(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 109409472 B
(45)授权公告日 2022.11.22

(21)申请号 201810974011.8
(22)申请日 2018.08.24
(65)同一申请的已公布的文献号
申请公布号 CN 109409472 A
(43)申请公布日 2019.03.01
(73)专利权人 创新先进技术有限公司
地址 开曼群岛大开曼岛乔治镇医院路27号开曼企业中心
(72)发明人 黄琪 赵生波 廖晖 王志伟 魏亚文
(74)专利代理机构 北京众达德权知识产权代理有限公司 11570
专利代理师 刘杰
(51)Int.Cl.
G06K 19/06(2006.01)
G06K 19/073(2006.01)

(56)对比文件
CN 106100850 A,2016.11.09
CN 106100850 A,2016.11.09
CN 107146124 A,2017.09.08
CN 108023732 A,2018.05.11
CN 102779263 A,2012.11.14
CN 105024824 A,2015.11.04
US 2009261158 A1,2009.10.22

审查员 刘瑞

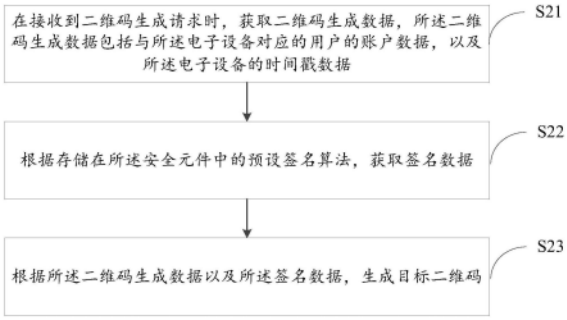
权利要求书4页 说明书9页 附图3页

(54)发明名称

二维码生成方法、数据处理方法、装置及服务器

(57)摘要

本发明公开一种二维码生成方法、数据处理方法、装置及服务器，所述二维码生成方法应用于电子设备中，所述电子设备设置有安全元件，在所述二维码生成方法中，获取二维码生成数据，以及通过存储在所述安全元件中的预设签名算法获取签名数据，根据所述二维码生成数据以及所述签名数据生成目标二维码，保证了目标二维码的安全。



CN 109409472 B

1.一种二维码生成方法,应用于电子设备中,所述电子设备设置有安全元件,所述方法包括:

在接收到基于定时更新任务生成的二维码生成请求时,获取动态的二维码生成数据,所述二维码生成数据包括与所述电子设备对应的用户的账户数据,以及所述电子设备的动态时间戳数据,所述动态时间戳数据用于表征二维码的动态生成时间;

根据存储在所述安全元件中的预设签名算法,获取签名数据;

根据所述二维码生成数据以及所述签名数据,生成动态的目标二维码;

其中,所述二维码为收款码或订单码或付款码;

电子设备在投入使用时进行入网操作,在设备入网的过程中,电子设备向可信服务管理服务器发送生成证书请求的指令,该指令中包含有该电子设备中设置的安全元件的标识,以用来唯一的表示发送请求的电子设备;可信服务管理服务器将生成证书请求的指令下发给该电子设备,以使该电子设备中的安全元件生成公私钥对,并将公私钥对与安全元件的标识进行关联;在安全元件生成公私钥对并与安全元件的标识关联之后,可信服务管理服务器向CA认证中心请求CA认证证书,CA认证中心生成证书文件,将证书进行存储,并将证书数据返回给可信服务管理服务器,可信服务管理服务器向电子设备下发写证书指令,电子设备将证书存储到安全元件中,以完成设备入网过程。

2.根据权利要求1所述的二维码生成方法,在根据所述存储在所述安全元件中的预设签名算法,获取签名数据之前,所述方法还包括:获取待签名数据;

所述根据存储在所述安全元件中的预设签名算法,获取签名数据,包括:根据所述预设签名算法,对所述待签名数据进行数字签名,获取所述签名数据。

3.根据所述权利要求2所述的二维码生成方法,所述预设签名算法为基于公钥基础设施的签名算法时,所述根据所述预设签名算法,对待签名数据进行数字签名,获取所述签名数据,包括:

获取所述安全元件生成的私钥;

根据所述私钥,对所述待签名数据进行数字签名,得到所述签名数据。

4.根据权利要求1所述的二维码生成方法,所述预设签名算法为基于一次性加密的签名算法时,所述根据存储在所述安全元件中的预设签名算法,获取签名数据,包括:

根据存储在所述安全元件中的共享秘钥,获得一次性加密口令,所述一次性加密口令为所述签名数据。

5.根据权利要求3所述的二维码生成方法,在所述根据所述私钥,对所述待签名数据进行数字签名,得到所述签名数据之后,所述方法还包括:根据存储在所述安全元件中的共享秘钥,生成一次性加密口令;

所述根据所述二维码生成数据以及所述签名数据,生成目标二维码,包括:根据所述二维码生成数据、所述签名数据以及所述一次性加密口令,生成所述目标二维码。

6.一种数据处理方法,所述数据处理方法包括:

接收目标电子设备扫描目标二维码得到的二维码扫描数据,其中,所述目标二维码为采用权利要求1-5任一项所述的方法生成的动态的二维码,所述二维码扫描数据中包括所述生成所述目标二维码的签名数据以及动态的二维码生成数据;

根据所述签名数据的签名方式,对所述签名数据进行验签,获得验签结果。

7.根据权利要求6所述的数据处理方法，所述签名方式为基于公钥基础设施的签名方式时，所述根据所述签名数据的签名方式，对所述签名数据进行验签，获得验签结果，包括：

根据与所述签名数据对应的公钥，对所述签名数据进行验签，获得验签结果。

8.根据权利要求6所述的数据处理方法，所述预设签名算法为基于一次性加密的签名方式时，所述根据所述签名数据的签名方式，对所述签名数据进行验签，获得验签结果，包括：

根据与所述签名数据对应的共享秘钥，获取目标一次性加密口令；

根据所述目标一次性加密口令，对所述签名数据进行验签，获得验签结果。

9.根据权利要求6所述的数据处理方法，所述接收目标电子设备扫描目标二维码得到的二维码扫描数据之后，所述方法还包括：

获取接收所述二维码扫描数据的目标时间戳数据；

获取所述二维码生成数据中的初始时间戳数据；

根据所述目标时间戳数据与所述初始时间戳数据之间的目标时间差，以及预设时间差，确定所述二维码是否有效，其中，在所述目标时间差小于或等于所述预设时间差时，确定所述目标二维码有效；在所述目标时间差大于所述预设时间差时，确定所述目标二维码无效。

10.根据权利要求9所述的数据处理方法，在所述目标二维码为收款码时，在所述获得验签结果之后，所述方法还包括：

在所述验签结果为验证成功时，获取所述二维码生成数据中的账户数据；

根据所述收款码对应的收款金额，对所述账户数据中的金额进行更新。

11.一种二维码生成装置，所述二维码生成装置设置有安全元件，所述二维码生成装置包括：

二维码生成数据获取模块，用于在接收到基于定时更新任务生成的二维码生成请求时，获取动态的二维码生成数据，所述二维码生成数据包括与电子设备对应的用户的账户数据，以及所述电子设备的动态时间戳数据，所述动态时间戳数据用于表征二维码的动态生成时间；

签名数据获取模块，用于根据存储在所述安全元件中的预设签名算法，获取签名数据；

二维码生成模块，用于根据所述二维码生成数据以及所述签名数据，生成动态的目标二维码；

其中，所述二维码为收款码或订单码或付款码；

电子设备在投入使用时进行入网操作，在设备入网的过程中，电子设备向可信服务管理服务器发送生成证书请求的指令，该指令中包含有该电子设备中设置的安全元件的标识，以用来唯一的表示发送请求的电子设备；可信服务管理服务器将生成证书请求的指令下发给该电子设备，以使该电子设备中的安全元件生成公私钥对，并将公私钥对与安全元件的标识进行关联；在安全元件生成公私钥对并与安全元件的标识关联之后，可信服务管理服务器向CA认证中心请求CA认证证书，CA认证中心生成证书文件，将证书进行存储，并将证书数据返回给可信服务管理服务器，可信服务管理服务器向电子设备下发写证书指令，电子设备将证书存储到安全元件中，以完成设备入网过程。

12.根据权利要求11所述的二维码生成装置，所述装置还包括：

第一获取模块，用于获取待签名数据；

所述签名数据获取模块，包括：

第二获取模块，用于根据所述预设签名算法，对所述待签名数据进行数字签名，获取所述签名数据。

13.根据所述权利要求12所述的二维码生成装置，所述预设签名算法为基于公钥基础设施的签名算法时，所述第一获取模块，包括：

私钥获取模块，用于获取所述安全元件生成的私钥；

第一处理模块，用于根据所述私钥，对所述待签名数据进行数字签名，得到所述签名数据。

14.根据权利要求11所述的二维码生成装置，所述预设签名算法为基于一次性加密的签名算法时，所述签名数据获取模块，包括：

第二处理模块，用于根据存储在所述安全元件中的共享秘钥，获得一次性加密口令，所述一次性加密口令为所述签名数据。

15.根据权利要求13所述的二维码生成装置，所述装置还包括：

第三处理模块，用于根据存储在所述安全元件中的共享秘钥，生成一次性加密口令；

所述二维码生成模块，包括：

第四处理模块，用于根据所述二维码生成数据、所述签名数据以及所述一次性加密口令，生成所述目标二维码。

16.一种数据处理装置，所述数据处理装置包括：

接收模块，用于接收目标电子设备扫描目标二维码得到的二维码扫描数据，其中，所述目标二维码为采用权利要求1-5任一项所述的方法生成的动态的二维码，所述二维码扫描数据中包括所述生成所述目标二维码的签名数据以及动态的二维码生成数据；

处理模块，用于根据所述签名数据的签名方式，对所述签名数据进行验签，获得验签结果。

17.根据权利要求16所述的数据处理装置，所述签名方式为基于公钥基础设施的签名方式时，所述处理模块，包括：

第一处理模块，用于根据与所述签名数据对应的公钥，对所述签名数据进行验签，获得验签结果。

18.根据权利要求16所述的数据处理装置，所述预设签名算法为基于一次性加密的签名方式时，所述处理模块，包括：

第一获取模块，用于根据与所述签名数据对应的共享秘钥，获取目标一次性加密口令；

第二处理模块，用于根据所述目标一次性加密口令，对所述签名数据进行验签，获得验签结果。

19.根据权利要求16所述的数据处理装置，所述数据处理装置还包括：

第二获取模块，用于获取接收所述二维码扫描数据的目标时间戳数据；

第三获取模块，用于获取所述二维码生成数据中的初始时间戳数据；

第三处理模块，用于根据所述目标时间戳数据与所述初始时间戳数据之间的目标时间差，以及预设时间差，确定所述二维码是否有效，其中，在所述目标时间差小于或等于所述预设时间差时，确定所述目标二维码有效；在所述目标时间差大于所述预设时间差时，确定

所述目标二维码无效。

20.根据权利要求19所述的数据处理装置,所述装置还包括:

第四获取模块,用于在所述验签结果为验证成功时,获取所述二维码生成数据中的账户数据;

第四处理模块,用于根据所述收款码对应的收款金额,对所述账户数据中的金额进行更新。

21.一种二维码生成装置,包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序,所述处理器执行所述程序时实现权利要求1-5任一项所述方法的步骤。

22.一种服务器,包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序,所述处理器执行所述程序时实现权利要求6-10任一项所述方法的步骤。

23.一种计算机可读存储介质,其上存储有计算机程序,该程序被处理器执行时实现权利要求1-10任一项所述方法的步骤。

二维码生成方法、数据处理方法、装置及服务器

技术领域

[0001] 本发明涉及计算机技术领域，尤其涉及一种二维码生成方法、数据处理方法、装置及服务器。

背景技术

[0002] 二维码是通过某种特定的几何图形按照一定规律，在平面上形成的黑白相间的图形来记录数据符号信息。随着科学技术的不断发展，二维码得到了越来越广泛的应用。例如在收付款时，可以通过扫描收款二维码和付款二维码来完成交易。但是二维码数据是以明文进行存储的，容易受到攻击者的篡改、攻击等。

发明内容

[0003] 本说明书实施例提供及一种二维码生成方法、数据处理方法、装置及服务器。

[0004] 第一方面，本说明书实施例提供一种二维码生成方法，应用于电子设备中，所述电子设备设置有安全元件，所述方法包括：

[0005] 在接收到二维码生成请求时，获取二维码生成数据，所述二维码生成数据包括与所述电子设备对应的用户的账户数据，以及所述电子设备的时间戳数据；

[0006] 根据存储在所述安全元件中的预设签名算法，获取签名数据；

[0007] 根据所述二维码生成数据以及所述签名数据，生成目标二维码。

[0008] 第二方面，本说明书实施例提供一种数据处理方法，所述数据处理方法包括：

[0009] 接收目标电子设备扫描目标二维码得到的二维码扫描数据，其中，所述目标二维码为采用权利要求1-5任一项所述的方法生成的二维码，所述二维码扫描数据中包括所述生成所述目标二维码的签名数据以及二维码生成数据；

[0010] 根据所述签名数据的签名方式，对所述签名数据进行验签，获得验签结果。

[0011] 第三方面，本说明书实施例提供一种二维码生成装置，所述二维码生成装置设置有安全元件，所述二维码生成装置包括：

[0012] 二维码生成数据获取模块，用于在接收到二维码生成请求时，获取二维码生成数据，所述二维码生成数据包括与所述电子设备对应的用户的账户数据，以及所述电子设备的时间戳数据；

[0013] 签名数据获取模块，用于根据存储在所述安全元件中的预设签名算法，获取签名数据；

[0014] 二维码生成模块，用于根据所述二维码生成数据以及所述签名数据，生成目标二维码。

[0015] 第四方面，本说明书实施例提供一种数据处理装置，包括：

[0016] 接收模块，用于接收目标电子设备扫描目标二维码得到的二维码扫描数据，其中，所述目标二维码为采用权利要求1-5任一项所述的方法生成的二维码，所述二维码扫描数据中包括所述生成所述目标二维码的签名数据以及二维码生成数据；

[0017] 处理模块，用于根据所述签名数据的签名方式，对所述签名数据进行验签，获得验签结果。

[0018] 第五方面，本说明书实施例提供一种二维码生成装置，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行第一方面所述的二维码生成方法的步骤。

[0019] 第六方面，本说明书实施例提供一种服务器，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行第二方面所述的数据处理方法的步骤。

[0020] 第七方面，本说明书实施例提供一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现上述任一项所述方法的步骤。

[0021] 本说明书实施例有益效果如下：

[0022] 在本说明书实施例中，在接收到二维码生成请求时，获取二维码生成数据，所述二维码生成数据包括与所述电子设备对应的用户的账户数据，以及所述电子设备的时间戳数据；根据存储在所述安全元件中的预设签名算法，获取签名数据；根据所述二维码生成数据以及所述签名数据，生成目标二维码。上述方案中，由于安全元件能够提供独立的运行空间，保证数据安全，通过存储在安全元件中的预设签名算法进行数字签名数据，并基于二维码生成数据以及数字签名数据生成目标二维码，保证了目标二维码的安全，另外，只有在目标二维码被认证中心验签成功时，才表明目标二维码未被篡改，因此有效的保证了数据传输的安全。

附图说明

[0023] 通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

[0024] 图1为本说明书实施例提供的数据处理方法的应用场景示意图；

[0025] 图2为本说明书实施例第一方面提供的一种二维码生成方法的流程图；

[0026] 图3为本说明书实施例第二方面提供的一种数据处理方法的流程图；

[0027] 图4为本说明书实施例第三方面提供的一种二维码生成装置的示意图；

[0028] 图5为本说明书实施例第四方面提供的一种数据处理装置的示意图；

[0029] 图6为本说明书实施例示出的一种服务器的示意图。

具体实施方式

[0030] 为了更好的理解上述技术方案，下面通过附图以及具体实施例对本说明书实施例的技术方案做详细的说明，应当理解本说明书实施例以及实施例中的具体特征是对本说明书实施例技术方案的详细的说明，而不是对本说明书技术方案的限定，在不冲突的情况下，本说明书实施例以及实施例中的技术特征可以相互组合。

[0031] 第一方面，本说明书实施例提供一种二维码生成方法，如图1所示，为本说明书实施例提供的数据处理方法的应用场景示意图。图1中，终端设备可以为支付机具、二维码生成器等设备。终端设备的个数可以为多个，每个终端设备均与服务器通信连接。在每个终端

设备中，均可以设置有安全元件 (Secure Element，SE)，通过安全元件获取生成二维码的数据。由于安全元件提供了与设备中微控制单元(Microcontroller Unit，MCU)隔离的运行空间，所以运行或存储在安全元件上的程序及数据不能被攻击者读取或篡改，保证了数据的安全性。终端设备还可以设置有显示单元，能够进行二维码显示。

[0032] 扫码设备可以为手机、平板电脑等设备，用于对终端设备显示的二维码进行扫描，获得扫码结果。扫码设备还可以将扫码结果发送至服务器，以使服务器对扫码结果进行验签，确定该二维码是否被篡改。

[0033] 服务器可以包括CA认证中心服务器、TSM(Trusted Service Management，可信服务管理)服务器等。其中，CA认证中心服务器可以对接收到的扫描数据进行验签，TSM服务器可以对终端设备上的安全元件进行管理，如完成安全元件的初始化、终端设备入网等。

[0034] 如图2所示，为本说明书实施例提供的一种二维码生成方法的流程图，该方法应用于一电子设备中，电子设备内设置有安全元件，该方法包括以下步骤。

[0035] 步骤S21：在接收到二维码生成请求时，获取二维码生成数据，所述二维码生成数据包括与所述电子设备对应的用户的账户数据，以及所述电子设备的时间戳数据；

[0036] 本说明书实施例中，电子设备可以为支付机具、二维码生成器等设备，电子设备内设置有安全元件。二维码可以为收款码、订单码、付款码等，二维码生成请求可以是定时请求，也可以是通过用户的操作触发生成的请求。在一个实施例中，电子设备为支付机具，二维码为收款码，收款码生成请求可以由定时更新任务来发送，例如，每隔1min发送一次收款码更新请求。在另一实施例中，支付机具可以设置有用于显示二维码的操作按键，当用户按下该操作按键后，发送二维码生成请求。当然还可以通过其他方式发送二维码生成请求，如在当前二维码被扫描之后，可以发送二维码生成请求，以更新二维码。

[0037] 本说明书实施例中，二维码生成数据可以保存在电子设备的安全元件中，也可以保存在安全元件以外的存储空间内。二维码生成数据包括与电子设备对应的用户的账户数据，以及电子设备的时间戳数据，当然，二维码生成数据还可以包括其他数据，这里不做限定。时间戳数据能够表明电子设备的时间信息，可以对二维码的生成时间进行标记，由于时间戳数据是实时变化的，进而使得二维码生成数据也为动态的，因此，根据二维码生成数据获得的二维码图形也是动态变化的。应理解的是，每个电子设备可以与用户的账户进行绑定，用户的账户数据可以是银行账户数据、支付宝账户数据等。在一个实施例中，当二维码为收款码时，用户的账户数据可以是用户的收款账号。

[0038] 步骤S22：根据存储在所述安全元件中的预设签名算法，获取签名数据；

[0039] 本说明书实施例中，电子设备在出厂前可以将预设签名算法写入安全元件中。预设签名算法可以根据实际需要进行选择，例如，PKI(Public Key Infrastructure，公钥基础设施)算法、HOTP(HMAC-based One-Time Password，基于HMAC算法加密的一次性密码)算法等，本说明书实施例不做限定。

[0040] 应理解的是，采用不同签名算法得到的签名数据也可以是不同的。另外，由于签名算法本身的特性，同一签名算法在每次进行数字签名的过程中，得到的签名数据也可以是不同的，例如，在预设签名算法为椭圆曲线公钥密码算法时，每次得到的签名数据是动态变化的。

[0041] 由于SE能够给数据提供安全的空间，在一个实施例中，数字签名的处理过程均可

以在SE中完成，生成签名数据。

[0042] 步骤S23：根据所述二维码生成数据以及所述签名数据，生成目标二维码。

[0043] 在获得了二维码生成数据以及签名数据之后，将这些数据转换为二维码图像，生成目标二维码。在一个实施例中，电子设备中可以保存有数据转换为二维码图像的对应模板，如二维码的版本信息、二维码的结构组成等，将二维码生成数据以及签名数据作为二维码的数据内容填充在二维码图像中的数据区域中，可以得到目标二维码。

[0044] 可选地，在根据所述存储在所述安全元件中的预设签名算法，获取签名数据之前，所述方法还包括：获取待签名数据；所述根据存储在所述安全元件中的预设签名算法，获取签名数据，包括：根据所述预设签名算法，对所述待签名数据进行数字签名，获取所述签名数据。

[0045] 本说明书实施例中，待签名数据可以根据实际需要进行设定，待签名数据可以保存在安全元件中，也可以是经过数据处理得到的。在一个实施例中，待签名数据可以是预设好的数据，在进行签名操作时直接读取。

[0046] 在另一个实施例中，根据所述二维码生成数据，生成与所述二维码生成数据对应的摘要数据，所述摘要数据为所述待签名数据。在该实施例中，在二维码生成数据的数据量较大时，为了减少数字签名的计算量，可以先对二维码生成数据进行处理，如通过对二维码生成数据进行哈希运算得到与二维码生成数据对应的摘要数据，然后再对摘要数据进行数字签名。当然也可以通过其他方式得到摘要数据，这里不做限定。

[0047] 可选地，所述预设签名算法为基于公钥基础设施的签名算法时，所述根据所述预设签名算法，对待签名数据进行数字签名，获取所述签名数据，包括：获取所述安全元件生成的私钥；根据所述私钥，对所述待签名数据进行数字签名，得到所述签名数据。

[0048] 本说明书实施例中，电子设备在投入使用时可以进行入网操作，在设备入网的过程中，电子设备可以向TSM服务器发送生成请求CSR(Cerificate Signing Request，证书请求)指令，该指令中包含有该电子设备中设置的SE 的标识，以用来唯一的表示发送请求的电子设备。TSM服务器将请求CSR指令下发给该电子设备，以使该电子设备中的SE生成公私钥对，并将公私钥对与SE的标识进行关联。在SE生成公私钥对并与SE的标识关联之后，TSM服务器向CA认证中心请求CA认证证书，CA认证中心根据SE生成的公钥以及其他信息生成证书文件，将证书进行存储，并将证书数据返回为TSM服务器，TSM服务器向电子设备下发写证书指令，电子设备将证书存储到SE 中，以完成设备入网过程。SE中保存有私钥和证书。

[0049] 当SE使用私钥对待签名数据进行签名时，SE可以直接读取私钥对待签名数据进行签名。对应的，当CA认证中心在对签名数据进行验签时，可以根据SE的标识，确定该SE生成的公钥，并利用该公钥对签名数据进行验签。

[0050] 在一个实施例中，待签名数据为二维码生成数据进行哈希运算得到的摘要信息，SE利用私钥对摘要信息进行数字签名，得到签名数据，将二维码生成数据以及签名数据转换为目标二维码。当扫码设备对目标二维码进行扫描后，获得扫码结果，扫码结果包括二维码生成数据以及签名数据。扫码设备将交扫码结果发送给CA认证中心，CA认证中心通过对二维码生成数据做哈希运算得到第一摘要数据，并利用SE的标识找到与该私钥对应的公钥，通过公钥对签名数据进行验签，得到第二摘要数据，当第一摘要数据与第二摘要数据相同时，表明该目标二维码为与SE的标识对应的电子设备生成的，未经过篡改。

[0051] 可选地，所述预设签名算法为基于一次性加密的签名算法时，所述预设签名算法为基于一次性加密的签名算法时，所述根据存储在所述安全元件中的预设签名算法，获取签名数据，包括：根据存储在所述安全元件中的共享秘钥，获得一次性加密口令，所述一次性加密口令为所述签名数据。

[0052] 本说明书实施例中，当预设签名算法为基于一次性加密的签名算法时，该签名算法可以为HTOP算法时。SE中可以存储有共享秘钥，该秘钥是SE 和认证服务器共享的。根据共享秘钥，可以生成一个一次性加密口令。在一个实施例中，电子设备中设置有一计数器，根据共享秘钥，以及计数器值，通过HMAC(Hash-based Message Authentication Code，哈希运算消息认证码) 运算，得到一次性加密口令。应理解的是，每次生成的一次性加密口令均是不同的，因此能够保证每次签名过程的安全性。同时，在认证服务器上，也会根据共享秘钥以及计数器值生成一个口令，当这个口令与SE生成的一次性加密口令相同时，则表明数据没有被篡改。

[0053] 当签名数据为一次性加密口令时，根据二维码生成数据以及一次性加密口令，生成目标二维码。

[0054] 可选地，在所述根据所述私钥，对所述待签名数据进行数字签名，得到所述签名数据之后，所述方法还包括：根据存储在所述安全元件中的共享秘钥，生成一次性加密口令；所述根据所述二维码生成数据以及所述签名数据，生成目标二维码，包括：根据所述二维码生成数据、所述签名数据以及所述一次性加密口令，生成所述目标二维码。

[0055] 本说明书实施例中，为了加强数据的安全性，可以先通过SE中存储的私钥对待签名数据进行数字签名，得到签名数据然后通过一次性加密口令对二维码生成数据以及签名数据进行加密保护。在生成目标二维码的过程中，将二维码生成数据、签名数据以及一次性加密口令进行处理，转换为目标二维码的图像信息。对应的，当认证服务器接收到该目标二维码数据时，先根据一次性加密口令对目标二维码数据进行解密，在根据公钥对待签名数据进行验签。

[0056] 在生成目标二维码时，可以根据电子设备中预设好的二维码信息来进行数据转换。二维码信息可以包括二维码的版本信息、二维码的结构信息等。在一个实施例中，可以将二维码生成数据、签名数据进行编码处理，得到数据码字序列，再进行纠错编码、分块处理、构造矩阵等步骤，得到最终的完整的目标序列，将完整的目标序列填充到相对的二维码矩阵区域中，得到目标二维码图像。

[0057] 第二方面，本说明书实施例提供一种数据处理方法，该数据处理方法可以应用于服务器侧。如图3所示，该数据处理方法包括以下步骤。

[0058] 步骤S31：接收目标电子设备扫描目标二维码得到的二维码扫描数据，其中，所述目标二维码为采用本说明书实施例中第一方面提供的二维码生成方法生成的二维码，所述二维码扫描数据中包括所述生成所述目标二维码的签名数据以及二维码生成数据；

[0059] 本说明书实施例中，目标电子设备可以是手机、平板电脑等能够扫描二维码的设备。目标二维码是采用本说明书实施例中第一方面提供的二维码生成方法生成的二维码。目标电子设备在扫描目标二维码之后，可以将目标二维码由图像信息转换成码字序列，并对码字序列进行处理，得到与目标二维码对应的签名数据以及二维码生成数据。二维码扫描数据可以是上述码字序列，也可以使处理后得到的二维码生成数据以及签名数据，还可

以是其他形式的数据，这里不做限定。目标电子设备将得到的二维码扫描数据发送给服务器，在一个实施例中，目标电子设备将二维码扫描数据发送给CA认证中心服务器。

[0060] 步骤S32：根据所述签名数据的签名方式，对所述签名数据进行验签，获得验签结果。

[0061] 由于签名数据可以是由不同的签名算法生成的，例如，PKI(Public Key Infrastructure，公钥基础设施)算法、HOTP(HMAC-based One-Time Password，基于HMAC算法加密的一次性密码)算法等。不同的签名方式，对应不同的验签方式。在一个实施例中，所述签名方式为基于公钥基础设施的签名方式时，所述根据所述签名数据的签名方式，对所述签名数据进行验签，获得验签结果，包括：根据与所述签名数据对应的公钥，对所述签名数据进行验签，获得验签结果。在另一实施例中，所述预设签名算法为基于一次性加密的签名方式时，所述根据所述签名数据的签名方式，对所述签名数据进行验签，获得验签结果，包括：根据与所述签名数据对应的共享秘钥，获取目标一次性加密口令；根据所述目标一次性加密口令，对所述签名数据进行验签，获得验签结果。由于上述两种验签方式在本说明书实施例的第一方面提供的二维码生成方法的实施例中进行了描述，此处就不做赘述了。

[0062] 另外，当二维码扫描数据表明该数据同时包含有一次性加密信息和签名信息时，根据目标一次性加密口令对二维码扫描数据进行解密，对解密后的数据使用对应的验签方式进行验签。

[0063] 可选地，所述接收目标电子设备扫描目标二维码得到的二维码扫描数据之后，所述方法还包括：获取接收所述二维码扫描数据的目标时间戳数据；获取所述二维码生成数据中的初始时间戳数据；根据所述目标时间戳数据与所述初始时间戳数据之间的目标时间差，以及预设时间差，确定所述二维码是否有效，其中，在所述目标时间差小于或等于所述预设时间差时，确定所述目标二维码有效；在所述目标时间差大于所述预设时间差时，确定所述目标二维码无效。

[0064] 为了保证数据的安全性，本说明书实施例中为二维码设置了有效时长，即在有效时长内二维码是有效的，超出了有效时长，二维码则无效。本说明书实施例中，二维码生成数据包括生成二维码时的初始时间戳数据，根据服务器接收到二维码扫描数据时的目标时间戳数据，目标时间戳数据与初始时间戳数据之间的目标时间差可以表示目标二维码的持续时间。预设时间差用来表示二维码的有效时长，可以根据实际需要进行设定，如30s、1min等。当目标时间差大于预设时间差时，表明目标二维码已经超时，确定目标二维码失效，反之，则表明目标二维码有效。

[0065] 可选地，在所述目标二维码为收款码时，在所述获得验签结果之后，所述方法还包括：在所述验证结果为验证成功时，获取所述二维码生成数据中的账户数据；根据所述收款码对应的收款金额，对所述账户数据中的金额进行更新。

[0066] 为了更好的理解本说明书实施例提供的方法，下面以二维码为收款码为例，对目标二维码的生成以及扫描过程进行说明。在该实施例中，电子设备为支付机具，二维码为收款码，二维码生成数据中的账户数据为该支付机具的使用用户的收款账户数据，电子设备内的SE中存储有PKI算法。目标电子设备为进行扫码的手机。服务器端包括CA认证中心服务器，以及交易平台，其中交易平台用于管理用户的账户数据。

[0067] 当支付机具接收到二维码生成请求时，获取收款账户数据，以及支付机具的时间

戳数据。SE通过PKI算法，使用私钥对收款账户数据以及时间戳数据进行数字签名，生成签名数据。将收款账户数据、时间戳数据以及签名数据进行处理，转换为目标二维码，并在支付机具上进行显示。

[0068] 当手机对支付机具上的目标二维码进行扫码时，获得二维码扫描数据(包括收款账户数据、时间戳数据以及签名数据)。同时，手机可以跳转至支付页面，手机用户在支付页面上填写支付的金额，填写完毕后，手机将二维码扫描数据以及支付金额发送至CA认证中心服务器。

[0069] CA认证中心服务器根据时间戳数据判断目标二维码是否有效，当目标二维码有效时，根据与支付机具对应的公钥，对签名数据进行验签。当验签成功时，可以将收款账户数据以及支付金额发送至交易平台，交易平台根据支付金额对收款账户中的总金额进行更新。

[0070] 第三方面，本说明书实施例提供一种二维码生成装置，如图4所示，所述二维码生成装置设置有安全元件，所述二维码生成装置包括：

[0071] 二维码生成数据获取模块41，用于在接收到二维码生成请求时，获取二维码生成数据，所述二维码生成数据包括与所述电子设备对应的用户的账户数据，以及所述电子设备的时间戳数据；

[0072] 签名数据获取模块42，用于根据存储在所述安全元件中的预设签名算法，获取签名数据；

[0073] 二维码生成模块43，用于根据所述二维码生成数据以及所述签名数据，生成目标二维码。

[0074] 在一种可选实现方式中，所述装置还包括：

[0075] 第一获取模块，用于获取待签名数据；

[0076] 所述签名数据获取模块，包括：

[0077] 第二获取模块，用于根据所述预设签名算法，对所述待签名数据进行数字签名，获取所述签名数据。

[0078] 在一种可选实现方式中，所述预设签名算法为基于公钥基础设施的签名算法时，所述第一获取模块，包括：

[0079] 私钥获取模块，用于获取所述安全元件生成的私钥；

[0080] 第一处理模块，用于根据所述私钥，对所述待签名数据进行数字签名，得到所述签名数据。

[0081] 在一种可选实现方式中，所述预设签名算法为基于一次性加密的签名算法时，签名数据获取模块42，包括：

[0082] 第二处理模块，用于根据存储在所述安全元件中的共享秘钥，获得一次性加密口令，所述一次性加密口令为所述签名数据。

[0083] 在一种可选实现方式中，所述装置还包括：

[0084] 第三处理模块，用于根据存储在所述安全元件中的共享秘钥，生成一次性加密口令；

[0085] 所述二维码生成模块，包括：

[0086] 第四处理模块，用于根据所述二维码生成数据、所述签名数据以及所述一次性加

密口令，生成所述目标二维码。

[0087] 关于上述装置，其中各个模块的具体功能已经在本发明实施例提供的二维码生成方法的实施例中进行了详细描述，此处将不做详细阐述说明。

[0088] 第四方面，本说明书实施例提供一种数据处理装置，如图5所示，所述数据处理装置包括：

[0089] 接收模块51，用于接收目标电子设备扫描目标二维码得到的二维码扫描数据，其中，所述目标二维码为采用本说明书实施例第一方面提供的二维码生成方法生成的二维码，所述二维码扫描数据中包括所述生成所述目标二维码的签名数据以及二维码生成数据；

[0090] 处理模块52，用于根据所述签名数据的签名方式，对所述签名数据进行验签，获得验签结果。

[0091] 可选地，所述签名方式为基于公钥基础设施的签名方式时，处理模块52，包括：

[0092] 第一处理模块，用于根据与所述签名数据对应的公钥，对所述签名数据进行验签，获得验签结果。

[0093] 可选地，所述预设签名算法为基于一次性加密的签名方式时，处理模块 52，包括：

[0094] 第一获取模块，用于根据与所述签名数据对应的共享秘钥，获取目标一次性加密口令；

[0095] 第二处理模块，用于根据所述目标一次性加密口令，对所述签名数据进行验签，获得验签结果。

[0096] 可选地，所述数据处理装置还包括：

[0097] 第二获取模块，用于获取接收所述二维码扫描数据的目标时间戳数据；

[0098] 第三获取模块，用于获取所述二维码生成数据中的初始时间戳数据；

[0099] 第三处理模块，用于根据所述目标时间戳数据与所述初始时间戳数据之间的目标时间差，以及预设时间差，确定所述二维码是否有效，其中，在所述目标时间差小于或等于所述预设时间差时，确定所述目标二维码有效；在所述目标时间差大于所述预设时间差时，确定所述目标二维码无效。

[0100] 可选地，所述装置还包括：

[0101] 第四获取模块，用于在所述验证结果为验证成功时，获取所述二维码生成数据中的账户数据；

[0102] 第四处理模块，用于根据所述收款码对应的收款金额，对所述账户数据中的金额进行更新。

[0103] 关于上述装置，其中各个模块的具体功能已经在本发明实施例提供的数据处理方法的实施例中进行了详细描述，此处将不做详细阐述说明。

[0104] 第五方面，基于与前述实施例中二维码生成方法同样的发明构思，本发明还提供一种二维码生成装置，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时实现前文所述二维码生成方法的任一方法的步骤。

[0105] 第六方面，基于与前述实施例中数据处理方法同样的发明构思，本发明还提供一种服务器，如图6所示，包括存储器604、处理器602及存储在存储器604上并可在处理器602上运行的计算机程序，所述处理器602执行所述程序时实现前文所述数据处理方法的任一

方法的步骤。

[0106] 其中，在图6中，总线架构(用总线600来代表)，总线600可以包括任意数量的互联的总线和桥，总线600将包括由处理器602代表的一个或多个处理器和存储器604代表的存储器的各种电路链接在一起。总线600还可以将诸如外围设备、稳压器和功率管理电路等之类的各种其他电路链接在一起，这些都是本领域所公知的，因此，本文不再对其进行进一步描述。总线接口606在总线600和接收器601和发送器603之间提供接口。接收器601 和发送器1103可以是同一个元件，即收发机，提供用于在传输介质上与各种其他装置通信的单元。处理器602负责管理总线600和通常的处理，而存储器604可以被用于存储处理器602在执行操作时所使用的数据。

[0107] 第七方面，基于与前述实施例中基于二维码生成方法以及数据处理方法的发明构思，本发明还提供一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现前文所述基于二维码生成方法以及数据处理方法的任一方法的步骤。

[0108] 本说明书是参照根据本说明书实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生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设备。

[0109] 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设备的制造品，该指令设备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。

[0110] 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。

[0111] 尽管已描述了本发明的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

[0112] 显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

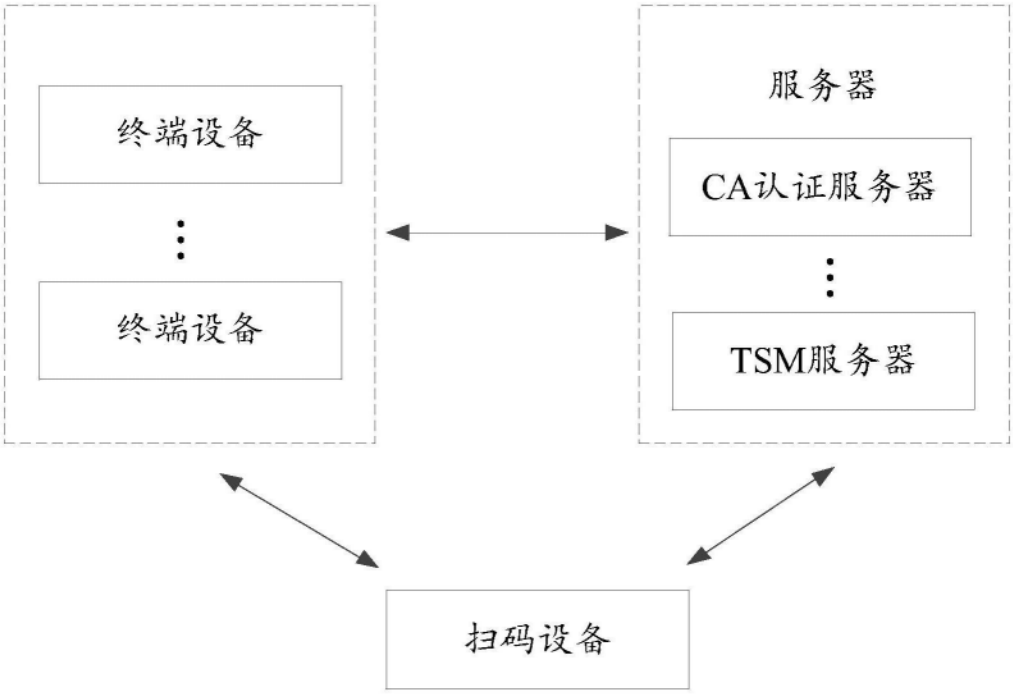

终端设备
终端设备
服务器
CA认证服务器
TSM服务器
扫码设备

图1

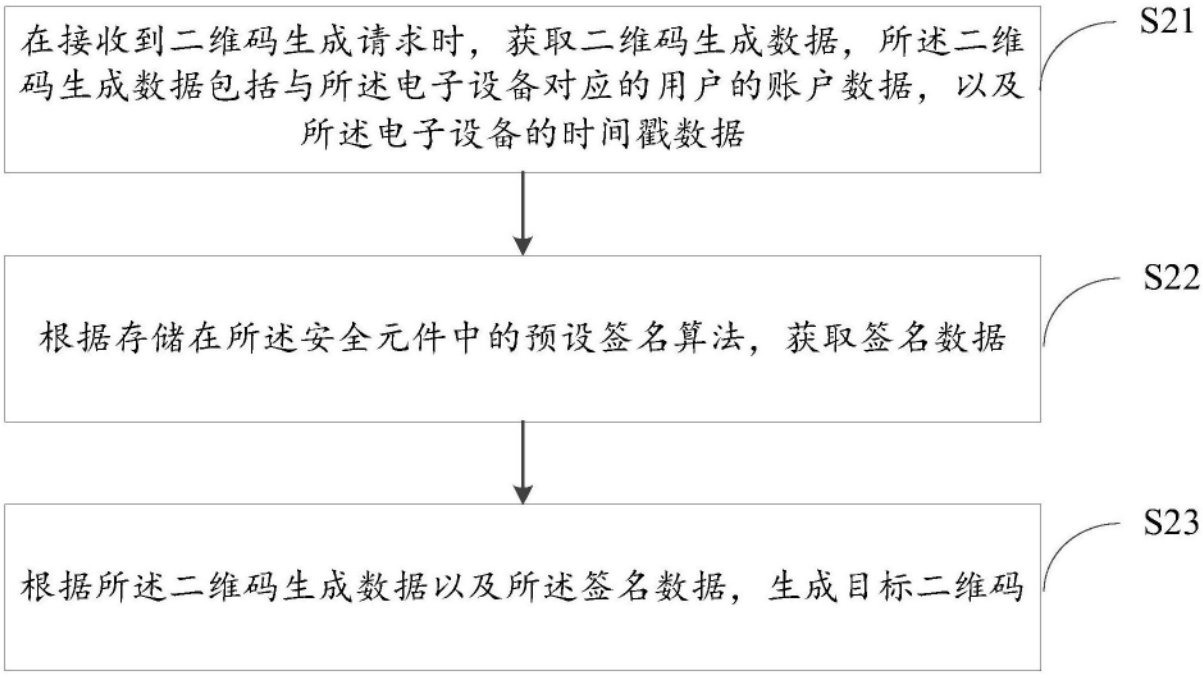

在接收到二维码生成请求时，获取二维码生成数据，所述二维码生成数据包括与所述电子设备对应的用户的账户数据，以及所述电子设备的时间戳数据
S21
根据存储在所述安全元件中的预设签名算法，获取签名数据
S22
根据所述二维码生成数据以及所述签名数据，生成目标二维码
S23

图2

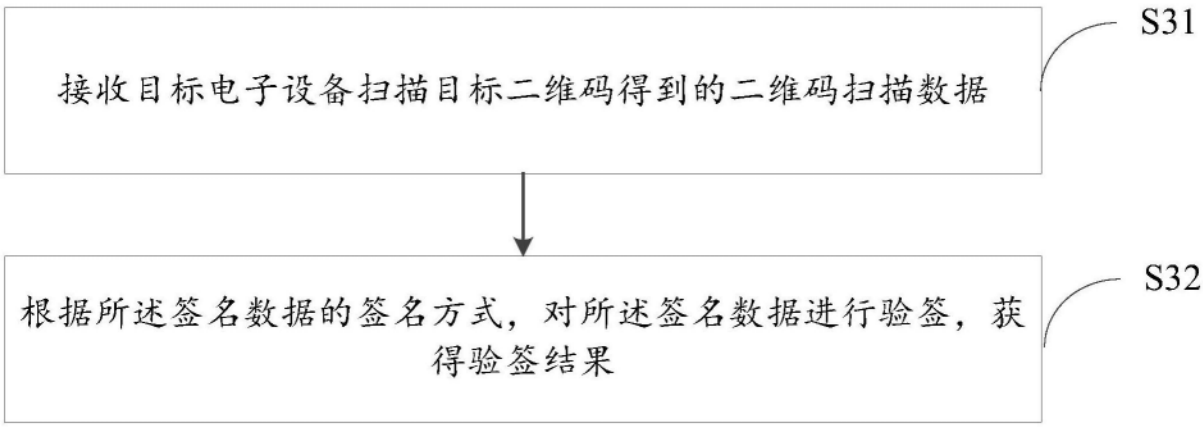

接收目标电子设备扫描目标二维码得到的二维码扫描数据
S31
根据所述签名数据的签名方式，对所述签名数据进行验签，获得验签结果
S32

图3


二维码生成装置
二维码生成数据获取模块41
签名数据获取模块42
二维码生成模块43

图4


数据处理装置
接收模块51
处理模块52

图5

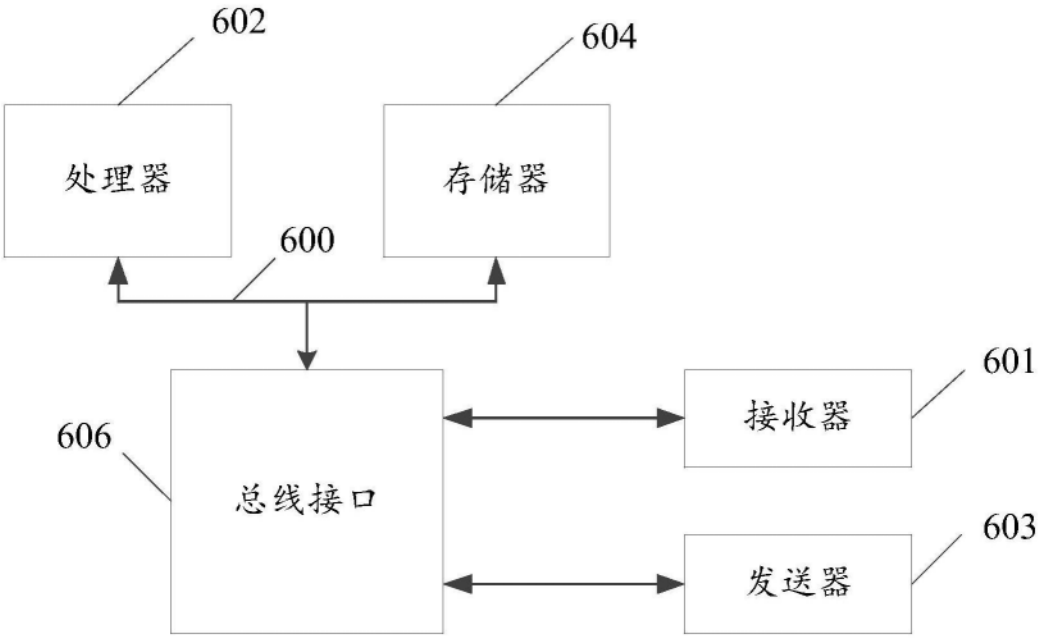

602
604
处理器
存储器
600
601
606
总线接口
接收器
603
发送器

图6