查看其是否对进出网络的信息内容进行过滤，实现对应用层HTTP、FTP、TELNET、SMTP、POP3等协议命令级的控制
3. 检查边界网络设备，查看是否能设置会话处于非活跃的时间或会话结束后自动终止网络连接；查看是否能设置网络最大流量数及网络连接数
4. 检查主要网络设备，查看是否有访问控制措施（如VLAN，访问控制列表，MAC地址绑定）控制便携式和移动式设备接入网络
5. 测试边界网络设备，可通过试图访问未授权的资源，验证访问控制措施对未授权的访问行为的控制是否有效（如可以使用扫描工具来探测等）
6. 测试主要网络设备，可通过试图用移动设备接入网络，验证网络设备的访问控制策略是否有效
7. 对网络访问控制措施进行渗透测试，可通过采用多种渗透测试技术（如http隧道等），验证网络访问控制措施是否不存在明显的弱点
8. 对测试结果进行判断、记录
 | 应符合DB11/T 159.4中的相关要求 | 通过/不通过 |
| 7 | 系统备份检测 | 1. 检查设计/验收文档，查看其是否有关于操作系统、网络设备、数据库管理系统、应用系统配置有本地系统级热备份和重要信息恢复功能的描述
2. 检查操作系统、网络设备、数据库管理系统、主要应用系统，查看其是否配置有本地/异地备份和重要信息恢复的功能，其配置是否正确
3. 检查重要网络设备、通信线路和服务器是否提供硬件冗余
4. 检查重要业务系统是否配备本地系统级热备份的功能
5. 对测试结果进行判断、记录
 | 应符合DB11/T 159.4中的相关要求 | 通过/不通过 |

* 1. 数据质量检测

系统数据质量检测见表15。

1. 数据质量检测

| 序号 | 检测项 | 测试步骤 | 检测要求 | 检测结论 |
| --- | --- | --- | --- | --- |
| 1 | 数据的准确性 | 1. 通过业务终端发起批量卡片业务（如消费、售卡、充值、退卡等）
2. 在终端层采集的数据记录内的各项数据项和实际业务进行匹配（如交易类型、交易时间、交易金额、网点信息等），检查是否一致
3. 对终端发送到总中心计算机处理的最终的数据记录进行检测，判定其是否和终端产生的交易记录一致
4. 对测试结果进行判断、记录
 | 应符合DB11/T 159.1中的相关要求 | 通过/不通过 |
| 2 | 数据的完整性 | 1. 通过业务终端发起批量卡片业务（如消费、售卡、充值、退卡等）
2. 在终端层采集的数据记录产生汇总数据和明细数据
3. 对终端发送到总中心计算机处理的流经的分中心系统或运营实体系统的汇总数据和明细数据进行检测，判定其是否和终端产生的记录一致，是否发生变异、丢失
4. 对终端发送到总中心计算机处理的最终的汇总数据和明细数据进行检测，判定其是否和终端产生的交易记录一致，是否发生变异、丢失
5. 对测试结果进行判断、记录
 | 在终端产生的交易汇总数据、交易明细，与数据传送到分中心系统或运营实体系统的汇总数据、交易明细，与总中心计算机系统的汇总数据、交易明细应完全一致 | 通过/不通过 |
| 3 | 数据的传输 | 1. 通过业务终端发起批量卡片业务（如消费、售卡、充值、退卡等）
2. 对终端交易数据，通过终端的自身通信方式，按照约定的通信协议，传送到分中心系统或运营实体系统终端，检测在数据传输过程中数据是否丢失
3. 对终端交易数据，通过各级分中心系统或运营实体系统终端，发送到总中心计算机系统，检测在数据传输过程中数据是否丢失
4. 对测试结果进行判断、记录
 | 应符合DB11/T 159.1中的相关要求 | 通过/不通过 |
| 4 | 数据的批量存储 | 1. 通过业务终端发起批量卡片业务（如消费、售卡、充值、退卡等），进行压力测试，压力测试数据量为网点实际最大业务量的120%
2. 对终端批量数据进行检测，其数据存储保持完整性，断电后不丢失，可以存储10天内的交易数据
3. 对终端发送到总中心计算机处理的最终的批量数据记录进行检测，判定其是否和终端产生的交易记录一致
4. 对系统进行压力数据测试，其测试数据达到系统设计能力的110%，验证系统的存储能力和处理能力
5. 对测试结果进行判断、记录
 | 应符合DB11/T 159.3中的相关要求 | 通过/不通过 |

1. 移动支付检测
	1. 可信服务管理系统测试

 可信服务管理系统测试包含功能测试、性能测试、安全测试，检测内容应符合JT/T 1059.8中的相关要求。

* 1. 安全单元测试
		1. 安全芯片检测

安全芯片包括处理器单元、安全算法模块、I/O接口、易失性和非易失性存储器等，整体共同构成了安全芯片安全功能基础。检测内容应符合JT/T 1059.8中的相关要求。

* + 1. SE嵌入式软件功能测试

SE嵌入式软件功能测试见表16。

 表16 SE嵌入式软件功能测试

| 序号 | 检测项 | 测试步骤 | 检测要求 | 检测结论 |
| --- | --- | --- | --- | --- |
| 1 | SE多应用平台规格符合性检测 | SE平台指令检测 | 1. 确认样卡功能正常
2. 检查设备状态并确认状态设置正常
3. 将样卡放入测试设备中，启动设备进行检测
4. 对输出的SE平台指令执行结果进行判断、记录
5. 对全局CVM服务各状态下的状态迁移指令执行结果进行判断、记录
6. 对安全通道的创建指令、SCP02和SCP03支持情况进行测试，执行结果进行判断、
7. 记录
8. 对SE内容管理的文件加载指令执行结果进行判断、记录
9. 对个人化指令执行结果进行判断、记录
10. 正常条件下各项命令的令牌验证是否正常执行，并对结果进行判断、记录
11. 执行迁移操作时令牌的签发者和收条生成者测试，并对结果进行判断、记录
12. 对SE平台的生命周期状态输出的一般充值执行结果进行判断、记录
13. 对SE平台支持的加密算法进行测试，对执行的结果进行判断、记录。
 | 应符合DB11/T 159.6中的相关要求 | 通过/不通过 |
| 2 | 全局CVM服务功能检测 | 通过/不通过 |
| 3 | 安全通道特性功能测试 | 通过/不通过 |
| 4 | SE内容管理 | 通过/不通过 |
| 5 | 个人化 | 通过/不通过 |
| 6 | 令牌验证 | 通过/不通过 |
| 7 | 收条生成 | 通过/不通过 |
| 8 | SE多应用平台规格符合性检测 | 生命周期状态管理 | 通过/不通过 |
| 9 | 加密算法 | 通过/不通过 |
| 10 | TSD功能符合性检测 | TSD特性检测 | 1. 确认样卡功能正常
2. 检查设备状态并确认状态设置正常
3. 将样卡放入测试设备中，启动设备进行检测
4. 对TSD的功能进行测试，执行结果进行判断、记录
 | 应符合DB11/T 159.6中的相关要求 | 通过/不通过 |
| 11 | TSD创建 | 通过/不通过 |
| 12 | TSD的安全域 | 通过/不通过 |

* + 1. SE嵌入式软件安全检测

SE嵌入式软件安全检测要求应符合JT/T 1059.8中的相关要求。

* + 1. 非接触电气特性和传输协议检测

非接触电气特性和通讯协议测试内容应符合DB11/T 159.2中的相关要求，并应保证与读写终端的兼容性。检测内容见5.1.2和5.1.3。

* + 1. SE安全和应用检测

安全和应用检测内容见 5.1.2和5.1.3。

* 1. 客户端软件测试
		1. 功能测试

客户端功能测试见表17。

 表17 功能测试

| 序号 | 检测项 | 测试步骤 | 检测要求 | 检测结论 |
| --- | --- | --- | --- | --- |
| 1 | 开卡 | 1. 确认SE-TSM平台功能正常
2. 确认客户端软件功能正常
3. 客户端请求SE-TSM平台进行SE安全域初始化，并下载应用、安装应用
4. 客户端请求SP-TSM平台应用个人化数据，完成开卡。
5. 将移动支付终端放入到检测设备中，对开出的卡片进行卡基本功能测试，并对结果进行判断、记录
 | 应符合DB11/T 159.6中的相关要求 | 通过/不通过 |
| 2 | 充值 | 1. 确认SE-TSM平台功能正常
2. 确认客户端软件功能正常
3. 客户端已完成开卡
4. 客户端向SP-TSM平台发起充值请求。SP-TSM平台向支付平台确认支付结果，下发卡片充值脚本，完成卡片充值
5. 将移动支付终端放入到检测设备中，对完成充值的卡片进行余额检测，并对结果进行判断、记录
 | 应符合DB11/T 159.6中的相关要求 | 通过/不通过 |
| 3 | 消费 | 1. 确认SE-TSM平台功能正常
2. 确认客户端软件功能正常
3. 客户端已完成开卡
4. 通过终端设备向移动支付终端发起消费交易，完成卡片消费
5. 将移动支付终端放入到检测设备中，对完成消费的卡片进行余额检测，并对结果进行判断、记录
 | 应符合DB11/T 159.6中的相关要求 | 通过/不通过 |
| 4 | 迁卡 | 1. 确认SE-TSM平台功能正常
2. 确认客户端软件功能正常
3. 客户端已完成开卡
4. SE-TSM确认卡片状态，并向SP-TSM请求迁出指令脚本，SP-TSM下发迁出指令脚本，完成迁卡
5. 将移动支付终端放入到检测设备中，对完成迁出的移动支付终端进行测试，确认是否迁出成功，并对结果进行判断、记录
6. SE-TSM确认SE状态，并向SP-TSM请求迁入指令脚本，SP-TSM确认卡片迁入状态，并下发迁入指令脚本，完成迁入
7. 将移动支付终端放入到检测设备中，对完成迁入的卡片进行数据扫描测试，判断迁入的卡片是否与迁出的卡片数据一致，并对结果进行记录
 | 应符合DB11/T 159.6中的相关要求 | 通过/不通过 |
| 5 | 退卡 | 1. 确认SE-TSM平台功能正常
2. 确认客户端软件功能正常
3. 客户端已完成开卡
4. 用户通过移动支付终端发起通用退卡请求到SE-TSM，SE-TSM下发获取退卡指令，完成退卡。
5. 将移动支付终端放入到检测设备中，对完成退卡的卡片进行测试，确认是否完成退卡，并对结果进行判断、记录
 | 应符合DB11/T 159.6中的相关要求 | 通过/不通过 |
| 6 | 用户注册 | 1. 确认SE-TSM平台功能正常
2. 确认客户端软件功能正常
3. 调用用户注册过程，并记录用户注册结果
 | 应符合DB11/T 159.6中的相关要求 | 通过/不通过 |
| 7 | 默认应用设置 | 1. 确认客户端软件功能正常
2. 使用客户端对移动支付终端的SE中的默认应用（支付交易时的默认应用）进行修改设置，并验证设置的结果
 | 应符合DB11/T 159.6中的相关要求 | 通过/不通过 |
| 8 | 信息查询 | 1. 确认SE-TSM平台功能正常
2. 确认客户端软件功能正常
3. 客户端移动支付终端的SE对余额和交易明细等信息进行查询
4. 使用客户端软件进行多次卡信息查询操作，并记录检测结果
 | 应符合DB11/T 159.6中的相关要求 | 通过/不通过 |
| 9 | 密码管理 | 1. 确认SE-TSM平台功能正常
2. 确认客户端软件功能正常
3. 验证密码的使用方式及安全保护机制，验证密码复杂度。
4. 验证修改密码功能，查看客户端是否提示输入原密码，以及原密码是否校验正确性
5. 验证密码找回功能，查看客户端是否可根据用户输入的信息验证通过后重置密码
6. 使用客户端软件进行多次密码修改、重置操作，并记录检测结果
 | 应符合DB11/T 159.6中的相关要求 | 通过/不通过 |
| 10 | 版本升级 | 1. 确认SE-TSM平台功能正常
2. 安装低版本客户端软件
3. 根据客户端软件升级流程进行升级测试，验证客户端是否具备在线版本检测、升级功能，且升级对应用数据无影响，不影响用户正常使用
 | 应符合DB11/T 159.6中的相关要求 | 通过/不通过 |

* + 1. 安全测试

客户端安全测试包含人机交互安全、软件安全、数据安全、通讯安全，检测内容应符合JT/T 1059.8中的相关要求。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_