(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 101916388 B

(45)授权公告日 2013.06.05

(21)申请号 201010240334.8

(22)申请日 2010.07.27

(73)专利权人 武汉天喻信息产业股份有限公司

地址 430012 湖北省武汉市东湖新技术开发区华工大学科技园

(72)发明人 余斌 周军龙

(51)Int.Cl.

G06K 19/07(2006.01)

H04L 29/06(2006.01)

H04W 12/06(2009.01)

G07G 1/12(2006.01)

(56)对比文件

CN 101470873 A,2009.07.01, 说明书第2页第1段.

CN 101098371 A,2008.01.02, 全文.

CN 101742481 A,2010.06.16, 说明书[0014]－[0015],[0032]段.

审查员 谢佳

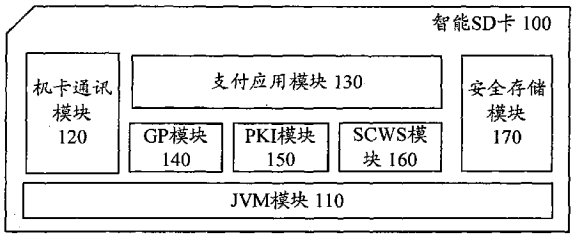
权利要求书1页 说明书5页 附图3页

(54)发明名称

智能SD卡及利用该智能SD进行移动支付的方法

(57)摘要

本发明提供一种智能SD卡和利用智能SD卡进行移动支付的方法，机卡通讯模块可与移动终端进行数据交互，支付应用模块用于处理从机卡通讯模块传送过来的支付指令，智能卡网络服务器模块用于提供解析HTTP/HTTPS协议的能力，公钥基础设施模块用于管理和验证证书、对数据进行加解密以及对数据签名并验证签名，安全存储模块用于存储与移动终端建立安全通道的密钥及数据，网络服务器通过智能卡网络服务器模块可与移动终端建立SSL安全通道并使用安全存储模块中所存储的表示智能SD卡合法身份的证书作为关键数据传输的加密密钥，智能卡网络服务器模块采用SSL安全通道的会话密码对请求支付应用模块对移动支付请求所产生的移动支付响应数据进行加密。本发明所提供的智能SD卡及移动支付方法可支持SCWS、PKI及JavaApplet等应用，为移动支付提供安全的应用环境。



CN 101916388 B

1. 一种用于移动支付的智能 SD 卡，其特征在于：所述智能 SD 卡包括机卡通讯模块、支付应用模块、智能卡网络服务器模块、公钥基础设施模块及安全存储模块，所述机卡通讯模块可与移动终端进行数据交互，所述支付应用模块用于处理从所述机卡通讯模块传送过来的支付指令，所述智能卡网络服务器模块用于提供解析 HTTP/HTTPS 协议的能力，所述公钥基础设施模块用于管理和验证证书、对数据进行加解密以及对数据签名并验证签名，所述安全存储模块用于存储与移动终端建立安全通道的密钥及数据，网络服务器通过所述智能卡网络服务器模块可与移动终端建立 SSL 安全通道并使用所述安全存储模块中所存储的表示所述智能 SD 卡合法身份的证书作为关键数据传输的加密密钥，所述智能卡网络服务器模块采用 SSL 安全通道的会话密码对请求所述支付应用模块对移动支付请求所产生的移动支付响应数据进行加密。

2. 一种利用如权利要求 1 所述的智能 SD 卡进行移动支付的方法，包括以下步骤：

移动终端提交支付请求给智能 SD 卡；

移动终端与智能卡网络服务器模块建立 SSL 安全通道；

支付应用模块从智能卡网络服务器模块获取支付请求数据并解析；以及

支付应用模块产生响应数据并通过智能卡网络服务器模块返回给移动终端。

3. 根据权利要求 2 所述的利用智能 SD 卡进行移动支付的方法，其特征在于：在所述支付应用模块产生响应数据并通过智能卡网络服务器模块返回给移动终端的步骤中：所述智能卡网络服务器模块采用移动终端的会话密钥对响应数据进行加密。

4. 根据权利要求 3 所述的利用智能 SD 卡进行移动支付的方法，其特征在于在所述支付应用模块从智能卡网络服务器模块获取支付请求数据并解析步骤之后，还包括以下步骤：

智能卡网络服务器模块检测是否需要链接移动支付服务器。

5. 根据权利要求 4 所述的利用智能 SD 卡进行移动支付的方法，其特征在于：如果不需要链接支付应用服务器，则进入所述支付应用模块产生响应数据并通过智能卡网络服务器模块返回给移动终端的步骤。

6. 根据权利要求 4 所述的利用智能 SD 卡进行移动支付的方法，其特征在于如果需要链接支付应用服务器，则进入如下步骤：

智能卡网络服务器模块通过移动终端与移动支付服务器建立 SSL 安全通道；

移动支付服务器处理支付请求数据并生成响应数据；以及

响应数据通过移动终端转发给支付应用模块。

7. 根据权利要求 6 所述的利用智能 SD 卡进行移动支付的方法，其特征在于：在所述智能卡网络服务器模块通过移动终端与移动支付服务器建立 SSL 安全通道步骤中，移动支付服务器与智能 SD 卡各自交互表示合法身份的证书信息，并进行对证书进行合法性校验，身份认证通过以后，进行会话密钥的协商，共同生成用于加密数据的会话密钥。

8. 根据权利要求 7 所述的利用智能 SD 卡进行移动支付的方法，其特征在于：所述移动支付服务器产生的响应数据采用所述会话密钥进行加密后反馈给智能 SD 卡。

智能 SD 卡及利用该智能 SD 进行移动支付的方法

【技术领域】

[0001] 本发明涉及 SD 卡，尤其涉及一种智能 SD 卡以及一种利用该智能 SD 卡进行移动支付的方法。

【背景技术】

[0002] 中国移动支付市场拥有超过一亿的远程支付用户，但目前仍是一个新兴市场，正处于多个公司之间以及多种技术之间的竞争阶段。

[0003] 现在移动支付服务在中国主要有两种方式：现场支付和远程支付。

[0004] 现场移动支付和银行账户绑定的远程支付目前处于初期阶段，非银行账户的远程支付目前是中国移动支付市场的主流。在现场支付领域，中国目前没有占绝对优势的移动支付解决方案，SIM 卡支付方案和 NFC 支付方案都处于尝试阶段。

[0005] 手机移动支付是允许移动用户使用其移动终端（通常是手机）对所消费的商品或服务进行账务支付的一种服务方式。手机支付的终端主体，就是消费者基于人手一台的手机。其拥有如下主要特点：

[0006] 1. 手机信号收到处，即可实现手机支付，方便快捷；

[0007] 2. 采用金融级别的安全机制，并增加手机实时验证，保证资料不被破解和修改；

[0008] 3. 手机支付支持现金充值、网银充值、移动话费充值卡充值等多种方式；

[0009] 4. 建立在 3G、GPRS 和 EDGE 网络基础上的手机支付，交易速度大大提高。

[0010] 最先在国内推行的远程支付应用就是采用银行卡与手机进行绑定，用户可以用手机进行水费、天然气费用等费用的定向支付功能。但是这种支付方式使用短信发送信息，容易出现延迟和丢失的问题，数据交换过程中会出现敏感信息泄露的问题，故只是适合定向方式。

[0011] 随着手机软硬件的发展，出现新的手机支付方式，用户从银行申请获取集成 PKI(Public Key Infrastructure，即公钥基础设施）应用的安全智能 SD 卡 (Secure Digital Card)，该 SD 卡提供身份认证、数字签名的功能，确保手机移动支付交易过程中的数据安全。

[0012] 在这个方案中，每次在提交银行业务服务器交易数据时候，终端应用都将数据传输给 SD 卡进行数据加密和签名，然后再将加密的数据发生给远程银行业务服务器。服务器进行数据解密和验签后，进行数据处理。在这个流程中，终端应用把数据传输给 SD 卡过程中，数据传输存在被截获、篡改的风险。同时，由于 SD 卡的数据加密、签名接口公开，存在被暴力破解的可能性。此外，不同银行的 SD 卡的终端接口不一样，这样如果用户有多个银行的卡，就需要安装多个银行支付应用和购买多个银行的 SD 卡。

[0013] 在上述两种远程支付的方案中，都存在数据被截取、篡改、被破解的风险，从而导致业内对手机支付安全性存在一定的担忧，目前业内也在寻找安全性更高相应的替代方案，应用在手机支付中。

[0014] 【发明内容】

[0015] 有鉴于此，本发明提供一种安全的智能 SD 卡。

[0016] 一种用于移动支付的智能 SD 卡，所述智能 SD 卡包括机卡通讯模块、支付应用模块、智能卡网络服务器模块、公钥基础设施模块及安全存储模块，所述机卡通讯模块可与移动终端进行数据交互，所述支付应用模块用于处理从所述机卡通讯模块传送过来的支付指令，所述智能卡网络服务器模块用于提供解析 HTTP/HTTPS 协议的能力，所述公钥基础设施模块用于管理和验证证书、对数据进行加解密以及对数据签名并验证签名，所述安全存储模块用于存储与移动终端建立安全通道的密钥及数据，网络服务器通过所述智能卡网络服务器模块可与移动终端建立 SSL 安全通道并使用所述安全存储模块中所存储的表示所述智能 SD 卡合法身份的证书作为关键数据传输的加密密钥，所述智能卡网络服务器模块采用 SSL 安全通道的会话密码对请求所述支付应用模块对移动支付请求所产生的移动支付响应数据进行加密。

[0017] 有鉴于此，本发明还提供一种利用智能 SD 卡进行安全的移动支付的方法。

[0018] 一种利用上述智能 SD 卡进行移动支付的方法，包括以下步骤：移动终端提交支付请求给智能 SD 卡；移动终端与智能卡网络服务器模块建立 SSL 安全通道；支付应用模块从智能卡网络服务器模块获取支付请求数据并解析；以及支付应用模块产生响应数据并通过智能卡网络服务器模块返回给移动终端。

[0019] 优选地，在所述支付应用模块产生响应数据并通过智能卡网络服务器模块返回给移动终端的步骤中：所述智能卡网络服务器模块采用移动终端的会话密钥对响应数据进行加密。

[0020] 优选地，在所述支付应用模块从智能卡网络服务器模块获取支付请求数据并解析步骤之后，还包括以下步骤：智能卡网络服务器模块检测是否需要链接移动支付服务器。

[0021] 优选地，如果不需要链接支付应用服务器，则进入所述支付应用模块产生响应数据并通过智能卡网络服务器模块返回给移动终端的步骤。

[0022] 优选地，如果需要链接支付应用服务器，则进入如下步骤：智能卡网络服务器模块通过移动终端与移动支付服务器建立 SSL 安全通道；移动支付服务器处理支付请求数据并生成响应数据；以及响应数据通过移动终端转发给支付应用模块。

[0023] 优选地，在所述智能卡网络服务器模块通过移动终端与移动支付服务器建立 SSL 安全通道步骤中，移动支付服务器与智能 SD 卡各自交互表示合法身份的证书信息，并进行对证书进行合法性校验，身份认证通过以后，进行会话密钥的协商，共同生成用于加密数据的会话密钥。

[0024] 优选地，所述移动支付服务器产生的响应数据采用所述会话密钥进行加密后反馈给智能 SD 卡。

[0025] 本发明所提供的智能 SD 卡 100 不同于一般仅仅具有存储功能的 SD 卡，可支持 SCWS、PKI 及 JavaApplet 等应用，使其成为智能卡，为移动支付提供安全的应用环境。本发明所提供的智能 SD 卡移动支付方法采用 SCWS 技术和 PKI 证书技术实现安全的远程支付应用。

[0026] 图 1 为本发明的较佳实施例智能 SD 卡的示意图。

[0027] 图 2 为采用图 1 中的智能 SD 卡进行移动支付时的连接示意图。

[0028] 【附图说明】

[0029] 图 3 为本发明的移动支付方法的流程示意图。

[0030] 图 4 为本发明的智能 SD 卡与移动终端之间的通讯机制示意图。

[0031] 为了更好地理解本发明，以下将结合附图对发明的实施例进行详细的说明。

[0032] 现有的 SD 卡主要是一个提供存储功能的数据存储设备。为了解决上述问题，本发明提供一种如图 1 中所示的智能 SD 卡 100，该智能 SD 卡 100 能够支持 SCWS(Smart Card Web Sever，智能卡网络服务器）、PKI(Public Key Infrastructure，公钥基础设施）和 JavaApplet 等应用。

[0033] 【具体实施方式】

[0034] 如图 1 和图 2 中所示，该智能 SD 卡 100 包括 JVM(Java Virtual Machine) 模块 110、机卡通讯模块 120、支付应用模块 130、GP 模块 140、PKI 功能模块 150、SCWS 模块 160 及 JVM 模块 170。

[0035] JVM 模块 110 为智能 SD 卡 100 提供一个基于 Java Card 虚拟机环境，提供整个智能 SD 卡 100 的应用与硬件交互、外界通讯的基本能力。

[0036] 机卡通讯模块 120 是智能 SD 卡 100 与移动终端 200 进行数据交互的模块。

[0037] 支付应用模块 130 主要提供生成与用户交互的 Web 页面并处理与支付服务器 300 交互的数据。

[0038] GP 模块 140 管理智能 SD 卡 100 上的 JavaApplet 应用的生命周期。

[0039] PKI 模块 150 是智能 SD 卡 100 的密钥管理中心，主要管理和验证证书、对数据进行加解密以及对数据签名并验证签名。

[0040] SCWS 模块 160 为智能 SD 卡 100 提供解析 HTTP/HTTPS(Hypertext Transfer Protocol/Secure Hypertext Transfer Protocol，超文本传输协议 / 安全超文本传输协议）的能力。

[0041] 安全存储模块 170 提供了智能 SD 卡 100 的关键数据安全存储能力，包括密钥、用户信息等数据。

[0042] 如图 2 中所示，智能 SD 卡 100 与移动终端 200 之间采用 SCWS 技术与 PKI 证书结合的方法，支付服务器 300 可通过移动终端 200 实现使用浏览器用 Web 方式来访问智能 SD 卡 100 上的支付应用。借助 SSL(Secure Socket Layer) 机制，可确保浏览器与智能 SD 卡 100 之间的数据安全。同时，在一张智能 SD 卡 100 中，采用符合 GlobalPlatform(以下简称 GP) 规范的管理方式可以集成多个不同银行的支付应用在其中，从而用户无需购买多张 SD 卡即可实现多个银行账户的移动支付。此外，智能 SD 卡 100 中的关键数据（例如密钥、用户信息等）的存储由安全存储模块 170 来进行管理，可确保关键数据的存储安全。另一方面，通过 GP 平台系统，可以远程对智能 SD 卡 100 的中支付应用模块 130 进行远程安装、卸载、挂起等操作。

[0043] 如图 3 中所示，本发明也提供一种安全协议实现智能 SD 卡 100 与支付服务器 300 进行移动支付的方法，可确保智能 SD 卡 100 与支付服务器 300 之间数据传输安全性和合法性。具体的步骤如下：

[0044] 在步骤 S1 中，用户在移动终端 200 的浏览器中输入指定的支付应用页面地址，提交支付页面的请求。同时，浏览器检测到该链接是否需要采用 HTTPS 方式进行连接。因为智能 SD 卡中的 SCWS 模块 160 是采用 HTTP 协议进行数据传输的，如果需要采用数据加密方

式，就需要采用 HTTPS 协议。

[0045] 在步骤 S2 中，浏览器检测是否建立 SSL 安全链接，如没有，则发起 SSL(Secure Socket Layer) 握手协议。该请求数据由移动终端 200 的代理程序（以下简称 Proxy）通过机卡通讯模块 120 转发给智能 SD 卡 100 中的 SCWS 模块 160，SCWS 模块 160 与移动终端 200 的浏览器完成 SSL 握手，同时生成用于加密传输数据的会话密码。其中，使用到安全存储模块 170 中的 SD 卡证书作为关键数据传输的加密密钥，该协商流程会在浏览器和 SD 卡 SCWS 模块中各自生成用于后续数据加密的相同会话密钥。

[0046] 在步骤 S3 中，移动终端 200 的浏览器采用会话密码对用户发起的支付应用请求进行加密，由 Proxy 转发给智能 SD 卡 100 的 SCWS 模块 160

[0047] 在步骤 S4 中，智能 SD 卡 100 的 SCWS 模块 160 使用会话密钥进行请求数据的解密，调用支付应用模块 130 的接口进行支付应用请求处理并生成响应数 据。

[0048] 在步骤 S5 中，智能 SD 卡 100 的支付应用模块 130 检测是否需要和支付服务器 300（以下简称服务器 300）进行数据交互。

[0049] 如果是，则在步骤 S6 中，通过 SCWS 模块 160 发起与服务器 300 的安全协议握手请求，该请求由通信终端 200 的 Proxy 进行转发。在服务器 300 与智能 SD 卡 100 的 SCWS 模块 160 进行安全协议的握手流程中，各自交互表示合法身份的证书信息，并进行对证书进行合法性校验，身份认证通过以后，进行会话密钥的协商，共同生成用于加密数据的会话密钥。在此同时，智能 SD 卡 100 通过 Proxy 发送采用与服务器 300 的会话密码加密后的支付业务请求数据给服务器 300。

[0050] 在步骤 S7 中，服务器 300 使用会话密码进行数据解密、处理后生成响应数据；并对支付业务的响应数据进行加密。

[0051] 在步骤 S8 中，加密后的数据通过移动终端 200 的 Proxy 转发给智能 SD 卡 100 的 SCWS 模块 160。

[0052] 在步骤 S9 中，智能 SD 卡 100 的 SCWS 模块 160 使用与服务器 300 之间会话密钥解密支付业务响应数据，然后调用支付应用模块 130 拼装页面数据，并返回给 SCWS 模块 160 采用与浏览器的会话密钥对数据进行加密。

[0053] 在步骤 S10 中，加密后的数据通过 Proxy 返回给移动终端 200，浏览器先对响应数据进行解密，再在浏览器的页面上进行渲染和显示。

[0054] 如果用户发起新的支付请求，则从步骤 S1 开始相应的流程。

[0055] 本发明所提供的移动终端 200 与智能 SD 卡 100 之间的数据通讯机制和原理如图 4 中所示，其具体的步骤如下：

[0056] 在步骤 T1 中，移动终端 200 在智能 SD 卡 100 中创建临时文件。

[0057] 在步骤 T2 中，移动终端 200 应用按照智能 SD 卡 100 与移动终端 200 的通讯协议组装机卡指令。

[0058] 在步骤 T3 中，移动终端 200 调用文件系统 API 将机卡指令写入临时文件。

[0059] 在步骤 T4 中，智能 SD 卡 100 的机卡通讯模块 120 拦截写入文件的请求。

[0060] 在步骤 T5 中，机卡通讯模块 120 检测写入数据是否为机卡通讯协议数据。

[0061] 如果不是机卡通讯协议数据，则进入步骤 T6。在步骤 T6 中，将数据则作为普通的文件写入请求，直接写入智能 SD 卡 100 中。

[0062] 如果是机卡通讯协议数据，则拦截该写入请求。在步骤 T7 中，机卡通讯模块 120 将写入数据作为机卡指令发送给 SCWS 模块 160，SCWS 模块 160 再转发给支付应用模块 130 进行处理。

[0063] 在步骤 T8 中，移动终端 300 写入数据成功以后，使用文件系统 API 进行读取该文件信息。

[0064] 在步骤 T9 中，支付应用模块 130 将响应数据通过 SCWS 模块 160 进行封装，再由机卡通讯模块 120 返回给移动终端 200。

[0065] 在步骤 T10 中，上述步骤完成一个完整的指令交互流程后，如果没有其它操作，移动终端 200 系统 API 关闭当前临时文件的句柄，释放资源。

[0066] 本发明所涉及的智能 SD 卡 100 不同于一般仅仅具有存储功能的 SD 卡，可支持 SCWS、PKI 及 JavaApplet 等应用，使其成为智能卡，为移动支付提供安全的应用环境。本发明所涉及的智能 SD 卡移动支付方法采用 SCWS 技术和 PKI 证书技术实现安全的远程支付应用。

[0067] 以上所述实施例仅表达了本发明的几种实施方式，其描述较为具体和详细，但并不能因此而理解为对本发明专利范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本发明构思的前提下，还可以做出若干变形和改进，这些都属于本发明的保护范围。因此，本发明专利的保护范围应以所附权利要求为准。

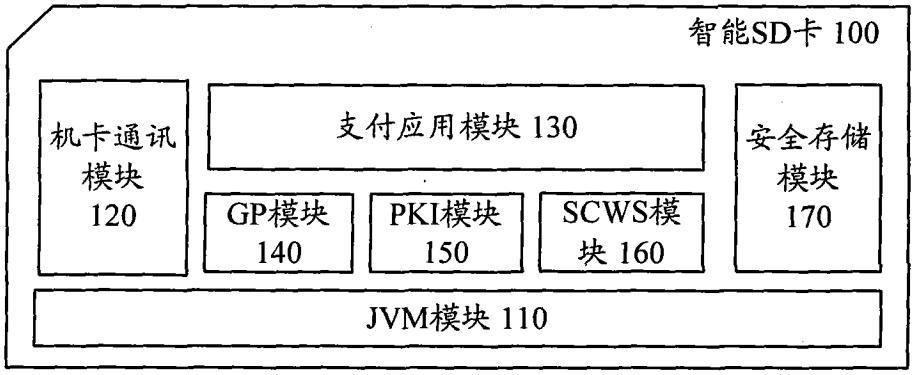

智能SD卡 100
机卡通讯模块 120
支付应用模块 130
GP模块 140
PKI模块 150
SCWS模块 160
安全存储模块 170
JVM模块 110

图 1

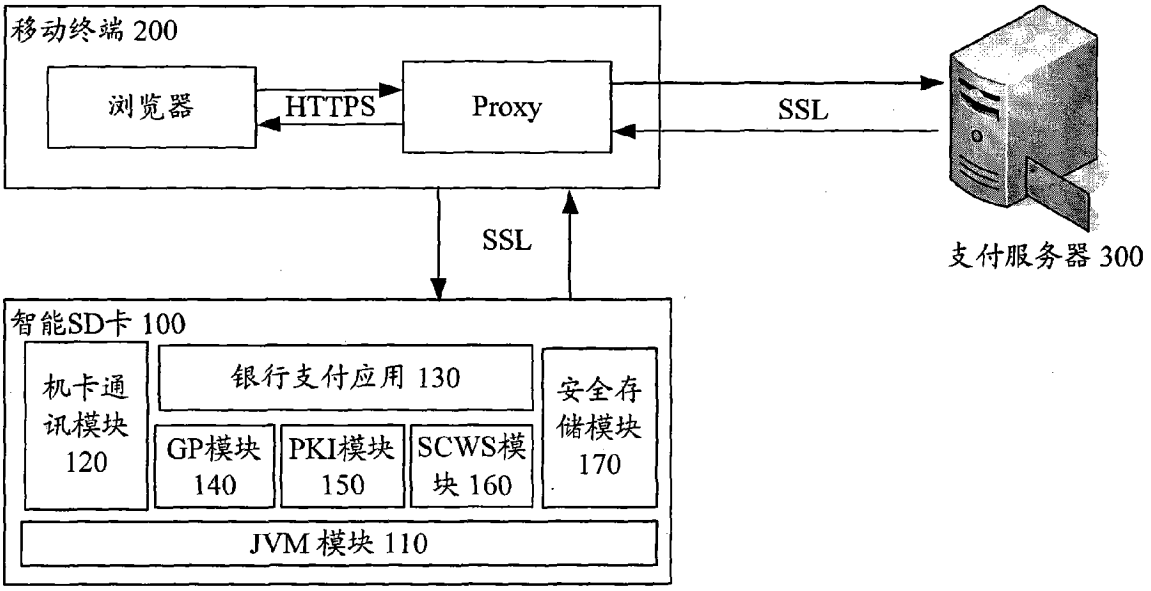

移动终端 200
浏览器
HTTPS
Proxy
SSL
SSL
支付服务器 300
智能SD卡 100
机卡通讯模块 120
银行支付应用 130
GP模块 140
PKI模块 150
SCWS模块 160
安全存储模块 170
JVM 模块 110

图 2

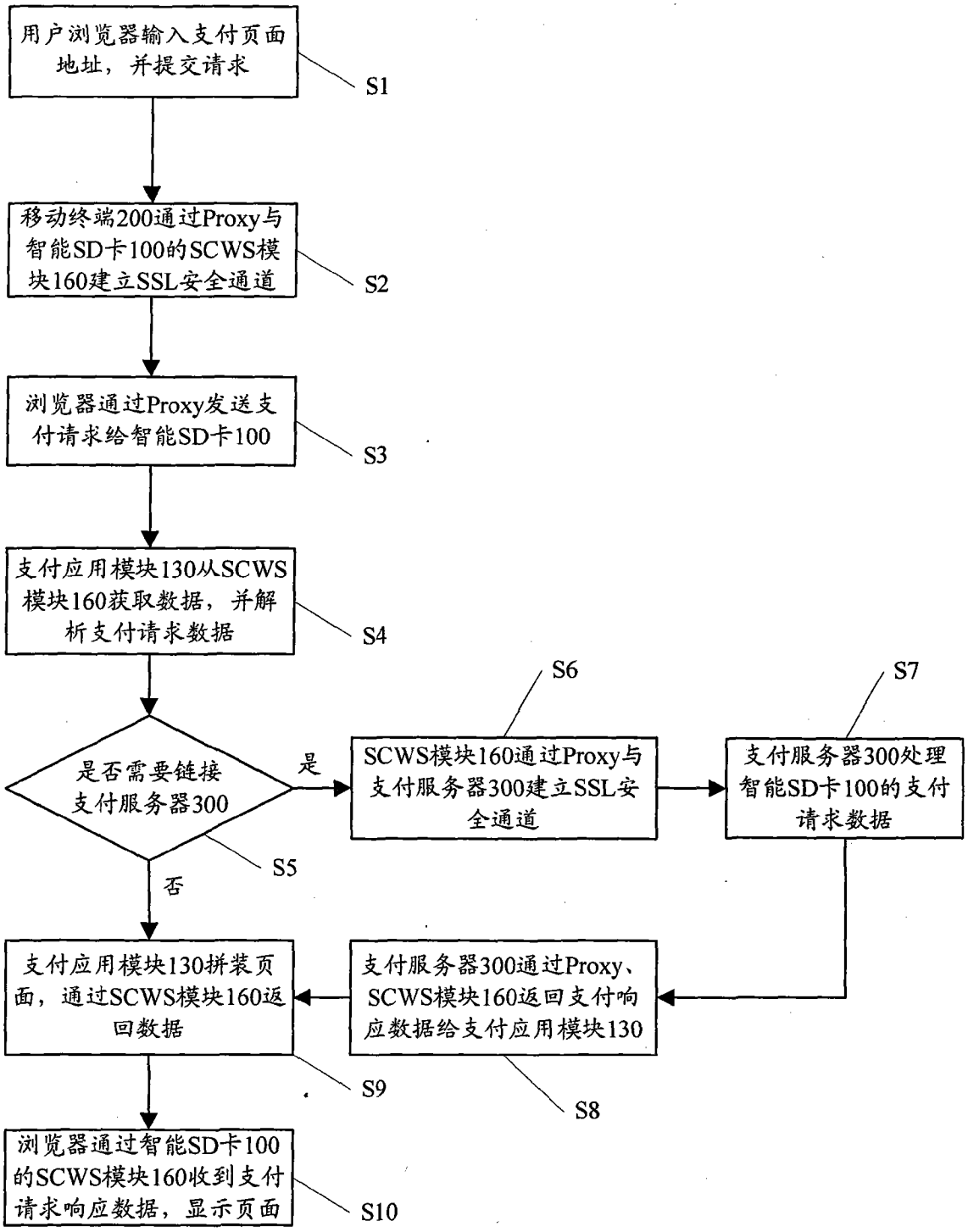

用户浏览器输入支付页面地址，并提交请求
S1
移动终端200通过Proxy与智能SD卡100的SCWS模块160建立SSL安全通道
S2
浏览器通过Proxy发送支付请求给智能SD卡100
S3
支付应用模块130从SCWS模块160获取数据，并解析支付请求数据
S4
是否需要链接支付服务器300
是
否
S5
S6
SCWS模块160通过Proxy与支付服务器300建立SSL安全通道
S7
支付服务器300处理智能SD卡100的支付请求数据
支付服务器300通过Proxy、SCWS模块160返回支付响应数据给支付应用模块130
S8
支付应用模块130拼装页面，通过SCWS模块160返回数据
S9
浏览器通过智能SD卡100的SCWS模块160收到支付请求响应数据，显示页面
S10

图 3

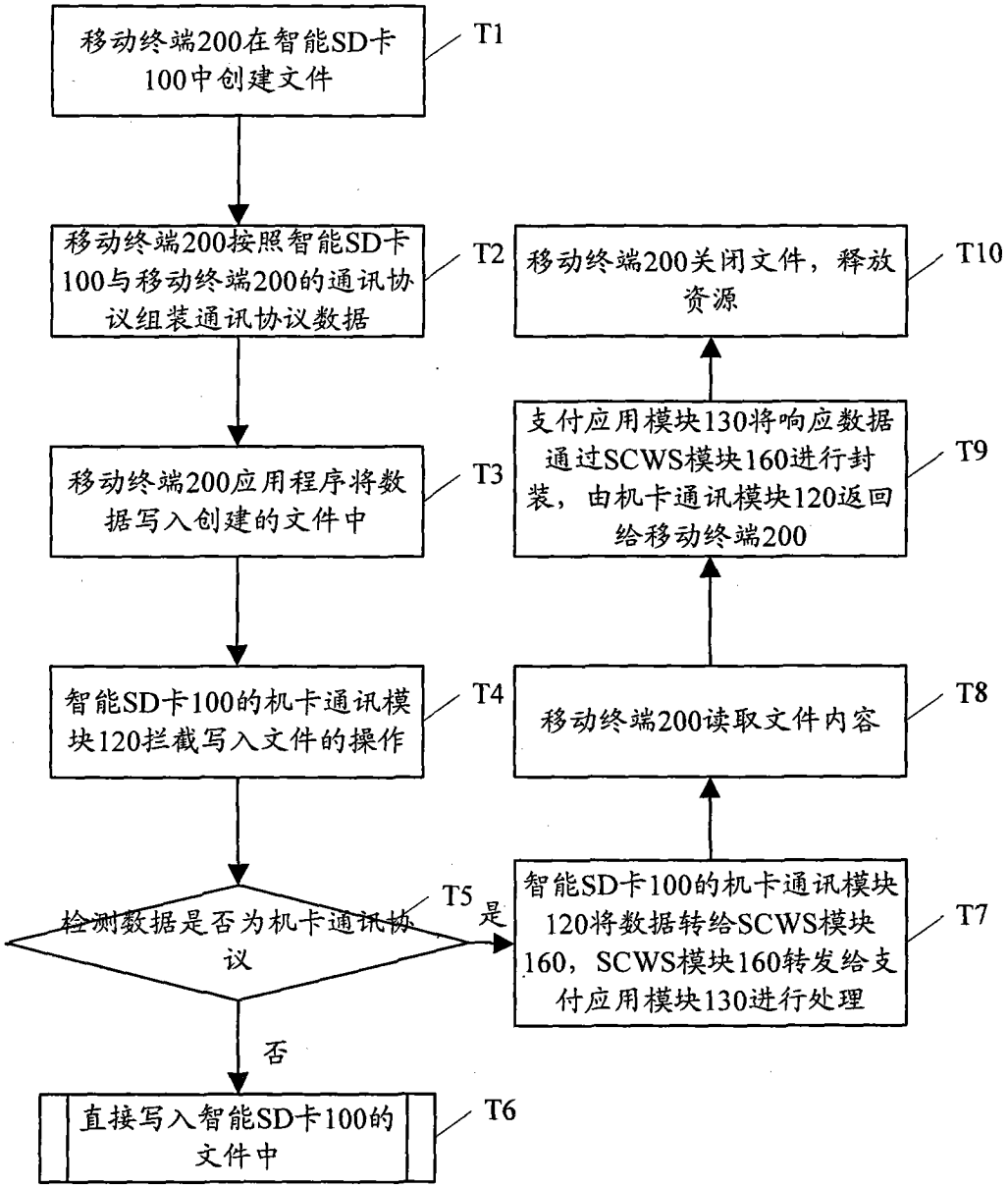

移动终端200在智能SD卡100中创建文件
T1
移动终端200按照智能SD卡100与移动终端200的通讯协议组装通讯协议数据
T2
移动终端200应用程序将数据写入创建的文件中
T3
智能SD卡100的机卡通讯模块120拦截写入文件的操作
T4
检测数据是否为机卡通讯协议
T5
是
否
直接写入智能SD卡100的文件中
T6
智能SD卡100的机卡通讯模块120将数据转给SCWS模块160，SCWS模块160转发给支付应用模块130进行处理
T7
移动终端200读取文件内容
T8
支付应用模块130将响应数据通过SCWS模块160进行封装，由机卡通讯模块120返回给移动终端200
T9
移动终端200关闭文件，释放资源
T10

图 4