数据交互方法及装置、离线信用支付方法及装置

本申请要求2016年01月05日递交的申请号为201610006675.6、发明名称为“数据交互方法及装置、离线信用支付方法及装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及数据交互技术领域，特别涉及数据交互方法及装置、离线信用支付方法及装置。

背景技术

传统的信用支付方式通常是基于磁条信用卡来完成的，存在被仿制，盗用等问题，虽然现在有部分新的信用卡采用了智能卡载体，安全性上有了提高，但还是有大量的信用卡交易是基于磁条来完成的，并且通常信用卡的支付额度较大，用户需要到信用卡发卡行才能调整信用额度，而且每次支付都需要使用信用卡，而这种磁条类型的信用卡安全系数较低，如果信用卡磁条信息被人复制或者信用卡丢失会造成用户很大的损失，安全度相对较低。另外，目前网络上的支付中，通常基于银行卡（包括信用卡）转账的方式来进行支付，该支付过程需要实时完成对用户资金的处理。

发明内容

本申请实施例具体提供了一种数据交互方法，包括，

采集智能终端从远端服务器获取的用于本次交互的授权数据；

记录所述授权数据及本次交互数据。

本申请实施例还提供了一种数据交互方法，包括，

获取远端服务器对用户本次交互的授权数据；

将所述授权数据提供给交互终端，以便所述交互终端基于所述授权数据进行处理。

本申请实施例还提供了一种数据交互方法，包括，

获取用户通过智能终端发送的授权请求；

根据智能终端的授权请求，向所述智能终端发送对用户本次交互的授权数据。

本申请实施例还提供了一种交互终端，包括，

采集单元，用于采集智能终端从远端服务器获取的用于本次交互的授权数据；

记录单元，用于记录所述授权数据及本次交互数据。

本申请实施例还提供了一种智能终端，包括，

获取单元，用于获取远端服务器对用户本次交互的授权数据；

通信单元，用于将所述授权数据提供给交互终端，以便所述交互终端基于所述授权数据进行处理。

本申请实施例还提供了一种远端服务器，包括，

获取单元，用于获取用户通过智能终端发送的授权请求；

处理单元，用于根据智能终端的授权请求，向所述智能终端发送对用户本次交互的授权数据。

本申请实施例还提供了一种离线信用支付方法，包括，

采集智能终端从远端服务器获取的用于本次交易的信用授权数据；

记录所述信用授权数据及本次交易数据。

本申请实施例还提供了一种离线信用支付方法，包括，

获取远端服务器对用户本次交易的信用授权数据；

将所述信用授权数据提供给扣费终端，以便所述扣费终端基于所述信用授权数据进行处理。

本申请实施例还提供了一种离线支付方法，包括，

获取用户通过智能终端发送的信用授权请求；

根据智能终端的信用授权请求，向所述智能终端发送对用户本次交易的信用授权数据。

本申请实施例还提供了一种扣费终端，包括，

采集单元，用于采集智能终端从远端服务器获取的用于本次交易的信用授权数据；

记录单元，用于记录所述信用授权数据及本次交易数据。

本申请实施例还提供了一种智能终端，包括，

获取单元，用于获取远端服务器对用户本次交易的信用授权数据；

通信单元，用于将所述信用授权数据提供给扣费终端，以便所述扣费终端基于所述信用授权数据进行处理。

本申请实施例还提供了一种远端服务器，包括，

获取单元，用于获取用户通过智能终端发送的信用授权请求；

处理单元，用于根据智能终端的信用授权请求，向所述智能终端发送对用户本次交

易的信用授权数据。

本申请实施例还提供了一种离线信用支付系统，包括，智能终端，远端服务器，扣费终端；

所述远端服务器，根据所述智能终端的信用授权请求，向所述智能终端发送对用户本次交易的信用授权数据；

所述智能终端，从所述远端服务器获取所述信用授权数据；

所述扣费终端，采集所述智能终端上的信用授权数据，并记录所述信用授权数据及本次交易数据。

由以上本申请实施例提供的技术方案可见，本申请可基于远端服务器的授权来进行交易的处理，提高支付效率。

当然实施本申请的任一产品或者方法必不一定需要同时达到以上所述的所有优点。

附图说明

为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请中记载的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

图 1 所示为本申请实施例一种数据交互方法的流程图；

图 2 所示为本申请实施例一种数据交互方法的流程图；

图 3 所示为本申请实施例一种数据交互方法的流程图；

图 4 所示为本申请实施例一种交互终端的结构示意图；

图 5 所示为本申请实施例一种智能终端的结构示意图；

图 6 所示为本申请实施例一种远端服务器的结构示意图；

图 7 所示为本申请实施例一种离线信用支付方法的流程图；

图 8 所示为本申请实施例一种离线信用支付方法的流程图；

图 9 所示为本申请实施例一种离线信用支付方法的流程图；

图 10 所示为本申请实施例一种扣费终端的结构示意图；

图 11 所示为本申请实施例一种智能终端的结构示意图；

图 12 所示为本申请一种远端服务器的结构示意图；

图 13 所示为本申请实施例一种离线信用支付系统的结构示意图；

图 14 所示为本申请实施例一种离线信用支付的具体方法流程图；

图 15 所示为本申请实施例另一种离线信用支付的具体方法流程图。

具体实施方式

本申请实施例提供一种数据交互方法及装置、离线信用支付方法及装置。

为了使本技术领域的人员更好地理解本申请中的技术方案，下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都应当属于本申请保护的范围。

本申请提供的技术方案可应用于信用支付中，例如小金额、频繁的支付场景，具体如公交、地铁等支付场景等。本申请提供的技术方案可在支付交易时，由交易用户端，例如用户持有的智能终端，和交易处理端，例如公交车上的扣费终端来交互实现扣费过程，同时交易用户端和交易处理端均可通过远端服务器之间的交互实现支付过程。当然，本申请提供的技术方案也可不局限于支付应用中，例如可应用于对用户积分（商家为用户提供的积分，该积分可在使用商家服务或购买商家产品时享受优惠）的处理中等等。

在传统的信用支付方式，即利用信用卡支付，在 POS 机上需要联机操作，对于某些应用场景，例如地铁购票等场景，交易时间相对较长，而本申请交互方法可实现离线支付，即在交易处理端可不用实时联网就可以实现对用户的扣费处理，避免了交互时交易处理端连接网络，提升了交互的速度，并且适用于网络状况不好的环境下实现双方的交互，使得扣费可以离线进行；同时每次交易生成的信用授权数据可以是临时生成的，不具有重复利用的可能，解决了现有技术中磁条类银行卡的信息泄露，而造成用户经济损失的问题。当然，在一些场景下，信用授权数据也可以是具有较长使用时间，例如一年、一个月或者一个星期等，即每次交易时可不用临时生成授权数据，而是每一年或每一个月或每一个星期获取一次授权，当授权失效时，可通知用户再获取一次授权。下面将对本申请技术方案做详细说明。

如图 1 所示为本申请实施例一种数据交互方法的流程图，该方法可应用于交易处理的交易用户端和交易处理端之间的交易处理，其中交易用户端可以是用户持有的智能终端，例如手机等，交易处理终端可以是商家持有的商家终端，本实施例将以用户持有的智能终端与商家终端之间的处理过程进行说明。具体可包括如下步骤：

步骤 101，采集智能终端从远端服务器获取的用于本次交互的授权数据。

步骤 102，记录所述授权数据及本次交互数据。

该步骤 101 和 102 的执行主体为上述的商家终端，可采集智能终端发送的授权数据，并记录该授权数据和交易数据。

作为本申请的一个实施例，商家终端记录了授权数据和本次交互数据后在预定的时间与所述远端服务器进行授权数据和交互数据的核对。即商家终端可以在后台与远端服务器进行交互，来对本次交易中的授权数据以及交互数据进行核对，并同步给远端服务器进行记录等处理。

作为本申请的一个实施例，所述采集智能终端从远端服务器获取的用于本次交互的授权数据进一步包括，通过扫描所述智能终端根据所述授权数据生成的条码获得所述授权数据；

或者，通过无线通信的方式从所述智能终端获得所述授权数据。

作为本申请的一个实施例，所述条码包括一维条码和/或二维条码，所述无线通信方式包括近场通信方式或 RFID 方式。

作为本申请的一个实施例，在采集智能终端从远端服务器获取的用于本次交互的授权数据之后还包括进行如下判断之一或者组合来对所述授权数据进行验证：

通过利用授权数据中的时间信息与当前时间的比较，如果当前时间超过授权数据中的时间信息，则所述授权数据过期，取消本次数据交互；

判断在以往的数据交互中是否存在所述授权数据中的随机数，如果存在，则所述授权数据为重复授权，取消本次数据交互；

判断本次交互数据是否超过所述授权数据中的一门限值，如果超过，则取消本次数据交互。

作为本申请的一个实施例，采集智能终端从远端服务器获取的用于本次交互的授权数据中，还包括有远端服务器通过私钥对授权数据进行签名的签名信息；该方法还包括：

在采集智能终端从远端服务器获取的用于本次交互的授权数据之后，记录所述授权数据及本次交互数据之前还包括：

利用预先从所述远端服务器获取的公钥，对所述签名信息进行验签，确定所述授权数据是否为远端服务器下发的，以便确定为远端服务器下发的授权数据时，执行记录所述授权数据以及本次交互数据的步骤。

上述的用于本次交互的授权数据可以是由智能终端临时从远端服务器来实时获取

的，或者，该授权数据也可以是智能终端从远端服务器获取后，在一定时间内生效的，例如一个月等。

上述的交互过程对于商家终端来说可以不用进行网络通信即可完成对智能终端的交互，节省了商家终端连接网络的时间，并且在一些网络状况不好的情况下，可以顺利的完成与智能终端的交互。

如图 2 所示为本申请实施例一种数据交互方法的流程图，在该图中描述了智能终端实现本申请的数据交互的过程，具体可包括一下步骤：

步骤 201，获取远端服务器对用户本次交互的授权数据。

步骤 202，将所述授权数据提供给交互终端，以便所述交互终端基于所述授权数据进行处理。

上述所述将授权数据发送给交互终端包括以条码形式呈现给扣费终端，还包括通过 RFID 等射频方式将授权数据等交互数据发送给扣费终端。

作为本申请的一个实施例，获取远端服务器对用户本次交互的授权数据中进一步包括，向所述远端服务器发送用户的唯一标识符；

接收所述远端服务器根据所述唯一标识符生成的包含了用户信息的授权数据。

作为本申请的一个实施例，所述授权数据中还包括，本次授权的时间信息、本次授权的随机数和门限值。

该步骤 201-步骤 202 可以上述的步骤 101-步骤 102 一起来实现交易用户端与交易处理端之间的交互过程。其中，步骤 201 和步骤 202 可以是交易用户端根据交易处理端触发的交易请求后进行。

如图 3 所示为本申请实施例一种数据交互方法的流程图，在该图中描述的是远端服务器在数据交互中的工作流程，远端服务器根据用户的请求生成授权数据并发送给智能终端。具体可包括如下步骤：

步骤 301，获取用户通过智能终端发送的授权请求。

步骤 302，根据智能终端的授权请求，向所述智能终端发送对用户本次交互的授权数据。

作为本申请的一个实施例，所述授权请求中包括用户的唯一标识，所述向所述智能终端发送对用户本次交互的授权数据，具体包括，根据所述唯一标识符生成的包含了用户信息的授权数据，向所述智能终端发送对用户本次交互的授权数据。该用户的唯一标识可以是用户的用户名，或者也可以是用户手持的智能终端的设备标识，或者也可以是

二者结合的数据，这样可保证用户获取授权数据的安全性。

作为本申请的一个实施例，向所述智能终端发送对用户本次交互的授权数据，具体包括：对用户信息进行加密，并利用私钥对授权数据进行签名，将签名信息和授权信息以口令方式下发给智能终端。

其中加密可以使用现有技术中的加密手段进行，例如可通过私钥、公钥对的方式来进行加密处理等，在此不再赘述。

通过上述本申请的实施例，远端服务器向智能终端发送了授权数据后，智能终端就可以根据该授权数据实现与交易处理端的进行离线数据交互。

如图 4 所示为本申请实施例一种交互终端的结构示意图，在本图中的功能单元均可以由逻辑电路或者芯片来实现，或者还可以通过高性能计算机来实现。

具体包括采集单元 401，用于采集智能终端从远端服务器获取的用于本次交互的授权数据。

记录单元 402，用于记录所述授权数据及本次交互数据。

作为本申请的一个实施例，还包括核对单元 403，用于在预定的时间与所述远端服务器进行授权数据和交互数据的核对。

作为本申请的一个实施例，所述采集单元进一步包括扫描模块 404，用于扫描所述智能终端根据所述授权数据生成的条码获得所述授权数据；

或者包括无线通信模块 405，用于以无线通信的方式从所述智能终端获得所述授权数据。

所述条码包括一维条码和/或二维条码，所述无线通信方式包括近场通信方式或 RFID 方式。

作为本申请的一个实施例，还包括验证单元 407，进行如下判断之一或者组合来对所述授权数据进行验证：

通过利用授权数据中的时间信息与当前时间的比较，如果当前时间超过授权数据中的时间信息，则所述授权数据过期，取消本次数据交互；

判断在以往的数据交互中是否存在所述授权数据中的随机数，如果存在，则所述授权数据为重复授权，取消本次数据交互；

判断本次交互数据是否超过所述授权数据中的一门限值，如果超过，则取消本次数据交互。

作为本申请的一个实施例，采集智能终端从远端服务器获取的用于本次交互的授权

数据中，还包括有远端服务器通过私钥对授权数据进行签名的签名信息；该交互终端还包括：

验签单元 406，用于利用预先从所述远端服务器获取的公钥，对所述签名信息进行验签，确定所述授权数据是否为远端服务器下发的，以便确定为远端服务器下发的授权数据时，由记录单元记录所述授权数据以及本次交互数据。

本实施例中的交互终端具体可以是上述的交易处理端，例如商家终端等，其可以实现上述对应方法中的各步骤。在此不再赘述。

如图 5 所示为本申请实施例一种智能终端的结构示意图，在该图中描述了能够实现本申请数据交互目的的智能终端的结构，当然智能终端还可以包括其它必要部分，例如触摸屏幕、电池、内存、电路板等在此不再赘述，该智能终端可以为智能手机、平板电脑、或者其它智能穿戴设备等。

具体包括获取单元 501，用于获取远端服务器对用户本次交互的授权数据。

通信单元 502，用于将所述授权数据提供给交互终端，以便所述交互终端基于所述授权数据进行处理。

作为本申请的一个实施例，所述获取单元 501 进一步用于，向所述远端服务器发送用户的唯一标识符；接收所述远端服务器根据所述唯一标识符生成的包含了用户信息的授权数据。

作为本申请的一个实施例，所述授权数据中还包括，本次授权的时间信息、本次授权的随机数和门限值。

如图 6 所示为本申请实施例一种远端服务器的结构示意图，在该图中描述了能够实现本申请数据交互目的的远端服务器的结构，当然远端服务器还可以包括其它必要部分，例如输入输出设备、通信单元、电源、内存、电路板等在此不再赘述，该远端服务器可以为高性能计算机或者为计算机集群。

具体包括获取单元 601，用于获取用户通过智能终端发送的授权请求。

处理单元 602，用于根据智能终端的授权请求，向所述智能终端发送对用户本次交互的授权数据。

根据本申请的一个实施例，所述授权请求中包括用户的唯一标识，所述处理单元，具体用于根据所述唯一标识符生成的包含了用户信息的授权数据，向所述智能终端发送对用户本次交互的授权数据。

根据本申请的一个实施例，所述处理单元向所述智能终端发送对用户本次交互的授

权数据，具体包括：对用户信息进行加密，并利用私钥对授权数据进行签名，将签名信息和授权信息以口令方式下发给智能终端。

下面将以在支付中的技术实现过程进行详细说明。

如图 7 所示为本申请实施例一种离线信用支付方法的流程图，该图描述了能够使得扣费终端不用网络通信就可以实现对用户的扣费工作流程，通过后期将信用授权数据和交易数据发送给银行等机构就可以实现离线扣费的目的。其中的扣费终端可以为 POS 机终端或者其它扣费设备，扣费终端需要事先在服务端注册并获得相应的授权才能进行信用扣费，在所述扣款终端记录本次支付交易的扣款记录后以完成本次支付交易，并定期将扣费记录发送到服务端进行核对，以实际上完成对用户的消费行为进行扣费的目的。具体可以包括如下步骤：

步骤 701，采集智能终端从远端服务器获取的用于本次交易的信用授权数据。

步骤 702，记录所述信用授权数据及本次交易数据。

根据本申请的一个实施例，在记录所述信用授权数据及本次交易的数据之后还包括，在预定的时间与远端服务器进行所述信用授权数据及本次交易数据的核对。

本步骤在核对之前，扣费终端记录信用授权数据及本次交易的数据后可以不立即与远端服务器进行通信。核对是需要扣费终端与远端服务器的通信，并且扣费终端将两次核对时间间隔中产生的所有信用授权数据和相应的交易数据一并打包发送给远端服务器，这样可以节省每次交易时都需要扣费终端与远端服务器进行信用授权通信的时间，可以在预定时间一次性向远端服务器发送大批的核对数据，其中，远端服务器将根据信用授权数据和交易数据对用户的账户进行扣款。

根据本申请的一个实施例，所述用于本次交易的信用授权数据至少包括，本次信用授权的时间信息、本次信用授权的随机数、用户的账户信息和信用额度。

其中，信用授权数据是从远端服务器中获得，本次信用授权的时间信息进一步包括，本次信用授权的当前时间和有效时长，从而可以确定本次信用授权从什么时间开始，在什么时间结束，超出了本次信用授权的时间规定，则不允许进行后续的扣款；所述本次信用授权的随机数为本次信用授权的唯一识别符，也就是说每次信用授权都是独立的，每次信用授权都将重新生成该识别符，从而可以区分每一次的信用授权；所述用户的账户信息进一步可以包括用户的账户 ID，或者银行卡号码（信用卡号码）等；所述信用额度可以用于指示本次交易的扣款金额上限，如果扣款金额超出该上限，则本次交易不成功。

根据本申请的一个实施例，所述采集智能终端从远端服务器获取的用于本次交易的信用授权数据进一步包括，通过扫描所述智能终端根据所述信用授权数据生成的条码获得所述信用授权数据；

或者，通过无线通信的方式从所述智能终端获得所述信用授权数据。

其中，所述条码包括二维条码或一维条码，所述无线通信方式包括 NFC（近场通信）、RFID（无线射频识别）或者蓝牙等方式。

根据本申请的一个实施例，在采集智能终端从远端服务器获取的用于本次交易的信用授权数据之后还包括，利进行如下判断之一或者组合来对所述信用授权数据进行验证：

通过利用信用授权数据中的时间信息与当前时间的比较，如果当前时间超过信用授权数据中的时间信息，则所述信用授权数据过期，取消本次交易；

判断在以往的交易数据中是否存在所述授权数据中的随机数，如果存在，则所述信用授权数据为重复授权，取消本次交易；

判断本次交易金额是否超过所述信用授权数据中的信用额度，如果超过，则取消本次交易。

在上述步骤中，信用授权数据中可以不包括时间信息，只是由智能终端一次性获得信用授权数据，并可以使用一段时间，例如一周、一个月，在每次需要扣费的场景中，只需要验证信用额度即可，每次扣费后（通常是无线通信的方式，这样可以实现数据的交互，通知智能终端本次交易扣费数额），智能终端中保存的信用授权数据都将被修改（递减），直到减为 0 或者低于一个门限值，则不允许继续使用该信用授权数据进行交易。

根据本申请的一个实施例，采集智能终端从远端服务器获取的用于本次交易的信用授权数据中，还包括有远端服务器通过私钥对信用授权数据进行签名的签名信息；该方法还包括：

在采集智能终端从远端服务器获取的用于本次交易的信用授权数据之后，记录所述信用授权数据及本次交易数据之前还包括:

利用预先从所述远端服务器获取的公钥，对所述签名信息进行验签，确定所述信用授权数据是否为远端服务器下发的，以便确定为远端服务器下发的信用授权数据时，执行记录所述信用授权数据以及本次交易数据的步骤。

本实施例中，智能终端从远端服务器获取的授权数据，可以是临时的，也可以是一次性的（例如可以是一次性授权，具有一定时间的有效性）。

通过上述本申请实施例的方法，在用户不使用银行卡的情况下，扣费终端不联网就可以快速的完成交易扣费，并且每次交易生成的信用授权数据可以是临时生成的，不具有重复利用的可能，解决了现有技术中磁条类银行卡的信息泄露，而造成用户经济损失的问题。

如图 8 所示为本申请实施例一种离线信用支付方法的流程图，在该图中描述了智能终端获取信用授权数据后与扣费终端进行离线支付的过程。

具体包括步骤 801，获取远端服务器对用户本次交易的信用授权数据。

步骤 802，将所述信用授权数据提供给扣费终端，以便所述扣费终端基于所述信用授权数据进行处理。

根据本申请的一个实施例，获取远端服务器对用户本次交易的信用授权数据中进一步包括，向所述远端服务器发送用户的唯一标识符；

接收所述远端服务器根据所述唯一标识符生成的包含了用户账户信息的信用授权数据。

其中，该标识符可以是用户的用户名，例如用户 ID，或者智能终端的设备标识，或者二者结合形成的一个标识信息等。

本步骤中智能终端可以在有网络的情况下与远端服务器通信获得包含用户账户信息的信用授权数据，这样可以减少扣费终端在对每个智能终端进行交易时连接网络的延迟。其中的信用授权数据可能包括的用户账户信息是指例如为银行卡号码、联系电话等信息。

根据本申请的一个实施例，所述信用授权数据中还可以包括，本次信用授权的时间信息、本次信用授权的随机数和信用额度。

如图 9 所示为本申请实施例一种离线信用支付方法的流程图，在该图中描述了远端服务器在离线支付方法中的工作流程。

具体包括步骤 901，获取用户通过智能终端发送的信用授权请求。

步骤 902，根据智能终端的信用授权请求，向所述智能终端发送对用户本次交易的信用授权数据。

根据本申请的一个实施例，所述信用授权请求中包括用户的唯一标识，所述向所述智能终端发送对用户本次交易的信用授权数据，具体包括：

根据所述唯一标识符生成的包含了用户信息的授权数据，向所述智能终端发送对用户本次交易的信用授权数据。

根据本申请的一个实施例，向所述智能终端发送对用户本次交易的授权数据，具体

包括：对用户信息进行加密，并利用私钥对信用授权数据进行签名，将签名信息和信用授权数据以口令方式下发给智能终端。

在本步骤中，使用私钥对信用授权数据进行签名后，扣费终端需要用公钥对信用授权数据的签名进行验证，即可以验证该信用授权数据是否为远端服务器下发的，如果用户的账户信息保留在扣费终端则是不安全的，因此需要对用户的账户信息进行加密，以保护用户的账户信息，具体的加密方法可以参考现有技术中的方法，在此不再赘述。

上述图 7、图 8 和图 9 所示的各步骤可以协同工作，来实现信用支付，具体而言，当支付时，可由智能终端主动发起，或者由扣费终端来主动发起，例如，在公交应用场景中，智能终端中的 NFC 设备和公交中的扣费终端的 NFC 设备之间可实现支付的交互过程，且可由扣费终端通过 NFC 设备发起支付过程，即扣费终端可发起支付请求，然后从智能终端获取授权数据，完成支付过程，又例如，在公交应用场景中，公交中的扣费终端可通过其上配置的条码扫描装置，来扫描用户手持的智能终端上显示的二维码来发起支付过程，等等。

如图 10 所示为本申请实施例一种扣费终端的结构示意图，在该图中所描述的扣费终端可以包括 POS 机、智能手机等设备，各功能单元均可以由逻辑电路或者芯片来实现，或者还可以通过高性能计算机来实现。

具体包括采集单元 1001，用于采集智能终端从远端服务器获取的用于本次交易的信用授权数据。

记录单元 1002，用于记录所述信用授权数据及本次交易数据。

根据本申请的一个实施例，还包括核对单元 1003，用于在预定的时间与所述远端服务器进行信用授权数据和交易数据的核对。

根据本申请的一个实施例，所述用于本次交易的信用授权数据至少包括，本次信用授权的时间信息、本次信用授权的随机数、用户的账户信息和信用额度。

根据本申请的一个实施例，所述采集单元进一步包括扫描模块 1004，用于扫描所述智能终端根据所述信用授权数据生成的条码获得所述信用授权数据；

或者，包括无线通信模块 1005，用于以无线通信的方式从所述智能终端获得所述信用授权数据。

根据本申请的一个实施例，所述条码包括一维条码和/或二维条码；所述无线通信方式包括近场通信方式或 RFID 方式。

根据本申请的一个实施例，还包括验证单元 1007，进行如下判断之一或者组合来对

所述信用授权数据进行验证：

通过利用信用授权数据中的时间信息与当前时间的比较，如果当前时间超过信用授权数据中的时间信息，则所述信用授权数据过期，取消本次交易；

判断在以往的交易数据中是否存在所述授权数据中的随机数，如果存在，则所述信用授权数据为重复授权，取消本次交易；

判断本次交易金额是否超过所述信用授权数据中的信用额度，如果超过，则取消本次交易。

根据本申请的一个实施例，采集智能终端从远端服务器获取的用于本次交易的信用授权数据中，还包括有远端服务器通过私钥对信用授权数据进行签名的签名信息；该扣费终端还包括：验签单元 1006，用于利用预先从所述远端服务器获取的公钥，对所述签名信息进行验签，确定所述信用授权数据是否为远端服务器下发的，以便确定为远端服务器下发的信用授权数据时，由记录单元记录所述信用授权数据以及本次交易数据。

如图 11 所示为本申请实施例一种智能终端的结构示意图，在该图中描述了实现本申请离线支付目的的智能终端的结构，当然智能终端还可以包括其它必要部分，例如触摸屏幕、电池、内存、电路板等在此不再赘述，该智能终端可以为智能手机、平板电脑、或者其它智能穿戴设备等。

具体包括，获取单元 1101，用于获取远端服务器对用户本次交易的信用授权数据。

通信单元 1102，用于将所述信用授权数据提供给扣费终端，以便所述扣费终端基于所述信用授权数据进行处理。

根据本申请的一个实施例，所述获取单元进一步用于，向所述远端服务器发送用户的唯一标识符；接收所述远端服务器根据所述唯一标识符生成的包含了用户账户信息的信用授权数据。

根据本申请的一个实施例，所述信用授权数据中还包括，本次信用授权的时间信息、本次信用授权的随机数和信用额度。

如图 12 所示为本申请一种远端服务器的结构示意图，在该图中描述了实现离线支付的远端服务器，当然远端服务器还可以包括其它必要部分，例如输入输出设备、通信单元、电源、内存、电路板等在此不再赘述，该远端服务器可以为高性能计算机或者为计算机集群。

具体包括：

获取单元 1201，用于获取用户通过智能终端发送的信用授权请求；

处理单元 1202，用于根据智能终端的信用授权请求，向所述智能终端发送对用户本次交易的信用授权数据。

根据本申请的一个实施例，所述信用授权请求中包括用户的唯一标识，所述处理单元，具体用于根据所述唯一标识符生成的包含了用户信息的信用授权数据，向所述智能终端发送对用户本次交易的信用授权数据。

根据本申请的一个实施例，所述处理单元向所述智能终端发送对用户本次交易的信用授权数据，具体包括：对用户信息进行加密，并利用私钥对信用授权数据进行签名，将签名信息和信用授权信息以口令方式下发给智能终端。

如图 13 所示为本申请实施例一种离线信用支付系统的结构示意图，在该图中描述了实现离线支付的系统结构，在本实施例中的智能终端可以包括智能手机、平板电脑等设备，扣费终端可以包括 POS 机、智能手机等设备，远端服务器可以包括高性能计算机等设备。

具体包括远端服务器 1301， 智能终端 1302，扣费终端 1303；

所述远端服务器 1301，根据所述智能终端的信用授权请求，向所述智能终端发送对用户本次交易的信用授权数据；

所述智能终端 1302，从所述远端服务器获取所述信用授权数据；

所述扣费终端 1303，采集所述智能终端上的信用授权数据，并记录所述信用授权数据及本次交易数据。

通过上述本申请实施例的系统，在用户不使用银行卡的情况下，扣费终端不联网就可以快速的完成交易扣费，并且每次交易生成的信用授权数据都是临时生成的，不具有重复利用的可能，解决了现有技术中磁条类银行卡的信息泄露，而造成用户经济损失的问题。

如图 14 所示为本申请实施例一种离线信用支付的具体方法流程图，在本图中扣费终端为 POS 机，智能终端为手机，远端服务器为高性能计算机，该高性能计算机被配置为能够生成信用授权数据，并且能够完成后期 POS 机对账业务的服务器，当然生成信用授权数据和对账业务可以分别由两台或者多台高性能计算机共同协助完成，但是为了附图的简要，本实施例中只以一台远端服务器完成上述两种业务。

具体包括步骤 1401，手机上的信用支付客户端在远端服务器注册。

在该注册过程中包括了验证用户身份、验证金融账户等内容，例如验证用户的身份证信息、信用卡信息或者银行卡信息等。远端服务器将会根据用户的身份或金融账户的

内容生成私钥，用于后期对信用授权数据进行签名。

所述信用支付客户端可以为软件实现的应用，或者将该信用支付客户端内置于手机的安全芯片（例如 eSE 安全芯片）中。

所述 POS 机也在远端服务器上注册，远端服务器向所述 POS 机下发公钥，用于后期 POS 机验证信用授权数据签名。

步骤 1402，信用支付客户端通过手机的射频通信单元（或者 WiFi 网络环境）向远端服务器发起生成信用授权数据的请求。

在附图中本步骤的 TOKEN（）为现有技术中手机与远端服务器通信时使用的令牌。

在该请求中可能进一步包括了手机的 IMEI（移动设备国际身份码）、用户身份标识等信息，以使得远端服务器可以唯一的确定发起请求的用户身份。

步骤 1403，远端服务器根据所述请求生成信用授权数据。

在本步骤中，远端服务器根据所述请求中的用户身份标识或者 IMEI 匹配到相应的用户的金融账户信息，并获得用户信息，所述金融账户信息可能包括信用额度等信息，所述用户信息可能包括用户身份标识、银行卡账号、私钥等信息。

远端服务器生成本次信用授权数据的时间信息，该时间信息中进一步包括当前时间，也就是本次交易所使用的信用授权数据的起始时间，并根据设定得到有效时间长度；远端服务器还生成一随机数，用以唯一的标记本次信用授权数据。

远端服务器将上述时间信息、随机数、以及上一步骤中得到的用户信息、金融账户信息一起生成本次的信用授权数据。

进一步的，远端服务器还可以对用户身份标识、银行卡账号等信息进行加密（也可以放置到智能终端进行加密），并利用私钥对上述信用授权数据进行签名，从而可以确保数据的真实可靠。

在本步骤中，远端服务器还可以根据用户的消费支付记录和信用额度进行判断，如果用户的消费支付记录已经接近或者超过金融账户信息中的信用额度，则拒绝本次信用授权请求，并反馈给手机上的信用支付客户端失败原因。

步骤 1404，远端服务器将信用授权数据拼装成 TOKEN（）下发给手机上的信用支付客户端。

步骤 1405，信用支付客户端将所述信用授权数据生成二维码。

本步骤中生成的二维码可以显示在手机的屏幕上，也可以存储于手机的存储器中，以备本次交易时所使用。

步骤 1406，POS 机的扫描模块通过扫描的方式获得二维码。

本步骤中的扫描二维码的步骤可以使用现有技术中条码扫描设备完成，并将该设备的数据、控制接口与 POS 机相连接，使得 POS 机可以控制该扫描设备完成扫描任务并传回扫描的条码数据。

本申请中的 POS 机可以为安装有扣费客户端应用的 POS 机，或者是一个具有数据处理能力的终端连接 POS 机，在该终端上安装扣费客户端，以执行后续的解析、记录等工作。

步骤 1407，POS 机上的扣费客户端解析所述二维码，获得信用授权数据。

在本步骤中，扣费客户端可以通过公钥对信用授权数据进行验签，验证该信用授权数据是来自于远端服务器。

扣费客户端还可以解析（或者解密）出信用授权数据中的金融账户信息，即本次交易的信用额度。

步骤 1408，扣费客户端利用信用授权数据对本次支付交易进行处理。

在本步骤中的处理可以包括，解析出信用授权数据中的时间信息，判断本次支付交易时间是否超过了信用授权数据中的当前时间+有效时间长度，如果超过则该信用授权数据已经过期，不能用于本次支付交易，可以通知信用支付客户端再次生成本次支付交易的信用授权数据。

判断信用授权数据中的随机数是否已经在以前的交易中使用过，如果没有出现在以前交易的记录中，则该信用授权数据可用，否则可能出现重复扣费，可以通知信用支付客户端再次生成本次支付交易的信用授权数据。

判断本次支付交易的金额是否超过所述信用额度，如果超过则本次支付交易不成功，并向信用支付客户端返回失败原因。

上述的处理可以不分先后顺序，或者可以只进行其中的一项或者几项，或者还可以进行其他的逻辑判断或者处理。

步骤 1409，扣费客户端记录本次扣款记录。

所述扣款记录中包括本次支付交易的金额以及信用授权数据。

在本步骤中的扣费客户端记录的本次支付交易金额以及信用授权数据可以存储于 POS 机本地，如果 POS 机包括计算机等处理设备，则可以存储于该计算机的磁盘中，或者还可以存储于其它可靠的存储器中（例如通过网络方式的备份存储等）。

其中，记录的信用授权数据可以为前述信用授权数据的全量信息，也可以为用户信

息，在前述扣费客户端的处理步骤中并没有对加密后的用户信息进行解密，在记录时可以只记录依然为加密的用户信息，从而可以进一步保证用户信息的安全性。

在所述扣款记录中，还可以存储包括商户信息等内容，例如商户的 ID、支付交易的类型、商品信息等等。

至此，用户的本次支付交易完成，如果 POS 机对应的是交通工具闸口，则可以开闸放行，如果是消费，则可以告知商户本次支付完成，此时，用户的金融账户并未产生变化，只是信用支付，并且商户的 POS 机也并未与远端服务器进行通信以完成本次支付交易的扣款，因此极大的缩短了用户通过手机与 POS 机之间的支付交易时间，提高了用户支付效率。

步骤 1410，在预定时间 POS 机将所述扣款记录发送给远端服务器进行核对。

在一个时间段内 POS 机可能记录了多条扣款记录，该 POS 机每次与远端服务器进行对账时都传送多条扣款记录，所述预定时间在本例中可以为每天的 0 点，此时为该 POS 机的空闲时间，POS 机将所述扣款记录通过网络的方式（有线网络或者无线网络）发送给远端服务器，在该扣款记录中如上一步骤所述，包括用户信息和支付金额，远端服务器解密所述用户信息，获得用户身份标识和银行卡账号，对该银行卡账号扣除所述支付金额，从而才真正的完成了用户支付的流程。

如图 15 所示为本申请实施例另一种离线信用支付的具体方法流程图，本图的实施例与图 14 所示实施例不同点在于手机上的信用支付客户端不是生成二维码，而是通过 NFC（近场通信）通信模块将信用授权数据发送给 POS 机，在本实施例中的 POS 机上也相应的具有 NFC 通信模块用以获得手机传送过来的信用授权数据，并且该 POS 机还具有 USB 接口，可以将扣款记录通过该 USB 接口存储于移动存储器中。

与图 14 实施例中相同或者相类似的步骤在本实施例中不再赘述，只描述不同点。

步骤 1505，智能终端的信用支付客户端将信用授权数据存储于本地存储器中，以供 NFC 通信模块访问。

作为可选的实施例，不用每次信用支付均由智能终端端获取信用授权数据，而是由远端服务器生成一个信用授权数据后，存储于智能终端的信用支付客户端中，以供多次信用支付所使用。

步骤 1506，POS 机的扣费客户端通过 NFC 通信模块与智能终端的 NFC 通信模块通信，获取信用支付客户端的信用授权数据。

步骤 1507，扣费客户端解析通过 NFC 通信模块获得的信用授权数据。

具体可以通过得自远端服务器发送的公钥对接收到的信用授权数据进行验签后，解密得到信用授权数据。

步骤 1508，扣费客户端利用信用授权数据对本次支付交易进行处理。

作为可选的实施例，在本步骤中，扣费客户端针对信用授权数据中的信用额度进行判断，如果信用额度满足本次消费，则将信用额度减去本次消费，将剩余信用额度通过 NFC 通信模块返回给手机，手机中的信用支付客户端会将本地保存的信用授权数据中的信用额度进行修改，改为剩余信用额度，以备下次信用支付时作为新的信用额度进行使用。

当然，在信用授权数据中的时间信息可以被删除或者为一个较长的时间，以使得该信用授权数据可以在多次信用支付中使用。

步骤 1509，扣费客户端通过 USB 接口将本次扣款记录记录于移动硬盘。

所述扣款记录中包括本次支付交易的金额以及信用授权数据。

步骤 1510，在预定时间 POS 机将所述扣款记录发送给远端服务器进行核对。

通过上述本申请实施例中的方法及系统，在用户不使用银行卡的情况下，扣费终端不联网就可以快速的完成交易扣费，并且每次交易生成的信用授权数据都是临时生成的，不具有重复利用的可能，解决了现有技术中磁条类银行卡的信息泄露，而造成用户经济损失的问题。

对于一个技术的改进可以很明显地区分是硬件上的改进（例如，对二极管、晶体管、开关等电路结构的改进）还是软件上的改进（对于方法流程的改进）。然而，随着技术的发展，当今的很多方法流程的改进已经可以视为硬件电路结构的直接改进。设计人员几乎都通过将改进的方法流程编程到硬件电路中来得到相应的硬件电路结构。因此，不能说一个方法流程的改进就不能用硬件实体模块来实现。例如，可编程逻辑器件（Programmable Logic Device, PLD）（例如现场可编程门阵列（Field Programmable Gate Array，FPGA））就是这样一种集成电路，其逻辑功能由用户对器件编程来确定。由设计人员自行编程来把一个数字系统“集成”在一片 PLD 上，而不需要请芯片制造厂商来设计和制作专用的集成电路芯片 2。而且，如今，取代手工地制作集成电路芯片，这种编程也多半改用 “逻辑编译器（logic compiler）”软件来实现，它与程序开发撰写时所用的软件编译器相类似，而要编译之前的原始代码也得用特定的编程语言来撰写，此称之为硬件描述语言（Hardware Description Language，HDL），而 HDL 也并非仅有一种，而是有许多种，如 ABEL（Advanced Boolean Expression Language）、AHDL（Altera

Hardware Description Language）、Confluence、CUPL（Cornell University Programming Language）、HDCal、JHDL（Java Hardware Description Language）、Lava、Lola、MyHDL、PALASM、RHDL（Ruby Hardware Description Language）等，目前最普遍使用的是 VHDL（Very-High-Speed Integrated Circuit Hardware Description Language ） 与 Verilog2。本领域技术人员也应该清楚，只需要将方法流程用上述几种硬件描述语言稍作逻辑编程并编程到集成电路中，就可以很容易得到实现该逻辑方法流程的硬件电路。

控制器可以按任何适当的方式实现，例如，控制器可以采取例如微处理器或处理器以及存储可由该（微）处理器执行的计算机可读程序代码（例如软件或固件）的计算机可读介质、逻辑门、开关、专用集成电路（Application Specific Integrated Circuit，ASIC）、可编程逻辑控制器和嵌入微控制器的形式，控制器的例子包括但不限于以下微控制器：ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20 以及 Silicone Labs C8051F320，存储器控制器还可以被实现为存储器的控制逻辑的一部分。

本领域技术人员也知道，除了以纯计算机可读程序代码方式实现控制器以外，完全可以通过将方法步骤进行逻辑编程来使得控制器以逻辑门、开关、专用集成电路、可编程逻辑控制器和嵌入微控制器等的形式来实现相同功能。因此这种控制器可以被认为是一种硬件部件，而对其内包括的用于实现各种功能的装置也可以视为硬件部件内的结构。或者甚至，可以将用于实现各种功能的装置视为既可以是实现方法的软件模块又可以是硬件部件内的结构。

上述实施例阐明的系统、装置、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。

为了描述的方便，描述以上装置时以功能分为各种单元分别描述。当然，在实施本申请时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

通过以上的实施方式的描述可知，本领域的技术人员可以清楚地了解到本申请可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在存储介质中，如 ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本申请各个实施例或者实施例的某些部分所述的方法。

本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于系统

实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

本申请可用于众多通用或专用的计算机系统环境或配置中。例如：个人计算机、服务器计算机、手持设备或便携式设备、平板型设备、多处理器系统、基于微处理器的系统、置顶盒、可编程的消费电子设备、网络 PC、小型计算机、大型计算机、包括以上任何系统或设备的分布式计算环境等等。

本申请可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本申请，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

虽然通过实施例描绘了本申请，本领域普通技术人员知道，本申请有许多变形和变化而不脱离本申请的精神，希望所附的权利要求包括这些变形和变化而不脱离本申请的精神。