(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 101562525 B
(45)授权公告日 2012.06.27

(21)申请号 200910083284.4

(22)申请日 2009.04.30

(73)专利权人 飞天诚信科技股份有限公司
地址 100085 北京市海淀区学清路 9 号汇智大厦 B 座 17 层

(72)发明人 陆舟 于华章

(74)专利代理机构 北京中博世达专利商标代理有限公司 11274
代理人 申健

(51)Int.Cl.
H04L 9/32(2006.01)

(56)对比文件
CN 101183456 A,2008.05.21,
CN 101231737 A,2008.07.30,
CN 101183456 A,2008.05.21,
CN 101221641 A,2008.07.16,
周化祥．一种基于 PKI 体系的 USB Key 认证客户端的设计研究．《电脑知识与技术》.2008, 第 3 卷（第 5 期）,

审查员 陈红英

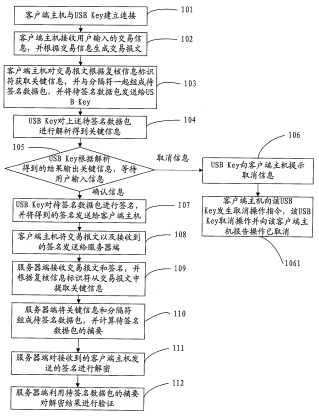
权利要求书 5 页 说明书 14 页 附图 2 页

(54)发明名称

签名方法、设备及系统

(57)摘要

本发明实施例公开了一种签名方法、设备及系统。涉及信息安全领域，解决了现有技术中用户的签名被他人冒用的技术问题。本发明实施例中主机在接收到用户输入的交易信息后，用交易信息生成交易报文并根据所述交易报文确定关键信息，组成待签名数据包发送到USB Key；USB Key则接收主机发送的待签名数据包，并在提取出其中的关键信息后，输出关键信息，等待用户确认，若用户输入确认信息，对该待签名数据包进行数字签名并发送该签名到主机；服务器接收主机转发的签名和交易报文，从交易报文中提取关键信息组成待签名数据包，并用组成的待签名数据包对接收到的签名进行验证。本发明实施例主要应用在信息安全方面。



CN 101562525 B

1. 一种签名方法，其特征在于，在客户端主机与服务器预先约定了复核信息标识符和分隔符后，包括：

所述客户端主机与智能密钥设备建立连接；

所述客户端主机通过输入装置接收用户输入的交易信息，所述输入装置包括所述客户端主机的输入装置和 / 或所述智能密钥设备的输入装置；

所述客户端主机根据所述交易信息生成交易报文；

所述客户端主机根据所述交易报文确定关键信息；

所述客户端主机将包含所述关键信息和所述分隔符的待签名数据包发送到所述智能密钥设备；

所述客户端主机等待接收所述智能密钥设备的反馈信息；

所述智能密钥设备接收所述客户端主机发送的待签名数据包；

所述智能密钥设备根据所述分隔符从所述待签名数据包中获取关键信息；

所述智能密钥设备输出对应所述关键信息的复核信息标识符和所述关键信息，并等待用户输入信息；

如果所述智能密钥设备在预设时间内接收到用户输入的确认信息，则所述智能密钥设备对所述待签名数据包进行签名，所述预设时间为所述等待用户输入信息的时间；

将得到的签名作为反馈信息发送到所述客户端主机；

所述服务器接收所述客户端主机发送的交易报文和签名；

所述服务器根据所述复核信息标识符从所述交易报文中获取关键信息；

所述服务器根据所述关键信息和所述分隔符生成待签名数据包；

所述服务器利用所述待签名数据包对所述客户端主机发送的签名进行验证；

如果所述智能密钥设备在预设时间内接收到用户输入的取消信息，则

将所述取消信息作为反馈信息发送到所述客户端主机。

2. 根据权利要求 1 所述的签名方法，其特征在于，所述客户端主机预先安装了本地接口；所述客户端主机通过输入装置接收用户输入的交易信息包括：

所述客户端主机的本地接口通过输入装置接收用户输入的交易信息。

3. 根据权利要求 1 所述的签名方法，其特征在于，所述客户端主机预先安置了本地接口和内嵌代码；若所述客户端主机通过所述客户端主机的输入装置和智能密钥设备的输入装置接收用户输入的交易信息；或者，若所述客户端主机通过所述智能密钥设备的输入装置接收用户输入的交易信息，在所述接收用户输入的交易信息之前，该方法还包括：

所述客户端主机的内嵌代码通过所述主机的本地接口激活所述智能密钥设备的输入装置。

4. 根据权利要求 3 所述的签名方法，其特征在于，所述客户端主机根据所述交易信息生成交易报文包括：

所述客户端主机的浏览器通过所述客户端主机的内嵌代码将所述交易信息生成交易报文。

5. 根据权利要求 1 所述的签名方法，其特征在于，所述客户端主机预先安置了本地接口和内嵌代码；所述客户端主机根据所述交易报文确定关键信息包括：

所述客户端主机根据所述复核信息标识符从所述交易报文中获取关键信息；或者

所述客户端主机的内嵌代码先通过本地接口激活所述智能密钥设备的输入装置，所述客户端主机接收用户通过所述智能密钥设备的输入装置输入的数字关键信息，并根据所述复核信息标识符从所述交易报文中提取关键信息，再根据所述提取得到的关键信息对所述数字关键信息进行确认，若得到确认，则将所述关键信息进行拼接。

6. 根据权利要求 1 至 5 中任意一项所述的签名方法，其特征在于，在所述客户端主机将所述待签名数据包发送给所述智能密钥设备之前，该方法还包括 ：

所述客户端主机将所述交易报文的字符类型转换成所述智能密钥设备可识别的字符类型。

7. 根据权利要求 1 至 5 中任意一项所述的签名方法，其特征在于，所述客户端主机设有预设时间 ；若所述客户端主机在所述预设时间内接收到所述智能密钥设备发送的反馈信息，且所述反馈信息具体为签名时，则该方法还包括 ：

所述客户端主机发送所述签名和所述交易报文到所述服务器。

8. 根据权利要求 1 至 5 中任意一项所述的签名方法，其特征在于，所述客户端主机设有预设时间 ；若所述客户端主机在所述预设时间内接收到智能密钥设备发送的反馈信息，且所述反馈信息具体为取消信息时，该方法还包括 ：

所述客户端主机向所述智能密钥设备发送取消操作指令 ；

所述客户端主机接收所述智能密钥设备报告的操作已取消的信息。

9. 根据权利要求 1 至 5 中任意一项所述的签名方法，其特征在于，所述客户端主机设有预设时间 ；在所述预设时间到时前，所述客户端主机在等待接收智能密钥设备发送反馈信息时，该方法还包括 ：

所述客户端主机随时向所述智能密钥设备发送取消操作指令 ；

所述客户端主机接收所述智能密钥设备报告的操作已取消的信息。

10. 根据权利要求 1 所述的签名方法，其特征在于，所述智能密钥设备根据所述分隔符从所述待签名数据包中获取关键信息包括 ：

所述智能密钥设备检测所述待签名数据包中的分隔符的数量 ；

所述智能密钥设备根据所述分隔符的数量解析出所述待签名数据包中的关键信息。

11. 根据权利要求 1 或 10 所述的签名方法，其特征在于，若所述智能密钥设备在所述预设时间内未接收到用户输入的确认信息或者取消信息，或者若所述智能密钥设备在所述预设时间内接收到所述客户端主机发送的取消操作指令，则该方法还包括 ：

所述智能密钥设备取消操作，并向所述客户端主机报告操作已取消。

12. 根据权利要求 1 或 10 所述的签名方法，其特征在于，在所述将取消信息作为反馈信息发送到所述客户端主机之后，该方法还包括 ：

所述智能密钥设备接收所述客户端主机发送的取消操作指令 ；

所述智能密钥设备取消操作并向所述客户端主机报告操作已取消。

13. 根据权利要求 1 或 10 所述的签名方法，其特征在于，所述智能密钥设备输出对应所述关键信息的复核信息标识符和所述关键信息包括 ：

所述智能密钥设备通过显示器显示对应所述关键信息的复核信息标识符和所述关键信息 ；或者

所述智能密钥设备通过语音播放器播报对应所述关键信息的复核信息标识符和所述

关键信息。

14. 根据权利要求 1 所述的签名方法，其特征在于，在所述服务器接收所述客户端主机发送的交易报文和签名之后，该方法还包括 ：

所述服务器将所述交易报文中的字符类型转换成所述智能密钥设备可识别的字符类型。

15. 一种签名系统，其特征在于，包括客户端主机、智能密钥设备和服务器，所述智能密钥设备连接到所述客户端主机，且所述客户端主机与服务器预先约定了复核信息标识符和分隔符 ；

所述客户端主机包括 ：

连接模块，用于与所述智能密钥设备建立连接 ；

本地接口模块，用于通过输入装置接收用户输入的交易信息，所述输入装置包括所述客户端主机的输入装置和 / 或所述智能密钥设备的输入装置 ；

生成模块，用于根据所述交易信息生成交易报文 ；

获取模块，用于根据所述交易报文确定关键信息 ；

第一发送模块，用于将包含所述关键信息和所述分隔符的待签名数据包发送到所述智能密钥设备 ；

接收模块，用于等待接收所述智能密钥设备的反馈信息 ；

所述智能密钥设备包括 ：

接收模块，用于接收所述客户端主机发送的待签名数据包 ；

获取模块，用于根据所述分隔符从所述待签名数据包中获取关键信息 ；

输出模块，用于输出对应所述关键信息的复核信息标识符和所述关键信息，并等待用户输入信息 ；

签名模块，用于若在预设时间内接收到用户输入的确认信息，则对所述待签名数据包进行签名，所述预设时间为输出模块等待用户输入信息的时间 ；

发送模块，用于将得到的签名作为反馈信息发送到所述客户端主机 ；

所述发送模块，还用于若在预设时间内接收到用户输入的取消信息，则将所述取消信息作为反馈信息发送到所述客户端主机 ；

所述服务器包括 ：

接收模块，用于接收所述客户端主机发送的交易报文和签名 ；

获取模块，用于根据所述复核信息标识符从所述交易报文中获取关键信息 ；

生成模块，用于根据所述关键信息和所述分隔符生成待签名数据包 ；

验证模块，用于利用所述待签名数据包，对所述客户端主机发送的签名进行验证。

16. 根据权利要求 15 所述的签名系统，其特征在于，所述客户端主机还包括 ：

内嵌代码模块，用于通过所述本地接口模块激活所述智能密钥设备的输入装置。

17. 根据权利要求 16 所述的签名系统，其特征在于，所述客户端主机的所述生成模块通过所述内嵌代码模块将所述交易信息生成交易报文。

18. 根据权要求 15 所述的签名系统，其特征在于，所述客户端主机的所述获取模块根据所述复核信息标识符从所述交易报文中获取关键信息 ；或者

在内嵌代码模块通过本地接口模块激活所述智能密钥设备的输入装置之后，所述客户

端主机的所述获取模块通过所述智能密钥设备的输入装置获取用户输入的数字关键信息，并根据所述复核信息标识符从所述交易报文中提取关键信息，再根据所述提取得到的关键信息对所述数字关键信息进行确认，若得到确认，则将所述关键信息进行拼接。

19. 根据权利要求 15 至 18 中任意一项所述的签名系统，所述客户端主机还包括：

转换模块，用于将所述交易报文的字符类型转换成所述智能密钥设备可识别的字符类型。

20. 根据权利要求 15 至 18 中任意一项所述的签名系统，其特征在于，所述客户端主机设有预设时间；所述客户端主机还包括：

第二发送模块，用于当所述本地接口模块在预设时间内接收到所述智能密钥设备发送的反馈信息，且所述反馈信息具体为签名时，发送所述签名和所述交易报文到所述服务器。

21. 根据权利要求 15 至 18 中任意一项所述的签名系统，其特征在于，所述客户端主机设有预设时间；所述客户端主机还包括：

取消发送模块，用于当所述本地接口模块在所述预设时间内接收到智能密钥设备发送的反馈信息，且所述反馈信息具体为取消信息时，向所述智能密钥设备发送取消操作指令；

取消接收模块，用于接收所述智能密钥设备报告的操作已取消的信息。

22. 根据权利要求 21 所述的签名系统，其特征在于，

所述取消发送模块还用于在所述预设时间到时前，所述客户端主机在等待接收智能密钥设备发送反馈信息时，随时向所述智能密钥设备发送取消操作指令。

23. 根据权利要求 15 所述的签名系统，其特征在于，所述智能密钥设备的所述获取模块包括：

检测单元，用于检测所述待签名数据包中的分隔符的数量；

解析单元，用于根据所述分隔符的数量解析所述待签名数据包中的关键信息。

24. 根据权利要求 15 或 23 所述的签名系统，其特征在于，所述智能密钥设备还包括：

取消模块，用于若在所述预设时间内未接收到用户输入的确认信息或者取消信息，或者若在所述预设时间内接收到所述客户端主机发送的取消操作指令，则取消操作，并向所述客户端主机报告操作已取消。

25. 根据权利要求 24 所述的签名系统，其特征在于，所述智能密钥设备还包括：

第一接收模块，用于接收所述客户端主机发送的取消操作指令；

则所述取消模块还用于当第一接收模块接收到所述取消操作指令时，取消操作并向所述客户端主机报告操作已取消。

26. 根据权利要求 15 或 23 所述的签名系统，其特征在于，所述智能密钥设备所述输出模块包括：

显示单元，用于通过显示器显示对应所述关键信息的复核信息标识符和所述关键信息；或者

播报单元，用于通过语音播放器播报对应所述关键信息的复核信息标识符和所述关键信息。

27. 根据权利要求 15 所述的签名系统，其特征在于，该服务器还包括：

转换模块，用于将所述交易报文中的字符类型转换成所述智能密钥设备可识别的字符

类型。

28. 根据权利要求 15 所述的签名系统，其特征在于，所述客户端主机设有预设时间；

所述服务器接收到的所述客户端主机发送的交易报文和签名是所述客户端主机在所述预设时间内接收到所述智能密钥设备发送的反馈信息，且所述反馈信息具体为签名时，所述客户端主机发送的交易报文和签名。

签名方法、设备及系统

技术领域

[0001] 本发明涉及信息安全领域，尤其涉及一种签名方法、设备及系统。

背景技术

[0002] 目前，网络文件的传输、网上银行交易已经成为人们生活或是工作的一部分。因此网络的安全性就更加成为了人们关注的焦点。

[0003] 为了确保网络数据在传输过程中不会被人恶意修改，出现了数字签名技术。数字签名技术即进行身份认证的技术。随着该项技术的发展和应用，尤其是在网上银行进行交易的过程中，对数据的签名过程已经发展到可在一种智能密钥设备中进行。对数据的签名在智能密钥设备中进行的过程主要包括：客户端主机在将数据发往服务器之前，先将数据发送到智能密钥设备内部，再在智能密钥设备内部完成对数据的签名过程。以此来保证数据信息的安全性。

[0004] 但是在上述的签名过程中发明人发现现有技术中至少存在如下问题：在智能密钥设备内部对数据进行签名之前，该数据仍旧是经过客户端主机的处理后再发送到智能密钥设备中的，如果此时客户端主机被黑客或病毒侵入，那么被客户端主机发送到智能密钥设备中的数据仍旧存在已经被篡改和截取的可能性，这就容易导致用户的数字签名被冒用，以至于无法保证数据信息的安全性。

发明内容

[0005] 本发明的实施例提供一种签名方法及系统，防止用户的签名被冒用，提高数据信息的安全性。

[0006] 为达到上述目的，本发明的实施例采用如下技术方案：

[0007] 一种签名方法，在客户端主机与服务器预先约定了复核信息标识符和分隔符后，包括：

[0008] 所述客户端主机与所述智能密钥设备建立连接；

[0009] 所述客户端主机通过输入装置接收用户输入的交易信息，所述输入装置包括所述客户端主机的输入装置和 / 或所述智能密钥设备的输入装置；

[0010] 所述客户端主机根据所述交易信息生成交易报文；

[0011] 所述客户端主机根据所述交易报文确定关键信息；

[0012] 所述客户端主机将包含所述关键信息和所述分隔符的待签名数据包发送到所述智能密钥设备；

[0013] 所述客户端主机等待接收所述智能密钥设备的反馈信息；

[0014] 所述智能密钥设备接收所述客户端主机发送的待签名数据包；

[0015] 所述智能密钥设备根据所述分隔符从所述待签名数据包中获取关键信息；

[0016] 所述智能密钥设备输出所述对应所述关键信息的复核信息标识符和所述关键信息，并等待用户输入信息；

[0017] 如果所述智能密钥设备在预设时间内接收到用户输入的确认信息，则

[0018] 所述智能密钥设备对所述待签名数据包进行签名，所述预设时间为所述等待用户输入信息的时间；

[0019] 将得到的签名作为反馈信息发送到所述客户端主机；

[0020] 所述服务器接收所述客户端主机发送的交易报文和签名；

[0021] 所述服务器根据所述复核信息标识符从所述交易报文中获取关键信息；

[0022] 所述服务器根据所述关键信息和所述分隔符生成待签名数据包；

[0023] 所述服务器利用所述待签名数字包对所述客户端主机发送的签名进行验证；

[0024] 如果所述智能密钥设备在预设时间内接收到用户输入的取消信息，则

[0025] 将所述取消信息作为反馈信息发送到所述客户端主机。

[0026] 一种签名系统，包括客户端主机、智能密钥设备和服务器，所述智能密钥设备连接到所述客户端主机，且所述客户端主机与服务器预先约定了复核信息标识符和分隔符；

[0027] 所述客户端主机包括：

[0028] 连接模块，用于与所述智能密钥设备建立连接；

[0029] 本地接口模块，用于通过输入装置接收用户输入的交易信息，所述输入装置包括所述客户端主机的输入装置和 / 或所述智能密钥设备的输入装置；

[0030] 生成模块，用于根据所述交易信息生成交易报文，

[0031] 获取模块，用于根据所述交易报文确定关键信息，

[0032] 第一发送模块，用于在将包含所述关键信息和所述分隔符的待签名数据包发送到所述智能密钥设备；

[0033] 接收模块，用于等待接收所述智能密钥设备的反馈信息；

[0034] 所述智能密钥设备包括：

[0035] 接收模块，用于接收所述客户端主机发送的待签名数据包；

[0036] 获取模块，用于根据所述分隔符从所述待签名数据包中获取关键信息；

[0037] 输出模块，用于输出所述对应所述关键信息的复核信息标识符和所述关键信息，并等待用户输入信息；

[0038] 签名模块，用于若在预设时间内接收到用户输入的确认信息，则对所述待签名数据包进行签名，所述预设时间为输出模块等待用户输入信息的时间；

[0039] 发送模块，用于将得到的签名作为反馈信息发送到所述客户端主机；

[0040] 所述发送模块，还用于若在预设时间内接收到用户输入的取消信息，则将所述取消信息作为反馈信息发送到所述客户端主机；

[0041] 所述服务器包括：

[0042] 接收模块，用于接收所述客户端主机发送的交易报文和签名；

[0043] 获取模块，用于根据所述复核信息标识符从所述交易报文中获取关键信息；

[0044] 生成模块，用于根据所述关键信息和所述分隔符生成待签名数据包；

[0045] 验证模块，用于利用所述待签名数字包，对所述客户端主机发送的签名进行验证。

[0046] 本发明提供的签名方法、设备及系统具有如下有益效果：在对接收到的交易报文进行数字签名前，采用了人机交互的方式使用户对关键信息进行复核，可避免在用户进行数字签名前，关键信息已经被篡改，数字签名被冒用的问题，取得了可防止用户的数字签名

被冒用，提高了数据信息安全性的技术效果。

附图说明

[0047] 为了更清楚地说明本发明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发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0048] 图 1 为本发明实施例 1 签名方法的流程示意图；

[0049] 图 2 为本发明实施例 2 中签名设备的结构示意图；

[0050] 图 3 为本发明实施例 3 中签名系统的结构示意图。

具体实施方式

[0051] 下面将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，都属于本发明保护的范围。

[0052] 实施例 1

[0053] 本实施例以智能密钥设备为USB Key时的情况为例下，具体说明一种签名方法。在本发明实施例中，USB Key 连接到客户端主机，且客户端主机与服务器预先约定了复核信息标识符和分隔符，其中上述USB Key上带有输出装置与按键，其中输出装置可以是液晶屏显示器，也可以是语音播报器。

[0054] 如图 1 所示，该方法包括：

[0055] 步骤 101：客户端主机与 USB Key 建立连接。

[0056] 步骤 102：客户端主机接收到用户输入的交易信息，并根据上述交易信息生成交易报文。

[0057] 在本实施例中，步骤 102 具体为：客户端主机的本地接口通过输入装置接收用户输入的交易信息，并将接收到的交易信息传给客户端主机的浏览器，客户端主机的浏览器通过运行内嵌代码将所述交易信息生成交易报文，并将所述交易报文传给该客户端主机的本地接口。

[0058] 其中，上述本地接口（可以是软件，也可以是硬件，或是两者结合）是预先安装在客户端主机上的，内嵌代码是指客户端主机的浏览器通过其软件从服务器端下载的网页中内嵌的代码。

[0059] 在本实施例步骤 102 中的提到的输入装置包括所述客户端主机的输入装置和 / 或所述 USB Key 的输入装置。即用户可以通过客户端主机的输入装置输入交易信息，也可以在 USB Key 带有输入装置时，用户通过 USB Key 的输入装置输入部分或全部交易信息。

[0060] 若用户通过 USB Key 的输入装置输入交易信息，则在步骤 102 之前还需要该客户端主机的内嵌代码先通过本地接口激活 USB Key 的输入装置。之后，在步骤 102 中用户才可通过 USB Key 的输入装置输入交易信息。

[0061] 在本发明实施例中，用户输入的交易信息为：

[0062] 转入户名：张三；

[0063] 转入帐号：4367420037465985234；

[0064] 转账金额：134.22；

[0065] 在本发明实施例中，交易报文的格式有多种，优选地，在本实施例中交易报文的格式为 XML 格式；

[0066] 在本发明实施例中，用户可以进行多种交易，相应地，客户端主机会生成多种交易报文，如，

[0067] 行内转账的交易报文为：

[0068]

```
<?xml version="1.0" encoding="utf-8"?>
<TradeInfo>
  <AccountInfo name="To"><!--转入帐号-->
    <AccountName>张三</AccountName><!--转入帐户姓名-->
    <AccountValue>4367420037465985234</AccountValue><!--转入帐
号-->
    <!--转入行信息-->
    <BankInfo>
      <BankName>北京分行</BankName><!--转入分行-->
    </BankInfo>
  </AccountInfo>
  <AccountInfo name="From">
    <AccountName>李四</AccountName><!--转出帐户姓名-->
```

[0069]

<AccountValue>4367420074923372387</AccountValue><!--转出帐号-->

<!--转出行信息-->

<BankInfo>

<BankName>上海分行</BankName><!--转出分行-->

</BankInfo>

</AccountInfo>

<TradeData>

<TradeMoney>134.22</TradeMoney> <!--转账金额-->

<TradeType>1</TradeType> <!--交易类型-->

<MoneyType>2</MoneyType> <!--货币类型-->

<TradeTime>20090206152645</TradeTime> <!--交易时间-->

<OtherData></OtherData> <!--其它数据-->

</TradeData>

<SignatureData> <!--base64 编码的签名数据-->

Mua1I09msIOE1IuIiH22Z8N57PzagkURn1xUgknTTXi88t+9u1Tzg01tcYZWdG+D3LOgDXfejPtjx01HSt293usQhRTt5SW8qte241Uvw0eMC0YHzH3Iwu0Jb5KErXrsg0OMWFZMnhbjF33pG1oQWMC23pe6Z98XCcnKR3nqBdY=

</SignatureData>

</TradeInfo>

[0070] 跨行转账的交易报文为：

[0071]

<?xml version="1.0" encoding="utf-8"?>

[0072]

```
<TradeInfo>
  <AccountInfo name="To"><!--转入帐号-->
    <AccountName>张三</AccountName><!--转入帐户姓名-->
    <AccountValue>60296930287452195</AccountValue><!--转入帐号
-->
    <!--转入行信息-->
    <BankInfo>
      <BankName> 北京银行</BankName><!--转入分行-->
    </BankInfo>
  </AccountInfo>
  <AccountInfo name="From">
    <AccountName>李四</AccountName><!--转出帐户姓名-->
    <AccountValue>4367420074923372387</AccountValue><!--转出帐
号-->
    <!--转出行信息-->
    <BankInfo>
      <BankName>中国建设银行北京分行</BankName><!--转出分行-->
    </BankInfo>
  </AccountInfo>
  <TradeData>
    <TradeMoney>134.22</TradeMoney>      <!--转账金额-->
    <TradeType>1</TradeType>             <!--交易类型-->
    <MoneyType>2</MoneyType>             <!--货币类型-->
```

[0073]

<TradeTime>20090206152645</TradeTime> <!--交易时间-->

<AddCode>5265</AddCode> <!--附加码-->

<OtherData></OtherData> <!--其它数据-->

</TradeData>

<SignatureData> <!--base64 编码的签名数据

-->

Mua1IO9msIOE1IuIiH22Z8N57PzagkURn1xUgknTTXi88t+9u1Tzg01tcYZWdG+D

3LOgDXfejPtjx01HSt293usQhRTt5SW8qte241Uvw0eMC0YHzH3Iwu0Jb5KErXrsg0OM

WFZMnhbjF33pG1oQWMC23pe6Z98XCcnKR3nqBdY=

</SignatureData>

</TradeInfo>

[0074] 追加账户的交易报文为：

[0075]

```
<?xml version="1.0" encoding="utf-8"?>
<!--追加帐号-->
<AccountInfo name="Add">
  <AccountType>1</AccountType><!--帐号类别-->
  <AccountName>张三</AccountName><!--户名-->
  <AccountValue>436742003746598523 4</AccountValue><!--帐号-->
  <AccountAlias>工资卡</AccountAlias><!--别名-->
  <AccountPwd>B53DC83D</AccountPwd><!--帐号密码-->
  <!--开户行信息-->
  <BankInfo>
    <BankName>北京分行</BankName>
```

[0076]

</BankInfo>

</AccountInfo>

[0077] 其中，在进行追加账户交易时，则该USB Key同样需要客户端主机的内嵌代码通过本地接口激活USB Key的输入装置，然后再由用户通过USB Key的输入装置输入密码，并由客户端主机的本地接口传给其内嵌代码，这样就可以避免被在客户端主机中运行的木马窃取密码。

[0078] 步骤103：客户端主机对交易报文进行解析，并根据预先约定的复核信息标识符提取关键信息，组成待签名数据包，再将上述待签名数据包发送给USB Key，同时等待该USB Key发送过来的反馈信息，该客户端主机设有预设时间，用于等待该USB Key发送过来的反馈信息。

[0079] 本实施例步骤103具体为：客户端主机的本地接口接收到该交易报文，并根据预先约定的复核信息标识符从交易报文中提取关键信息，客户端主机的本地接口将提取各个关键信息以预先约定的顺序拼接在一起，并用“；”作为各个关键信息之间的分隔符将各个关键信息进行分隔，以组成待签名数据包，同时等待该USB Key发送过来的反馈信息，该客户端主机设有预设时间，用于等待该USB Key发送过来的反馈信息。在本实施例中该反馈信息可以为取消信息，也可以为签名等。

[0080] 例如：设在行内转账交易报文中，复核信息标识符为户名、帐号、金额。根据该复核信息标识符从行内转账交易报文中提取的关键信息为：

[0081] 张三（户名）4367420037465985234（帐号）134.22（金额）

[0082] 生成的待签名数据包为：

[0083] 4367420037465985234；张三；134.22；

[0084] 设在跨行转账交易报文中，复核信息标识符为户名、帐号、金额、附加验证码。则根据该复核信息标识符从跨行转账交易报文提取的关键信息为：

[0085] 张三（户名）60296930287452195（帐号）134.22（金额）5265（附加验证码）

[0086] 其中的附加验证码是由服务器端随机生成的；

[0087] 生成的待签名数据包为：

[0088] 60296930287452195；张三；134.22；5265；

[0089] 设在追加账户交易报文中，复核信息标识符为帐号、密码。则根据该复核信息标识符从追加账户交易报文中提取的关键信息为：

[0090] 4367420037465985234（帐号）B53DC83D（密码）

[0091] 生成的待签名数据包为：

[0092] 4367420037465985234；B53DC83D；

[0093] 在本实施例中步骤103还可以为：

[0094] 客户端主机接收用户通过USB Key的输入装置输入的数字关键信息（例如：当为行内转账交易报文时，该数字关键信息可为：4367420037465985234（帐号）134.22（金额）），并根据预先约定的复核信息标识符从步骤102中生成的交易报文中提取关键信息（例如：当为行内转账交易报文时，该提取的关键信息可为：张三（户名）134.22（金额）），再将提取的金额关键信息返回给USB Key，USB Key比较上述用户输入的金额与

客户端主机返回的金额是否一致，若不一致，则提示出错信息，若一致，则再次将金额关键信息发送给客户端主机，客户端主机对上述户名、帐号和金额关键信息（即对：张三4367420037465985234134.22）进行拼接，并用“；”作为各个关键信息之间的分隔符将各个关键信息进行分隔，组成待签名数据包，再将上述待签名数据包发送给 USB Key，并等待接收 USB Key 发送的反馈信息；该客户端主机设有预设时间，用于等待该 USBKey 发送过来的反馈信息。

[0095] 其中，需要说明的是：因为现有技术中的 USB Key 的输入装置只带有数字按键，所以所述用户通过USB Key的输入装置输入的关键信息也只可能是由数字构成的数字关键信息，该数字关键信息可以只是关键信息的一部分；并且在步骤 102 中，若用户仅是通过客户端主机的输入装置输入交易信息的，那么在上述客户端主机接收用户通过 USB Key 的输入装置输入的关键信息之前，还需要进行如下步骤：

[0096] 客户端主机的内嵌代码通过本地接口激活 USB Key 的输入装置。

[0097] 在本实施例中，客户端主机还需对交易报文中的某些字符进行转换以适应 USB Key。

[0098] 例如：若交易报文中的户名是 UTF-8 编码的汉字字符，而 USB Key 支持的是 GB18030 字符集，则客户端主机将户名转换成 GB18030 编码的字符。

[0099] 步骤 104：USB Key 接收上述待签名数据包，并根据所述分隔符从所述待签名数据包中获取关键信息。

[0100] 在本实施例步骤 104 中，所述根据所述分隔符从所述待签名数据包中获取关键信息具体为：USB Key 检测上述待签名数据包中的分隔符“；”数量，并根据所述分隔符的数量解析待签名数据包，从解析的结果中 USB Key 可获取关键信息，具体如下：

[0101] 若 USB Key 检测到 2 个分隔符，则表示该交易信息为追加账户交易，关键信息依次为帐号和密码。即在本实施例中为：

[0102] 4367420037465985234（帐号）B53DC83D（密码）

[0103] 若 USB Key 检测到 3 个分隔符，则表示该交易信息为行内转账交易，关键信息依次为帐号、户名和金额。即在本实施例中为

[0104] 张三（户名）4367420037465985234（帐号）134.22（金额）

[0105] 若 USB Key 检测到 4 个分隔符，则表示该交易信息为跨行转账交易，关键信息依次为帐号、户名、金额和附加验证码；即在本实施例中为

[0106] 张三（户名）60296930287452195（帐号）134.22（金额）5265（附加验证码）

[0107] 其他，则表示为非交易报文。

[0108] 步骤 105：USB Key 根据解析得到的结果输出所述与所述关键信息对应的复核信息标识符和所述关键信息，并等待用户输入信息；

[0109] 在本实施例中，步骤 105 具体可为：

[0110] 若为追加账户交易，则USB Key显示或者语音播报复核信息标识符——帐号，和关键信息——4367420037465985234，等待用户输入密码并按键确认，USBKey 对用户输入的密码进行验证，如果验证失败，则执行步骤 106，否则执行步骤 107；

[0111] 若为行内转账交易，则 USB Key 分别对应显示或者语音播报复核信息标识符——户名、帐号和金额，和关键信息——张三 4367420037465985234134.22，等待用户输入信息。

若用户通过按键输入的信息为取消信息，则执行步骤 106，若用户通过按键输入的信息为确认信息，则执行步骤 107 ；

[0112] 若为跨行转账交易，则 USB Key 分别对应显示或者语音播报复核信息标识符——户名、帐号、金额和附加验证码，关键信息——张三 60296930287452195134.225 265，等待用户输入信息，若用户通过按键输入的信息为取消信息，则执行步骤 106，若用户通过按键输入的附加验证码并且按键确认，则 USB Key 使用用户输入的附加验证码代替交易报文中的验证码进行运算，若运算出错，则执行步骤 106，若运算成功，则执行步骤 107 ；

[0113] 若为其他，则执行步骤 107。

[0114] 步骤 106 ：USB Key 向客户端主机提示出错信息或取消信息。

[0115] 步骤 1061 ：客户端主机向该 USB Key 发生取消操作指令，该 USB Key 接收到该取消操作的指令后取消操作并向该客户端主机报告操作已取消。

[0116] 在本实例中客户端主机还可以随时向该 USB Key 发送取消操作指令，即客户端主机可以随时执行步骤 1061。

[0117] 另外需要说明的是在本实施例中执行过步骤 1061 后将不再执行本实施例中的下述步骤。

[0118] 步骤 107 ：USB Key 对上述待签名数据包进行签名，并将得到的签名发送给客户端主机。

[0119] USB Key 对待签名数据包进行签名具体为 ：USB Key 可以采用散列 (HASH) 算法计算待签名数据包的摘要，然后采用公钥密码算法对摘要进行加密，得到签名。

[0120] 步骤 108 ：客户端主机在预设时间内接收到该 USB Key 发送的签名，并将交易报文以及接收到的签名发送给服务器端。

[0121] 步骤 109 ：服务器端接收客户端主机发送的所述交易报文和签名，并根据预先约定的复核信息标识符从接收到的交易报文中提取关键信息。

[0122] 在本实施例步骤 109 中，服务器端与客户端主机事先进行约定，若客户端主机在步骤 103 中进行了字符转换，则服务器端也需要进行相应地字符转换。

[0123] 步骤 110 ：服务器端根据提取得到的关键信息组成待签名数据包，并计算待签名数据包的摘要 ；

[0124] 在本实施例步骤 110 中，服务器端根据提取得到的关键信息生成待签名数据包的步骤具体为 ：服务器根据将提取得到的各个关键信息以预先约定的顺序拼接在一起，并用“ ；”作为各个关键信息之间的分隔符将各个关键信息进行分隔，以组成待签名数据包。

[0125] 在本实施例步骤 110 中，服务器端计算待签名数据包的摘要所使用的算法与步骤 107 中 USB Key 计算待签名数据包的摘要所使用的算法相同。

[0126] 步骤 111 ：服务器端对接收到的客户端主机发送的签名进行解密，得到解密结果。

[0127] 步骤 112 ：服务器端比较步骤 110 中计算得到的待签名数据包的摘要与步骤 111 中得到的解密结果是否相同，若相同，则验证成功，若不相同，则验证失败。

[0128] 本实施例提供的签名方法具有如下有益效果 ：在签名流程中增加了人机交互复核过程，使智能密钥设备在执行数字签名前可经过用户的复核，降低了数字签名被他人冒用的可能性，提高了数据信息的安全性，并且本实施例的交易报文中，复核信息与交易信息分开表示有利于提高系统的可扩展性。

[0129] 实施例 2

[0130] 本实施例提供一种客户端主机 20，一种智能密钥设备 30 和一种服务器 40。以便于上述实施例 1 中的方法实施。其中，智能密钥设备 30 连接到客户端主机 20，且客户端主机 20 与服务器 40 预先约定了复核信息标识符和分隔符。如图 2 所示，该客户端主机 20 包括：连接模块 21，本地接口模块 22，生成模块 23，获取模块 24，第一发送模块 25，接收模块 26。

[0131] 连接模块 21 用于与智能密钥设备 30 建立连接；在连接模块 21 与智能密钥设备 30 建立起连接后，本地接口模块 22 用于通过输入装置接收用户输入的交易信息，所述输入装置包括所述客户端主机的输入装置和 / 或所述智能密钥设备的输入装置；生成模块 23 用于根据所述交易信息生成交易报文；获取模块 24 用于根据所述交易报文确定关键信息；第一发送模块 25 用于将包含所述分隔符和所述获取模块 24 获取的所述关键信息的待签名数据包发送到所述智能密钥设备 30；接收模块 26 用于在发送模块 25 将所述待签名数据包发送后，等待接收所述智能密钥设备 30 的反馈信息。

[0132] 进一步，在本实施例中客户端主机 20 还包括如下可选模块：内嵌代码模块 27，转换模块 28。

[0133] 内嵌代码模块 27 用于通过所述本地接口模块 22 激活所述智能密钥设备 30 的输入装置；转换模块 28 用于将所述交易报文的字符类型转换成所述智能密钥设备 30 可识别的字符类型。

[0134] 其中，上述生成模块 23 通过所述内嵌代码模块 27 将所述交易信息生成交易报文。上述本地接口模块 22 还用于对生成模块 23 生成的交易报文进行解析，并获得关键信息。

[0135] 其中，获取模块 24 具体可用于根据所述复核信息标识符从本地接口模块 22 接收到的所述交易报文中获取关键信息；或者在内嵌代码模块 27 通过本地接口模块激活所述智能密钥设备的输入装置之后，获取模块 24 通过所述智能密钥设备的输入装置获取用户输入的数字关键信息，并根据所述复核信息标识符从所述交易报文中提取关键信息，再根据得到得到的关键信息对所述数字关键信息进行确认，若得到确认，则将所述关键信息进行拼接。

[0136] 本发明实施例的各个模块可以集成于一体，也可以分离部署。上述模块可以合并为一个模块，也可以进一步拆分成多个子模块。

[0137] 进一步，在本实施例中客户端主机 20 设有预设时间，并且客户端主机 20 还可包括如下可选模块：第二发送模块 29，取消发送模块 210，取消接收模块 211。

[0138] 第二发送模块 29 用于当所述本地接口模块 22 在预设时间内接收到所述智能密钥设备 30 发送的反馈信息，且所述反馈信息具体为签名时，发送所述签名和所述交易报文到服务器 40；取消发送模块 210 用于当所述本地接口模块 22 在所述预设时间内接收到智能密钥设备 30 发送的反馈信息，且所述反馈信息具体为取消信息时，向所述智能密钥设备发送取消操作指令，取消发送模块 210 还用于在所述预设时间到时前，所述客户端主机 20 在等待接收智能密钥设备 30 发送反馈信息时，随时向所述智能密钥设备 30 发送取消操作指令；取消接收模块 211 用于接收所述智能密钥设备 30 报告的操作已取消的信息。

[0139] 本实施例所提供的客户端主机具有如下有益效果：可通过智能密钥设备的输入装置输入交易信息，降低了交易信息被盗用的可能性。可获取关键信息，并将获取的关键信息

发送到智能密钥设备，以便智能密钥设备对其进行复核，增加数据信息的安全性。

[0140] 本实施例提供的智能密钥设备30可以具体为USB Key，如图2所示，该智能密钥设备30包括：接收模块31，获取模块32，输出模块33，签名模块34，发送模块35。

[0141] 接收模块31用于接收客户端主机20发送的待签名数据包；获取模块32用于根据所述分隔符从接收模块31接收到的所述待签名数据包中获取关键信息；输出模块33用于输出所述对应所述关键信息的复核信息标识符和所述关键信息，并等待用户输入信息，该关键信息是由获取模块32获取到的；签名模块34用于当在预设时间内接收到用户输入的确认信息时，对所述待签名数据包进行签名，所述预设时间为输出模块33等待用户输入信息的时间；发送模块35用于将签名模块34得到的签名作为反馈信息发送到所述客户端主机20；所述发送模块35还用于若在预设时间内接收到用户输入的取消信息，则将所述取消信息作为反馈信息发送到所述客户端主机30。

[0142] 其中，获取模块32包括：检测单元321，解析单元322。

[0143] 检测单元321用于检测所述待签名数据包中的分隔符的数量；解析单元322用于根据检测单元321检测出的所述分隔符的数量解析所述待签名数据包中的关键信息。

[0144] 输出模块33包括：显示单元331。显示单元331用于通过显示器显示对应所述关键信息的复核信息标识符和所述关键信息；或者在本实施例中，显示单元331还可以用播报单元进行替换，该播报单元用于通过语音播放器播报对应所述关键信息的复核信息标识符和所述关键信息。

[0145] 进一步，在本实施例中提供的智能密钥设备30还可包括如下可选模块：取消模块36，第一接收模块37。

[0146] 取消模块36用于若在所述预设时间内未接收到用户输入的确认信息或者取消信息，或者若在所述预设时间内接收到所述客户端主机20发送的取消操作指令，则取消操作，并向客户端主机20报告操作已取消；第一接收模块37用于接收到客户端主机20发送的取消操作指令；则所述取消模块还用于当第一接收模块37接收到所述取消操作指令时，取消操作并向所述客户端主机20报告操作已取消。

[0147] 本实施例提供的智能密钥设备具有如下有益效果：可进行人机交互复核，使用户对交易的关键信息进行确认，可防止交易信息被篡改，用户签名被冒用，提高了数据信息的安全性。

[0148] 下面继续介绍本实施例提供的服务器40，如图2所示，该服务器40包括：接收模块41，获取模块42，生成模块43，验证模块44。

[0149] 接收模块41用于接收客户端主机20发送的交易报文和签名；获取模块42用于根据所述复核信息标识符从接收模块41所述交易报文中获取关键信息；生成模块43用于根据获取模块42获取的关键信息和所述分隔符生成待签名数据包；验证模块44用于利用生成模块43生成的待签名数字包对客户端主机20发送的签名进行验证。

[0150] 其中，在本实施例中的验证模块44包括：计算单元441、解密单元442和判断单元443。

[0151] 计算单元441用于计算所述待签名数据包的摘要；解密单元442用于对接收到的客户端主机20发送的签名进行解密；判断单元443用于判断解密单元442得到的解密结果是否与计算单元441得到的待签名数据包的摘要一致，如果两者一致，则判定通过验证；如

果两者不一致，则判定验证失败。

[0152] 进一步，在本实施例中服务器 40 还可包括如下可选模块：转换模块 45。

[0153] 转换模块 45 用于将所述交易报文中的字符类型转换成智能密钥设备 30 可识别的字符类型。

[0154] 本实施例提供的服务器方案可配置客户端主机和智能密钥设备完成对交易信息的人机交互复核的实现，解决了现有技术中用户的签名被他人冒用的技术问题，进而取得了可防止合法用户的签名被他人冒用，提高了数据信息的安全性的技术效果。

[0155] 实施例 3

[0156] 本实施例提供一种签名系统，如图 3 所示，该系统包括客户端主机 200、智能密钥设备 300 和服务器 400，智能密钥设备 300 连接到客户端主机 200，且客户端主机 200 与服务器 400 预先约定了复核信息标识符和分隔符；

[0157] 其中，客户端主机 200 用于与智能密钥设备 300 建立连接，通过输入装置接收用户输入的交易信息，所述输入装置包括客户端主机 200 的输入装置和 / 或智能密钥设备 300 的输入装置，根据所述交易信息生成交易报文，并根据所述交易报文确定关键信息，在将包含所述关键信息和所述分隔符的待签名数据包发送到所述智能密钥设备 300 之后，等待接收所述智能密钥设备 300 的反馈信息；智能密钥设备 300 用于接收客户端主机 200 发送的待签名数据包，并根据所述分隔符从所述待签名数据包中获取关键信息，输出所述对应所述关键信息的复核信息标识符和所述关键信息，并等待用户输入信息，当在预设时间内接收到用户输入的确认信息时，对所述待签名数据包进行签名，所述预设时间为所述等待用户输入信息的时间，将得到的签名作为反馈信息发送到所述客户端主机 200；当在预设时间内接收到用户输入的取消信息时，将所述取消信息作为反馈信息发送到客户端主机 200；服务器 400 用于接收所述客户端主机 200 发送的交易报文和签名，根据所述复核信息标识符从所述交易报文中获取关键信息，并根据所述关键信息和所述分隔符生成待签名数据包，利用所述待签名数字包对所述客户端主机 200 发送的签名进行验证。

[0158] 在本实施例中的述客户端主机 200 设有预设时间。服务器 400 接收到的客户端主机 200 发送的交易报文和签名是客户端主机 200 在所述预设时间内接收到所述智能密钥设备 300 发送的反馈信息，且所述反馈信息具体为签名时，客户端主机 200 发送的交易报文和签名。

[0159] 本实施例提供的签名系统具有如下有益效果：在签名流程中增加了人机交互复核过程，使智能密钥设备在执行数字签名前可经过用户的复核，降低了数字签名被他人冒用的可能性，提高了数据信息的安全性。

[0160] 通过以上的实施方式的描述，所属领域的技术人员可以清楚地了解到本发明可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明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，该计算机软件产品存储在可读取的存储介质中，如计算机的软盘，硬盘或光盘等，包括若干指令用以使得一台设备或装置执行本发明各个实施例所述的方法。

[0161] 以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到变化或替换，都应涵

盖在本发明的保护范围之内。因此，本发明的保护范围应所述以权利要求的保护范围为准。

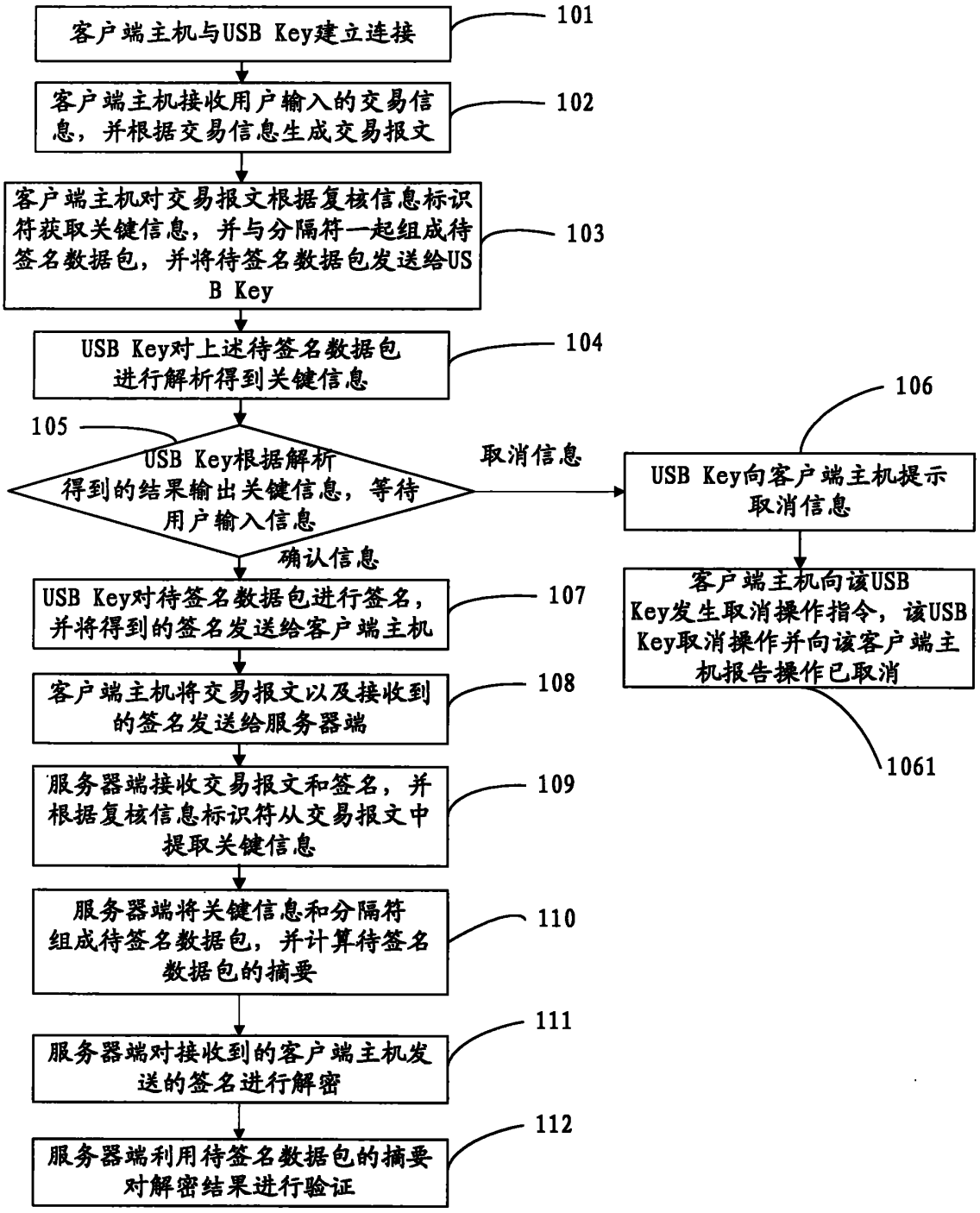

客户端主机与USB Key建立连接
101
客户端主机接收用户输入的交易信息，并根据交易信息生成交易报文
102
客户端主机对交易报文根据复核信息标识符获取关键信息，并与分隔符一起组成待签名数据包，并将待签名数据包发送给USB Key
103
USB Key对上述待签名数据包进行解析得到关键信息
104
105
USB Key根据解析得到的结果输出关键信息，等待用户输入信息
取消信息
106
USB Key向客户端主机提示取消信息
客户端主机向该USB Key发生取消操作指令，该USB Key取消操作并向该客户端主机报告操作已取消
1061
确认信息
USB Key对待签名数据包进行签名，并将得到的签名发送给客户端主机
107
客户端主机将交易报文以及接收到的签名发送给服务器端
108
服务器端接收交易报文和签名，并根据复核信息标识符从交易报文中提取关键信息
109
服务器端将关键信息和分隔符组成待签名数据包，并计算待签名数据包的摘要
110
服务器端对接收到的客户端主机发送的签名进行解密
111
服务器端利用待签名数据包的摘要对解密结果进行验证
112

图 1

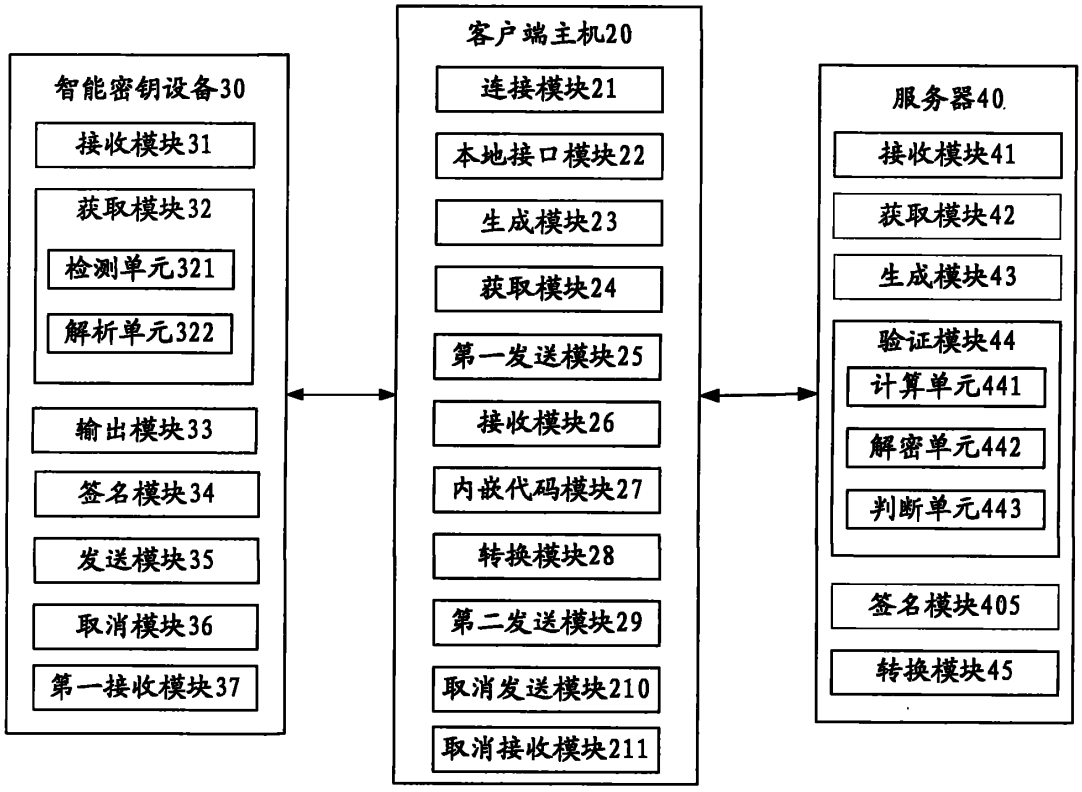

智能密钥设备30
接收模块31
获取模块32
检测单元321
解析单元322
输出模块33
签名模块34
发送模块35
取消模块36
第一接收模块37
客户端主机20
连接模块21
本地接口模块22
生成模块23
获取模块24
第一发送模块25
接收模块26
内嵌代码模块27
转换模块28
第二发送模块29
取消发送模块210
取消接收模块211
服务器40
接收模块41
获取模块42
生成模块43
验证模块44
计算单元441
解密单元442
判断单元443
签名模块405
转换模块45

图 2

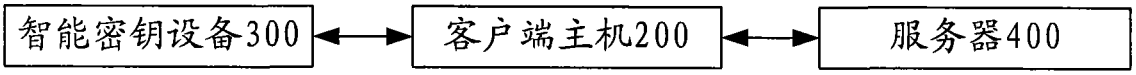

智能密钥设备300
客户端主机200
服务器400

图 3