(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101938520 B
(45)授权公告日 2015.01.28

(21)申请号 201010276067.X
(22)申请日 2010.09.07
(73)专利权人 中兴通讯股份有限公司
地址 518057 广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦法务部
(72)发明人 张治邦 廉殿斌
(74)专利代理机构 北京安信方达知识产权代理有限公司 11262
代理人 李健 龙洪
(51)Int.Cl.
H04L 29/08(2006.01)
H04L 29/06(2006.01)
H04W 12/06(2009.01)
G06Q 20/00(2012.01)

(56)对比文件
CN 101118630 A,2008.02.06,
WO 0229742 A1,2002.04.11,
CN 101394615 A,2009.03.25,
CN 101436280 A,2009.05.20,

审查员 黄淑美

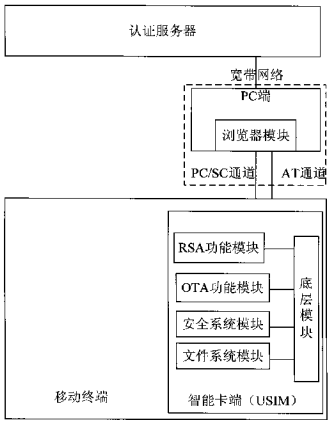
权利要求书3页 说明书6页 附图4页

(54)发明名称

一种基于移动终端签名的远程支付系统及方法

(57)摘要

本发明公开了一种基于移动终端签名的远程支付系统及方法，以及所述系统中的移动终端和移动终端的智能卡。本发明通过对移动终端的智能卡（例如USIM卡）进行改造，并提供与PC侧交互的PC/SC通道。所述智能卡上存储有数字证书，在认证时智能卡导出存储的数字证书后由移动终端发送给认证服务器进行证书注册；认证服务器向移动终端下发签名指令，移动终端向内置的智能卡发送私钥签名指令，所述智能卡送出签名结果并由移动终端上报至认证服务器。所述数字证书可由智能卡与认证服务器在线交互获得。本发明具有更高的安全性和便携性，从而给用户在实行远程支付时带来使用上的方便，有利于保护用户的个人隐私信息，保障远程支付的安全性。



CN 101938520 B

1. 一种基于移动终端签名的远程支付系统，其特征在于，包括：

认证服务器，用于在远程支付时向移动终端索要数字证书以及签名信息进行远程支付认证；

移动终端，包括存储有数字证书的智能卡；所述智能卡用于在收到索要证书请求时导出存储的数字证书后由移动终端发送给认证服务器，用于在收到签名指令时送出签名结果并由移动终端上传签名结果至认证服务器；移动终端与个人计算机端之间设置有个人计算机 / 智能卡 PC/SC 通道，用于在智能卡与个人计算机标准设备之间进行通讯，PC/SC 通道是为智能卡访问 Windows 平台而定义的一种标准结构，用于传递自定义的 APDU 指令；

浏览器模块，用于提供认证服务器与智能卡的交互界面，向移动终端的智能卡下发索要证书请求及签名指令，向认证服务器上传数字证书及签名结果；所述浏览器模块位于与移动终端相连的个人计算机的操作系统中；

所述浏览器模块与所述智能卡采用个人计算机 / 智能卡通道进行交互，并且所述浏览器模块内置有加密服务提供者 CSP 应用插件。

2. 如权利要求 1 所述的远程支付系统，其特征在于，

所述移动终端的智能卡，还用于向认证服务器申请数字证书，在收到公私密钥对生成请求时，生成公私密钥对，并在收到公钥信息请求命令后上传公钥信息至认证服务器，从认证服务器接收并保存认证服务器下发的数字证书；

所述认证服务器，用于根据移动终端的请求下发公私密钥对生成请求，接收公钥信息，并生成数字证书下发给移动终端。

3. 如权利要求 2 所述的远程支付系统，其特征在于，

所述移动终端的智能卡，包括：文件系统模块、安全系统模块、空口 OTA 功能模块和 RSA 功能模块，其中：

RSA 功能模块，用于生成公私密钥对；

所述安全系统模块，用于起加密作用；

所述文件系统模块，用来存储数字证书；

空口 OTA 功能模块，属于空中接口模块，用于连接无线网络。

4. 一种基于移动终端签名的远程支付方法，其特征在于，移动终端与个人计算机端之间设置有个人计算机 / 智能卡 PC/SC 通道，用于在智能卡与个人计算机标准设备之间进行通讯，PC/SC 通道是为智能卡访问 Windows 平台而定义的一种标准结构，用于传递自定义的 APDU 指令；包括：

认证服务器向移动终端索要数字证书，移动终端向内置的智能卡发送读取证书指令，智能卡导出存储的数字证书后由移动终端发送给认证服务器进行证书注册；

认证服务器向移动终端下发签名指令，移动终端向内置的智能卡发送私钥签名指令，所述智能卡送出签名结果并由移动终端上报至认证服务器；

所述移动终端与认证服务器通过浏览器进行交互；

所述浏览器内置有加密服务提供者 CSP 应用插件，并与所述智能卡采用个人计算机 / 智能卡通道进行交互，所述浏览器模块位于与移动终端相连的个人计算机的操作系统中。

5. 如权利要求 4 所述的远程支付方法，其特征在于，所述移动终端的智能卡保存的数字证书是由移动终端向认证服务器在线申请获得，其获取步骤如下：

移动终端向认证服务器申请数字证书，所述认证服务器根据移动终端的请求下发公私密钥对生成请求；

移动终端根据公私密钥对生成请求生成公私密钥对，在收到公钥信息请求命令后上传公钥信息至认证服务器；

认证服务器对公钥信息验签后，生成数字证书并向移动终端下发数字证书；

移动终端接收并保存认证服务器下发的数字证书至智能卡中。

6. 如权利要求 4 所述的远程支付方法，其特征在于，

所述移动终端与认证服务器进行交互的指令包括：安全服务指令和返回数据 / 状态指令；

其中，安全服务指令包括如下指令之一或它们的组合：公私密钥生成指令；签名验签指令；加密解密指令；读取证书指令；读取公钥指令；

其中，返回的数据 / 状态包括如下之一或它们的组合：公钥数据；公钥证书数据；私钥签名的结果值；出错状态信息。

7. 一种采用如权利要求 4 所述基于移动终端签名的远程支付方法的移动终端，其特征在于，所述移动终端包括存储有数字证书的智能卡；

所述智能卡用于在收到索要证书请求时导出存储的数字证书后由移动终端发送给认证服务器，用于在收到签名指令时送出签名结果并由移动终端上传签名结果至认证服务器。

8. 如权利要求 7 所述的移动终端，其特征在于，

所述智能卡，还用于向认证服务器申请数字证书，在收到公私密钥对生成请求时，生成公私密钥对，并在收到公钥信息请求命令后上传公钥信息至认证服务器，从认证服务器接收并保存认证服务器下发的数字证书。

9. 如权利要求 7 或 8 所述的移动终端，其特征在于，

所述智能卡包括：文件系统模块、安全系统模块、空口 OTA 功能模块和 RSA 功能模块，其中：

RSA 功能模块，用于生成公私密钥对；

所述安全系统模块，用于起加密作用；

所述文件系统模块，用来存储数字证书；

空口 OTA 功能模块，属于空中接口模块，用于连接无线网络。

10. 一种采用如权利要求 4 所述基于移动终端签名的远程支付方法的智能卡，其特征在于，所述智能卡内置于移动终端中，通过个人计算机 / 智能卡通道与个人计算机端进行交互；

所述智能卡包括：文件系统模块、安全系统模块、空口 OTA 功能模块和 RSA 功能模块，其中：

RSA 功能模块，用于生成公私密钥对；

所述安全系统模块，用于起加密作用；

所述文件系统模块，用来存储数字证书；

空口 OTA 功能模块，属于空中接口模块，用于连接无线网络。

11. 如权利要求 10 所述的智能卡，其特征在于，

所述文件系统模块存储的数字证书，用于在收到索要证书请求时由移动终端发送给认证服务器；

所述安全系统模块，用于在收到签名指令时对签名进行加密，将加密的签名结果上传至认证服务器；

RSA 功能模块，用于在移动终端向认证服务器申请数字证书过程中收到公私密钥对生成请求时，生成公私密钥对。

一种基于移动终端签名的远程支付系统及方法

技术领域

[0001] 本发明涉及移动通信技术领域，尤其涉及一种基于移动终端签名的远程支付系统及方法，以及所述系统中的移动终端和移动终端的智能卡。

背景技术

[0002] 随着网络购物在日常生活中的逐渐普及，远程支付功能越来越被更多的人接受，目前网络支付手段一般是通过银行卡来实现，且对网络的安全性要求很高，一般都需要使用数字证书。随着手机支付概念的推广应用，手机支付因手机普及度高支付方便等特点而受到人们的青睐。

[0003] 目前主流的手机支付技术主要有如下三种：

[0004] 第一种是来自欧洲的NFC(Near Field Communication，即近距离通信)技术，是时间最长，影响力最广泛的方案。这种方案将非接触式智能卡技术与手机结合，将射频芯片集成到手机主板上，实现手机与POS机或读卡器之间的通讯，从而实现手机支付。这种方式的最大缺陷在于用户若要使用手机支付，必须更换为带有NFC功能的手机。

[0005] 第二种是目前比较常用的基于13.56MHZ的SIM PASS标准。SIMpass技术融合了DI卡技术和SIM(用户识别卡，Subscriber Identity Module)卡技术，或者称为双界面SIM卡，也即具有接触和非接触两个工作接口，接触界面用于实现SIM功能，非接触界面用于实现支付功能，兼容多个智能卡应用规范。

[0006] 第三种是基于2.4GHz的RFID_SIM，其实现机制与上面的SIMpass类似。

[0007] 从上面对主流手机支付技术的介绍可以看出，目前的手机支付技术还基本局限于近距离支付技术。

[0008] 远程支付功能受到网络安全性和当前技术的限制，没有得到广泛应用。目前的技术手段主要是通过对手机用户的ID信息，登陆密码和手机密码等信息进行验证，即进行远程支付。但手机用户的这些个人信息在通过短信或WAP传输时，很容易被一些不法分子截获，从而造成巨大损失，可以预见，手机支付的安全性能将是限制其能否广泛应用的关键因素。

[0009] 因而，如何实现安全简便的移动终端的远程支付，就成为需要解决的技术问题。

发明内容

[0010] 本发明所要解决的技术问题在于，提供一种基于移动终端签名的远程支付系统及方法，以及所述系统中的移动终端和移动终端的智能卡，用于实现移动终端签名的远程支付。

[0011] 为了解决上述问题，本发明提出了一种基于移动终端签名的远程支付系统，包括：

[0012] 认证服务器，用于在远程支付时向移动终端索要数字证书以及签名信息进行远程支付认证；

[0013] 移动终端，包括存储有数字证书的智能卡；所述智能卡用于在收到索要证书请求时生成数字证书发送给认证服务器，用于在收到签名指令时送出签名结果并上传签名结果至认证服务器。

[0014] 所述远程支付系统进一步包括：浏览器模块，用于提供认证服务器与智能卡的交互界面，向移动终端的智能卡下发索要证书请求及签名指令，向认证服务器上传数字证书及签名结果；所述浏览器模块与所述智能卡采用个人计算机 / 智能卡通道进行交互，并且所述浏览器模块内置有加密服务提供者 (CSP) 应用插件。

[0015] 所述浏览器模块位于移动终端的计算机操作系统中，或者是与移动终端相连的个人计算机的操作系统中。

[0016] 所述移动终端的智能卡，还用于向认证服务器申请数字证书，在收到公私密钥对生成请求时，生成公私密钥对，并在收到公钥信息请求命令后上传公钥信息至认证服务器，从认证服务器接收并保存认证服务器下发的数字证书；所述认证服务器，用于根据移动终端的请求下发公私密钥对生成请求，接收公钥信息，并生成数字证书下发给移动终端。

[0017] 所述移动终端的智能卡，包括：文件系统模块，安全系统模块，空口 (OTA) 功能模块，RSA 功能模块，其中：

[0018] RSA 功能模块，用于生成公私密钥对；

[0019] 所述安全系统模块，用于起加密作用；

[0020] 所述文件系统模块，用来存储数字证书；

[0021] 空口 (OTA) 功能模块，属于空中接口模块，用于连接无线网络。

[0022] 一种基于移动终端签名的远程支付方法，包括：

[0023] 认证服务器向移动终端索要数字证书，移动终端向内置的智能卡发送读取证书指令，智能卡导出存储的数字证书后由移动终端发送给认证服务器进行证书注册；

[0024] 认证服务器向移动终端下发签名指令，移动终端向内置的智能卡发送私钥签名指令，所述智能卡送出签名结果并由移动终端上报至认证服务器。

[0025] 所述移动终端的智能卡保存的数字证书是由移动终端向认证服务器在线申请获得，其获取步骤如下：

[0026] 移动终端向认证服务器申请数字证书，所述认证服务器根据移动终端的请求下发公私密钥对生成请求；

[0027] 移动终端根据公私密钥对生成请求生成公私密钥对，在收到公钥信息请求命令后上传公钥信息至认证服务器；

[0028] 认证服务器对公钥信息验签后，生成数字证书并向移动终端下发数字证书；

[0029] 移动终端接收并保存认证服务器下发的数字证书至智能卡中。

[0030] 所述移动终端与认证服务器通过浏览器进行交互；所述浏览器内置有加密服务提供者 (CSP) 应用插件，并与所述智能卡采用个人计算机 / 智能卡通道进行交互。

[0031] 所述移动终端与认证服务器进行交互的指令包括：安全服务指令和返回数据 / 状态指令；

[0032] 其中，安全服务指令包括如下指令之一或它们的组合：公私密钥生成指令；签名验签指令；加密解密指令；读取证书指令；读取公钥指令；

[0033] 其中，返回的数据 / 状态包括如下之一或它们的组合：公钥数据；公钥证书数据；

私钥签名的结果值；出错状态信息。

[0034] 一种移动终端，所述移动终端包括存储有数字证书的智能卡；所述智能卡用于在收到索要证书请求时生成数字证书发送给认证服务器，用于在收到签名指令时送出签名结果并上传签名结果至认证服务器。

[0035] 所述智能卡，还用于向认证服务器申请数字证书，在收到公私密钥对生成请求时，生成公私密钥对，并在收到公钥信息请求命令后上传公钥信息至认证服务器，从认证服务器接收并保存认证服务器下发的数字证书。

[0036] 所述智能卡包括：文件系统模块，安全系统模块，空口 (OTA) 功能模块，RSA 功能模块，其中：RSA 功能模块，用于生成公私密钥对；所述安全系统模块，用于起加密作用；所述文件系统模块，用来存储数字证书；空口 (OTA) 功能模块，属于空中接口模块，用于连接无线网络。

[0037] 一种智能卡，所述智能卡内置于移动终端中，通过个人计算机 / 智能卡通道与个人计算机系统端进行交互；所述智能卡包括：文件系统模块，安全系统模块，空口 (OTA) 功能模块，RSA 功能模块，其中：

[0038] RSA 功能模块，用于生成公私密钥对；

[0039] 所述安全系统模块，用于起加密作用；

[0040] 所述文件系统模块，用来存储数字证书；

[0041] 空口 (OTA) 功能模块，属于空中接口模块，用于连接无线网络。

[0042] 所述文件系统模块存储的数字证书，用于在收到索要证书请求时由移动终端发送给认证服务器；所述安全系统模块，用于在收到签名指令时对签名进行加密，将加密的签名结果上传至认证服务器；RSA 功能模块，用于在移动终端向认证服务器申请数字证书过程中收到公私密钥对生成请求时，生成公私密钥对。

[0043] 和现行技术相比，本发明中公私密钥对的生成和证书的存放都是在移动终端本地，具有更高的安全性和便携性。在远程支付过程中，需要使用用户的数字证书和签名（即密码），同样是移动终端通过数据接口和 PC 端相连，PC 端的服务器网站下发证书请求，移动终端获取请求，上传数字证书。PC 端将证书注册到浏览器后发送给服务器，以备验证签名。服务器端收到证书后发起公私密钥对请求，移动终端成功上传公私密钥后，验证签名结束。

[0044] 本发明不但突破了手机支付近距离的限制，同时相比使用短信和 WAP 方式传递个人 ID 和密码的方式，更具安全性和保密性。同时，如果利用移动终端自身的浏览器，可以不依赖于外部电脑，而由移动终端直接与认证服务器进行交互，实现自助证书申请及签名验签等操作。本发明具有更高的安全性和便携性，从而给用户在实行远程支付时带来使用上的方便，有利于保护用户的个人隐私信息，保障远程支付的安全性。

附图说明

[0045] 图 1 是移动终端与外部 PC 机相连实现远程支付系统的示意图；

[0046] 图 2 是移动终端利用内部 PC 操作系统实现远程支付系统的示意图；

[0047] 图 3 是移动终端的智能卡与 PC 侧之间的 PC/SC 通道的连接示意图；

[0048] 图 4 是智能卡侧与 PC 侧的功能模块示意图；

[0049] 图 5 是移动终端执行证书申请的流程图；

[0050] 图 6 是移动终端执行远程支付签名验签的流程图。

具体实施方式

[0051] 为使本发明的目的、技术方案和优点更加清楚，以下结合附图对本发明作进一步地详细说明。

[0052] 本发明的基于移动终端签名的远程支付系统，通过对移动终端、浏览器模块，以及移动终端的智能卡与浏览器之间的数据通道进行改造，实现对远程支付功能的支持。

[0053] 如图 1 所示，显示了一种典型的基于移动终端签名的远程支付系统的示意图。所述基于移动终端签名的远程支付系统包括 :移动终端，PC 端，认证服务器。

[0054] 所述移动终端包括智能卡 (SC，Smart Card)，移动终端与 PC 端之间现已有 AT 通道，还需增加个人计算机 / 智能卡 PC/SC 通道，用于在智能卡与 PC 标准的设备之间可以进行通讯。PC/SC 通道，是为智能卡访问 Windows 平台而定义的一种标准结构，用于传递自定义的 APDU(APL 协议数据单元，APLProtocol Data Unit) 指令。相应的，移动终端的驱动程序中需要增加 PC/SC 驱动。

[0055] 所述 PC 端，具有浏览器模块，需要对浏览器进行改进，以便支持 CSPAPI。加密服务提供者 C SP(Cryptographic Service Provider)，用于密钥生成 / 交换、加解密等服务。

[0056] 认证服务器，用于数字证书的生成，下发及验证数字证书。

[0057] 由于移动终端的证书申请与签名验签都主要发生在认证服务器与智能卡之间，中间需要浏览器与移动终端的转发，相互的数据交互通过 PC/SC 通道进行。

[0058] 所述 PC 端，可以是普通的个人计算机或笔记本电脑或者是具有个人计算机系统的移动设备，其与认证服务器可以通过有线宽带网络或者无线宽带网络进行网络连接。

[0059] 在图 1 所示的系统中，移动终端连同其内置的智能卡，相当于直接连接与计算机系统上的卡盾设备，例如银行的 USBKEY。该智能卡可以同时具备通信功能和卡盾功能。所述智能卡可以是 USIM 卡。

[0060] 如图 2 所示，显示了另一种典型的基于移动终端签名的远程支付系统的示意图。随着智能手机等智能移动终端的普及，移动终端的功能越来越强大，很多移动终端具有个人操作系统，可以实现普通 PC 机所能实现的功能，例如移动终端可以通过浏览器实现互联网业务，也就是说相当于可以将 PC 端也内置在移动终端内部，智能卡与浏览器模块交互，移动终端通过无线网络与认证服务器连接。

[0061] 在图 2 中，同样需要对移动终端进行改造，即增加内置智能卡与浏览器模块之间的个人计算机 / 智能卡 PC/SC 通道以及相应的驱动程序，在浏览器模块增加加密服务提供者 CSP(Cryptographic Service Provider) 应用插件。

[0062] 在图 1 和图 2 所示的系统中，经过改进之后，具有智能卡的移动终端，就能够保证对安全服务指令和返回的数据流的通道支持，相关的 APDU 指令通过这个 PC/SC 通道传递到智能卡端 (例如 USIM 卡 (Universal SubscriberIdentity Module，全球用户识别卡))，使用户在远程支付过程中，通过对浏览器的操作，实现电子签名，身份认证的功能。认证服务器的数字证书的下发，移动终端生成的公私密钥对及数字证书的下载、上传都是通过 PC/SC 通道进行。

[0063] 在图 1 和图 2 所示的系统中，所述智能卡，包括 :文件系统模块，安全系统模块，

OTA(over the air,空口）功能模块，RSA 协处理器等。其中：文件系统模块用来存储数字证书，RSA 协处理器用来生成公私密钥对，安全系统模块主要是起加密作用，OTA 功能模块属于空中接口模块，用户可以用来连接网络。

[0064] 如图 3 所示，显示了基于 PC/SC 通道传递认证服务器下发的安全服务指令以及移动终端返回的数据状态信息的示意图。用于远程支付的安全服务指令及数据都通过 PC/SC 通道传递，而普通指令及数据可以通过现有的 AT 通道传递。

[0065] 如图 4 所示，显示了基于 PC/SC 通道划分的 PC 侧与智能卡侧（USIM 卡侧）的详细示意图。

[0066] 其中，在 PC 侧，密钥容器（Key Container）是密钥数据库的一部分，其包含了属于一个特定用户的所有的密钥对。加密库，包括硬件加密库和软件加密库，其可以是密钥数据库，用于存放多个用户的密钥容器。CSP API 插件可以嵌入结合在浏览器中，与认证服务器间通过 SSL 进行通讯。

[0067] 其中，在智能卡（USIM 卡）侧，包括：文件系统模块，安全系统模块，OTA 功能模块，RSA 功能模块。所述 RSA 功能模块是 RSA 协处理器，用于生成公私密钥对。文件系统模块用于存储数字证书。

[0068] 在 PC 侧与智能卡侧之间，增加了个人计算机（Personal computer）/ 智能卡（Smart Card）通道，PC/SC 通道是为智能卡访问 Windows 平台而定义的一种标准结构，用于传递自定义的 APDU(APL 协议数据单元，APL Protocol DataUnit）指令。所述指令包括安全服务指令和状态信息指令。PC/SC 通道还用于传递数据证书的下发和下载等。CSP 属于 WINDOWS 开发内容，在开发完毕后作为一个组件集成到浏览器中，以实现浏览器对公私密钥的支持。

[0069] 图 1 中移动终端与 PC 端连接时，可以通过物理性的 USB 接口和 PC 端相连，而移动终端和 PC 端之间的数据传递通过标准的 PC/SC 通道进行，保证数据的保密性。

[0070] 为实现本发明的移动终端的远程支付，新增 APDU 指令主要分为：安全服务指令和返回数据 / 状态指令。

[0071] 其中，安全服务指令主要包括：公私密钥生成指令；签名验签指令；加密解密指令；读取证书指令；读取公钥指令。

[0072] 其中，返回的数据 / 状态主要包括：公钥数据；公钥证书数据；私钥签名的结果值；出错状态信息。

[0073] 为实现移动终端的远程支付，需要先向认证服务器请求数字证书，在移动终端保存了数字证书之后，才可实现在线支付。如图 5 所示，给出了移动终端向认证服务器申请证书的证书申请阶段流程图。由于移动终端中采用的是智能卡，因而，其向认证服务器申请的客户证书的类型为：智能卡用户类型。

[0074] 移动终端可以利用自身操作系统中的浏览器或通过相连接的 PC 机上的操作系统中的浏览器，在证书申请网站（CA 或 CA 代理）申请客户证书，向认证服务器发送申请请求。具体申请过程如下：

[0075] 501：移动终端通过浏览器向认证服务器申请证书；

[0076] 502：认证服务器向移动终端下发公私密钥对生成请求；

[0077] 503：移动终端将公私密钥对生成指令透传给智能卡（USIM 卡）；

[0078] 504：智能卡利用内部的RSA协处理器，生成公私密钥对，并保存在安全存储区（即文件系统模块）；

[0079] 505：智能卡向移动终端返回状态信息；

[0080] 506：移动终端向认证服务器上传状态信息；

[0081] 507：认证服务器向移动终端下发公钥信息请求命令；

[0082] 508：移动终端透传公钥信息请求命令给智能卡，智能卡读取公钥信息；

[0083] 509：智能卡送出公钥数据给移动终端

[0084] 510：移动终端上传公钥数据至认证服务器；

[0085] 511：认证服务器下发客户证书给移动终端；

[0086] 512：移动终端下载证书，将客户证书保存到智能卡中。

[0087] 在移动终端保存有数字证书时，就可以与认证服务器进行交互实现远程支付，当然，移动终端获取数字证书的方式并不限于图5所示的在线获取方式，也可以预置或者采用其它方式获得。

[0088] 如图6所示，给出了移动终端远程支付时进行签名验签阶段的流程图。

[0089] 601：认证服务器向移动终端索要客户的数字证书；

[0090] 602：移动终端透传读取证书指令给智能卡；

[0091] 603：智能卡送出客户的公钥证书信息给移动终端；

[0092] 604：移动终端将公钥证书信息注册到PC端的IE浏览器，并发送给认证服务器用于验证公钥证书信息；

[0093] 605：认证服务器向移动终端下发签名指令，并将HASH过的数据下发移动终端；

[0094] 606：移动终端透传私钥签名指令到智能卡；

[0095] 607：智能卡送出签名结果给移动终端；

[0096] 608：移动终端将签名结果上传给认证中心，完成远程支付的签名验签。

[0097] 本发明在移动终端内置支持基本安全指令的智能卡，例如USIM卡，可称之为“卡盾”，改进后的智能卡除具有通信功能之外，还具有远程支付及安全功能。为了实现智能卡与外部浏览器之间的交互，在移动终端通过增加PC/SC通道和对PC/SC驱动的支持，以及对PC端的浏览器、应用程序插件CSPAPI等改造，开发一系列APDU指令，实现了移动证书的申请，存储及签名的验签。

[0098] 和传统的手机支付相比，本发明不但突破了手机支付近距离的限制，同时相比使用短信和WAP方式传递个人ID和密码的方式，更具安全性和保密性。同时，如果利用移动终端自身的浏览器，可以不依赖于外部电脑，而由移动终端直接与认证服务器进行交互，实现自助证书申请及签名验签等操作。本发明具有更高的安全性和便携性，从而给用户在实行远程支付时带来使用上的方便，有利于保护用户的个人隐私信息，保障远程支付的安全性。

[0099] 以上所述仅为本发明的实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的权利要求范围之内。

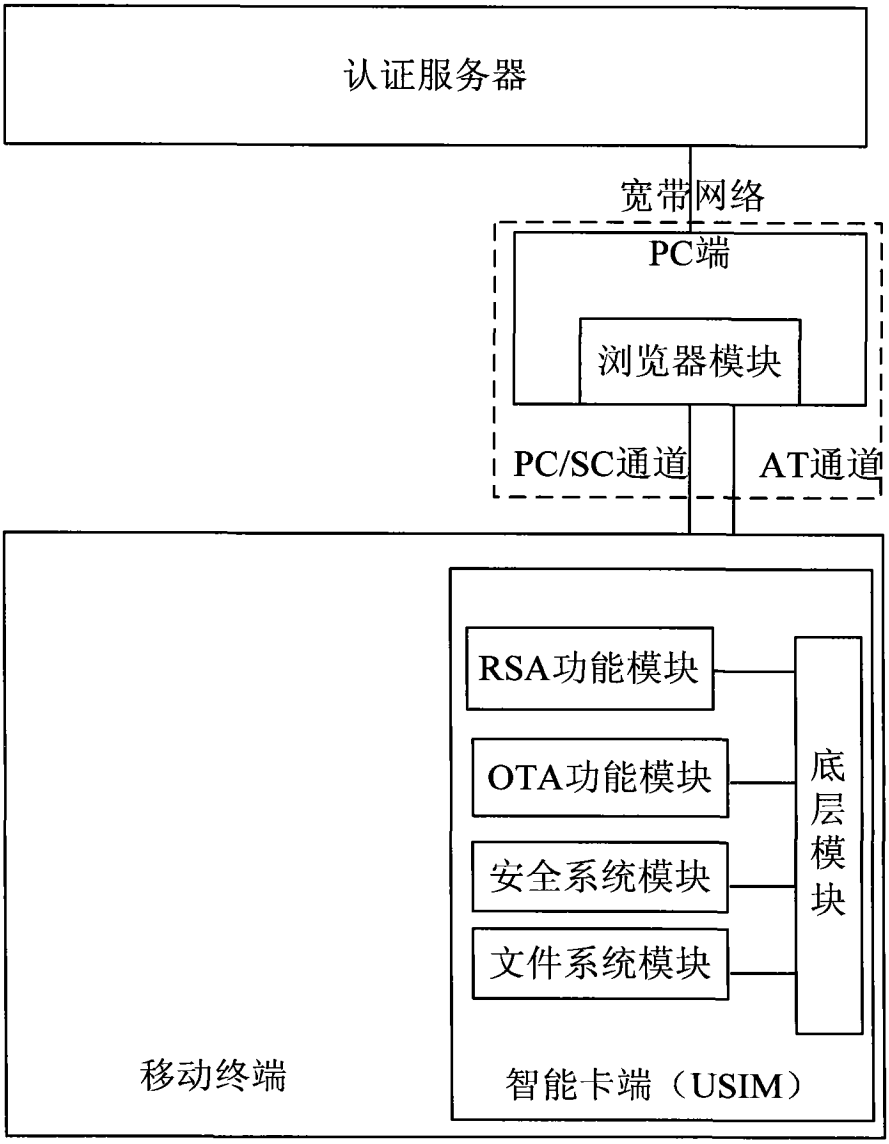

认证服务器
宽带网络
PC端
浏览器模块
PC/SC通道
AT通道
RSA功能模块
OTA功能模块
安全系统模块
文件系统模块
底层模块
移动终端
智能卡端（USIM）

图 1

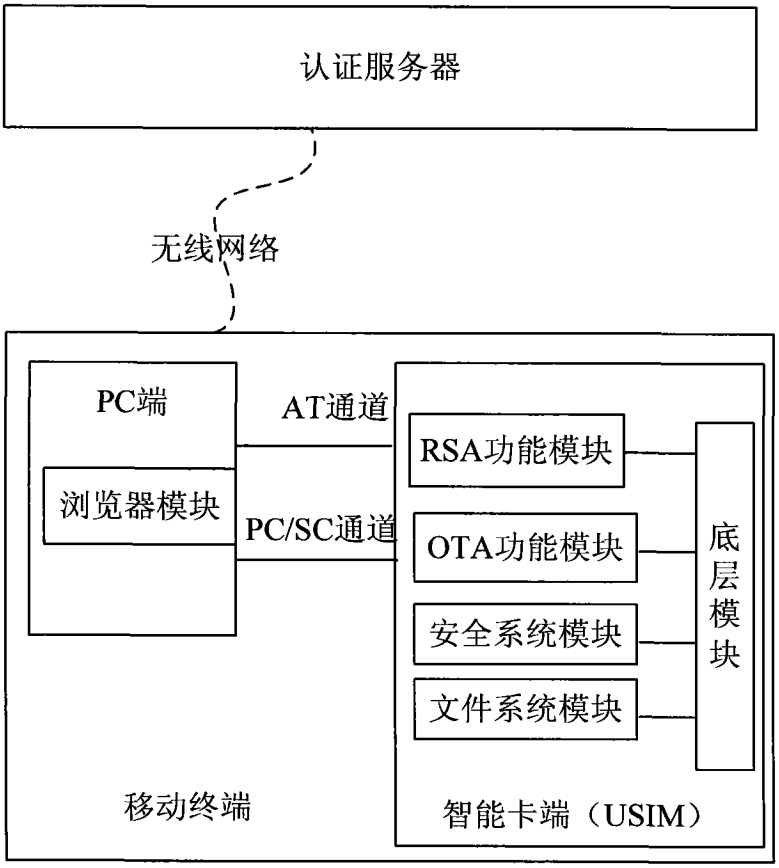

认证服务器
无线网络
PC端
浏览器模块
AT通道
PC/SC通道
RSA功能模块
OTA功能模块
安全系统模块
文件系统模块
底层模块
移动终端
智能卡端（USIM）

图 2

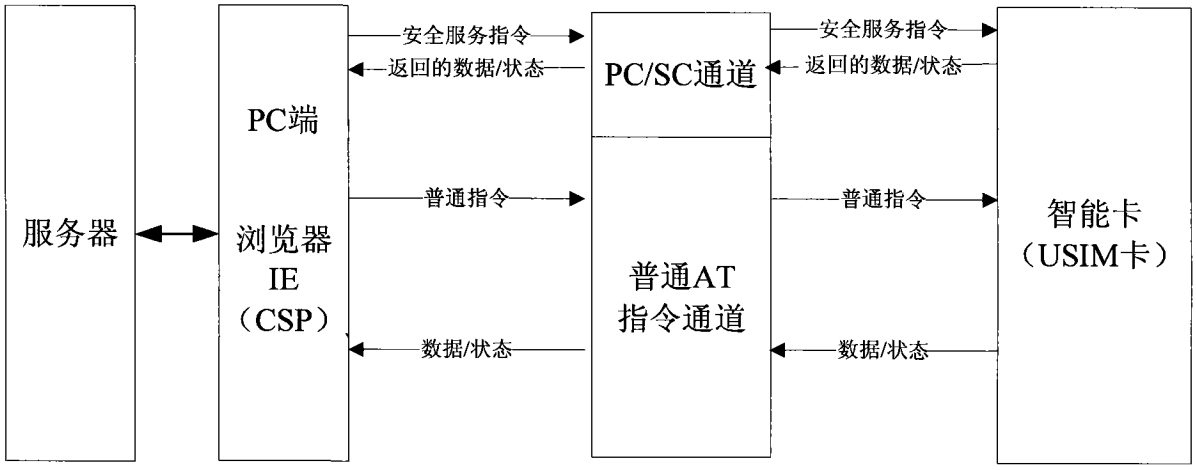

服务器
PC端
浏览器
IE
（CSP）
安全服务指令
返回的数据/状态
普通指令
数据/状态
PC/SC通道
普通AT
指令通道
安全服务指令
返回的数据/状态
普通指令
数据/状态
智能卡
（USIM卡）

图 3

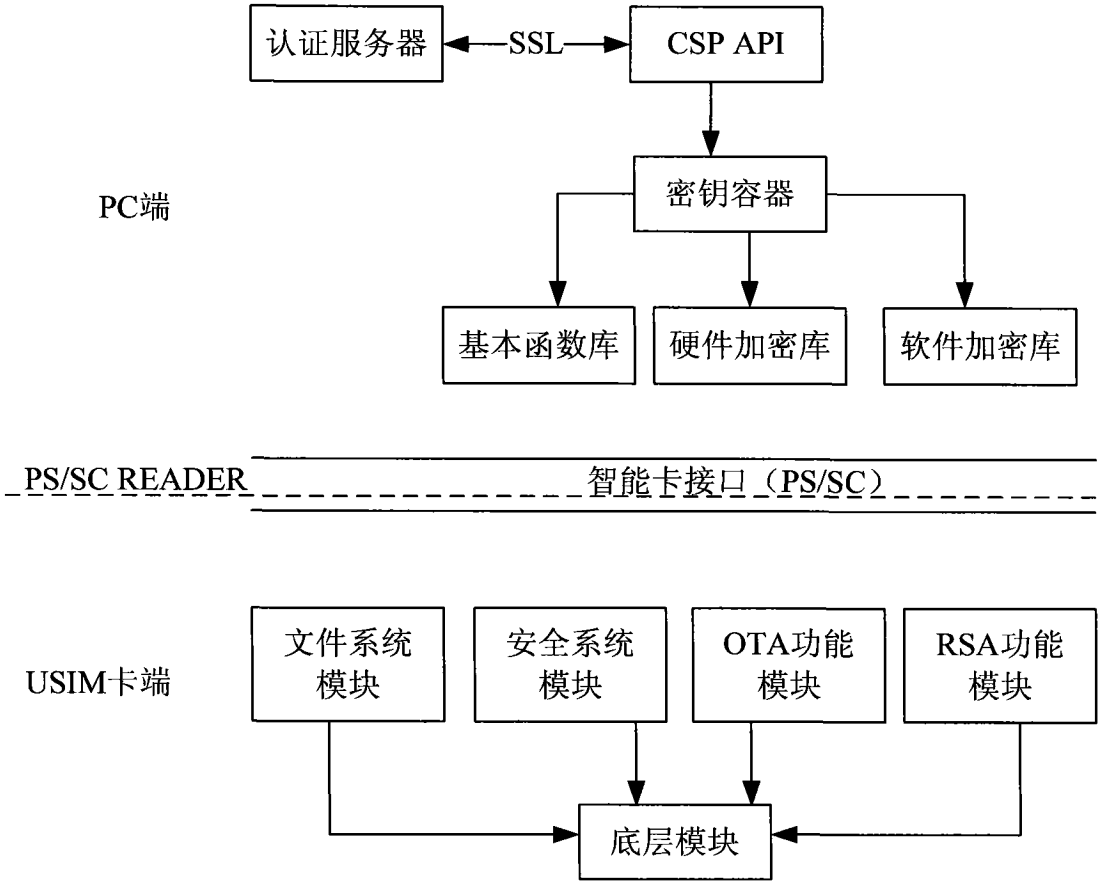

认证服务器
SSL
CSP API
PC端
密钥容器
基本函数库
硬件加密库
软件加密库
PS/SC READER
智能卡接口（PS/SC）
USIM卡端
文件系统模块
安全系统模块
OTA功能模块
RSA功能模块
底层模块

图 4

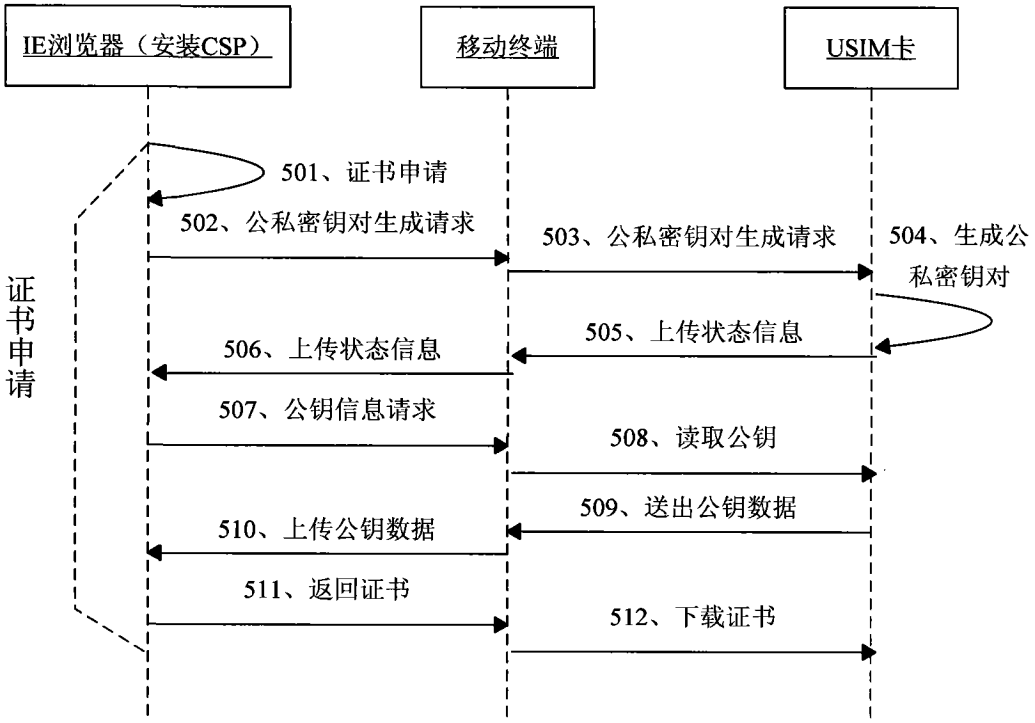

IE浏览器（安装CSP）
移动终端
USIM卡
证书申请
501、证书申请
502、公私密钥对生成请求
503、公私密钥对生成请求
504、生成公私密钥对
505、上传状态信息
506、上传状态信息
507、公钥信息请求
508、读取公钥
509、送出公钥数据
510、上传公钥数据
511、返回证书
512、下载证书

图 5

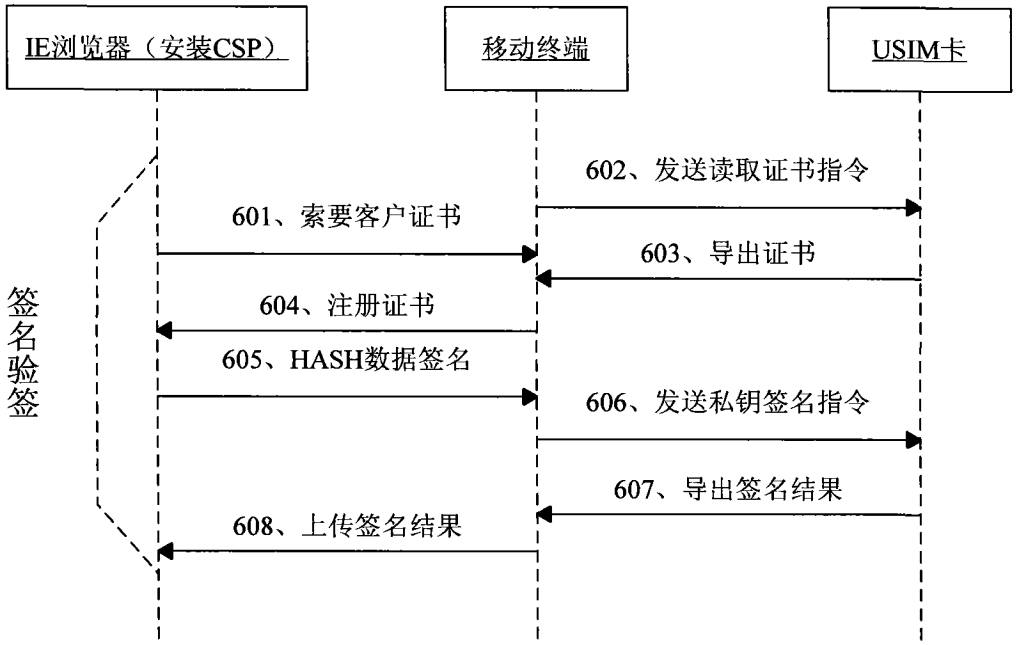

IE浏览器（安装CSP）
移动终端
USIM卡
签名验签
602、发送读取证书指令
601、索要客户证书
603、导出证书
604、注册证书
605、HASH数据签名
606、发送私钥签名指令
607、导出签名结果
608、上传签名结果

图 6