社会保障（个人）卡规范
第 8 部分：终端技术要求

引言

本规范作为《社会保障（个人）卡规范》的第 8 部分，对一般的终端特性和功能提出了最低需求。有关系统设计及后台处理的内容不属于本规范的范围，本规范也不涉及终端管理方面的内容。本规范包括以下主要内容：

——基本要求。规定了终端的机电特性、逻辑接口、传输协议要求。

——终端功能。从功能角度对终端的功能部件的特性进行了描述。此部分也规定了终端实施多应用管理的一般原则。同时为保证终端数据存储、处理安全，特别针对安全存取模块的物理安全及逻辑安全两方面对终端的安全要求做了比较全面的描述。

——黑名单管理。原则性地阐述了黑名单管理必须的查询检索方式、检查的内容以及对黑名单更新的安全性要求。对黑名单的收集、存储格式、存储内容等与系统设计有关的内容不在本规范范围内。

本规范附录 A 与规范正文具有同等的效力。

1　适用范围

本规范适用于支持《社会保障（个人）卡规范》所规定的人力资源和社会保障应用的专用终端以及其他类似的终端设备。其中的“终端功能”、“黑名单管理”不适用于读卡器。其使用对象主要是与社会保障卡应用相关的终端设计、制造、管理以及应用系统的研制、开发、集成和维护等组织机构。

2　参考标准

GB/T 1988—1998	信息处理交换用的七位编码字符集
GB/T 15273	信息处理八位单字节代码型图型字符集（ISO 8859：1987）
GB/T 16649．1—2006	识别卡　带触点集成电路卡　第 1 部分：物理特性（ISO/IEC 7816-1：1987）
GB/T 16649．2—2006	识别卡　带触点集成电路卡　第 2 部分：触点的尺寸和位置（ISO/IEC 7816-2：1988）
GB/T 16649．3—2006	识别卡　带触点集成电路卡　第 3 部分：电信号和传输协议（ISO/IEC 7816-3：1989）
IEC 512-2：1979	机电设备机电器件规范　第 2 部分：触点电阻测试、绝缘测试和电压测试
ISO/IEC 7816-3：1997	识别卡　带触点的集成电路卡　第 3 部分：电气信号和传输协议
ISO/IEC 7816-4：1995	识别卡　带触点的集成电路卡　第 4 部分：行业间交换用命令

ISO/IEC 7816-5：1994　　识别卡　带触点的集成电路卡　第 5 部分：应用标识符的编号系统和注册程序

3　定义

以下定义适用于本规范。

3.1　冷复位（Cold Reset）

当 IC 卡的电源电压和其他信号从静止状态中复苏且申请复位信号时，IC 卡产生的复位。

3.2　热复位（Warm Reset）

在时钟（CLK）和电源电压（VCC）处于激活状态的前提下，IC 卡收到复位信号时产生的复位。

3.3　接口设备（Interface Device）

终端上插入 IC 卡的部分，包括其中的机械、电气和逻辑控制部分。

3.4　终端（Terminal）

为处理社会保障卡业务而在服务网点安装的设备，用于同 IC 卡的连接。它包括接口设备，也可包括其他部件和接口，例如与主机通讯的接口。

3.5　命令（Command）

终端向 IC 卡发出的一条信息，该信息启动一个操作或请求一个应答。

3.6　触点（Contact）

在集成电路卡和外部接口设备之间保持电流连续性的导电元件。

3.7　响应（Response）

IC 卡处理完成收到的命令报文后，回送给终端的报文。

3.8　交易（Transaction）

持卡者和业务、管理部门之间根据社会保障卡所支持的应用接受、提供服务的行为。

3.9　功能（Function）

由一个或多个命令实现的处理过程，其操作结果用于完成全部或部分交易。

3.10　静止状态（Inactive）

当 IC 卡上的电源电压（VCC）和其他信号相对于地的电压值小于或等于 0.4 伏时，则称电源电压和这些信号处于静止状态。

3.11　集成电路（Integrated Circuit， IC）

设计用于完成处理和/或存储功能的电子器件。

3.12　集成电路卡（IC 卡）（Integrated Circuit（s） Card）

内部封装一个或多个集成电路的 ID-1 型卡（如 ISO/IEC 7810、ISO/IEC 7811 第一至第五部分、ISO/IEC 7812 和 ISO/IEC 7813 中描述的）。

3.13　ICC 类型标识符（Identifier of ICC Type）

ICC 类型标识符是应用用来向终端表明需要它处理的 ICC 的类型的一个字符串。

3.14　ICC 连接器（ICC Connector）

ICC 连接器是 IFD 与 ICC 电气连接的物理实现部分。在逻辑上，本规范规定用它来标识与它电气上稳定连接的 ICC。

3.15 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。

3.16 报文鉴别代码（Message Authentication Code）

对交易数据及其相关参数进行运算后产生的代码。主要用于验证报文的完整性。

3.17 半字节（Nibble）

一个字节的高四位或低四位。

3.18 密钥（Key）

控制加密转换操作的符号序列。

3.19 加密算法（Cryptographic Algorithm）

为了隐藏或揭露信息内容而变换数据的算法。

3.20 数据完整性（Data Integrity）

数据不受未经许可的方法变更或破坏的属性。

3.21 T=0

面向字符的异步半双工传输协议。

3.22 T=1

面向块的异步半双工传输协议。

3.23 T=15

不是传输协议，而是特指其后所传输字符的属性为全局接口字符。

4 缩略语和符号表示

以下缩略语和符号表示适用于本规范。

C_{IN}	输入电容（Input Capacitance）
CLK	时钟（Clock）
etu	基本时间单元（Elementary Time Unit）
GND	地（Ground）
IC	集成电路（Integrated Circuit）
ICC	集成电路卡（Integrated Circuit Card）
IEC	国际电工委员会（International Electrotechnical Commission）
IFD	接口设备（Interface Device）
I_{IH}	高电平输入电流（High Level Input Current）
I_{IL}	低电平输入电流（Low Level Input Current）
I/O	输入/输出（Input/Output）
I_{OH}	高电平输出电流（High Level Output Current）
I_{OL}	低电平输出电流（Low Level Output Current）
ISO	国际标准化组织（International Organization for Standardization）
MAC	报文鉴别代码（Message Authentication Code）
RFU	保留为将来使用（Reserved for Future Use）
RST	复位（Reset）

SAM	安全存取模块（Secure Access Module）
SW1	状态码 1（Status Word One）
SW2	状态码 2（Status Word Two）
t_F	信号幅度从 90%下降到 10%的时间（Fall Time Between 90% and 10% of Signal Amplitude）
t_R	信号幅度从 10%上升到 90%的时间（Rise Time Between 10% and 90% of Signal Amplitude）
V_{CC}	VCC 触点上的测量电压（Voltage Measured on VCC Contact）
VCC	电源电压（Supply Voltage）
V_{IH}	高电平输入电压（High Level Input Voltage）
V_{IL}	低电平输入电压（Low Level Input Voltage）
V_{OH}	高电平输出电压（High Level Output Voltage）
V_{OL}	低电平输出电压（Low Level Output Voltage）
V_{PP}	VPP 触点上测量到的编程电压（Programming Voltage Measured on VPP Contact）
VPP	编程电压（Programming Voltage）
‘0’-‘9’ ‘A’-‘F’	十六进制数字
A=B	A 等于 B
xx	任意值

5 基本要求

5.1 终端的机电特性、逻辑接口、通信（传输）协议

终端的逻辑接口、通信协议应符合《社会保障（个人）卡规范》第 2 部分：机电特性、逻辑接口与传输协议中的有关内容。且终端必须支持 T=0 传输协议。终端的标准指标和 IC 卡的有所不同，其目的是为防止对 IC 卡的损坏而预留安全余地。

5.1.1 终端的机械特性

本节描述终端接口设备的机械特性。

5.1.1.1 接口设备

用于插入 IC 卡的接口设备应具备接收 IC 卡的能力，并具有以下特性：

——物理特性满足 ISO/IEC 7816-1 的规定。

——正面触点位置应满足 ISO/IEC 7816-2 中图 2 的规定。

定位的导轨和甲板（如果使用）不应损坏 IC 卡，特别是对印制在卡表面的照片、文字信息等区域。

注：作为一个基本原则，持卡人应在任何时候都能将 IC 卡插入或拔出。因而接口设备上插入 IC 卡位置处，应该配有一种机械设备，从而使得持卡人能够在设备发生故障（如掉电）时取回 IC 卡。

5.1.1.2 触点压力

任何一个接口设备触点对相应的 IC 卡触点所施加的压力应在 0.2N 到 0.6N 之间。

5.1.1.3 可接受卡片 IC 模块高度

接口设备可接受卡片 IC 模块表面的最高点不高于卡表面平面 0.10mm，兼容符合 JR/T0025.3 的卡片。

接口设备可接受卡片 IC 模块表面的最低点不低于卡表面平面 0.10mm。

5.1.1.4 触点分配

接口设备触点的分配如表 1 表示：

表 1 接口设备触点的分配

触电号	分配	触电号	分配
C1	电源电压（VCC）	C5	地（GND）
C2	复位信号（RST）	C6	不使用
C3	时钟信号（CLK）	C7	输入/输出（I/O）

C4 和 C8 不使用，在物理上可以不存在。C6 应是电隔离的。

5.1.1.5 ICC 连接器的配置和要求

符合本规范的接口设备至少应配置两个 ICC 连接器，其中一个用作与社会保障卡连接的应用 ICC 连接器，另一个用作与安全访问模块（SAM）连接的安全 ICC 连接器。

接口设备可以配置更多的 ICC 连接器，但这已超出了本规范的范围。

接口设备所使用的应用 ICC 连接器应具有至少 10 万次的插拔寿命。

5.1.1.6 终端的结构安全

终端应提供一定的结构上对安全访问模块的安全保护措施。

5.1.2 终端的电气特性

本节描述了在 IFD 触点上测量出的信号的电气特性。

5.1.2.1 操作条件

5.1.2.1.1 操作条件的类别

本规范定义了三类操作条件。接口设备应通过触点 VCC 向卡提供下列正常的电源电压：

- 在 A 类条件下为 5V。
- 在 B 类条件下为 3V。
- 在 C 类条件下为 1.8V。

卡片应至少同时支持 A 类和 B 类，关于 C 类的要求参见 JR/T0025.3。

5.1.2.1.2 操作条件的选择

图 3 给出了接口设备在选择用于卡的操作条件类别过程的判断条件。所给出的判断条件除出现“卡”字的之外，都是基于隐含在接口设备中的信息的。

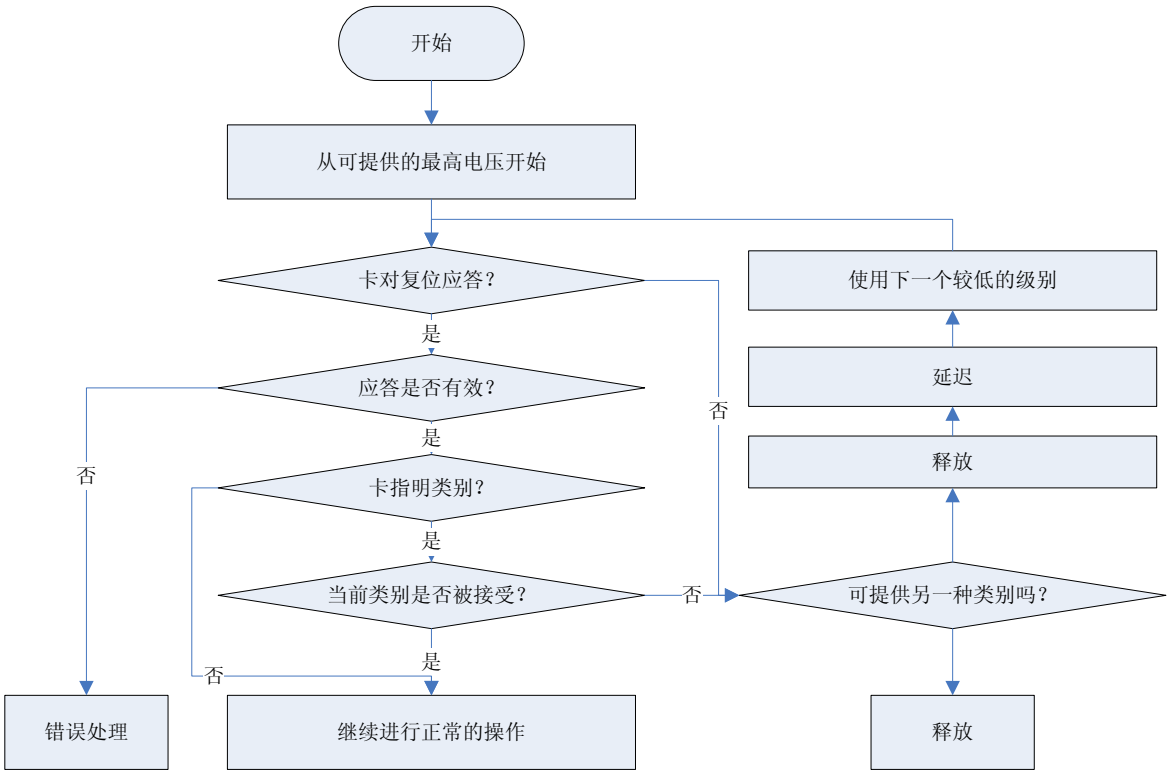

图 3　接口设备对操作条件类别的选择

5.1.2.2　测量约定

所有测量应是在 IC 卡和接口设备之间的触点上进行，并以 GND 为参考。环境温度范围为 0℃～50℃。

所有流出终端的电流均为正值。

接口设备的工作电压为 5V、3V 或 1.8V，允差±5%。

5.1.2.3　输入/输出（I/O）

该触点作为输出端（传输模式）向 IC 卡传送数据，作为输入端（接收模式）从 IC 卡接收数据。在操作过程中，终端和 IC 卡不能同时处于传输模式，若万一发生此情况，I/O 触点的状态（电平）将处于不确定状态，但不应损坏终端。

当终端和 IC 卡都处于接收模式时，触点将处于高电平状态。为了达到这种状态，终端应在 VCC 上或其他装置上连接一个上拉电阻。除非 Vcc 加电并稳定在 5.1.2.7 条中允许的范围内，终端不应将 I/O 置于高电平状态。参见《社会保障（个人）卡规范》第 2 部分：机电特性、逻辑接口与传输协议中有关触点激活的内容。

在任何情况下，均应将流入或流出 I/O 触点的电流限定在±5mA 以内。

5.1.2.3.1　传输模式

在传输模式下，终端向 IC 卡传送数据，其特性如表 2 所示：

表 2　传输模式下 I/O 的电气特征

符号	条件	最小值	最大值	单位
V_{OH}	-20μ A < I_{OH} < 20μ A，　Vcc = 最小值	0.8 × Vcc	Vcc	V
V_{OL}	-1mA <I_{OL} < 0，　Vcc = 最小值	0	0.3	V
t_R 和 t_F	C_{IN}（ICC） = 30pF　最大	-	0.8	μ s
正负脉冲峰值		-0.25	Vcc + 0.25	V

除向 IC 卡传送数据时，终端应将其 I/0 信号驱动模式设置为接收模式。

5.1.2.3.2　接收模式

在接收模式下，终端应能正确解释从 IC 卡发来的具有表 3 所示特性的信号。

表 3　接收模式下 I/O 的电气特征

符号	最小值	最大值	单位
V_{IH}	0.6 × Vcc	Vcc	V
V_{IL}	0	0.5	V
t_R 和 t_F	-	1.2	μ s

5.1.2.4　编程电压（VPP）

不要求终端产生编程电压 VPP（见 5.1.1.3）。

5.1.2.5　时钟（CLK）

终端将产生一个具有表 4 所示特性的时钟信号。

表 4　CLK 的电气特征

符号	条件	最小值	最大值	单位
V_{OH}	0 < I_{OH} < 50μ A，　Vcc = 最小值	Vcc-0.5	Vcc	V
V_{OL}	-50μ A < I_{OL} < 0，　Vcc = 最小值	0	0.4	V
t_R 和 t_F	C_{IN}（ICC） = 30pF　最大	-	8%的时钟周期	μ s
正负脉冲峰值		-0.25	Vcc + 0.25	V

频率范围在 1MHz～5MHz（对 A 类卡操作时）或 1MHz～4MHz（对 B 类卡操作时）之间，且在整个交易期间，其变化范围不应超过±1%（见《社会保障（个人）卡规范》第 2 部分：机电特性、逻辑接口与传输协议中的“卡片操作过程”）。时钟占空因数应在其稳定运行周期的 45%～55%之间。

5.1.2.6　复位（RST）

终端产生一个具有表 5 所示特性的复位信号。

表 5　RST 的电气特征

符号	条件	最小值	最大值	单位
V_{OH}	0 < I_{OH} < 50μ A，　Vcc = 最小值	Vcc-0.5	Vcc	V
V_{OL}	-50μ A < I_{OL} < 0，　Vcc = 最小值	0	0.4	V
t_R 和 t_F	C_{IN}（ICC） = 30pF　最大	-	0.8	μ s
正负脉冲峰值		-0.25	Vcc + 0.25	V

5.1.2.7　电源电压（VCC）

终端提供一个 5V±0.4V（对 A 类卡操作时）或 3V±0.24V（对 B 类卡操作时）或 1.8V±0.14V

（对 C 类卡操作时）的直流电压，并能稳定输出 0～65mA（对 A 类卡操作时）或 0～55mA（对 B 类卡操作时）或 0～35mA（对 C 类卡操作时）的电流。终端应带有保护电路以防止在误操作如对地或 VCC 短路时所造成的损坏。误操作既可能来源于内部，也可能来自外部接口如电源干扰、通讯链路故障等。以 GND 为基准，Vcc 决不可以低于-0.25V。

在 IC 卡的正常操作中，电流脉冲可在 IC 卡触点上引起 Vcc 波动。电源应能中和小于 40nAs 且持续时间不超过 400ns 的电源波动，并能承受 IC 卡上 100mA 的电源消耗。

注：如果需要，终端应能够具有大于 65mA 的传输能力，但建议终端将稳定电流限制在 200mA 以内。

5.1.2.8 触点电阻

在终端的整个设计寿命期间，触点电阻（在清洁的接口设备和清洁的标准 IC 卡触点间测量时）应小于 500mΩ （见 ISO/IEC 10373 的测试方法）。

注：标准的 IC 卡触点可以看作是在 5.00μ m 的镍表面上的 1.25μ m 镀金触点。

5.1.2.9 短路保护

当任何两个触点之间发生短路时，无论时间长短，终端都不应被损坏或功能失常。例如：插入一块金属板或插入一块带有金属性表面的 IC 卡。

接口设备所有的 ICC 连接器都应具有短路保护功能。

5.1.2.10 插入 IC 卡后，终端的加电和断电

插入 IC 卡后，当对终端进行加电或断电时，触点的接口界面不应出现杂乱信号或电源干扰，触点激活和释放的时序应分别符合《社会保障（个人）卡规范》第 2 部分：机电特性、逻辑接口与传输协议中的规定。

5.1.3 接口设备在复位应答期间的操作

本节规定了接口设备在复位应答期间接收到 IC 卡回送字符后的相关操作。有关的字符定义在《社会保障（个人）卡规范》第 2 部分：机电特性、逻辑接口与传输协议中规定。

5.1.3.1 TS-初始字符

终端应能够同时支持反向和正向逻辑约定，并接收 IC 卡回送的值为‘3B’或‘3F’的 TS，但应拒绝接收其他 TS 值。

5.1.3.2 T0-格式字符

T0 回送值正确且包含了所需的接口字符（TA1 到 TD1）和历史字符时，终端不应拒绝 IC 卡回送任何值。

5.1.3.3 接口字符 TA1 到 TC3

5.1.3.3.1 接口字符 TA1

终端不应拒绝 IC 卡回送 TA1=‘01’或‘11’（如果 T0 的 b5 位为‘1’），并在整个后续交易过程中继续使用缺省值 F=372 和 D=1。

注：如果回送 TA1，终端应能对其低半字节正确译码，并得出 D 的有效值 1、2 或 4。本规范以后的版本可能支持其他的 D 值，以提高 TTL 和 IC 卡之间的数据传送速率和选择其他协议类型。

5.1.3.3.2 接口字符 TB1

如果 T0 的 b6 位为‘1’，终端不应拒绝回送任何 TB1 的 IC 卡：如果 T0 的 b6 位为‘0’，则 IC 卡不回送 TB1，此时终端仍应继续卡片操作过程，且不提供编程电压 VPP，就象回送了 TB1=‘00’一样。

注：终端可以保持 VPP 为静止状态（见 5.1.2.3）。

5.1.3.3.3 接口字符 TC1

如果 T0 的 b7 位为‘0’，终端不应拒绝不回送 TC1 的 IC 卡，但如果终端接受了这样的 IC 卡，应能够继续卡片操作过程，就象回送了 TC1=‘00’一样。

注：应将 TC1 设置为 IC 卡可接受的最小值。TC1 取值过大将导致终端与 IC 卡之间的通讯缓慢，这样将延长交易时间。

5.1.3.3.4 接口字符 TD1

如果回送值正确且包含了所需的接口字符 TA2 到 TD2，终端不应拒绝这样的 IC 卡，即：其所回送 TD1 的高半字节为任意值且低半字节的值为‘0’或‘1’。终端应拒绝回送其他 TD1 值的 IC 卡。

5.1.3.3.5 接口字符 TA2

如果终端在复位应答期间能够支持由 IC 卡通过 TA2 所指明的额外条件，它不应拒绝这样的 IC 卡，并应能立即使用这些条件。

5.1.3.3.6 接口字符 TB2

终端不应拒绝 IC 卡回送 TB2。但不论 TB2 是否回送、回送何值，终端均不应提供 VPP。

注：终端可以保持 VPP 为静止状态（见 5.1.2.3）。

5.1.3.3.7 接口字符 TC2

终端不应拒绝回送 TC2=‘10’的 IC 卡。

5.1.3.3.8 接口字符 TD2

如果回送值正确且包含了所需的接口字符 TA3 到 TD3，终端不应拒绝这样的 IC 卡，即：其所回送 TD2 的高半字节为任意值且低半字节的值为‘l’或‘F’。终端应拒绝 IC 卡回送其他的 TD2 值。

5.1.3.3.9 接口字符 TA3

如果此前 T=15 已存在，TD2 的 b5 位为‘0’，终端不应拒绝不回送 TA3 的 IC 卡。但如果终端接受了这样的 IC 卡，则应令 TA3=‘01’来继续卡片操作过程。终端应拒绝那些回送的 TA3 值不满足《社会保障（个人）卡规范》第 2 部分：机电特性、逻辑接口与传输协议要求的 IC 卡。

如果此前 T=15 不存在，终端不应拒绝正确回送接口字符 TA3 的 IC 卡。

5.1.3.3.10 接口字符 TB3 和 TC3

尽管《社会保障（个人）卡规范》第 2 部分：机电特性、逻辑接口与传输协议规定了社会保障卡只使用 T=0 的 IC 卡，但终端不应拒绝正确回送接口字符 TB3 和 TC3 的 IC 卡。

5.1.3.4 校验字符 TCK

在使用 T=0 协议且 T=15 不存在时，终端应拒绝回送了 TCK 的 IC 卡。如果 IC 卡回送了 TCK，终端应能对 TCK 进行计算。

注：《社会保障（个人）卡规范》第 2 部分：机电特性、逻辑接口与传输协议对 TCK 的描述仅适用于那些支持 T=0 和（或）T=1 协议的 IC 卡。如果出于特殊原因 IC 卡支持 T=14 协议，TCK 所遵循的条件应由该协议的规范确定，且这种条件的确定不属本规范定义的范围。

5.1.4 接口设备在协商模式中的操作

在协商模式中，接口设备宜发起 PPS 请求，与 IC 卡协商后确定 F 和 D 的参数值。

5.1.5 终端与接口设备之间的数据交换

终端设备应能够接收 IC 卡一次返回 256 字节的数据及后续的状态码。

6 终端功能

6.1 终端类型

支持社会保障应用的终端根据其使用环境的不同可以分为社保应用终端和社保金融联合终端。

表 6 给出了这两类终端的最低功能部件的配置要求。

表 6 终端的最低功能部件配置要求

终端部件	社保应用终端	社保金融联合终端
显示器	必备型（Mandatory）	必备型（Mandatory）
IC 卡接口设备	必备型（Mandatory）	必备型（Mandatory）
键盘	必备型（Mandatory）	必备型（Mandatory）
密码键盘	可选型（Optional）	必备型（Mandatory）
安全存取模块	必备型（Mandatory）	必备型（Mandatory）
存储设备	可选型（Optional）	必备型（Mandatory）
打印机	可选型（Optional）	必备型（Mandatory）
网络通信接口	可选型（Optional）	可选型（Optional）
实时时钟	必备型（Mandatory）	必备型（Mandatory）
汉字扩展字符集	必备型（Mandatory）	必备型（Mandatory）
电源	必备型（Mandatory）	必备型（Mandatory）
磁条阅读器	--	必备型（Mandatory）

6.2 功能部件的特性

6.2.1 显示器

用于交易过程显示及错误指示。本规范要求显示器具有显示汉字、字母、数字和符号的能力。

6.2.2 IC 卡接口设备

终端应提供用户卡接口的 IC 卡读卡器，用来接受用户 IC 卡插入并与 IC 卡进行命令数据传递通讯。该读卡器模块包括机械、电气和逻辑协议等部分。

建议终端的用户卡 IC 卡读卡器插槽附近有一明显标记指示如何插入 IC 卡。如果终端有锁卡或吞卡功能，则应保证在掉电、设备异常或交易取消时能释放或退出卡。

6.2.3 键盘

用于输入交易数据（如进行确认）、业务信息，它至少应配置的数字字母键及确认功能健。

6.2.4 密码键盘

终端应提供输入个人识别码（PIN）验证的密码键盘，允许持卡人输入 4－12 位的 PIN。

可以是与终端键盘集成在一起的内置式密码键盘，也可以是与终端通过通讯线连接的外置式密码键盘。密码键盘的设计应当符合应用的要求。

6.2.5 安全存取模块

用于对终端操作社会保障卡的权限鉴别，包括权限控制密钥的存储、鉴别数据的计算等功能。

6.2.6 打印机

终端可根据社保业务的需要配置相应的打印机。本规范对其特性不作规定。

社保金融联合终端应配置有能打印借记卡交易单据的打印机，可以是针式或热敏打印机。对每笔批准的借记卡交易，不论是脱机或联机都能打印出交易单据。打印单据格式由各关联收单银行自定，但应包含如下数据：卡号、应用标识符 AID、交易日期时间、签名栏。

6.2.7 网络通信接口

终端应当配置有与主机后台通信的模块。用于联机交易或终端与主机之间的数据传输。具有联机交易功能的终端其通信模块与主机的通信速度应能满足实时传送 IC 卡交易数据的要求。

社保金融联合终端的网络通信接口还可用于下载管理。关于下载管理的规定参照 JR/T 0025.3。

6.2.8 存储设备

用于存储交易记录、黑名单、特殊的业务数据和（或）扩展中文字符集等信息。建议根据其用途为终端配备有足够存储容量的存储设备。

6.2.9 实时时钟

用于提供业务处理所需的终端时间，如交易时间。

6.2.10 扩展中文字符集

用于持卡人姓名中 GBK 字符集之外的汉字字符处理。它可以以存储设备中的软件形式存在，也可以是专用的硬件部件。

6.2.11 电源

移动式终端应保证可连续工作 4 小时，待机时间不小于 24 小时。

固定式终端的工作电压为 220V，允差±10％。

6.2.12 磁条阅读器

社保金融联合终端应针对金融应用配置磁条阅读器。关于磁条阅读器的具体要求参见 JR/T 0025.3。

6.3 多应用管理

6.3.1 基本要求

IC 卡与终端必须配合使用以保证交易安全、有效地运行。为了支持《社会保障（个人）卡规范》第 6 部分：应用数据结构中规定的应用，本规范对实现多应用的终端提出一些管理应用和选择应用的具体原则。一般来说，支持超过一种以上的社会保障卡中应用的终端应给用户一个按应用优先级排序的列表以供选择。

6.3.2 终端应用的管理

终端应用的管理应达到如下目标：

1.应用之间不能互相影响：各应用必须相互独立运行，相互之间数据和程序不可交换。

2.共享数据必须保证：

——各应用的内部数据不能被其他应用得到；

——所有的应用可以共享终端中的通用数据。

3.提供应用选择的标准界面。

4.对应用进行管理（提供应用程序的选择、激活、禁止、参数设置等等）。

6.3.3 IC 卡应用选择

符合《社会保障（个人）卡规范》第 2 部分：机电特性、逻辑接口与传输协议的社会保障卡将实现多个应用，终端应能够选择并支持这些应用。应用选择过程应符合《社会保障（个人）卡规范》第 6 部分：应用数据结构的规定。

6.4 终端的安全要求

本节规定了终端数据存储、处理的一般性安全要求，同时也对安全存取模块提出了具体的要求。如何实现这些安全要求超出了本规范的范围。

6.4.1 一般要求

终端中一般存在两种类型的数据：

1.通用数据：包括时间、终端识别号及终端业务记录等。外界可以对这些数据进行访问，但不允许进行无授权修改。

2.敏感数据：包括密钥、应用程序内部的参数。在未授权的情况下，外界不允许对这类数据进行访问和修改。

6.4.1.1 通用数据的安全要求

通用数据一般存放在存储器中。在更新参数以及下载新的应用程序时，终端必须做到：

1.验证更新方的身份，对于应用程序重新下载，只允许终端制造厂商、终端所有者或者经终端所有者或代理方批准的第三方执行。

2.校验下载参数及应用程序的完整性。

对存储器要求必须做到：无论在什么情况下，终端的应用数据都不会随意改变或丢失，并保证其有效。

所有与交易相关的数据均应以记录形式存储于终端存储器中。终端必须保证这些数据的完整性。

6.4.1.2 敏感数据的安全要求

敏感数据一般应存放在安全存取模块中。

安全存取模块是一种能够提供必要的安全机制以防止外界对终端所储存或处理的数据进行非法攻击的硬件加密模块。

此模块主要负责保存和处理所有的敏感数据，这些数据包括《社会保障（个人）卡规范》第 6 部分：应用数据结构中定义的各种密钥及其他相关的与安全有关的信息。本规范对安全存取存取模块的具体物理形式不作具体的要求。

在正常的操作环境下，安全存取模块必须保证：出入模块的、以及其内部存放的和正在处理的数据不会出于模块自身或其接口造成任何泄露和改变。

6.4.2 安全存取模块的物理安全要求

安全存取模块的硬件设计必须能保证在物理上限制对其内部存贮的敏感数据的存取与窃取，以及对安全存取模块的非授权使用和修改。一旦安全存取模块受到非法的篡改及攻击，其自身必须能够立即完成对内部敏感数据的删除。要实现这些目标，安全存取模块应具有防窃、查窃、窃取显示或窃取响应机制。

同时，安全存取模块也必须具有足够的防范特性，能够发现是否被篡改过。

总之，安全存取模块的设计和构造必须满足以下要求：

1.只有通过特别的技巧与工具或严重破坏的方法，才能对模块的硬件或软件进行增加、替换或修改。

2.任何对敏感数据的访问或修改，只有通过对模块的有效接触才能达到。

3.安全存取模块的任何部分的损坏或失效都不会导致敏感数据的泄露。

4.如果安全存取模块是由多个分离部件组合而成，而处理的数据又必须在这些部件之间传递，那么各部件必须保持相同的安全级别。

6.4.3 安全存取模块的逻辑安全要求

一个安全存取模块的逻辑设计应保证，调用任何单一功能或组合功能，都不会导致敏感数据的泄露。对于某些敏感操作，必须有一定的权限限制。

安全存取模块中可存放多组不同版本的主密钥。所有的主密钥通常必须在终端投入使用之前，被下载到安全存取模块中。如果在终端使用过程中，主密钥需要修改，必须使用安全报文。实现这一操作通常必须在特殊的授权情况下完成，对外部不能存在任何取得存放在安全存取模块中密钥的机会。

为避免伪操作，存放在安全存取模块中的任何类型的主密钥必须与某个特定的操作相结合，而不适用于其他操作。

对于需要报文鉴别码的交易，安全存取模块应能够生成并传递符合《社会保障（个人）卡规范》第 4 部分：安全机制定义的 MAC。

在每次交易结束或超时状态下，安全存取模块应自动清除内部缓存区中存放的数据。

安全存取模块必须能够实现规定的加密算法和主密钥到子密钥的分散算法，以及用于 PINPAD 到终端的用户 PIN 加密以及脱机数据认证。

6.4.4 终端设备安全要求

6.4.4.1 防入侵设备

一个防入侵的设备必须保证在它的正常的运行环境中，设备或它的接口不会泄露或改变任何输入或输出设备的、存储在设备中的或者在设备中处理的敏感数据。

当一个防入侵的设备在一个安全的受控环境中运行时，对该设备特性的要求可以降低，因为受控环境和对设备的管理提供了对设备的保护。

6.4.4.2 物理安全性

一个防入侵的设备必须被设计为限制对内部存储的敏感数据的物理访问,并且阻止窃取数据,未经授权的使用或者未经授权的对设备的修改。这些目标总体上要求将对入侵的抵御、对入侵的检测、对入侵的指示或反应机制结合起来，如可视或有声的报警。

一台不处于运行状态的防入侵的设备，必须不包含在任何以前的交易中用过的加密密钥

或者其它的敏感数据（例如 PIN），但可以包含只是出于提高防入侵能力的目的的认证信息。如果是在该设备和存储在其中的密钥重新投入使用前能够监测到闯入即使它被非法闯入也不会影响安全。如果设备被设计为允许内部访问，那么在进入时敏感数据必须立即被擦除。一个防入侵的设备依赖于用户对针对物理安全的攻击的监测。因此，这种设备必须被设计为具有足够的防入侵特性，使得任何入侵对于持卡人都应该是明显的或者能被监测到。

设备必须被设计和构造为：

- 不允许轻易入侵设备并对设备的软硬件进行增加、替换或修改；如果在没有特别的技巧和专门的装备，并且不对设备造成严重的、显而易见的破坏的前提下，不允许测定或修改任何敏感数据后重新安装设备。
- 只有真正进入设备，才能做到对输入的、存储的或处理的敏感数据的未经授权的访问或修改。
- 不能采用普通的包装材料，以防止使用一般条件下都具备的材料生产‘看上去一样’的假冒复制品。
- 当设备的任何部件发生任何故障时，不会导致秘密或敏感的数据的泄露。
- 如果设备的设计需要部分部件在物理上分离，并且处理的数据或持卡人的指令在这些分离的部件之间传递，那么对设备的所有部件的保护等级应该是相同的。

对交换敏感数据如明文 PIN 来说，将不同的部件整合在单一的防入侵的外壳中是必要的条件。

6.4.4.3 逻辑安全性

防入侵的设备必须被设计为没有单一的函数或函数的组合能够导致敏感数据的泄露，不被一些多指令或任何指令的混合体轻易攻破，除了在终端中实现的安全机制明确允许的以外。即使在使用合法的函数的情况下，也必须有足够的逻辑保护使其不会危及敏感数据的安全。这个要求可以通过内部的统计监控或控制对敏感函数调用的最小时间间隔来实现。

如果终端可以被置于一种‘敏感状态’，即允许通常情况下不被允许的函数的状态（例如，人工安装密钥），这样的转换必须在两个或两个以上可信赖的人员的协助下进行。如果用密码或其它明文数据来控制转换到敏感状态，那么这些密码的输入也要用和其它敏感数据一样的方式来保护。

为了将由未经授权的对敏感函数的使用所导致的风险降到最小，对敏感状态必须有调用函数次数（适当的）的限制和时间限制。一旦达到了这些限制，设备必须返回正常状态。

在交易结束或超时后，防入侵的设备必须自动清除内部的缓存。

6.4.4.4 密码键盘安全性

密码键盘必须是一个防入侵的设备。它必须支持输入 4-12 个数字的 PIN。如果密码键盘有显示屏，必须以不泄露 PIN 值的方式显示每一个输入的数字。

如果终端支持脱机 PIN 校验，则 IC 卡读卡器和密码键盘要么被集成为单一的防入侵的设备，要么是两个分离的防入侵的设备。

- 如果 IC 卡读卡器和密码键盘是集成的并且脱机 PIN 被以明文格式传递给卡片，那么在明文 PIN 被直接从密码键盘传到 IC 卡读卡器的情况下，密码键盘不对脱机 PIN 进行加密。
- 如果 IC 卡读卡器和密码键盘是集成的并且脱机 PIN 被以明文格式传递给

卡片，但脱机明文 PIN 不是被直接从集成的密码键盘传到 IC 卡读卡器，那么密码键盘必须依照 ISO 9564-1（或相当的被支付系统批准的其它方式）对脱机 PIN 进行加密，再将其传递给 IC 卡读卡器。IC 卡读卡器随后对脱机 PIN 解密，再以明文传递给卡。

- 如果 IC 卡读卡器和密码键盘不是集成的并且脱机 PIN 以明文格式传递给卡片，那么密码键盘必须依照 ISO 9564-1（或相当的被支付系统批准的其它方式）对脱机 PIN 进行加密，再将其传递给 IC 卡读卡器。IC 卡读卡器随后对脱机 PIN 解密，再以明文传递给卡。

PIN 的加密过程必须发生在下面两种其一的情况

如果终端支持联机 PIN 校验，当 PIN 被输入后，必须依照 ISO 9564-1 对 PIN 进行加密来保护 PIN，并且对 PIN 的传输必须符合支付系统的规则。

显示在密码键盘上提示输入 PIN 的信息必须由密码键盘生成。这并不意味着只有和 PIN 相关的信息才能在密码键盘上显示，但其它的信息在显示前必须被密码键盘批准。密码键盘必须拒绝任何未经批准的的信息的显示。

对于有人值守的终端，金额输入过程必须和 PIN 输入过程分开，以避免意外地将 PIN 显示在终端的显示屏上。特别是如果在同一个键盘上输入金额和 PIN，那么金额输入和 PIN 输入必须是明显分开的两个操作，如果没有其他确认操作，持卡人输入的 PIN 应被用于金额确认。

密码键盘必须被设计为能提供隐私性和机密性，使得在正常的使用中，只有持卡人能够看到输入或显示的信息。密码键盘的安装和替换必须保证它的周边环境为持卡人输入 PIN 提供了足够的隐密性，从而将 PIN 暴露给他人的风险降到最低。

密码键盘必须在以下两种条件发生后自动清除内部缓存：

- 在交易结束后。

在超时的情况下，包括在一个 PIN 字符输入后过去了很长的时间的情况。

7 黑名单管理

终端应具有黑名单存储和检索功能，以实现社会保障卡交易的安全处理。黑名单管理包括黑名单的收集、分发、存储、检索、更新等。本规范原则性地对黑名单的记录格式、检索和更新作出了规定，与黑名单管理有关的其他内容不在本规范范围内。

7.1 黑名单的记录类型

终端的黑名单文件应该能够存储两种格式的黑名单记录：

——卡的识别码和卡号

——卡号区段

7.2 黑名单检查

黑名单检查操作在《社会保障（个人）卡规范》第 7 部分：应用流程中的“IC 卡有效性检查”过程中进行。终端根据卡的识别码和卡号进行黑名单检查操作，包括：

——该卡是否包含在黑名单区段范围内；

——该卡是否在终端存储的黑名单卡之列。

7.3 黑名单更新

黑名单文件更新包括增加、删除等操作，且需要在安全环境下进行。安全要求应包括：

——主机和终端间通信数据的安全性和完整性；

——终端对黑名单更新操作的安全认证。

附录 A

高级应用编程接口

本附录描述了读卡器的高级应用编程接口：

高级应用编程接口是提供给终端上的应用程序用来与读卡器进行交互操作的函数集。

高级应用编程接口的具体表现形式必须包括：

a. 可以在 32 位 Windows 环境下（Windows95 及 Windows95 以上各版本）运行的动态

链接库（SSSE32.DLL）；

b. 可以在 16 位 Windows 环境下（Windows3.1 等）运行的动态链接库（SSSE16.DLL）；

c. 可以在 DOS 环境下运行的 C 语言（MSC 或 Borland C）函数库（SSSE16.LIB）；

d. 可以在 DOS 环境下运行的 Foxpro 函数库（SSSE16.PLB）。

高级应用编程接口的具体表现形式也可以包括：

a. 可以在 Unix 环境下运行的 C 语言函数库；

b. 可以在基于特定硬件平台上的 C 语言函数库。

上述所有高级应用编程接口应具有本规范所规定的统一的库名、函数名、参数类型和顺序。

应用开发者或用户在对读卡器编程时，可使用相应的库名和函数名。

注：在以下的描述中，分别使用 C 语言和 Foxpro 语言风格来说明高级应用编程接口中的函数。

A1 C 语言函数

A1.1 打开设备”函数

函数：

long ICC_Reader_Open （char* dev_Name）

功能：

该函数通知终端操作系统打开与读卡器所对应的终端设备端口，以便两者建立通信的逻辑关系。

参数说明：

dev_Name：设备名称。取值范围”AUTO”、”COMn”、”USBn”、”LPTn”，其中”n”的取值范围为 1~9。

返回值：

若正常，返回值为不小于 0 的设备句柄；反之返回值为状态码，其含义见 B1.8。

注：对 16 位 Windows 环境下运行的动态链接库、DOS 环境下运行的静态函数库返回的设备句柄，其含义均不同于 32 位 Windows 环境下动态链接库返回的设备句柄，仅为区分设备之用。

A1.2 “关闭设备”函数

函数：

long ICC_Reader_Close （long ReaderHandle）

功能：

该函数通知操作系统关闭所指定的设备。

参数说明：

ReaderHandle：设备句柄。

返回值：

返回值含义见 B1.8。

A1.3 “卡上电”或“热复位“函数

函数：

long ICC_Reader_PowerOn （long ReaderHandle，unsigned char ICC_Slot_No，unsigned char* Response）

功能：

该函数要求读卡器对 ICC 进行冷复位，若冷复位失败读卡器应启动一个热复位。

参数说明：

1. ReaderHandle：设备句柄；

2. ICC_Slot_No：ICC 连接器号；用户卡连接器号 0x0n，SAM 卡连接器号 0x1n，其中“n”的取值范围为 1~F；

3. Response：指向存放响应数据的存储区的指针。

返回值：

如果对 ICC 复位成功，则在 Response 的存储区中返回 ICC 的复位应答字节，返回值为存储区中的字节数；返回值小于 0 为状态码，其含义见 B1.8。

A1.4 “卡下电”函数

函数：

long ICC_Reader_PowerOff （long ReaderHandle，unsigned char ICC_Slot_No）

功能：

该函数要求读卡器撤消与 ICC 之间的电气连接。

参数说明：

1. ReaderHandle：设备句柄；

2. ICC_Slot_No：ICC 连接器号。

返回值：

如果该函数成功执行，则返回值为 0；返回值小于 0 为状态码，其含义见 B1.8。

A1.5 “获取卡片状态”函数

函数：

long ICC_Reader_GetStatus （long ReaderHandle，unsigned char ICC_Slot_No）

功能：

查询有无卡以及卡片当前状态信息。

参数说明：

1. ReaderHandle：设备句柄；

2. ICC_Slot_No：ICC 连接器号。

返回值：

返回 0 表示有卡且已上电；返回值小于 0 为状态码，其含义见 B1.8。

A1.6 “应用命令”函数

函数：

long ICC_Reader_Application （long ReaderHandle，unsigned char ICC_ Slot _No，
long Lenth_of_Command_APDU，unsigned char* Command_APDU，
unsigned char* Response_APDU）

功能：

该函数用于将符合 ISO/IEC 7816 中所规定的基本和特殊功能的行业间交换用命令发送给指定的 ICC 连接器，并获取对应的响应。

参数说明：

1. ReaderHandle：设备句柄；

2. ICC_Slot_No：ICC 连接器号；

3. Lenth_of_Command_APDU：其值为 Command_APDU 所指向缓冲区中的字节数；

4. Command_APDU：指向存放命令的缓冲区的指针；

5. Response_APDU：指向存放响应数据的存储区的指针（包括 sw1，sw2）。

返回值：

如果函数执行成功，则在 Response_APDU 的存储区中返回响应数据，函数返回值为存储区中的字节数；返回值小于 0 为状态码，其含义见 B1.8，Response_APDU 的存储区无任何数据。

A1.7 “取信息”函数

函数：

long ICC_Reader_Libinfo （char* info）

功能：

该函数取得当前函数库的厂家信息。

参数说明：

info：指向存放厂家信息的存储区的指针。

表 A1.1 厂家信息的存储格式

第 1~16 字符	第 17~30 字符	第 31、32 字符
厂家名称（不足补空格）	设备型号或系列号（不足补空格）	函数库版本号

返回值：

返回值的含义见 B1.8。

A1.8 函数返回值

表 A1.2 高级编程接口 C 语言函数的返回值

应用编程的标识符	返回值	含义
IFD_OK	0	执行成功
IFD_ICC_TypeError	-1	卡片类型不对
IFD_ICC_NoExist	-2	无卡
IFD_ICC_NoPower	-3	有卡未上电
IFD_ICC_NoResponse	-4	卡片无应答
IFD_ConnectError	-11	读卡器连接错
IFD_UnConnected	-12	未建立连接（没有执行打开设备函数）
IFD_BadCommand	-13	（动态库）不支持该命令
IFD_ParameterError	-14	（发给动态库的）命令参数错
IFD_CheckSumError	-15	信息校验和出错

A2 Foxpro 语言函数

注：在以下的描述中，所指字符为 ASCII 字符。

A2.1 “打开设备”函数

函数：

ICCR_Open （dev_Name）

功能：

该函数通知终端操作系统打开与读卡器所对应的终端设备端口，以便两者建立通信的逻辑关系。

参数说明：

dev_Name：设备名称。取值范围”AUTO”、”COMn”、”LPTn”，其中”n”的取值范围为 1~9。

返回值：

返回值为一字符串， 前两个字符为函数执行状态码，其含义见 B2.8；若执行成功，第 3、4 个字符为函数执行后返回的设备句柄 R_Handle，该句柄仅为区分设备之用。

A2.2 “关闭设备”函数

函数：

ICCR_Close （R_Handle）

功能：

该函数通知操作系统关闭所指定的设备。

参数说明：

R_Handle：设备句柄。

返回值：

返回值为两个字符的状态码，其含义见 B2.8。

A2.3 “卡上电”或“热复位“函数

函数：

ICCR_Pon （R_Handle，ICCSlotNo）

功能：

该函数要求读卡器对 ICC 进行冷复位，若冷复位失败读卡器应启动一个热复位。

参数说明：

1. R_Handle：设备句柄；

2. ICCSlotNo：ICC 连接器号；用户卡连接器号 0x0n，SAM 卡连接器号 0x1n，其中”n”的取值范围为 1~F。

返回值：

返回值为一字符串， 前两个字符为函数执行状态码，其含义见 B2.8；若执行成功，第 3、4 两个字符为复位应答中的字节数（十六进制），从第五字符起为 ICC 的复位应答字符（字符个数为字节数的 2 倍）。

A2.4 “卡下电”函数

函数：

ICCR_Poff （R_Handle，ICCSlotNo）

功能：

该函数要求读卡器撤消与 ICC 之间的电气连接。

参数说明：

1. R_Handle：设备句柄；

2. ICCSlotNo：ICC 连接器号。

返回值：

返回值为两个字符的状态码，其含义见 B2.8。

A2.5 “获取卡片状态”函数

函数：

ICCR_GetS （R_Handle，ICCSlotNo）

功能：

查询有无卡以及卡片当前状态信息。

参数说明：

1. R_Handle：设备句柄；

2. ICCSlotNo：ICC 连接器号。

返回值：

返回值为两个字符的状态码，“00”表示有卡且已上电，其他含义见 B2.8。

A2.6 “应用命令”函数

函数：

ICCR_App （R_Handle，ICCSlotNo，ComAPDU）

功能：

该函数用于将符合 ISO/IEC 7816 中所规定的基本和特殊功能的行业间交换用命令发送给指定的 ICC 连接器，并获取对应的响应。

参数说明：

1. R_Handle：设备句柄；

2. ICCSlotNo：ICC 连接器号；

3. ComAPDU：命令字符串，每两字符表示发送命令的一字节。

返回值：

返回值为一字符串， 前两个字符为函数执行状态码，其含义见 B2.8；若执行成功，第 3、4、5、6 字符为响应数据的字节数（十六进制），从第 7 字符起为响应数据字符（字符个数为字节数的 2 倍）。

A2.7 “取信息”函数

函数：

ICCR_Linfo（ ）

功能：

该函数取得当前函数库的厂家信息。

参数说明：

返回值：

返回值为一字符串， 前两个字符为函数执行状态码，其含义见 B2.8；若执行成功，从第 3 字符起为厂家信息字符串。

表 A2.1 厂家信息的存储格式

第 1~16 字符	第 17~30 字符	第 31、32 字符
厂家名称（不足补空格）	设备型号或系列号（不足补空格）	函数库版本号

A2.8 函数返回值

表 A2.2 高级编程接口 Foxpro 函数的返回值

应用编程的标识符	返回值	含义
IFD_OK	00	执行成功
IFD_ICC_TypeError	01	卡片类型不对
IFD_ICC_NoExist	02	无卡
IFD_ICC_NoPower	03	有卡未上电
IFD_ICC_NoResponse	04	卡片无应答
IFD_ConnectError	11	读卡器连接错
IFD_UnConnected	12	未建立连接（没有执行打开设备函数）
IFD_BadCommand	13	（动态库）不支持该命令
IFD_ParameterError	14	（发给动态库的）命令参数错
IFD_CheckSumError	15	信息校验和出错