(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114697117 B
(45)授权公告日 2023.11.24

(21)申请号 202210359883.X
(22)申请日 2022.04.07
(65)同一申请的已公布的文献号
申请公布号 CN 114697117 A
(43)申请公布日 2022.07.01
(73)专利权人 中国工商银行股份有限公司
地址 100140 北京市西城区复兴门内大街55号
(72)发明人 欧少焕 雷斌 李冠彬 胡文涛
(74)专利代理机构 北京三友知识产权代理有限公司 11127
专利代理师 刘熔 董骁毅
(51)Int.Cl.
H04L 9/40(2022.01)
H04L 9/06(2006.01)
H04L 9/08(2006.01)
G01S 19/14(2010.01)

(56)对比文件
CN 101399666 A,2009.04.01
CN 103577996 A,2014.02.12
CN 114124480 A,2022.03.01
CN 114157451 A,2022.03.08
US 10673617 B1,2020.06.02
US 2018176017 A1,2018.06.21
US 2019052467 A1,2019.02.14
WO 2021208037 A1,2021.10.21

审查员 牛犇

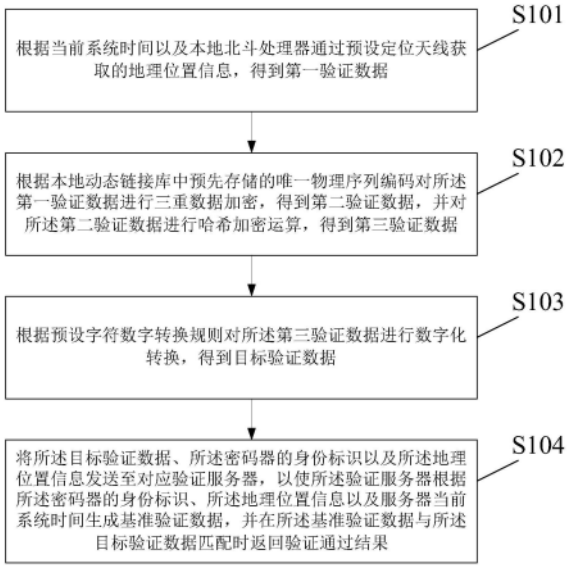
权利要求书3页 说明书13页 附图5页

(54)发明名称

基于定位信息的验证方法、装置、密码器及系统

(57)摘要

本申请实施例提供一种基于定位信息的验证方法、装置、密码器及系统，可用于金融领域，方法包括：根据当前系统时间以及本地北斗处理器通过预设定位天线获取的地理位置信息，得到第一验证数据；根据本地动态链接库中预先存储的唯一物理序列编码对所述第一验证数据进行三重数据加密，得到第二验证数据，并对所述第二验证数据进行哈希加密运算，得到第三验证数据；根据预设字符数字转换规则对所述第三验证数据进行数字化转换，得到目标验证数据；将所述目标验证数据、所述密码器的身份标识以及所述地理位置信息发送至对应验证服务器；本申请能够准确、便捷得对交易进行验证。



CN 114697117 B

1.一种基于定位信息的验证方法,其特征在于,应用于密码器,所述方法包括:

根据当前系统时间以及本地北斗处理器通过预设定位天线获取的地理位置信息,得到第一验证数据;

根据本地动态链接库中预先存储的唯一物理序列编码对所述第一验证数据进行三重数据加密,得到第二验证数据,并对所述第二验证数据进行哈希加密运算,得到第三验证数据;

根据预设字符数字转换规则对所述第三验证数据进行数字化转换,得到目标验证数据;

将所述目标验证数据、所述密码器的身份标识以及所述地理位置信息发送至对应验证服务器,以使所述验证服务器根据所述密码器的身份标识、所述地理位置信息以及服务器当前系统时间生成基准验证数据,并在所述基准验证数据与所述目标验证数据匹配时返回验证通过结果。

2.根据权利要求1所述的基于定位信息的验证方法,其特征在于,所述当前系统时间以及本地北斗处理器通过预设定位天线获取的地理位置信息,得到第一验证数据,包括:

将当前系统时间和本地北斗处理器通过预设定位天线获取的地理位置信息转换为二进制编码,并拼接得到第一验证数据。

3.根据权利要求1所述的基于定位信息的验证方法,其特征在于,所述根据本地动态链接库中预先存储的唯一物理序列编码对所述第一验证数据进行三重数据加密,得到第二验证数据,包括:

对本地动态链接库中预先存储的唯一物理序列编码进行混淆和对半交换处理,得到第一加密密钥;

根据所述本地动态链接库中预先存储的第二加密密钥对所述第一加密密钥进行密文分组链接模式的三重数据加密,得到第三加密密钥;

根据所述第三加密密钥对所述第一验证数据进行三重数据加密,得到第二验证数据。

4.根据权利要求1所述的基于定位信息的验证方法,其特征在于,所述根据预设字符数字转换规则对所述第三验证数据进行数字化转换,得到目标验证数据,包括:

根据预设字符数字转换规则将所述第三验证数据中的英文字符段转换为相应的数字段;

根据所述数字段生成对应的目标验证二维码进行展示,以使验证服务器获取所述目标验证二维码中的目标验证数据。

5.一种基于定位信息的验证方法,其特征在于,应用于验证服务器,所述方法包括:

接收密码器发送的目标验证数据、密码器的身份标识以及地理位置信息,其中,所述密码器的身份标识与密码器本地动态链接库中预先存储的唯一物理序列编码对应,所述地理位置信息由密码器本地北斗处理器通过预设定位天线获取得到,所述目标验证数据是由所述密码器根据当前系统时间和所述地理位置信息得到第一验证数据后,根据所述唯一物理序列编码对所述第一验证数据进行三重数据加密,得到第二验证数据,并对所述第二验证数据进行哈希加密运算,得到第三验证数据,根据预设字符数字转换规则对所述第三验证数据进行数字化转换得到的;

根据所述密码器的身份标识、所述地理位置信息以及服务器当前系统时间生成基准验

证数据,并在所述基准验证数据与所述目标验证数据匹配时返回验证通过结果。

6.根据权利要求5所述的基于定位信息的验证方法,其特征在于,在所述接收密码器发送的目标验证数据、密码器的身份标识以及地理位置信息后,还包括:

若所述地理位置信息中的经纬度坐标超出与所述密码器的身份标识对应的电子围栏,则向所述密码器返回一交易报错信号。

7.一种基于定位信息的密码器,其特征在于,包括:中央处理器、北斗处理器以及时钟模块;

所述北斗处理器用于通过预设定位天线获取的地理位置信息;

所述时钟模块用于获取当前系统时间;

所述中央处理器用于:

根据所述当前系统时间和所述地理位置信息,得到第一验证数据;

根据本地动态链接库中预先存储的唯一物理序列编码对所述第一验证数据进行三重数据加密,得到第二验证数据,并对所述第二验证数据进行哈希加密运算,得到第三验证数据;

根据预设字符数字转换规则对所述第三验证数据进行数字化转换,得到目标验证数据;

将所述目标验证数据、所述密码器的身份标识以及所述地理位置信息发送至对应验证服务器,以使所述验证服务器根据所述密码器的身份标识、所述地理位置信息以及服务器当前系统时间生成基准验证数据,并在所述基准验证数据与所述目标验证数据匹配时返回验证通过结果。

8.一种基于定位信息的验证装置,其特征在于,包括:

数据接收模块,用于接收密码器发送的目标验证数据、密码器的身份标识以及地理位置信息,其中,所述密码器的身份标识与密码器本地动态链接库中预先存储的唯一物理序列编码对应,所述地理位置信息由密码器本地北斗处理器通过预设定位天线获取得到,所述目标验证数据是由所述密码器根据当前系统时间和所述地理位置信息得到第一验证数据后,根据所述唯一物理序列编码对所述第一验证数据进行三重数据加密,得到第二验证数据,并对所述第二验证数据进行哈希加密运算,得到第三验证数据,根据预设字符数字转换规则对所述第三验证数据进行数字化转换得到的;

数据验证模块,用于根据所述密码器的身份标识、所述地理位置信息以及服务器当前系统时间生成基准验证数据,并在所述基准验证数据与所述目标验证数据匹配时返回验证通过结果。

9.一种基于定位信息的验证系统,其特征在于,包括:密码器和与所述密码器通信连接的验证服务器;

所述密码器包括:中央处理器、北斗处理器以及时钟模块;

所述北斗处理器用于通过预设定位天线获取的地理位置信息;

所述时钟模块用于获取当前系统时间;

所述中央处理器用于:

根据所述当前系统时间和所述地理位置信息,得到第一验证数据;

根据本地动态链接库中预先存储的唯一物理序列编码对所述第一验证数据进行三重

数据加密,得到第二验证数据,并对所述第二验证数据进行哈希加密运算,得到第三验证数据;

根据预设字符数字转换规则对所述第三验证数据进行数字化转换,得到目标验证数据;

将所述目标验证数据、所述密码器的身份标识以及所述地理位置信息发送至对应验证服务器;

所述验证服务器包括:

数据接收模块,用于接收密码器发送的目标验证数据、密码器的身份标识以及地理位置信息;

数据验证模块,用于根据所述密码器的身份标识、所述地理位置信息以及服务器当前系统时间生成基准验证数据,并在所述基准验证数据与所述目标验证数据匹配时返回验证通过结果。

10.一种电子设备,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,其特征在于,所述处理器执行所述程序时实现权利要求1至6任一项所述的基于定位信息的验证方法的步骤。

11.一种计算机可读存储介质,其上存储有计算机程序,其特征在于,该计算机程序被处理器执行时实现权利要求1至6任一项所述的基于定位信息的验证方法的步骤。

基于定位信息的验证方法、装置、密码器及系统

技术领域

[0001] 本申请涉及交易安全领域，也可用于金融领域，具体涉及一种基于定位信息的验证方法、装置、密码器及系统。

背景技术

[0002] 随着科技发展，人们的生活水平越来越高，互联网无处不在，收单形式也多样化。线上交易、手机银行转帐也越来越多。

[0003] 现有技术中为了交易安全，往往在线上交易或转帐时通过插u盾或数字动态密码器来增加交易安全性，但是，插u盾需要装驱动，数字动态密码器也需要在规定时间内输入，两者在使用时均存在不便捷的问题，怎样才能使转帐能够快速又安全的完成密码或动态码的校验、提升交易便捷性，是亟需解决的问题。

发明内容

[0004] 针对现有技术中的问题，本申请提供一种基于定位信息的验证方法、装置、密码器及系统，能够准确、便捷得对交易进行验证。

[0005] 为了解决上述问题中的至少一个，本申请提供以下技术方案：

[0006] 第一方面，本申请提供一种基于定位信息的验证方法，包括：

[0007] 根据当前系统时间以及本地北斗处理器通过预设定位天线获取的地理位置信息，得到第一验证数据；

[0008] 根据本地动态链接库中预先存储的唯一物理序列编码对所述第一验证数据进行三重数据加密，得到第二验证数据，并对所述第二验证数据进行哈希加密运算，得到第三验证数据；

[0009] 根据预设字符数字转换规则对所述第三验证数据进行数字化转换，得到目标验证数据；

[0010] 将所述目标验证数据、所述密码器的身份标识以及所述地理位置信息发送至对应验证服务器，以使所述验证服务器根据所述密码器的身份标识、所述地理位置信息以及服务器当前系统时间生成基准验证数据，并在所述基准验证数据与所述目标验证数据匹配时返回验证通过结果。

[0011] 进一步地，所述当前系统时间以及本地北斗处理器通过预设定位天线获取的地理位置信息，得到第一验证数据，包括：

[0012] 将当前系统时间和本地北斗处理器通过预设定位天线获取的地理位置信息转换为二进制编码，并拼接得到第一验证数据。

[0013] 进一步地，所述根据本地动态链接库中预先存储的唯一物理序列编码对所述第一验证数据进行三重数据加密，得到第二验证数据，包括：

[0014] 对本地动态链接库中预先存储的唯一物理序列编码进行混淆和对半交换处理，得到第一加密密钥；

[0015] 根据所述本地动态链接库中预先存储的第二加密密钥对所述第一加密密钥进行密文分组链接模式的三重数据加密,得到第三加密密钥;

[0016] 根据所述第三加密密钥对所述第一验证数据进行三重数据加密,得到第二验证数据。

[0017] 进一步地,所述根据预设字符数字转换规则对所述第三验证数据进行数字化转换,得到目标验证数据,包括:

[0018] 根据预设字符数字转换规则将所述第三验证数据中的特定字符段转换为相应的数字段;

[0019] 根据所述数字段生成对应的目标验证二维码进行展示,以使验证服务器获取所述目标验证二维码中的目标验证数据。

[0020] 第二方面,本申请提供一种基于定位信息的验证方法,包括:

[0021] 接收密码器发送的目标验证数据、密码器的身份标识以及地理位置信息,其中,所述密码器的身份标识与密码器本地动态链接库中预先存储的唯一物理序列编码对应,所述地理位置信息由密码器本地北斗处理器通过预设定位天线获取得到,所述目标验证数据是由所述密码器根据当前系统时间和所述地理位置信息得到第一验证数据后,根据所述唯一物理序列编码对所述第一验证数据进行三重数据加密,得到第二验证数据,并对所述第二验证数据进行哈希加密运算,得到第三验证数据,根据预设字符数字转换规则对所述第三验证数据进行数字化转换得到的;

[0022] 根据所述密码器的身份标识、所述地理位置信息以及服务器当前系统时间生成基准验证数据,并在所述基准验证数据与所述目标验证数据匹配时返回验证通过结果。

[0023] 进一步地,在所述接收密码器发送的目标验证数据、密码器的身份标识以及地理位置信息后,还包括:

[0024] 若所述地理位置信息中的经纬度坐标超出与所述密码器的身份标识对应的电子围栏,则向所述密码器返回一交易报错信号。

[0025] 第三方面,本申请提供一种基于定位信息的密码器,包括:中央处理器、北斗处理器以及时钟模块;

[0026] 所述北斗处理器用于通过预设定位天线获取的地理位置信息;

[0027] 所述时钟模块用于获取当前系统时间;

[0028] 所述中央处理器用于:

[0029] 根据所述当前系统时间和所述地理位置信息,得到第一验证数据;

[0030] 根据本地动态链接库中预先存储的唯一物理序列编码对所述第一验证数据进行三重数据加密,得到第二验证数据,并对所述第二验证数据进行哈希加密运算,得到第三验证数据;

[0031] 根据预设字符数字转换规则对所述第三验证数据进行数字化转换,得到目标验证数据;

[0032] 将所述目标验证数据、所述密码器的身份标识以及所述地理位置信息发送至对应验证服务器,以使所述验证服务器根据所述密码器的身份标识、所述地理位置信息以及服务器当前系统时间生成基准验证数据,并在所述基准验证数据与所述目标验证数据匹配时返回验证通过结果。

[0033] 第四方面,本申请提供一种基于定位信息的验证装置,包括:

[0034] 数据接收模块,用于接收密码器发送的目标验证数据、密码器的身份标识以及地理位置信息,其中,所述密码器的身份标识与密码器本地动态链接库中预先存储的唯一物理序列编码对应,所述地理位置信息由密码器本地北斗处理器通过预设定位天线获取得到,所述目标验证数据是由所述密码器根据当前系统时间和所述地理位置信息得到第一验证数据后,根据所述唯一物理序列编码对所述第一验证数据进行三重数据加密,得到第二验证数据,并对所述第二验证数据进行哈希加密运算,得到第三验证数据,根据预设字符数字转换规则对所述第三验证数据进行数字化转换得到的;

[0035] 数据验证模块,用于根据所述密码器的身份标识、所述地理位置信息以及服务器当前系统时间生成基准验证数据,并在所述基准验证数据与所述目标验证数据匹配时返回验证通过结果。

[0036] 第五方面,本申请提供一种基于定位信息的验证系统,包括:密码器和与所述密码器通信连接的验证服务器;

[0037] 所述密码器包括:中央处理器、北斗处理器以及时钟模块;

[0038] 所述北斗处理器用于通过预设定位天线获取的地理位置信息;

[0039] 所述时钟模块用于获取当前系统时间;

[0040] 所述中央处理器用于:

[0041] 根据所述当前系统时间和所述地理位置信息,得到第一验证数据;

[0042] 根据本地动态链接库中预先存储的唯一物理序列编码对所述第一验证数据进行三重数据加密,得到第二验证数据,并对所述第二验证数据进行哈希加密运算,得到第三验证数据;

[0043] 根据预设字符数字转换规则对所述第三验证数据进行数字化转换,得到目标验证数据;

[0044] 将所述目标验证数据、所述密码器的身份标识以及所述地理位置信息发送至对应验证服务器;

[0045] 所述验证服务器包括:

[0046] 数据接收模块,用于接收密码器发送的目标验证数据、密码器的身份标识以及地理位置信息;

[0047] 数据验证模块,用于根据所述密码器的身份标识、所述地理位置信息以及服务器当前系统时间生成基准验证数据,并在所述基准验证数据与所述目标验证数据匹配时返回验证通过结果。

[0048] 第六方面,本申请提供一种电子设备,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所述的基于定位信息的验证方法的步骤。

[0049] 第七方面,本申请提供一种计算机可读存储介质,其上存储有计算机程序,该计算机程序被处理器执行时实现所述的基于定位信息的验证方法的步骤。

[0050] 第八方面,本申请提供一种计算机程序产品,包括计算机程序/指令,该计算机程序/指令被处理器执行时实现所述的基于定位信息的验证方法的步骤。

[0051] 由上述技术方案可知,本申请提供一种基于定位信息的验证方法、装置、密码器及

系统,通过密码器基于当前系统时间、北斗处理器获取的地理位置信息以及其唯一物理序列编码进行加密处理,得到用于验证的目标验证数据并发送至验证服务器端进行交易验证,而无需采用现有技术中的特定验证U盾或限定有效时间的数字动态密码等不便捷的操作,由此能够准确、便捷得对交易进行验证。

附图说明

[0052] 为了更清楚地说明本申请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,下面描述中的附图是本申请的一些实施例,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。

[0053] 图1为本申请实施例中的基于定位信息的验证方法的流程示意图之一;

[0054] 图2为本申请实施例中的基于定位信息的验证方法的流程示意图之二;

[0055] 图3为本申请实施例中的基于定位信息的验证方法的流程示意图之三;

[0056] 图4为本申请实施例中的基于定位信息的验证方法的流程示意图之四;

[0057] 图5为本申请实施例中的基于定位信息的密码器的结构图;

[0058] 图6为本申请实施例中的基于定位信息的验证装置的结构图;

[0059] 图7为本申请实施例中的基于定位信息的验证系统的结构图;

[0060] 图8为本申请实施例中的电子设备的结构示意图。

具体实施方式

[0061] 为使本申请实施例的目的、技术方案和优点更加清楚,下面将结合本申请实施例中的附图,对本申请实施例中的技术方案进行清楚、完整的描述,显然,所描述的实施例是本申请一部分实施例,而不是全部的实施例。基于本申请中的实施例,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,都属于本申请保护的范围。

[0062] 考虑到现有技术中进行交易验证时操作不便捷的问题,本申请提供一种基于定位信息的验证方法、装置、密码器及系统,通过密码器基于当前系统时间、北斗处理器获取的地理位置信息以及其唯一物理序列编码进行加密处理,得到用于验证的目标验证数据并发送至验证服务器端进行交易验证,而无需采用现有技术中的特定验证U盾或限定有效时间的数字动态密码等不便捷的操作,由此能够准确、便捷得对交易进行验证。

[0063] 为了能够准确、便捷得对交易进行验证,本申请提供一种基于定位信息的验证方法的实施例,执行主体为一密码器,参见图1,所述基于定位信息的验证方法具体包含有如下内容:

[0064] 步骤S101:根据当前系统时间以及本地北斗处理器通过预设定位天线获取的地理位置信息,得到第一验证数据。

[0065] 可选的,本申请方法的执行主体为一密码器,其可以通过现有技术(例如现有时钟模块电路)获取当前系统时间。

[0066] 可选的,本申请的密码器可以内置本地北斗处理器和定位天线,该北斗处理器为现有技术,且其可以通过定位天线获取当前时区的北斗卫星广播信号,以此解析密码器当前的地理位置信息(例如经纬度信息)。

[0067] 可选的,当前系统时间和地理位置信息可以反映密码器在进行交易验证时的时效性,因此本申请将当前系统时间和地理位置信息进行结合,得到用于计算目标验证数据的第一验证数据。

[0068] 步骤S102:根据本地动态链接库中预先存储的唯一物理序列编码对所述第一验证数据进行三重数据加密,得到第二验证数据,并对所述第二验证数据进行哈希加密运算,得到第三验证数据。

[0069] 可选的,本申请密码器的本地存储器中可以以so文件(动态链接库)形式预先存储密码器的唯一物理序列编码,该唯一物理序列编码也存储于验证服务器中,可以通过密码器的身份标识查询得到。

[0070] 可以理解的是,以so文件(动态链接库)形式保存唯一物理序列编码能够保障该编码不会被反编译,有利于数据的安全。

[0071] 可选的,密码器的唯一物理序列编码可以反映目标验证数据的唯一性,因此本申请可以根据唯一物理序列编码对所述第一验证数据进行三重数据加密(3DES加密),得到第二验证数据。

[0072] 可选的,为了进一步混淆数据,增强数据安全性,本申请还可以对所述第二验证数据进行哈希加密运算,得到第三验证数据,即计算第二验证数据的摘要并将其作为第三验证数据。

[0073] 步骤S103:根据预设字符数字转换规则对所述第三验证数据进行数字化转换,得到目标验证数据。

[0074] 可选的,由于第三验证数据中存在字母,不利于后续计算,因此本申请可以根据预设字符数字转换规则将所述第三验证数据中的特定字符段转换为相应的数字段,例如A转化为1,B转化为2,C转化为3,D转化为4,E转化为5,F转化为6。

[0075] 同时,本申请可以仅截取第三验证数据中的特定字符段进行转换,例如前六位1fa73c,将其转换为161733,最终得出了6位动态数字(即最终的目标验证数据)为161733。

[0076] 步骤S104:将所述目标验证数据、所述密码器的身份标识以及所述地理位置信息发送至对应验证服务器,以使所述验证服务器根据所述密码器的身份标识、所述地理位置信息以及服务器当前系统时间生成基准验证数据,并在所述基准验证数据与所述目标验证数据匹配时返回验证通过结果。

[0077] 从上述描述可知,本申请实施例提供的基于定位信息的验证方法,能够通过密码器基于当前系统时间、北斗处理器获取的地理位置信息以及其唯一物理序列编码进行加密处理,得到用于验证的目标验证数据并发送至验证服务器端进行交易验证,而无需采用现有技术中的特定验证U盾或限定有效时间的数字动态密码等不便捷的操作,由此能够准确、便捷得对交易进行验证。

[0078] 为了能够保证目标验证数据的真实性,在本申请的基于定位信息的验证方法的一实施例中,上述步骤S101还可以具体包含如下内容:

[0079] 将当前系统时间和本地北斗处理器通过预设定位天线获取的地理位置信息转换为二进制编码,并拼接得到第一验证数据。

[0080] 可选的,针对当前系统时间,本申请可以年月日时分格式,将该格式的当前系统时间进行十进制到二进制的编码转换,例如从时钟模块电路获取当前系统时间:

202109291603,对其进行二进制编码(即BCD编码)后得到:323032313039323931363033。

[0081] 可选的,针对地理位置信息,例如经纬度:213.338784和33.13376,本申请可以先利用添加空格将其补足为10位(目的是让转化为BCD码后拼接起来为64位,方便3DES加密运算),而后对其进行二进制编码(即BCD编码)后得到:3231332E333338373834和33332E31333337362020。

[0082] 而后,将上述时间BCD编码和地理位置BCD编码进行拼接,得到第一验证数据,例如:

[0083] 323032313039323931363033323133 2E333338373834333332E31333337362020。

[0084] 可以理解的是,对当前系统时间和地理位置信息进行二进制编码是为了便于后续数据加密操作。

[0085] 为了能够保证目标验证数据的唯一性,在本申请的基于定位信息的验证方法的一实施例中,参见图2,上述步骤S102还可以具体包含如下内容:

[0086] 步骤S201:对本地动态链接库中预先存储的唯一物理序列编码进行混淆和对半交换处理,得到第一加密密钥。

[0087] 步骤S202:根据所述本地动态链接库中预先存储的第二加密密钥对所述第一加密密钥进行密文分组链接模式的三重数据加密,得到第三加密密钥。

[0088] 步骤S203:根据所述第三加密密钥对所述第一验证数据进行三重数据加密,得到第二验证数据。

[0089] 可选的,首先,获取本地动态链接库中预先存储的唯一物理序列编码(例如16位),该序列号有唯一性,如ABCDEF0000000001。然后,对序列号ABCDEF0000000001采用混淆处理,将其第1位与3位、2位与4位、5位与7位、6位与8位、9位与11位、10位与12位、13位与15位、14位与16位对换位置生成str1(CDAB00EF00000100),再然后进行对半交换处理,分别取str1的后8位为str2(00000100)和前8位为str3(CDAB00EF),由此str3+str2+str1拼接而成得出第一加密密钥key1(00000100CDAB00EFCDAB00EF00000100)。

[0090] 接着,根据所述本地动态链接库中预先存储的第二加密密钥(例如so内置32位密钥key2:ABCD1234567890EFABCD1234567890EF)对key1做3DES CBC模式加密得到第三加密密钥key3(065319DA9A450FD22C71DD5A452A8D0A)。

[0091] 最后,以第三加密密钥key3为密钥对第一验证数据做3DES CBC模式运算得出第二验证数据的密文:

[0092] 546C0CC84831A9FF2ACF5987BFF3A0BF95E29BF03EED98C40EA98735E6039846。

[0093] 在本申请的一可行实施例中,为了进一步混淆数据,增强数据安全性,本申请还可以对所述第二验证数据进行哈希加密运算,得到第三验证数据,即计算第二验证数据的摘要并将其作为第三验证数据。

[0094] 具体的,对第二验证数据做SHA256的hash运算得出第二验证数据的摘要,即第三验证数据:

[0095] 1fa73c1969ae0584297530e7ad6d8195d262a53af0eecd7623a5f23c7e90ad03。

[0096] 为了能够便于传输目标验证数据,在本申请的基于定位信息的验证方法的一实施例中,参见图3,上述步骤S103还可以具体包含如下内容:

[0097] 步骤S301:根据预设字符数字转换规则将所述第三验证数据中的特定字符段转换

为相应的数字段。

[0098] 步骤S302:根据所述数字段生成对应的目标验证二维码进行展示,以使验证服务器获取所述目标验证二维码中的目标验证数据。

[0099] 可选的,由于第三验证数据中存在字母,不利于后续计算,因此本申请可以根据预设字符数字转换规则将所述第三验证数据中的特定字符段转换为相应的数字段,例如A转化为1,B转化为2,C转化为3,D转化为4,E转化为5,F转化为6。

[0100] 同时,本申请可以仅截取第三验证数据中的特定字符段进行转换,例如前六位,由此,1fa73c转换为了161733,最终得出了6位动态数字(即最终的目标验证数据)为161733。

[0101] 可选的,本申请可以通过设置显示器将上述目标验证数据转换为二维码进行展示,以便于其他设备扫描该二维码并将其中包含的目标验证数据发送至验证服务器。

[0102] 为了能够准确、便捷得对交易进行验证,本申请提供一种基于定位信息的验证方法的实施例,执行主体为一验证服务器,参见图4,所述基于定位信息的验证方法具体包含有如下内容:

[0103] 步骤S401:接收密码器发送的目标验证数据、密码器的身份标识以及地理位置信息,其中,所述密码器的身份标识与密码器本地动态链接库中预先存储的唯一物理序列编码对应,所述地理位置信息由密码器本地北斗处理器通过预设定位天线获取得到,所述目标验证数据是由所述密码器根据当前系统时间和所述地理位置信息得到第一验证数据后,根据所述唯一物理序列编码对所述第一验证数据进行三重数据加密,得到第二验证数据,并对所述第二验证数据进行哈希加密运算,得到第三验证数据,根据预设字符数字转换规则对所述第三验证数据进行数字化转换得到的。

[0104] 步骤S402:根据所述密码器的身份标识、所述地理位置信息以及服务器当前系统时间生成基准验证数据,并在所述基准验证数据与所述目标验证数据匹配时返回验证通过结果。

[0105] 从上述描述可知,本申请实施例提供的基于定位信息的验证方法,能够通过密码器基于当前系统时间、北斗处理器获取的地理位置信息以及其唯一物理序列编码进行加密处理,得到用于验证的目标验证数据并发送至验证服务器端进行交易验证,而无需采用现有技术中的特定验证U盾或限定有效时间的数字动态密码等不便捷的操作,由此能够准确、便捷得对交易进行验证。

[0106] 为了能够灵活基于地理位置信息进行验证,在本申请的基于定位信息的验证方法的一实施例中,还可以具体包含如下内容:

[0107] 若所述地理位置信息中的经纬度坐标超出与所述密码器的身份标识对应的电子围栏,则向所述密码器返回一交易报错信号。

[0108] 可选的,本申请的验证服务器可以针对每一密码器设置相应的电子围栏,根据密码器发送来的身份标识确定其电子围栏,并判断其发送来的地理位置是否超出该电子围栏,若超出,则返回一交易报错信号并拒绝执行交易。

[0109] 为了能够准确、便捷得对交易进行验证,本申请提供一种用于实现所述基于定位信息的验证方法的全部或部分内容的密码器的实施例,参见图5,所述基于定位信息的密码器10具体包含有如下内容:

[0110] 中央处理器12、北斗处理器11以及时钟模块13。

[0111] 所述北斗处理器11用于通过预设定位天线获取的地理位置信息。

[0112] 所述时钟模块13用于获取当前系统时间。

[0113] 所述中央处理器12用于：

[0114] 根据所述当前系统时间和所述地理位置信息，得到第一验证数据。

[0115] 根据本地动态链接库中预先存储的唯一物理序列编码对所述第一验证数据进行三重数据加密，得到第二验证数据，并对所述第二验证数据进行哈希加密运算，得到第三验证数据。

[0116] 根据预设字符数字转换规则对所述第三验证数据进行数字化转换，得到目标验证数据。

[0117] 将所述目标验证数据、所述密码器的身份标识以及所述地理位置信息发送至对应验证服务器，以使所述验证服务器根据所述密码器的身份标识、所述地理位置信息以及服务器当前系统时间生成基准验证数据，并在所述基准验证数据与所述目标验证数据匹配时返回验证通过结果。

[0118] 从上述描述可知，本申请实施例提供的基于定位信息的密码器，能够通过密码器基于当前系统时间、北斗处理器获取的地理位置信息以及其唯一物理序列编码进行加密处理，得到用于验证的目标验证数据并发送至验证服务器端进行交易验证，而无需采用现有技术中的特定验证U盾或限定有效时间的数字动态密码等不便捷的操作，由此能够准确、便捷得对交易进行验证。

[0119] 为了能够准确、便捷得对交易进行验证，本申请提供一种用于实现所述基于定位信息的验证方法的全部或部分内容的装置的实施例，例如一验证服务器，参见图6，所述基于定位信息的验证服务器20具体包含有如下内容：

[0120] 数据接收模块21，用于接收密码器发送的目标验证数据、密码器的身份标识以及地理位置信息，其中，所述密码器的身份标识与密码器本地动态链接库中预先存储的唯一物理序列编码对应，所述地理位置信息由密码器本地北斗处理器通过预设定位天线获取得到，所述目标验证数据是由所述密码器根据当前系统时间和所述地理位置信息得到第一验证数据后，根据所述唯一物理序列编码对所述第一验证数据进行三重数据加密，得到第二验证数据，并对所述第二验证数据进行哈希加密运算，得到第三验证数据，根据预设字符数字转换规则对所述第三验证数据进行数字化转换得到的。

[0121] 数据验证模块22，用于根据所述密码器的身份标识、所述地理位置信息以及服务器当前系统时间生成基准验证数据，并在所述基准验证数据与所述目标验证数据匹配时返回验证通过结果。

[0122] 从上述描述可知，本申请实施例提供的基于定位信息的验证装置，能够通过密码器基于当前系统时间、北斗处理器获取的地理位置信息以及其唯一物理序列编码进行加密处理，得到用于验证的目标验证数据并发送至验证服务器端进行交易验证，而无需采用现有技术中的特定验证U盾或限定有效时间的数字动态密码等不便捷的操作，由此能够准确、便捷得对交易进行验证。

[0123] 为了能够准确、便捷得对交易进行验证，本申请提供一种用于实现所述基于定位信息的验证方法的全部或部分内容的验证系统的实施例，参见图7，所述基于定位信息的验证系统具体包含有如下内容：密码器10和与所述密码器10通信连接的验证服务器20。

[0124] 所述密码器10包括:中央处理器12、北斗处理器11以及时钟模块13。

[0125] 所述北斗处理器11用于通过预设定位天线获取的地理位置信息。

[0126] 所述时钟模块13用于获取当前系统时间。

[0127] 所述中央处理器12用于:

[0128] 根据所述当前系统时间和所述地理位置信息,得到第一验证数据。

[0129] 根据本地动态链接库中预先存储的唯一物理序列编码对所述第一验证数据进行三重数据加密,得到第二验证数据,并对所述第二验证数据进行哈希加密运算,得到第三验证数据。

[0130] 根据预设字符数字转换规则对所述第三验证数据进行数字化转换,得到目标验证数据。

[0131] 将所述目标验证数据、所述密码器的身份标识以及所述地理位置信息发送至对应验证服务器。

[0132] 所述验证服务器20包括:

[0133] 数据接收模块21,用于接收密码器发送的目标验证数据、密码器的身份标识以及地理位置信息。

[0134] 数据验证模块22,用于根据所述密码器的身份标识、所述地理位置信息以及服务器当前系统时间生成基准验证数据,并在所述基准验证数据与所述目标验证数据匹配时返回验证通过结果。

[0135] 从上述描述可知,本申请实施例提供的基于定位信息的验证系统,能够通过密码器基于当前系统时间、北斗处理器获取的地理位置信息以及其唯一物理序列编码进行加密处理,得到用于验证的目标验证数据并发送至验证服务器端进行交易验证,而无需采用现有技术中的特定验证U盾或限定有效时间的数字动态密码等不便捷的操作,由此能够准确、便捷得对交易进行验证。

[0136] 从硬件层面来说,为了能够准确、便捷得对交易进行验证,本申请提供一种用于实现所述基于定位信息的验证方法中的全部或部分内容的电子设备的实施例,所述电子设备具体包含有如下内容:

[0137] 处理器(processor)、存储器(memory)、通信接口(Communications Interface)和总线;其中,所述处理器、存储器、通信接口通过所述总线完成相互间的通信;所述通信接口用于实现基于定位信息的密码器与核心业务系统、用户终端以及相关数据库等相关设备之间的信息传输;该逻辑控制器可以是台式计算机、平板电脑及移动终端等,本实施例不限于此。在本实施例中,该逻辑控制器可以参照实施例中的基于定位信息的验证方法的实施例,以及基于定位信息的密码器的实施例进行实施,其内容被合并于此,重复之处不再赘述。

[0138] 可以理解的是,所述用户终端可以包括智能手机、平板电子设备、网络机顶盒、便携式计算机、台式电脑、个人数字助理(PDA)、车载设备、智能穿戴设备等。其中,所述智能穿戴设备可以包括智能眼镜、智能手表、智能手环等。

[0139] 在实际应用中,基于定位信息的验证方法的部分可以在如上述内容所述的电子设备侧执行,也可以所有的操作都在所述客户端设备中完成。具体可以根据所述客户端设备的处理能力,以及用户使用场景的限制等进行选择。本申请对此不作限定。若所有的操作都在所述客户端设备中完成,所述客户端设备还可以包括处理器。

[0140] 上述的客户端设备可以具有通信模块(即通信单元),可以与远程的服务器进行通信连接,实现与所述服务器的数据传输。所述服务器可以包括任务调度中心一侧的服务器,其他的实施场景中也可以包括中间平台的服务器,例如与任务调度中心服务器有通信链接的第三方服务器平台的服务器。所述的服务器可以包括单台计算机设备,也可以包括多个服务器组成的服务器集群,或者分布式装置的服务器结构。

[0141] 图8为本申请实施例的电子设备9600的系统构成的示意框图。如图8所示,该电子设备9600可以包括中央处理器9100和存储器9140;存储器9140耦合到中央处理器9100。值得注意的是,该图8是示例性的;还可以使用其他类型的结构,来补充或代替该结构,以实现电信功能或其他功能。

[0142] 一实施例中,基于定位信息的验证方法功能可以被集成到中央处理器9100中。其中,中央处理器9100可以被配置为进行如下控制:

[0143] 步骤S101:根据当前系统时间以及本地北斗处理器通过预设定位天线获取的地理位置信息,得到第一验证数据。

[0144] 步骤S102:根据本地动态链接库中预先存储的唯一物理序列编码对所述第一验证数据进行三重数据加密,得到第二验证数据,并对所述第二验证数据进行哈希加密运算,得到第三验证数据。

[0145] 步骤S103:根据预设字符数字转换规则对所述第三验证数据进行数字化转换,得到目标验证数据。

[0146] 步骤S104:将所述目标验证数据、所述密码器的身份标识以及所述地理位置信息发送至对应验证服务器,以使所述验证服务器根据所述密码器的身份标识、所述地理位置信息以及服务器当前系统时间生成基准验证数据,并在所述基准验证数据与所述目标验证数据匹配时返回验证通过结果。

[0147] 从上述描述可知,本申请实施例提供的电子设备,通过密码器基于当前系统时间、北斗处理器获取的地理位置信息以及其唯一物理序列编码进行加密处理,得到用于验证的目标验证数据并发送至验证服务器端进行交易验证,而无需采用现有技术中的特定验证U盾或限定有效时间的数字动态密码等不便捷的操作,由此能够准确、便捷得对交易进行验证。

[0148] 在另一个实施方式中,基于定位信息的密码器可以与中央处理器9100分开配置,例如可以将基于定位信息的密码器配置为与中央处理器9100连接的芯片,通过中央处理器的控制来实现基于定位信息的验证方法功能。

[0149] 如图8所示,该电子设备9600还可以包括:通信模块9110、输入单元9120、音频处理器9130、显示器9160、电源9170。值得注意的是,电子设备9600也并不是必须要包括图8中所示的所有部件;此外,电子设备9600还可以包括图8中没有示出的部件,可以参考现有技术。

[0150] 如图8所示,中央处理器9100有时也称为控制器或操作控件,可以包括微处理器或其他处理器装置和/或逻辑装置,该中央处理器9100接收输入并控制电子设备9600的各个部件的操作。

[0151] 其中,存储器9140,例如可以是缓存器、闪存、硬驱、可移动介质、易失性存储器、非易失性存储器或其它合适装置中的一种或更多种。可储存上述与失败有关的信息,此外还可存储执行有关信息的程序。并且中央处理器9100可执行该存储器9140存储的该程序,以

实现信息存储或处理等。

[0152] 输入单元9120向中央处理器9100提供输入。该输入单元9120例如为按键或触摸输入装置。电源9170用于向电子设备9600提供电力。显示器9160用于进行图像和文字等显示对象的显示。该显示器例如可为LCD显示器,但并不限于此。

[0153] 该存储器9140可以是固态存储器,例如,只读存储器(ROM)、随机存取存储器(RAM)、SIM卡等。还可以是这样的存储器,其即使在断电时也保存信息,可被选择性地擦除且设有更多数据,该存储器的示例有时被称为EPROM等。存储器9140还可以是某种其它类型的装置。存储器9140包括缓冲存储器9141(有时被称为缓冲器)。存储器9140可以包括应用/功能存储部9142,该应用/功能存储部9142用于存储应用程序和功能程序或用于通过中央处理器9100执行电子设备9600的操作的流程。

[0154] 存储器9140还可以包括数据存储部9143,该数据存储部9143用于存储数据,例如联系人、数字数据、图片、声音和/或任何其他由电子设备使用的数据。存储器9140的驱动程序存储部9144可以包括电子设备的用于通信功能和/或用于执行电子设备的其他功能(如消息传送应用、通讯录应用等)的各种驱动程序。

[0155] 通信模块9110即为经由天线9111发送和接收信号的发送机/接收机9110。通信模块(发送机/接收机)9110耦合到中央处理器9100,以提供输入信号和接收输出信号,这可以和常规移动通信终端的情况相同。

[0156] 基于不同的通信技术,在同一电子设备中,可以设置有多个通信模块9110,如蜂窝网络模块、蓝牙模块和/或无线局域网模块等。通信模块(发送机/接收机)9110还经由音频处理器9130耦合到扬声器9131和麦克风9132,以经由扬声器9131提供音频输出,并接收来自麦克风9132的音频输入,从而实现通常的电信功能。音频处理器9130可以包括任何合适的缓冲器、解码器、放大器等。另外,音频处理器9130还耦合到中央处理器9100,从而使得可以通过麦克风9132能够在本机上录音,且使得可以通过扬声器9131来播放本机上存储的声音。

[0157] 本申请的实施例还提供能够实现上述实施例中的执行主体为服务器或客户端的基于定位信息的验证方法中全部步骤的一种计算机可读存储介质,所述计算机可读存储介质上存储有计算机程序,该计算机程序被处理器执行时实现上述实施例中的执行主体为服务器或客户端的基于定位信息的验证方法的全部步骤,例如,所述处理器执行所述计算机程序时实现下述步骤:

[0158] 步骤S101:根据当前系统时间以及本地北斗处理器通过预设定位天线获取的地理位置信息,得到第一验证数据。

[0159] 步骤S102:根据本地动态链接库中预先存储的唯一物理序列编码对所述第一验证数据进行三重数据加密,得到第二验证数据,并对所述第二验证数据进行哈希加密运算,得到第三验证数据。

[0160] 步骤S103:根据预设字符数字转换规则对所述第三验证数据进行数字化转换,得到目标验证数据。

[0161] 步骤S104:将所述目标验证数据、所述密码器的身份标识以及所述地理位置信息发送至对应验证服务器,以使所述验证服务器根据所述密码器的身份标识、所述地理位置信息以及服务器当前系统时间生成基准验证数据,并在所述基准验证数据与所述目标验证

数据匹配时返回验证通过结果。

[0162] 从上述描述可知,本申请实施例提供的计算机可读存储介质,通过密码器基于当前系统时间、北斗处理器获取的地理位置信息以及其唯一物理序列编码进行加密处理,得到用于验证的目标验证数据并发送至验证服务器端进行交易验证,而无需采用现有技术中的特定验证U盾或限定有效时间的数字动态密码等不便捷的操作,由此能够准确、便捷得对交易进行验证。

[0163] 本申请的实施例还提供能够实现上述实施例中的执行主体为服务器或客户端的基于定位信息的验证方法中全部步骤的一种计算机程序产品,该计算机程序/指令被处理器执行时实现所述的基于定位信息的验证方法的步骤,例如,所述计算机程序/指令实现下述步骤:

[0164] 步骤S101:根据当前系统时间以及本地北斗处理器通过预设定位天线获取的地理位置信息,得到第一验证数据。

[0165] 步骤S102:根据本地动态链接库中预先存储的唯一物理序列编码对所述第一验证数据进行三重数据加密,得到第二验证数据,并对所述第二验证数据进行哈希加密运算,得到第三验证数据。

[0166] 步骤S103:根据预设字符数字转换规则对所述第三验证数据进行数字化转换,得到目标验证数据。

[0167] 步骤S104:将所述目标验证数据、所述密码器的身份标识以及所述地理位置信息发送至对应验证服务器,以使所述验证服务器根据所述密码器的身份标识、所述地理位置信息以及服务器当前系统时间生成基准验证数据,并在所述基准验证数据与所述目标验证数据匹配时返回验证通过结果。

[0168] 从上述描述可知,本申请实施例提供的计算机程序产品,通过密码器基于当前系统时间、北斗处理器获取的地理位置信息以及其唯一物理序列编码进行加密处理,得到用于验证的目标验证数据并发送至验证服务器端进行交易验证,而无需采用现有技术中的特定验证U盾或限定有效时间的数字动态密码等不便捷的操作,由此能够准确、便捷得对交易进行验证。

[0169] 本领域内的技术人员应明白,本发明的实施例可提供为方法、装置、或计算机程序产品。因此,本发明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,本发明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。

[0170] 本发明是参照根据本发明实施例的方法、设备(装置)、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装置。

[0171] 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。

[0172] 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。

[0173] 本发明中应用了具体实施例对本发明的原理及实施方式进行了阐述,以上实施例的说明只是用于帮助理解本发明的方法及其核心思想;同时,对于本领域的一般技术人员,依据本发明的思想,在具体实施方式及应用范围上均会有改变之处,综上所述,本说明书内容不应理解为对本发明的限制。

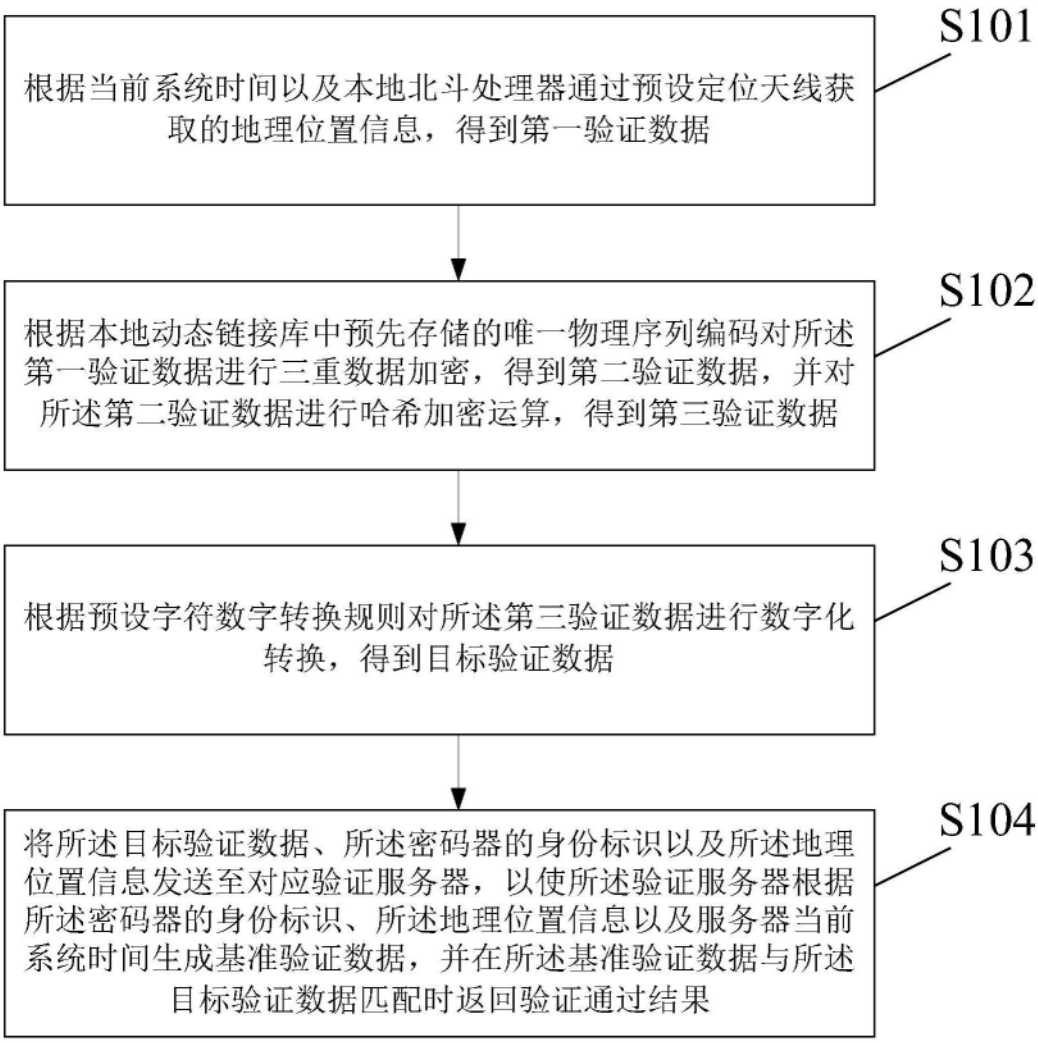

S101
根据当前系统时间以及本地北斗处理器通过预设定位天线获取的地理位置信息，得到第一验证数据
S102
根据本地动态链接库中预先存储的唯一物理序列编码对所述第一验证数据进行三重数据加密，得到第二验证数据，并对所述第二验证数据进行哈希加密运算，得到第三验证数据
S103
根据预设字符数字转换规则对所述第三验证数据进行数字化转换，得到目标验证数据
S104
将所述目标验证数据、所述密码器的身份标识以及所述地理位置信息发送至对应验证服务器，以使所述验证服务器根据所述密码器的身份标识、所述地理位置信息以及服务器当前系统时间生成基准验证数据，并在所述基准验证数据与所述目标验证数据匹配时返回验证通过结果

图1

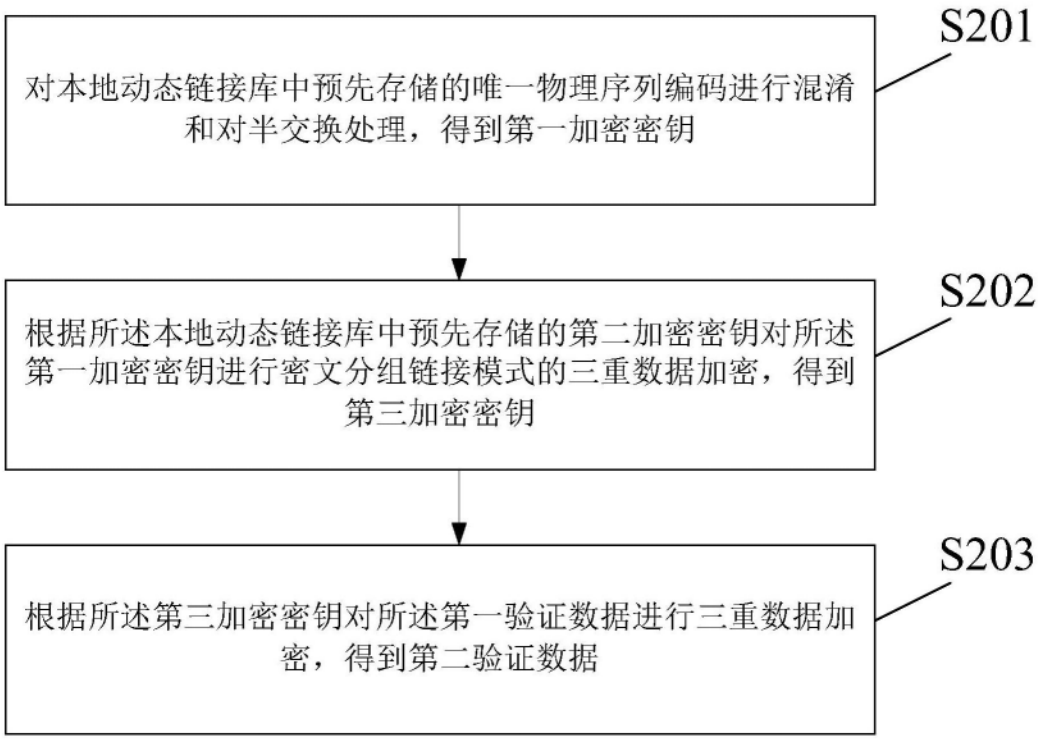

S201
对本地动态链接库中预先存储的唯一物理序列编码进行混淆和对半交换处理，得到第一加密密钥
S202
根据所述本地动态链接库中预先存储的第二加密密钥对所述第一加密密钥进行密文分组链接模式的三重数据加密，得到第三加密密钥
S203
根据所述第三加密密钥对所述第一验证数据进行三重数据加密，得到第二验证数据

图2

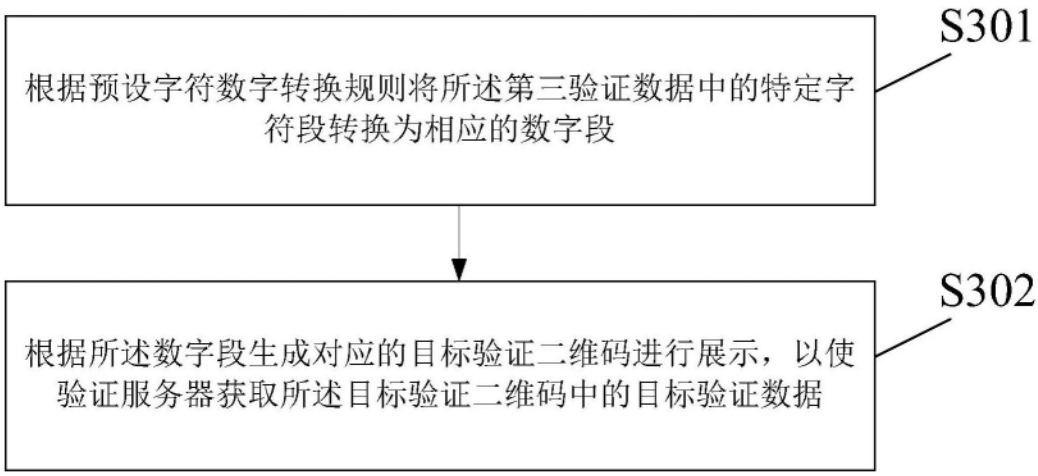

S301
根据预设字符数字转换规则将所述第三验证数据中的特定字符段转换为相应的数字段
S302
根据所述数字段生成对应的目标验证二维码进行展示，以使验证服务器获取所述目标验证二维码中的目标验证数据

图3

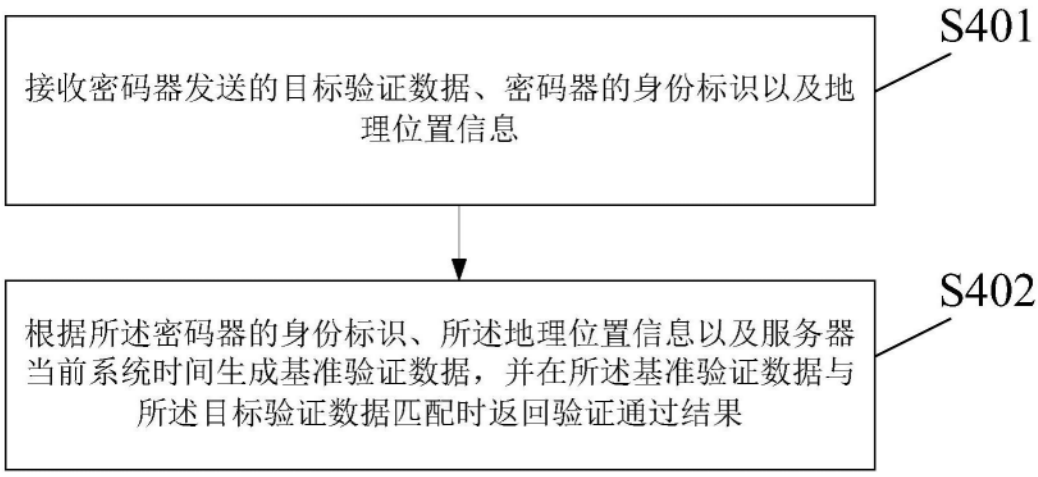

S401
接收密码器发送的目标验证数据、密码器的身份标识以及地理位置信息
S402
根据所述密码器的身份标识、所述地理位置信息以及服务器当前系统时间生成基准验证数据，并在所述基准验证数据与所述目标验证数据匹配时返回验证通过结果

图4

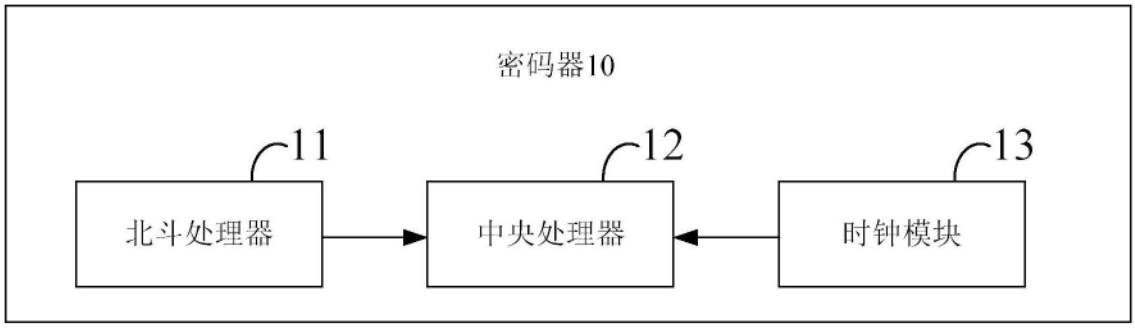

密码器10
11
12
13
北斗处理器
中央处理器
时钟模块

图5

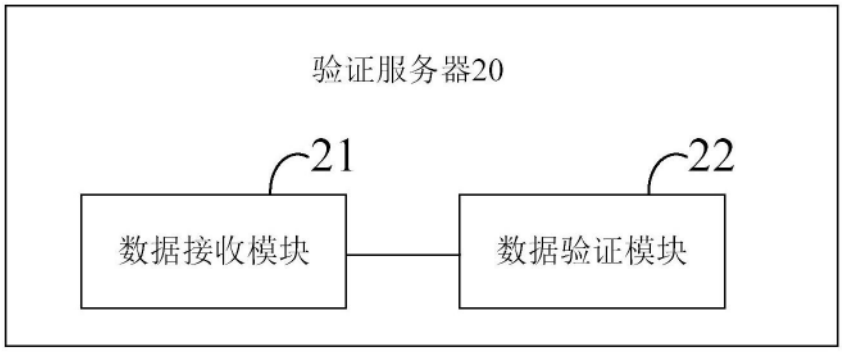

验证服务器20
21
22
数据接收模块
数据验证模块

图6

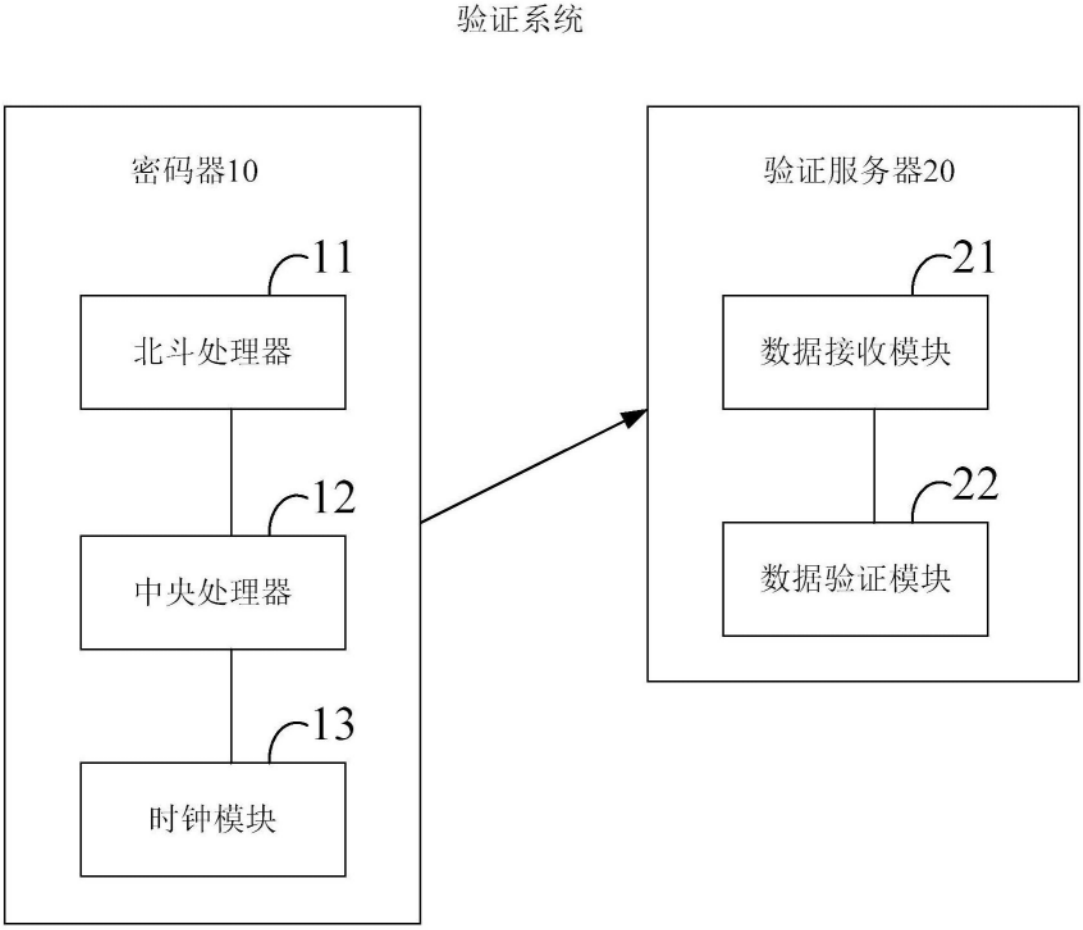

验证系统
密码器10
11
北斗处理器
12
中央处理器
13
时钟模块
验证服务器20
21
数据接收模块
22
数据验证模块

图7

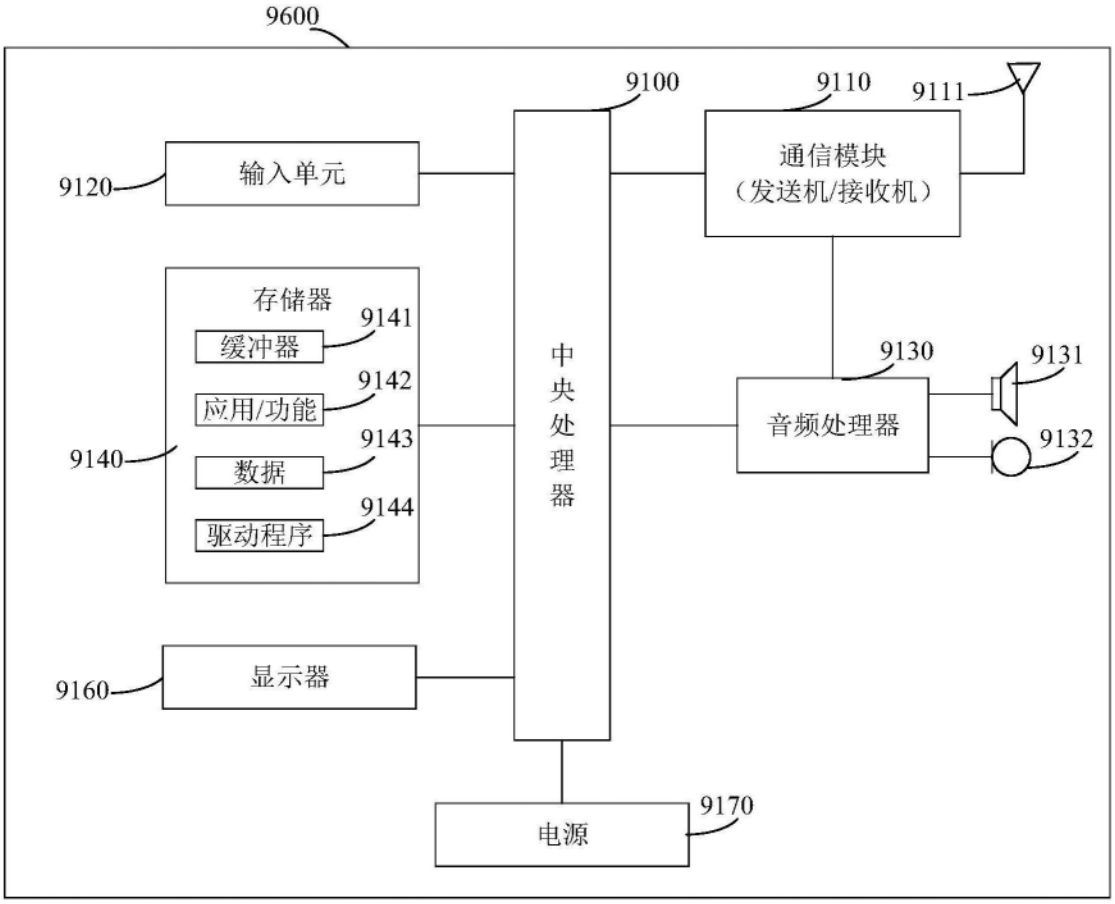

9600
9100
9110
9111
输入单元
9120
通信模块
（发送机/接收机）
存储器
9141
缓冲器
9142
应用/功能
9143
数据
9144
驱动程序
9140
中央处理器
9130
9131
音频处理器
9132
显示器
9160
电源
9170

图8