密钥体系介绍

总体的密钥分为主密钥（TMK），工作密钥(TPK)，MAC 密钥(TAK)。

一、 主密钥（TMK）

由银行科技人员提供，可以采用手工输入（在安全环境下）或密钥母 POS 注入密码键盘，密码键盘将主密钥写入密钥保护芯片，此芯片具有开机程序自毁功能，能很好的保护银行主密钥的安全性，生产中应保持密码键盘主密钥与银行后台主密钥的一致性。

二、 工作密钥（TPK）

工作密钥为 POS 机向银行签到时从银行后台获取，由于签到交易需要通讯，所以需要对工作密钥进行加密传输（签到时银行返回 POS 的工作密钥是密文），POS 终端收到银行返回的报文后，对工作密钥用主密钥进行解密，然后将工作密钥存储在专用的密钥保护芯片里，此过程用密码键盘的专用芯片进行处理，此密钥同样具有开机自毁功能。此密钥专用于计算 PIN_BLOCK（对磁卡人输入的密码进行加密）。

三、 MAC 密钥（TAK）

同工作密钥的处理方式一样，POS 机向银行签到时从银行后台获取，由于签到交易需要通讯，所以需要对 MAC 密钥进行加密传输（签到

时银行返回 POS 的 MAC 密钥是密文），POS 终端收到银行返回的报文后，对 MAC 密钥用主密钥进行解密，然后将 MAC 密钥存储在专用的密钥保护芯片里，此过程用密码键盘的专用芯片进行处理，此密钥同样具有开机自毁功能。此密钥专用于计算 MAC(对数据包生成校验数据)。

四、 持卡人密码(工作密钥使用场合)

用来确定持卡人的身份与信用卡相符，通常是 6 位数字（明文）。密码应该只有持卡人自己知道。密码要送到银行主机内核对，也就是说在密码的传送过程中不能被其他人获得密码明文，就算是银行人员也不能知道。因此在密码明文输入后就必须一直以密文的形式存在，就算是银行核对密码也应该 S 核对密码密文。以下图说明：

生成密码时： 密码明文(持卡人生成) —加密→ 密码密文（保存于银行主机）

核对密码时：持卡人输入密码明文 加密 密码密文 传输 与保存在主机中的密码密文比较

在 POS 上使用信用卡，持卡人在密码键盘上输入密码明文，从密码键盘出来的数据就是加密过的密码密文数据，这样在密码传输过程中（密码键盘到 POS，POS 到银行主机）就算被截取了，也无法获知密码明文。

五、数据包校验（MAC 密钥使用场合）

按照通讯双方约定的要求，对整个需传送的数据报文或者一些具

体的域组成的字符串用 MAC 密钥，按照约定的要求进行运算，结果为 8 位的校验数据，放在发送报文的后面一起发送，如果参与运算的字符串被恶意修改，则运算的结果会不同，对方收到此数据包后，也需先按照相同的方式来对数据包进行运算，并对运算的结果与收到的结果进行比对，以判断此报文的合法性。只有合法的报文才能进行下一步的操作，否则认为是非法包，拒绝处理。

六、加密和密钥 （举例介绍，仅供参考）

假设有一块金子，可以换成钱，无论谁获得这块金子，都能拿到钱。再假设这金块在送到银行的过程中很容易被他人劫获。于是在送往银行之前要用一炼金棒，把金块变成铅块。这个炼金棒变成的铅块必须不能被其它炼金棒变成金块，因此银行也须有一个相同的炼金棒，等铅块被送到后再把它变成金块。就算在路上铅块被他人劫获，他没有相同的炼金棒，只能望“铅”兴叹了。因此这一对炼金棒必须严格保密，不被别人获得。

加密过程同以上的过程类似：密码明文就是金块，密钥的作用同炼金棒相同，在传输过程中的密码密文就好比铅块；在密码键盘中将输入的密码明文变成密码密文的过程相当于把金块变成铅块。

必须保护密钥（炼金棒）不备他人获知，百富公司 POS 将密钥放在密码键盘里，不在其它不安全的地方保存，也不在通讯线路上传输，因此具有很好的安全性。百富密码键盘（PP20-C、PP20-D、

SP30）都具有开机自毁功能，使企图获取密钥的人打开密码键盘机壳时，密钥自动丢失（开机自毁功能）。

七、百富密码键盘介绍

a) 百富密码键盘：PP20-C、PP20-D、SP30支持DES/3DES 算法，支持ANSI X9.8/ISO9564,ANSI X9.9/ISO8731,ANSI X3.92、RSA1984位等各种密码算法(运算速度1秒内)

b) 符合VISA PED规范，可下装最多100个主密钥，100个工作密钥

c) 符合PCI PED规范，可下装最多100个主密钥，100个工作密钥

d) 通过的认证及符合的规范

通过银行磁条卡销售点终端测试

通过PBOC2.0借记/贷记终端测试

EMV Level 1&2 认证

CCC认证

电信设备进网许可证

中国银联入网许可证

中国银联香港前置系统直联POS入网认证

香港EPS认证

Proton World 电子钱包认证

JCB J/SMART 认证

VISA的VLP和ADVT应用认证

MasterCard M/CHIP应用认证

AMERICAN EXPRESS AEIPS应用认证

NETS认证

CE认证

外置密码键盘符合VISA PED规范

外置密码键盘符合PCI PED规范（配SP30）