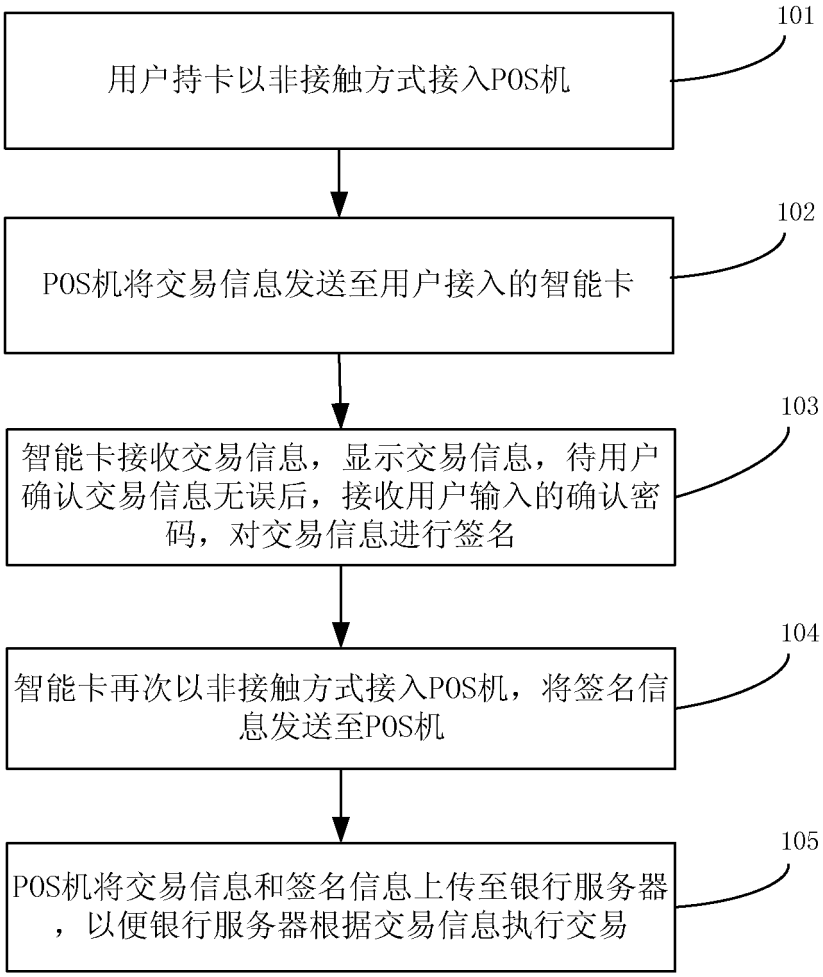

101
用户持卡以非接触方式接入POS机
102
POS机将交易信息发送至用户接入的智能卡
103
智能卡接收交易信息，显示交易信息，待用户确认交易信息无误后，接收用户输入的确认密码，对交易信息进行签名
104
智能卡再次以非接触方式接入POS机，将签名信息发送至POS机
105
POS机将交易信息和签名信息上传至银行服务器，以便银行服务器根据交易信息执行交易

图 1

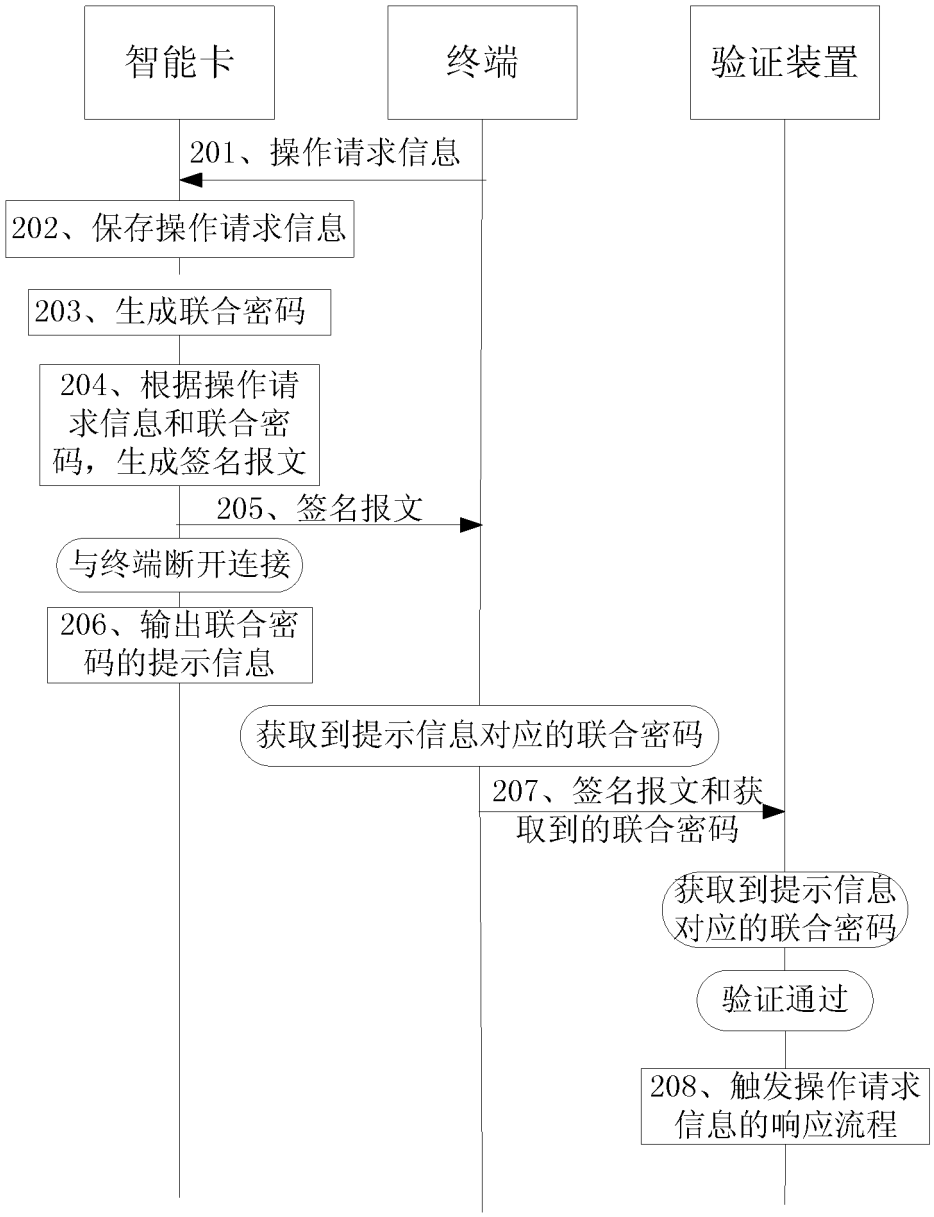

智能卡
终端
验证装置
201、操作请求信息
202、保存操作请求信息
203、生成联合密码
204、根据操作请求信息和联合密码，生成签名报文
205、签名报文
与终端断开连接
206、输出联合密码的提示信息
获取到提示信息对应的联合密码
207、签名报文和获取到的联合密码
获取到提示信息对应的联合密码
验证通过
208、触发操作请求信息的响应流程

图 2

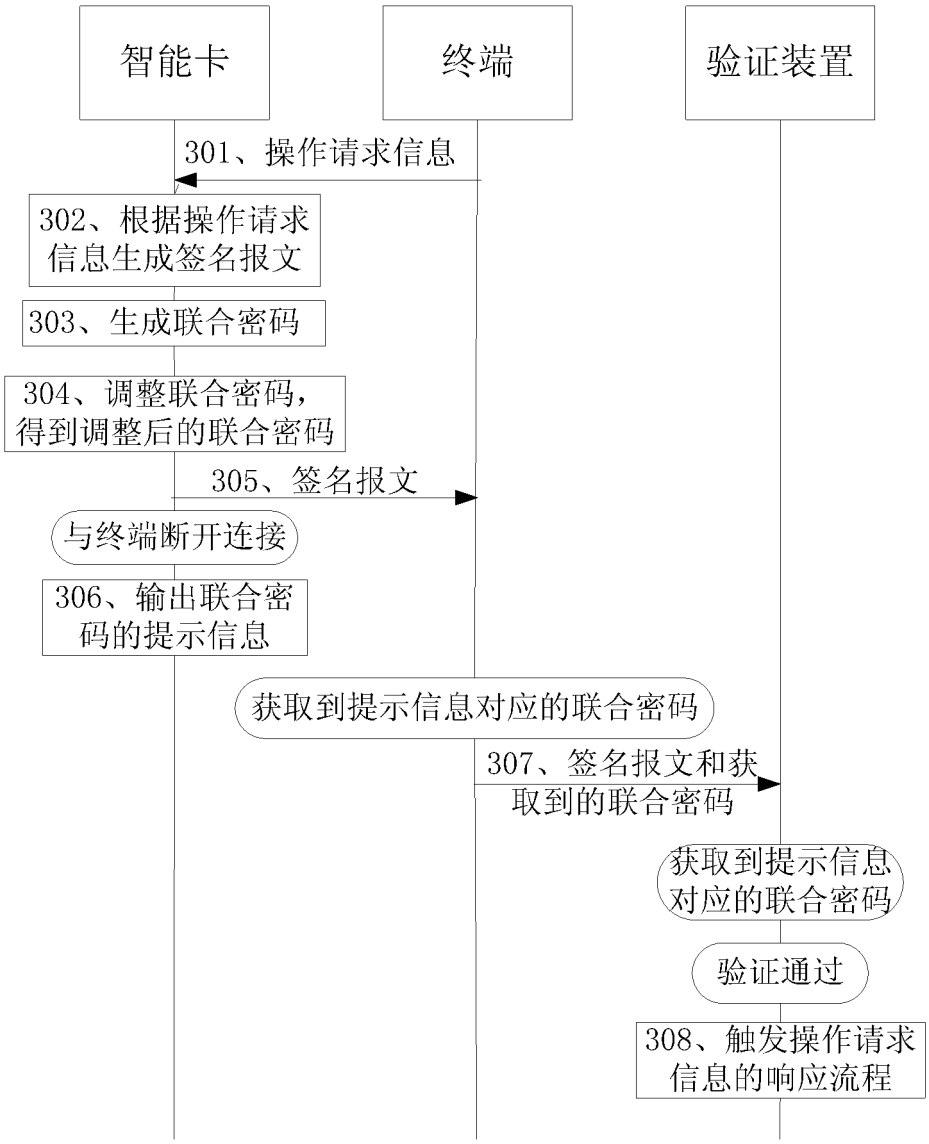

智能卡
终端
验证装置
301、操作请求信息
302、根据操作请求信息生成签名报文
303、生成联合密码
304、调整联合密码，得到调整后的联合密码
305、签名报文
与终端断开连接
306、输出联合密码的提示信息
获取到提示信息对应的联合密码
307、签名报文和获取到的联合密码
获取到提示信息对应的联合密码
验证通过
308、触发操作请求信息的响应流程

图 3

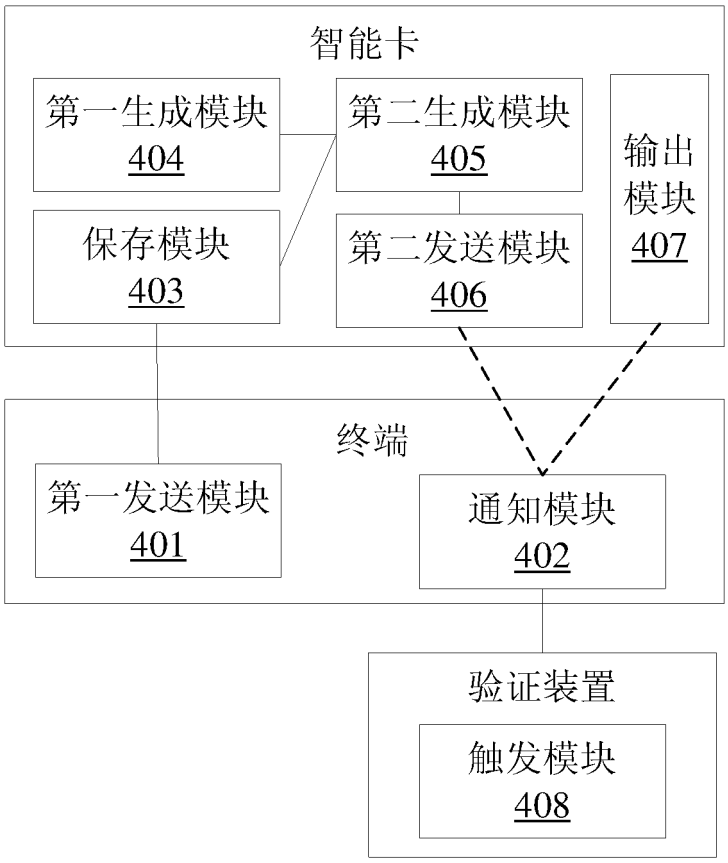

智能卡
第一生成模块
404
第二生成模块
405
输出
模块
407
保存模块
403
第二发送模块
406
终端
第一发送模块
401
通知模块
402
验证装置
触发模块
408

图 4

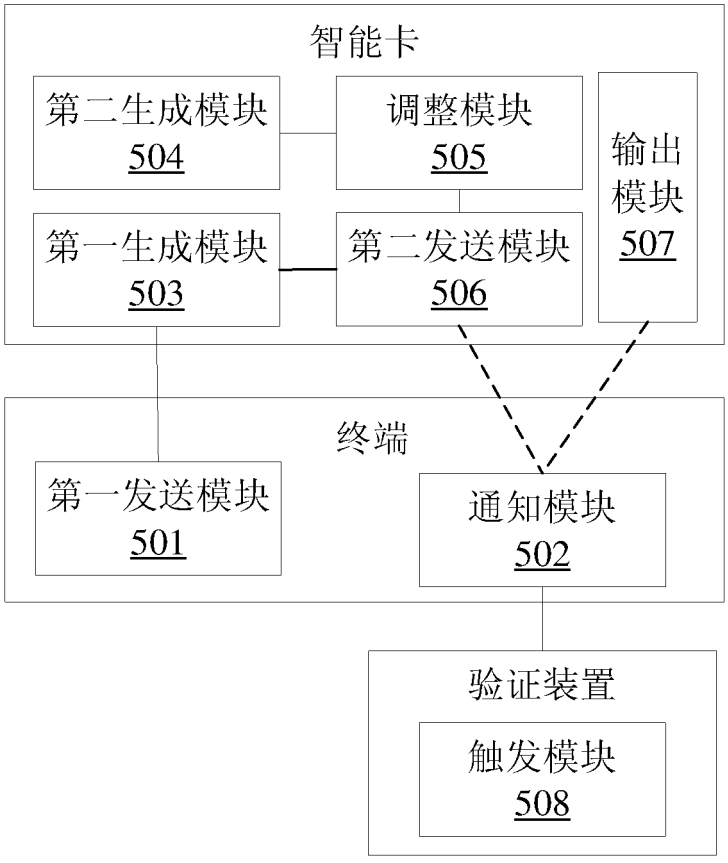

智能卡
第二生成模块
504
调整模块
505
输出
模块
507
第一生成模块
503
第二发送模块
506
终端
第一发送模块
501
通知模块
502
验证装置
触发模块
508

图 5