

一种给电子签名工具授权校验的方法、系统及电子签名工具

技术领域

5 本发明涉及信息安全领域，特别涉及一种给电子签名工具授权校验的方法及装置。

背景技术

10 目前，随着网上银行的普及，通过 USB（Universal Serial Bus，通用串行总线）接口与交易终端连接的电子签名工具也越来越多的被使用。现在使用电子签名的具体方法为，用户将电子签名工具与交易终端连接，交易终端接收交易指令与交易信息并生成相应的交易报文，将其发送给电子签名工具，电子签名工具从交易报文中提取特定的交易信息显示给用户，用户判断交易信息正确后，通过按下电子签名工具上的确认按钮启动电子签名生成、电子签名认证、加密及解密等处理并将结果发送给交易终端完成相应的电子交易。

15 但是目前无论是个人用户还是企业用户，对应账户的电子签名工具都只有一个，因此，现有的企业网银电子签名工具至少存在以下几个问题：

（1）企业网银电子签名工具以及交易密码均由同一个人保管，因此存在该保管人私自将公司账户转账的安全隐患。

20 （2）企业网银电子签名工具唯一且仅由一个人保管，则每次企业进行电子交易时，该保管人必须到场，否则无法完成此次交易，给企业带来极大的不方便。

发明内容

本发明旨在至少解决上述技术问题之一。

为此，本发明的第一个目的在于提出一种用于电子签名工具的授权校验方法。

25 本发明的第二个目的在于提出一种用于电子签名工具的授权校验系统。

本发明的第三个目的在于提出一种用于签名的电子签名工具。

本发明的第四个目的在于提出一种用于授权的电子签名工具。

本发明的第五个目的在于提出一种用于电子签名工具的授权校验系统。

本发明的第六个目的在于提出一种用于电子签名工具的授权校验方法。

30 本发明的第七个目的在于提出一种用于电子签名工具的授权校验系统。

为了实现上述目的，根据本发明的第一方面实施例的用于电子签名工具的授权校验方法包括以下步骤：第一电子签名工具向第二电子签名工具发送授权请求；所述第二电子签名工具根据所述授权请求生成相应的授权信息，并将所述授权信息反馈至所述第一电子签名工具；所述第一电子签名工具根据所述授权信息判断是否进入安全状态；以及如果判断进入安全状态，则所述第一电子签名工具打开签名功能。

35

根据本发明实施例的用于电子签名工具的授权校验方法，通过第二电子签名工具对第一电子签名工具进行授权，再通过第一电子签名工具对电子交易进行签名，可以在授权人不在身边时，交易人也可完成交易，提高了电子签名工具的使用方便性，同时降低了交易人私自对公司转账的风险，提高了公司电子交易的安全性。

5 为实现上述目的，本发明第二方面的实施例的一种用于电子签名工具的授权校验系统包括：所述第一电子签名工具，用于向所述第二电子签名工具发送授权请求，并根据所述第二电子签名工具反馈的授权信息判断是否进入安全状态，以及在判断进入安全状态之后，根据该次交易信息进行签名支付；所述第二电子签名工具，用于根据所述授权请求生成相应的授权信息，并将所述授权信息反馈至所述第一电子签名工具。

10 根据本发明实施例的用于电子签名工具的授权校验系统，通过第一电子签名工具向第二电子发送授权请求，第二电子签名工具返回授权信息给第一电子签名工具，再通过第一电子签名工作完成签名认证，因此可以在授权人与交易人不在同一地点时仍可完成交易，提高了电子签名工具的使用方便性，同时降低了交易人私自对公司转账的风险，提高了公司电子交易的安全性。

15 为实现上述目的，本发明第三方面的实施例的一种用于签名的电子签名工具包括：发送模块，用于向用于授权的电子签名工具发送授权请求；接收模块，用于接收所述用于授权的电子签名工具反馈的授权信息；以及状态控制模块，用于根据所述授权信息判断是否进入安全状态，以及在判断进入安全状态之后，进行签名支付。

20 根据本发明实施例的用于签名的电子签名工具，通过发送模块发送授权请求并通过接收模块接收授权信息，在通过状态控制模块来控制是否进入安全状态，提高了电子签名工具的安全性。

为实现上述目的，本发明第四方面的实施例的用于授权的电子签名工具包括：接收模块，用于接收用于签名的电子签名工具发送的授权请求；生成模块，用于根据所述授权请求生成相应的授权信息；以及发送模块，用于将所述授权信息反馈至所述用于签名的电子签名工具。

25 根据本发明实施例的用于授权的电子签名工具，通过接收模块接收授权请求，且通过生成模块生成相应的授权信息，并通过发送模块发送，提高了电子签名工具的安全性和可用性。

为实现上述目的，本发明第五方面的实施例的一种用于电子签名工具的授权校验系统包括：第一电子签名工具和第二电子签名工具，以及分别与所述第一电子签名工具和第二电子签名工具相连的第一终端和第二终端，且所述第一终端和所述第二终端之间相互通信，其中，所述第一电子签名工具，用于生成授权请求，并将所述授权请求发送至所述第一终端，并接收所述第一终端反馈的授权信息，以及在根据所述授权信息进入安全状态之后，进行签名支付；所述第一终端，用于将所述授权请求发送至所述第二终端，并将所述第二终端发送的授权信息转发至所述第一电子签名工具；所

述第二终端，用于将所述授权请求转发至所述第二电子签名工具，并将所述授权信息转发至所述第一终端；所述第二电子签名工具，用于根据所述授权请求生成相应的授权信息，并将所述授权信息发送至所述第二终端。

根据本发明实施例的用于电子签名工具的授权校验系统，通过在分别在第一终端、第二终端上连接的第一电子签名工具、第二电子签名工具来完成电子交易签名，并通过两个终端进行通信，提高了系统的易用性及安全性。

为实现上述目的，本发明第六方面的实施例的用于电子签名工具的授权校验方法包括以下步骤：第一电子签名工具需要执行签名功能时，通过互联网向第二电子签名工具发送包含请求信息的授权请求；所述第二签名工具对所述第一签名工具发送的授权请求进行授权，并将授权信息返回给第一签名工具；所述第一电子签名工具对所述授权信息解密后，将解密的授权信息与所述请求信息进行匹配验证，判断所述授权是否成功；如果判断所述授权成功，则打开安全状态；以及如果判断所述授权不成功，则所述安全状态无法打开。

根据本发明实施例的，通过第一电子签名工具发送授权请求，第二电子签名工具对第一电子签名工具授权，再由第一电子签名工具完成电子交易签名。提高了企业电子交易的安全性及方便性。

为实现上述目的，本发明第七方面的实施例的用于电子签名工具的授权校验系统包括：包括第一电子签名工具和第二电子签名工具，其中，所述第一电子签名工具，用于在电子交易签名时，向所述第二电子签名工具发送授权请求，并根据所述第二电子签名工具反馈的授权信息判断是否签名正确，并在签名正确时打开安全状态进行所述电子交易签名；所述第二电子签名工具，用于根据所述第一电子签名工具发送的所述授权请求生成相应的授权信息并返回给所述第一签名工具。

根据本发明实施例的用于电子签名工具的授权校验系统，通过第一电子签名工具发送授权请求，第二电子签名工具对第一电子签名工具授权，再由第一电子签名工具完成电子交易签名。提高了企业电子交易的安全性及方便性。

本发明的附加方面和优点将在下面的描述中部分给出，部分将从下面的描述中变得明显，或通过本发明的实践了解到。

附图说明

本发明上述的和/或附加的方面和优点从下面结合附图对实施例的描述中将变得明显和容易理解，其中：

图 1 为根据本发明一个实施例的一种用于电子签名工具的授权校验方法的流程图；
图 2 为根据本发明一个实施例的一种用于电子签名工具的授权校验方法的流程图；
图 3 为根据本发明一个实施例的一种用于电子签名工具的授权校验方法的流程图；
图 4 为根据本发明一个实施例的用于电子签名工具的授权校验系统的结构示意图；

图 5 为根据本发明一个实施例的用于签名的电子签名工具的结构示意图；
图 6 为根据本发明一个实施例的用于签名的电子签名工具的结构示意图；
图 7 为根据本发明一个实施例的用于签名的电子签名工具的结构示意图；
图 8 为根据本发明一个实施例的用于授权的电子签名工具的结构示意图；
图 9 为根据本发明一个实施例的用于电子签名工具的授权校验系统的结构示意图；
图 10 为根据本发明一个实施例的用于电子签名工具的授权校验方法的流程图；以及
图 11 为根据本发明一个实施例的用于电子签名工具的授权校验系统的结构示意图。

图。

具体实施方式

下面详细描述本发明的实施例，所述实施例的示例在附图中示出，其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的，仅用于解释本发明，而不能解释为对本发明的限制。参照下面的描述和附图，将清楚本发明的实施例的这些和其他方面。在这些描述和附图中，具体公开了本发明的实施例中的一些特定实施方式，来表示实施本发明的实施例的原理的一些方式，但是应当理解，本发明的实施例的范围不受此限制。相反，本发明的实施例包括落入所附加权利要求书的精神和内涵范围内的所有变化、修改和等同物。

下面参考说明书附图描述根据本发明实施例的用于电子签名工具的授权校验方法一种用于电子签名工具的授权校验方法，包括以下步骤：第一电子签名工具向第二电子签名工具发送授权请求；第二电子签名工具根据授权请求生成相应的授权信息，并将授权信息反馈至第一电子签名工具；第一电子签名工具根据授权信息判断是否进入安全状态；以及如果判断进入安全状态，则第一电子签名工具打开签名功能。

图 1 为本发明一个实施例的用于电子签名工具的授权校验方法的流程图。

如图 1 所示，根据本发明实施例的用于电子签名工具的授权校验方法包括下述步骤。

步骤 S101：第一电子签名工具向第二电子签名工具发送授权请求。
具体地，第一电子签名工具在电子交易时生成一个授权请求，并将该授权请求发送给第二电子签名工具。
步骤 S102：第二电子签名工具根据授权请求生成相应的授权信息，并将授权信息反馈至第一电子签名工具。
具体地，第二电子签名工具接收第一电子签名工具授权请求，对授权请求进行签名，在根据签名信息生成授权信息，返回给第一电子签名工具。
步骤 S103：第一电子签名工具根据授权信息判断是否进入安全状态。

在本发明的一个实施例中，授权请求包括第一电子签名工具生成的随机数，且授权信息包括第二电子签名工具根据随机数生成的签名信息。

具体地，首先第一电子签名工具对签名信息进行解密以生成解密信息；然后第一电子签名工具判断解密信息是否与其生成的随机数匹配；最后如果判断匹配，则第一电子签名工具进入安全状态。

更具体地，第一电子签名工具根据预设的密钥对第二电子签名工具返回的授权信息进行解码，将授权信息解密出一组数字，在将该组数字与当初第一电子签名工具中生成的授权请求中的随机数进行匹配对比，如果两组数据完全匹配，则判断授权签名成功，第一电子签名工具进入安全状态。

步骤 S104：如果判断进入安全状态，则第一电子签名工具打开签名功能。

具体地，如果第一电子签名工具进入安全状态，则可以进行对相关的电子交易进行签名认证完成交易。

在本发明的一个实施例中，第一电子签名工具和第二电子签名工具具有相匹配的密钥。

具体的，第一电子签名工具和第二电子签名工具可以采用对称密钥进行加密和/或解密，或者采用非对称密钥进行加密和/或解密。

更具体地，第一电子签名工具对第二电子签名工具返回的授权信息进行解密时则根据该密钥对签名信息进行解密，这个预设的电子签名工具中的密钥可以是对称和/或解密用的对称密钥，也可以是用于非对称和/或解密用的非对称密钥。

在本发明的一个实施例中，授权请求包括第一电子签名工具生成的随机数，且授权信息包括第二电子签名工具根据随机数生成的签名信息。

在本发明的一个实施例中，第一电子签名工具将随机数显示给用户，或者通过语音提示给用户

根据本发明实施例的用于电子签名工具的授权校验方法，通过第二电子签名工具对第一电子签名工具进行授权，再通过第一电子签名工具对电子交易进行签名，其中通过随机数来验证授权信息，可以在授权人不在身边时，交易人也可完成交易，提高了电子签名工具的使用方便性，同时降低了交易人私自对公司转账的风险，提高了公司电子交易的安全性。

图 2 为本发明又一个实施例的用于电子签名工具的授权校验方法的流程图。

如图 2 所示，根据本发明实施例的用于电子签名工具的授权校验方法包括下述步骤。

步骤 S201：第一电子签名工具向第二电子签名工具发送授权请求。

步骤 S202：将付款账户和/或支付金额在第二电子签名工具中显示。

具体地，在第二电子签名工具中会根据第一电子签名工具发来的授权请求获取该次电子交易的信息，并将其中付款账户和/或支付金额在其显示屏幕上显示。

步骤 S203: 第二电子签名工具根据授权请求生成相应的授权信息, 并将授权信息反馈至第一电子签名工具。

步骤 S204: 第一电子签名工具根据授权信息判断是否进入安全状态。

具体地, 第一电子签名工具根据密钥对签名信息进行解密以生成解密信息; 第一
5 电子签名工具判断解密信息是否与付款账户和/或支付金额匹配; 以及如果判断匹配, 则第一电子签名工具进入安全状态。

更具体地, 第一电子签名工具根据预设的密钥对第二电子签名工具返回的授权信息进行解码, 将授权信息解密出一组信息, 在将该组信息与当初第一电子签名工具中授权请求中的信息进行匹配对比, 如果两组信息完全匹配, 则判断授权签名成功, 第
10 一电子签名工具进入安全状态。

步骤 S205: 如果判断进入安全状态, 则第一电子签名工具打开签名功能。

上述步骤 S201、S203 和 S205 的具体实现过程可参见步骤 S101 S102 和 S104 的描述, 此处不再详细介绍。

在本发明的一个实施例中, 授权请求包括此次交易相关的付款账户和/或支付金额,
15 且授权信息包括第二电子签名工具根据付款账户和/或支付金额生成的签名信息。

具体地, 在第一电子签名工具中生成授权请求时将该次电子交易的付款账户和支付金额信息添加到授权请求中, 而第二电子签名工具在生成授权信息时则根据付款账户和/或支付金额生成相关的授权信息。

在本发明的一个实施例中, 第一电子签名工具进入安全状态之后, 第一电子签名
20 工具根据付款账户和/或支付金额进行与其匹配的交易签名, 完成签名后退出安全状态; 再次进行交易时, 若所需签名的交易的付款账户和/或支付金额与付款账户和/或支付金额不匹配, 则退出安全状态。

具体地, 第一电子签名工具进入安全状态之后, 会根据授权信息中包含的付款账户和/或支付金额与实际需要签名的付款账户和/或支付金额进行匹配对比, 如果匹配相
25 同, 则对该交易进行签名, 并退出安全状态, 当再次交易需要再次签名的时候, 如果该次需要签名的交易的付款账户和/或支付金额与之前接收的授权信息中包含的付款账户和/或支付金额不匹配, 则自动退出安全状态。

根据本发明实施例的用于电子签名工具的授权校验方法, 在第一电子签名工具与第二电子签名工具的交互信息中包含了电子交易的信息, 并能通过第二电子签名工具
30 展示给授权人, 能通过电子交易信息匹配对比来控制安全状态的退出, 使电子签名工具更加人性化且增加了电子签名工具的易用性与安全性。

图 3 为本发明又一个实施例的用于电子签名工具的授权校验方法的流程图。

如图 3 所示, 根据本发明实施例的用于电子签名工具的授权校验方法包括下述步骤。

35 步骤 S301: 第一电子签名工具向第二电子签名工具发送授权请求。

步骤 S302: 将付款账户和/或支付金额在第二电子签名工具中显示。

步骤 S303: 第二电子签名工具根据授权请求生成相应的授权信息, 并将授权信息反馈至第一电子签名工具。

步骤 S304: 第一电子签名工具根据授权信息判断是否进入安全状态。

5 步骤 S305: 如果判断进入安全状态, 则第一电子签名工具打开签名功能。

上述步骤 S301 到 S305 的具体实现过程可参见步骤 S201 到 S205 的描述, 此处不再详细介绍。

步骤 S306: 第一电子签名工具在预设时间之后退出安全状态。

10 具体地, 在第一电子签名工具进入安全状态后, 超过预定的时间后, 则退出安全状态, 无法继续再进行签名。

步骤 S307: 或者, 第一电子签名工具在掉电之后退出安全状态。

具体地, 在第一电子签名工具进入安全状态后, 在断开第一电子签名工具与交易终端连接后则第一电子签名工具掉电, 此时第一电子签名工具退出安全状态, 无法继续再进行签名。

15 步骤 S308: 或者, 第一电子签名工具在完成签名之后退出安全状态。

具体地, 在第一电子签名工具进入安全状态后, 在完成对应的电子交易的签名后, 此时第一电子签名工具退出安全状态, 无法继续再进行签名

20 在本发明的一个实施例中, 第一电子签名工具为多个, 且每个第一电子签名工具具有唯一的密钥, 第二电子签名工具具有与多个第一电子签名工具的密钥相匹配的多个密钥。

具体地, 第一电子签名工具可以有多个, 且每个第一电子签名工具中都预设有解密用的唯一的密钥, 可以提供给多个人在不同地方进行交易, 而第二电子签名工具中则存有所有第一电子签名工具中的密钥相匹配的密钥, 可以给不同的电子签名工具进行授权。

25 在本发明的一个实施例中, 第二电子签名工具为多个, 且每个第二电子签名工具具有唯一的密钥, 第一电子签名工具具有与多个第二电子签名工具的密钥相匹配的多个密钥, 第一电子签名工具分别向多个第二电子签名工具发送授权请求。

30 具体地, 第二电子签名工具可以有多个, 且每个第二电子签名工具中则存有与各个第一电子签名工具中的密钥相匹配的密钥, 可以给不同的电子签名工具进行授权, 如果第一电子签名工具收到全部第二电子签名工具的授权信息, 且授权信息均满足要求, 则第一电子签名工具进入安全状态; 或者, 如果第一电子签名工具收到任一个第二电子签名工具的授权信息, 且授权信息均满足要求, 则第一电子签名工具进入安全状态。

35 例如, 第一电子签名工具获得授权可以设定为必须收到所有第二电子签名工具授权才可进入安全状态, 也可以设定为收到一部分第二电子签名工具授权即可进入安全

状态,或者设定为收到一个第二电子签名工具授权就可进入安全状态。

在本发明的一个实施例中,第一电子签名工具和第二电子签名工具通过有线网络或无线网络或相互之间的直接连接进行通信。

具体地,第一电子签名工具可以通过网络向第二电子签名工具发送授权请求并接收授权信息,但也可通过本地直接连接来进行信息交互,无需通过网络传输。

5 在本发明的一个实施例中,第二电子签名工具具有USB插座,第一电子签名工具的USB插头插入USB插座以建立第一电子签名工具与第二电子签名工具的通信。

例如,如果授权人和交易人都在同一个地方则无需通过网络进行连接,可以直接将第一电子签名工具插入到第二电子签名工具的USB插座中,再将第二电子签名工具连接到交易终端上,即可直接授权给第一电子签名工具,使该第一电子签名工具有权

10 对该次电子交易进行签名。

根据本发明实施例的用于电子签名工具的授权校验方法,进入安全状态后,在一定条件下会退出安全状态,使电子签名工具更加人性化且增加了电子签名工具的易用性。

15 下面参考说明书附图描述根据本发明实施例的用于电子签名工具的授权校验系统。

一种包括用于电子签名工具的授权校验系统:包括第一电子签名工具和第二电子签名工具,其中,第一电子签名工具,用于向第二电子签名工具发送授权请求,并根据第二电子签名工具反馈的授权信息判断是否进入安全状态,以及在判断进入安全状态之后,进行签名支付;第二电子签名工具,用于根据授权请求生成相应的授权信息,并将授权信息反馈至第一电子签名工具。

图4为本发明一个实施例的用于电子签名工具的授权校验系统的结构示意图。

如图4所示,根据本发明实施例的用于电子签名工具的授权校验系统,包括:第一电子签名工具110和第二电子签名工具120。

25 具体地,第一电子签名工具110,用于向第二电子签名工具120发送授权请求,并根据第二电子签名工具120反馈的授权信息判断是否进入安全状态,以及在判断进入安全状态之后,进行签名支付;第二电子签名工具120,用于根据授权请求生成相应的授权信息,并将授权信息反馈至第一电子签名工具110。

在本发明的一个实施例中,第一电子签名工具110和第二电子签名工具120具有相匹配的密钥。

30 在本发明的一个实施例中,第一电子签名工具110还用于生成随机数,并将随机数添加至授权请求之中。

在本发明的一个实施例中,第二电子签名工具120还用于根据随机数生成签名信息。

35 在本发明的一个实施例中,第一电子签名工具110还用于将随机数显示给用户,

- 或者通过语音提示给用户。
- 在本发明的一个实施例中，第一电子签名工具 110 还用于根据密钥对签名信息进行解密以生成解密信息，并在判断解密信息与随机数匹配时，进入安全状态。
- 5 在本发明的一个实施例中，第一电子签名工具 110 还用于在接收该次交易信息之后，将该次交易相关的付款账户和/或支付金额添加至授权请求之中。
- 在本发明的一个实施例中，第二电子签名工具 120 还用于根据第二电子签名工具 120 根据付款账户和/或支付金额生成签名信息。
- 下面结合上述实施例详细说明本发明的用于电子签名工具的授权校验系统的工作流程。
- 10 例如，在电子交易需要签名时，将第一电子签名工具 110 连上交易终端，第一电子签名工具 110 接收该次交易信息，读取此次交易的交易信息，包括付款账户和/或支付金额，并生成一个随机数，将这些信息添加到授权请求中发送给第二电子签名工具 120，第二电子签名工具 120 接收授权请求，将授权请求中的一些信息展示给用户，如付款账户，交易支付金额及随机数，在授权人确认过交易信息后，第二电子签名工具 120 根据授权请求中的交易信息及随机数生成授权信息返回给第一电子签名工具 110，
- 15 第一电子签名工具 110 根据预设的密钥对授权信息进行解密，将解密后的到的信息与交易信息及随机数进行匹配对比，如果匹配则进入安全状态，可以对电子交易进行签名。
- 在本发明的一个实施例中，第一电子签名工具 110 在进入安全状态之后，还用于在满足以下任一条件时退出安全状态：超过预设时间；第一电子签名工具 110 掉电；
- 20 第一电子签名工具 110 完成对该次交易的签名。
- 具体地，如果在第一电子签名工具 110 进入安全状态，超过预定的时间后，则退出安全状态，无法继续进行签名；或者在第一电子签名工具 110 进入安全状态后，
- 25 在断开第一电子签名工具 110 与交易终端连接后则第一电子签名工具 110 掉电，此时第一电子签名工具 110 退出安全状态，无法继续进行签名；或者在第一电子签名工具 110 进入安全状态后，在完成对应的电子交易的签名后，此时第一电子签名工具 110 具 110 进入安全状态后，在完成对应的电子交易的签名后，此时第一电子签名工具 110 退出安全状态，无法继续进行签名。
- 30 在本发明的一个实施例中，第一电子签名工具 110 为多个，且每个第一电子签名工具 110 具有唯一的密钥，第二电子签名工具 120 具有与多个第一电子签名工具 110 的密钥相匹配的多个密钥。
- 在本发明的一个实施例中，第二电子签名工具 120 为多个，且每个第二电子签名工具 120 具有唯一的密钥，第一电子签名工具 110 具有与多个第二电子签名工具 120 的密钥相匹配的多个密钥，第一电子签名工具 110 分别向多个第二电子签名工具 120 发送授权请求。
- 35 在本发明的一个实施例中，如果第一电子签名工具 110 收到全部第二电子签名工

具 120 的授权信息，且授权信息均满足要求，则第一电子签名工具 110 进入安全状态；或者，如果第一电子签名工具 110 收到任一个第二电子签名工具 120 的授权信息，且授权信息均满足要求，则第一电子签名工具 110 进入安全状态；

5 在本发明的一个实施例中，第一电子签名工具 110 和第二电子签名工具 120 通过有线网络或无线网络或相互之间的直接连接进行通信。

具体地，第一电子签名工具可以通过网络向第二电子签名工具发送授权请求并接收授权信息，但也可通过本地直接连接来进行信息交互，无需通过网络传输。

10 在本发明的一个实施例中，第二电子签名工具 120 具有 USB 插座，第一电子签名工具 110 的 USB 插头插入 USB 插座之后建立第一电子签名工具 110 与第二电子签名工具 120 的通信。

根据本发明实施例的用于电子签名工具的授权校验系统，通过第一电子签名工具向第二电子签名工具发出授权请求，并执行签名，第一电子签名工具则确认信息并进行授权，保证了企业电子交易支付或转账的安全性及方便性。

下面参考说明书附图描述根据本发明实施例的用于签名的电子签名工具。

15 一种用于签名的电子签名工具，包括：发送模块，用于向用于授权的电子签名工具发送授权请求；接收模块，用于接收用于授权的电子签名工具反馈的授权信息；以及状态控制模块，用于根据授权信息判断是否进入安全状态，以及在判断进入安全状态之后，进行签名支付。

图 5 为本发明另一个实施例的用于签名的电子签名工具的结构示意图。

20 如图 5 所示，根据本发明实施例的用于签名的电子签名工具，包括：发送模块 210，接收模块 220，状态控制模块 230。

具体地，发送模块 210 用于向用于授权的电子签名工具发送授权请求；接收模块 220 用于接收用于授权的电子签名工具反馈的授权信息；以及状态控制模块 230 用于根据授权信息判断是否进入安全状态，以及在判断进入安全状态之后，进行签名支付。

25 在本发明的一个实施例中，用于签名的电子签名工具和用于授权的电子签名工具具有相匹配的密钥。

具体地，用于签名的电子签名工具通过接收模块 220 接收到授权信息并通过上述的相匹配的密钥对授权信息进行解密，获取授权信息解密后的信息。

30 根据本发明实施例的用于签名的电子签名工具，发送模块和接收模块与用于授权的电子签名工具交互，并通过状态控制模块来判断控制是否进入安全状态，增加了电子签名工具的易用性与安全性。

图 6 为本发明另一个实施例的用于签名的电子签名工具的结构示意图。

如图 6 所示，根据本发明实施例的用于签名的电子签名工具，还包括：生成模块 240、添加模块 250 和提示模块 260。

35 具体地，生成模块 240 用于生成随机数；添加模块 250 用于将随机数添加至授权

请求之中；提示模块 260 用于将随机数显示给用户，或者通过语音提示给用户。

更具体地，该用于签名的电子签名工具通过生成模块 240 生成的随机数在通过添加模块 250 添加到授权请求后，会通过发送模块 210 发送给用于授权的电子签名工具，并通过提示模块 260 将该随机数展示给用户或者直接语音播报给用户进行确认，通过接收模块 220 接收到的授权信息也是根据该随机数生成的，并且状态控制模块 230 通过将授权信息与随机数进行匹配对比来判断是否进入安全状态。

根据本发明实施例的用于签名的电子签名工具，通过随机数加入授权请求，在判断是否进入安全状态时与该随机数进行对比，提高了电子签名工具的安全性。

图 7 为本发明另一个实施例的用于签名的电子签名工具的结构示意图。

如图 7 所示，根据本发明实施例的用于签名的电子签名工具，还包括：退出控制模块 270，同时状态控制模块 230 进一步包括解密子模块 231 和状态控制子模块 232。

具体地，退出控制模块 270 用于在满足以下任一项条件时退出安全状态：超过预设时间；第一电子签名工具掉电；第一电子签名工具完成对该次交易的签名。解密子模块 231 用于根据密钥对签名信息进行解密以生成解密信息；以及状态控制子模块 232 用于在判断解密信息与随机数匹配时，进入安全状态。

根据本发明实施例的用于签名的电子签名工具，通过提示模块将解密子模块对接收到的签名信息进行解密，并且通过状态控制子模块将解密后的签名信息与原随机数进行对比匹配判断是否进入安全状态，在进入安全状态后同样有退出控制模块控制签名工具退出安全状态，提高了该用于签名的电子签名工具的安全性。

下面结合图 5 到图 7 的实施例详细说明本发明的用于签名的电子签名工具的工作流程。

该用于签名的电子签名工具通过生成模块生成一个随机数与交易信息一起通过添加模块添加到授权请求中，该随机数可以通过提示模块展示给用户，然后通过发送模块将授权请求发送给用于授权的电子签名工具，再通过接收模块接收用于授权的电子签名工具反馈的授权信息，将接收的授权信息用状态控制模块中的解密模块根据预设在该用于签名的电子签名工具中的密钥进行解密，将解密后的得到的数字与之前的随机数通过状态控制子模块进行匹配对比来判断是否进入安全状态，若完全匹配则进入安全状态，可以对电子交易进行签名，但是退出控制模块则会对该电子签名工具进行状态监控如果进入安全状态超过预设时间，或者第一电子签名工具与交易终端断开连接掉电，又或者第一电子签名工具完成签名，则控制该用于签名的电子签名工具退出安全状态。

下面参考说明书附图描述根据本发明实施例的用于授权的电子签名工具。

一种用于授权的电子签名工具，包括：接收模块，用于接收用于签名的电子签名工具发送的授权请求；生成模块，用于根据授权请求生成相应的授权信息；发送模块，用于将授权信息反馈至用于签名的电子签名工具。以及 USB 插座，用于与用于签名的

电子签名工具的 USB 插头相连。

图 8 为本发明一个实施例的用于授权的电子签名工具的结构示意图。

如图 8 所示, 根据本发明实施例的用于授权的电子签名工具, 包括: 接收模块 310 生成模块 320, 发送模块 330 及 USB 插座 340。

5 具体地, 接收模块 310 用于接收用于签名的电子签名工具发送的授权请求; 生成模块 320 用于根据授权请求生成相应的授权信息; 以及发送模块 330 用于将授权信息反馈至用于签名的电子签名工具。USB 插座 340 用于与用于签名的电子签名工具的 USB 插头相连。

10 更具体地, 该用于授权的电子签名工具通过接收模块 310 接收来自于用于签名的电子签名工具的授权请求, 并根据该授权请求中的信息通过生成模块来 320 生成相应的授权信息并通过发送模块 330 发送给申请授权的用于签名的电子签名工具。如果该用于授权的电子签名工具和申请授权的用于签名的电子签名工具都在一处, 则用于签名的电子签名工具可以直接插在该用于授权的电子签名工具的 USB 插座 340 上连接, 然后连接交易终端直接签名。

15 在本发明的一个实施例中, 用于签名的电子签名工具和用于授权的电子签名工具具有相匹配的密钥。

根据本发明实施例的用于授权的电子签名工具, 通过接收模块和发送模块与用于签名的电子签名工具进行交互, 并通过生成模块来生成相应的授权信息, 在某些情况下还可以直接通过 USB 插座与用于签名的电子签名工具相连, 提高了电子签名工具的
20 易用性。

下面参考说明书附图描述根据本发明实施例的用于电子签名工具的授权校验系统。

一种用于电子签名工具的授权校验系统, 包括: 第一电子签名工具, 用于生成授权请求, 并将授权请求发送至第一终端, 并接收第一终端反馈的授权信息, 以及在根据授权信息进入安全状态之后, 进行签名支付; 第一终端, 用于将授权请求发送至第二终端, 并将第二终端发送的授权信息转发至第一电子签名工具; 第二终端, 用于将授权请求转发至第二电子签名工具, 并将授权信息转发至第一终端; 第二电子签名工具, 用于根据授权请求生成相应的授权信息, 并将授权信息发送至第二终端。
25

图 9 为本发明一个实施例的用于电子签名工具的授权校验系统的结构示意图。

30 如图 9 所示, 根据本发明实施例的用于电子签名工具的授权校验系统, 其特征在于, 包括: 第一电子签名工具 410 和第二电子签名工具 420, 以及分别与第一电子签名工具 410 和第二电子签名工具 420 相连的第一终端 430 和第二终端 440, 且第一终端 430 和第二终端 440 之间相互通信。

具体地, 第一电子签名工具 410, 用于生成授权请求, 并将授权请求发送至第一终端 430, 并接收第一终端 430 反馈的授权信息, 以及在授权信息进入安全状态之后, 进
35

行签名支付；第一终端 430，用于将授权请求发送至第二终端 440，并将第二终端 440 发送的授权信息转发至第一电子签名工具 410；第二终端 440，用于将授权请求转发至第二电子签名工具 420，并将授权信息转发至第一终端 430；第二电子签名工具 420，用于根据授权请求生成相应的授权信息，并将授权信息发送至第二终端 440。

5 在本发明的一个实施例中，第一电子签名工具 410 还用于在生成授权请求前，生成随机数，并将随机数添加至授权请求之中。

具体地，第一电子签名工具 410 在生成授权请求前，生成一个随机数，然后将该随机数添加到发送给第二电子签名工具 420 的授权请求中去。

10 在本发明的一个实施例中，第二电子签名工具 420 还用于根据随机数生成的签名信息。

具体地，第二电子签名工具 420 收到授权请求后，根据授权请求信息中包含的随机数生成签名信息。

在本发明的一个实施例中，第一电子签名工具 410 还用于根据密钥对签名信息进行解密以生成解密信息，并在判解密信息与随机数匹配时，进入安全状态。

15 具体地，在第一电子签名工具 410 接收到签名信息后会根据预设的密钥对该签名信息进行解密，生成解密信息，将解密信息与随机数进行匹配对比，如果完全匹配，则第一电子签名工具 410 进入安全状态。

在本发明的一个实施例中，第一电子签名工具 410 还用于在接收交易的信息之后，将交易的信息相关的付款账户和/或支付金额添加至授权请求之中。

20 具体地，第一电子签名工具 410 获取该次电子交易的信息，如相关的付款账户和/或支付金额，并将这些信息添加到授权请求中。

在本发明的一个实施例中，第二电子签名工具 420 还用于根据付款账户和/或支付金额生成签名信息。

25 具体地，第二电子签名工具 420 在接收到授权请求后，从授权请求中获取付款账户和/或支付金额，并根据这些交易信息生成签名信息。

在本发明的一个实施例中，第一电子签名工具 410 在进入安全状态之后，还用于在满足以下任一项条件时退出安全状态：超过预设时间；第一电子签名工具 410 掉电；第一电子签名工具 410 完成签名。

30 具体地，如果在第一电子签名工具 410 进入安全状态，超过预定的时间后，则退出安全状态，无法继续再进行签名；或者在第一电子签名工具 410 进入安全状态后，在断开第一电子签名工具 410 与交易终端连接后则第一电子签名工具 410 掉电，此时第一电子签名工具 410 退出安全状态，无法继续再进行签名；或者在第一电子签名工具 410 进入安全状态后，在完成对应的电子交易的签名后，此时第一电子签名工具 410 退出安全状态，无法继续再进行签名。

35 在本发明的一个实施例中，第一电子签名工具 410 为多个，且每个第一电子签名

工具 410 具有唯一的密钥，第二电子签名工具 420 具有与多个第一个电子签名工具 410 的密钥相匹配的多个密钥。

具体地，第一电子签名工具 410 可以有多个，且每个第一个电子签名工具 410 中都预设了解密用的唯一的密钥，可以提供给多个人在不同地方进行交易，而第二电子签名工具 420 中则存有与所有第一个电子签名工具 410 中的密钥相匹配的多个密钥，可以

给不同的电子签名工具进行授权。

在本发明的一个实施例中，第二电子签名工具 420 为多个，且每个第二电子签名工具 420 具有唯一的密钥，第一电子签名工具 410 具有与多个第二个电子签名工具 420 的密钥相匹配的多个密钥，第一电子签名工具 410 分别向多个第二个电子签名工具 420 发送授权请求。

具体地，第二电子签名工具 420 可以有多个，且每个第二个电子签名工具 420 中则存有与各个第一个电子签名工具 410 中的密钥相匹配的多个密钥，可以给不同的电子签名工具进行授权，如果第一个电子签名工具 410 收到全部第二个电子签名工具 420 的授权信息，且授权信息均满足要求，则第一个电子签名工具 410 进入安全状态；或者，如果第一个电子签名工具 410 收到任一个第二个电子签名工具 420 的授权信息，且授权信息均满足要求，则第一个电子签名工具 410 进入安全状态；

根据本发明实施例的用于电子签名工具的授权校验系统，通过第一个电子签名工具进行签名，第二电子签名工具对第一个电子签名工具授权，而两个电子签名工具则是连在不同的终端上，通过终端来互相交互，提高了系统的在电子交易过程中的安全性与易用性。

下面参考说明书附图描述根据本发明实施例的用于电子签名工具的授权校验方法。

一种用于电子签名工具的授权校验方法，包括以下步骤：第一电子签名工具需执行签名功能时，通过互联网向第二电子签名工具发送包含请求信息的授权请求；第二电子签名工具对所述第一签名工具发送的授权请求进行授权，并将授权信息返回给第一电子签名工具；第一电子签名工具根据授权信息解密后，将解密的授权信息与随机数匹配进行签名验证，判断授权是否成功；如果判断授权成功，则打开安全状态；如果判断授权不成功，则安全状态无法打开；在签名授权不成功时，第一电子签名工具还可向第二电子签名工具重新发送授权请求；以及第一电子签名工具若在安全状态中掉电，则退出安全状态。

图 10 为本发明一个实施例的用于电子签名工具的授权校验方法的流程图。

如图 10 所示一种用于电子签名工具的授权校验方法，包括以下步骤：

步骤 S401：第一电子签名工具需要执行签名功能时，通过互联网向第二电子签名工具发送包含请求信息的授权请求。

具体地，第一电子签名工具在电子交易需要执行签名功能时，生成一个包含请求

授权信息的授权请求，并通过互联网发送给处于另一个地方的第二电子签名工具。

步骤 S402：第二电子签名工具对所述第一签名工具发送的授权请求进行授权，将授权信息返回给第一电子签名工具。

具体地，第二电子签名工具接收授权请求，获取授权请求中包含的请求信息进行
5 核对，在根据该授权请求生成相应的授权信息，返回给第一电子签名工具进行授权。

步骤 S403：第一电子签名工具对授权信息解密后，将解密的授权信息与请求信息进行匹配验证，判断所述授权是否成功。

具体地，首先第一电子签名工具根据预存的密钥对授权信息进行解密，获取解密后的信息，然后根据解密后的信息与之前生成的包含在授权请求的中的请求信息进行
10 匹配对比，验证是否授权成功。

步骤 S404：如果判断授权成功，则打开安全状态。

具体地，如果解密后的授权信息与请求信息匹配对比完全一样，则打开安全状态，可以对交易进行签名。

步骤 S405：如果判断授权不成功，则安全状态无法打开。

具体地，解密后的授权信息与请求信息匹配对比不完全一样，则无法打开安全状态，无法对此次交易进行签名。
15

步骤 S406：签名授权不成功后，第一电子签名工具还可向第二电子签名工具重新发送授权请求。

具体地，在第一电子签名工具授权签名不成功，无法进行签名时，可以对第二电子签名工具进行反馈，并重新发出授权请求。
20

步骤 S407：第一电子签名工具若在安全状态中掉电，则退出安全状态。

具体地，第一电子签名工具如果进入安全状态后，与交易终端断开连接掉电，则退出安全状态，无法对交易进行签名。

在本发明的一个实施例中，授权请求包括第一电子签名工具生成的随机数，且授权信息包括第二电子签名工具对随机数进行签名的相关签名信息。
25

具体地，在第一电子签名工具生成授权请求时还同时生成一个随机数，并将该随机数添加到授权请求中发送给第二电子签名工具，而第二电子签名工具则根据该随机数生成相应的授权信息，对该随机数进行签名。

在本发明的一个实施例中，第二电子签名工具具有 USB 插座，第二电子签名工具对第一电子签名工具授权还可通过点对点连接授权，且通过点对点连接授权产生的随机数可以保密也可以展示给用户。
30

具体地，在第一电子签名工具与第二电子签名工具都处于同一个地方的时候，可以不通过互联网来进行交互，可以直接通过第一电子签名工具插入第二电子签名工具上的 USB 插座来进行连接，通过 USB 插座连接的两个电子签名工具在授权时生成的
35 随机数可以直接内部生成且验证，无需通知用户，也可以通过展示给用户显示屏或者

语言展示给用户。

在本发明的一个实施例中，第一电子签名工具可以有多个，第二电子签名工具也可以有多个。

具体地，第一电子签名工具可以有多个，可以提供给多个人在不同地方进行交易，而第二电子签名工具则对应可以给不同的电子签名工具进行授权。第二电子签名工具也可以有多个，可以给不同的电子签名工具进行授权，用户可以进行设定，如果第一电子签名工具收到全部第二电子签名工具的授权信息，且授权信息均满足要求，则第一电子签名工具进入安全状态；或者设定为，如果第一电子签名工具收到任一第二电子签名工具的授权信息，且授权信息均满足要求，则第一电子签名工具进入安全状态。且授权信息均满足要求，则第一电子签名工具进入安全状态。

根据本发明实施例的用于电子签名工具的授权校验方法，通过第二电子签名工具对第一电子签名工具进行授权，再通过第一电子签名工具对电子交易进行签名，其中通过随机数来验证授权信息，可以在授权人不在身边时，交易人也可完成交易，提高了电子签名工具的使用方便性，同时降低了交易人私自对公司转账的风险，提高了公司电子交易的安全性；且授权失败的第一电子签名工具可以再次提出授权请求，提高了电子签名工具的易用性。

下面参考说明书附图描述根据本发明实施例的用于电子签名工具的授权校验系统。

一种用于电子签名工具的授权校验系统：包括一个或多个第一电子签名工具和一个或多个第二电子签名工具，其中，第一电子签名工具，用于在电子交易签名时，向第二电子签名工具发送授权请求，并根据第二电子签名工具反馈的授权信息判断是否签名正确，并在签名正确时打开安全状态进行电子交易签名；第二电子签名工具，用于根据第一电子签名工具发送的授权请求生成相应的授权信息并返回给第一签名工具。

图 11 为本发明一个实施例的用于电子签名工具的授权校验系统的结构示意图。如图 11 所示，根据本发明实施例的用于电子签名工具的授权校验系统，包括：一个或多个第一电子签名工具 510 和一个或多个第二电子签名工具 520。

具体地，第一电子签名工具 510，用于在电子交易签名时，向第二电子签名工具 520 发送包含随机数的授权请求，并根据第二电子签名工具 520 反馈的授权信息判断是否签名正确，并在签名正确时打开安全状态进行电子交易签名；第二电子签名工具 520 用于根据第一电子签名工具 510 发送的授权请求生成相应的授权信息并返回给第一签名工具 510。

更具体地，第一电子签名工具 510 可以有多个，可以提供给多个人在不同地方进行交易，而第二电子签名工具 520 中对应可以给不同的电子签名工具进行授权。第二电子签名工具 520 可以有多个，可以给不同的电子签名工具进行授权，用户可以设定，

如果第一电子签名工具 510 收到全部第二电子签名工具 520 的授权信息，且授权信息均满足要求，则第一电子签名工具 510 进入安全状态；或者设定为，如果第一电子签名工具 510 收到任一个第二电子签名工具 520 的授权信息，且授权信息满足要求，则第一电子签名工具 510 进入安全状态。

- 5 在本发明的一个实施例中，第一电子签名工具 510 若在安全状态中掉电，则退出安全状态。

具体地，第一电子签名工具 510 如果进入安全状态后，从交易终端中拔出，该第一电子签名工具 510 掉电，退出安全状态，再插上该第一电子签名工具 510 也无法进入安全状态。

- 10 在本发明的一个实施例中，第二电子签名工具 520 还包括与第一电子签名工具 510 对接的 USB 接口，用于点对点连接授权，且通过 USB 接口对接授权产生的随机数可以展示给用户也可以不展示给用户。

- 具体地，在第一电子签名工具 510 与第二电子签名工具 520 都处于同一个地方的时候，可以不通过互联网来进行交互，可以直接通过第一电子签名工具 510 插入第二
15 电子签名工具 520 上的 USB 插座来进行连接，通过 USB 插座连接的两个电子签名工具在授权时生成的随机数可以直接内部生成且验证，无需通知用户，也可以通过展示给用户显示屏或者语言展示给用户。

- 根据本发明实施例的用于电子签名工具的授权校验系统，通过第一电子签名工具向第二电子签名工具发出授权请求，并执行签名，第一电子签名工具则确认信息并进行授权，同时可以通过不同方式使第一电子签名工具与第二电子签名工具交互，保证了企业电子交易支付或转账的安全性与方便性；同时可以设定不同数量的第一电子签名工具和第二电子签名工具，使安全性得到更大的提高。
- 20

- 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。
- 25

- 尽管已经示出和描述了本发明的实施例，对于本领域的普通技术人员而言，可以理解在不脱离本发明的原理和精神的情况下可以对这些实施例进行多种变化、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。
- 30

权利要求书

1、一种用于电子签名工具的授权校验方法，其特征在于，包括以下步骤：

第一电子签名工具向第二电子签名工具发送授权请求；

5 所述第二电子签名工具根据所述授权请求生成相应的授权信息，并将所述授权信息反馈至所述第一电子签名工具；

所述第一电子签名工具根据所述授权信息判断是否进入安全状态；以及
如果判断进入安全状态，则所述第一电子签名工具打开签名功能。

2、如权利要求1所述的用于电子签名工具的授权校验方法，其特征在于，其中，
10 所述第一电子签名工具和所述第二电子签名工具具有相匹配的密钥。

3、如权利要求1或2所述的用于电子签名工具的授权校验方法，其特征在于，所述授权请求包括所述第一电子签名工具生成的随机数，且所述授权信息包括所述第二电子签名工具根据所述随机数生成的签名信息。

4、如权利要求3所述的用于电子签名工具的授权校验方法，其特征在于，所述第
15 一电子签名工具根据所述授权信息判断是否进入安全状态进一步包括：

所述第一电子签名工具对所述签名信息进行解密以生成解密信息；

所述第一电子签名工具判断所述解密信息是否与所述随机数匹配；以及
如果判断匹配，则所述第一电子签名工具进入所述安全状态。

5、如权利要求3所述的用于电子签名工具的授权校验方法，其特征在于，还包括：
20 所述第一电子签名工具将所述随机数显示给用户，或者通过语音提示给所述用户。

6、如权利要求2所述的用于电子签名工具的授权校验方法，其特征在于，所述授权请求包括此次交易相关的付款账户和/或支付金额，且所述授权信息包括所述第二电子签名工具根据所述付款账户和/或支付金额生成的签名信息。

7、如权利要求6所述的用于电子签名工具的授权校验方法，其特征在于，还包括：
25 将所述付款账户和/或支付金额在所述第二电子签名工具中显示。

8、如权利要求6所述的用于电子签名工具的授权校验方法，其特征在于，所述第
一电子签名工具根据所述授权信息判断是否进入安全状态进一步包括：

所述第一电子签名工具根据所述密钥对所述签名信息进行解密以生成解密信息；

30 所述第一电子签名工具判断所述解密信息是否与所述付款账户和/或支付金额匹配；以及

如果判断匹配，则所述第一电子签名工具进入所述安全状态。

9、如权利要求6所述的用于电子签名工具的授权校验方法，其特征在于，在所述第一电子签名工具进入安全状态之后，还包括：

35 所述第一电子签名工具根据所述付款账户和/或支付金额进行与其匹配的交易签名，完成所述签名后退出所述安全状态；

再次进行交易时，若所需签名的交易的付款账户和/或支付金额与所述付款账户和/或支付金额不匹配，则退出所述安全状态。

10、如权利要求 1-8 任一项所述的用于电子签名工具的授权校验方法，其特征在于，在所述第一电子签名工具进入安全状态之后，还包括：

- 5 所述第一电子签名工具在预设时间之后退出所述安全状态；
 或者，所述第一电子签名工具在掉电之后退出所述安全状态；
 或者，所述第一电子签名工具在完成签名之后退出所述安全状态。

11、如权利要求 1-10 任一项所述的用于电子签名工具的授权校验方法，其特征在于，所述第一电子签名工具为多个，且每个所述第一电子签名工具具有唯一的密钥，
10 所述第二电子签名工具具有与所述多个第一电子签名工具的密钥相匹配的多个密钥。

12、如权利要求 1-10 任一项所述的用于电子签名工具的授权校验方法，其特征在于，所述第二电子签名工具为多个，且每个所述第二电子签名工具具有唯一的密钥，
 所述第一电子签名工具具有与所述多个第二电子签名工具的密钥相匹配的多个密钥，
 所述第一电子签名工具分别向所述多个第二电子签名工具发送授权请求。

13、如权利要求 12 所述的用于电子签名工具的授权校验方法，其特征在于，
15 如果所述第一电子签名工具收到全部所述第二电子签名工具的授权信息，且所述授权信息均满足要求，则所述第一电子签名工具进入所述安全状态；

 或者，如果所述第一电子签名工具收到任一个所述第二电子签名工具的授权信息，
 且所述授权信息满足要求，则所述第一电子签名工具进入所述安全状态。

14、如权利要求 1 所述的用于电子签名工具的授权校验方法，其特征在于，所述
20 第一电子签名工具和所述第二电子签名工具通过有线网络或无线网络或相互之间的直接连接进行通信。

15、如权利要求 1 所述的用于电子签名工具的授权校验方法，其特征在于，所述
25 第二电子签名工具具有 USB 插座，所述第一电子签名工具的 USB 插头插入所述 USB 插座以建立所述第一电子签名工具与所述第二电子签名工具的通信。

16、一种用于电子签名工具的授权校验系统，其特征在于，包括第一电子签名工具
 和第二电子签名工具，其中，

 所述第一电子签名工具，用于向所述第二电子签名工具发送授权请求，并根据所
 述第二电子签名工具反馈的授权信息判断是否进入安全状态，以及在判断进入安全状
30 态之后，根据该次交易信息进行签名支付；

 所述第二电子签名工具，用于根据所述授权请求生成相应的授权信息，并将所述
 授权信息反馈至所述第一电子签名工具。

17、如权利要求 16 所述的用于电子签名工具的授权校验系统，其特征在于，其中，
 所述第一电子签名工具和所述第二电子签名工具具有相匹配的密钥。

18、如权利要求 17 所述的用于电子签名工具的授权校验系统，其特征在于，所述
35

第一电子签名工具还用于生成随机数，并将所述随机数添加至所述授权请求之中。

19、如权利要求 18 所述的用于电子签名工具的授权校验系统，其特征在于，所述第二电子签名工具还用于根据所述随机数生成签名信息。

20、如权利要求 18 所述的用于电子签名工具的授权校验系统，其特征在于，所述
5 第一电子签名工具还用于将所述随机数显示给用户，或者通过语音提示给所述用户。

21、如权利要求 17 所述的用于电子签名工具的授权校验系统，其特征在于，所述第一电子签名工具还用于根据所述密钥对所述签名信息进行解密以生成解密信息，并在判断所述解密信息与所述随机数匹配时，进入安全状态。

22、如权利要求 21 所述的用于电子签名工具的授权校验系统，其特征在于，所述
10 第一电子签名工具还用于在接收所述该次交易的信息之后，将该次交易相关的付款账户和/或支付金额添加至所述授权请求之中。

23、如权利要求 22 所述的用于电子签名工具的授权校验系统，其特征在于，所述第二电子签名工具还用于根据所述第二电子签名工具根据所述付款账户和/或支付金额生成签名信息。

15 24、如权利要求 16 所述的用于电子签名工具的授权校验系统，其特征在于，所述第一电子签名工具在进入安全状态之后，还用于在满足以下任一项条件时退出所述安全状态：

超过预设时间；

所述第一电子签名工具掉电；

20 所述第一电子签名工具完成对该次交易的签名。

25、如权利要求 16 所述的用于电子签名工具的授权校验系统，其特征在于，所述第一电子签名工具为多个，且每个所述第一电子签名工具具有唯一的密钥，所述第二电子签名工具具有与所述多个第一电子签名工具的密钥相匹配的多个密钥。

26、如权利要求 16 所述的用于电子签名工具的授权校验系统，其特征在于，所述
25 第二电子签名工具为多个，且每个所述第二电子签名工具具有唯一的密钥，所述第一电子签名工具具有与所述多个第二电子签名工具的密钥相匹配的多个密钥，所述第一电子签名工具分别向所述多个第二电子签名工具发送授权请求。

27、如权利要求 26 所述的用于电子签名工具的授权校验系统，其特征在于，

30 如果所述第一电子签名工具收到全部所述第二电子签名工具的授权信息，且所述授权信息均满足要求，则所述第一电子签名工具进入所述安全状态；

或者，如果所述第一电子签名工具收到任一个所述第二电子签名工具的授权信息，且所述授权信息均满足要求，则所述第一电子签名工具进入所述安全状态。

28、如权利要求 16 所述的用于电子签名工具的授权校验系统，其特征在于，所述
35 第一电子签名工具和所述第二电子签名工具通过有线网络或无线网络或相互之间的直接连接进行通信。

29、如权利要求 16 所述的用于电子签名工具的授权校验系统，其特征在于，所述第二电子签名工具具有 USB 插座，所述第一电子签名工具的 USB 插头插入所述 USB 插座之后建立所述第一电子签名工具与所述第二电子签名工具的通信。

30、一种用于签名的电子签名工具，其特征在于，包括：

5 发送模块，用于向用于授权的电子签名工具发送授权请求；

接收模块，用于接收所述用于授权的电子签名工具反馈的授权信息；以及

状态控制模块，用于根据所述授权信息判断是否进入安全状态，以及在判断进入安全状态之后，进行签名支付。

10 31、如权利要求 30 所述的用于签名的电子签名工具，其特征在于，所述用于签名的电子签名工具和所述用于授权的电子签名工具具有相匹配的密钥。

32、如权利要求 31 所述的用于签名的电子签名工具，其特征在于，还包括：

生成模块，用于生成随机数；以及

添加模块，用于将所述随机数添加至所述授权请求之中。

33、如权利要求 32 所述的用于签名的电子签名工具，其特征在于，还包括：

15 提示模块，用于将所述随机数显示给用户，或者通过语音提示给所述用户。

34、如权利要求 32 所述的用于签名的电子签名工具，其特征在于，所述状态控制模块进一步包括：

解密子模块，用于根据所述密钥对所述签名信息进行解密以生成解密信息；以及
状态控制子模块，用于在判断所述解密信息与所述随机数匹配时，进入安全状态。

20 35、如权利要求 31 所述的用于签名的电子签名工具，其特征在于，还包括：

退出控制模块，用于在满足以下任一项条件时退出所述安全状态：

超过预设时间；

所述第一电子签名工具掉电；

所述第一电子签名工具完成对该次交易的签名。

25 36、一种用于授权的电子签名工具，其特征在于，包括：

接收模块，用于接收用于签名的电子签名工具发送的授权请求；

生成模块，用于根据所述授权请求生成相应的授权信息；以及

发送模块，用于将所述授权信息反馈至所述用于签名的电子签名工具。

30 37、如权利要求 36 所述的用于授权的电子签名工具，其特征在于，所述用于签名的电子签名工具和所述用于授权的电子签名工具具有相匹配的密钥。

38、如权利要求 36 所述的用于授权的电子签名工具，其特征在于，还包括：

USB 插座，用于与所述用于签名的电子签名工具的 USB 插头相连。

35 39、一种用于电子签名工具的授权校验系统，其特征在于，包括第一电子签名工具和第二电子签名工具，以及分别与所述第一电子签名工具和第二电子签名工具相连的第一终端和第二终端，且所述第一终端和所述第二终端之间相互通信，其中，

所述第一电子签名工具，用于生成授权请求，并将所述授权请求发送至所述第一终端，并接收所述第一终端反馈的授权信息，以及再根据所述授权信息进入安全状态之后，进行签名支付；

5 所述第一终端，用于将所述授权请求发送至所述第二终端，并将所述第二终端发送的授权信息转发至所述第一电子签名工具；

所述第二终端，用于将所述授权请求转发至所述第二电子签名工具，并将所述授权信息转发至所述第一终端；

所述第二电子签名工具，用于根据所述授权请求生成相应的授权信息，并将所述授权信息发送至所述第二终端。

10 40、如权利要求 39 所述的用于电子签名工具的授权校验系统，其特征在于，所述第一电子签名工具还用于在生成授权请求前，生成随机数，并将所述随机数添加至所述授权请求之中。

41、如权利要求 40 所述的用于电子签名工具的授权校验系统，其特征在于，所述第二电子签名工具还用于根据所述随机数生成的签名信息。

15 42、如权利要求 39 所述的用于电子签名工具的授权校验系统，其特征在于，所述第一电子签名工具还用于根据所述密钥对所述签名信息进行解密以生成解密信息，并在判断所述解密信息与所述随机数匹配时，进入安全状态。

43、如权利要求 42 所述的用于电子签名工具的授权校验系统，其特征在于，所述第一电子签名工具还用于在接收交易的信息之后，将与所述交易的信息相关的付款账户和/或支付金额添加至所述授权请求之中。

20 44、如权利要求 43 所述的用于电子签名工具的授权校验系统，其特征在于，所述第二电子签名工具还用于根据所述第二电子签名工具根据所述付款账户和/或支付金额生成签名信息。

25 45、如权利要求 39 所述的用于电子签名工具的授权校验系统，其特征在于，所述第一电子签名工具在进入安全状态之后，还用于在满足以下任一项条件时退出所述安全状态：

超过预设时间；

所述第一电子签名工具掉电；

所述第一电子签名工具完成对该次交易的签名。

30 46、如权利要求 39 所述的用于电子签名工具的授权校验系统，其特征在于，所述第一电子签名工具为多个，且每个所述第一电子签名工具具有唯一的密钥，所述第二电子签名工具具有与所述多个第一电子签名工具的密钥相匹配的多个密钥。

35 47、如权利要求 39 所述的用于电子签名工具的授权校验系统，其特征在于，所述第二电子签名工具为多个，且每个所述第二电子签名工具具有唯一的密钥，所述第一电子签名工具具有与所述多个第二电子签名工具的密钥相匹配的多个密钥，所述第一

电子签名工具分别向所述多个第二电子签名工具发送授权请求。

48、一种用于电子签名工具的授权校验方法，其特征在于，包括以下步骤：

第一电子签名工具需要执行签名功能时，通过互联网向第二电子签名工具发送包含请求信息的授权请求；

5 所述第二电子签名工具对所述第一签名工具发送的授权请求进行授权，并将授权信息返回给所述第一电子签名工具；

所述第一电子签名工具对所述授权信息解密后，将解密的授权信息与所述请求信息进行匹配验证，判断所述授权是否成功；

如果判断所述授权成功，则打开安全状态；

10 如果判断所述授权不成功，则所述安全状态无法打开；

在所述签名授权不成功后，所述第一电子签名工具还可向所述第二电子签名工具重新发送授权请求；以及

所述第一电子签名工具若在安全状态中掉电，则退出所述安全状态。

49、如权利要求 48 所述的用于电子签名工具的授权校验方法，其特征在于，其中，
15 所述授权请求包括所述第一电子签名工具生成的随机数，且所述授权信息包括所述第二电子签名工具对所述随机数进行签名的相关签名信息。

50、如权利要求 48 所述的用于电子签名工具的授权校验方法，其特征在于，述第一电子签名工具和所述第二电子签名工具还可以通过交易终端进行授权。且所述第二电子签名工具具有 USB 插座，所述第二电子签名工具对所述第一电子签名工具授权
20 还可通过点对点连接授权。且通过所述点对点连接授权产生的随机数可以保密也可以展示给用户。

51、如权利要求 50 所述的用于电子签名工具的授权校验方法，其特征在于，所述
第一电子签名工具可以有多个，所述第二电子签名工具也可以有多个。

52、一种用于电子签名工具的授权校验系统，其特征在于，包括一个或多个第一
25 电子签名工具和一个或多个第二电子签名工具，其中，

所述第一电子签名工具，用于在电子交易签名时，向所述第二电子签名工具发送包含随机数的授权请求，并根据所述第二电子签名工具反馈的授权信息判断是否签名正确，并在签名正确时打开安全状态进行所述电子交易签名；

30 所述第二电子签名工具，用于根据所述第一电子签名工具发送的所述授权请求生成相应的授权信息并返回给所述第一签名工具。

53、如权利要求 52 所述的用于电子签名工具的授权校验系统，其特征在于，所述
第一电子签名工具若在安全状态中掉电，则退出所述安全状态。

54、如权利要求 52 所述的用于电子签名工具的授权校验系统，其特征在于，所述
35 第二电子签名工具还包括与所述第一电子签名工具对接的 USB 接口，用于点对点连接授权，且通过 USB 接口对接授权产生的随机数可以展示给用户也可以不展示给用户。