ICS 35.240.40
A11

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

JR/T XXXXX—XXXX

中国金融移动支付 远程支付应用 第6部分：基于SE的安全服务

China financial mobile payment--Remote payment application
Part 6: Security service based on SE

（报批稿）

（本稿完成日期：2012年10月22日）

XXXX－XX－XX 发布 XXXX－XX－XX 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6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；

——第5部分：短信支付技术规范；

——第6部分：基于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：。

本部分参加起草单位：。

本部分主要起草人：。

引　言

随着移动支付新业务、新产品、新管理模式的不断涌现，以客户需求为主导的移动支付业务出现了不断交融和细化的趋势，不同机构、不同部门、不同业务之间的信息交换和信息共享变得越来越频繁。统一交易模型、交易流程及报文接口可以有效加强银行、非金融支付服务组织、商户之间的互联、互通及信息共享，降低交易成本，提高市场效率。

考虑到移动支付中远程支付涉及面广、业务种类繁杂以及各商业银行和非金融支付机构的业务系统现状，为便于标准的推广，本标准仅对目前支付业务中比较成熟的、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、或商业银行和非金融支付机构定制的个性化安全服务，在标准后续的修订过程中逐步纳入。

移动支付-远程支付应用 第6部分：基于SE的安全服务技术规范

1 范围

本部分对基于SE远程支付的安全服务进行了抽象和规范，主要描述基于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，及与客户端支付应用软件的层次关系。

本部分适用于移动支付中远程支付业务的SE应用、客户端支付应用软件、远程支付系统的设计、应用开发及检测。

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。

GB/T 25069-2010 信息安全技术 术语

GB/T 25064-2010 信息安全技术 公钥基础设施 电子签名格式规范

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

GB/T 20518-2006 信息安全技术 公钥基础设施 数字证书格式

JR/T ×××× 中国金融移动支付 应用基础 第1部分：术语

3 术语与定义

3.1

电子认证 electronic authentication

指采用PKI技术检验用户合法性的操作。

3.2

电子认证服务 certification service

指为电子签名相关各方提供真实性、可靠性验证的活动。

3.3

假名证书 pseudonym certificate

证书中未载明证书所有者的真实名称，而是以在特定应用环境中具有实际意义的名称作为证书主体标识的证书。

3.4

移动证书 mobile certificate

是指以移动终端作为数字证书载体，采用移动终端硬件作为证书安全保护介质的移动数字证书。

3.5

证书撤销列表 certificate revocation list

一个已标识的列表，指定了一套证书发布者认为无效的证书。

3.6

证书策略 certificate policy

一套指定的规则集，用以指明证书对一个特定团体和（或者）具有相同安全需求的应用类型的适用性；或用以指明证书对于具有相同安全需求的某类应用的适用性。

3.7

证书主体 certificate subject

证书主体是证书公钥对应的实体，它可以是个人、机构、域名等。

3.8

客户 customer

向证书认证机构申请证书的实体，包括个人客户和机构客户。

3.9

服务器证书 webserver certificate

以机构客户名义向证书认证机构申请，用以表示域名或IP地址所有者身份信息的证书。

3.10

私钥 private key

在公钥密码体系中，客户的密钥对中只有客户本身才能持有的密钥。

3.11

公钥 public key

在公钥密码体系中，客户的密钥对中可以被其它客户所持有的密钥。

4 缩略语

定义本规范所使用的缩略语。

COS 卡片操作系统（Chip Operation System）
CRL 证书撤销列表（Certificate Revocation List）
DN 证书主题甄别名（Distinguished Name）
OCSP 在线证书状态协议（Online Certificate Status Protocol）
PIN 个人识别号码（Personal Identification Number）
SSL 安全套接层协议（Secure Sockets Layer）

5 基于 SE 的安全服务应用

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。安全服务作为 SE 的应用，实现了加密、解密、签名、验签等多种功能，对运算及存储有较高等级的安全保护，对外提供了统一的安全服务接口。从而降低了各支付应用提供方在开发电子认证服务时的个性化差异，提高了通用性，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、合理地开展。

SE 安全服务应用作为 SE 的一种标准应用，其使用过程如下：

——应用的安装下载：SE 安全服务应用的生命周期管理应符合 JR/T XXXX 《中国金融移动支付 可信服务管理技术规范》中 7.4 应用生命周期管理的要求；支付机构可以在 SE 中为用户预置应用，也可为用户提供在线方式下载应用，在线下载应用的流程参见 JR/T XXXX 《中国金融移动支付 可信服务管理技术规范》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 安全服务后，需要申请并安装证书后才能使用；

——应用的使用：用户在进行远程支付时，SE 安全服务为移动终端支付应用程序提供了数据的加密/解密、签名/验签等服务。

5.2 与远程支付系统的关系

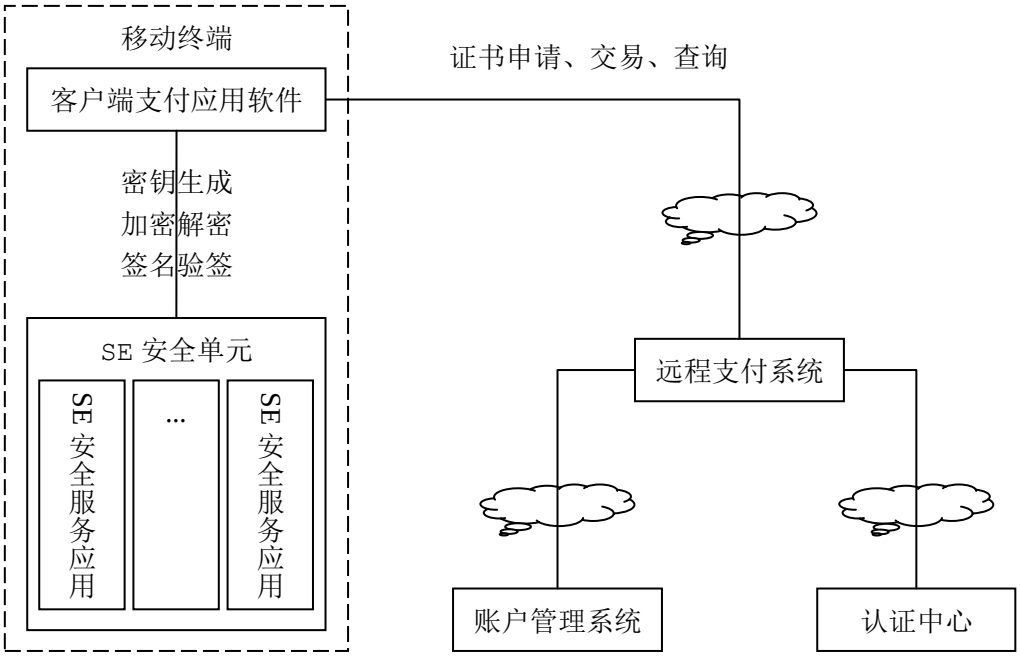

图1 安全服务应用与远程支付系统的关系示意图

图2描述了SE安全服务应用在移动终端中的角色定位，与远程支付系统之间的关系。

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。

在初始化时，首先由客户提交数字证书的申请，远程支付系统进行客户的身份认证与申请验证，再由SE安全服务应用生成密钥并输出公钥，由远程支付系统向认证中心上送公钥，认证中心依据公钥来颁发数字证书，在这个过程中，SE安全服务应用负责密钥的生成与证书的安装。

在交易发生时，由客户端支付应用软件请求，远程支付系统响应，两者之间有着频繁的数据传输，SE安全服务应用使用远程支付系统的公钥对交易数据进行加密，使用客户的私钥对交易数据进行签名等操作，以确保交易的安全性、数据的完整性、行为的不可抵赖。

5.3 应用的层次结构及调用层次

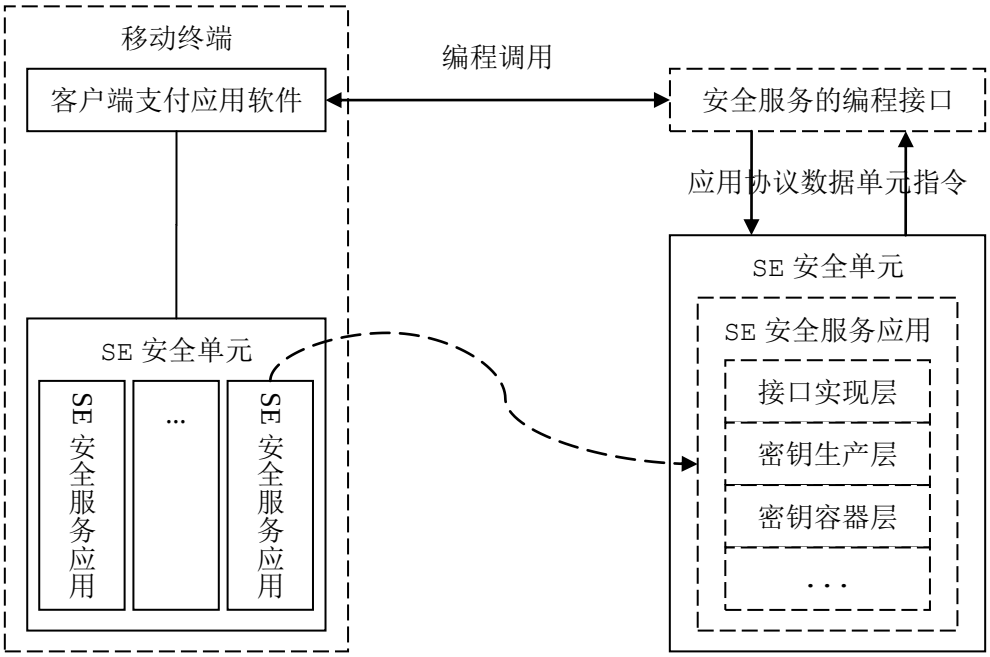

图2 安全服务应用的层次结构与调用关系图

图3描述了客户端支付应用软件与SE安全服务应用之间的调用关系，及后者的层次结构。

任何一次完整的运算过程，均由客户端支付应用软件发起指令，调用安全服务的编程接口，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，直到客户端支付应用软件得到运算结果。

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 服务接口

SE安全服务应用对客户端支付应用软件提供的接口，包括但不仅限于证书申请、证书安装、证书卸载、加密、解密、签名、验签。

客户端支付应用软件与SE安全服务应用在移动终端上的不同安全区域，前者通过调用后者的接口来实现运算，因此后者提供的接口应具有访问控制权限。

5.5 安全服务的实现

5.5.1 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：

1.证书申请/安装

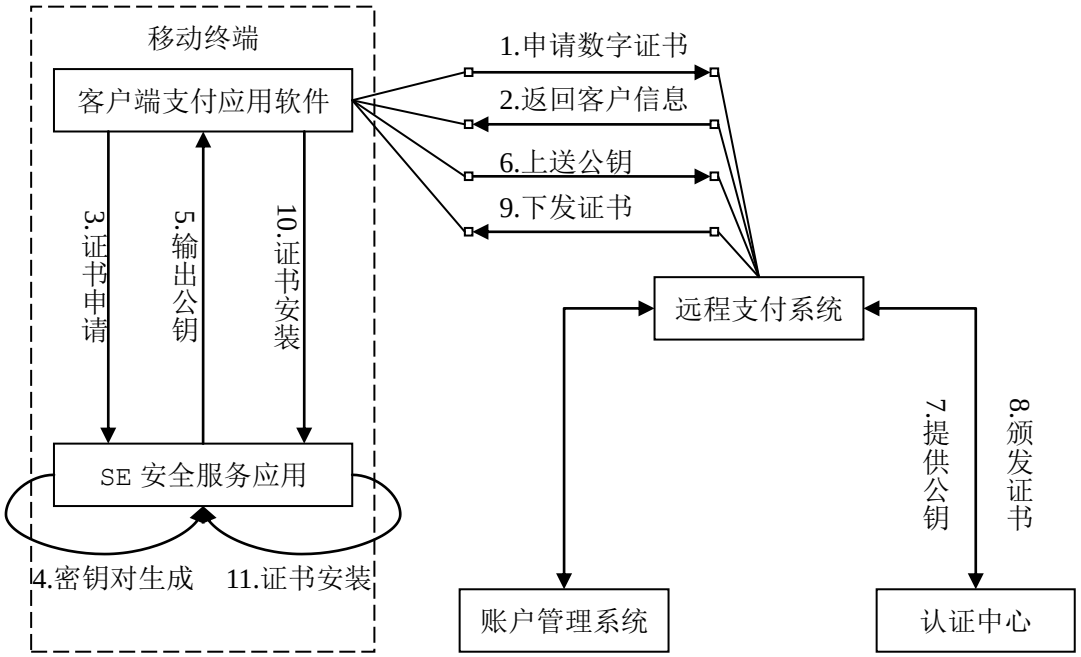

图3　安全服务证书申请的示意图

图4描述了客户从客户端支付应用软件上发起申请，到SE安全服务应用将数字证书安装的过程。

1-客户在客户端支付应用软件上发起数字证书的请求；

2-远程支付系统进行客户的身份认证与请求验证；

3-验证通过后，客户端支付应用软件调用SE安全服务应用的证书申请功能；

4-SE安全服务应用在内容生成密钥对，并存储到密钥容器中；

5-SE安全服务应用以同步方式输出公钥响应客户端支付应用软件；

6-客户端支付应用软件将公钥上送到远程支付系统；

7-远程支付系统将公钥与客户信息提交到认证中心；

8-认证中心进行客户的身份认证与公钥验证后，颁发证书；

9-远程支付系统接收到数字证书后，将下发到客户端支付应用软件；

10-客户端支付应用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；

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。

2.证书卸载

卸载一个数字证书,文件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丢失,需要满足访问控制权限，才能够卸载。

3.读取证书列表

读取密钥容器中的所有数字证书。

4.读取指定证书

根据证书的序列号、主题、有效的起止日期等检索到指定的数字证书。

5. 加密/解密

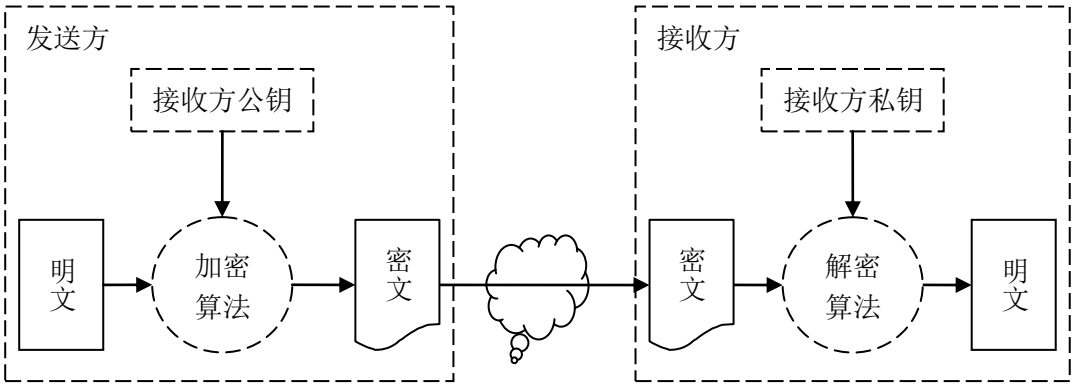

图4　安全服务应用的加密与解密示意图

图5描述了SE安全服务应用基于数字证书的非对称加密方式完成加密与解密的过程。

客户端支付应用软件作为交易数据的发送方，在交易数据传输前，会获取到接收方远程支付系统的公钥数字证书，而接收方的私钥则始终保存在远程支付系统中。

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

6. 签名/验签

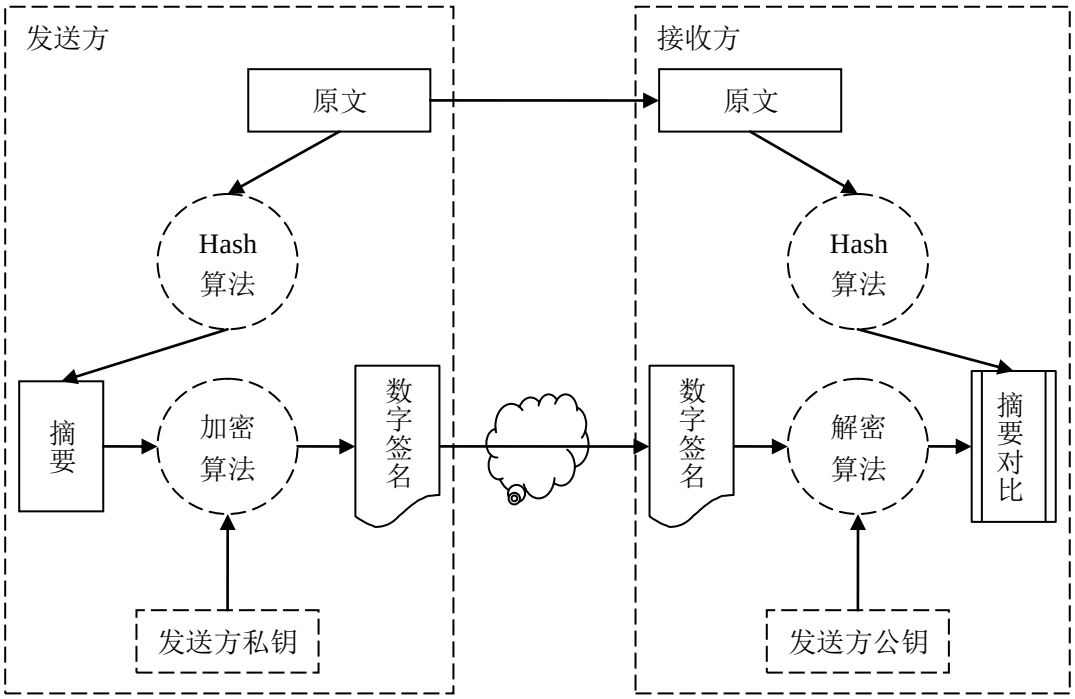

图5　安全服务应用的签名与验签示意图

图6描述了SE安全服务应用基于数字证书的非对称加密方式完成签名与验签的过程。

远程支付系统作为交易数据的接收方，在数字证书申请安装过程中，会接收到认证中心颁发给客户的数字证书，客户端支付应用软件作为交易的发起方，只能通过SE安全服务应用才能调用客户的私钥。

在交易数据传输前，发送方将原文按照约定的Hash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Hash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。

5.5.2 密钥生成层

密钥生成层的功能包括但不仅限于：

1. 密钥对生成

密钥对生产后，SE安全服务应用会将生成的公钥和私钥分别写到不同的文件中，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。

2.私钥签名

采用私钥对原文的Hash运算结果摘要进行加密所得签名，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，应具备较高的访问控制权限。

3.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、主题、有效的起止日期才能调用。

私钥的访问除与公钥数字证书对应外，应具备如客户身份认证等较高的访问控制权限。

4.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。

5.删除过期私钥

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

5.5.3 密钥容器层

密钥生成层的功能包括但不仅限于：

1.容器的实现

一个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，需要为每个密钥容器指定唯一的名称。

2.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。

3.证书的导入

数字证书安装时，需要将数字证书导入到容器中，并与之前的密钥对匹配关联。

4.证书的导出

数字证书导出时，需要将容器中的数字证书复制一份并输出。

5.证书的删除

数字证书删除时，需要将数字证书与匹配的密钥对一起清除，释放容器的空间。

6.证书的读取

数字证书的读取，会根据序列号、主题、有效的起止日期检索到指定证书。

7.证书的枚举

数字证书的枚举，不设定任何条件，列举所有的数字证书，仅限于内部实现，不对外暴露接口。

8.证书调用的访问控制

数字证书明确指定了证书的使用者，在用户运行客户端支付应用软件时，应调用该用户账户授权的数字证书，其它数字证书不应授权调用。

5.6 安全服务的作用

5.6.1 身份认证

证书认证机构签发的数字证书包含了证书客户的身份信息，交易各方可以利用数字证书验证对方身份的真实性。

签发给客户的证书标识了客户的身份，是各支付机构验证客户身份，允许客户使用客户端支付应用软件与远程支付系统进行各种交易活动的身份凭证。各支付机构客户证书采用假名证书的，假名证书应符合《金融领域电子认证服务规范》中对假名证书的要求。

签发给各支付机构的服务器证书，标识了各支付机构的身份，是客户验证支付机构真实性，防止假冒站点的有效手段。

签发给各支付机构的代码签名证书，标识了各支付机构所提供的代码软件的身份，保证客户所下载的代码软件来源于所信任的机构。

5.6.2 电子签名

在远程支付的各支付应用中，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。

5.6.3 加密解密

在远程支付的各支付应用中，交易一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，可确保数据只有持有相应私钥的人才可以解密，保证了信息的机密性。

6 安全服务数字证书应用

6.1 身份认证

6.1.1 证书认证机构

在移动支付业务中采用电子认证服务，各支付机构选择合作的证书认证机构，其获取的《电子认证服务许可证》、提供的数字证书、电子认证服务均是行业主管部门认可的。

各支付机构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，以及由电子认证服务引起的纠纷的处理流程和赔偿事宜。

6.1.2 数字证书业务办理

各支付机构接受证书认证机构委托，为客户提供数字证书业务办理服务的，应遵循《电子认证服务管理办法》（中华人民共和国工业和信息化部令 2009 年第 1 号）中的相关条款要求开展；委托方与被委托方的权限和责任应在各支付机构与证书认证机构的合作协议或合同中予以明确。

6.1.3 证书与应用的关联

客户申领数字证书后，各支付机构应将客户的数字证书信息注册到远程支付系统中，并与相关的账户信息如客户账号、客户名称、移动终端标识等进行关联。

远程支付系统中所记录的证书信息必须是证书的唯一识别信息，如证书主题甄别名（即证书DN），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他证书信息。

6.1.4 客户身份认证

各支付机构采用数字证书验证客户的身份，必须符合如下要求：

1. 客户的电子签名作为各支付机构鉴别客户身份的必要因素；
2. 客户的电子签名应符合6.3.1节要求；
3. 各支付机构必须验证客户签名的有效性；
4. 各支付机构必须验证产生签名的数字证书与客户关联的一致性；
5. 各支付机构应遵循6.3.2节要求完成对客户证书验证处理。

6.2 安全要求

6.2.1 密钥对生成

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素数。

6.2.2 SE 安全服务应用

SE安全服务应用，作为远程支付客户端支付应用软件运行的基础，应满足如下要求：

——主文件(Master File)应受到 COS 安全机制保护，保证客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客户身份鉴别；
- 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际通用标准的要求；

——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；
- PlN 码连续输错次数达到错误次数上限(不超过 6 次)，SE 安全服务应用应锁定；
- 使用的密码算法应是行业主管部门认定的。

6.3 电子签名

6.3.1 电子签名要求

使用电子签名技术产生电子签名，应满足如下要求：

1. 签名者证书的密钥用法必须包含“电子签名”；
2. 签名只能由签名私钥计算；签名私钥采用SE保护且签名运算必须在SE内完成；
3. 所使用的签名算法应采用行业主管部门批准使用的签名算法；
4. 所使用的数据摘要算法应采用行业主管部门批准使用的数据摘要算法。

6.3.2 数字证书验证

验证证书的内容，必须包括如下基本验证：

1. 验证证书的颁发者名称与颁发者证书的主体名称匹配；
2. 验证证书的签名并确保签名算法是行业密码主管部门批准使用的算法；
3. 验证证书的有效期；
4. 验证证书的密钥用法与业务系统应用需求相符；
5. 正确构造证书链到受信任的颁发者；
6. 验证证书符合金融领域证书策略；
7. 各支付机构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；
8. 各支付机构根据应用安全要求，验证证书中与应用相关的其它信息。

6.3.3 电子签名认证

1. 遵循6.3.2节要求完成对客户证书验证处理；
2. 验证签名的有效性；
3. 验证签名算法应使用行业主管部门批准使用的算法；
4. 验证签名所使用的数据摘要算法是行业主管部门批准使用的算法；
5. 必须验证产生签名的数字证书与客户关联的一致性。

6.4 加密解密

6.4.1 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：

1. 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；
2. 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。

6.4.2 非对称加密解密

使用数字证书实现非对称加解密功能，应满足如下要求：

1. 加密证书的密钥用法必须包含“数据加密”；
2. 数据加解密应采用行业主管部门认可的非对称密码算法；
3. 数据加密须先检查接收方加密证书的有效性，不应使用无效证书向其持有人发送加密数据；
4. 如有在客户端进行解密的需求，则解密私钥运算必须在SE安全服务应用内部完成。

6.4.3 数字信封加解密

使用数字证书来实现数字信封的功能，应满足如下要求：

1. 加密证书的密钥用法必须包含“数据加密”；
2. 数据加解密应采用行业主管部门认可的密码算法，包括对称算法与非对称算法；
3. 数据加密须先检查接收方加密证书的有效性，不应使用无效证书向其持有人发送加密数据。

参 考 文 献

[1] 《中华人民共和国电子签名法》（中华人民共和国主席令第十八号）
[2] 《电子支付指引（第一号）》（中国人民银行 [2005] 23号文印发）
[4] 《网上银行系统信息安全通用规范<试行>》（中国人民银行 2010年1月）
[5] 《关丁进一步加强银行业金融机构信息安全保障工作的指导意见》(银发[2006]123号文印发）