ICS 35.030
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0106—2021

银行卡终端产品密码应用技术要求

Cryptograph application requirements for bank card terminal

2021-10-18 发布　　2022-05-01 实施

国家密码管理局　　发 布

中华人民共和国密码
行业标准
银行卡终端产品密码应用技术要求
GM/T 0106—2021
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2022年7月第一版
*
书号:155066·2-36721

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。

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。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：东方通信股份有限公司、福建联迪商用设备有限公司、恒银金融科技股份有限公司、广电运通金融电子股份有限公司、长城信息产业股份有限公司、深圳市证通电子股份有限公司、国家密码管理局商用密码检测中心。

本文件主要起草人：刘俐训、徐盛舟、戴永峰、罗伟、李大为、邓开勇、罗鹏、李国友、吕景丽、耿佳、高志权、于海涛、雷正生、高晓飞、马兴旺。

引　言

本文件描述了银行卡终端产品上的密码技术应用要求。

银行卡终端产品是受理银行卡业务的设备，包括自动柜员机(ATM)、销售点终端(POS)、移动销售点终端(mPOS)等产品形态。这些设备中的账号、磁道信息、个人识别码和密钥等敏感数据的关系持卡人资金安全，设备中这些数据的安全一般依赖于密码技术进行保护。

为了提高银行卡终端产品风险防控能力，进一步加强和保障持卡人隐私信息安全，助力金融支付业务的安全发展，密钥技术在银行卡终端上的规范化应用应作为关键工作进行开展。

按照全面性原则，密码技术的规范化应用方法要适用于新设备并考虑存量旧设备，使之通过有条件的升级改造也可以达到设备安全提升的目的。

目前具有指导银行卡终端产品进行密码技术规范化改造和升级的标准尚不完善，亟需提出标准化文件。

银行卡终端产品密码应用技术要求

1 范围

本文件规定了银行卡终端产品上密码应用相关的技术要求，包括终端基本安全要求、终端密钥管理要求、终端数据安全要求以及密码算法正确性和性能要求。

本文件适用于银行卡终端产品上密码技术的应用，使用对象主要是与密码技术应用相关的银行卡终端产品设计、制造、使用等单位，以及需要对存量银行卡终端产品进行密码应用技术改造升级的相关单位。

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。

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

GB/T 21078.2 银行业务 个人识别码的管理与安全 第2部分：ATM和POS系统中脱机PIN处理的要求

GB/T 27909(所有部分) 银行业务 密钥管理(零售)

GB/T 32905 信息安全技术 SM3密码杂凑算法

GB/T 32907 信息安全技术 SM4分组密码算法

GB/T 32915 信息安全技术 二元序列随机性检测规范

GB/T 32918(所有部分) 信息安全技术 SM2椭圆曲线公钥密码算法

GB/T 32918.3—2016 信息安全技术 SM2椭圆曲线公钥密码算法 第3部分：密钥交换协议

GM/T 0008 安全芯片密码检测准则

GM/T 0028—2014 密码模块安全技术要求

GM/Z 4001 密码术语

JR/T 0025.6 中国金融集成电路(IC)卡规范 第6部分：借记/贷记应用终端规范

JR/T 0025.7 中国金融集成电路(IC)卡规范 第7部分：借记/贷记应用安全规范

JR/T 0055(所有部分) 银行卡联网联合技术规范

JR/T 0120.1 银行卡受理终端安全规范 第1部分：销售点(POS)终端

JR/T 0120.3 银行卡受理终端安全规范 第3部分：自助终端

JR/T 0120.5 银行卡受理终端安全规范 第5部分：PIN输入设备

ANSI X9.24(所有部分) 零售金融业务 对称密钥管理

3 术语和定义

GM/Z 4001和GM/T 0028界定的以及下列术语和定义适用于本文件。

3.1

现金处理模块 cash handling module

自动柜员机(ATM)的出钞模块或现金循环模块。