ICS 35.240.40
A 11

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

JR/T 0093.6—2015
代替 JR/T 0093.6—2012

中国金融移动支付　远程支付应用 第6部分：基于安全单元（SE）的安全服务技术规范

China financial mobile payment—Remote payment applications—
Part 6: Technical specification for security service based on secure element（SE）

2015－12－22 发布　　2015－12－22 实施

中国人民银行　发布

目　次

前　言

《中国金融移动支付　远程支付应用》标准由以下六部分构成：

——第 1 部分：数据元；

——第 2 部分：交易模型及流程规范；

——第 3 部分：报文结构及要素；

——第 4 部分：文件数据格式规范；

——第 5 部分：短信支付技术规范；

——第 6 部分：基于安全单元（SE）的安全服务技术规范。

本部分为该标准的第6部分。

本部分按照GB/T 1.1-2009给出的规则起草。

本部分代替JR/T 0093.6-2012《中国金融移动支付　远程支付应用 第6部分：基于安全单元（SE）的安全服务技术规范》。本部分除编辑性修改外主要技术变化如下：

——增加了第 2 章规范性引用文件；

——在第 3 章中修改或删除了一些术语和定义；

——在第 5 章中进行了统一梳理完善，将 5.6 安全服务作用相关内容进行删减纳入 5.1 概述中统一说明，修改 5.2 中图示及相关说明，对 5.4 SE 安全服务应用的实现的内容和流程进行了全面梳理修改；

——对于第 6 章内容进行全面整理并补充，形成本次修订版本的第 7 章安全要求，其中增加或补充了对 SE 安全单元、SE 安全服务应用、电子认证、客户端执行环境、客户端软件、后台服务器等方面的安全要求；

——增加了本次修订版本的第 6 章 SE 安全服务数字证书生命周期管理；

——增加了附录 A 基于 PBOC 应用的手机银行、附录 B 基于 PBOC 应用的手机信贷；

——参考文献中删除了部分文献说明。

本部分由中国人民银行提出。

本部分由全国金融标准化技术委员会（SAC/TC180）归口。

本部分负责起草单位：中国人民银行科技司、中国金融电子化公司。

本部分参加起草单位：中国工商银行、中国农业银行、中国银行、中国建设银行、交通银行、中国邮政储蓄银行、中国民生银行、上海浦东发展银行、中信银行、中国银联股份有限公司、银行卡检测中心、中国软件评测中心、上海市信息安全测评认证中心、中国金融认证中心、中钞信用卡产业发展有限公司、中国电子科技集团公司第十五研究所、北京握奇数据系统有限公司。

本部分主要起草人：王永红、陆书春、李兴锋、杜宁、潘润红、邬向阳、杨倩、吴永强、王禄禄、刘运、马小琼、涂长东、廖志江、史大鹏、谢元呈、延冰、宋捷、庞杰、李晓、姜鹏、汤沁莹、张栋、黄江、王欢、马哲、安焘、宋铮、李国俊、金铭彦、高志民、高强裔、杨明庆、魏娜、王冠华、王晓东。

本标准代替JR/T 0093.6-2012，JR/T 0093.6-2012于2012年12月首次发布，本次为第1次修订。

引　言

随着移动金融新业务、新产品、新管理模式的不断涌现，以用户需求为主导的移动金融服务出现了不断交融和细化的趋势。本部分仅对目前移动金融业务中比较成熟的、通用的基于SE的安全服务进行了抽象和规范，对于仍存在不确定性的或商业银行和支付机构定制的个性化的安全服务，在标准后续的修订过程中逐步纳入。

中国金融移动支付　远程支付应用
第6部分：基于安全单元（SE）的安全服务技术规范

1　范围

本部分对基于安全单元（包含普通金融IC卡）的安全服务进行了抽象和规范，主要规定了基于安全单元（简称 SE）的安全服务所提供的接口规范、数字证书申请流程、安全认证流程、与客户端软件的层次关系、SE安全服务生命周期管理及相关安全要求。

本部分适用于移动金融SE应用、客户端软件和后台系统的设计、开发、应用及检测等方面。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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。

JR/T 0025　中国金融集成电路（IC）卡规范

JR/T 0068　网上银行系统信息安全通用规范

JR/T 0092　中国金融移动支付 客户端技术规范

JR/T 0093.1　中国金融移动支付　应用基础　第1部分：术语

JR/T 0095　中国金融移动支付 可信服务管理技术规范

JR/T 0097　中国金融移动支付 应用安全规范

JR/T 0098.2　中国金融移动支付 检测规范 第2部分：安全芯片

JR/T 0098.5　中国金融移动支付 检测规范 第5部分：安全单元（SE）嵌入式软件安全

JR/T 0118　金融电子认证规范

3　术语与定义

下列术语和定义适用于本文件。

3.1

电子认证　electronic authentication

以数字证书为核心、以PKI技术为基础，对传输的信息进行加密、解密、数字签名和数字验证。

3.2

电子认证服务　certification service

为电子签名相关各方提供真实性、可靠性验证的服务。

3.3

私钥　private key

在公钥密码体系中，用户的密钥对中只有用户本身才能持有的密钥。

3.4

公钥 public key

在公钥密码体系中，用户的密钥对中可以被其它用户所持有的密钥。

3.5

敏感信息 sensitive information

影响基于SE的移动金融安全的密码、密钥以及交易敏感数据等信息，密码包括但不限于转账密码、查询密码、登录密码、证书的PIN等，密钥包括但不限于用于确保通讯安全、报文完整性等的密钥，交易敏感数据包括但不局限于完整磁道信息、有效期、CVN、CVN2、证件号码等。

4 缩略语

下列缩略语适用于本文件。

COS：卡片操作系统（Chip Operation System）

CRL：证书撤销列表（Certificate Revocation List）

OCSP：在线证书状态协议（Online Certificate Status Protocol）

PIN：个人识别码（Personal Identification Number）

SSL：安全套接层协议（Secure Sockets Layer）

TLS：安全传输层协议（Transport Layer Security）

IPSec：网络协议安全（Internet Protocol Security）

TSM：可信服务管理（Trusted Service Management）

5 基于 SE 的安全服务

5.1 概述

基于 SE 远程支付的安全服务应用，采用公开密钥体系为核心，构建统一的电子认证服务手段来确保远程支付交易的真实性、可靠性，降低各移动金融应用提供方在开发电子认证服务时的个性化差异，提高通用性，简化了复杂度，保障采用数字证书的电子认证服务能够安全、有序地开展，相关电子认证要求应符合 JR/T 0118。

SE 安全服务应用实现了身份验证、电子签名、加密解密等多种功能。证书认证机构签发的数字证书包含了证书用户的身份信息，交易各方可以利用数字证书验证对方身份的真实性。交易参与各方对交易数据进行电子签名，确保交易数据的完整性和交易行为的不可否认性。交易发送方使用接收方的公钥证书对信息加密，接收方使用相应的私钥解密数据，基于数字证书的非对称加解密，可确保数据只有私钥持有方才可以解密，保证了信息的机密性。

实现案例参见附录 A、附录 B。

5.2 SE 安全服务应用与后台系统的关系

图 1 描述了 SE 安全服务应用的角色定位以及与后台系统之间的关系。

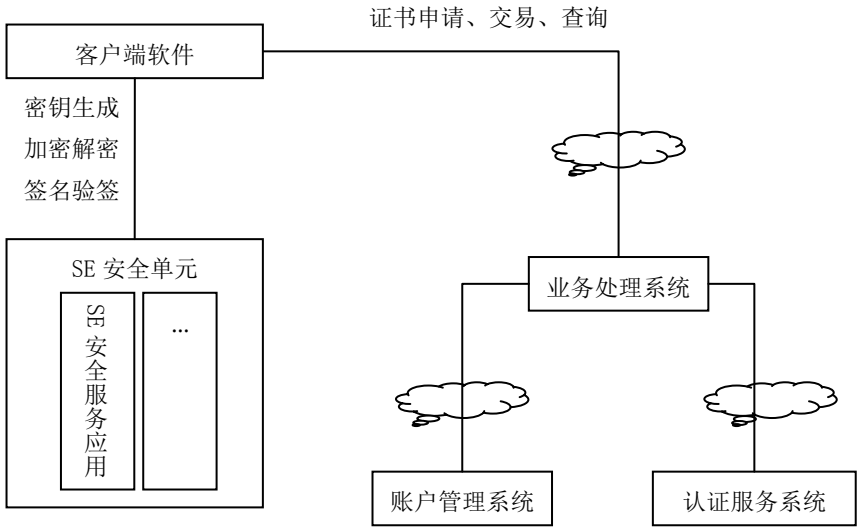


图1　SE 安全服务应用与后台系统的关系示意图

SE安全服务应用安装在SE内部，对外提供如密钥生成、证书安装、加密解密、签名验签等安全服务。

5.3　SE 安全服务应用的层次结构

图2描述了客户端软件与SE安全服务应用之间的调用关系，及SE安全服务应用的层次结构。

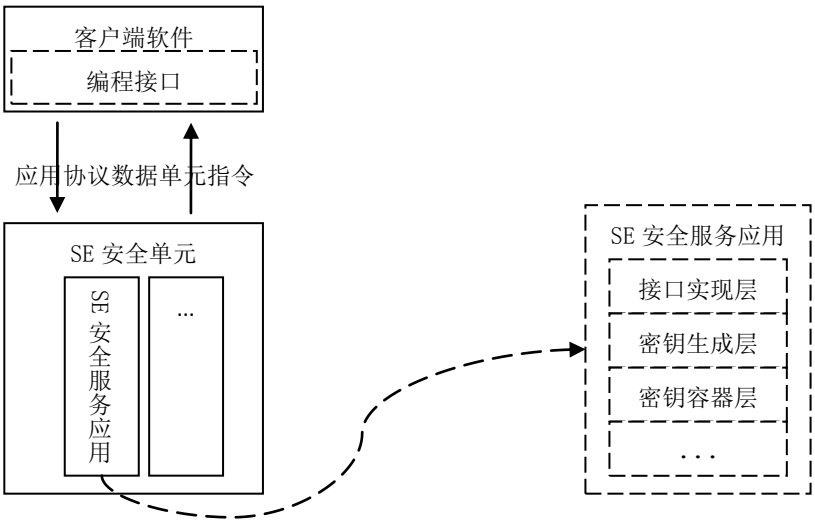


图2　SE 安全服务应用的层次结构与调用关系图

完整的运算过程，均由客户端软件发起指令，调用SE安全服务应用的编程接口，通过应用协议数据单元指令的转化，从而到达SE安全服务应用的内部进行运算，执行结果会以同步方式逐层响应上级调用者，直到客户端软件得到运算结果。

SE安全服务应用作为SE的应用之一，在提供基础的安全服务功能的同时，需要加强对调用指令的访问控制。其内部构造可以分为多个层次来实现，比如接口实现层主要完成对外提供接口的功能实现，密

钥生成层主要完成密钥对的生成，密钥容器层主要完成密钥的存储、数字证书的安装、容器和密钥的访问控制。

5.4 SE 安全服务应用的实现

5.4.1 接口实现层

接口实现层主要完成对外提供接口的功能实现，功能包括但不仅限于：

a) 证书申请/安装

证书申请/安装分为预置和动态申请/安装方式。图3描述了动态申请/安装方式用户从客户端软件上发起申请，到SE安全服务应用将数字证书安装的过程。

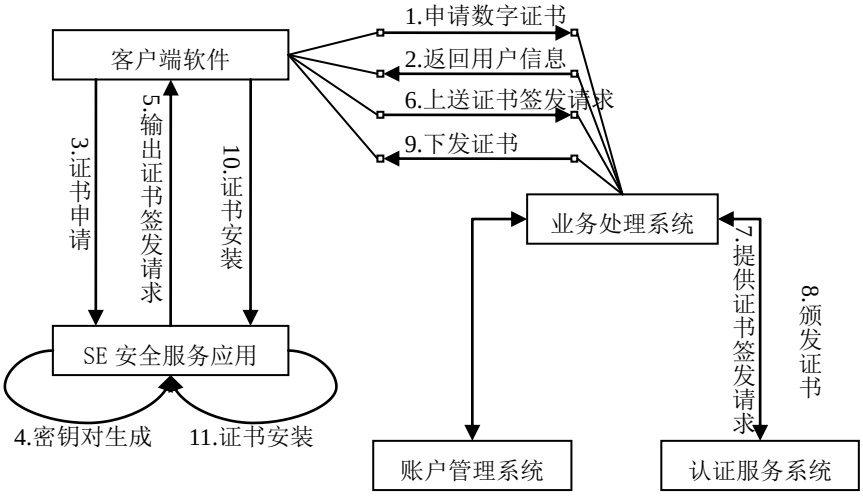


图3 SE 安全服务应用证书申请的示意图

步骤1：用户在客户端软件上发起数字证书申请的请求；

步骤2：业务处理系统进行用户的身份认证与请求验证；

步骤3：验证通过后，客户端软件调用SE安全服务应用的证书申请功能；

步骤4：SE安全服务应用在内部生成密钥对，并存储到密钥容器中；

步骤5：SE安全服务应用输出证书签发请求，响应客户端软件；

步骤6：客户端软件将证书签发请求上送到业务处理系统；

步骤7：业务处理系统将证书签发请求与用户信息提交到认证服务系统；

步骤8：认证服务系统对用户身份和证书签发请求的合法性认证后，颁发证书；

步骤9：业务处理系统接收到数字证书后，下发到客户端软件；

步骤10：客户端软件获得下发的数字证书后，调用SE安全服务应用的证书安装功能；

步骤11：SE安全服务应用将数字证书匹配密钥对，存储到容器中，完成数字证书的安装。

b) 证书卸载

卸载数字证书后，数字证书在密钥容器中占用的空间将被释放，该数字证书及对应的私钥信息将销毁。数字证书的卸载应具有访问控制权限。

c) 读取证书列表

读取密钥容器中的所有数字证书。

d) 读取指定证书

根据证书的序列号、有效的起止日期等检索到指定的数字证书。

e） 加密/解密

图4描述了SE安全服务应用基于非对称加密方式完成加密与解密的过程。

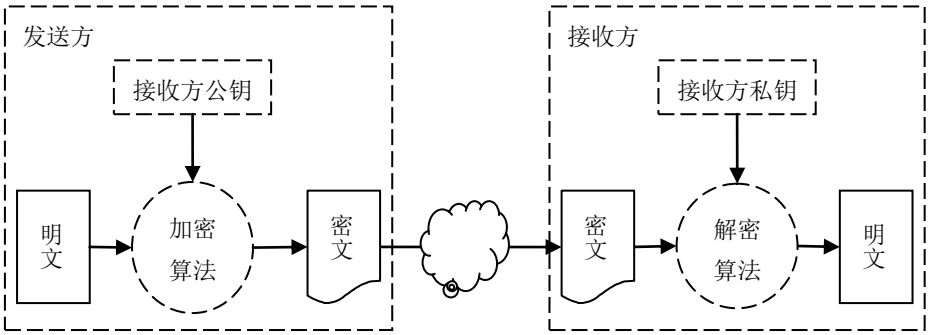


图4 SE 安全服务应用的加密与解密示意图

客户端软件作为交易数据的发送方，在交易数据传输前，会获取到接收方的公钥数字证书，而接收方的私钥则始终保存在接收方的后台系统中。

发送方使用接收方的公钥对交易数据进行加密并发送给接收方，接收方得到加密数据后，使用与公钥对应的私钥进行解密。

f） 签名/验签

图5描述了SE安全服务应用基于非对称加密方式完成签名与验签的过程。

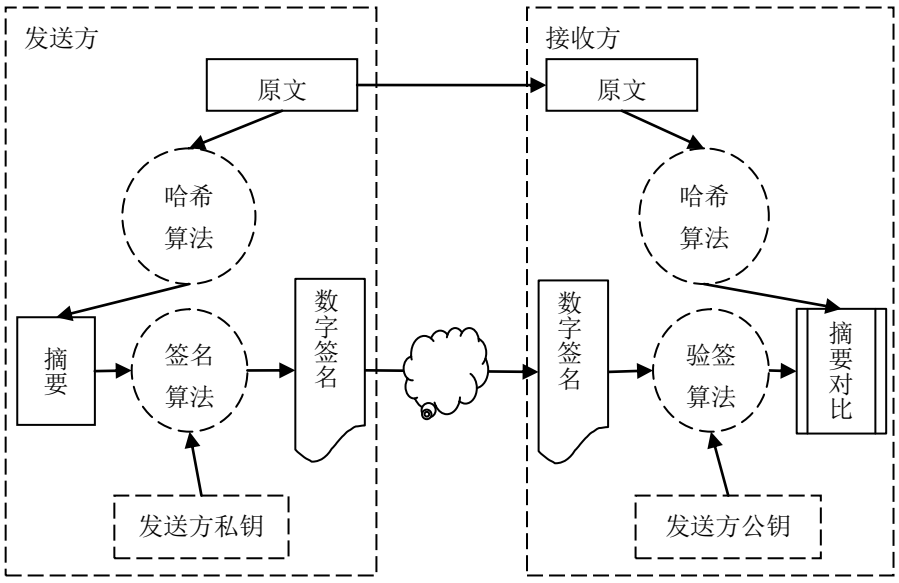


图5 SE 安全服务应用的签名与验签示意图

在交易数据传输前，发送方将原文按照约定的哈希算法计算得到摘要，并使用自己的私钥对摘要进行加密得到数字签名，与原文一同发送给接收方，接收方使用同样的哈希算法对原文计算摘要，然后与使用发送方的公钥对数字签名进行解密得到的摘要进行对比。

5.4.2 密钥生成层

密钥生成层的功能包括但不仅限于：

a） 密钥对生成

密钥对生成后，SE安全服务应用会将生成的公钥和私钥分别存储，公钥可以非加密的方式对外公开，私钥则始终保存在密钥生成地。

b） 私钥签名

采用私钥对原文的哈希运算结果进行加密所得签名，只有私钥持有者才能产生，在交易过程中用以鉴别发送者身份。私钥签名应具备较高的访问控制权限。

c） 密钥调用时的访问控制

公钥数字证书的访问应指定序列号、有效的起止日期等才能调用。

私钥的访问应具备较高的访问控制权限。

d） 私钥不可导出

私钥应始终保存在SE安全服务应用内部，从生成直到销毁，SE安全服务应用不应提供导出功能。

e） 删除过期私钥

由于公钥、私钥的一一对应关系，私钥过期后，由客户端软件发起删除过期数字证书的请求，SE安全服务应用应将公钥数字证书与私钥一并删除。

5.4.3 密钥容器层

密钥容器层的功能包括但不仅限于：

a） 容器的实现

密钥容器包含某个特定用户的所有非对称密钥对，包括签名密钥对、加密密钥对。创建密钥容器时，应为每个密钥容器指定唯一的名称。

b） 容器调用的访问控制

密钥容器存储着密钥对，应具备较高等级的安全访问权限。

c） 证书的导入

数字证书安装时，应将数字证书导入到容器中，并与之前的密钥对匹配关联。

d） 证书的导出

数字证书导出时，应将容器中的数字证书复制一份并输出。

e） 证书的删除

数字证书删除时，应将数字证书与匹配的密钥对一同销毁，释放容器的空间。

f） 证书的读取

数字证书的读取，会根据序列号、有效的起止日期等检索到指定证书。

g） 证书的枚举

数字证书的枚举，不设定任何条件，可列举所有的数字证书。证书的枚举仅限于内部实现，不对外提供接口。

h） 证书调用的访问控制

应限制客户端仅可访问授权的证书。

6 SE 安全服务生命周期管理

6.1 应用生命周期管理

SE 安全服务应用作为 SE 的一种标准应用，其使用过程如下：

——应用的下载安装：应符合 JR/T 0097-2012 中 7.4 应用生命周期管理的要求。可以在 SE 中预置

应用，也可提供在线动态下载应用，在线动态下载应用的流程应满足 JR/T 0097 中 7.4.2 应用下载与授权的流程；

——应用的初始化：用户下载 SE 安全服务应用后，需要申请并安装证书才能使用；

——应用的使用：用户在进行远程交易时，SE 安全服务应用提供数据的加密/解密、签名/验签等服务。

图6描述了用户从下载、安装SE安全服务应用，到使用SE安全服务应用完成交易的过程。

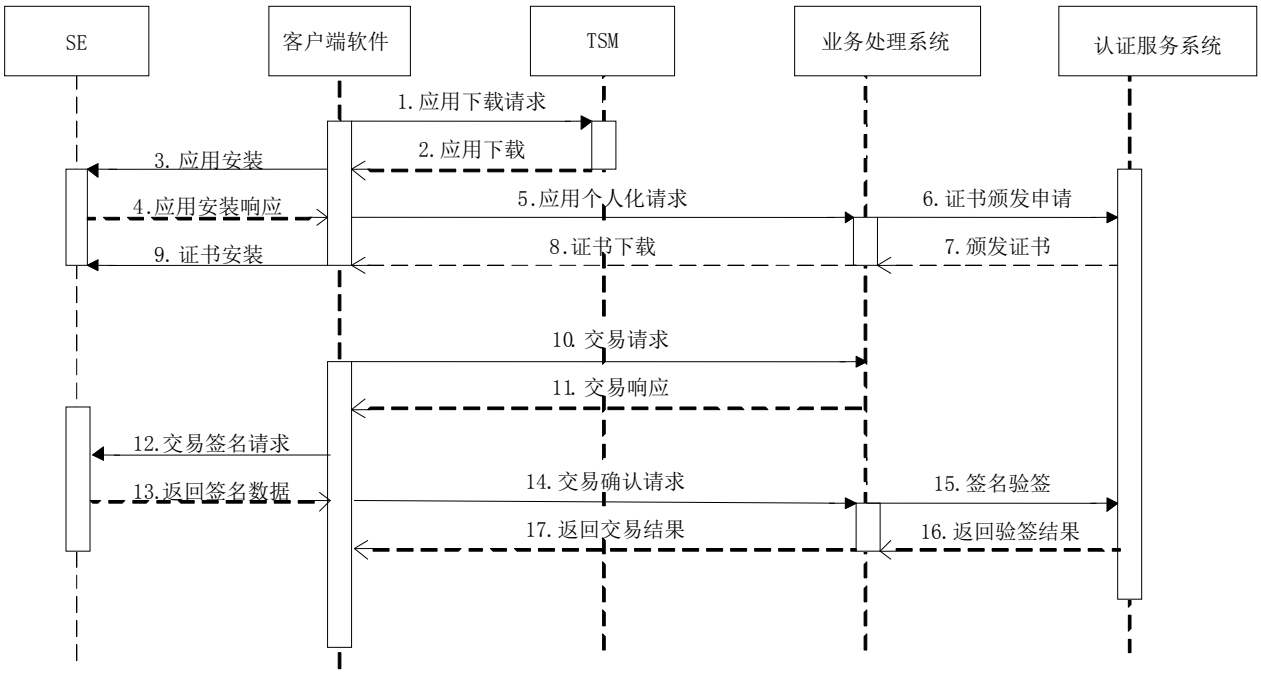


图6　SE 安全服务应用的使用流程

步骤1：用户在客户端软件上发起SE安全服务应用下载的请求；

步骤2：通过相关认证后，TSM系统返回SE安全服务应用；

步骤3：客户端软件将SE安全服务应用安装在SE中；

步骤4：SE向客户端软件返回应用安装结果；

步骤5：用户从客户端软件向业务处理系统发起应用个人化请求；

步骤6：业务处理系统向认证服务系统发起证书颁发申请；

步骤7：认证服务系统颁发证书并返回业务处理系统；

步骤8：业务处理系统将证书下发给客户端软件；

步骤9：客户端软件将证书安装在SE中；

步骤10：用户从客户端软件向业务处理系统发起交易请求；

步骤11：业务处理系统向客户端软件返回交易响应信息；

步骤12：客户端软件组装交易签名请求报文，调用SE安全服务应用，发起签名请求；

步骤13：SE安全服务应用向客户端返回签名结果；

步骤14:客户端软件向业务处理系统发起交易确认请求,请求信息包含SE安全服务应用的签名结果；

步骤15：业务处理系统将交易信息及签名结果发送到认证服务系统；

步骤16：认证服务系统进行验证并向业务系统返回验签结果；

步骤17：业务处理系统进行交易处理后，向客户端软件返回交易结果。

6.2 数字证书生命周期管理

6.2.1 概述

数字证书的生命周期管理包括证书的申请、更新、卸载/吊销、签名/验签、加密/解密等处理过程。证书分为预置和动态申请两种方式。6.2.2、6.2.3、6.2.4流程适用于动态申请方式。

6.2.2 证书申请

证书申请为初次使用SE安全服务应用时进行的第一个交易，证书申请流程如图7所示。

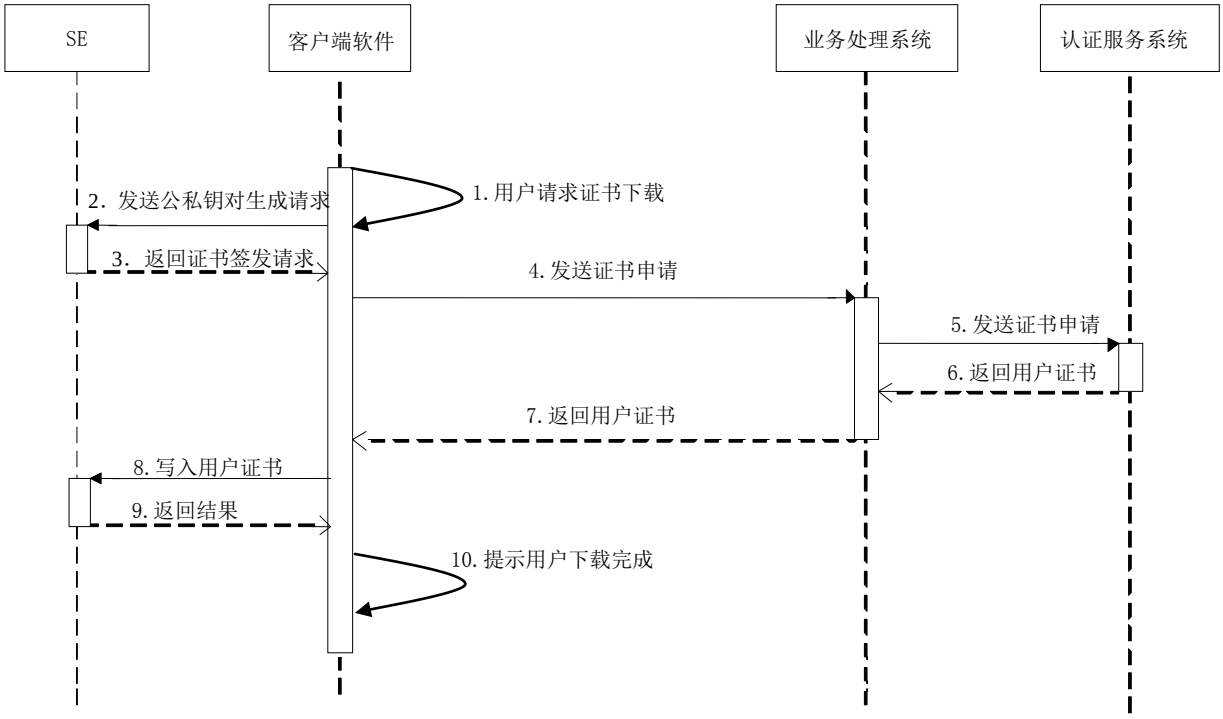


图7 证书申请流程图

步骤1：SE持有人使用客户端软件（如手机银行）发起证书申请交易，并通过业务处理系统进行身份验证；

步骤2：客户端软件向SE发送生成公私钥对的请求；

步骤3：SE生成数字证书对应的公私钥对，将证书签发请求返回给客户端软件；

步骤4：客户端软件按照业务处理系统的格式要求，组织请求签发证书的报文，上送到业务处理系统。报文内容中至少需要包括SE内的公钥，以及对应的用户信息；

步骤5：业务处理系统完成请求报文的解析，并进行相关的处理和身份验证后，转发证书签发请求和相关数据到认证服务系统；

步骤6：认证服务系统签发数字证书，返回给业务处理系统；

步骤7：业务处理系统完成相关处理后，将生成的证书回送给客户端软件；

步骤8：客户端软件组织并发送更新文件的指令，指令数据域的内容为新签发的证书，发送到SE；

步骤9：SE将新生成的公钥证书写入SE的安全域中，如果是证书的更新操作，新的证书内容将覆盖原证书的内容，并返回更新证书成功的确认信息；

步骤10：客户端软件向用户提示证书申请完成。

6.2.3 证书更新

证书应定期更新，更新流程与证书申请流程基本相同，只是在签名验签流程中的认证服务系统在调用“验证证书有效性”接口时会验证证书的有效期，若证书即将到期，该接口将返回“证书即将到期”的返回码，客户端软件收到该返回码后，应再次执行证书申请流程。

6.2.4 证书卸载/吊销

证书卸载后，该数字证书及对应的私钥将被删除，在删除时需要满足访问控制权限。

证书卸载或丢失后，应通知业务处理系统和认证服务系统吊销用户证书。

6.2.5 证书签名/验签

证书签名、验签实现对本次交易数据及SE持有人合法身份的认证，基本流程如图8所示：

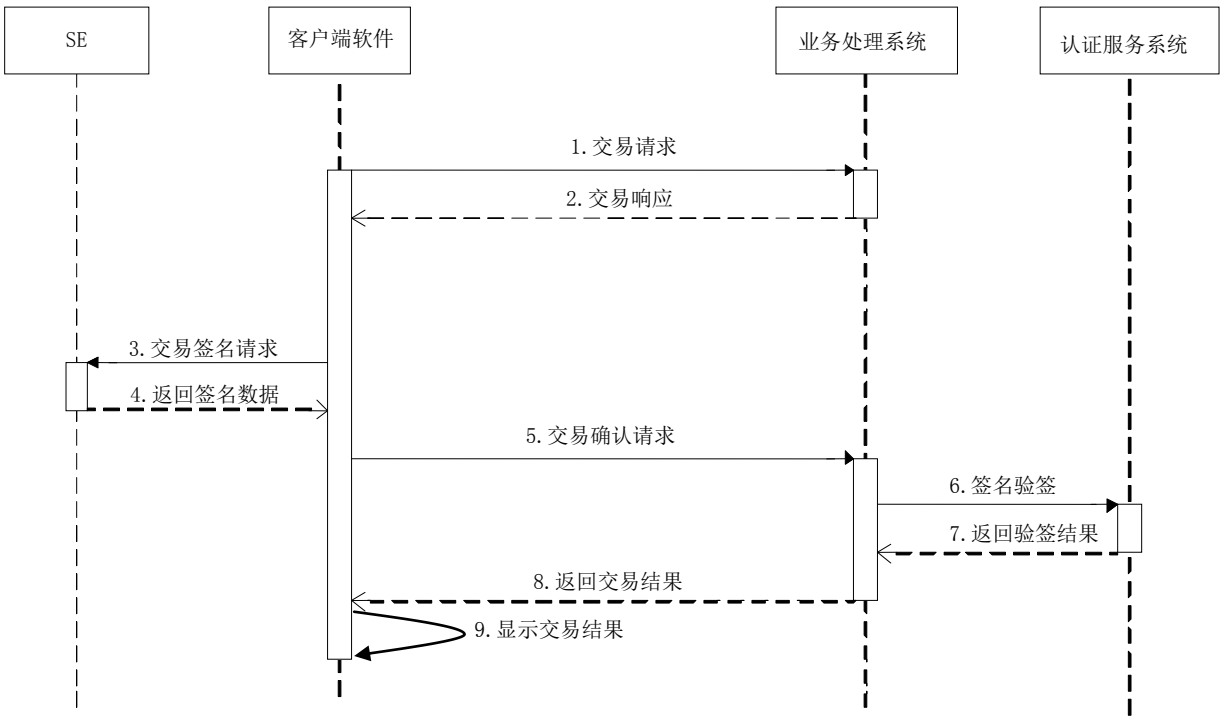


图8 证书签名验签流程图

步骤1：用户通过客户端软件向业务处理系统发起交易请求；

步骤2：业务处理系统返回交易响应；

步骤3：客户端软件根据业务处理系统返回的响应显示交易界面，用户按要求输入交易信息，并调用SE安全服务应用，进行交易敏感信息签名。在调用SE安全服务应用时需要进行身份验证；

步骤4：SE安全服务应用使用SE中数字证书的私钥，对输入的交易数据进行签名计算，将签名结果返回给移动终端的客户端软件；

步骤5：客户端软件按照业务处理系统指定的格式要求，组织签名和认证交易的上送报文，并上送到业务处理系统。报文内容中至少需要包括数字签名、参与签名的相关交易数据以及对应的用户信息；

步骤6：业务处理系统完成请求报文的解析，并进行相关的处理和身份验证后，转发签名数据到认证服务系统，请求验证；

步骤7：认证服务系统验证签名的有效性，确认交易数据的正确性。完成验证后，返回验证结果给业务处理系统；

步骤8：业务处理系统完成相关处理后，按照要求回送认证结果以及交易处理的返回数据，发送给客户端软件；

步骤9：客户端软件向用户提示交易结果。

6.2.6 证书加密/解密

客户端软件在与后台系统进数据传输前，通过与其交互完成公钥交换，从而获得后台系统的公钥证书。

发送方使用接收方的公钥对交易数据进行加密并发送给接收方，接收方得到加密数据后，使用与公钥对应的私钥进行解密。

7 安全要求

7.1 安全单元（SE）

SE 应满足如下要求：

——SE 安全芯片应符合 JR/T 0098.2 的要求；

——SE 嵌入式软件应符合 JR/T 0098.5 的要求；

——密钥对应在 SE 安全服务应用内部生成，不得固化密钥对和用于生成密钥对的因子；

——SE 安全芯片、嵌入式系统软件等应经过认可的第三方专业机构的检测认证。

7.2 SE 安全服务应用

SE安全服务应用应满足如下要求：

——主文件(Master File)应受到 COS 安全机制保护，保证用户无法对其进行删除；

——应具有密钥对生成和电子签名等运算能力，保证敏感操作在内部进行；

——应保证私钥在生成、存储和使用等阶段的安全：

- 禁止以任何形式读取或写入私钥；
- 私钥文件应与普通文件类型不同，应与密钥文件类型相同或类似；
- 在执行签名等敏感操作前应经过用户身份鉴别；
- 密钥文件在启用期应封闭，禁止以添加新密钥文件的方式对密钥进行删除操作。

——参与密钥、PIN 码运算的随机数应在内部生成，其随机性指标应符合国家密码管理部门的相关要求；

——签名交易完成后，状态机应立即复位；

——应保证 PIN 码和密钥的安全：

- 采用安全的方式存储和访问 PIN 码、密钥等敏感信息；
- PIN 码连续输错次数达到错误次数上限，SE 安全服务应用应锁定；
- 使用的密码算法应符合国家密码管理部门的相关要求。

SE 安全服务应用的下载和个人化过程应符合 JR/T 0097 中应用生命周期管理部分的要求。

SE 安全服务应用的密钥管理应符合 JR/T 0095 密钥管理安全部分的要求。

7.3 电子认证

7.3.1 身份认证

7.3.1.1 证书认证机构

应采用具有资质的第三方认证机构提供认证服务。

应在与证书认证机构的合作协议或合同中，明确双方的权益和责任。

7.3.1.2 证书与应用的关联

用户申领数字证书后，应将用户的数字证书信息注册到后台系统中，并与相关的账户信息如用户账号、用户名称、移动终端标识等进行关联。

后台系统中所记录的证书信息应为证书的唯一识别信息，如证书序列号，以及各机构认为有必要在其应用系统中记录的其它证书信息。

7.3.1.3 身份认证

采用数字证书验证用户身份的，应满足如下要求：

a) 用户的电子签名作为鉴别用户身份的必要因素；
b) 应验证用户签名的有效性；
c) 应验证产生签名的数字证书与用户关联的一致性。

7.3.2 电子签名

7.3.2.1 电子签名基本要求

使用电子签名技术产生电子签名，应满足如下要求：

a) 数字证书的密钥用法应包含电子签名标识；
b) 签名只能由签名私钥计算，签名私钥通过 SE 保护且签名运算应在 SE 内完成；
c) 所使用的签名算法、数据摘要算法应采用国家密码管理部门认可的算法；
d) 签名的交易数据应包含账号、金额、时间，或能与这些信息关联的其他相关信息。

7.3.2.2 数字证书验证

数字证书应验证如下内容：

a) 验证证书的颁发者名称与颁发者证书的主体名称匹配；
b) 验证证书的签名并确保签名算法是国家密码管理部门认可的算法；
c) 验证证书的有效期；
d) 验证证书的密钥用法与业务系统应用需求相符；
e) 正确构造证书链到受信任的颁发者；
f) 验证证书符合金融领域证书策略；
g) 应通过证书认证机构提供的 CRL、OCSP 或者其它可靠的方式查询证书或者验证证书的状态；
h) 应根据应用安全要求，验证证书中与应用相关的其它信息。

7.3.2.3 电子签名认证

电子签名认证，应满足如下要求：

a) 验证签名的有效性；
b) 验证签名算法应使用国家密码管理部门认可的算法；
c) 验证数据摘要算法应使用国家密码管理部门认可的算法；
d) 应验证产生签名的数字证书与用户关联的一致性。

7.3.3 加密/解密

7.3.3.1 传输通道加密

选择基于数字证书的安全传输协议，建立加密传输通道，应满足如下要求：
a) 应采用健壮的加密算法和安全协议来保障客户端与服务器之间所有连接的安全，协议包括但不限于 SSL/TLS 和 IPSEC；
b) 如果使用 SSL 协议，应使用 3.0 及以上相对高版本的协议，取消对低版本协议的支持。

7.3.3.2 非对称加密/解密

使用数字证书实现非对称加密/解密功能，应满足如下要求：
a) 数字证书的密钥用法应包含数据加密标识；
b) 数据加密/解密应采用国家密码管理部门认可的非对称密码算法；
c) 数据加密应先检查接收方数字证书的有效性，不应使用无效证书。

7.3.3.3 数字信封

使用数字证书来实现数字信封的功能，应满足如下要求：
a) 数字证书的密钥用法应包含数据加密标识；
b) 数据加密/解密应采用国家密码管理部门认可的密码算法，包括对称算法与非对称算法；
c) 数据加密须先检查接收方加密证书的有效性，不应使用无效证书。

7.4 客户端执行环境

客户端执行环境，包括但不限于操作系统等，应满足如下要求：
——在安装和更新客户端软件前，应首先验证客户端软件安装包的数字签名，保证客户端软件安装包来源于可信实体；
——应保证客户端软件拥有独立的程序运行空间和私有的文件系统，保证客户端软件私有数据不被其它软件非法访问；
——应实现对 SE 整体的访问控制功能，只允许使用特定数字证书签名的客户端软件访问 SE。宜实现对单个 SE 安全服务应用的命令级别的访问控制功能；
——宜实现主动的安全防御机制，例如，内置恶意软件检测模块、安全检查工具等；
——当发现重大安全缺陷或安全威胁时，应在门户站点发布警示通知，并通过消息推送、短信、邮件等方式主动通知用户。

7.5 客户端软件

7.5.1 生命周期管理

7.5.1.1 客户端开发和上线

客户端开发和上线应满足如下要求：
——客户端软件开发和上线流程应符合规范 JR/T 0092 中客户端软件管理部分的要求；

——应严格区分测试环境和生产环境，测试环境中严禁使用生产环境真实的账户信息、个人身份信息等，测试环境中的账户在进入生产环境前应删除或禁用；
——客户端软件发布时应清除未使用的程序代码、可能暴露实现细节的调试信息和所有的测试环境数据，并永久禁用调试级别和详细级别的日志打印功能；
——客户端软件上线前应进行内部安全审计，并出具风险评估报告；
——客户端软件上线前应制定详细的安全事故应急预案，并指定相关责任人；
——客户端软件在首次上线和发生重大变更时应经过认可的第三方专业检测机构的检测，检测的内容包括但不限于代码审计、渗透测试、业务流程审计等，每年应至少开展一次。

7.5.1.2 客户端分发

客户端分发应满足如下要求：
——在进行客户端软件（如手机银行）签约时应对用户进行风险教育，要求用户必须从官方认可的渠道下载客户端软件；
——通过门户网站进行分发时，应提供客户端软件的哈希值供用户参考，同时在显著位置标注官方授权的其他发布途径；
——客户端软件在应用分发平台中显示的提供商名称应与企业在工商注册的名称一致；
——应定期从分发平台上下载客户端软件进行校验和检测，防止客户端软件安装包被篡改，如果发现异常，应立即对客户端软件下架处理，并在官方网站上进行公布；
——宜通过网站、微博、互动平台等渠道对客户端软件安装、使用中的注意事项进行宣传，培养用户的安全使用习惯。

7.5.1.3 客户端启用

客户端启用应满足如下要求：
对于同一用户名下的每个SE安全服务应用实例，应保证同时至多有一个客户端实例与之绑定，绑定新的客户端实例后，旧客户端实例自动解除绑定。

7.5.1.4 客户端更新

客户端更新应满足如下要求：
——应有计划的对客户端软件进行更新，客户端软件应具备自动检查更新的功能；
——应禁用过期超过一个版本的客户端软件中的金融交易功能，并在软件界面中提醒用户进行更新；
——宜通过短信方式对超过一定时间仍未更新的用户进行提醒，短信中应包含官方下载地址。

7.5.1.5 客户端卸载

客户端软件卸载完成后，文件系统中不应残留任何与用户相关的个人信息及交易数据等。

7.5.2 防逆向

防逆向要求如下：
——客户端软件应采取有效的干扰措施增加对代码静态分析的难度，如代码混淆、花指令、程序加壳等；
——客户端软件应至少对以下代码或数据进行混淆，如非公开的函数名称、变量名称、参数名称、可能泄露实现细节的字符串、硬编码的密钥或公钥等；
——客户端软件宜对于关键的代码段进行加密处理；

——客户端软件宜通过动态组件下载等方式实现动态防逆向机制，动态下载的组件应在使用完毕后立即清除。

7.5.3 防篡改

防篡改要求如下：

——客户端软件应在启动和更新过程中对自身的完整性和真实性进行检查，防范软件代码被篡改或替换；

——客户端软件宜定期或每次交易前对自身完整性和真实性进行检查，定期检查宜至少每 24 小时执行一次；

——客户端软件检查自身完整性和真实性的算法应符合 JR/T 0095 中密码算法部分的要求。

7.5.4 防重放

防重放要求如下：

——客户端软件输出的所有编码后的敏感信息、数字签名等与认证和交易相关的数据应保证仅一次有效；

——随机因素的生成应同时满足随机性和不可预测性，交易完成后应立即失效；

——客户端软件进行加密和签名运算时数据块应采用随机数进行填充。

7.5.5 安全输入组件

安全输入组件用于保证用户输入数据的秘密性和完整性，例如密码键盘、专用文本框等，应满足如下要求：

——所有的敏感信息（PIN、CVN、有效期等）和关键的交易信息（交易金额、收款人账号、交易验证码等）应通过安全输入组件进行输入和显示；

——通过安全输入组件输入的敏感信息在输入完成后应立即加密，在输入的任何阶段，内存中都不应出现完整的明文数据；

——通过安全输入组件输入的关键的交易信息应采用密码学技术保证其完整性；

——安全输入组件使用的秘密性和完整性保护密钥应基于非对称密码算法协商，并保证每交易唯一；

——应对安全输入组件使用的静态密钥进行保护，如采用拆分、编码等方式，防范该密钥被非法篡改和替换；

——如采用第三方安全输入组件，应保证其通过认可的第三方专业检测机构的检测。

——密码键盘应满足如下要求：

- 使用密码键盘输入敏感信息时，按键应随机排列，宜采用图片按键方式；
- 宜采取防录屏手段防范恶意软件获得密码键盘当前的按键排列顺序。

——专用文本框应满足如下要求：

- 显示敏感信息时，应以屏蔽方式显示；
- 显示交易信息时，应逐字符显示，避免在内存中出现完整的交易信息明文。

7.5.6 图片验证码

图片验证码应满足如下要求：

——图片验证码应由后台服务端产生和验证，图片验证码文本内容不应在客户端出现；

——每个图片验证码应只验证一次，无论验证结果如何，均应使当前验证码失效；

——图片验证码应具有一定的复杂度，有效的枚举空间不得低于 1 万个；

——图片验证码应能有效防范程序自动识别，如采取字符变形、字符叠加、背景干扰、颜色变换等方式；
——如果图片验证码包含数字，宜采用大写数字显示，如壹、贰等；
——图片验证码应具有时效性，有效期不宜超过 3 分钟。

7.5.7 外部接口

外部接口包括但不限于用户交互接口、进程间通信接口等，应满足如下要求：
——客户端软件不应暴露任何影响自身安全性的外部接口；
——客户端软件应对用户或软件输入的内容进行约束，如禁止输入非法字符、对取值范围进行判断、对输入长度进行限制等；
——对于软件调用接口，客户端软件宜对调用方的身份合法性进行验证。

7.5.8 敏感信息保护

敏感信息保护要求如下：
——客户端软件不应在文件系统中存储任何明文或密文的非业务必需的敏感信息；
——银行卡主账号除交易流程中必须由用户确认的情况外，显示时应屏蔽部分字段。

7.5.9 交易流程

7.5.9.1 交易流程总体要求

客户端软件的交易流程应符合 JR/T 0068 业务安全交易机制章节中交易流程部分的要求。

7.5.9.2 用户登录

客户端软件登录后应主动向用户提示上次登录时间等信息。如用户有预留信息，应提示用户确认。

7.5.9.3 交易确认

客户端软件应采用结合交易要素的图片验证码向用户确认收款人账号、交易金额等交易关键信息。

7.5.9.4 数字签名

数字签名应使用SE对交易报文进行数字签名，保证交易数据的完整性、真实性和抗抵赖。

7.5.9.5 会话管理

会话管理应满足如下要求：
——客户端软件应包含非活动状态超时计时器，超过一定时间后唤醒需要重新对用户身份进行验证；
——客户端软件正常退出前应通知后台服务端结束当前会话。

7.5.10 安全通信

7.5.10.1 客户端与后台服务端的通信

客户端与后台服务端的通信应满足如下要求：
——客户端软件应使用安全协议保证与后台服务端通信的秘密性、完整性和真实性，如使用 TLS 协议等；
——客户端软件与后台服务端建立连接时应进行双向认证，即客户端软件要验证服务端合法性，服

务端也要验证客户端合法性；

——后台服务端应使用经过行业主管部门认可的第三方认证机构颁发的电子认证证书以标识其真实性；

——安全协议不应包含任何已公开的安全缺陷，无法彻底修复的宜采用其它措施弥补；

——安全协议所使用的对称加密密钥长度不应低于128位，用于签名的RSA密钥长度应不低于1024位，用于签名的SM2密钥长度应为256位；

——经过认证的通讯线路应一直保持安全连接状态；

——客户端软件应确保认证使用的CA根证书真实有效。

7.5.10.2 客户端与SE的通信

客户端与SE的通信应满足如下要求：

——客户端软件应使用安全协议保证与SE通信的秘密性、完整性和真实性，如使用SCP02协议等；

——在建立安全通道之前，SE安全服务应用不应向客户端软件开放任何敏感服务；

——客户端软件与SE的通信应采用一次一密的方式，客户端软件不得在文件系统中存储会话密钥。

7.6 后台服务端

后台服务端应满足如下要求：

——后台服务端应符合JR/T 0068中服务器端安全的要求；

——如果存在独立的线上交易密码，后台服务端应强制要求与银行卡密码不能设置为相同值；

——后台服务端应实现对客户端异常事件的审计功能，应能根据规则进行自动或人工处理，异常事件包括但不限于客户端证书无效、客户端软件版本过旧、报文不合法、密码错误次数超限、数字签名无效、重复报文等，如确定为攻击行为应及时切断与客户端的连接并告警；

——后台服务端应对接收数据的有效性进行校验，防止客户端提交非法数据，进行SQL注入等攻击；

——在后台服务端禁用客户端软件（如手机银行）时，应同时禁用所有通过该客户端软件发起的交易，操作应立即生效；

——后台服务端存储的用户认证要素，例如PIN等，应加密或使用安全哈希函数编码，应能防范统计分析、彩虹表等攻击方式；

——后台服务端在首次上线和发生重大变更时应经过认可的第三方专业检测机构的检测，每年应至少开展一次。

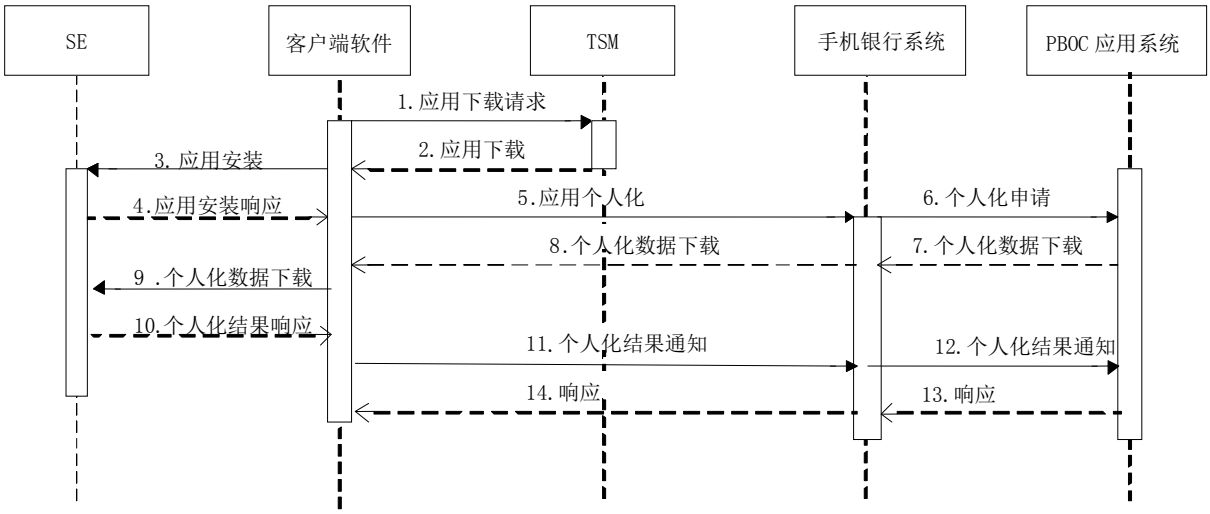
附 录 A
（资料性附录）
基于 PBOC 应用的手机银行

A.1 概述

本附录描述了基于承载于SE（含普通金融IC卡）中的PBOC应用的PKI认证体系，对现有手机银行等业务的交易进行保护的方案。

A.2 应用加载

PBOC应用加载分为预置和动态加载方式，动态加载方式的具体流程如图A.1所示。



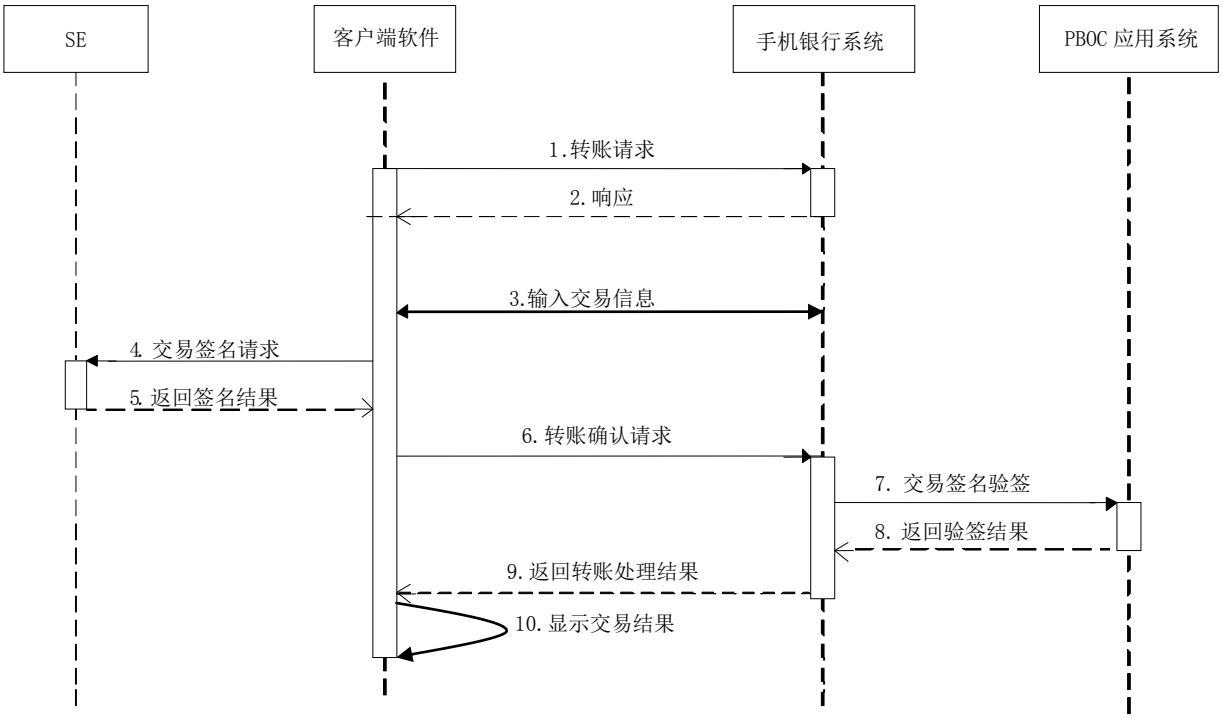
图A.1 PBOC 应用动态加载流程图

步骤1：用户通过客户端软件向TSM系统发出PBOC应用下载请求；
步骤2：TSM系统返回PBOC应用安装文件；
步骤3：客户端软件将TSM系统返回的PBOC应用安装文件发送给SE；
步骤4：SE安装PBOC应用，并返回安装结果给客户端软件；
步骤5：客户端软件发送PBOC应用个人化请求给手机银行系统；
步骤6：手机银行系统验证用户身份，通过验证后将个人化请求转发给PBOC应用系统；
步骤7：PBOC应用系统将个人化数据发送给手机银行系统；
步骤8：手机银行系统将个人化数据转发给客户端软件；
步骤9：客户端软件将个人化数据发送给PBOC应用；
步骤10：PBOC应用进行个人化，并将结果返回给客户端软件；
步骤11：客户端软件将PBOC应用个人化结果发送给手机银行系统；
步骤12：手机银行系统将PBOC应用个人化结果发送给PBOC应用系统；
步骤13：PBOC应用系统返回响应给手机银行系统；

步骤14：手机银行系统返回响应给客户端软件。

A.3 交易签名/验签

在交易过程中PBOC应用使用私钥对交易数据计算签名数据，并将其公钥证书、发卡行公钥证书等信息一起返回。PBOC应用系统根据返回的信息验证签名数据是否一致。具体流程如图A.2所示：



图A.2 PBOC 应用签名流程图

步骤1：用户通过客户端软件向手机银行系统发起转账请求；

步骤2：手机银行系统返回响应给客户端软件；

步骤3：用户根据客户端软件提示输入转入\转出账户信息、账户密码等信息，并确认交易；

步骤4：将交易信息发送给SE内的PBOC应用进行签名处理，签名流程应符合JR/T 0025.4或JR/T 0025.12规定的要求；

步骤5：PBOC应用返回转账交易签名结果、公钥证书等认证数据给客户端软件；

步骤6：客户端软件将要交易数据、签名数据、认证数据统一发送给手机银行系统；

步骤7：手机银行系统将签名数据和认证数据发送PBOC应用系统进行验签请求；

步骤8：PBOC应用系统返回转账交易验签结果；

步骤9：手机银行系统返回转账交易结果给客户端软件；

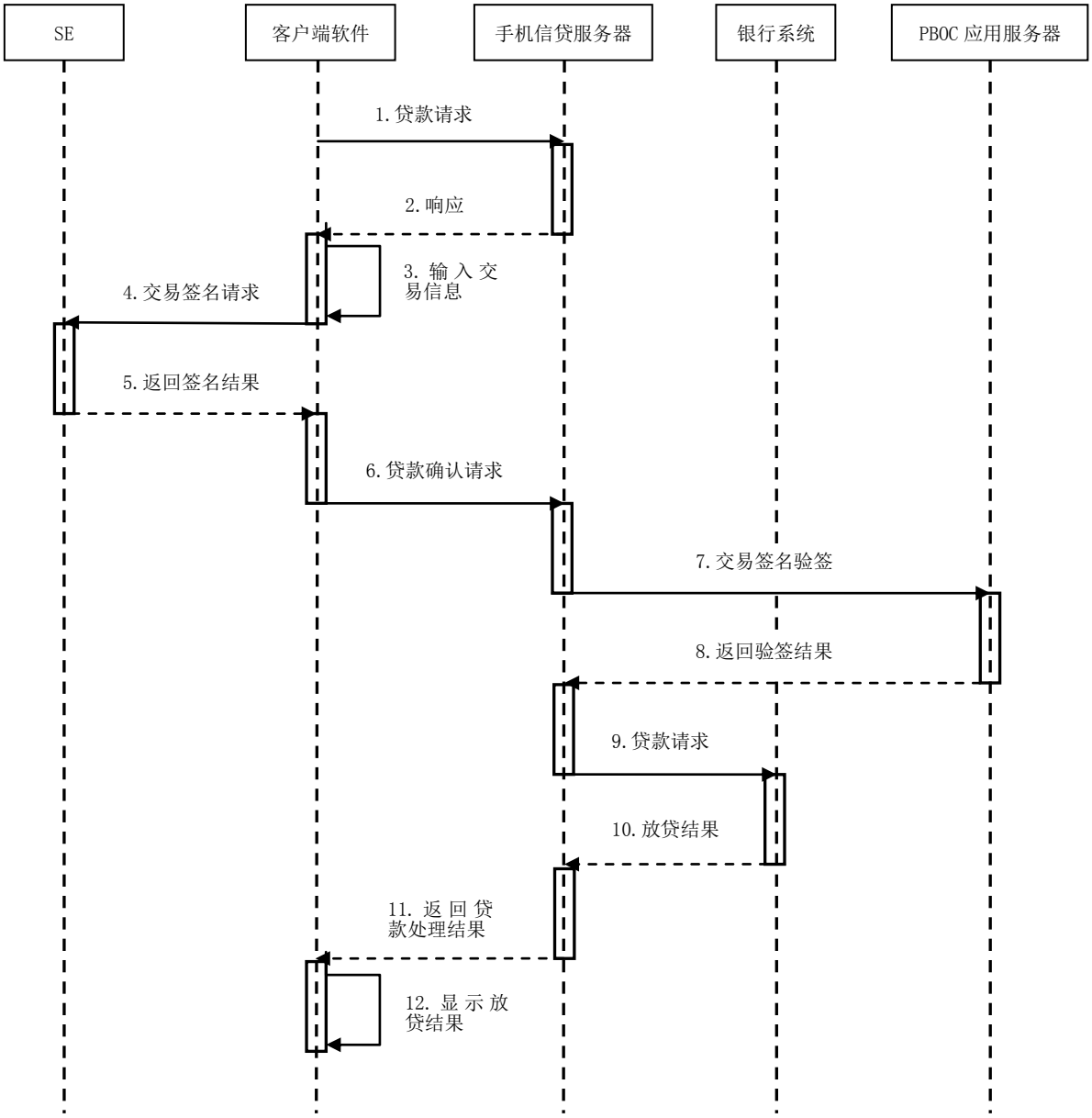
步骤10：客户端软件将交易结果显示给用户。

附 录 B
（资料性附录）
基于 PBOC 应用的手机信贷

B.1 概述

本附录描述了基于承载于SE（含普通金融IC卡）中的PBOC应用的PKI认证体系实现手机信贷业务的方案。

手机信贷是指以SE作为用户身份认证工具和信息存储媒介，通过移动网络来实现自助循环小额贷款，兼具远程交易、近场支付等移动金融功能。手机信贷用户可以通过手机完成贷款、还款和转账等交易。流程如图B.1所示。



图B.1　基于 PBOC 应用的手机信贷流程图

步骤1：用户通过手机客户端应用向手机信贷服务器发起贷款请求；

步骤2：手机信贷服务器返回响应给手机客户端应用；

步骤3：用户根据手机客户端应用提示选择贷款合同，输入贷款金额、期限、账户密码等信息，用户根据返现信息确认交易；

步骤4：经过身份认证后，将贷款交易信息发送给SE内的PBOC应用进行签名处理；

步骤5：PBOC应用返回交易信息签名结果、公钥证书等认证数据给手机客户端应用；

步骤6：手机客户端将交易数据、认证数据统一发送给手机信贷服务器；

步骤7：手机信贷服务器将交易数据、认证数据发送PBOC应用服务器进行验签请求；

步骤8：PBOC应用服务器返回贷款交易验签结果，给手机信贷服务器；

步骤9：手机信贷服务器向银行核心系统发送贷款请求；

步骤10：银行核心服务器处理贷款请求，返回处理结果；
步骤11：手机信贷服务器返回贷款交易结果给手机客户端应用；
步骤12：手机客户端应用将交易结果显示给用户。

B.2 业务流程

基于PBOC应用的手机信贷主要包括激活、贷款、还款、转账、账户余额查询、授信查询、贷款查询、利息试算、交易明细查询等业务功能，本附录仅选取贷款、还款等主要业务流程进行详细描述，其它可参考实现。

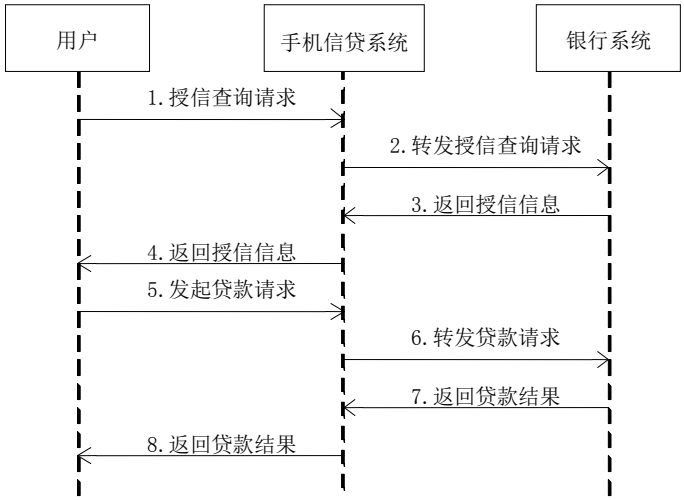
B.2.1 贷款

B.2.1.1 功能说明

用户完成银行贷款授信的前提下，通过操作本功能，将贷款资金直接发放至手机中的PBOC应用账户内。

B.2.1.2 业务流程

贷款业务流程见图B.2。



图B.2 贷款业务流程图

步骤1：用户操作手机终端，向手机信贷系统发起授信查询请求；
步骤2：手机信贷系统向银行系统发起授信查询请求；
步骤3：银行系统下发此用户的授信明细数据至手机信贷系统；
步骤4：手机信贷系统向手机端反馈授信明细数据，并将详细信息展现给用户；
步骤5：用户选择一个授信申请贷款，输入贷款金额、贷款到期日等信息，确认输入无误后，提示输入主账户密码，手机终端向手机信贷系统发起贷款申请；
步骤6：手机信贷系统验证用户贷款信息的合法性，并向银行系统申请请贷款；
步骤7：银行系统处理贷款请求，将贷款资金直接发放至主账户内，并通知手机信贷系统贷款成功；

步骤8：手机信贷系统向手机终端下发贷款成功提示，完成贷款流程。

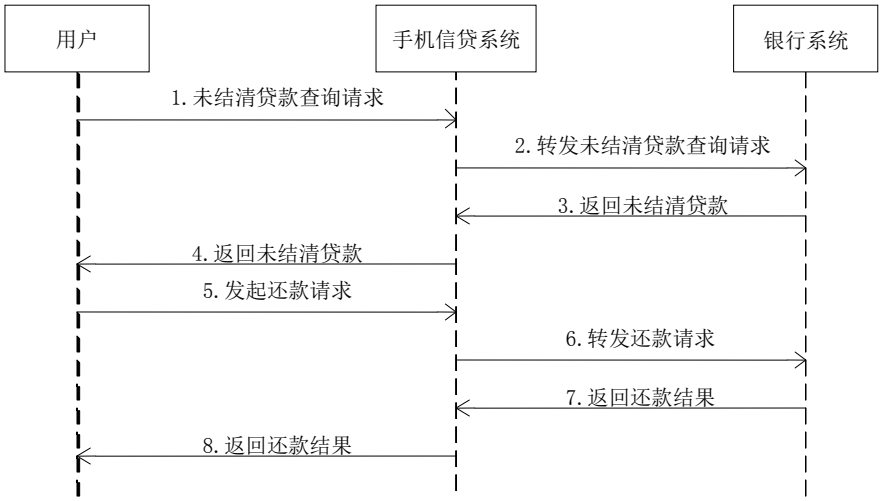
B.2.2 还款

B.2.2.1 功能说明

用户选择一笔未结清的贷款进行还款，并根据此笔贷款详细信息，输入所需归还的金额进行还款。

B.2.2.2 业务流程

还款业务流程见图B.3。



图B.3 还款业务流程图

步骤1：用户选择还款功能，发起贷款账号查询请求；

步骤2：手机信贷系统查询用户所有未结清贷款的贷款账号；

步骤3：所有未结清贷款的贷款账号下发至用户手机，并展现；

步骤4：用户选择所需归还的贷款账号，系统应提示用户输入所需归还的贷款金额，用户输入还款金额并确认无误后，输入主账户密码，上送还款请求；

步骤5：手机信贷系统验证用户上送还款请求数据的合法性，验证通过后转发还款请求给银行系统；

步骤6：银行系统处理还款请求，反馈还款处理成功；

步骤7：手机信贷系统下发还款处理成功通知用户；

步骤8：用户手机端接收到下发结果，提示用户还款成功。

B.3 安全体系架构

手机信贷交易过程中，应确保用户信息、交易信息安全，防止用户敏感信息、核心交易数据被非法窃取或篡改，应基于SE提供多种数据保护措施。

参 考 文 献

[1] GB/T 19713-2005 信息技术 安全技术 公钥基础设施在线证书状态协议
[2] GB/T 20518-2006 信息安全技术 公钥基础设施 数字证书格式
[3] GB/T 25064-2010 信息安全技术 公钥基础设施 电子签名格式规范
[4] GB/T 25069-2010 信息安全技术 术语