校园卡系统问题记录

1. 余额查询请求新增如下两个报文域
   102 账户标识 1 ans…30(LLVAR) 填写身份证
   103 账户标识 2 ans…30(LLVAR) 填写校园卡卡号,学号
   对应的请求报文和应答报文 MAC 校验域中增加 F102 和 F103 域。
2. 密码长度要求为 6 位。
3. 报文 MAC 检查函数调用,由于增加授权密码作为交易合法性判定条件，所以对报文 MAC 校验函数做了调整，具体如下：

报文名称	MAC 计算函数
余额查询请求	Caculate_Session_MAC()
余额查询应答	Caculate_String_MAC()
下帐请求	Caculate_Session_MAC()
下帐应答	Caculate String_MAC()
协议签订/撤销请求	改为 Caculate_Session_MAC()
协议签订/撤销应答	改为 Caculate_Session_MAC()
冲正请求	Caculate_String_MAC()
冲正应答	Caculate_String_MAC()
对帐请求	Caculate_String_MAC()
对帐应答	Caculate_FS_MAC()

4. 将文档中所有提到的“协议”改为“授权”，“协议确认”改为“授权信息初始化”，“协议撤销”改为“授权撤销”。
5. 授权信息初始化阶段身份验证
   在银行方收到学校提供的学生信息后进行开卡，完成开卡后银行方完成学生到银行卡的对应关系（身份证号至银行卡号），
   但是缺少学生的学号等信息，所以预录入的信息只有身份证号至银行卡号的对应关系。学生自助发起授权信息初始化时以该对应关系作为依据进行授权信息初始化。验证内容：
   1)商户号（F42 域）
   2)银行卡号（F2 域）
   3)身份证号（F102 域客户识别号）
6. 交易授权信息验证
   交易中需要对授权信息进行验证：
   1)授权密码
   2)商户号（F42 域）
   3)银行卡号（F2 域）
   4)身份证号（F102 域客户识别号）
   只有上述授权信息完全验证通过才能允许进行交易。
7. 授权密码重置
   通过 F32 域“代理机构标识码 AcquiringCode”来区分是哪个节点发起的交易，如果 AcquiringCode 的后四位为 0，则表示从管理节点发起的交易，否则为自助终端发起的交易。对于同一学校同一校区发起的交易“发送机构标识码”始终保持不变。
   例如：某机构机构码前四位为 0107

管理节点发起的交易：
代理机构标识码（F32）：01070000
发送机构标识码（F33）：01070001
自助终端发起的交易：F32 和 F33 保持一致。
代理机构标识码（F32）：01070001
发送机构标识码（F33）：01070001

8.学生补办金碧校园联名卡

学生如果将我行通过校园卡业务发送至手中的金碧校园联名卡丢失或者损坏，需要补办新卡，由于需要修改授权密码，所以需要撤销原有授权，重新发起授权初始化交易，上送报文中银行卡号采用新补办的银行卡号，根据上送银卡号，判断新银行卡号与原银行卡号对应关系是否合法，不合法则不允许交易，必须保证学生重新确认时的卡与原卡归属同一个固定卡号，否则不允许进行授权信息重置交易。

9.需要输入授权密码的交易

1）协议确认（初始化授权密码）
2）协议撤销
3）查询余额
4）圈存
5）授权密码修改

10.交易报文中不再涉及协议号，F102 域填入学生的唯一客户识别号（身份证号等），F103 域填入学生的学号或者校园卡号。

2011-8-10