ICS 35.240.40
A 11

JR

中华人民共和国金融行业标准

JR/T 0120.3—2016

银行卡受理终端安全规范
第3部分：自助终端

Security specification for bank card terminals—

Part 3: Self-service terminal

2016-09-06 发布　　2016-09-06 实施

中国人民银行　发布

目　次

前　言

JR/T 0120—2016《银行卡受理终端安全规范》由以下五个部分组成：

——第1部分：销售点(POS)终端；

——第2部分：受理商户信息系统；

——第3部分：自助终端；

——第4部分：电话支付终端；

——第5部分：PIN输入设备。

本部分按照GB/T 1.1—2009 给出的规则起草。

本部分为《银行卡受理终端安全规范》的第3部分。

本部分由中国人民银行提出。

本部分由全国金融标准化技术委员会(SAC/TC 180)归口。

本标准负责起草单位：中国人民银行科技司、中国银联股份有限公司。

本部分起草单位：中国工商银行、中国农业银行、中国银行、中国建设银行、交通银行、中国光大银行、招商银行、中国邮政储蓄银行、中国金融电子化公司、中金金融认证中心有限公司、北京银联金卡科技有限公司、银联商务有限公司、福建联迪商用设备有限公司、飞天诚信科技有限公司、无线网络安全技术国家工程实验室、工业和信息化部计算机与微电子发展研究中心（中国软件评测中心）、信息产业信息安全测评中心。

本部分主要起草人：李伟、王永红、陆书春、李兴锋、杜宁、陈则栋、曲维民、汤沁莹、王禄禄、吴永强、赵哲、贾铮、周皓、王兰、李伟（中国银联）、吴潇、张志波、潘润红、邬向阳、杨倩、刘运、张晓欢、谭颖、严伟锋、曹宇、俞纹雯、周英斌、夏庆凡、王治纲、王伯铮、于华东、李同勋、冯健诚、代伟、钱菲、李穗申、李石超、顾才泉、侯智勇、张晓琪、高志民、高强裔、李超、高峰、周诗扬、孙茂增、马哲、尚可、胡盖、张俊江、蒋利兵、郭鑫、林眺、于海涛、白艳雷、李琴、宋铮、刘健、董晶晶。

银行卡受理终端安全规范

第3部分：自助终端

1 范围

本部分规定了磁条卡及IC卡受理自助终端标准，主要内容包括磁条卡及IC卡自助终端的硬件要求、软件要求以及自助终端的安全要求，其中不涉及自助终端应用部分。

本部分适用于受理银行磁条卡或IC卡的各种自助终端设备（包括ATM等设备），可用于售卡、售票、售货、缴费、充值、加油、停车等。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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 228—1987 金属拉伸试验方法

GB 4943.1—2011 信息技术设备 安全 第1部分：通用要求

GB 5007.1—2001 信息技术 汉字编码字符集(基本集)24点阵字型

GB 5199 信息交换用汉字15X16点阵字模集

GB 9254 信息技术设备的无线电干扰限值和测量方法

GB 10409—2001 防盗保险柜

GB 13000.1—1993 信息技术通用多八位编码字符集 第1部分：体系结构和基本多文种平面

GB 16793—1997 信息技术 通用多八位编码字符集(Ⅰ区)汉字24点阵字型

GB 17625.1 低压电气及电子设备发出的谐波电流限值（设备每项输入电流≤16A）

GB 17698—1999 信息技术 通用多八位编码字符集(I 区)汉字16点阵字型

GB 18030—2005 信息技术 中文编码字符集

GB/T 14081—1993 信息处理用键盘(西文)通用技术条件

GB/T 14715—1993 信息技术设备用不间断电源通用技术条件

GB/T 15120—2012（所有部分） 识别卡 记录技术

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

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

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

GB/T 17183—1997 数据终端设备和数据电路终接设备用的高速25插针接口暨可替换的26插针连接器

GB/T 17618—1998 信息技术设备抗扰度限值和测量方法

GB/T 18031—2000 信息技术数字键盘汉字输入通用要求

GB/T 21078.1 银行业务 个人识别码的管理与安全 第1部分：ATM终端和POS系统中联机PIN处理的基本原则和要求

GB/T 6107—2000 使用串行二进制数据交换的数据终端设备和数据电路终接设备之间的接口

JR/T 0001 银行卡销售点（POS）终端技术规范

JR/T 0002 银行卡自动柜员机（ATM）终端技术规范

GM/T 0002 SM4分组密码算法
GM/T 0003 SM2椭圆曲线公钥密码算法
GM/T 0004 SM3密码杂凑算法
GM/T 0009 SM2密码算法使用规范
ISO/IEC 14443 识别卡 无触点集成电路卡 近程卡(Identification cards-Contactless integrated circuit(s) cards-Proximity cards)
GA/T 73—1994 机械防盗锁

3 术语和定义

JR/T 0001和JR/T 0002中界定的以及下列术语和定义适用于本文件。

3.1
卡片验证码2 card verified number（CVN2）

在邮购/电话订购等非面对面交易中对银行卡卡片合法性进行验证的代码。

3.2
密钥加密密钥（KEK） key encryption key（KEK）

自助终端工作时对工作密钥进行加密的密钥。

3.3
工作密钥（WK） working key（WK）

在自助终端正常情况下，对PIN加密、参与MAC计算等的密钥。

3.4
自助服务 self-service

通过人机交互自主选择并获得所需服务的方式。

3.5
自动付款终端 unattended payment terminal（UPT）

由持卡人操作的设备或装置，在无人值守的环境中读取、捕捉和传输卡中的信息，提供自助服务功能，简称“自助终端”。

3.6
无人看护受理终端 Unattended Acceptance Terminal（UAT）

在无人看护环境下，由持卡人自助操作、能够读取和传输银行卡信息的设备，包括但是不限于以下几种设备：自动售票机、自动加油机、自动售卖机。

3.7
机柜 cabin

用于安装自动付款终端的机电部件的外壳。可以是一整台机子，也可以是包含所有自动付款终端界面装置的最小的可拆卸机柜或外壳。

3.8

现金取款机 cash dispenser

合法用户可实现取款等金融服务的自动柜员机。

3.9

现金存款机 cash deposit machine

合法用户可实现存款等金融服务的自动柜员机。

3.10

钓现 fishing

将任何形式的带有一个或多个钩子或其他装置的绳索、金属线或类似物品作用于自助服务终端，以非法获取现金。

3.11

暴力取现 forcing

用撬棍、螺丝起子、扳手、或其他类似工具扩大缝隙，或通过打破一个部件或使一个部件变形以获取现金。

3.12

断电保护

终端异常断电时，采取的数据不丢失、功能不损坏的措施。

4 自助终端硬件安全要求

4.1 硬件设计原则

硬件设计应遵循以下原则：

——自助终端应用在不同的场合时应分别具备防火、防盗、防尘、防淋、防震、防暴等要求，保证人身安全；

——配置的密封装置及门锁应耐久、安全、可靠，应符合GA/T 73的要求，对异常情况有报警及日志记录功能；

——硬件系统和各模块单元的逻辑设计应尽量采用统一校验等技术，并留有适当的逻辑余量；

——硬件系统应具有一定的自检功能。产品的零部件应紧固无松动；

——框架和机柜应有一定的刚度和强度，以防止由于空间变动、部件变松或移位造成的全部或部分损坏，并应防止和减少部件发生火灾、电冲击和人身伤害的可能性；

——外形应具备人性化特点，客户操作应感到舒适方便，并应具备人文特征；

——安全模块需遵循严格的密钥机制，保证持卡人磁道信息、PIN等账户信息的安全。

4.2 电气安全

自助终端的电气安全要求应符合GB 4943.1的有关规定。

4.3 抗破坏能力

自助终端的抗破坏能力应满足附录C的有关要求。

4.4 抗破坏报警

自助终端遇到非操作员、非管理员开启机柜或遇到暴力攻击等非正常使用时，应能报警并有记录。

4.5 一机一钥

自助终端的机柜钥匙应当实现一机柜一钥匙，不能多机柜共用一把钥匙，简称“一机一钥”的要求。

4.6 读卡器等安全设备防移除

自助终端的读卡器等安全设备要防止恶意拆除，攻击和绕开该保护功能的机制至少需要18分，实施攻击分值至少9分。分值计算方式应符合JR/T 0120.5的要求。

4.7 防恶意窃卡机制

自助终端应具备安全机制，防止有目的地保留或偷取持卡人卡片（比如循环攻击）。

4.8 防渗透替换机制

不允许通过条件改变、替换或修改磁条卡读写器、自助终端的硬件软件，达到替换或者修改磁道数据的目的，至少需要16分值，实施攻击分至少8分。分值计算方式应符合JR/T 0120.5的要求。

4.9 其他

其他相关要求见附录A。

5 自助终端软件安全要求

5.1 软件设计原则

软件设计应遵循以下原则：

——自助终端的软件设计应与硬件系统的硬件资源相适应；

——除应用软件外，还应配备完善的测试（诊断）软件；

——对同一系列的产品，软件应遵循通用化、系列化、模块化和向下兼容的原则；

——应用软件需保密的参数与文件以及数据传输过程中需保密的数据，均应经过数据安全模块处理；

——软件的文件技术规范以及字符集中字符的编码、字型等都应符合相应的国家标准。

5.2 系统软件

应具有系统初始化，对软件、硬件的自检及报警功能，具备断电保护功能，并方便应用程序的加载和参数设定。

5.3 二次开发平台

提供高级语言（如C语言）开发环境，提供二次开发专用接口，并提供应用模块，具备应用程序的调试和测试环境。

5.4 模块化结构

支持模块化结构设计，软件应封装成几个相对独立、性能稳定的模块，供应用开发者使用。

5.5 其他

其他相关要求参见附录B。

6 自助终端逻辑安全要求

6.1 非PIN数据输入

如果自助终端的密码键盘需要输入非PIN数据，那么至少要满足以下条件的一个：

——提示信息由加密单元控制：

输入非PIN数据时设备显示的提示内容应在安全模块的控制下，对非PIN数据的攻击至少需要18分攻击分值，实施攻击分至少9分。 如果该提示内容是存储在安全模块内部，那么改变该提示内容会导致安全模块内密钥的擦除。如果该提示内容是存储在安全模块外部，那么设备安全机制要保证提示内容的完整性、正确使用和不被非法修改或使用。

——改变用户界面提示攻击可能性分析：

在未授权情况下，改变非PIN数据输入时显示的提示内容危及PIN安全（例如：当输出信息不加密时提示输入PIN）的攻击至少需要16分的攻击分值。分值计算方式应符合JR/T 0120.5的要求。

——安全模式：

自助终端应确保持卡人可见信息与操作状态之间的关联关系。

6.2 多应用

如果自助终端支持多个应用程序，则应能够将这些程序分离开来。一个应用程序不能干扰或篡改另外一个应用程序或自助终端的操作系统，包括修改属于另外一个程序的数据对象。

6.3 操作系统

自助终端操作系统只能包含设计应用用途所必需的零部件和服务。应以最少的特权来配置和运行。

6.4 单一的PIN数据接口

自助终端只能通过一个单独的接口接收PIN数据，如果另外有一个键盘，应阻止通过这个接口接收PIN数据。

6.5 卡号屏蔽要求

自助终端凭证宜将持卡人关注内容醒目表示，具体位置不作要求，对涉及现金和账户变化的异常情况，宜打印凭证，以方便客户。交易凭证打印的卡号，除被吞卡和转账交易的转入卡外，应对卡号进行屏蔽，屏蔽方式为隐去卡号校验位前4位数字，如62220123456789****6。

7 ATM终端安全要求

7.1 ATM基本安全要求

ATM终端在遵循上述自助终端硬件、软件、逻辑安全要求基础上，同时应遵循本章其他安全要求。

ATM终端应用程序、各模块驱动程序应采取有效措施防范缓冲区溢出漏洞等问题，应具备容错能力，应采取措施防止攻击者利用程序错误进入桌面系统，应定期对应用程序进行安全测试。

ATM终端程序升级时应进行严格的签名验证，防止恶意程序被安装。

ATM终端设备应具备异常状态检测报警机制，当检测到终端设备存在异常时，应及时报警并停止服务。

无人值守的ATM终端应定期进行安全检查，检查终端按键区域、读卡器等组件是否被恶意改造。

应采用物理保护手段，防止ATM终端的网线或者网络接口裸露在外。

7.2 加密要求

应采取措施保障从ATM终端到所连ATMP的数据传输不泄漏银行卡信息。

采用安全可控的密码算法，保证ATM交易数据的完整性和机密性，应支持SM2、SM3、SM4、RSA、SHA、3DES等。SM算法见GM/T 0002、GM/T 0003、GM/T 0004、GM/T 0009；密码算法应保证ATM终端交易数据的安全性。PIN要求用硬加密，PIN处理的原则和要求见GB/T 21078.1。

7.3 密钥管理

7.3.1 二级密钥体系

密钥体系应不少于二级，ATM终端密钥分为二级：密钥加密密钥（KEK）和工作密钥（WK）。

7.3.2 密钥加密密钥（KEK）

KEK用于对工作密钥（WK）进行加密保护，每台ATM终端有唯一的KEK。

KEK应有安全保护措施（如采用分量输入方式、远程密钥加载方式等）。只能写入并参与运算，不能被读取。

7.3.3 工作密钥（WK）

ATM终端采用三种工作密钥用于数据的加解密，即对个人识别码（PIN）加解密的PIN密钥（PIK），计算报文鉴别码（MAC）的MAC密钥（MAK）和对磁道信息加解密的磁道加密密钥（TDK）。

ATM终端工作密钥在下载时和传输时都应以密文方式出现，不应明文传送。

7.4 通讯要求

ATM终端内部各关键模块间通讯时，应采取严格的双向验证机制，防止伪造请求。吐钞模块应当对请求指令的来源和合法性进行严格验证。

ATM终端的外设接口应严格限制使用，对USB、串口等通讯接口应采取严格的控制措施，防止通过外设接口植入木马等恶意程序。

ATM终端与后台服务器信息交互时，应使用强壮的加密算法和安全协议保护敏感数据在网络上的传输安全，并且应采取双向认证等方式，对交易报文进行合法性验证，防范中间人攻击。

7.5 操作系统要求

ATM终端操作系统应定期维护更新，及时安装系统补丁，部署防病毒程序，并采取白名单等方式，禁止非法程序执行。定期对操作系统安全性进行测试。操作系统应最小化安装，关闭不安全、不必要的服务。ATM终端在进入维护模式时应采取多因素验证等方式。

7.6 其他要求

银行卡敏感数据信息（如完整的磁道信息、PIN、卡片验证码及卡片有效期等）不能在ATM终端中保存。

对银行卡操作（特别是非接触操作）进行蜂鸣、指示灯、语音、文字、画面等提示。例如，在非接读卡器放卡或移卡操作时进行提示。

对于接触式受理情况，如果交易处理失败且响应码要求吞卡，则ATM终端应执行吞卡操作，同时打印客户凭证。交易环节中应有相应的安全提示和安全警示（例如：个人密码输入界面宜增加密码防窥提示，交易结束宜增加客户取卡提示）。如果在交易进行过程中，持卡人在限定时间内没有任何操作，则应将银行卡退回至入卡口，同时提示持卡人取卡。如果在限定时间内持卡人未将银行卡从入卡口取走，则应执行吞卡操作，并给予客户相应提示信息。对于非指令性的吞卡，银行可经过客户信息验证后，即时通过设备端返还吞卡。

对于非接触式受理情况，由于机具无法执行吞卡操作，为避免引起持卡人误解，发卡机构不应对非接触式受理的情况返回吞卡指令。

电子日志类信息应具备保护机制。

银行卡信息可采用人体生物特征识别技术增强其安全性。

附 录 A
（资料性附录）
自助终端硬件要求

A.1 外观和结构

自助终端的外观和结构应满足以下条件：

——自助终端的外型结构尺寸由产品规范规定；

——自助终端表面不应有明显的凹痕、划伤、裂缝、变形和污染等，表面涂镀层应均匀，不应起泡、龟裂、脱落和磨损，金属零部件不应有锈蚀及其他机械损伤；

——自助终端的零部件应紧固无松动，键盘、开关及其他活动部件的动作应灵活可靠。

A.2 电源模块

A.2.1 UPS 电源

具体指标由产品规范规定，但应符合GB/T 14715的规定，另外还应具备以下功能：

——模拟正弦波输出，可电池启动；

——具有电池稳压功能（AVR）；

——具有输出短路保护及过载保护；

——具有全天候防雷击、噪声及突波保护。

A.2.2 开关电源

具体指标由产品规范规定。

A.2.3 加热模块

具体指标由产品规范规定，且应具备以下功能：

——低温加热自动升温功能；

——过热保护自动切断功能；

——温度降低再次启动加热升温功能。

A.2.4 高温强排模块

具体指标由产品规范规定。

A.3 终端控制模块

多媒体计算机的类型、主要配置和性能由产品规范规定。

A.4 显示模块

要求防刮、防尘、防水，显示器的规格、种类及分辨率等由产品规范规定。 亮度≥350 lx。

A.5 输入模块

具体指标由产品规范规定。

A.5.1 键盘使用寿命

主机键盘、密码键盘的使用寿命应符合GB/T 14081—1993、GB/T 18031—2000的规定。

A.5.2 触摸屏输入

触摸反应时间≤20ms；透光率≥95%；单点触摸大于或等于3500万次的使用寿命（正常情况下使用）。

A.6 卡处理模块

磁卡处理应符合GB/T 15120的规定。

IC 卡处理符合GB/T 14916、GB/T 16649.1、GB/T 16649.2、GB/T 16649.3 的要求。非接触卡读写模块应符合ISO 14443 Type A/B要求。

A.7 PSAM 卡模块

可用于产品安全控制模块，符合《中国人民银行PSAM 卡规范》，具体指标由产品规范规定。

A.8 打印模块

具体指标由产品规范规定。应具备以下模块：

——票据打印模块；

——凭条打印模块；

——日志打印模块；

——报表打印模块。

A.9 存折页码识别模块

扫描用以标识银行存折页码的条码信息，提供给上位机处理的模块。

A.10 保险柜

保险柜应至少配置一把密码锁，密码锁可为机械密码锁或电子密码锁。密码应可调，调码应操作方便、可靠。机械锁具应符合GA/T 73的有关要求；电子密码锁应符合GB 10409要求。保险柜应符合GB 10409要求。

A.11 监视设备

自助终端如配备监视摄像机，其安装位置应确保摄像机镜头对准自助终端前方的使用者，但不应摄入用户的键盘操作动作。

A.12 红外线探头

可用于进入自助终端时启动界面，具体指标由产品规范规定。

A.13 智能灯控

可用于进入自助终端时启动照明部件，具体指标由产品规范规定。

A.14 其他

以下模块具体指标由产品规范规定：

——纸币出钞模块；
——硬币出钞模块；
——纸币识别模块；
——硬币识别模块；
——存款模块；
——通信模块；
——多媒体模块；
——身份认证模块；
——票卡发行模块；
——图像输出模块；
——存储卡读写模块；
——客户服务模块；
——后台维护模块；
——数据安全模块；
——安全监控模块；
——报警模块。

A.15 接口要求

A.15.1 IC卡接口

自助终端应提供符合GB/T 6107规范的IC卡接口。

A.15.2 串行接口

串行接口规范应符合GB/T 6107的规定（对于最大20 kbit/s 的数据信号速率的操作）或GB/T 17183（对于大于20 kbit/s 的数据信号速率的操作）要求的通信接口，支持ASYNCH或SYNC 数据传输，支持多种通信协议（如：X.25、SDLC、TCP/IP 等），具体通信协议由产品规范规定；

A.15.3 银行卡接口

自助终端使用银行卡接口的物理要求、电气要求和传递协议如下：

——物理要求：

卡接口的尺寸应满足银行卡的尺寸要求，触点技术要求按照GB/T 16649.1的规定。

——电气要求：

自助终端与银行卡接口的电气特性应满足GB/T 16649.3有关规定。

——传递协议：

自助终端与银行卡的数据交换采用T=0面向字符的异步半双工传递协议或T=1面向字节的异步半双工传递协议。

A.15.4 其他接口

如USB等其他接口，连接诸如IC 卡或磁卡读卡机、票据打印机、网络接口等部件的接口，应符合国家关于各种接口的有关的规定。

A.16 电源适应性

自助终端应在频率50 Hz±1 Hz，电压AC 187V～253V的条件下正常工作。

A.17 设备安装要求

设备稳定性需符合GB 4943.1—2011中4.1的要求。

A.18 噪声

自助终端主机工作在空闲状态（开机后的稳定无操作状态）下，产品声功率不超过5.5Bel。

A.19 电磁兼容性

A.19.1 无线电骚扰限值

自助终端的无线电骚扰限值应符合GB 9254的规定。在产品规范中应明确规定选用 A级或 B 级所规定的无线电骚扰限值。

A.19.2 抗扰度限值

自助终端的抗扰度限值应符合 GB/T 17618的规定。

A.19.3 谐波电流限值

自助终端的谐波电流限值应符合GB 17625.1的有关规定。

A.20 环境条件

气候环境适应性、盐雾环境、流动混合气体腐蚀、模拟地面上的太阳辐射等具体的要求由产品规范规定。

A.21 可靠性

采用平均失效间工作时间(MTBF，Mean Time Between Failure)衡量系统的可靠性水平。自助终端的平均失效间工作时间(MTBF)的m1≥6000h。

附 录 B
（资料性附录）
自助终端软件要求

B.1 功能

自助终端具体的功能实现由应用规范明确规定，至少要满足表B.1中的一个或多个功能。

表 B.1 自助终端服务功能分类

功能分类		功能举例
服务功能	查询	
	取款/存款	
	交易	售票、售卡、售货、缴费、充值、转账服务
	打印	账单/详单/发票打印
	信息发布	文字、图片、视频、音频
	其他	业务体验
安全鉴别	身份识别	用户合法身份识别、维护人员合法身份识别
	数据安全	加/解密、保存密钥、数据合法性检查
管理功能	系统设置	日期及时间、机号信息、日志记录及转储
	数据管理	数据统计、数据备份、日志记录及转储
	系统自检	
	检查系统状态	
	应用安全管理	对应用运行的安全和发行认证管理
	远程监控	
其他	中/英文操作界面	
	联/脱机运行	

B.2 中文信息处理

B.2.1 字符集

自助终端的汉字字符应符合GB 13000.1和GB 18030的规定。

B.2.2 输出用汉字字型

自助终端应采用国家标准或行业标准规定的点阵汉字字型，其采用的汉字至少应符合下述标准：
——显示用字型不应采用低于15×16 点阵的字型，应符合GB 5199、GB 17698；
——打印用字型不应采用低于24×24 点阵的字型，应符合GB 5007.1、GB 16793；
——曲线汉字字型，其对简省笔划的处理应与相应尺寸的点阵汉字字型一致。

B.2.3 汉语词库

自助终端配备的汉语词库应优先采用GB/T 15732规定的词库。在GB/T 15732的基础上扩充的词汇应符合我国语言文字规范或习惯，并应有该词汇来源的依据。

附 录 C
（规范性附录）
抗破坏能力

C.1 目的

抗破坏性能力试验的目的：

——试验的目的是检验自助终端的抗破坏能力。试验人员可在试验程序的范围内选择一系列攻击，并且在试验时间内尝试每个攻击方案。如果自助终端在指定的净工作时间内，在指定的点或面上，能够抵抗最严酷的攻击方法或几种攻击方法的最佳组合，那么该项试验可以通过；

——净工作时间是指对样品进行破坏的时间，不包括测试的准备时间、安全防范所需的时间、以及不可预期的延误时间；

——除了设陷取现，成功的攻击应该在特定的时间内，移走自助终端内至少10%的现金，或将现金暴露在外，以致现金都可以被移走；

——设陷取现应能成功地进行三次取现而不被发现或不打断自助终端的运行。设陷取现可以在操作中进行调节；

——所有的攻击应该由熟悉设计的一个或两个有经验的人员来进行。

C.2 用户界面的试验-24h 服务式

C.2.1 概述

提供24h服务的自助终端对通过用户界面采用钓现、设陷取现及暴力取现的各种企图应能抵抗30min。

所有的试验只限于在用户界面上所进行的攻击。

C.2.2 工具

试验中的攻击过程是相对安静的，其中所用的工具仅限于能被藏于两个试验人员衣服内的绳索、金属丝、钩子、撬棍、扳钳、螺丝刀、钢锯片及其类似工具。除像绳索、金属丝、钩子那样可被卷起或被折叠的工具外，其他工具的长度不应超过0.6m。

C.2.3 时间

一次试验可选用多种攻击方式，每种攻击可进行30min。

每种攻击方式只可进行一次。如果两种攻击共用了30min，那么第一种攻击所造成的破坏可延用在第二种攻击中。

C.2.4 方法

钓现、暴力取现、设陷取现是由自助终端的设计所决定的。

在试验中，只使用不超过1.4kg 重的锤子，或与长度不超过0.6m的凿子、钻孔机及螺丝刀等一起使用的时间最长不超过30s。

C.3 保险柜的试验——24h 服务式

C.3.1 概述

概述说明如下：

——C.3.4 中所述的任何一种或全部攻击方式均可选作从保险柜中取现的方法；

——样机的门间隙应代表以后生产产品的最大门间隙；

——提供附有材料规格的完整结构图；

——随样机应有两个按金属材料的拉伸测试GB 228中所定的抗张力试验样品，此试验样品直径为12.7mm，长为50.8mm，并用制造样机门及机壳所用的钢所制成的；

——如果所用材料不是钢，则不需提供这些样品。

C.3.2 工具

工具说明如下：

——试验工具包括普通的手持工具、机械式或便携式电动工具、锉、硬质合金钻、挖凿工具，但不包括磁性钻床及其他应用压力的机械、砂轮和电锯；

——普通的手持工具为重量不超过 3.6kg 的凿子、冲具、扳钳、螺丝刀、锤子及撬杆，长度不超过 1.5m的撬棍及割锯工具，以及套筒；

——挖凿工具为普通型或标准型，但不应被特别设计用于一个特别的产品。便携式电动工具指规格为 12.7mm的高速手持电钻。

C.3.3 时间

时间说明如下：

——24h 服务式的保险柜应能抵抗15min破坏攻击。可选用C.3.4中所述的一种方法或所有方法，采用指定的工具，每种方法可持续15min；

——每种攻击方法只可进行一次。如果两种攻击共用了15min，那么第一种攻击所造成的破坏可延用在第二种攻击中；

——保险柜应该如正常营业时一样装载现金。成功的攻击以满足C.1中所述的要求为准。

C.3.4 方法

方法说明如下：

——打孔和钻孔的组合——通过用凿掘工具、金属线、钩子或其他的普通手持工具敲掉密码锁的拨号盘，在转轴上打孔或钻孔以打开锁紧机构；

——锁紧机构——试图接近锁盒、接线片、拨杆或其他机械部分，通过打孔、撬凿或切断来松开锁舌；

——锁舌——通过门上的开口切断或移动主要锁舌使其脱离连接；

——切断锁舌——刺穿门的旁柱并切断主要锁舌；

——通过打孔、钻孔来开锁——通过在密码拨号盘轴上打孔、钻孔，同时用力转动门把手以打开锁紧机构，也可以用挖凿工具或其他的手持工具打开锁紧机构；

——把手施力——通过扳手或金属杆在门闩操作杆上加力，以旋转门闩把手，或通过在门闩把手上打孔，使锁被打开；

——撬开或劈开门——用楔子、凿子和撬刺破或打开门以取走现金；

——开口——通过在保险柜上钻一圈很密的孔，然后用铁锤凿开这部分金属，以在保险柜上打出一个洞；

——保险柜边缝——通过保险柜设计中的上边缝、侧边缝及下边缝用暴力打开保险柜并从其中钓现。不能使用电动、风动以及类似的能源驱动的工具攻击保险柜。