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

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。

3.2

银行卡终端　bank card terminal

终端　terminal

受理银行卡业务的商用设备，如 ATM、POS、mPOS 等产品。

3.3

出钞密码认证模块　cash dispense cryptographic authentication module

一种 ATM 上控制现金处理模块访问权限的独立硬件密码模块或硬件功能单元。

3.4

使用授权　use authorization

密码技术控制下访问密码模块敏感功能的权限认证。

3.5

双重控制　dual control

采用两个或以上独立实体（通常是人）协同去保护敏感数据或限制敏感功能访问的机制，单一实体无法获取敏感数据或访问敏感功能。

3.6

PIN 数据块　PIN block

经过填充后的含有个人身份识别码的数据块。

3.7

敏感功能　sensitive function

包含敏感数据，能影响终端密码安全的功能。

3.8

敏感服务状态　sensitive service state

可使用敏感功能的状态。

3.9

工作密钥　working key

在银行卡终端正常情况下，对 PIN 加密、参与 MAC 计算等的密钥。

3.10

安全通信密钥　secure communication key

用于终端内密码模块之间通信加密的对称密钥。

3.11

根公钥　root public key

认证中心（CA）的公钥，常用于验证认证中心给自己、下级认证中心或其他客户颁发的公钥证书或公钥签名。

3.12

根证书　root certificate

认证中心（CA）给自己颁发的未被签名的或自签名的公钥证书，是信任链的起始点。

3.13

PIN 输入设备　PIN entry device；PED

支持个人身份识别码输入的密码模块，如密码键盘 EPP、外置密码键盘等。

3.14

密码键盘　encrypting pin pad；EPP

接受用户 PIN 输入和提供终端所需密码服务的密码模块。

3.15

外置密码键盘　external encrypted pin pad

用于金融支付领域的 PIN 输入设备，该设备可以是 POS，也可以是常用于连接 POS 受理银行卡业

务的密码键盘等。

3.16

保险柜　safety box

ATM 内部安放现金处理模块的装置，用于物理上保护现金处理模块和现金的安全。

4　缩略语

下列缩略语适用于本文件。

ATM：自动柜员机（Automatic Teller Machine）

CA：认证中心（Certificate Authority）

CBC：密码分组链接（Cipher Block Chaining）

ECB：电子译码本（Electronic Code Book）

EPP：密码键盘（Encrypted Pin Pad）

Kbps：千比特每秒（Kilo Bit Per Second）

MAC：报文鉴别码（Message Authentication Code）

MAK：MAC 计算密钥（MAC Key）

MK：主密钥（Master Key）

mPOS：移动销售终端（Mobile Point Of Sale）

PAN：主账号（Primary Account Number）

PIK：PIN 加密密钥（PIN Key）

PIN：个人身份识别码（Personal Identification Number）

PK：公开密钥（Public Key）

POS：销售点终端（Point Of Sale）

RKL：远程密钥装载（Remote Key Loading）

SK：私密密钥（Secret Key）

TDK：磁道数据加密密钥（Track Data Key）

TMK：终端主密钥（Terminal Master Key）

5　终端基本安全要求

5.1　概述

本章规定了银行卡终端产品应遵循的基本要求和相关标准，包含银行卡终端及其密码模块在硬件、物理安全、逻辑安全和业务功能等方面的要求，是实施密码技术应用的基础。

5.2　终端基本要求

5.2.1　概述

银行卡终端产品是受理银行卡业务的终端设备，包括销售点终端（POS）类产品（POS、mPOS、智能 POS 等）和自动柜员机（ATM）类产品（ATM、金融自助设备等）。银行卡终端应包含密码模块，如包含密码键盘、外置密码键盘等，也可以本身就是一个密码模块。

5.2.2　通用要求

应符合 JR/T 0025.6—2018、JR/T 0025.7—2018 的规定。

应符合 GM/T 0028—2014 的规定并划分密码边界。

应支持 GB/T 32905、GB/T 32907、GB/T 32918(所有部分)给出的密码算法,这些密码算法应由终端的密码模块执行。

5.2.3 POS 类终端要求

应符合 JR/T 0120.1 的规定。

5.2.4 ATM 类终端要求

应符合 JR/T 0120.3 的规定。

5.3 密码模块要求

银行卡终端产品上的密码模块应符合 GM/T 0028 规定的安全要求并达到安全一级或更高安全等级。应具备随机数生成功能,并支持符合 GB/T 32905、GB/T 32907、GB/T 32918 规定的密码算法。这些密码算法应由安全芯片提供。密码模块应使用国家密码管理主管部门认可的安全芯片,安全芯片安全等级应达到 GM/T 0008 规定的安全等级 2。

银行卡终端可包含多个密码模块,如果密码模块之间需要进行数据交换,应保证敏感数据机密性和完整性,如使用安全通信密钥加密和带有消息鉴别码(MAC)的方式通信。

6 终端密钥管理要求

6.1 密钥分类

本文件涉及的密钥按照密钥形式可分为对称密钥和非对称密钥,按照密钥用途可分为业务类密钥和终端安全类密钥。业务类密钥用于保证终端交易处理过程及数据的安全,终端安全类密钥用于保证终端内各种敏感数据的安全。终端中可能存在的密钥种类见表 1。

表 1 银行卡终端密钥分类

密钥形式	密钥分类	密钥名称	用途	存在条件	
				POS 类	ATM 类
对称密钥	业务类密钥	终端主密钥(TMK)	用于对密钥加密密钥或工作密钥进行加密保护	应存在	可选
		密钥加密密钥(KEK)	用于对工作密钥进行加密保护	可选	应存在
		工作密钥(WK)	包括 PIN 加密密钥、MAC 密钥、数据加密密钥等	应存在	应存在
	终端安全类密钥	固件验证密钥	用于软件/固件完整性、真实性验证	应存在	应存在
		SM4 算法自检密钥	用于 SM4 密码算法的开机自检和周期自检	应存在	应存在
		授权认证密钥	用于敏感功能使用授权	应存在	应存在
		安全通信密钥	用于终端内多个密码模块之间的安全通信	可选	可选
		出钞安全密钥	用于保证 ATM 出钞安全	可选	应存在

表 1　银行卡终端密钥分类（续）

密钥形式	密钥分类	密钥名称	用途	存在条件	
				POS 类	ATM 类
非对称密钥	业务类密钥	认证中心公钥	用于脱机数据认证	应存在	可选
		认证中心公钥维护密钥	用于导入、更新和撤回认证中心公钥	应存在	可选
非对称密钥	终端安全类密钥	RKL 认证中心公钥	用于远程密钥装载	可选	可选
		密码模块公私钥对	用于远程密钥装载	可选	可选
		固件验证密钥	用于软件/固件完整性、真实性验证	应存在	应存在
		SM2 算法自检密钥对	用于 SM2 密码算法的开机自检和周期自检	应存在	应存在
		授权认证密钥	用于敏感功能使用授权	应存在	应存在
		出钞安全密钥	用于保证 ATM 出钞安全	可选	应存在
注：固件验证密钥、授权认证密钥、出钞安全密钥的密钥形式可选对称密钥或非对称密钥					

6.2　通用管理要求

终端应对终端中存在的密钥进行生命周期管理，包括密钥生成、密钥分散、密钥传输、密钥导入、密钥存储、密钥备份、密钥归档、密钥销毁等。

终端基本密钥生命周期管理应符合 GB/T 27909（所有部分）和/或 ANSI X9.24（所有部分）的规定。

终端所有密钥应存储在密码模块中，密钥应只可在密码模块中被使用。

6.3　业务类密钥管理

6.3.1　密钥体系

银行卡终端用于联机交易的密钥体系应不少于二级。

POS 类终端常采用二级密钥体系：终端主密钥（TMK）和工作密钥（WK）。

ATM 类终端常采用二级密钥体系：密钥加密密钥（KEK）和工作密钥（WK）。

密钥体系应支持符合 GB/T 32907 规定的密码算法。

6.3.2　终端主密钥管理

终端主密钥（TMK）在 POS 类终端上用于对工作密钥（WK）进行加密保护，每台 POS 类终端应有唯一的 TMK。

TMK 应使用密码技术手段导入 POS 类终端，如通过其他密码设备（POS 密钥机、IC 卡等）加密导入，也可采用基于 SM2 密码算法的远程密钥装载方式导入，导入时应保证密钥的完整性和机密性。

6.3.3　密钥加密密钥管理

密钥加密密钥（KEK）在 ATM 类终端的上用于对工作密钥（WK）进行加密保护，是 ATM 类终端密钥体系中的一级密钥，每台 ATM 类终端应有唯一的 KEK。

KEK 应采用双重控制方式导入，即通过口令的方法对至少两个密钥管理员进行鉴别，鉴别通过后

密钥管理员输入各自执有的密钥分量，密钥分量在密码模块内组合形成 KEK 并保存。

KEK 可采用远程密钥装载（RKL）方式导入，远程导入方式参见附录 B 或符合 GB/T 32918.3—2016 的规定。

6.3.4 工作密钥管理

终端应包含用于个人识别码（PIN）加密的 PIK，计算报文鉴别码（MAC）的 MAK 和对磁道数据加解密的 TDK 三种工作密钥。

工作密钥应使用 TMK 或 KEK 加密后以密文传输和导入，每一种工作密钥应只可被用于一种用途。

6.3.5 认证中心公钥管理

见 JR/T 0025.7。

6.3.6 认证中心公钥维护密钥管理

见 JR/T 0025.7。

6.4 终端安全类密钥管理

终端安全类密钥管理应符合以下生命周期管理方法：

——密钥生成：对称密钥应由密码模块使用随机数方式生成，非对称密钥应采用 GB/T 32918 规定的密钥生成算法生成；

——密钥导入：RKL 认证中心公钥导入时应验证公钥完整性，其他终端安全类密钥生成后存储在密码模块中，无需导入；

——密钥存储：密钥应保存在密码模块中，除密码模块公钥外，不应以明文形式出现在密码模块之外；

——密钥使用：应在密码模块中使用，每种密钥应只有一种用途；

——密钥导出：除密码模块公钥外，其他密钥应不可导出；

——密钥更换：应采用删除旧密钥后重新生成的方式进行密钥更换；

——密钥删除：应由密码模块固件控制删除；

——密钥销毁：密码模块检测到入侵时销毁。

7 终端数据安全要求

7.1 概述

本章规定了使用密码技术保护终端内敏感数据的方法和要求，其他未使用密码技术保护的数据和安全要求本文件不做规定。

7.2 密钥

密钥数据安全管理要求见第 6 章。

7.3 随机数

终端内的随机数应由安全芯片中的随机数发生器生成，并依据 GB/T 32915 检测合格。

7.4 软件和固件

银行卡终端内软件和/或固件应使用认可的数字签名或带密钥的消息鉴别码进行保护，即应符合GM/T 0028—2014规定的软件/固件安全二级要求。如果终端内的软件和固件完整性验证失败，终端应立即停止服务并报错。

如果支持软件和/或固件更新，密码模块应使用认可的数字签名算法或带密钥的消息鉴别码验证更新数据的正确性、完整性和真实性，如果验证失败，终端应拒绝进行软件和/或固件更新，或清除模块中的所有密钥。如果验证成功，新的软件和/或固件在提供敏感服务前应按照7.6的要求进行自检。

固件验证密钥管理要求见6.4。

7.5 账户数据

账户数据包括完整磁道信息、PIN、卡片验证码、卡片有效期等敏感数据，在终端密码模块之外不应以明文形式出现，应保证数据在处理和传输过程中不被泄露、窃取和篡改。

联机PIN管理和保护应符合GB/T 21078.1的规定。

脱机PIN管理和保护应符合GB/T 21078.2的规定。

终端应具备PIN防穷举功能，应限制PIN加密密钥使用频率不得高于每小时120次。

PIN Block加密应支持SM4分组密码算法，对应的PIN Block填充方法和加密方法按照附录A的规定。

7.6 自检

终端或密码模块应具备自检功能，每次运行前须进行自检，连续运行状态下则应在每24小时内至少执行一次自检，自检内容应包含但不限于以下内容：

a) 软件/固件完整性；

b) 密钥数据完整性；

c) 随机数发生器有效性；

d) 密码算法正确性。

如果自检失败，终端或密码模块应立刻停止提供密码服务。

自检使用的完整性验证技术应采用SM2数字签名算法或带有SM4密钥的MAC算法。

自检使用的密钥管理要求见6.4。

7.7 敏感功能使用授权

使用银行卡终端的敏感功能(如密钥管理、固件更新、PIN输入和加密等)前应进行使用授权认证，授权认证使用的密码算法应采用国家密码管理主管部门批准的算法，如SM2密码算法或SM4分组密码算法。

授权认证过程应不影响敏感数据安全，授权认证应有错误次数限制和超时控制。

7.8 联机交易报文

联机交易报文处理应符合JR/T 0055的规范，保证交易报文真实性、完整性，且应支持SM4分组密码算法计算的报文鉴别码(MAC)。支持SM4分组密码算法的报文接口改造方法和报文鉴别码计算方法参见Q/CUP 006。

7.9 脱机数据认证

见JR/T 0025.7。

7.10 出钞密码认证

ATM类终端产品一般具备现金处理功能，在其主控部件与现金处理模块之间宜建立安全通信机制来保证ATM内的现金安全，例如，主控部件与现金处理模块通信前应进行使用授权认证或采用密文通信。不具备认证或加密功能的现金处理模块宜在其与主控部件的通信链路上装置出钞密码认证模块。

如果终端支持现金处理模块和主控部件之间的认证功能，符合：

a) 应至少具备现金处理模块对主控部件进行单向认证功能，只有认证通过后，现金处理模块才可执行主控部件发送的取款、存款等现金处理命令；

b) 出钞密码认证模块宜安装在保险柜中，或符合GM/T 0028—2014中7.7规定的安全二级的要求。

c) 应使用国家密码管理主管部门批准的密码算法实现出钞密码安全功能，且具有防穷举、重放等攻击方式的能力，具体采用何种方法实现本文件不做规定。

8 密码算法正确性和性能要求

终端应保证密码算法由密码模块硬件完成。

应保证所有使用的密码算法的正确性，如果使用了一种密码算法中的多种工作模式(如分组密码算法的ECB，CBC)，应验证密码算法在这些工作模式下的正确性。

终端应通过上电自检和周期性自检的方式验证密码算法正确性，以保证密码模块处于正常状态。

终端应保证密码算法的稳定性和运算性能。如终端支持SM2算法验签功能，应保证验签速度不低于20次/s。

附 录 A
（规范性）
支持 SM4 算法的 PIN Block 填充和加密方法

A.1 概述

支持 SM4 算法的 PIN Block 填充方法以 ANSI X9.8 和 ISO 9564-1 为参考，并结合 Q/CUP 006 给出的方法，本附录给出了 PIN 和主账号的填充格式，填充后的 PIN 和填充后的主账号再进行异或运算（脱机交易可不异或填充后的主账号），得到 PIN Block。PIN Block 长度由原 64 位扩展为 128 位，PIN Block 加密算法使用国家密码管理主管部门认可的对称算法。

A.2 PIN 填充格式

使用 SM4 算法加密 PIN Block 时，PIN 应填充到 128 位的二进制数。其格式见图 A.1。

C	N	P	P	P	P	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F

C ——4-bit 控制码，%B0000。

N ——PIN 的长度（4-bit）。

P ——4-bit 二进制 PIN 的数码。

P/F——4-bit 二进制 PIN 的数码/FILLER。

F ——4-bit FILLER，%B1111。

图 A.1 PIN 填充格式

A.3 主账号填充格式

主账号填充格式见图 A.2 或图 A.3：

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12

0 ——4-bit 控制码，%B0000。

A1～A12——主账号的右 12 位（不包括最右边的校验位），主账号不足 12 位左补 0。

图 A.2 主账号填充格式 1（推荐）

0	0	0	0	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	0	0	0	0	0	0	0	0	0	0	0	0	0	0

0 ——4-bit 控制码，%B0000。

A1～A12——主账号的右 12 位(不包括最右边的校验位)，主账号不足 12 位左补 0。

图 A.3 主账号填充格式 2

A.4 PIN Block 填充示例

——示例 1(PIN 填充格式 1，不带主账号信息，仅脱机交易环境使用)

明文 PIN 123456，

则 PIN Block 为 0x06 0x12 0x34 0x56 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF

——示例 2(PIN 填充格式 1，带主账号信息格式 1)

PIN 明文：123456

磁卡上的 PAN：1234 5678 9012 3456 78

截取下的 PAN：6789 0123 4567

则用于 PIN 加密的 PAN 为：0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x67 0x89 0x01 0x23 0x45 0x67

则 PIN Block 为：0x06 0x12 0x34 0x56 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF

异或：0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x67 0x89 0x01 0x23 0x45 0x67

结果为：0x06 0x12 0x34 0x56 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0x98 0x76 0xFE 0xDC 0xBA 0x98

——示例 3(PIN 填充格式 1，带主账号信息格式 2)

PIN 明文：123456

磁卡上的 PAN：1234 5678 9012 3456 78

截取下的 PAN：6789 0123 4567

则用于 PIN 加密的 PAN 为：0x00 0x00 0x67 0x89 0x01 0x23 0x45 0x67 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00

则 PIN Block 为：

0x06 0x12 0x34 0x56 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF

异或：

0x00 0x00 0x67 0x89 0x01 0x23 0x45 0x67 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00

结果为：

0x06 0x12 0x53 0xDF 0xFE 0xDC 0xBA 0x98 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF

A.5 PIN Block 加密方法

根据 A.4 获得的 PIN Block，使用存储在密码模块中的 PIN 密钥加密，得到 PIN Block 密文，其中加密应使用 SM4 算法。

附 录 B
（资料性）
ATM 远程密钥装载（RKL）流程

B.1 概述

远程密钥装载（RKL）是指使用密码技术，远程主机（HOST）和 ATM 终端之间经过双向认证，将密钥（通常是密钥体系的最上层密钥）从远程主机安全的导入 ATM 终端的过程。

B.2 认证中心

认证中心（CA）拥有高级别安全性的加密设备，为远程主机和 ATM 终端的公钥签发公钥证书或公钥签名，同时对自己的公钥签发证书或签名。

B.3 目的

远程主机以安全的方式远程下载或更新 ATM 终端中密钥。

B.4 前提

远程密钥下载前，ATM 终端和远程主机应完成以下前提配置，见图 B.1 和图 B.2：

a） 远程主机已获得 CA 的公钥（PK_{CA}）。

b） 远程主机向 CA 提交公钥（PK_{HOST}），CA 使用自己的私钥（SK_{CA}）对远程主机提交的公钥签名，主机得到该公钥签名 $Sign(SK_{CA})[PK_{HOST}]$。

c） （可选）远程主机拥有合法 ATM 终端的 EPP 序列号的列表。CA 使用自己的私钥（SK_{CA}）对 EPP 序列号进行签名得到 $Sign(SK_{CA})[UI_{EPP}]$并载入 ATM 终端。

d） CA 将自己的公钥（PK_{CA}）载入 ATM 终端，并使用自身私钥（SK_{CA}）对 ATM 终端的公钥（PK_{ATM}）签名，得到 $Sign(SK_{CA})[PK_{ATM}]$并载入 ATM 终端。

e） ATM 终端内置自身公私钥对（PK_{ATM}和 SK_{ATM}）。

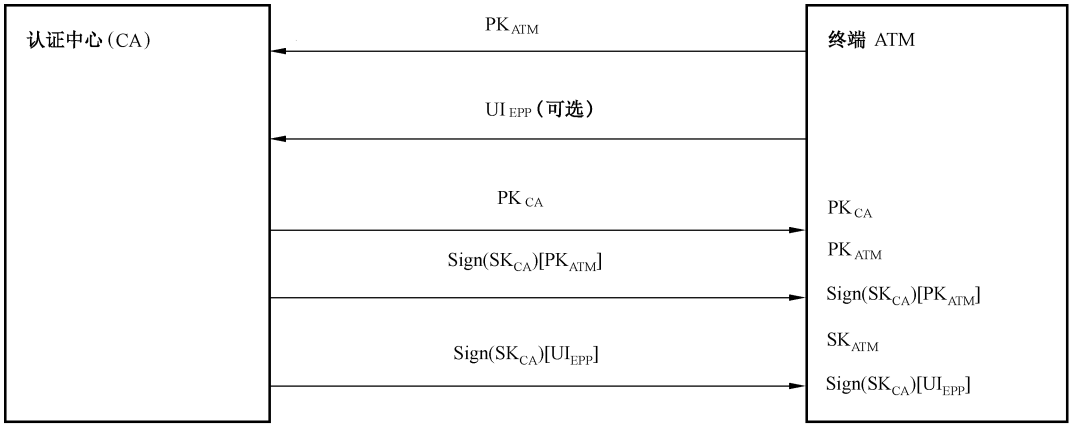

图 B.1 终端 ATM 前提配置

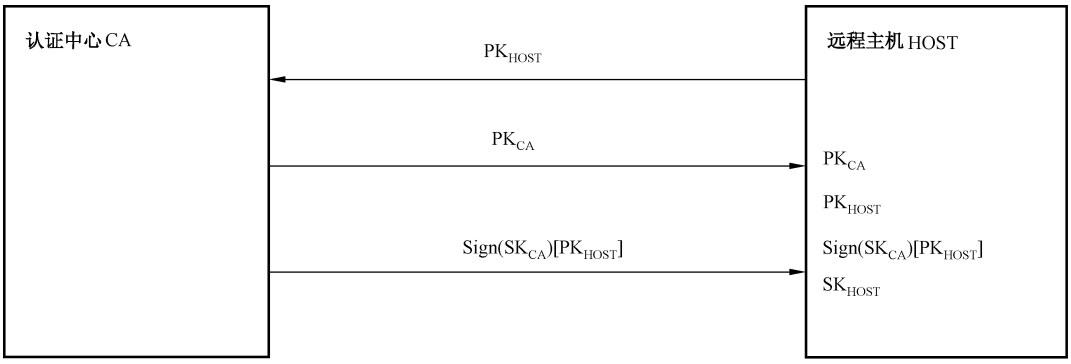

图 B.2　远程主机 HOST 前提配置

B.5　密钥装载流程

密钥装载按如下步骤执行，图示见图 B.3：

a）终端 ATM 将公钥（PK_{ATM}）和 CA 对公钥的签名 $Sign(SK_{CA})[PK_{ATM}]$ 发送到远程主机 HOST，远程主机使用 CA 的公钥（PK_{CA}）对接收到数据验签，验签通过后获得终端 ATM 的公钥（PK_{ATM}）；

b）（可选）远程主机 HOST 验证步骤 a）的公钥来自合法的 ATM 终端，方法是 ATM 终端发送 EPP 序列号 UI_{EPP} 和对应的签名 $Sign(SK_{CA})[UI_{EPP}]$ 到远程主机 HOST，远程主机收到数据后使用 CA 的公钥（PK_{CA}）验签，验签通过后得到 UI_{EPP}，并检索保存的 EPP 序列号列表，若对应，则成功；

c）远程主机 HOST 发送公钥（PK_{HOST}）和对应的签名 $Sign(SK_{CA})[PK_{HOST}]$ 给终端 ATM，终端 ATM 使用 CA 公钥（PK_{CA}）验签所得数据，验签通过后获得远程主机的公钥（PK_{HOST}）；

d）远程主机 HOST 向终端 ATM 请求 16 字节随机数，终端 ATM 使用随机数生成器产生 16 字节随机数 RATM 返回远程主机 HOST；

e）远程主机 HOST 生成主密钥 MK，然后使用终端 ATM 公钥（PK_{ATM}）加密生成的主密钥 MK 得到 $Crypt(PK_{ATM})[MK]$，并附加到步骤 d）中请求得到的 R_{ATM} 之后，即 $R_{ATM}||Crypt(PK_{ATM})[MK]$，再使用自身私钥（$SK_{HOST}$）对 $R_{ATM}||Crypt(PK_{ATM})[MK]$ 签名，得到 $Sign(SK_{HOST})[R_{ATM}||Crypt(PK_{ATM})[MK]]$；

f）远程主机 HOST 将步骤 e）中得到的 $R_{ATM}||Crypt(PK_{ATM})[MK]$ 和 $Sign(SK_{HOST})[R_{ATM}||Crypt(PK_{ATM})[MK]]$ 发送到终端 ATM；

g）终端 ATM 接收到步骤 f）的数据后首先使用远程主机 HOST 的公钥（PK_{HOST}）验签，确认 $R_{ATM}||Crypt(PK_{ATM})[MK]$ 的真实性，然后验证 R_{ATM} 是否与步骤 d）中远程主机请求的随机数一致，再使用自身私钥（SK_{ATM}）解密 $Crypt(PK_{ATM})[MK]$ 得到主密钥 MK。

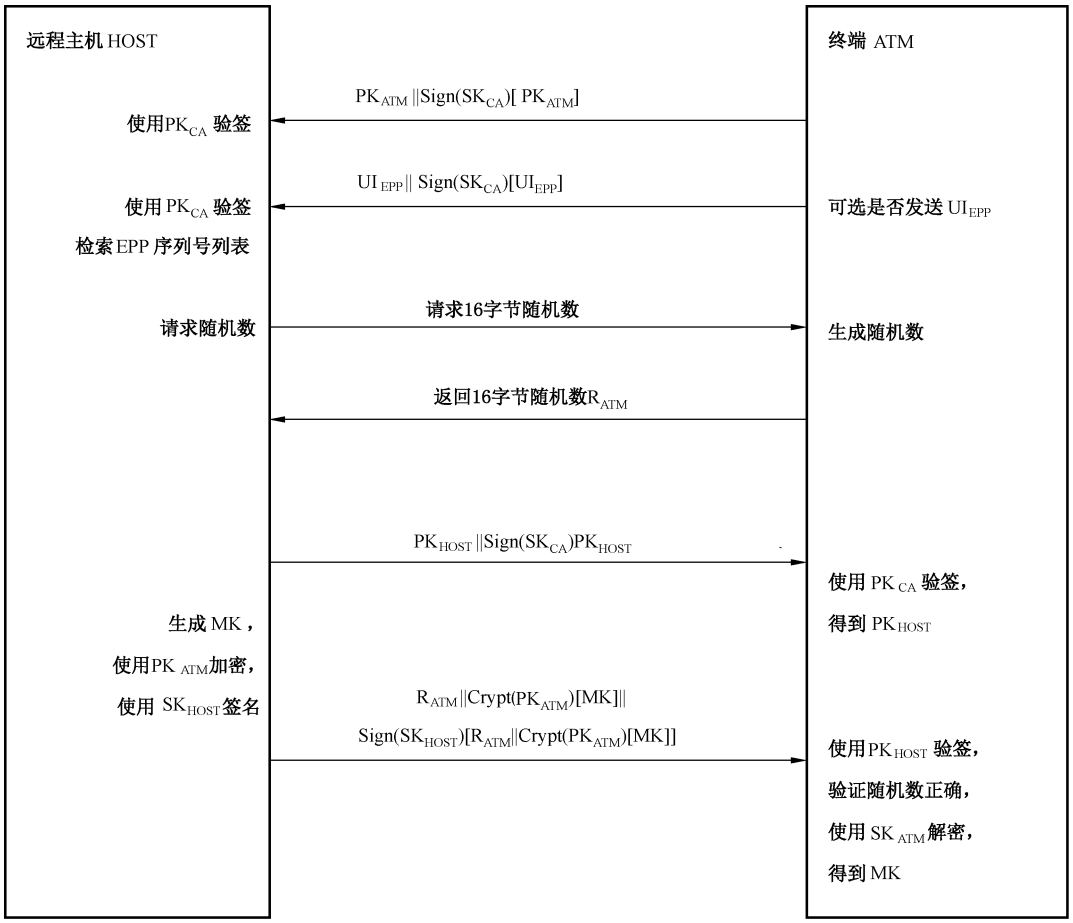

图 B.3　远程密钥装载流程

B.6　默认密钥名称

为统一多厂商应用情景，通常将默认密钥名称等按表 B.1 的规定。

表 B.1　默认密钥名称和说明

密钥名称	类型	签名方	说明
“_CertCenKey_SM”	公钥	N/A	认证中心 CA 的公钥 PK_{CA}
“_EPPCryptKey_SM”	公钥/私钥	认证中心 CA 的私钥	EPP 自生成密钥对，用于加密和解密主密钥 MK。远程主机使用公钥 PK_{ATM} 加密主密钥 MK，终端 ATM 使用私钥 SK_{ATM} 解密得到主密钥 MK

B.7　使用的密码算法

应使用 GB/T 32918 规定的密码算法。

参 考 文 献

[1] Q/CUP 006.4 中国银联银行卡联网联合技术规范 V2.1 第4部分:数据安全传输控制规范

[2] Q/CUP 006 中国银联银行卡联网联合技术规范 V2.1(SM4算法试点技术指引)

[3] 金融PIN输入设备安全要求手册

[4] ISO 9564-1 Financial services—Personal Identification Number(PIN)management and security—Part 1:Basic principles and requirements for PINs in card-based systems