(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 106228349 B
(45)授权公告日 2021.01.15

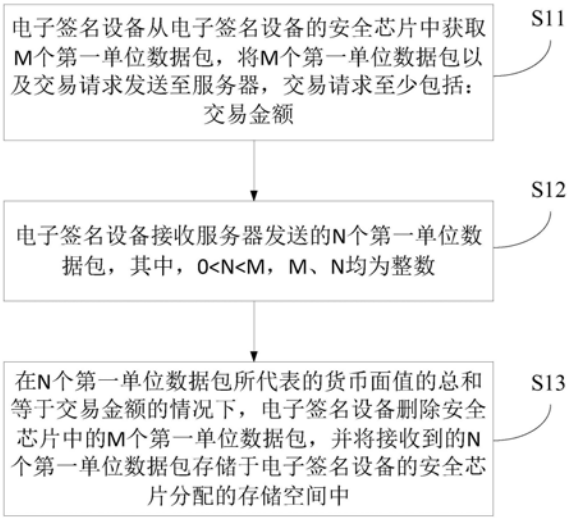
(21)申请号 201610584717.4
(22)申请日 2016.07.22
(65)同一申请的已公布的文献号
申请公布号 CN 106228349 A
(43)申请公布日 2016.12.14
(73)专利权人 天地融科技股份有限公司
地址 100083 北京市海淀区学清路38号B座1810
(72)发明人 李东声
(51)Int.Cl.
G06Q 20/08(2012.01)
G06Q 20/30(2012.01)
G06Q 20/40(2012.01)
(56)对比文件
CN 105913255 A,2016.08.31
审查员 王胜丹
权利要求书2页 说明书20页 附图1页

(54)发明名称

一种电子签名设备的交易方法和电子签名设备

(57)摘要

本发明提供了一种电子签名设备的交易方法及电子签名设备，该方法包括：电子签名设备从电子签名设备的安全芯片中获取M个第一单位数据包，将M个第一单位数据包以及交易请求发送至服务器，交易请求至少包括：交易金额，其中，每个第一单位数据包代表多种货币面值中的一种货币面值，M个第一单位数据包所代表的货币面值的总和等于交易金额；电子签名设备接收服务器发送的N个第一单位数据包，其中，0<N<M，M、N均为整数；在N个第一单位数据包所代表的货币面值的总和等于交易金额的情况下，电子签名设备删除安全芯片中的M个第一单位数据包，并将接收到的N个第一单位数据包存储于电子签名设备的安全芯片分配的存储空间中。



CN 106228349 B

1.一种电子签名设备的交易方法,其特征在于,包括:

电子签名设备从所述电子签名设备的安全芯片中获取M个第一单位数据包,将所述M个第一单位数据包以及交易请求发送至服务器,所述交易请求至少包括:交易金额,其中,每个所述第一单位数据包代表多种货币面值中的一种货币面值,所述M个第一单位数据包所代表的货币面值的总和等于所述交易金额;

所述电子签名设备接收所述服务器发送的N个第一单位数据包,其中,0<N<M,M、N均为整数;

在所述N个第一单位数据包所代表的货币面值的总和等于所述交易金额的情况下,所述电子签名设备删除所述安全芯片中的所述M个第一单位数据包,并将接收到的所述N个第一单位数据包存储于所述电子签名设备的安全芯片分配的存储空间中;

所述电子签名设备将所述M个第一单位数据包发送至所述服务器,包括:

所述电子签名设备对所述M个第一单位数据包进行加密,得到M个第二单位数据包,并用所述M个第二单位数据包覆盖所述安全芯片中存储的所述M个第一单位数据包,将所述M个第二单位数据包发送至服务器;

所述电子签名设备删除所述安全芯片中的所述M个第一单位数据包,包括:

所述电子签名设备删除所述安全芯片中的所述M个第二单位数据包。

2.根据权利要求1所述的交易方法,其特征在于,

在所述电子签名设备从所述电子签名设备的安全芯片中获取M个第一单位数据包之前,所述方法还包括:

所述电子签名设备接收到释放所述安全芯片的存储空间的触发指令,或者,所述电子签名设备检测到所述安全芯片中当前存储的第一单位数据包的总个数达到预设数值。

3.根据权利要求1或2所述的交易方法,其特征在于,

所述第一单位数据包至少包括:第一单位数据,所述第一单位数据至少包括:货币面值数据,或者,货币序号和货币面值数据;

所述第一单位数据包至少还包括以下之一:发行银行标识和银行证书序号。

4.根据权利要求3所述的交易方法,其特征在于,

所述电子签名设备对所述M个第一单位数据包进行加密,包括:

所述电子签名设备利用所述服务器的公钥至少对所述M个第一单位数据包中的每个第一单位数据包中的所述第一单位数据进行加密。

5.根据权利要求3所述的交易方法,其特征在于,

所述电子签名设备对所述M个第一单位数据包进行加密,包括:

所述电子签名设备利用对称密钥至少对所述M个第一单位数据包中的每个第一单位数据包中的所述第一单位数据进行加密;

在所述电子签名设备对所述M个第一单位数据包进行加密之后,所述方法还包括:

删除所述对称密钥。

6.一种电子签名设备,其特征在于,所述电子签名设备包括:

安全模块,用于获取自身存储的M个第一单位数据包;

通信模块,用于将所述M个第一单位数据包以及交易请求发送至服务器,所述交易请求包括:交易金额,其中,每个第一单位数据包代表多种货币面值中的一种货币面值,所述M个

第一单位数据包所代表的货币面值的总和等于所述交易金额；

获取模块，用于接收所述服务器发送的N个第一单位数据包，其中，0<N<M，M、N均为整数；

所述安全模块，还用于在所述N个第一单位数据包所代表的货币面值的总和等于所述交易金额的情况下，删除所述自身存储的M个第一单位数据包，并将接收到的所述N个第一单位数据包存储于所述安全模块分配的存储空间中；

所述安全模块，还用于对所述M个第一单位数据包进行加密，得到M个第二单位数据包，并用所述M个第二单位数据包覆盖自身存储的所述M个第一单位数据包；

所述通信模块，还用于将所述M个第二单位数据包发送至所述服务器；

所述安全模块，还用于删除所述自身存储的M个第一单位数据包，包括：

所述安全模块，还用于删除所述M个第二单位数据包。

7.根据权利要求6所述的电子签名设备，其特征在于，

所述安全模块，还用于在获取自身存储的M个第一单位数据包之前，接收到释放其存储空间的触发指令；或者，还用于在获取自身存储的M个第一单位数据包之前，检测到自身当前存储的第一单位数据包的总个数达到预设数值。

8.根据权利要求6或7所述的电子签名设备，其特征在于，

所述第一单位数据包括至少包括：第一单位数据，所述第一单位数据至少包括：货币面值数据，或者，货币序号和货币面值数据；

所述第一单位数据包至少还包括以下之一：发行银行标识和银行证书序号。

9.根据权利要求8所述的电子签名设备，其特征在于，

所述安全模块，还用于对所述M个第一单位数据包进行加密，包括：

所述安全模块，还用于利用所述服务器的公钥至少对所述M个第一单位数据包中的每个第一单位数据包中的所述第一单位数据进行加密。

10.根据权利要求8所述的电子签名设备，其特征在于，

所述安全模块，还用于对所述M个第一单位数据包进行加密，包括：所述安全模块利用对称密钥至少对所述M个第一单位数据包中的每个第一单位数据包中的所述第一单位数据进行加密；

所述安全模块，还用于在对所述M个第一单位数据包进行加密之后，删除所述对称密钥。

一种电子签名设备的交易方法和电子签名设备

技术领域

[0001] 本发明涉及一种电子技术领域，尤其涉及一种电子签名设备的交易方法和电子签名设备。

背景技术

[0002] 现有的电子交易中，用户的资金以数字的形式存在账户中，例如：用户持有100元的资金，该资金以数字的形式存储于银行服务器的用户账户中，当用户消费了10元以后，银行服务器需要将用户账户中的资金100改写为90，以完成账户的清算。为了保证资金数值的安全，在银行服务器改写数值后，要对改写后的资金数值90进行签名。因为用户每次进行交易后账户中的金额数值都会发生变动，所以银行服务器要针对每次变动后的数值进行处理。也就是说，现有的电子交易要依托于银行服务器，用户进行的电子交易需要与银行服务器进行实时同步，不能实现在不联网的情况下独立完成多笔线下交易。

发明内容

[0003] 本发明旨在至少解决上述问题之一。

[0004] 本发明的主要目的在于提供一种电子签名设备的交易方法。

[0005] 本发明的另一目的在于提供一种电子签名设备。

[0006] 为达到上述目的，本发明的技术方案具体是这样实现的：

[0007] 本发明一方面提供了一种电子签名设备的交易方法，包括：电子签名设备从电子签名设备的安全芯片中获取M个第一单位数据包，将M个第一单位数据包以及交易请求发送至服务器，交易请求至少包括：交易金额，其中，每个第一单位数据包代表多种货币面值中的一种货币面值，M个第一单位数据包所代表的货币面值的总和等于交易金额；电子签名设备接收服务器发送的N个第一单位数据包，其中，0<N<M，M、N均为整数；在N个第一单位数据包所代表的货币面值的总和等于交易金额的情况下，电子签名设备删除安全芯片中的M个第一单位数据包，并将接收到的N个第一单位数据包存储于电子签名设备的安全芯片分配的存储空间中。

[0008] 此外，在电子签名设备从电子签名设备的安全芯片中获取M个第一单位数据包之前，方法还包括：电子签名设备接收到释放安全芯片的存储空间的触发指令，或者，电子签名设备检测到安全芯片中当前存储的第一单位数据包的总个数达到预设数值。

[0009] 此外，电子签名设备将M个第一单位数据包发送至服务器，包括：电子签名设备对M个第一单位数据包进行加密，得到M个第二单位数据包，并用M个第二单位数据包覆盖安全芯片中存储的M个第一单位数据包，将M个第二单位数据包发送至服务器；电子签名设备删除安全芯片中的M个第一单位数据包，包括：电子签名设备删除安全芯片中的M个第二单位数据包。

[0010] 此外，第一单位数据包至少包括：第一单位数据，第一单位数据至少包括：货币面值数据，或者，货币序号和货币面值数据；第一单位数据包至少还包括以下之一：发行银行

标识和银行证书序号。

[0011] 此外，电子签名设备对M个第一单位数据包进行加密，包括：电子签名设备利用服务器的公钥至少对M个第一单位数据包中的每个第一单位数据包中的第一单位数据进行加密。

[0012] 此外，电子签名设备对M个第一单位数据包进行加密，包括：电子签名设备利用对称密钥至少对M个第一单位数据包中的每个第一单位数据包中的第一单位数据进行加密；在电子签名设备对M个第一单位数据包进行加密之后，方法还包括：删除对称密钥。

[0013] 本发明另一方面提供了一种电子签名设备，包括：安全模块，用于获取自身存储的M个第一单位数据包；通信模块，用于将M个第一单位数据包以及交易请求发送至服务器，交易请求包括：交易金额，其中，每个第一单位数据包代表多种货币面值中的一种货币面值，M个第一单位数据包所代表的货币面值的总和等于交易金额；获取模块，用于接收服务器发送的N个第一单位数据包，其中，0<N<M，M、N均为整数；安全模块，还用于在N个第一单位数据包所代表的货币面值的总和等于交易金额的情况下，删除自身存储的M个第一单位数据包，并将接收到的N个第一单位数据包存储于安全模块分配的存储空间中。

[0014] 此外，安全模块，还用于在获取自身存储的M个第一单位数据包之前，接收到释放其存储空间的触发指令；或者，还用于在获取自身存储的M个第一单位数据包之前，检测到自身当前存储的第一单位数据包的总个数达到预设数值。

[0015] 此外，安全模块，还用于对M个第一单位数据包进行加密，得到M个第二单位数据包，并用M个第二单位数据包覆盖自身存储的M个第一单位数据包；通信模块，还用于将M个第二单位数据包发送至服务器；安全模块，还用于删除自身存储的M个第一单位数据包，包括：安全模块，还用于删除M个第二单位数据包。

[0016] 此外，第一单位数据包括至少包括：第一单位数据，第一单位数据至少包括：货币面值数据，或者，货币序号和货币面值数据；第一单位数据包至少还包括以下之一：发行银行标识和银行证书序号。

[0017] 此外，安全模块，还用于对M个第一单位数据包进行加密，包括：安全模块，还用于利用服务器的公钥至少对M个第一单位数据包中的每个第一单位数据包中的第一单位数据进行加密。

[0018] 此外，安全模块，还用于对M个第一单位数据包进行加密，包括：安全模块利用对称密钥至少对M个第一单位数据包中的每个第一单位数据包中的第一单位数据进行加密；安全模块，还用于在对M个第一单位数据包进行加密之后，删除对称密钥。

[0019] 由上述本发明提供的技术方案可以看出，本发明提供了一种电子签名设备的交易方法和电子签名设备。在电子签名设备使用第一单位数据包进行交易时，由于每个第一单位数据包都会占用电子签名设备的安全芯片中的一定存储空间，因此安全芯片的存储空间可能会被占满，从而使电子签名设备不能进行后续的交易。采用本实施例提供的技术方案，在接收到释放存储空间的触发指令或者安全芯片中当前存储的第一单位数据包的总个数达到预设数值时，电子签名设备可以将自身存储的M个小面值的第一单位数据包发送给服务器，向服务器兑换货币面值总和相同的N个大面值的第一单位数据包，由此，可以使安全芯片释放出M-N个第一单位数据包所占用的存储空间，从而保障电子签名设备有足够的存储空间以支持后续的交易能够顺序进行。此外，在使用时，电子签名设备可以通过将这些第

一单位数据包发送至对端电子签名设备来完成付款操作，而无需联网至后台服务器才能完成付款，从而使电子签名设备具有离线交易的功能。

附图说明

[0020] 为了更清楚地说明本发明实施例的技术方案，下面将对实施例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发明的一些实施例，对于本领域的普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他附图。

[0021] 图1为本发明实施例1提供的电子签名设备的交易方法的流程图；

[0022] 图2为本发明实施例2提供的电子签名设备的结构示意图。

具体实施方式

[0023] 下面结合本发明实施例中的附图，对本发明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发明一部分实施例，而不是全部的实施例。基于本发明的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明的保护范围。

[0024] 在本发明的描述中，需要理解的是，术语“中心”、“纵向”、“横向”、“上”、“下”、“前”、“后”、“左”、“右”、“竖直”、“水平”、“顶”、“底”、“内”、“外”等指示的方位或位置关系为基于附图所示的方位或位置关系，仅是为了便于描述本发明和简化描述，而不是指示或暗示所指的装置或元件必须具有特定的方位、以特定的方位构造和操作，因此不能理解为对本发明的限制。此外，术语“第一”、“第二”仅用于描述目的，而不能理解为指示或暗示相对重要性或数量或位置。

[0025] 在本发明的描述中，需要说明的是，除非另有明确的规定和限定，术语“安装”、“相连”、“连接”应做广义理解，例如，可以是固定连接，也可以是可拆卸连接，或一体地连接；可以是机械连接，也可以是电连接；可以是直接相连，也可以通过中间媒介间接相连，可以是两个元件内部的连通。对于本领域的普通技术人员而言，可以具体情况理解上述术语在本发明中的具体含义。

[0026] 下面将结合附图对本发明实施例作进一步地详细描述。

[0027] 实施例1

[0028] 图1为本实施例提供的一种电子签名设备的交易方法的流程图，图1所示的方法实施例，包括以下步骤S11至S13：

[0029] 步骤S11，电子签名设备从其安全芯片中获取M个第一单位数据包，将M个第一单位数据包以及交易请求发送至服务器，交易请求至少包括：交易金额。

[0030] 其中，每个第一单位数据包代表多种货币面值中的一种货币面值，M个第一单位数据包所代表的货币面值的总和等于交易金额；

[0031] 在本实施例中，电子签名设备为具有签名功能的电子设备，例如，具有签名功能的智能卡(公交卡、银行卡、购物卡等等)、工行的U盾等等。在本实施例一种可选的实施方式中，电子签名设备中设置有安全芯片，该安全芯片内部拥有独立的处理器和存储单元，可存储PKI数字证书和密钥，以及其他特征数据，对数据进行加解密运算，为用户提供数据加密

和身份安全认证服务，本实施例中，电子签名设备可以将从服务器(如银行服务器或商场购物充值服务器等第三方服务器)或者从其他电子签名设备接收到的第一单位数据包存储于安全芯片中，由于安全芯片的存储单元内的数据不能被非法读出，由此可以保证存储单元中存储数据的安全性。

[0032] 本实施例中，每个第一单位数据包代表多种货币面值中的一种货币面值，例如，第一单位数据包所代表的货币面值包括：1元、2元、5元、10元、20元、50元和100元，当然，如果未来国家发行了新的货币面值、或者除了使用人民币之外的其他地区、国家的货币面值也属于本发明的保护范围，本实施例中仅以人民币面值进行举例说明。货币面值共有多种，当电子签名设备从其安全芯片中获取多个第一单位数据包时(即M>1时)，多个第一单位数据包可以代表多种不同的货币面值，例如，当M＝3时，第一单位数据包的个数为3个，3个第一单位数据包分别代表货币面值1元、2元以及5元；或者，多个第一单位数据包可以代表相同的货币面值，例如，当M＝3时，3个第一单位数据包均代表货币面值1元；再或者，多个第一单位数据包所代表的货币面值中既包括相同的也包括不相同的货币面值，例如，当M＝3时，3个第一单位数据包分别代表货币面值1元、1元以及2元。由此，电子签名设备从其安全芯片中获取的M个第一单位数据包所代表的货币面值具有灵活的组合方式。

[0033] 在本实施例一种可选的实施方式中，第一单位数据包中至少包括第一单位数据，该第一单位数据至少包括：货币面值数据，或者，货币序号和货币面值数据。其中，货币面值数据为第一单位数据包所代表的货币面值，以此来标识第一单位数据包所代表的货币面值，货币序号为每个第一单位数据包的唯一序号，即不同的第一单位数据包中的货币序号是不同的。由此，能够保证每个第一单位数据包的唯一性，以便于辨认第一单位数据包的真伪。作为一种可选的实施方式，第一单位数据包至少还包括以下之一：发行银行标识和银行证书序号。其中，发行银行标识为发行该第一单位数据包的银行的标识信息，由此可以根据该标识查询到对应的发行银行的相关信息，而且，电子签名设备可以根据发行银行标识和银行证书序号获取对应的发行银行的银行证书，银行证书中包含有发行银行的公钥，以便于后续步骤中电子签名设备利用发行银行的公钥对第一单位数据的签名完成验证。

[0034] 在本实施例一种可选的实施方式中，电子签名设备自身存储的第一单位数据包至少还包括：第一单位数据以及服务器对第一单位数据签名得到的第一签名数据。作为一种可选的实施方式，服务器(如银行服务器或商场购物充值服务器等第三方服务器)利用自身的私钥分别对每个第一单位数据包中的第一单位数据进行签名，得到与每个第一单位数据包对应的第一签名数据。服务器将至少一个携带有第一签名数据的第一单位数据包发送至电子签名设备，在本实施例中，电子签名设备的安全芯片在存储服务器发送的多个第一单位数据包之前，可以利用服务器的公钥验证第一单位数据包的真实性，在验证通过后，才存储，因此，安全芯片中存储的第一单位数据包均真实且安全。

[0035] 在本实施例另一种可选的实施方式中，电子签名设备发送给服务器的交易请求中还包括：电子签名设备的设备标识；电子签名设备自身存储的第一单位数据包至少包括：第一单位数据、服务器对第一单位数据和电子签名设备的设备标识签名得到的第二签名数据。作为一种可选的实施方式，服务器利用自身的私钥对第一单位数据和电子签名设备的设备标识签名，得到与第一单位数据包对应的第二签名数据。服务器将至少一个携带有第二签名数据的第一单位数据包发送至电子签名设备，以便电子签名设备在接收到服务器发

送的第一单位数据包后，对第一单位数据包中的第二签名数据验签，如果验签通过，则该第一单位数据包是真实的，且该第一单位数据包是发送给此电子签名设备的。

[0036] 由于第一单位数据包存储在电子签名设备的安全芯片中，且每个第一单位数据包都需要占用一定的存储空间，因此，安全芯片剩余的存储空间不足时，则无法再存储新的第一单位数据包，从而使电子签名设备无法再进行后续的交易。因此，本实施例中，在步骤S11之前，该方法还可以包括：电子签名设备接收到释放所述安全芯片的存储空间的触发指令，或者，电子签名设备检测到安全芯片中当前存储的第一单位数据包的总个数达到预设数值。作为一种可选的实施方式，在电子签名设备接收到用户输入的释放安全芯片的存储空间的触发指令后，电子签名设备执行步骤S11。其中，用户可以通过键盘、语音等方式输入触发指令，用户输入的触发指令可以包括交易金额，电子签名设备可以根据交易金额随机或者按照预设的规则从其安全芯片中获取M个第一单位数据包，该M个第一单位数据包所代表的货币面值总和等于交易金额，在该可选方式中M的数值是随机确定的，但为了释放最大的空间，电子签名设备可以选择M为所代表的货币面值总和等于交易金额的最大值，例如，存在10个1元数据包和2个5元数据包时，电子签名设备选择10个1元数据包，M等于10，需要说明的是，在该可选实施方式中，无论第一单位数据包所代表的货币面值是否相同，每个第一单位数据包所占的存储空间的大小是相同的。作为另一种可选的实施方式，在电子签名设备检测到安全芯片当前存储的第一单位数据包的总个数达到预设数值M后，电子签名设备执行步骤S11。其中，该预设数值M可以是用户设定的，也可以是在电子签名设备出厂时预先设定的，电子签名设备从其安全芯片中获取M个第一单位数据包，并计算M个第一单位数据包所代表的货币面值总和，将该货币面值总和作为交易金额，电子签名设备将M个第一单位数据包和交易金额发送至服务器。可选地，达到预设数值的第一单位数据包占用安全芯片的一半存储空间，也就是说，每当安全芯片的存储空间的一半被占用时，就会触发步骤S11。由此，电子签名设备可以在存储空间不足时，触发释放存储空间的步骤(S11-S13)，通过与服务器进行的数据包交换，来达到释放存储空间的目的，从而保证电子签名设备的安全芯片保持有足够的存储空间。

[0037] 在本实施例一种可选的实施方式中，电子签名设备可以与外接设备(如PC或移动终端等)建立连接，通过该外接设备将M个第一单位数据包以及交易请求发送至服务器。或者，电子签名设备具有有线接口或无线接口，与服务器建立有线连接或无线连接，直接将M个第一单位数据包和交易请求发送至服务器。其中，无线连接方式可以包括蓝牙、NFC近场通讯以及WIFI等方式。由此，本实施例中电子签名设备可以通过多种方式将交易请求发送至服务器。作为一种可选的实施方式，服务器包括银行服务器或第三方服务器，例如，第三方服务器可以是某商场的购物卡储值服务器。

[0038] 步骤S12，电子签名设备接收服务器发送的N个第一单位数据包，其中，0<N<M，M、N均为整数。

[0039] 在本步骤中，同样的，N个第一单位数据包中的每个第一单位数据包代表多种货币面值中的一种货币面值，其中，第一单位数据包中至少包括第一单位数据，该第一单位数据至少包括：货币面值数据，或者，货币序号和货币面值数据。对于该第一单位数据的描述具体可以参照步骤S11中的描述，此处不再赘述。作为一种可选的实施方式，N个第一数据包中的每个第一单位数据包至少还包括：服务器对第一单位数据签名得到的第一签名数据。由

此,电子签名设备可以通过验证第一签名数据来确定接收到的N个第一单位数据包是否是真实的,具体的验证方式可以参见以下步骤S13中电子签名设备对第一签名数据进行验证的方式。作为另一种可选的实施方式,N个第一单位数据包中的每个第一单位数据包至少包括:服务器对第一单位数据和电子签名设备的设备标识签名得到的第二签名数据。由此,电子签名设备可以通过验证第二签名数据来确定接收到的N个第一单位数据包是否是真实的,以及是否是发给该电子签名设备的,具体的验证方式可以参见以下步骤S13中电子签名设备对第二签名数据进行验证的方式。

[0040] 本实施例中,每个第一单位数据包可以占用相同的存储空间(例如,每个第一单位数据包占用1M的存储空间)。电子签名设备发送至服务器的第一单位数据包的个数M大于服务器接收的第一单位数据包的个数N,例如,电子签名设备从安全芯片中获取100个货币面值为2元的第一单位数据包,该100个第一单位数据包所代表的货币面值总和为200元,即交易金额为200元,占用存储空间100M。服务器在接收到电子签名设备发送的第一单位数据包以及交易金额后,根据交易金额,向电子签名设备下发2个代表货币面值100的第一单位数据包(货币面值总和仍为200,占用空间2M)。由此,电子签名设备在保持货币面值不变的情况下,将100个第一单位数据包兑换成2个第一单位数据包,由此,电子签名设备的安全芯片可以释放出98M存储空间,即98个第一单位数据包所占用的存储空间。

[0041] 步骤S13,在N个第一单位数据包所代表的货币面值的总和等于交易金额的情况下,电子签名设备删除安全芯片中的M个第一单位数据包,并将接收到的N个第一单位数据包存储于电子签名设备的安全芯片分配的存储空间中。

[0042] 本实施例中,在N个第一单位数据包所代表的货币面值的总和等于交易金额的情况下,即服务器发送的第一单位电子货币数据包在传输过程中没有丢失的情况下,电子签名设备删除安全芯片中的M个第一单位数据包,并将接收到的N个第一单位数据包存储于电子签名设备的安全芯片分配的存储空间中。由此,电子签名设备可以将完成存储空间的释放。

[0043] 在本实施例中,为了进一步保证步骤S13中电子签名设备存储的第一单位数据包的真实性,作为本实施例中的一种可选实施方式,步骤S13中的电子签名设备将接收到的N个第一单位数据包存储于电子签名设备的安全芯片分配的存储空间中,具体包括:电子签名设备对第一签名数据进行验证,在验证通过后,电子签名设备将接收到的N个第一单位数据包存储于电子签名设备的安全芯片分配的存储空间中。其中,第一签名数据是服务器对第一单位数据进行签名得到的,因此,作为一种可选的实施方式,服务器发送至电子签名设备的第一单位数据包至少还包括:服务器对第一单位数据签名得到的第一签名数据,由此使得电子签名设备可以验证第一单位数据包的真实性。作为一种可选的实施方式,第一签名数据为服务器利用自身的私钥对第一单位数据进行签名得到的签名数据。相应的,电子签名设备对第一签名数据进行验证具体包括:电子签名设备利用该服务器的公钥对第一签名数据进行验签。以服务器为银行服务器为例,银行服务器对第一单位数据进行HASH运算得到第一单位数据的摘要报文A1,并利用银行服务器自身的私钥对该摘要报文A1进行签名运算得到第一签名数据,并携带在第一单位数据包中下发至电子签名设备。电子签名设备可以利用该银行服务器的公钥对第一签名数据进行验签,具体地,电子签名设备利用银行服务器的公钥对第一电子签名数据进行运算得到运算结果A2,并对接收到的第一单位数据

包中的第一单位数据进行HASH运算得到第一单位数据的摘要报文A3，将运算结果A2与摘要报文A3进行比对，如果比对结果一致，则电子签名设备对第一电子签名数据验签通过。其中，电子签名设备可以根据第一单位数据包中的银行证书序号和/或发行银行标识获取银行的公钥，例如，电子签名设备可以根据第一单位数据包中的发行银行标识，从与待验证的第一签名数据对应的发行银行服务器获取该银行的银行证书，并从银行证书中获取该银行的公钥；再例如，电子签名设备可以预存各个银行的银行证书，根据第一单位数据包中的银行证书序号从预存的各个银行证书中获取与待验证的第一签名数据对应的银行证书，并从对应的银行证书中获取银行的公钥。由此，电子签名设备利用银行的公钥对第一单位数据包中携带的第一签名数据进行验签，可以验证第一单位数据包的真实性。上述描述仅以服务器为银行服务器为例进行说明，但本实施例并不限于银行服务器，其他第三方服务器如超市购物卡储值服务器等的具体实施方式均属于本发明的保护范围之内。

[0044] 进一步地，电子签名设备在确保收到的第一单位数据包是真实的前提下，还想再确认服务器发送的对象是否确实为本电子签名设备，以避免存储服务器误发的数据包，步骤S13中的电子签名设备将接收到的N个第一单位数据包存储于电子签名设备的安全芯片分配的存储空间中，具体包括：电子签名设备对第二签名数据进行验证，在验证通过后，电子签名设备将接收到的N个第一单位数据包存储于电子签名设备的安全芯片分配的存储空间中。其中，第二签名数据是服务器对第一单位数据和电子签名设备的设备标识签名得到的，因此，在本实施例一种可选的实施方式中，电子签名设备发送给服务器的交易请求中还包括：电子签名设备的设备标识；服务器返回的N个第一单位数据包中的每个第一单位数据包至少还包括：服务器对第一单位数据和电子签名设备的设备标识签名得到的第二签名数据，由此使得电子签名设备可以验证第一单位数据包的真实性和正确性。作为一种可选的实施方式，第二签名数据为服务器利用服务器自身的私钥对第一单位数据和电子签名设备的设备标识进行签名得到的签名数据，也就是说，每个第二签名数据的签名对象为每个第一单位数据和电子签名设备的设备标识的组合。相应的，电子签名设备对第二签名数据进行验证具体包括：电子签名设备利用服务器的公钥分别对每个第二签名数据进行验签。以服务器为银行服务器为例，银行服务器利用自身的私钥对第一单位数据和电子签名设备的设备标识进行签名得到第二签名数据，并携带在第一单位数据包中下发至电子签名设备。电子签名设备可以利用该银行服务器的公钥对第二签名数据进行验签。其中，电子签名设备可以根据第一单位数据包中的银行证书序号和/或发行银行标识获取该银行的银行证书，并从银行证书中获取该银行的公钥，例如，电子签名设备可以根据第一单位数据中的发行银行标识，从与待验证的第二签名数据对应的发行银行服务器获取该银行的公钥；再例如，电子签名设备可以预存各个银行的银行证书，根据第一单位数据包中的银行证书序号从预存的各个银行证书中获取与待验证的第二签名数据对应的银行证书，并从对应的银行证书中获取银行的公钥。由此，电子签名设备利用银行的公钥对第一单位数据包中携带的第二签名数据进行验签，不仅可以验证第一单位数据包的真实性，还可以证明第一单位数据包确实是银行服务器下发给该电子签名设备的，即验证第一单位数据包的正确性。上述描述仅以服务器为银行服务器为例进行说明，但本实施例并不限于银行服务器，其他第三方服务器如超市购物卡储值服务器等的具体实施方式均属于本发明的保护范围之内。

[0045] 在数据传输的过程中，可能会出现第一单位数据包丢失的情况，当第一单位数据

包在传输过程中丢失，那么电子签名设备接收到的N个第一单位数据包所代表的货币面值的总和小于所述交易金额。本实施例一种可选的实施方式中，在N个第一单位数据包所代表的货币面值的总和不等于交易金额(即大于或小于交易金额)的情况下，该方法还可以包括：电子签名设备删除安全芯片中的M个第一单位数据包，并将接收到的N个第一单位数据包存储于电子签名设备的安全芯片分配的存储空间中；电子签名设备向服务器发送重发请求；电子签名设备接收服务器根据重发请求发送的重发信息，重发信息包括：重发的X个第一单位数据包，其中，X个第一单位数据包所代表的货币面值的总和等于交易金额，或者，X个第一单位数据包所代表的货币面值的总和加上N个第一单位数据包所代表的货币面值的总和等于交易金额；电子签名设备将接收到的X个第一单位数据包存储于电子签名设备的安全芯片分配的存储空间中。具体地，在电子签名设备向服务器发送重发请求后，电子签名设备会接收到服务器返回的重发信息，根据重发请求的内容不同，服务器返回的重发信息也会不同，例如，重发请求中可以携带电子签名设备的设备标识、交易记录(如每笔交易的编号、账户信息、时间戳、交易金额以及接收到的第一单位数据包的个数以及所代表的货币面值等等，这些服务器侧也会对应记录)，以便于服务器查询到该电子签名设备对应的某一笔交易，全部重发该笔交易对应的第一单位数据包至电子签名设备，又例如，重发请求中还可以携带接收到的第一单位数据包的数据包标识(可以唯一标识一个第一单位数据包的标识，如服务器为每个第一单位数据包配置的唯一标识，或者货币序号)，服务器接收到这些数据包标识后，可以查询到漏发或传输过程中丢失了哪些第一单位数据包，将这些漏发的或传输过程中丢失的第一单位数据包发送至电子签名设备。下面就服务器重发第一单位电子数据包进行示例性说明：

[0046] 例如，作为一种可选的实施方式，电子签名设备接收服务器根据重发请求发送的重发信息，其中，该重发请求中至少包括：电子签名设备的设备标识以及交易记录，重发信息包括X个第一单位数据包，X个第一单位数据包所代表的货币面值的总和等于交易金额，即在该可选的实施方式中，服务器向电子签名设备重发了一笔交易对应的全部第一单位数据包，在本实施例中，服务器在与单位电子签名设备进行交易时，也会存储每一笔交易对应的交易记录(如每笔交易的编号、账户信息、时间戳、交易金额以及发送的第一单位数据包的个数以及所代表的货币面值等等)以及电子签名设备的设备标识，根据设备标识以及交易记录可以查询到该电子签名设备对应的某一笔交易，在该可选实施方式中，服务器会将查询到的电子签名设备请求重发的该笔交易的第一单位数据包全部重发给电子签名设备，以保证电子签名设备收到完整的第一单位数据包，服务器与电子签名设备的交易无误(即空间释放操作无误)。在该可选的实施方式中，电子签名设备接收到服务器重发的X个第一单位数据包后，判断该X个第一单位数据包中的每个第一单位数据包是否存在与之前存储的N个第一单位数据包相同的第一单位数据包，具体地，电子签名设备将X个第一单位数据包中的第一个第一单位数据包a依次与自身存储的每个第一单位数据包进行比较，如果自身存储的第一单位数据包中存在与第一单位数据包a相同的第一单位数据包，则跳过该第一单位数据包a，或者将之前存储的与第一单位数据包a相同的第一单位数据包删除，重新存储该第一单位数据包a；在完成对第一个第一单位数据包a的判断之后，电子签名设备继续逐一对X个第一单位数据包中的第二个第一单位数据包b、第三个第一单位数据包c……最后一个第一单位数据包x进行判断。由此，电子签名设备可以将服务器重发的X个第一单

位数据包存储在其安全芯片分配的存储空间中。

[0047] 举例来说，对于一笔编号为1*******的交易，电子签名设备的交易请求中的交易金额为10元，电子签名设备接收服务器发送的2个分别代表5元货币面值的第一单位数据包(2个第一单位数据包分别为数据包a和数据包b)，但由于传输过程中数据丢失，电子签名设备仅接收到1个代表5元货币面值的第一单位数据包(只接收到数据包a)，货币面值总和为5元，与交易金额10元不相等。针对该笔交易，电子签名设备将数据包a存储，并向服务器发送重发请求，并接收服务器根据重发请求发送的重发信息，该重发请求中包括：电子签名设备的设备标识以及交易记录，服务器在接收到该重发请求后，可以根据设备标识以及交易记录查询到该电子签名设备对应的该笔交易，服务器会将查询到的电子签名设备请求重发的该笔交易的第一单位数据包全部重发给电子签名设备，即服务器发送给电子签名设备的该重发信息包括数据包a和数据包b。电子签名设备判断重发的第一单位数据包中的数据包a与之前存储的数据包a相同，则跳过数据包a，只存储重发的数据包b，或者，将之前存储的数据包a删除，重新存储数据包a和数据包b。由此，当电子签名设备没有接收到一笔交易所需的全部第一单位数据包时，服务器可以将该笔交易所需的全部第一单位数据包重发给电子签名设备，从而使交易能够顺利完成。

[0048] 再例如，作为一种可选的实施方式，电子签名设备在向服务器发送重发请求后，电子签名设备接收服务器根据重发请求发送的重发信息，其中，该重发请求中至少包括：电子签名设备的设备标识、交易记录以及接收到的各个第一单位数据包的数据包标识，重发信息包括X个第一单位数据包，且该X个第一单位数据包所代表的货币面值的总和加上之前接收到的N个第一单位数据包所代表的货币面值的总和等于交易金额，即该X个第一单位数据包为电子签名设备未接收到的第一单位数据包，在该可选的实施方式中，服务器向电子签名设备重发了一笔交易中漏发的或传输过程中丢失的第一单位数据包，根据设备标识以及交易记录可以查询到该电子签名设备对应的某一笔交易，服务器会将查询到的该电子签名设备请求重发的该笔交易中没有查询到的数据包标识对应的那些第一单位数据包重发给电子签名设备，以保证电子签名设备收到完整的第一单位数据包，服务器与电子签名设备的交易无误(即空间释放操作无误)。与上一例中的可选实施方式相比，本可选实施方式可以减少服务器的数据传输量，大大降低服务器的工作负荷，提高服务器重发的工作效率。

[0049] 举例来说，对于一笔编号为1*******的交易，电子签名设备的交易请求中的交易金额为15元，电子签名设备接收服务器发送的1个代表5元货币面值的第一单位数据包(数据包c)，以及1个代表10元货币面值的第一单位数据包(数据包d)，但由于传输过程中数据丢失，电子签名设备仅接收到数据包c，货币面值总和为5元，与交易金额15元不相等。针对该笔交易，电子签名设备向服务器发送重发请求，并接收服务器根据重发请求发送的重发信息，在重发请求中还携带有数据包c的数据包标识，服务器接收到该重发请求后，针对该电子签名设备的该笔交易可以查询到其对应的所有第一单位数据包，便可以发现重发请求中没有数据包d的数据包标识，服务器可以将数据包d重发给电子签名设备。电子签名设备将服务器重发的数据包d存储于安全芯片中。本实施例中，电子签名设备向服务器发送的重发请求中可以包括已经被接收到的部分第一单位数据包的数据包标识，服务器可以根据重发请求中的数据包标识来确定重发信息中需要携带的第一单位数据包。由此，当电子签名设备没有接收到一笔交易所需的全部第一单位数据包时，服务器可以将未收到的部分第一

单位数据包重发给电子签名设备，不仅减少了重发数据的传输量，也保证了交易能够顺利完成。

[0050] 以上均是以一笔交易的实施方式为例进行说明的，在本实施例中，对于多笔交易中的每笔交易都可以按照上述方式来实现。

[0051] 本实施例中，为了防止电子签名设备非法重复使用同一个第一单位数据包，造成电子金融流通的混乱，保证同一个第一单位数据包在交易过程中的唯一性，步骤S11中电子签名设备将M个第一单位数据包发送至服务器，具体包括：电子签名设备对M个第一单位数据包进行加密，得到M个第二单位数据包，并用M个第二单位数据包覆盖安全芯片中存储的M个第一单位数据包，将M个第二单位数据包发送至服务器；步骤S13中电子签名设备删除安全芯片中的M个第一单位数据包，具体包括：电子签名设备删除安全芯片中的M个第二单位数据包。本实施例中，电子签名设备对M个第一单位数据包进行的加密操作为不可逆操作，即，电子签名设备可以加密第一单位数据包得到第二单位数据包，却不能从第二单位数据包解密得到第一单位数据包，因此，当得到的M个第二单位数据包覆盖了对应的M个第一单位数据包时，电子签名设备中仅仅存储了加密的第二单位数据包，由于其不能对第二单位数据包解密，所以无法恢复出第一单位数据包，也就不能再重复使用这些第一单位数据包，从而防止持有电子签名设备的用户重复使用这些第一单位数据包进行消费，造成第一单位数据包流通混乱。

[0052] 具体地，作为一种可选的实施方式，电子签名设备对M个第一单位数据包进行加密，具体包括：电子签名设备利用服务器的公钥至少对M个第一单位数据包中的每个第一单位数据包中的第一单位数据进行加密。作为另一种可选的实施方式，电子签名设备对M个第一单位数据包进行加密，具体包括：电子签名设备利用对称密钥至少对M个第一单位数据包中的每个第一单位数据包中的第一单位数据进行加密；在电子签名设备对M个第一单位数据包进行加密之后，该方法还包括：删除该对称密钥。

[0053] 对于后一种可选的实施方式，对称密钥可以由电子签名设备和服务器协商得到。可选地，对称密钥可以为与服务器关联的异或因子。电子签名设备利用对称密钥至少对M个第一单位数据包中的每个第一单位数据包中的第一单位数据进行加密，具体包括：电子签名设备利用异或因子至少对M个第一单位数据包中的每个第一单位数据包中的第一单位数据进行异或运算。异或运算也属于一种对称加密运算方式，但相比其他对称加密运算的方式，异或运算的速度较快，由此，可以提高电子签名设备对第一单位数据包进行加密生成第二单位数据包的效率。

[0054] 本实施例一种可选的实施方式中，在步骤S11之后，步骤S12之前，该方法还可以包括：电子签名设备接收服务器发送的重发请求；电子签名设备将M个第二单位数据包重新发送至服务器，或者，电子签名设备根据服务器发送的重发请求将服务器未接收到的第二单位数据包发送至服务器。具体地，服务器在接收到电子签名设备发送的第二单位数据包和交易请求后，计算接收到的第二单位数据包所代表的货币面值总和是否与交易请求中的交易金额相等，如果该货币面值总和小于交易金额，则说明在传输过程中有第二单位数据包遗失，此时，服务器将重发请求发送至电子签名设备。由此，电子签名设备可以通过重发第二单位数据包来保证服务器接收到所发送的全部第二数据包。

[0055] 本实施例中，至少可以通过使用对称密钥或者服务器的公钥对第一单位数据包进

行加密的方式，来防止电子签名设备非法重复使用同一个第一单位数据包，造成第一单位数据包流通的混乱，保证同一个第一单位数据包在交易过程中的唯一性。当然本实施例并不排除其他实施方式，只要可以达到相同的技术效果即可。在使用时，电子签名设备可以通过将这些第一单位数据包发送至对端电子签名设备来完成付款操作，而无需联网至后台服务器才能完成付款，从而使电子签名设备具有离线交易的功能。此外，需要说明的是，本实施例中第一单位数据包可以理解为包括：明文方式和密文方式的两种数据包，第二单位数据包可以理解为第一单位数据包的一种，即第一单位数据包加密后的数据包，即是第一单位数据包的密文形式。此外，第二单位数据包为密文，保证了传输数据的安全性，且即便被其他设备截获，也很难破解，进一步提高了第一单位数据包流通的安全性。

[0056] 在电子签名设备使用第一单位数据包进行交易时，由于每个第一单位数据包都会占用电子签名设备的安全芯片中的一定存储空间，因此安全芯片的存储空间可能会被占满，从而使电子签名设备不能进行后续的交易。采用本实施例提供的技术方案，在接收到释放存储空间的触发指令或者安全芯片中当前存储的第一单位数据包的总个数达到预设数值时，电子签名设备可以将自身存储的M个小面值的第一单位数据包发送给服务器，向服务器兑换货币面值总和相同的N个大面值的第一单位数据包，由此，可以使安全芯片释放出M-N个第一单位数据包所占用的存储空间，从而保障电子签名设备有足够的存储空间以支持后续的交易能够顺序进行。

[0057] 实施例2

[0058] 图2为本实施例提供的一种电子签名设备的结构示意图，现结合图2对本实施例提供的电子签名设备的结构进行详细的说明。

[0059] 本实施例提供了一种电子签名设备2，该电子签名设备2包括：安全模块21，用于获取自身存储的M个第一单位数据包；通信模块22，用于将M个第一单位数据包以及交易请求发送至服务器，交易请求包括：交易金额，其中，每个第一单位数据包代表多种货币面值中的一种货币面值，M个第一单位数据包所代表的货币面值的总和等于交易金额；获取模块23，用于接收服务器发送的N个第一单位数据包，其中，0<N<M，M、N均为整数；安全模块21，还用于在N个第一单位数据包所代表的货币面值的总和等于交易金额的情况下，删除自身存储的M个第一单位数据包，并将接收到的N个第一单位数据包存储于该安全模块分配的存储空间中。

[0060] 本实施例中，在电子签名设备2使用第一单位数据包进行交易时，由于每个第一单位数据包都会占用电子签名设备2的安全模块21中的一定存储空间，因此安全模块21的存储空间可能会被占满，从而使电子签名设备2不能进行后续的交易。采用本实施例提供的电子签名设备2，该电子签名设备2在接收到释放存储空间的触发指令或者安全芯片中当前存储的第一单位数据包的总个数达到预设数值时，可以将自身存储的M个小面值的第一单位数据包发送给服务器，向服务器兑换货币面值总和相同的N个大面值的第一单位数据包，由此，可以使安全芯片释放出M-N个第一单位数据包所占用的存储空间。

[0061] 本实施例中，安全模块21，用于获取自身存储的M个第一单位数据包，其中，每个第一单位数据包代表多种货币面值中的一种货币面值，M个第一单位数据包所代表的货币面值的总和等于交易金额其中，每个第一单位数据包代表多种货币面值中的一种货币面值，M个第一单位数据包所代表的货币面值的总和等于交易金额。

[0062] 在本实施例中，电子签名设备2为具有签名功能的电子设备，例如，具有签名功能的智能卡(公交卡、银行卡、购物卡等等)、工行的U盾等等。在本实施例一种可选的实施方式中，安全模块21可以采用安全芯片，该安全芯片内部拥有独立的处理器和存储单元，可存储PKI数字证书和密钥，以及其他特征数据，对数据进行加解密运算，为用户提供数据加密和身份安全认证服务，本实施例中，电子签名设备2可以将从服务器(如银行服务器或商场购物充值服务器等第三方服务器)或者从其他电子签名设备2接收到的第一单位数据包存储于安全芯片中，由于安全芯片的存储单元内的数据不能被非法读出，由此可以保证存储单元中存储数据的安全性。

[0063] 本实施例中，每个第一单位数据包代表多种货币面值中的一种货币面值，例如，第一单位数据包所代表的货币面值包括：1元、2元、5元、10元、20元、50元和100元，当然，如果未来国家发行了新的货币面值、或者除了使用人民币之外的其他地区、国家的货币面值也属于本发明的保护范围，本实施例中仅以人民币面值进行举例说明。也就是说，货币面值共有多种，当安全模块21从自身的存储空间中获取多个第一单位数据包时(即M>1时)，多个第一单位数据包可以代表多种不同的货币面值，例如，当M＝3时，第一单位数据包的个数为3个，3个第一单位数据包分别代表货币面值1元、2元以及5元；或者，多个第一单位数据包可以代表相同的货币面值，例如，当M＝3时，3个第一单位数据包均代表货币面值1元；再或者，多个第一单位数据包所代表的货币面值中既包括相同的也包括不相同的货币面值，例如，当M＝3时，3个第一单位数据包分别代表货币面值1元、1元以及2元。由此，电子签名设备2从其安全芯片中获取的M个第一单位数据包所代表的货币面值具有灵活的组合方式。

[0064] 在本实施例一种可选的实施方式中，第一单位数据包中至少包括第一单位数据，该第一单位数据至少包括：货币面值数据，或者，货币序号和货币面值数据。其中，货币面值数据为第一单位数据包所代表的货币面值，以此来标识第一单位数据包所代表的货币面值，货币序号为每个第一单位数据包的唯一序号，即不同的第一单位数据包中的货币序号是不同的。由此，能够保证每个第一单位数据包的唯一性，以便于辨认第一单位数据包的真伪。作为一种可选的实施方式，第一单位数据包至少还包括以下之一：发行银行标识和银行证书序号。其中，发行银行标识为发行该第一单位数据包的银行的标识信息，由此可以根据该标识查询到对应的发行银行的相关信息，而且，电子签名设备2可以根据发行银行标识和银行证书序号获取对应的发行银行的银行证书，银行证书中包含有发行银行的公钥，以便于后续步骤中电子签名设备2中的安全模块21利用发行银行的公钥对第一单位数据的签名完成验证。

[0065] 在本实施例一种可选的实施方式中，安全模块21自身存储的第一单位数据包至少还包括：第一单位数据以及服务器对第一单位数据签名得到的第一签名数据。作为一种可选的实施方式，服务器(如银行服务器或商场购物充值服务器等第三方服务器)利用自身的私钥分别对每个第一单位数据包中的第一单位数据进行签名，得到与每个第一单位数据包对应的第一签名数据。服务器将至少一个携带有第一签名数据的第一单位数据包发送至电子签名设备2，本实施例中，安全模块21在存储服务器发送的多个第一单位数据包之前，可以利用服务器的公钥验证第一单位数据包的真实性，在验证通过后，才存储，因此，安全模块21中存储的第一单位数据包均为真实且安全。

[0066] 在本实施例另一种可选的实施方式中，通信模块22发送给服务器的交易请求中还

包括:电子签名设备2的设备标识;安全模块21自身存储的每个第一单位数据包至少包括:第一单位数据、服务器对第一单位数据和电子签名设备2的设备标识签名得到的第二签名数据。作为一种可选的实施方式,服务器利用自身的私钥对第一单位数据和电子签名设备2的设备标识签名,得到与每个第一单位数据包对应的第二签名数据。服务器将至少一个携带有第二签名数据的第一单位数据包发送至电子签名设备2,以便在接收到服务器发送的第一单位数据包后,安全模块21可以对第一单位数据包中的第二签名数据验签,如果验签通过,则该第一单位数据包是真实的,且该第一单位数据包是发送给此电子签名设备的。

[0067] 由于第一单位数据包存储在安全模块21的存储空间中,且每个第一单位数据包都需要占用一定的存储空间,因此,安全模块21剩余的存储空间不足时,则无法再存储新的第一单位数据包,从而使电子签名设备2无法再进行后续的交易。因此,本实施例中,安全模块21,还用于在获取自身存储的M个第一单位数据包之前,接收到释放安全模块21的存储空间的触发指令;或者,还用于在获取自身存储的M个第一单位数据包之前,检测到自身当前存储的第一单位数据包的总个数达到预设数值。作为一种可选的实施方式,电子签名设备2还包括交互模块24,交互模块24用于接收用户输入的释放存储空间的触发指令。其中,用户可以通过键盘、语言等方式输入触发指令,用户输入的触发指令可以包括交易金额,安全模块21可以根据交易金额随机或按预设的规则获取自身存储的M个第一单位数据包,该M个第一单位数据包所代表的货币面值总和等于交易金额,在该可选方式中M的数值是随机确定的,但为了释放最大的空间,安全模块21可以选择M为所代表的货币面值总和等于交易金额的最大值,例如,存在10个1元数据包和2个5元数据包时,安全模块21选择10个1元数据包,M等于10,需要说明的是,在该可选实施方式中,无论第一单位数据包所代表的货币面值是否相同,每个第一单位数据包所占的存储空间的大小是相同的。作为另一种可选的实施方式,安全模块21检测到自身当前存储的第一单位数据包的总个数达到预设数值M后,执行获取M个第一单位数据包的操作。其中,该预设数值M可以是用户设定的,也可以是在电子签名设备2出厂时预先设定的,安全模块21获取M个第一单位数据包,并计算该M个第一单位数据包所代表的货币面值总和,将该货币面值总和作为交易金额,由通信模块22将M个第一单位数据包和交易金额发送至服务器。可选地,达到预设数值的第一单位数据包占用安全模块21的一半存储空间,也就是说,每当安全模块21的存储空间的一半被占用时,就会触发电子签名设备2释放存储空间的操作。由此,电子签名设备2可以在存储空间不足时,通过与服务器进行的数据包交换,来达到释放存储空间的目的,从而保证安全模块21保持有足够的存储空间。

[0068] 通信模块22,用于将M个第一单位数据包以及交易请求发送至服务器,交易请求包括:交易金额。

[0069] 本实施例中,同样的,N个第一单位数据包中的每个第一单位数据包代表多种货币面值中的一种货币面值,其中,第一单位数据包中至少包括第一单位数据,该第一单位数据至少包括:货币面值数据,或者,货币序号和货币面值数据。对于该第一单位数据的描述具体可以参见上文所述,在此不再赘述。作为一种可选的实施方式,N个第一数据包中的每个第一单位数据包至少还包括:服务器对第一单位数据签名得到的第一签名数据。由此,安全模块21可以通过验证第一签名数据来确定接收到的N个第一单位数据包是否是真实的,具体的验证方式可以参见下文中对第一签名数据进行验证的方式。作为另一种可选的实施方

式,N个第一单位数据包中的每个第一单位数据包至少包括:服务器对第一单位数据和电子签名设备的设备标识签名得到的第二签名数据。由此,安全模块21可以通过验证第二签名数据来确定接收到的N个第一单位数据包是否是真实的,以及是否是发给该电子签名设备的,具体的验证方式可以参见下文中对第二签名数据进行验证的方式。

[0070] 在本实施例一种可选的实施方式中,通信模块22可以与外接设备(如PC或移动终端等)建立连接,通过该外接设备将M个第一单位数据包以及交易请求发送至服务器。或者,通信模块22具有有线接口或无线接口,与服务器建立有线连接或无线连接,直接将M个第一单位数据包和交易请求发送至服务器。其中,无线连接方式可以包括蓝牙、NFC近场通讯以及WIFI等方式。由此,本实施例中通信模块22可以通过多种方式将交易请求发送至服务器。作为一种可选的实施方式,服务器包括银行服务器或第三方服务器,例如,第三方服务器可以是某商场的购物卡储值服务器。

[0071] 获取模块23,用于接收服务器发送的N个第一单位数据包,其中,0<N<M,M、N均为整数。

[0072] 本实施例中,每个第一单位数据包可以占用相同的存储空间(例如,每个第一单位数据包占用1M的存储空间)。通信模块22发送至服务器的第一单位数据包的个数M大于获取模块23从服务器接收的第一单位数据包的个数N,例如,安全模块21从自身存储空间中获取100个货币面值为2元的第一单位数据包,该100个第一单位数据包所代表的货币面值总和为200元,即交易金额为200元,占用存储空间100M。服务器在接收到通信模块22发送的第一单位数据包以及交易金额后,根据交易金额,向电子签名设备2下发2个代表货币面值100的第一单位数据包(货币面值总和仍为200,占用空间2M)。由此,电子签名设备2在保持货币面值不变的情况下,将100个第一单位数据包兑换成2个第一单位数据包,由此,安全模块21可以释放出98M存储空间,即98个第一单位数据包所占用的存储空间。

[0073] 安全模块21,还用于在N个第一单位数据包所代表的货币面值的总和等于所述交易金额的情况下,删除自身存储的M个第一单位数据包,并将接收到的N个第一单位数据包存储于其存储空间中。

[0074] 本实施例中,在N个第一单位数据包所代表的货币面值的总和等于交易金额的情况下,即服务器发送的第一单位电子货币数据包在传输过程中没有丢失的情况下,安全模块21删除自身存储的M个第一单位数据包,并将接收到的N个第一单位数据包存储于在其存储空间中。由此,电子签名设备2可以将完成存储空间的释放。

[0075] 在本实施例中,为了进一步保证安全模块21存储的第一单位数据包的真实性,作为本实施例中的一种可选实施方式,安全模块21,用于将接收到的N个第一单位数据包存储于其存储空间中,具体包括:安全模块21,用于对第一签名数据进行验证,并在验证通过后,将接收到的N个第一单位数据包存储在其存储空间中。其中,第一签名数据是服务器对第一单位数据进行签名得到的,因此,作为一种可选的实施方式,服务器发送至电子签名设备的第一单位数据包至少还包括:服务器对第一单位数据签名得到的第一签名数据,由此使得安全模块21可以验证第一单位数据包的真实性。作为一种可选的实施方式,第一签名数据为服务器利用自身的私钥对第一单位数据进行签名得到的签名数据。相应的,安全模块21,用于对第一签名数据进行验证,具体包括:安全模块21,用于利用该服务器的公钥对第一签名数据进行验签。以服务器为银行服务器为例,银行服务器对第一单位数据进行HASH运算

得到第一单位数据的摘要报文A1，并利用银行服务器自身的私钥对该摘要报文A1进行签名运算得到第一签名数据，并携带在第一单位数据包中下发至电子签名设备2。安全模块21可以利用该银行服务器的公钥对第一签名数据进行验签，具体地，安全模块21利用银行服务器的公钥对第一电子签名数据进行运算得到运算结果A2，并对接收到的第一单位数据包中的第一单位数据进行HASH运算得到第一单位数据的摘要报文A3，将运算结果A2与摘要报文A3进行比对，如果比对结果一致，则安全模块21对第一电子签名数据验签通过。其中，安全模块21可以根据第一单位数据包中的银行证书序号和/或发行银行标识获取银行的公钥，例如，安全模块21可以根据第一单位数据包中的发行银行标识，从与待验证的第一签名数据对应的发行银行服务器获取该银行的银行证书，并从银行证书中获取该银行的公钥；再例如，安全模块21可以预存各个银行的银行证书，根据第一单位数据包中的银行证书序号从预存的各个银行证书中获取与待验证的第一签名数据对应的银行证书，并从对应的银行证书中获取银行的公钥。由此，安全模块21利用银行的公钥对第一单位数据包中携带的第一签名数据进行验签，可以验证第一单位数据包的真实性。上述描述仅以服务器为银行服务器为例进行说明，但本实施例并不限于银行服务器，其他第三方服务器如超市购物卡储值服务器等的具体实施方式均属于本发明的保护范围之内。

[0076] 进一步地，电子签名设备2在确保收到的第一单位数据包是真实的前提下，还想再确认服务器发送的对象是否确实为本电子签名设备2，以避免存储服务器误发的数据包，安全模块21，用于将接收到的N个第一单位数据包存储于其存储空间中，具体包括：安全模块21，用于对第二签名数据进行验证，在验证通过后，将接收到的N个第一单位数据包存储于其存储空间中。其中，第二签名数据是服务器对第一单位数据和电子签名设备2的设备标识签名得到的，因此，在本实施例一种可选的实施方式中，电子签名设备2通过通信模块22发送给服务器的交易请求中还包括：电子签名设备2的设备标识；服务器返回的N个第一单位数据包中的每个第一单位数据包至少还包括：第一单位数据、服务器对第一单位数据和电子签名设备2的设备标识签名得到的第二签名数据，由此使得安全模块21可以验证第一单位数据包的真实性和正确性。作为一种可选的实施方式，第二签名数据为服务器利用服务器自身的私钥对第一单位数据和电子签名设备2的设备标识进行签名得到的签名数据，也就是说，每个第二签名数据的签名对象为每个第一单位数据和电子签名设备2的设备标识的组合。相应的，安全模块21，用于对第二签名数据进行验证，具体包括：安全模块21，用于利用服务器的公钥分别对每个第二签名数据进行验签。以服务器为银行服务器为例，银行服务器利用自身的私钥对第一单位数据和电子签名设备2的设备标识进行签名得到第二签名数据，并携带在第一单位数据包中下发至电子签名设备2。安全模块21可以利用该银行服务器的公钥对第二签名数据进行验签。其中，安全模块21可以根据第一单位数据包中的银行证书序号和/或发行银行标识获取该银行的银行证书，并从银行证书中获取该银行的公钥，例如，安全模块21可以根据第一单位数据中的发行银行标识，通过获取模块23从与待验证的第二签名数据对应的发行银行服务器获取该银行的公钥；再例如，安全模块21可以预存各个银行的银行证书，根据第一单位数据包中的银行证书序号从预存的各个银行证书中获取与待验证的第二签名数据对应的银行证书，并从对应的银行证书中获取银行的公钥。由此，安全模块21利用银行的公钥对第一单位数据包中携带的第二签名数据进行验签，不仅可以验证第一单位数据包的真实性，还可以证明第一单位数据包确实是银行服务器下发

给该电子签名设备2的，即验证第一单位数据包的正确性。上述描述仅以服务器为银行服务器为例进行说明，但本实施例并不限于银行服务器，其他第三方服务器如超市购物卡储值服务器等的具体实施方式均属于本发明的保护范围之内。

[0077] 在数据传输的过程中，可能会出现第一单位数据包丢失的情况，当第一单位数据包在传输过程中丢失，那么获取模块23接收到的N个第一单位数据包所代表的货币面值的总和小于所述交易金额。本实施例一种可选的实施方式中，安全模块21，还用于在N个第一单位数据包所代表的货币面值的总和不等于交易金额(即大于或小于交易金额)的情况下，删除自身存储的M个第一单位数据包，并将接收到的N个第一单位数据包存储在其存储空间中；通信模块22，还用于向服务器发送重发请求；获取模块23，还用于接收服务器根据重发请求发送的重发信息，重发信息包括：重发的X个第一单位数据包，其中，X个第一单位数据包所代表的货币面值的总和等于交易金额，或者，X个第一单位数据包所代表的货币面值的总和加上N个第一单位数据包所代表的货币面值的总和等于交易金额；安全模块21，还用于将接收到的X个第一单位数据包存储于其存储空间中。具体地，在通信模块22向服务器发送重发请求后，获取模块23会接收到服务器返回的重发信息，根据重发请求的内容不同，服务器返回的重发信息也会不同，例如，重发请求中可以携带电子签名设备2的设备标识、交易记录(如每笔交易的编号、账户信息、时间戳、交易金额以及接收到的第一单位数据包的个数以及所代表的货币面值等等，这些服务器侧也会对应记录)，以便于服务器查询到该电子签名设备2对应的某一笔交易，全部重发该笔交易对应的第一单位数据包至电子签名设备2，又例如，重发请求中还可以携带接收到的第一单位数据包的数据包标识(可以唯一标识一个第一单位数据包的标识，如服务器为每个第一单位数据包配置的唯一标识，或者货币序号)，服务器接收到这些数据包标识后，可以查询到漏发或传输过程中丢失了哪些第一单位数据包，将这些漏发的或传输过程中丢失的第一单位数据包发送至电子签名设备2。下面就服务器重发第一单位电子数据包进行示例性说明：

[0078] 例如，作为一种可选的实施方式，获取模块23，还用于接收服务器根据重发请求发送的重发信息，其中，该重发请求中至少包括：电子签名设备2的设备标识以及交易记录，重发信息包括X个第一单位数据包，X个第一单位数据包所代表的货币面值的总和等于交易金额，即在该可选的实施方式中，服务器向电子签名设备2重发了一笔交易对应的全部第一单位数据包，在本实施例中，服务器在与单位电子签名设备2进行交易时，也会存储每一笔交易对应的交易记录(如每笔交易的编号、账户信息、时间戳、交易金额以及发送的第一单位数据包的个数以及所代表的货币面值等等)以及电子签名设备2的设备标识，根据设备标识以及交易记录可以查询到该电子签名设备2对应的某一笔交易，在该可选实施方式中，服务器会将查询到的电子签名设备2请求重发的该笔交易的第一单位数据包全部重发给电子签名设备2，以保证电子签名设备2收到完整的第一单位数据包，服务器与电子签名设备2的交易无误(即空间释放操作无误)。在该可选的实施方式中，获取模块23，还用于接收到服务器重发的X个第一单位数据包后，安全模块21，还用于判断该X个第一单位数据包中的每个第一单位数据包是否存在与之前存储的N个第一单位数据包相同的第一单位数据包，具体地，安全模块21将X个第一单位数据包中的第一个第一单位数据包a依次与自身存储的每个第一单位数据包进行比较，如果自身存储的第一单位数据包中存在与第一单位数据包a相同的第一单位数据包，则跳过该第一单位数据包a，或者将之前存储的与第一单位数据包a相

同的第一单位数据包删除，重新存储该第一单位数据包a；在完成对第一个第一单位数据包a的判断之后，安全模块21继续逐一对X个第一单位数据包中的第二个第一单位数据包b、第三个第一单位数据包c……最后一个第一单位数据包x进行判断。由此，安全模块21可以将服务器重发的X个第一单位数据包存储在其存储空间中。

[0079] 举例来说，对于一笔编号为1*******的交易，通信模块22发送的交易请求中的交易金额为10元，获取模块23接收服务器发送的2个分别代表5元货币面值的第一单位数据包(2个第一单位数据包分别为数据包a和数据包b)，但由于传输过程中数据丢失，获取模块23仅接收到1个代表5元货币面值的第一单位数据包(只接收到数据包a)，货币面值总和为5元，与交易金额10元不相等。针对该笔交易，安全模块21将数据包a存储，并由通信模块22向服务器发送重发请求，并由获取模块23接收服务器根据重发请求发送的重发信息，该重发请求中包括：电子签名设备2的设备标识以及交易记录，服务器在接收到该重发请求后，可以根据设备标识以及交易记录查询到该电子签名设备2对应的该笔交易，服务器会将查询到的电子签名设备2请求重发的该笔交易的第一单位数据包全部重发给电子签名设备2，即服务器发送给电子签名设备2的该重发信息包括数据包a和数据包b。安全模块21判断重发的第一单位数据包中的数据包a与之前存储的数据包a相同，则跳过数据包a，只存储重发的数据包b，或者，将之前存储的数据包a删除，重新存储数据包a和数据包b。由此，当电子签名设备2没有接收到一笔交易所需的全部第一单位数据包时，服务器可以将该笔交易所需的全部第一单位数据包重发给电子签名设备2，从而使交易能够顺利完成。

[0080] 再例如，作为一种可选的实施方式，电子签名设备2在向服务器发送重发请求后，电子签名设备2接收服务器根据重发请求发送的重发信息，其中，该重发请求中至少包括：电子签名设备2的设备标识、交易记录以及接收到的各个第一单位数据包的数据包标识，重发信息包括X个第一单位数据包，且该X个第一单位数据包所代表的货币面值的总和加上之前接收到的N个第一单位数据包所代表的货币面值的总和等于交易金额，即该X个第一单位数据包为电子签名设备2未接收到的第一单位数据包，在该可选的实施方式中，服务器向电子签名设备2重发了一笔交易中漏发的或传输过程中丢失的第一单位数据包，根据设备标识以及交易记录可以查询到该电子签名设备2对应的某一笔交易，服务器会将查询到的该电子签名设备2请求重发的该笔交易中没有查询到的数据包标识对应的那些第一单位数据包重发给电子签名设备2，以保证电子签名设备2收到完整的第一单位数据包，服务器与电子签名设备2的交易无误(即空间释放操作无误)。与上一例中的可选实施方式相比，本可选实施方式可以减少服务器的数据传输量，大大降低服务器的工作负荷，提高服务器重发的工作效率。

[0081] 举例来说，对于一笔编号为1*******的交易，通信模块22发送的交易请求中的交易金额为15元，获取模块23接收服务器发送的1个代表5元货币面值的第一单位数据包(数据包c)，以及1个代表10元货币面值的第一单位数据包(数据包d)，但由于传输过程中数据丢失，获取模块23仅接收到数据包c，货币面值总和为5元，与交易金额15元不相等。针对该笔交易，通信模块22向服务器发送重发请求，并接收服务器根据重发请求发送的重发信息，在重发请求中还携带有数据包c的数据包标识，服务器接收到该重发请求后，针对该电子签名设备2的该笔交易可以查询到其对应的所有第一单位数据包，便可以发现重发请求中没有数据包d的数据包标识，服务器可以将数据包d重发给电子签名设备2。安全模块21将服务

器重发的数据包d存储于其存储空间中。本实施例中，通信模块22向服务器发送的重发请求中可以包括已经被接收到的部分第一单位数据包的数据包标识，服务器可以根据重发请求中的数据包标识来确定重发信息中需要携带的第一单位数据包。由此，当电子签名设备2没有接收到一笔交易所需的全部第一单位数据包时，服务器可以将未收到的部分第一单位数据包重发给电子签名设备2，不仅减少了重发数据的传输量，也保证了交易能够顺利完成。

[0082] 以上均是以一笔交易的实施方式为例进行说明的，在本实施例中，对于多笔交易中的每笔交易都可以按照上述方式来实现。

[0083] 本实施例中，为了防止电子签名设备2非法重复使用同一个第一单位数据包，造成电子金融流通的混乱，保证同一个第一单位数据包在交易过程中的唯一性，安全模块21，还用于对M个第一单位数据包进行加密，得到M个第二单位数据包，并用M个第二单位数据包覆盖安全芯片中存储的M个第一单位数据包；通信模块22，还用于将M个第二单位数据包发送至服务器；安全模块21，还用于删除M个第一单位数据包，具体包括：安全模块21，还用于删除M个第二单位数据包。本实施例中，安全模块21对M个第一单位数据包进行的加密操作为不可逆操作，即，安全模块21可以加密第一单位数据包得到第二单位数据包，却不能从第二单位数据包解密得到第一单位数据包，因此，当得到的M个第二单位数据包覆盖了对应的M个第一单位数据包时，安全模块21中仅仅存储了加密的第二单位数据包，由于其不能对第二单位数据包解密，所以无法恢复出第一单位数据包，也就不能再重复使用这些第一单位数据包，从而防止持有电子签名设备的用户重复使用这些第一单位数据包进行消费，造成第一单位数据包流通混乱。

[0084] 具体地，作为一种可选的实施方式，安全模块21，用于对M个第一单位数据包进行加密，具体包括：安全模块21，用于利用服务器的公钥至少对M个第一单位数据包中的每个第一单位数据包中的第一单位数据进行加密。作为另一种可选的实施方式，安全模块21，用于对M个第一单位数据包进行加密，具体包括：安全模块21，用于利用对称密钥至少对M个第一单位数据包中的每个第一单位数据包中的第一单位数据进行加密；并在对M个第一单位数据包进行加密之后，删除该对称密钥。

[0085] 对于后一种可选的实施方式，对称密钥可以由电子签名设备2和服务器协商得到。可选地，对称密钥可以为与服务器关联的异或因子。安全模块21，用于利用对称密钥至少对M个第一单位数据包中的每个第一单位数据包中的第一单位数据进行加密，具体包括：安全模块21，用于利用异或因子至少对M个第一单位数据包中的每个第一单位数据包中的第一单位数据进行异或运算。异或运算也属于一种对称加密运算方式，但相比其他对称加密运算的方式，异或运算的速度较快，由此，可以提高安全模块21对第一单位数据包进行加密生成第二单位数据包的效率。

[0086] 本实施例一种可选的实施方式中，获取模块23，还用于接收服务器发送的重发请求；通信模块22，还用于将M个第二单位数据包重新发送至服务器，或者，根据服务器发送的重发请求将服务器未接收到的第二单位数据包发送至服务器。具体地，服务器在接收到电子签名设备发送的第二单位数据包和交易请求后，计算接收到的第二单位数据包所代表的货币面值总和是否与交易请求中的交易金额相等，如果该货币面值总和小于交易金额，则说明在传输过程中有第二单位数据包遗失，此时，服务器将重发请求发送至电子签名设备。由此，电子签名设备可以通过重发第二单位数据包来保证服务器接收到所发送的全部第二

数据包。

[0087] 本实施例中，至少可以通过使用对称密钥或者服务器的公钥对第一单位数据包进行加密的方式，来防止电子签名设备2非法重复使用同一个第一单位数据包，造成第一单位数据包流通的混乱，保证同一个第一单位数据包在交易过程中的唯一性。当然本实施例并不排除其他实施方式，只要可以达到相同的技术效果即可。在使用时，电子签名设备可以通过将这些第一单位数据包发送至对端电子签名设备来完成付款操作，而无需联网至后台服务器才能完成付款，从而使电子签名设备具有离线交易的功能。此外，需要说明的是，本实施例中第一单位数据包可以理解为包括：明文方式和密文方式的两种数据包，第二单位数据包可以理解为第一单位数据包的一种，即第一单位数据包加密后的数据包，即是第一单位数据包的密文形式。此外，第二单位数据包为密文，保证了传输数据的安全性，且即便被其他设备截获，也很难破解，进一步提高了第一单位数据包流通的安全性。

[0088] 采用本实施例提供的电子签名设备2，该电子签名设备2在接收到释放存储空间的触发指令或者安全芯片中当前存储的第一单位数据包的总个数达到预设数值时，可以将自身存储的M个小面值的第一单位数据包发送给服务器，向服务器兑换货币面值总和相同的N个大面值的第一单位数据包，由此，可以使安全芯片释放出M-N个第一单位数据包所占用的存储空间，从而保障电子签名设备有足够的存储空间以支持后续的交易能够顺序进行。

[0089] 流程图中或在此以其他方式描述的任何过程或方法描述可以被理解为，表示包括一个或更多个用于实现特定逻辑功能或过程的步骤的可执行指令的代码的模块、片段或部分，并且本发明的优选实施方式的范围包括另外的实现，其中可以不按所示出或讨论的顺序，包括根据所涉及的功能按基本同时的方式或按相反的顺序，来执行功能，这应被本发明的实施例所属技术领域的技术人员所理解。

[0090] 应当理解，本发明的各部分可以用硬件、软件、固件或它们的组合来实现。在上述实施方式中，多个步骤或方法可以用存储在存储器中且由合适的指令执行系统执行的软件或固件来实现。例如，如果用硬件来实现，和在另一实施方式中一样，可用本领域公知的下列技术中的任一项或他们的组合来实现：具有用于对数据信号实现逻辑功能的逻辑门电路的离散逻辑电路，具有合适的组合逻辑门电路的专用集成电路，可编程门阵列(PGA)，现场可编程门阵列(FPGA)等。

[0091] 本技术领域的普通技术人员可以理解实现上述实施例方法携带的全部或部分步骤是可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，该程序在执行时，包括方法实施例的步骤之一或其组合。

[0092] 此外，在本发明各个实施例中的各功能单元可以集成在一个处理模块中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。所述集成的模块如果以软件功能模块的形式实现并作为独立的产品销售或使用时，也可以存储在一个计算机可读取存储介质中。

[0093] 上述提到的存储介质可以是只读存储器，磁盘或光盘等。

[0094] 在本说明书的描述中，参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不

一定指的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任何的一个或多个实施例或示例中以合适的方式结合。

[0095] 尽管上面已经示出和描述了本发明的实施例，可以理解的是，上述实施例是示例性的，不能理解为对本发明的限制，本领域的普通技术人员在不脱离本发明的原理和宗旨的情况下在本发明的范围内可以对上述实施例进行变化、修改、替换和变型。本发明的范围由所附权利要求及其等同限定。

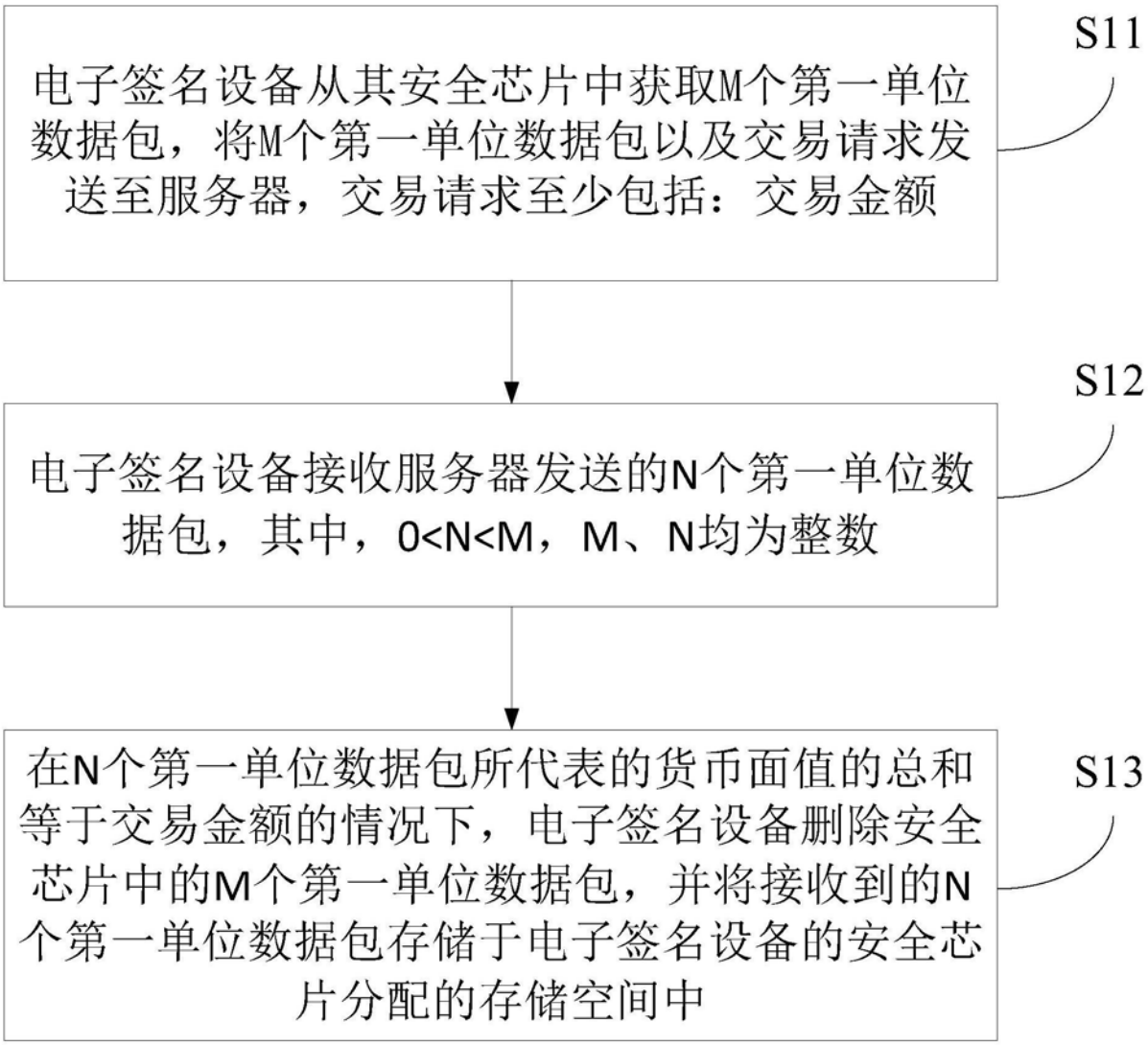

S11
电子签名设备从其安全芯片中获取M个第一单位数据包，将M个第一单位数据包以及交易请求发送至服务器，交易请求至少包括：交易金额
S12
电子签名设备接收服务器发送的N个第一单位数据包，其中，0<N<M，M、N均为整数
S13
在N个第一单位数据包所代表的货币面值的总和等于交易金额的情况下，电子签名设备删除安全芯片中的M个第一单位数据包，并将接收到的N个第一单位数据包存储于电子签名设备的安全芯片分配的存储空间中

图1

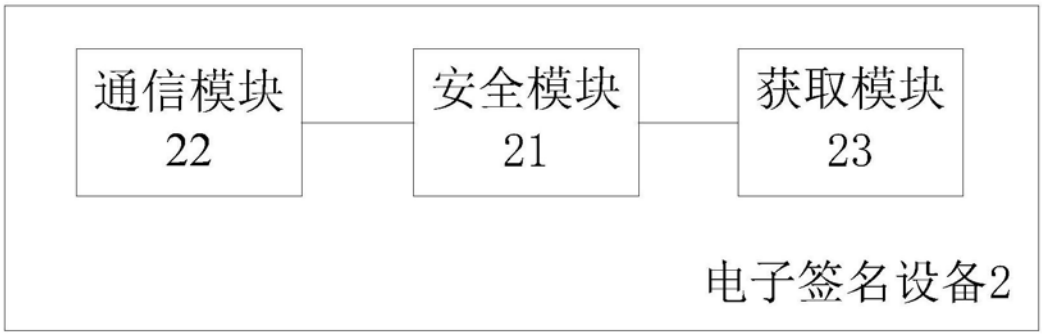

通信模块
22
安全模块
21
获取模块
23
电子签名设备2

图2