

一种支付二维码的生成方法和装置

技术领域

[01]本公开涉及支付技术领域，特别涉及一种支付二维码的生成方法和装置。

背景技术

- 5 [02]目前绝大部分的基于二维码的支付机具都是被扫模式，即用户出示手机上的付款码/条码，店主主动扫描用户的付款码，并进行扣款。这需要商户的设备有摄像头模块，且对摄像头的精度有一定要求，每次需要商户手动输入金额，并不适合小额高频的商户使用。并且，在条码支付业务中，对安全性有较高的要求，如果安全性较低，可以对支付限额进行控制。

10 发明内容

[03]有鉴于此，本说明书一个或多个实施例提供一种支付二维码的生成方法和装置，以提高条码支付的安全性。

[04]具体地，本说明书一个或多个实施例是通过如下技术方案实现的：

- [05]第一方面，提供一种支付二维码的生成方法，所述方法由二维码显示设备中的安全
15 芯片执行，所述方法包括：

[06]接收待加签的码信息，所述码信息中包括绑定了所述二维码显示设备的支付账号的账号标识；

[07]在确认安全芯片中存储的私钥处于可用状态时，使用所述私钥对所述码信息进行加签；所述可用状态表示所述私钥已经获得了数字证书；

- 20 [08]将加签后的码信息返回给二维码显示设备，以使得二维码显示设备将码信息显示成用于支付的二维码，所述二维码中包括所述账号标识，且所述二维码动态变化。

[09]第二方面，提供一种支付交易方法，所述方法由支付服务器执行，所述方法包括：

[10]接收支付交易请求，所述支付交易请求是通过扫描二维码显示设备上的动态二维码后发送，并且，所述支付交易请求中携带通过解析该动态二维码得到的支付账号的账号

标识, 所述账号标识经二维码显示设备上的安全芯片进行私钥加签;

[11]在对所述支付账号的账号标识进行公钥验签通过后, 根据支付账号的账号标识进行支付交易处理。

[12]第三方面, 提供一种支付二维码的生成装置, 所述装置应用于二维码显示设备中的安全芯片, 所述装置包括:

[13]信息接收模块, 用于接收待加签的码信息, 所述码信息中包括绑定了所述二维码显示设备的支付账号的账号标识;

[14]签名处理模块, 用于在确认安全芯片中存储的私钥处于可用状态时, 使用所述私钥对码信息进行加签; 所述可用状态表示所述私钥已经获得了数字证书;

10 [15]显码发送模块, 用于将加签后的码信息返回给二维码显示设备, 以使得二维码显示设备将码信息显示成用于支付的二维码, 所述二维码中包括所述账号标识, 且所述二维码动态变化。

[16]第四方面, 提供一种支付交易装置, 所述装置应用于支付服务器, 所述装置包括:

15 [17]请求接收模块, 用于接收支付交易请求, 所述支付交易请求是通过扫描二维码显示设备上的动态二维码后发送, 并且, 所述支付交易请求中携带通过解析该动态二维码得到的支付账号的账号标识, 所述账号标识经二维码显示设备上的安全芯片进行私钥加签;

[18]交易处理模块, 用于在对所述支付账号的账号标识进行公钥验签通过后, 根据支付账号的账号标识进行支付交易处理。

20 [19]第五方面, 提供一种支付二维码的显示设备, 所述设备包括: 安全芯片, 所述安全芯片中存储有安全数据, 所述安全数据由支付服务器根据二维码显示设备绑定的支付账号得到并下发至安全芯片;

[20]所述安全芯片包括存储器、处理器, 以及存储在存储器上并可在处理器上运行的计算机指令, 所述处理器执行指令时实现以下步骤:

25 [21]接收待加签的码信息, 所述码信息中包括绑定了所述二维码显示设备的支付账号的账号标识; 且所述码信息是根据所述安全数据生成得到;

[22]在确认安全芯片中存储的私钥处于可用状态时, 使用所述私钥对所述码信息进行加签; 所述可用状态表示所述私钥已经获得了数字证书;

[23]将加签后的码信息返回给二维码显示设备, 以使得二维码显示设备将码信息对应的

用于支付的二维码在显示屏上显示,所述二维码中包括所述账号标识,且所述二维码动态变化。

[24]第六方面,提供一种支付服务器,所述服务器包括存储器、处理器,以及存储在存储器上并可在处理器上运行的计算机指令,所述处理器执行指令时实现以下步骤:

- 5 [25]接收支付交易请求,所述支付交易请求是通过扫描二维码显示设备上的动态二维码后发送,并且,所述支付交易请求中携带通过解析该动态二维码得到的支付账号的账号标识,所述账号标识经二维码显示设备上的安全芯片进行私钥加签;

[26]在对所述支付账号的账号标识进行公钥验签通过后,根据支付账号的账号标识进行支付交易处理。

- 10 [27]本说明书一个或多个实施例的方法和装置,通过利用设备中的 SE 芯片对二维码进行数字签名,并且用于签名的私钥经过了数字认证,该方法保证了二维码交易的安全性。

附图说明

[28]为了更清楚地说明本说明书一个或多个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

15 附图仅仅是本说明书一个或多个实施例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。

[29]图 1 为本说明书一个或多个实施例提供的支付交易方法的应用系统架构图;

[30]图 2 为本说明书一个或多个实施例提供的芯片执行流程示意图;

[31]图 3 为本说明书一个或多个实施例提供的二维码生成的示意图;

- 20 [32]图 4 为本说明书一个或多个实施例提供的支付服务器的交易处理;

[33]图 5 为本说明书一个或多个实施例提供的芯片加签处理的流程图;

[34]图 6 为本说明书一个或多个实施例提供的二维码生成装置的结构示意图;

[35]图 7 为本说明书一个或多个实施例提供的支付交易装置的结构示意图。

具体实施方式

- 25 [36]为了使本技术领域的人员更好地理解本说明书一个或多个实施例中的技术方案,下面将结合本说明书一个或多个实施例中的附图,对本说明书一个或多个实施例中的技术

方案进行清楚、完整地描述，显然，所描述的实施例仅仅是一部分实施例，而不是全部的实施例。基于本说明书一个或多个实施例，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，都应当属于本申请保护的范围。

[37]近年来，扫码支付几乎渗透到人们生活中的各个角落，现在很多商店，超市，零售商店，街边摊位和生活用品的小商贩，他们都有着自己的收款码，买东西的人也早已经习惯了这种方便快捷的付钱方式。商家在收款时一般采用静态条码，例如粘贴的静态收款码。通过扫“条码”或者“二维码”，完成收付款的支付方式，都称之为条码支付。

[38]然而，条码支付本身存在一定的技术风险，并且随着市场日益壮大，安全问题也越发凸出。为了提高条码支付的安全性，本说明书至少一个实施例提供了一种支付交易方法，该方法使用了包括数字证书和电子签名在内的方式对交易进行验证，并且还在收款码的生成中使用了安全芯片（Secure Element，安全元件，通常以芯片形式提供），以保证条码支付的安全。

[39]在本说明书至少一个例子的应用场景中，可以由商家出示收款码，通过本说明书至少一个实施例的支付二维码的生成方式来生成该收款码，付款方可以扫描该收款码付款；并且，该商家出示的收款码是可以动态变化的动态码。可以理解的是，该方法同样也可以应用于付款码的生成。在如下的描述中，是以收款码的生成为例进行描述。

[40]图 1 示例了本支付交易方法的应用系统架构图，如图 1 所示，商家可以购买一个二维码显示设备 11，在该设备中可以包括安全芯片（SE）12，安全芯片 12 中可以下载和安装一个 Applet 13，该 Applet 13 可以是 Javacard 操作系统中运行的应用，一般运行在 SE 芯片中。在本说明书提供的支付交易方法中，Applet 13 可以用于在 SE 芯片中执行收款码的加签等处理。

[41]请继续参见图 1，二维码显示设备 11 在 SE 芯片中的 Javacard 操作系统之外，还可以具有一个设备操作系统，该系统可以是嵌入式系统（或者是安卓等其他系统），在该嵌入式系统中，可以包括一个码处理组件 SDK 14，该码处理组件 14 可以与 Applet 13 配合共同完成动态收款码的生成。最终生成的动态收款码可以显示在显示屏 15 上，以供付款方扫描该收款码进行付款。此外，需要说明的是，图 1 中的 SDK 是以设置在二维码显示设备的嵌入式操作系统为例，但是 SDK 的设置位置并不局限于此，比如，SDK 也可以设置在 SE 芯片中，这样可以更加安全。如下的例子描述中，以 SDK 设置在嵌入式系统为例。

[42]此外,安全芯片 12 可以与云端的支付服务器 16 连接,支付服务器 16 可以向安全芯片 12 下发一些收款码生成过程中所需要的信息;并且,安全芯片 12 与支付服务器 16 也可以在支付交易中配合进行安全保障,比如,安全芯片 12 可以使用私钥对收款码进行加签,而支付服务器可以利用对应的公钥解密来获取收款码中的信息,从而保证支付交易的安全。

[43]如下以二维码是收款码为例,示例一个商家如何使用本说明书至少一个实施例提供的方法来进行收款,其中,还将描述如何使用二维码显示设备以及该设备与支付服务器之间的交互配合。

[44]首先,设备与支付服务器的绑定:

10 [45]在可信环境中,将二维码显示设备 11 连接到云端的支付服务器进行绑定。

[46]例如,支付服务器 16 可以根据该设备的 MAC 地址(也可以是设备特有的其他属性),生成服务器内部进行设备管理使用的唯一 ID,该唯一 ID 可以称为设备标识(deviceId)。

[47]支付服务器 16 可以将所述的设备标识下发到二维码显示设备中存储,具体可以是将该设备标识存储在安全芯片 12 中。

15 [48]此外,如果出于安全考虑,设备标识不允许被直接读取,则 SE 中还可以存储加密密钥,当每次需要由 SE 中读取该设备标识时,SE 可以使用该加密密钥对设备标识进行加密(或者,还可以将该设备标识混合随机数、时间戳等其他信息后再加密,以提高解密的复杂度),防止除云端支付服务器之外的其他系统获取到该信息。

20 [49]在设备标识之外,支付服务器 16 还可以向安全芯片 12 中下发其他一些只与设备有关的配置信息,例如,连接网络的密钥,该密钥可以用于后续二维码显示设备与支付服务器之间连接后的传输数据进行加密使用,以保证数据安全。

[50]接着,设备与商家的支付账户之间绑定,且将设备进行初始化操作:

[51]例如,上述的二维码显示设备中存储设备标识,可以是在设备出厂前就已经完成。因此,当商家购买了一个二维码显示设备后,该设备中已经存储有上述的设备标识。在第一次使用该设备时,商家可以启动购买的二维码显示设备,该设备上可以显示一个二维码,二维码中包括 SE 芯片中存储的上述设备标识。此外,二维码中的设备标识也可以使用密钥加密,支付服务器也可以预先存储了解密密钥,能够对加密的设备标识进行解密获得该标识。

25

[52]商家可以用自己的手机扫描该二维码，手机上安装有支付服务器对应的支付应用，可以用支付应用中的“扫一扫”功能来进行扫码。当扫码后，支付应用可以向支付服务器 16 发送一个消息，其中携带：加密的二维码显示设备的设备标识、以及商家的支付应用使用的支付账号（支付应用使用账号登录）。

5 [53]支付服务器 16 可以根据该消息，将商家的支付账号与商家购买的二维码显示设备进行绑定操作。例如，可以在服务器侧记录如下对应关系：

表 1 支付账号和设备绑定	
二维码显示设备	支付账号
ID-1	Account-1

[54]在绑定了商家的支付账号和商家的二维码显示设备后，支付服务器可以通知 SE 芯片已经完成绑定，并触发芯片开始执行图 2 所示的流程，SE 芯片开始生成公私钥对。
10 需要说明的是，本例子并不限制各步骤之间的执行顺序：

[55]在步骤 200 中，安全芯片生成公私钥对。

[56]在步骤 202 中，安全芯片将公钥上传到云端的支付服务器。

[57]在步骤 204 中，支付服务器将公钥发往证书中心进行认证。

15 [58]在步骤 206 中，支付服务器接收到认证通过返回的数字证书。所述数字证书表明所述公私钥对中的公钥已经被认证通过。

[59]在步骤 208 中，支付服务器将数字证书下发到安全芯片。

[60]在步骤 210 中，安全芯片存储该数字证书，并将私钥置为可用状态。

[61]本步骤中，SE 芯片在接收到数字证书后，知晓自己刚刚生成的公私钥中的公钥已经被认可，后面都可以使用该公私钥对进行加签验签，否则，如果没通过认证，SE 芯片不会使用刚刚生成的公私钥对。SE 芯片可以存储该数字证书，并将对应的私钥设置为可用状态。
20

[62]在步骤 212 中，支付服务器根据支付账号生成安全数据。

[63]本步骤中，支付服务器可以进行两方面的处理：

25 [64]一个方面是，支付服务器可以将公钥存储在表 1 的对应关系中，存储该公钥可以用于后续对扫描该二维码显示设备上的收款码发起的支付请求，使用该公钥进行解密。更新后的对应关系可以参见表 2 所示：

表 2 支付账号和设备绑定

二维码显示设备的设备标识	支付账号	公钥
ID-1	Account-1	public key-1

[65]另一个方面是，支付服务器可以生成安全数据。其中，安全数据都是与用户有关的，比如，不同的商家具有不同的支付账号，那么对应的安全数据就可以不同。这里的安全数据，可以包括用于生成二维码的相关配置参数，也可以包括与二维码生成无关的其他参数。

[66]在步骤 214 中，支付服务器将安全数据下发到安全芯片存储。

[67]至此，完成了二维码显示设备的初始化。由上述描述可以看到，商家在拿到二维码显示设备以后，只要用手机上的支付应用中的“扫一扫”扫描设备上的二维码，就可以触发云端的支付服务器将商家的支付账号和设备绑定，并且触发设备公私钥的生成、以及配置参数的下发等处理。设备初始化完成后，二维码显示设备的安全芯片中已经存储了数字证书和可用的私钥，还存储了二维码生成过程中要使用到的一些配置参数。接下来就可以使用该设备进行收款了。

[68]此外，当商户解绑后，也可以触发 SE 删除公私钥对。比如，商户可以通过自己手机上的支付应用来解绑，支付服务器接收到解绑请求后，可以通知 SE 删除公私钥对。

[69]然后，商家使用设备进行收款：

[70]在设备初始化完成后，商家就可以使用该设备进行收款。在日常使用中，设备可以生成并显示动态二维码，付款方可以扫描该动态二维码进行付款。

[71]其中，二维码显示设备的嵌入式系统可以向 SE 芯片发送指令，表明后续操作都由芯片中的 Applet 进行处理。图 3 示意了 SDK 与 Applet 配合生成二维码的过程，如图 3 所示，可以包括如下处理：

[72]首先，Applet 可以将芯片中存储的安全数据传给码处理组件 SDK。

[73]接着，SDK 对安全数据进行处理，根据安全数据生成待加签的码信息。该码信息中可以包括绑定了所述二维码显示设备的支付账号的账号标识，付款方扫码时就可以解析得到账号标识，并且支付服务器可以据此得到支付账号。

[74]最后，在 SE 芯片中，Applet 可以对码信息进行复杂化处理，例如，对码信息混合时间戳或者随机数的至少一种；并对复杂处理后的码信息进行显码处理，并使用私钥进行加签，加签后的码信息就可以转换成二维码进行显示了。其中，Applet 在使用私钥前，

可以先确定该私钥是否可用，如果不可用（比如，未标记为可用状态），则可以拒绝加签，以防止可能发生的交易风险。

[75]在加签后，芯片可以将加签后的码信息发送给二维码显示设备的嵌入式系统，以使得设备操作系统将码信息显示成二维码，在显示屏上进行显示，该二维码中也包括了账号标识。通过将二维码的生成放入 SE 芯片中进行黑盒处理，提高了二维码的安全性，使得二维码信息很难被篡改。

[76]此外，生成的二维码是动态二维码，该动态二维码生成的实现，如下列举两种示例的二维码刷新机制：

[77]例如，可以是定时刷新，图 3 示例的是一次二维码的生成过程，那么可以在每隔预设的时间段后，安全芯片将码种子传给二维码显示设备中的码处理组件 SDK，然后依次执行图 3 中的各个处理，生成二维码进行显示。比如，每间隔时间 t ，就执行一次图 3 的流程。

[78]又例如，还可以是事件触发二维码刷新。每次一个付款方扫描了设备上的收款码后，将向支付服务器发送支付交易请求，请求付款。设备的安全芯片可以在接收到支付服务器发送的码刷新通知后，将安全数据传给二维码显示设备中的码处理组件 SDK，开始新的一次二维码生成。所述码刷新通知是支付服务器在接收到扫码事件触发时发送，比如，一个付款方在扫码付款时，一扫码将通知支付服务器，支付服务器接收到扫码事件触发，则可以向 SE 芯片发送码刷新通知。那么，一个付款方付款后，设备上的收款码将刷新一次；另一个付款方付款后，设备上的收款码又将刷新一次，从而实现动态刷新。

[79]每次执行图 3 的二维码生成过程，生成的二维码可以不同，这种不同可以是：码处理组件根据安全数据生成的码信息是动态变化的，使得收款码对应变化；或者，安全芯片在对所述码信息进行加签时，对码信息混合动态变化的随机数或者时间戳，使得二维码对应变化。

[80]上述说明了二维码显示设备如何生成动态的二维码进行收款，在该收款码的生成过程中，使用了数字证书和电子签名，而且是动态的收款码。接着，图 4 示意了本说明书至少一个实施例中的支付服务器侧的支付处理，该支付处理可以是支付服务器收到了付款方扫描动态收款码发起的支付请求后执行，如图 4 所示，可以包括：

[81]在步骤 400 中，支付服务器接收付款方发送的支付交易请求，所述支付交易请求是付款方扫描二维码显示设备上的动态收款码后发送。

[82]例如，所述支付交易请求中可以携带：通过二维码显示设备上的安全芯片私钥加签的码信息，该码信息中可以含有唯一标识支付账号的账号标识。

[83]在步骤 402 中，支付服务器根据所述账号标识得到收款方的支付账号，并获取支付账号对应的公钥。

- 5 [84]例如，支付服务器可以查找预先存储的支付账号和公钥的对应关系，得到用于验签的公钥。

[85]在步骤 404 中，支付服务器对私钥加签的账号标识进行公钥验签。

[86]在步骤 406 中，支付服务器在验签通过后，根据支付账号进行支付交易处理。例如，由付款方的付款账号向商家的支付账号进行转账。

- 10 [87]由上述的支付交易方法的描述可以看到，在 SE 芯片中，主要的处理是由 Applet 来执行的。在收款码的生成过程中，Applet 所执行的处理可以是图 5 所示的流程，包括：

[88]在步骤 500 中，接收二维码显示设备传入的码信息。例如，可以是设备的嵌入式系统中的 SDK 传给 SE 芯片的码信息，或者还可以是位于 SE 芯片中的 SDK 发送的码信息。

- 15 [89]在步骤 502 中，在确认安全芯片中存储的私钥处于可用状态时，使用所述私钥对所述码信息进行加签；所述可用状态表示所述私钥已经获得了数字证书。

[90]在步骤 504 中，将加签后的码信息返回给二维码显示设备，以使得二维码显示设备将码信息显示成用于支付的二维码，所述二维码动态变化。

- 20 [91]此外，本说明书的至少一个实施例，还提供了一种二维码显示设备，该设备利用了数字证书和数字签名，来生成动态二维码，保证了二维码交易的安全性，并且，该二维码显示设备可以使得商家能够利用动态收款码进行收款，收款方便且安全。

[92]为了实现上述的支付二维码的生成方法，本说明书至少一个实施例提供了一种支付二维码的生成装置，该装置应用于二维码显示设备中的安全芯片。如图 6 所示，该装置可以包括：信息接收模块 61、签名处理模块 62 和显码发送模块 63。

- 25 [93]信息接收模块 61，用于接收待加签的码信息，所述码信息中包括绑定了所述二维码显示设备的支付账号的账号标识；

[94]签名处理模块 62，用于在确认安全芯片中存储的私钥处于可用状态时，使用所述私钥对码信息进行加签；所述可用状态表示私钥已经获得了数字证书；

[95]显码发送模块 63, 用于将加签后的码信息返回给二维码显示设备, 以使得二维码显示设备将码信息显示成用于支付的二维码, 所述二维码中包括所述账号标识, 且所述二维码动态变化。

5 [96]在一个例子中, 信息接收模块 61, 还用于接收支付服务器下发的安全数据, 所述安全数据是支付服务器根据二维码显示设备绑定的支付账号得到; 存储所述安全数据;

[97]所述显码发送模块 63, 还用于将所述安全数据传给二维码显示设备中的码处理组件 (SDK), 以使得所述码处理组件根据安全数据生成待加签的码信息。

10 [98]在一个例子中, 签名处理模块 62, 还用于生成公私钥对; 将公钥上传到所述支付服务器, 以使得所述支付服务器将公钥发往证书中心进行认证; 接收并存储支付服务器下发的数字证书, 所述数字证书表明所述公私钥对中的公钥已经被认证通过; 设置公私钥对中的私钥为所述可用状态。

[99]为了实现上述的支付交易方法, 本说明书至少一个实施例提供了一种支付交易装置, 该装置应用于支付服务器。如图 7 所示, 该装置可以包括: 请求接收模块 71 和交易处理模块 72。

15 [100] 请求接收模块 71, 用于接收支付交易请求, 所述支付交易请求是通过扫描二维码显示设备上的动态二维码后发送, 并且, 所述支付交易请求中携带通过解析该动态二维码得到的支付账号的账号标识, 所述账号标识经二维码显示设备上的安全芯片进行私钥加签;

20 [101] 交易处理模块 72, 用于在对所述支付账号的账号标识进行公钥验签通过后, 所述支付服务器根据支付账号的账号标识进行支付交易处理。

25 [102] 上述方法实施例中所示流程中的各个步骤, 其执行顺序不限制于流程图中的顺序。此外, 各个步骤的描述, 可以实现为软件、硬件或者其结合的形式, 例如, 本领域技术人员可以将其实现为软件代码的形式, 可以为能够实现所述步骤对应的逻辑功能的计算机可执行指令。当其以软件的方式实现时, 所述的可执行指令可以存储在存储器中, 并被设备中的处理器执行。

[103] 例如, 对应于上述方法, 本说明书一个或多个实施例同时提供一种支付二维码的显示设备, 所述设备包括: 安全芯片, 所述安全芯片中存储有安全数据, 所述安全数据由支付服务器根据二维码显示设备绑定的支付账号得到并下发至安全芯片; 所述安全芯片可以包括处理器、存储器、以及存储在存储器上并可在处理器上运行的计算机指令,

所述处理器通过执行所述指令，用于实现如下步骤：

[104] 接收待加签的码信息，所述码信息中包括绑定了所述二维码显示设备的支付账号的账号标识；且所述码信息是根据所述安全数据生成得到；

5 [105] 在确认安全芯片中存储的私钥处于可用状态时，使用所述私钥对所述码信息进行加签；所述可用状态表示所述私钥已经获得了数字证书；

[106] 将加签后的码信息返回给二维码显示设备，以使得二维码显示设备将码信息对应的用于支付的二维码在显示屏上显示，所述二维码中包括所述账号标识，且所述二维码动态变化。

10 [107] 例如，对应于上述方法，本说明书一个或多个实施例同时提供一种支付服务器，所述服务器包括处理器、存储器、以及存储在存储器上并可在处理器上运行的计算机指令，所述处理器通过执行所述指令，用于实现如下步骤：

[108] 接收支付交易请求，所述支付交易请求是通过扫描二维码显示设备上的动态二维码后发送，并且，所述支付交易请求中携带通过解析该动态二维码得到的支付账号的账号标识，所述账号标识经二维码显示设备上的安全芯片进行私钥加签；

15 [109] 在对所述支付账号的账号标识进行公钥验签通过后，所述支付服务器根据支付账号的账号标识进行支付交易处理。

20 [110] 上述实施例阐明的装置或模块，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。一种典型的实现设备为计算机，计算机的具体形式可以是个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件收发设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任意几种设备的组合。

[111] 为了描述的方便，描述以上装置时以功能分为各种模块分别描述。当然，在实施本说明书一个或多个实施例时可以把各模块的功能在同一个或多个软件和/或硬件中实现。

25 [112] 本领域内的技术人员应明白，本说明书一个或多个实施例可提供为方法、系统、或计算机程序产品。因此，本说明书一个或多个实施例可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本说明书一个或多个实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

[113] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中,使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品,该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

- 5 [114] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上,使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理,从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

- 10 [115] 还需要说明的是,术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含,从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素,而且还包括没有明确列出的其他要素,或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

- 15 [116] 本说明书一个或多个实施例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说明书一个或多个实施例,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。

- 20 [117] 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,对于数据采集设备或者数据处理设备实施例而言,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。

- 25 [118] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下,在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外,在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中,多任务处理和并行处理也是可以的或者可能是有利的。

[119] 以上所述仅为本说明书一个或多个实施例的较佳实施例而已,并不用以限制本

公开，凡在本公开的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本公开保护的范围之内。

权利要求书

1、一种支付二维码的生成方法，所述方法由二维码显示设备中的安全芯片执行，所述方法包括：

5 接收待加签的码信息，所述码信息中包括绑定了所述二维码显示设备的支付账号的账号标识；

在确认安全芯片中存储的私钥处于可用状态时，使用所述私钥对所述码信息进行加签；所述可用状态表示所述私钥已经获得了数字证书；

将加签后的码信息返回给二维码显示设备，以使得二维码显示设备将码信息显示成用于支付的二维码，所述二维码中包括所述账号标识，且所述二维码动态变化。

10 2、根据权利要求 1 所述的方法，在所述接收待加签的码信息之前，所述方法还包括：

接收支付服务器下发的安全数据，所述安全数据是支付服务器根据二维码显示设备绑定的支付账号得到；

存储所述安全数据；

15 将所述安全数据传给二维码显示设备中的码处理组件，以使得所述码处理组件根据所述安全数据生成待加签的码信息。

3、根据权利要求 2 所述的方法，所述将所述安全数据传给二维码显示设备中的码处理组件，包括：

在每隔预设的时间段后，将所述安全数据传给所述码处理组件；

20 或者，在接收到支付服务器发送的码刷新通知后，将所述安全数据传给二维码显示设备中的码处理组件，所述码刷新通知是支付服务器在接收到扫码事件触发时发送。

4、根据权利要求 2 所述的方法，所述接收支付服务器下发的安全数据之前，所述方法还包括：

生成公私钥对；

25 将公钥上传到所述支付服务器，以使得所述支付服务器将公钥发往证书中心进行认证；

接收并存储支付服务器下发的数字证书，所述数字证书表明所述公私钥对中的公钥已经被认证通过；

设置公私钥对中的私钥为所述可用状态。

30 5、根据权利要求 2 所述的方法，所述二维码动态变化，包括：

所述码处理组件根据安全数据生成的码信息动态变化，使得二维码对应变化；或者，

安全芯片在对所述码信息进行加签时,对码信息混合动态变化的随机数或者时间戳,使得二维码对应变化。

6、一种支付交易方法,所述方法由支付服务器执行,所述方法包括:

5 接收支付交易请求,所述支付交易请求是通过扫描二维码显示设备上的动态二维码后发送,并且,所述支付交易请求中携带通过解析该动态二维码得到的支付账号的账号标识,所述账号标识经二维码显示设备上的安全芯片进行私钥加签;

在对所述支付账号的账号标识进行公钥验签通过后,根据支付账号的账号标识进行支付交易处理。

7、根据权利要求6所述的方法,所述方法还包括:查找预先存储的对应关系,得到与
10 所述支付账号对应的公钥。

8、一种支付二维码的生成装置,所述装置应用于二维码显示设备中的安全芯片,所述装置包括:

信息接收模块,用于接收待加签的码信息,所述码信息中包括绑定了所述二维码显示设备的支付账号的账号标识;

15 签名处理模块,用于在确认安全芯片中存储的私钥处于可用状态时,使用所述私钥对码信息进行加签;所述可用状态表示所述私钥已经获得了数字证书;

显码发送模块,用于将加签后的码信息返回给二维码显示设备,以使得二维码显示设备将码信息显示成用于支付的二维码,所述二维码中包括所述账号标识,且所述二维码动态变化。

20 9、根据权利要求8所述的装置,

所述信息接收模块,还用于接收支付服务器下发的安全数据,所述安全数据是支付服务器根据二维码显示设备绑定的支付账号得到;存储所述安全数据;

所述显码发送模块,还用于将所述安全数据传给二维码显示设备中的码处理组件,以使得所述码处理组件根据所述安全数据生成待加签的码信息。

25 10、根据权利要求8所述的装置,

所述签名处理模块,还用于生成公私钥对;将公钥上传到所述支付服务器,以使得所述支付服务器将公钥发往证书中心进行认证;接收并存储支付服务器下发的数字证书,所述数字证书表明所述公私钥对中的公钥已经被认证通过;设置公私钥对中的私钥为所述可用状态。

30 11、一种支付交易装置,所述装置应用于支付服务器,所述装置包括:

请求接收模块,用于接收支付交易请求,所述支付交易请求是通过扫描二维码显示

设备上的动态二维码后发送,并且,所述支付交易请求中携带通过解析该动态二维码得到的支付账号的账号标识,所述账号标识经二维码显示设备上的安全芯片进行私钥加签;

交易处理模块,用于在对所述支付账号的账号标识进行公钥验签通过后,根据支付账号的账号标识进行支付交易处理。

- 5 12、一种支付二维码的显示设备,所述设备包括:安全芯片,所述安全芯片中存储有安全数据,所述安全数据由支付服务器根据二维码显示设备绑定的支付账号得到并下发至安全芯片;

所述安全芯片包括存储器、处理器,以及存储在存储器上并可在处理器上运行的计算机指令,所述处理器执行指令时实现以下步骤:

- 10 接收待加签的码信息,所述码信息中包括绑定了所述二维码显示设备的支付账号的账号标识;且所述码信息是根据所述安全数据生成得到;

在确认安全芯片中存储的私钥处于可用状态时,使用所述私钥对所述码信息进行加签;所述可用状态表示所述私钥已经获得了数字证书;

- 15 将加签后的码信息返回给二维码显示设备,以使得二维码显示设备将码信息对应的用于支付的二维码在显示屏上显示,所述二维码中包括所述账号标识,且所述二维码动态变化。

13、一种支付服务器,所述服务器包括存储器、处理器,以及存储在存储器上并可在处理器上运行的计算机指令,所述处理器执行指令时实现以下步骤:

- 20 接收支付交易请求,所述支付交易请求是通过扫描二维码显示设备上的动态二维码后发送,并且,所述支付交易请求中携带通过解析该动态二维码得到的支付账号的账号标识,所述账号标识经二维码显示设备上的安全芯片进行私钥加签;

在对所述支付账号的账号标识进行公钥验签通过后,根据支付账号的账号标识进行支付交易处理。