ICS 35.040
L80

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术 移动签名通用技术规范

Information security technology – Technical requirements of mobile signature

点击此处添加与国际标准一致性程度的标识

（征求意见稿）

（本稿完成日期：2017 年 6 月）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准依据GB/T 1.1-2009《标准化工作导则 第1部分：标准的结构和编写》给出的规则起草。

本标准由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本标准起草单位：中国移动通信集团公司、中国信息通信研究院、北京数字认证股份有限公司。

本标准主要起草人：杨志强、张滨、于蓉蓉、袁捷、刘海龙、罗红、路晓明、杨超、董靖宇、邱勤、霍薇靖、蔡准、杨正军、马臣云、林雪焰。

信息安全技术
移动签名通用技术规范

1 范围

本标准规定了实现移动签名的通用方法，包括基本框架、基本流程、参与实体功能、接口功能及安全要求等。

本标准适用于采用具备移动通信功能的设备或移动设备中的专用安全模块作为电子签名生成装置的情形。

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，其最新版本适用于本文件。

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 25065-2010 信息安全技术 公钥基础设施 签名生成应用程序的安全要求

GB/T 25056-2010 信息安全技术 证书认证系统密码及其相关安全技术规范

RFC2986 PKCS #10: Certification Request Syntax Specification

3 术语和定义

GB/T25064-2010、GB/T 25065-2010确立的以及下列术语和定义适用于本文件。

3.1

应用提供者 application provider

为用户提供某种服务或应用的实体。

3.2

移动签名 mobile signature

采用移动设备对数据电文进行电子签名的通用方法。

3.3

移动签名服务 mobile signature service

由某机构提供、能够帮助应用提供者和用户实现移动签名功能的业务。

3.4

移动签名服务提供者 mobile signature service provider

向应用提供者和公众提供移动签名服务的机构实体。

3.5

移动签名生成设备 mobile signature creation device

签名人所持有的、能够生成电子签名的独立移动设备或移动设备的内置模块。

4 缩略语

下列缩略语适用于本文件：

AP：应用提供者（Application Provider）

ATM：自动柜员机（Automatic Teller Machine）

CA：证书认证机构（Certification Authority）

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

MSCD：移动签名生成设备（Mobile Signature Creation Device）

MSSP：移动签名服务提供者（Mobile Signature Service Provider）

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

PIN：个人身份识别码（Personal Identification Number）

PKCS：公钥密码标准（Public-Key Cryptography Standards）

PKI：公钥基础设施（Public Key Infrastructure）

RA：注册机构（Registration Authority）

5 移动签名概述

5.1 移动签名

移动签名是指采用具备移动通信功能的电子设备或移动设备中的专用安全模块对数据进行电子签名的通用方法。

移动签名的主要特征在于，当用户需要对某交易进行签名确认时，用户会触发业务服务器将待签数据通过移动网络传输到用户的移动设备，用户在该移动设备上完成对待签数据的签名，并将签名结果返回至业务服务器进行验证。

移动设备是指用户可随身携带、并能够随时接入移动通信网络的计算设备，如手机、平板电脑、笔记本或其他专用设备。为实现签名功能，移动设备中需有一个独立的安全模块，由该模块来对待签数据进行计算，以生成电子签名，该模块称为移动签名生成设备（MSCD）。

5.2 移动签名的基本特征

移动签名具有如下基本特征：

a) 终端无关性

移动签名采用从网络侧获取待签数据的方式,无需签名设备与业务终端相连,从而具备终端无关性。用户无论采用什么样的设备来操作业务流程，如电脑、笔记本、平板电脑、手机、电视、电话、自动柜员机（ATM）等，都可触发业务系统将需要签署的交易数据发送到用户随身携带的移动签名生成设备中，在该设备上完成确认、签名，从而使任何终端上的交易都可得到电子签名的保护。

b) 业务无关性

移动签名作为一种通用方法可用于各种业务，无需改变业务与证书认证机构（CA）的固有信任关系，实现了业务无关性。MSCD 作为一个公共设备可存储用户的多个私钥，当用户需要在某个业务中使用电子签名时，只需到该业务所信任的 CA 申请一张证书，并将证书及其对应的私钥存储到 MSCD 中，即可使用 MSCD 对该业务中的交易进行签名，无需因使用不同的业务而持有多个签名硬件设备。

综上，移动签名不仅可以节约成本（无需多个签名硬件设备），降低用户操作复杂度（无需安装客户端程序），还可最大限度地发挥电子签名对电子交易的保护作用（适用于各种形态的业务终端、各种业务）。

5.3 移动签名服务的相关实体

移动签名的形成和使用过程中共涉及四类实体：用户、应用提供者（AP）、证书认证机构（CA）和

移动签名服务提供者（MSSP），各实体的作用描述如下，相互基本关系如图 1 所示：

a) 用户，即电子签名人，是移动签名服务的使用者，用户在 AP 的网站上选择商品或服务，并进行交易，用户需要对交易数据进行签名，代表自己对交易内容的认可。帮助用户随时随地实现电子签名的设备为移动签名生成设备（MSCD）。

b) AP 是向用户提供业务的实体，AP 需要验证用户的签名，通过验证的结果来判断当前交易是否是真实用户的行为，故 AP 是电子签名依赖方。

c) CA 作为电子认证服务机构为用户签发数字证书，CA 应保证所签发证书的真实、可信。AP 在验证签名时应首先验证用户的数字证书，故 AP 需信任 CA。

d) 移动签名服务提供者（MSSP）是提供移动签名服务的实体，MSSP 介于用户与 AP、CA 之间，主要实现如下两个功能：

   1) 作为用户与 CA 的连接桥梁，协助 CA 能够实现对用户 MSCD 中证书的生命周期管理，如申请、更新、撤销；

   2) 作为用户与 AP 的连接桥梁，实现 AP 与用户之间待签数据与签名结果的传递，使 AP 中的交易能够得到电子签名的保护。

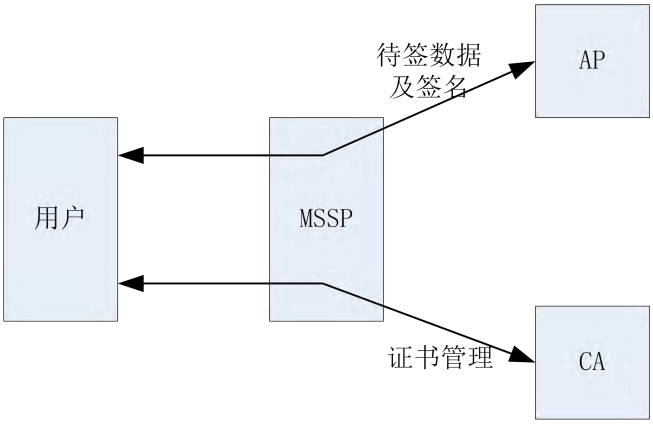

图 1　移动签名的基本框架

6　业务流程

6.1　移动签名基本流程

移动签名的基本实现流程如图 2 所示。

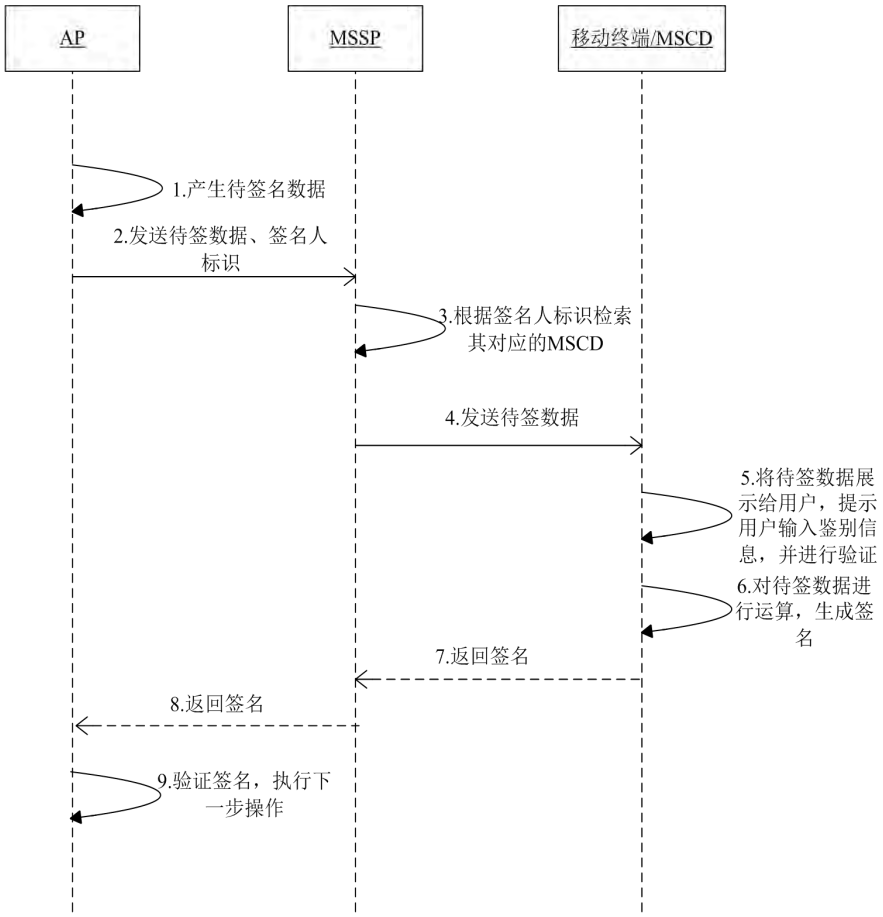

图 2　移动签名的基本流程

用户访问应用提供者（AP），当需要用户对某消息进行确认时，即可触发 AP 发起一个移动签名流程：

1）　AP 产生待签数据；
2）　AP 将待签数据及签名人标识发送给移动签名服务提供者（MSSP）；
3）　MSSP 根据签名人标识检索对应的移动终端/MSCD；
4）　MSSP 将待签数据转发给移动终端/MSCD；
5）　移动终端/MSCD 将待签数据展示给用户，提示用户输入鉴别信息，并对鉴别信息进行验证；
6）　验证通过后，移动终端/MSCD 对待签数据进行运算，生成对应该消息的电子签名；
7）　移动终端/MSCD 将签名结果返回给 MSSP；
8）　MSSP 将进一步将签名结果返回给 AP；
9）　AP 对签名进行验证，根据验证结果来执行对应操作。

6.2　业务管理相关流程

移动签名向用户及应用提供服务时，MSSP 需提供如下业务流程：

a）　对用户的业务流程
　　1）　申请/受理
　　2）　业务开通

3) 业务暂停及恢复
4) 业务注销
5) 客户服务

b) 对 AP 的业务流程
1) 申请/受理
2) 业务开通
3) 业务暂停及恢复
4) 业务注销
5) 业务查询
6) 客户服务

c) 对 CA 的业务流程
1) 申请/受理
2) 业务开通
3) 业务暂停及恢复
4) 业务注销
5) 业务查询
6) 客户服务

6.3 证书管理相关流程

6.3.1 概述

本标准所述流程中，均将 MSSP 作为可信实体。用户在 MSSP 申请移动签名业务后，还需申请目标 AP 所信任 CA 的证书，才能实现在该 AP 上使用移动签名。MSSP 应提供完善的证书管理流程，以保证签名服务的连续性。证书管理相关流程应包括：

a) 证书申请；
b) 证书更新；
c) 证书撤销；

本标准除下述流程外，其它证书管理流程或协议均参照相关国家标准执行。

6.3.2 证书申请

第三方 CA 证书申请需包含两个过程：身份审核/预受理和证书申请/下载。

a) 身份审核/预受理

身份审核/预/受理指的是用户到 CA 的指定网点提出证书申请请求，CA 受理用户的请求，核实用户合法身份。身份审核/预受理过程是 CA 证书生命周期管理的原有流程，除应符合 CA 自身的安全要求外，还应实现 MSCD 与真实身份的绑定，并为用户颁发授权码（authorization code），以便后续下载证书使用。

b) 证书申请/下载

用户在完成业务层面证书申请/受理流程之后，即可进行技术层面证书申请/下载，如图 3 所示。

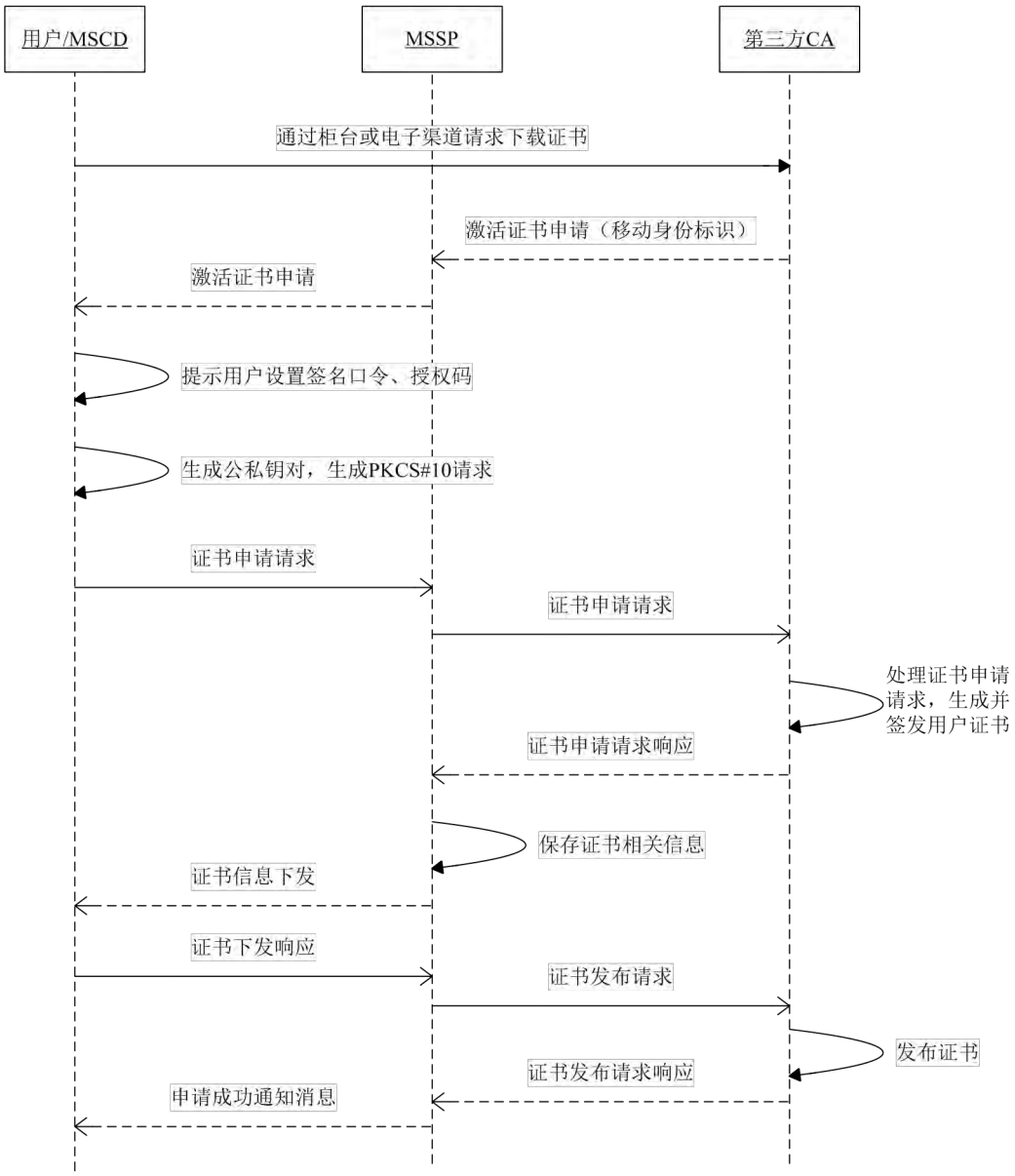

图 3　用户证书申请下载/流程

证书申请/下载的过程如下：

1） 通过柜台或电子渠道请求证书下载；
2） CA 向 MSSP 发送激活证书申请；
3） MSSP 向用户 MSCD 发送激活证书申请指令；
4） MSCD 提示用户设置签名口令，输入授权码；
5） MSCD 生成公私钥对，生成符合 PKCS#10（参见 RFC2986）格式的证书请求；
6） MSCD 向 MSSP 发起证书申请请求；
7） MSSP 向 CA 发送证书申请请求；
8） CA 处理证书申请请求，生成并签发用户证书；
9） CA 向 MSSP 返回证书申请请求响应，其中包含用户证书；
10）MSSP 解析证书，保存证书相关信息；
11）MSSP 向用户 MSCD 发送证书信息下发指令，其中含有证书或部分证书信息；

12) 用户 MSCD 向 MSSP 发送证书下发响应；
13) MSSP 将证书发布请求发送至 CA；
14) CA 根据证书发布请求发布证书；
15) CA 向 MSSP 返回证书发布请求响应；
16) MSSP 向用户发送提示消息（如明文短信），提示用户证书申请成功。

6.3.3 证书更新

为增强用户体验，应支持服务器侧发起的证书更新。根据实际需求，证书更新可从 MSSP 发起，也可从 CA 发起，如图 4 所示。

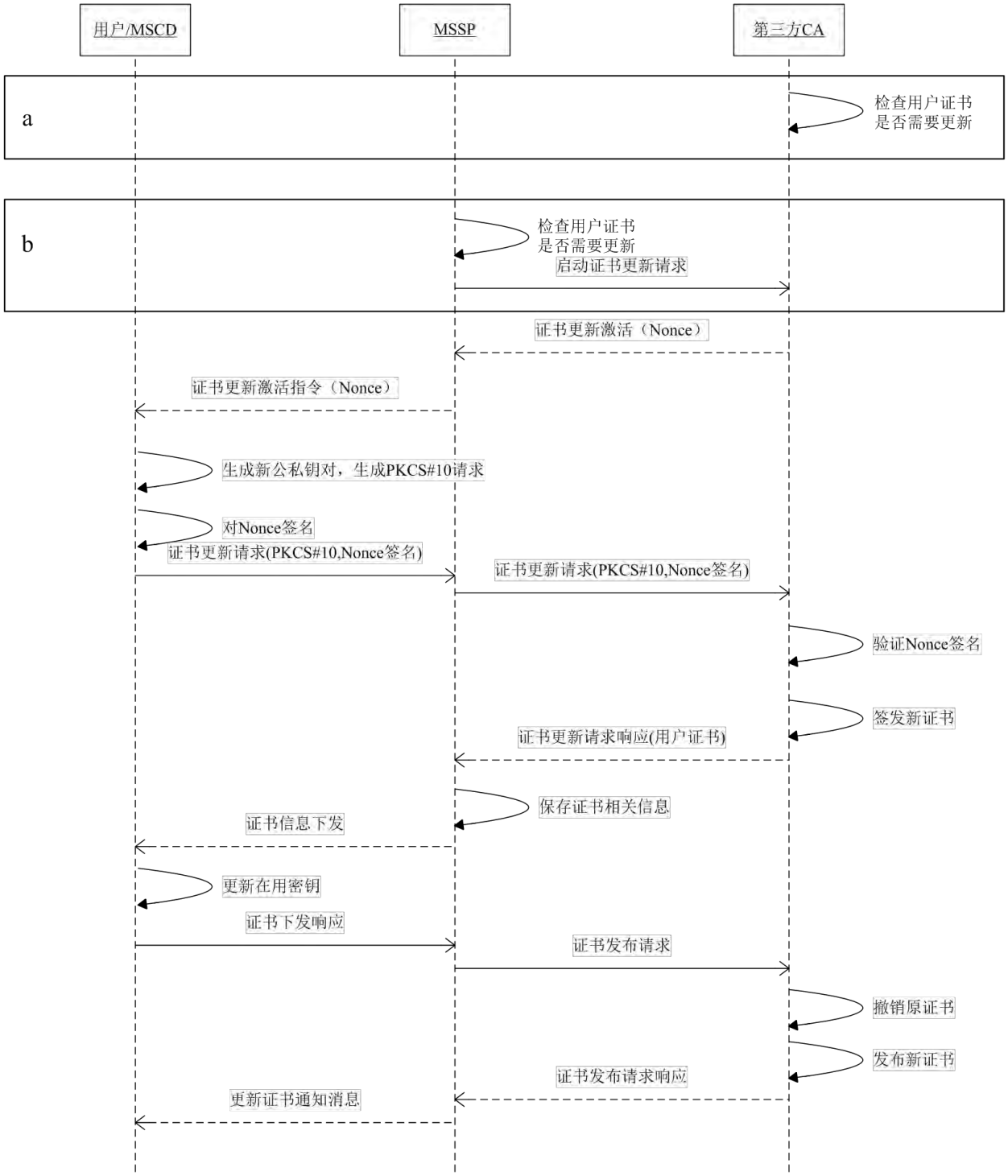

图 4　证书更新流程

证书更新的具体过程如下：

1）　相关方发起证书更新流程，证书更新流程具有两种发起方式：

a）　CA 发起方式

i.　　CA 检查用户证书的有效期，根据预定策略判断用户是否需要更新证书；

b）　MSSP 发起方式

i. MSSP 检查用户证书的有效期，根据预定策略判断用户是否需要更新证书；
ii. MSSP 向 CA 发送启动证书更新请求；

2) CA 向 MSSP 发送证书申请激活消息，该指令包含一个随机数（Nonce）；
3) MSSP 向用户 MSCD 发送证书申请激活指令；
4) 用户 MSCD 收到激活指令后，生成新的公私钥对，并生成 PKCS#10 请求；
5) 用户用原私钥对 Nonce 进行签名；
6) MSCD 将证书更新请求给 MSSP，包含 PKCS#10 请求、Nonce 签名；
7) MSSP 将 PKCS#10 请求、Nonce 签名发送至 CA；
8) CA 验证 Nonce 签名，鉴别签名人身份；
9) CA 处理 PKCS#10，签发新证书；
10) CA 返回新证书给 MSSP；
11) MSSP 解析证书，保存证书相关信息；
12) MSSP 下发证书信息给 MSCD；
13) MSCD 启用新密钥，并删除旧密钥；
14) MSCD 发送证书下发响应给 MSSP；
15) MSSP 发送证书发布请求给 CA；
16) CA 撤销用户原证书；
17) CA 发布用户新证书；
18) CA 向 MSSP 发送证书发布请求响应；
19) MSSP 向用户发送证书更新成功消息。

6.3.4 证书撤销

移动签名应支持两种形式的撤销流程：

a) 用户主动发起撤销流程；
b) MSSP 判断需撤销证书，发起撤销流程。

证书撤销流程如图 5 所示。

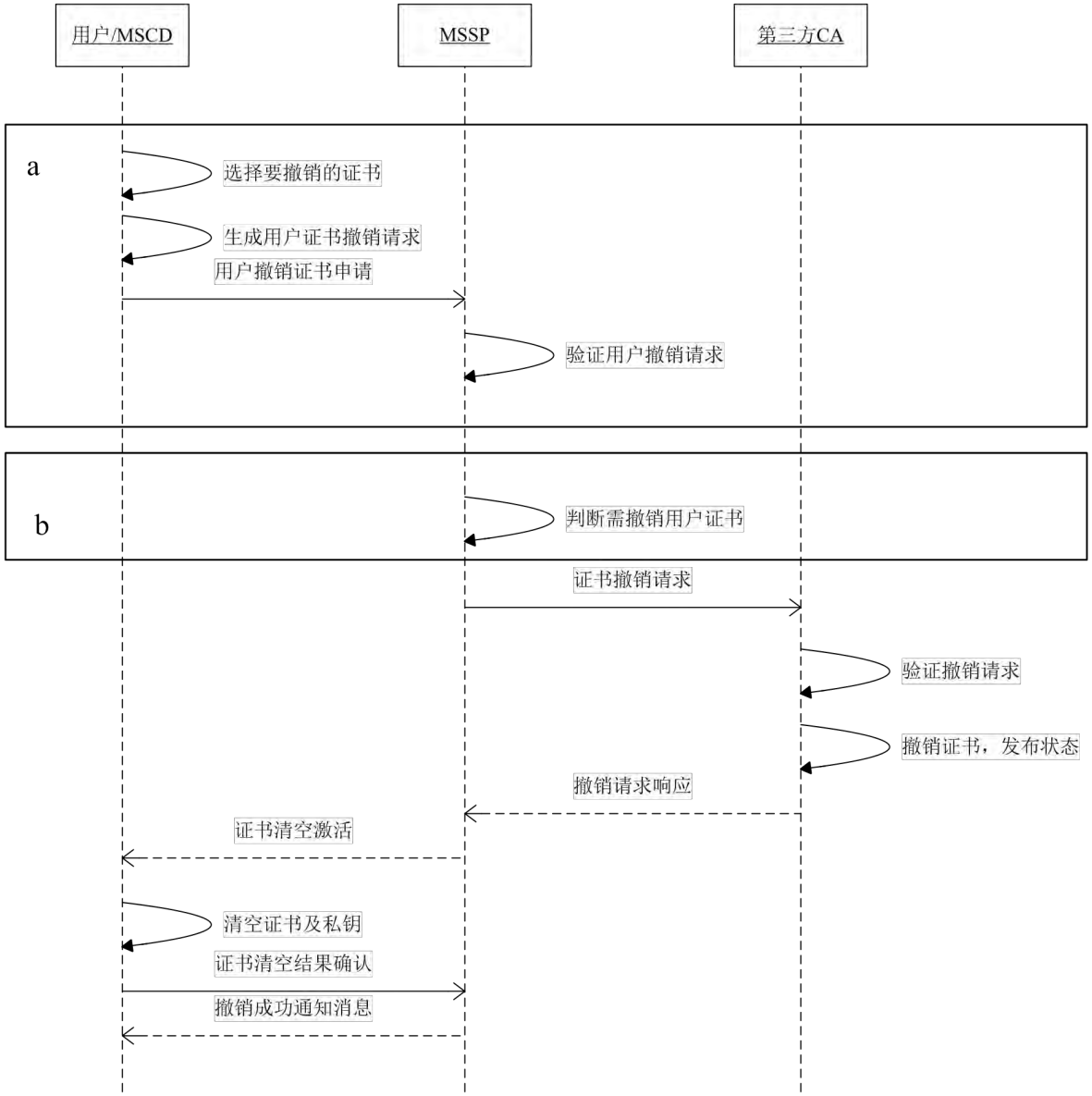

图 5　证书撤销流程

证书撤销的具体过程如下：

1) 相关方发起证书撤销流程，包括两类撤销证书发起方式：
   a) 用户主动撤销
      i. 用户在 MSCD 中需撤销的证书；
      ii. MSCD 生成用户证书撤销请求；
      iii. MSCD 向 MSSP 发起用户证书撤销申请；
      iv. MSSP 验证用户证书撤销请求；
   b) MSSP 发起撤销
      i. MSSP 判断需撤销用户证书，如得知用户的 MSCD 遗失或更换
2) MSSP 向第三方 CA 发起证书撤销请求；
3) CA 验证证书撤销请求；
4) CA 撤销用户证书，并发布状态；

5) CA 向 MSSP 发送证书撤销请求响应；
6) MSSP 向 MSCD 发送证书清空激活指令；
7) MSCD 清空自身所存储的证书及私钥；
8) MSCD 向 MSSP 发送证书清空结果确认；
9) MSSP 向用户发送证书撤销成功通知消息。

7 实体功能

7.1 移动签名服务提供者（MSSP）

MSSP 平台作为移动签名服务系统的核心业务平台，应具备如下功能：

a) 对用户、AP 及第三方 CA 进行管理，应能实现对这三类实体的业务管理，如增加、删除、修改等操作；
b) 允许多 CA 接入，AP 可根据自己的需要选择所信任的 CA，用户可选择不同的 CA 申请证书；
c) 签名事务管理，MSSP 应提供完善的签名事务管理机制，保证用户的每一次签名操作都能够走完全部流程，若无法完成全部流程，则需要明确提示 AP 和用户签名未完成；
d) 证书生命周期管理，对于证书申请、更新、撤销等管理流程，MSSP 应提供相应的差错管理机制，最大限度保持流程的完整性，若无法完成时，需明确提示 CA 和用户；
e) 安全管理，MSSP 应提供相应的安全通信机制，以确保其与 MSCD、AP、CA 之间的通信安全；
f) 历史交易记录管理，MSSP 应移动签名、证书管理等操作进行历史交易记录管理，用户、AP、CA 可分别进行交易记录查询、统计等。

7.2 移动签名生成设备（MSCD）

移动签名生成设备（MSCD）应满足如下要求：

a) 具备密码运算功能，能够实现签名/验签等功能，密码算法应符合国家密码主管部门的相关规定；
b) 应能实现私钥安全存储功能，不提供私钥导出指令，并能够抵御物理攻击；
c) 签名消息显示，为实现“所见即所签”，MSCD 应具备显示功能，用户可根据显示的待签数据核查是否为当前交易；
d) 签名人鉴别功能，MSCD 在启用私钥进行签名之前，应对签名人进行鉴别，如口令或生物识别方式，只有鉴别通过才能生成签名，若鉴别不通过，则应拒绝生成签名；
e) 签名人鉴别数据管理，MSCD 应对签名人鉴别数据提供安全管理机制，保证该数据不能被导出，也能防止穷举攻击；
f) 签名交易记录管理，MSCD 应能够保存签名历史交易记录，供用户事后查看。

8 接口功能

8.1 MSSP 与 AP 之间的接口

8.1.1 签名请求

该接口用于 AP 向 MSSP 发起签名请求，其中应包含待签数据和签名人标识。

8.1.2 签名结果推送

该接口用于 MSSP 向 AP 推送签名结果，其中包含用户签名结果。

8.1.3 状态查询

该接口用于 AP 向 MSSP 查询某次签名交易的状态，MSSP 在查询当前交易的状态，并将结果返回。

8.2 MSSP 与 MSCD 之间的接口

8.2.1 用户签名

该接口用于实现用户的签名操作，包含签名请求和签名响应两条消息。

a) 签名请求：MSSP 向 MSCD 发送，其中包含待签数据。

b) 签名响应：MSCD 向 MSSP 发送，其中包含签名结果或用户取消信息。

8.2.2 证书申请

该接口用于 MSCD 通过 MSSP 实现证书申请/下载操作，包含证书申请激活指令、证书申请请求、证书信息下发、证书下发响应四条消息：

a) 证书申请激活指令：MSSP 向 MSCD 发送，用于激活 MSCD 的证书申请界面，提示用户可进行证书申请；

b) 证书申请请求：MSCD 向 MSSP 发送，其中包含 MSCD 内生成的 PKCS#10 格式的证书申请；

c) 证书信息下发：MSSP 向 MSCD 发送，其中包含用户证书或根据证书解析出来的信息，以供用户查看；

d) 证书下发响应：MSCD 向 MSSP 发送，作为证书信息下发的响应，表示 MSCD 已正确处理证书信息。

8.2.3 证书更新

该接口用于实现 MSCD 内的证书更新操作，包含证书更新激活指令、证书更新请求、证书更新信息下发、证书下发响应四条消息：

a) 证书更新激活指令：MSSP 向 MSCD 发送，用于激活 MSCD 内的证书更新界面，提示用户可进行证书更新；

b) 证书更新请求：MSCD 向 MSSP 发送，其中包含 MSCD 新生成的 PKCS#10 证书请求及认证信息；

c) 证书更新信息下发：MSSP 向 MSCD 发送，其中包含新的用户证书或用新证书解析出来的信息；

d) 证书下发响应：MSCD 向 MSSP 发送，作为证书更新信息下发的响应，表示 MSCD 已正确处理证书更新信息，可以启用新密钥对。

8.2.4 证书撤销

该接口用于实现 MSCD 内的证书撤销操作，包括用户证书撤销请求、证书清空激活指令、证书清空结果确认：

a) 用户证书撤销请求：MSCD 向 MSSP 发送，表示用户要撤销当前证书；

b) 证书清空激活指令：MSSP 向 MSCD 发送，用于激活 MSCD 内部程序，清空当前证书及对应的私钥；

c) 证书清空结果确认：MSCD 向 MSSP 发送，告知 MSSP 当前证书及私钥清空完成。

8.3 MSSP 与 CA 之间的接口

8.3.1 证书申请

在证书申请过程中，MSSP 与 CA 之间可能需要进行多次交互，可包含如下消息：

a) 证书申请激活：CA 向 MSSP 发送，表示 CA 要激活某用户来申请证书，MSSP 在接到该指令后应向对应的 MSCD 发送证书申请激活指令；

b) 证书申请请求：MSSP 向 CA 发送，表示当前用户要申请证书，其中包含由 MSCD 生成的 PKCS#10 格式的证书申请文件；
c) 证书申请请求响应：CA 给 MSSP 的响应，其中包含用户证书或错误信息；
d) 证书发布请求：MSSP 向 CA 发送，表示用户证书已下载完成，CA 可发布当前用户证书；
e) 证书发布请求响应：CA 给 MSSP 的响应，表示发布成功或失败。

8.3.2 证书更新

在证书更新过程中，MSSP 与 CA 之间可能需要进行多次交互，可包含如下消息：
a) 启动证书更新请求：MSSP 向 CA 发送，请求 CA 启动证书更新流程；
b) 证书更新激活：CA 向 MSSP 发送，表示 CA 要激活某用户关于本 CA 的证书更新流程，MSSP 接到该指令后应向对应的 MSCD 发送证书更新激活指令；
c) 证书更新请求：MSSP 向 CA 发送，表示当前用户要更新证书，其中包含由 MSCD 获得的 PKCS#10 证书请求及认证信息；
d) 证书更新请求响应：CA 给 MSSP 的响应，其中包含用户的新证书或错误信息。

8.3.3 证书撤销

在证书撤销过程中，MSSP 与 CA 间包含如下消息：
a) 证书撤销请求：MSSP 向 CA 发送，表示需撤销某证书，其中包含待撤销证书的序列号；
b) 证书撤销请求响应：CA 向 MSSP 发送，表示撤销成功或失败。

9 安全要求

在移动签名实现过程中应满足如下安全要求：
a) MSSP 与 MSCD 之间：应具备双向认证和完整性保护机制，保证 MSCD 只能接受来自 MSSP 的指令，可选具备机密性保护机制。
b) MSSP 与 APP、CA 之间：应具备双向认证机制和完整性保护机制，可选实现机密性保护机制。
c) APP 与 MSCD 之间：可选实现从 APP 到 MSCD 的端到端机密性保护机制，保证只有签名人才能看到待签数据。
d) MSCD：应实现对签名人的鉴别，即在生成电子签名之前，应对电子签名人的身份进行鉴别，如要求签名人输入口令、生物特征信息等，并在 MSCD 内部进行验证，验证通过后方可生成签名；应实现“所见即所签”。

参考文献

[1] ETSI TR 102 203 v1.1.1 Mobile Commerce (M-COMM); Mobile Signatures; Business and Functional Requirements

[2] ETSI TS 102 204 v1.1.4 Mobile Commerce (M-COMM); Mobile Signature Service ; Web Service Interface

[3] ETSI TR 102 206 v1.1.3 Mobile Commerce (M-COMM); Mobile Signature Service ; Security Framework

[4] ETSI TS 102 207 v1.1.3 Mobile Commerce (M-COMM); Mobile Signature Service ; Specification for Roaming in Mobile Signature Services