(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2017 年 2 月 2 日 (02.02.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/016272 A1

(51) 国际专利分类号:
H04L 9/00 (2006.01) *G06Q 30/00* (2012.01)

(21) 国际申请号: PCT/CN2016/081565

(22) 国际申请日: 2016 年 5 月 10 日 (10.05.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201510455785.6 2015 年 7 月 29 日 (29.07.2015) CN

(71) 申请人: **腾讯科技（深圳）有限公司 (TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED)** [CN/CN]; 中国广东省深圳市福田区振兴路赛格科技园 2 栋东 403 室李满芳, Guangdong 518000 (CN)。

(72) 发明人: **李建立 (LI, Jianli)**; 中国广东省深圳市福田区振兴路赛格科技园 2 栋东 403 室李满芳, Guangdong 518000 (CN)。

(74) 代理人: **深圳翼盛智成知识产权事务所(普通合伙)等(ESSEN PATENT&TRADEMARK AGENCY et al.)** 等; 中国广东省深圳市福田区深南大道 6021 号喜年中心 A 座 1709-1711, Guangdong 518000 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:
— 包括国际检索报告(条约第 21 条(3))。

(54) **Title**: METHOD, APPARATUS AND SYSTEM FOR PROCESSING VIRTUAL RESOURCE DATA

(54) **发明名称** : 一种虚拟资源数据的处理方法、装置及系统

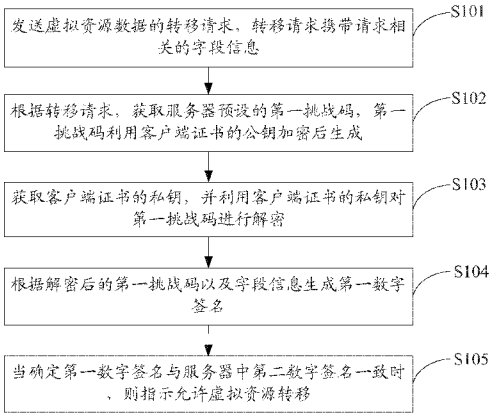

图 1

S101 Sending a virtual resource data transfer request, wherein the transfer request carries field information related to the request
S102 Acquiring, according to the transfer request, a first challenge code pre-set by a server, wherein the first challenge code is generated by means of encryption using a public key of a client certificate
S103 Acquiring a private key of the client certificate, and using the private key of the client certificate to decrypt the first challenge code
S104 Generating a first digital signature according to the decrypted first challenge code and the field information
S105 When it is determined that the first digital signature is consistent with a second digital signature in the server, instructing permission for virtual resource transfer

(57) **Abstract**: Provided is a method for processing virtual resource data. The method comprises: sending a virtual resource transfer request; acquiring a first challenge code, which is generated by means of encryption using a public key of a client certificate, and a private key of the client certificate, and using the private key to decrypt the first challenge code; generating a first digital signature according to the decrypted first challenge code; and when the first digital signature is consistent with a second digital signature in a server, allowing virtual resource transfer. Further provided are an apparatus and system for processing virtual resource data.

(57) **摘要**: 一种虚拟资源数据的处理方法，包括: 发送虚拟资源转移请求；获取利用客户端证书的公钥加密生成的第一挑战码及客户端证书的私钥，利用该私钥对第一挑战码进行解密；根据解密后第一挑战码生成第一数字签名；当第一数字签名与服务器中第二数字签名一致时，则允许虚拟资源转移。本发明还提供一种虚拟资源数据的处理装置及系统。

WO 2017/016272 A1

说明书

发明名称：一种虚拟资源数据的处理方法、装置及系统

[1] 本申请要求于2015年07月29日提交中国专利局、申请号为201510455785.6、发明名称为“一种虚拟资源数据的处理方法、装置及系统”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

[2] 本发明属于通信技术领域，尤其涉及一种虚拟资源数据的处理方法、装置及系统。

背景技术

[3] 随着互联网络技术的不断进步，人们对互联网络安全的要求也越来越高。

[4] 以基于客户端数字证书的快捷支付为例，目前通常在发起支付请求时，首先使用客户端数字证书中的私钥对支付请求中的部分字段对进行数字签名，然后将签名后的数据作为一个新的字段和支付请求中的其他信息一起提交到支付后台服务器，后台服务器收到请求后，使用证书的公钥对签名进行解密，如果解密成功且解密后的数据正确，则认为是用户的正确支付请求。由于客户端证书的私钥只有用户的终端设备上才可以获得，其他人很难仿冒用户的签名。

对发明的公开

技术问题

[5] 后台处理用户的支付请求时，需要实时的对用户的使用非对称加密算法加密的签名进行解密，而非对称加密算法加解密的效率是相当低的。以公钥加密算法（RSA，RSA algorithm）为例，其加解密速度相当于同等加密强度的对称加密算法的1/1000左右。在这种设计下，证书用户对后台服务器造成的压力必然显著大于非证书用户，运行效率相对较低。

问题的解决方案

技术解决方案

[6] 本发明的目的在于提供一种虚拟资源数据的处理方法及装置，旨在减轻服务器的负载压力，提高服务器的运行速率。

[7] 为解决上述技术问题，本发明实施例第一方面提供：

[8] 一种虚拟资源数据的处理方法，其中包括：

[9] 发送虚拟资源数据的转移请求，所述转移请求携带请求相关的字段信息；

[10] 根据所述转移请求，获取服务器预设的第一挑战码，所述第一挑战码利用客户端证书的公钥加密后生成；

[11] 获取客户端证书的私钥，并利用所述客户端证书的私钥对所述第一挑战码进行解密；

[12] 根据解密后的第一挑战码以及所述字段信息生成第一数字签名；

[13] 当确定所述第一数字签名与所述服务器中第二数字签名一致时，则指示允许所述虚拟资源转移。

[14] 本发明实施例第二方面提供：

[15] 一种虚拟资源数据的处理方法，其中包括：

[16] 接收虚拟资源数据的转移请求，所述转移请求携带请求相关的字段信息；

[17] 根据所述转移请求，向客户端发送预设的第一挑战码，所述第一挑战码利用客户端证书的公钥加密后生成；

[18] 接收客户端发送的第一数字签名，所述第一数字签名由所述客户端利用客户端证书的私钥对所述第一挑战码进行解密，并根据解密后的第一挑战码以及所述字段信息所生成；

[19] 当确定所述第一数字签名与所述服务器中第二数字签名一致时，则指示允许所述虚拟资源转移。

[20] 本发明实施例第三方面提供：

[21] 一种虚拟资源数据的处理装置，其中包括处理器，所述处理器用于：

[22] 发送虚拟资源数据的转移请求，所述转移请求携带请求相关的字段信息；

[23] 根据所述转移请求，获取服务器预设的第一挑战码，所述第一挑战码利用客户端证书的公钥加密后生成；

[24] 获取客户端证书的私钥，并利用所述客户端证书的私钥对所述第一挑战码进行解密；

[25] 根据解密后的第一挑战码以及所述字段信息生成第一数字签名；

[26] 当确定所述第一数字签名与所述服务器中第二数字签名一致时，则指示允许所述虚拟资源转移。

[27] 本发明实施例第四方面提供：

[28] 一种虚拟资源数据的处理装置，其中包括处理器，所述处理器用于：

[29] 接收虚拟资源数据的转移请求，所述转移请求携带请求相关的字段信息；

[30] 根据所述转移请求，向客户端发送预设的第一挑战码，所述第一挑战码利用客户端证书的公钥加密后生成；

[31] 接收客户端发送的第一数字签名，所述第一数字签名由所述客户端利用客户端证书的私钥对所述第一挑战码进行解密，并根据解密后的第一挑战码以及所述字段信息所生成；

[32] 当确定所述第一数字签名与所述服务器中第二数字签名一致时，则指示允许所述虚拟资源转移。

[33] 本发明实施例第五方面提供：

[34] 一种虚拟资源数据的处理系统，包括客户端和服务器，其中，所述客户端为第三方面提供的虚拟资源数据的处理装置，所述服务器为第四方面提供的虚拟资源数据的处理装置。

[35] 另外，一种存储介质，其内存储有处理器可执行指令，其中该处理器可执行指令用于让处理器完成以下操作：

[36] 发送虚拟资源数据的转移请求，所述转移请求携带请求相关的字段信息；

[37] 根据所述转移请求，获取服务器预设的第一挑战码，所述第一挑战码利用客户端证书的公钥加密后生成；

[38] 获取客户端证书的私钥，并利用所述客户端证书的私钥对所述第一挑战码进行解密；

[39] 根据解密后的第一挑战码以及所述字段信息生成第一数字签名；

[40] 当确定所述第一数字签名与所述服务器中第二数字签名一致时，则指示允许所述虚拟资源转移。

发明的有益效果

有益效果

[41] 相对于现有技术，本实施例，服务器提前使用客户端证书中的公钥为用户生成挑战码；用户请求虚拟资源转移时使用客户端证书的私钥解密挑战码；然后根据将解密后的挑战码和请求相关的字段信息生成数字签名；服务器通过验证客户端生成的数字签名的正确性来确认该虚拟资源转移请求是否合法；由于攻击者没有用户的客户端证书，无法对公钥加密的挑战码进行解密，因此无法模仿用户的签名。生成的数字签名包含与对应支付请求的相关信息，且该签名只能用于本次交易，更能保证交易的安全性；并且，由于挑战码提前设置，大大降低了支付高峰时给服务器带来的负载压力，提高服务器的运行速率。

对附图的简要说明

附图说明

[42] 下面结合附图，通过对本发明的具体实施方式详细描述，将使本发明的技术方案及其它有益效果显而易见。

[43] 图1是本发明第一实施例提供的虚拟资源数据的处理方法的流程示意图；

[44] 图2为本发明第二实施例提供的虚拟资源数据的处理方法的流程示意图；

[45] 图3为本发明第三实施例提供的虚拟资源数据的处理方法的流程示意图；

[46] 图4为本发明第四实施例提供的虚拟资源数据的处理装置的结构示意图；

[47] 图5为本发明第五实施例提供的虚拟资源数据的处理装置的结构示意图；

[48] 图6为本发明第六实施例提供的虚拟资源数据的处理系统的结构示意图。

实施该发明的最佳实施例

本发明的最佳实施方式

[49] 请参照图式，其中相同的组件符号代表相同的组件，本发明的原理是以实施在一适当的运算环境中来举例说明。以下的说明是基于所例示的本发明具体实施例，其不应被视为限制本发明未在此详述的其它具体实施例。

[50] 在以下的说明中，本发明的具体实施例将参考由一部或多部计算机所执行的步骤及符号来说明，除非另有述明。因此，这些步骤及操作将有数次提到由计算机执行，本文所指的计算机执行包括了由代表了以一结构化型式中的数据的电子信号的计算机处理单元的操作。此操作转换该数据或将其维持在该计算机的内存系统中的位置处，其可重新配置或另外以本领域测试人员所熟知的方式来

改变该计算机的运作。该数据所维持的数据结构为该内存的实体位置，其具有由该数据格式所定义的特定特性。但是，本发明原理以上述文字来说明，其并不代表为一种限制，本领域测试人员将可了解到以下所述的多种步骤及操作亦可实施在硬件当中。

[51] 本发明的原理使用许多其它泛用性或特定目的运算、通信环境或组态来进行操作。所熟知的适合用于本发明的运算系统、环境与组态的范例可包括(但不限于)手持电话、个人计算机、服务器、多处理器系统、微电脑为主的系统、主架构型计算机、及分布式运算环境，其中包括了任何的上述系统或装置。

[52] 本文所使用的术语「模块」可看做为在该运算系统上执行的软件对象。本文所述的不同组件、模块、引擎及服务可看做为在该运算系统上的实施对象。而本文所述的装置及方法优选的以软件的方式进行实施，当然也可在硬件上进行实施，均在本发明保护范围之内。

[53] 应当理解是，以下实施例的顺序不受实施例序号限制，即第一实施例非最佳实施例，可以根据实际需求设定，比如，可以将第一实施例作为第二优选实施例实施，第三实施例作为第一优选实施例实施等等，第一、第二之类的描述仅为便于表述使用。

[54] 第一实施例

[55] 请参阅图1，图1是本发明第一实施例提供的虚拟资源数据的处理方法的流程示意图。所述方法包括：

[56] 在步骤S101中，发送虚拟资源数据的转移请求，所述转移请求携带请求相关的字段信息。

[57] 可以理解的是，所述虚拟资源数据的处理方法可基于一客户端上运行，所述客户端可以为笔记型计算机、平板PC（Personal Computer）、手机等具备储存单元并安装有微处理器而具有运算能力的终端机构成，本发明对此不作具体限定。

[58] 本发明实施例中所述虚拟资源数据的转移请求可以包括移动支付处理、扣款处理，转账处理等，此处不作具体限定。

[59] 在步骤S102中，根据所述转移请求，获取服务器预设的第一挑战码，所述第一挑战码利用客户端证书的公钥加密后生成。

[60] 在步骤S103中，获取客户端证书的私钥，并利用所述客户端证书的私钥对所述第一挑战码进行解密。

[61] 在步骤S104中，根据解密后的第一挑战码以及所述字段信息生成第一数字签名。

[62] 其中，所述步骤S102至步骤S104可具体为：

[63] 可以理解的是，挑战码（challenge）也称作挑战口令，是指遵循握手验证协议生成的一组加密口令，用于在传输过程中保证用户的真实密码不被泄露。本发明实施例中所述第一挑战码是指服务器利用客户端证书的公钥加密后生成的挑战码；容易想到的是，本实施例中“第一”、“第二”仅为便于区别说明，并不构成限定。

[64] 客户端获取服务器所述第一挑战码后，利用客户端证书的私钥对所述第一挑战码进行解密，然后根据解密后的第一挑战码以及请求相关的字段信息生成第一数字签名，由于攻击者没有用户的客户端证书，无法对公钥加密的第一挑战码进行解密，因此无法模仿用户的数字签名，提高交易安全性。

[65] 在步骤S105中，当确定所述第一数字签名与所述服务器中第二数字签名一致时，则指示允许所述虚拟资源转移。

[66] 服务器获取所述客户端生成的第一数字签名，将所述第一数字签名与其生成的第二数字签名进行比较，若确定出第一数字签名与第二数字签名一致时，则接受所述客户端发送的虚拟资源转移请求，所述客户端向用户指示允许所述虚拟资源转移。

[67] 由上述可知，本实施例提供的虚拟资源数据的处理方法，服务器提前使用客户端证书中的公钥为用户生成挑战码；用户请求虚拟资源转移时使用客户端证书的私钥解密挑战码；然后根据将解密后的挑战码和请求相关的字段信息生成数字签名；服务器通过验证客户端生成的数字签名的正确性来确认该虚拟资源转移请求是否合法；由于攻击者没有用户的客户端证书，无法对公钥加密的挑战码进行解密，因此无法模仿用户的签名。生成的数字签名包含与对应支付请求的相关信息，且该签名只能用于本次交易，更能保证交易的安全性；并且，由于挑战码提前设置，大大降低了支付高峰时给服务器带来的负载压力，提高服

务器的运行速率。

[68] 第二实施例

[69] 请参阅图2，图2为本发明第二实施例提供的虚拟资源数据的处理方法的流程示意图。

[70] 其中，本实施例提供与第一实施例相对应的虚拟资源数据的处理方法；该方法基于一服务器上运行，所述服务器接收客户端发送的虚拟资源的转移请求，并对所述虚拟资源的转移请求进行处理；其中，所述客户端可以为笔记型计算机、平板PC、手机等具备储存单元并安装有微处理器而具有运算能力的终端机构成；本发明实施例中所述虚拟资源数据的转移请求可以包括移动支付处理、扣款处理，转账处理等，此处不作具体限定。

[71] 所述方法包括：

[72] 在步骤S201中，接收虚拟资源数据的转移请求，所述转移请求携带请求相关的字段信息。

[73] 在步骤S202中，根据所述转移请求，向客户端发送预设的第一挑战码，所述第一挑战码利用客户端证书的公钥加密后生成。

[74] 在步骤S203中，接收客户端发送的第一数字签名，所述第一数字签名由所述客户端利用客户端证书的私钥对所述第一挑战码进行解密，并根据解密后的第一挑战码以及所述字段信息所生成。

[75] 其中，所述步骤S201与步骤S203可具体为：

[76] 可以理解的是，挑战码也称作挑战口令，是指遵循握手验证协议生成的一组加密口令，用于在传输过程中保证用户的真实密码不被泄露。本发明实施例中所述第一挑战码是指服务器利用客户端证书的公钥加密后生成的挑战码。

[77] 客户端获取服务器所述第一挑战码后，利用客户端证书的私钥对所述第一挑战码进行解密，然后根据解密后的第一挑战码以及请求相关的字段信息生成第一数字签名，并发送至所述服务器；由于攻击者没有用户的客户端证书，无法对公钥加密的第一挑战码进行解密，因此无法模仿用户的数字签名，提高交易安全性。

[78] 在步骤S204中，当确定所述第一数字签名与所述服务器中第二数字签名一致时

，则指示允许所述虚拟资源转移。

[79] 服务器获取所述客户端生成的第一数字签名，将所述第一数字签名与其生成的第二数字签名进行比较，若确定出第一数字签名与第二数字签名一致时，则接受所述客户端发送的虚拟资源转移请求，所述客户端向用户指示允许所述虚拟资源转移。

[80] 由上述可知，本实施例提供的虚拟资源数据的处理方法，服务器提前使用客户端证书中的公钥为用户生成挑战码；用户请求虚拟资源转移时使用客户端证书的私钥解密挑战码；然后根据将解密后的挑战码和请求相关的字段信息生成数字签名；服务器通过验证客户端生成的数字签名的正确性来确认该虚拟资源转移请求是否合法；由于攻击者没有用户的客户端证书，无法对公钥加密的挑战码进行解密，因此无法模仿用户的签名。生成的数字签名包含与对应支付请求的相关信息，且该签名只能用于本次交易，更能保证交易的安全性；并且，由于挑战码提前设置，大大降低了支付高峰时给服务器带来的负载压力，提高服务器的运行速率。

[81] 第三实施例

[82] 请参阅图3，图3为本发明第三实施例提供的虚拟资源数据的处理方法的流程示意图。所述方法包括：

[83] 在步骤S301中、服务器接收用户信息；

[84] 在步骤S302中、服务器根据所述用户信息，生成相对应的第二挑战码，所述第二挑战码携带对应的挑战码明文和挑战码密文；

[85] 在步骤S303中、服务器获取所述用户信息指示的用户客户端证书的公钥；

[86] 在步骤S304中、服务器利用所述客户端证书的公钥对所述挑战码进行加密，生成第一挑战码，并存储所述挑战码明文和挑战码密文。

[87] 其中，所述步骤S301至步骤S304可具体为：服务器中预设的第一挑战码可以在虚拟资源转移之前进行设置，所述第一挑战码是服务器利用客户端证书的公钥加密后生成。

[88] 可以理解的是，针对于客户端，在发送虚拟资源的转移请求之前，发送用户信息，以使所述服务器根据所述用户信息进行处理以生成第一挑战码，所述处理

包括：所述服务器根据所述用户信息相对应的第二挑战码，获取所述用户信息指示的客户端证书的公钥，所述服务器利用所述客户端证书的公钥对所述第二挑战码进行加密，生成第一挑战码。

[89] 在步骤S305中，客户端发送虚拟资源数据的转移请求，所述转移请求携带请求相关的字段信息；

[90] 其中，本发明实施例中所述虚拟资源数据的转移请求可以包括移动支付处理、扣款处理，转账处理等，此处不作具体限定。

[91] 在步骤S306中，服务器根据所述转移请求，向客户端发送预设的第一挑战码；

[92] 在步骤S307中，客户端获取客户端证书的私钥，并利用所述客户端证书的私钥对所述第一挑战码进行解密；

[93] 在步骤S308中，客户端根据解密后的第一挑战码以及所述字段信息生成第一数字签名；

[94] 其中，所述步骤S306至步骤S308可具体为：

[95] 优选的，所述客户端根据解密后的第一挑战码以及所述字段信息中的订单号字段，使用单向散列算法生成第一数字签名。

[96] 客户端获取服务器所述第一挑战码后，利用客户端证书的私钥对所述第一挑战码进行解密，然后根据解密后的第一挑战码以及请求相关的字段信息生成第一数字签名，并将所述第一数字签名以及所述字段信息发送至服务器；由于攻击者没有用户的客户端证书，无法对公钥加密的第一挑战码进行解密，因此无法模仿用户的数字签名，提高交易安全性。

[97] 在步骤S309中，服务器获取所述第一数字签名，并将所述第一数字签名与所述服务器中第二数字签名进行比较；

[98] 可以理解的是，服务器获取到第一数字签名以及所述字段信息之后，可根据所述挑战码明文和所述字段信息，利用同样的算法，如上述单向散列算法生成第二数字签名；服务器获取客户端生成的第一数字签名，将第一数字签名与第二数字签名进行比较，得到比较结果，并将比较结果发送至客户端。

[99] 针对于客户端，客户端接收所述服务器发送的比较结果，所述比较结果由服务器根据所述挑战码明文和所述字段信息生成第二数字签名，并将所述第一数字

签名与所述第二数字签名进行比较而得到。

[100] 在步骤S310中，当确定所述第一数字签名与所述服务器中第二数字签名一致时，则指示允许所述虚拟资源转移。

[101] 针对于客户端，当客户端根据所述比较结果确定所述第一数字签名与所述第二数字签名一致时，则指示允许所述虚拟资源转移。

[102] 为方便理解本发明技术方案，基于上述实施例，下面以一具体应用场景对所述虚拟资源数据的处理方法进行分析说明：

[103] 该场景中，虚拟资源转移具体指客户端与服务器之间的支付处理，其中，该服务器可具体为支付后台服务器，该客户端可具体为手机；

[104] 其步骤包括：

[105] 步骤S1、客户端向支付后台服务器发送一个支付请求；

[106] 即用户使用客户端下单后点击支付，以触发向服务器发起支付请求。

[107] 步骤S2、支付后台服务器接收该支付请求，返回一个使用客户端证书的公钥加密的第一挑战码；

[108] 支付后台服务器检测该订单的合法性，返回所述第一挑战码，以及该订单的详情、支持的支付方式等信息。

[109] 步骤S3、客户端收到第一挑战码后，弹出支付确认界面，以供用户确认支付方式及订单信息的正确性。

[110] 用户点击确定后进入步骤S4。

[111] 步骤S4、客户端使用客户端证书中的私钥对所述第一挑战码进行解密，然后将解密后的第一挑战码，同订单号、用户选择的支付方式等字段使用MD5算法生成签名字段Signstr（即第一数字签名）；然后将SignStr和订单号、支付方式及其他支付相关信息一起发送到支付后台服务器。

[112] 步骤S5、支付后台服务器使用挑战码明文和订单号等信息采用客户端同样的算法生成签名字段（即第二数字签名），并同客户端传来的签名字段进行比较验证，若签名验证通过，则根据可以直接向客户端返回支付成功，或者要求用户加验支付密码、短信验证码后再完成支付。

[113] 由上述可知，本实施例提供的虚拟资源数据的处理方法，服务器提前使用客户

端证书中的公钥为用户生成挑战码；用户请求虚拟资源转移时使用客户端证书的私钥解密挑战码；然后根据将解密后的挑战码和请求相关的字段信息生成数字签名；服务器通过验证客户端生成的数字签名的正确性来确认该虚拟资源转移请求是否合法；由于攻击者没有用户的客户端证书，无法对公钥加密的挑战码进行解密，因此无法模仿用户的签名。生成的数字签名包含与对应支付请求的相关信息，且该签名只能用于本次交易，更能保证交易的安全性；并且，由于挑战码提前设置，大大降低了支付高峰时给服务器带来的负载压力，提高服务器的运行速率。进一步的，减低基于客户端数字证书的快捷支付的业务运营成本。

[114] 第四实施例

[115] 为便于更好的实施本发明实施例提供的虚拟资源数据的处理方法，本发明实施例还提供一种基于上述虚拟资源数据的处理方法的装置。其中名词的含义与上述第一实施例中的虚拟资源的处理的方法中相同，具体实现细节可以参考方法实施例中的说明。

[116] 请参阅图4，图4为本发明实施例提供的虚拟资源数据的处理装置的结构示意图，其中所述虚拟资源数据的处理装置可基于一客户端上运行，所述客户端可以为笔记型计算机、平板PC、手机等具备储存单元并安装有微处理器而具有运算能力的终端机构成，本发明对此不作具体限定。

[117] 如图4所示，本发明所述虚拟资源数据的处理装置可以包括第一发送模块401、第一获取模块402、解密模块403、第一生成模块404以及第一指示模块405。

[118] 其中，所述第一发送模块401，用于发送虚拟资源数据的转移请求，所述转移请求携带请求相关的字段信息；所述第一获取模块402，用于根据所述转移请求，获取服务器预设的第一挑战码，所述第一挑战码利用客户端证书的公钥加密后生成；

[119] 所述解密模块403，用于获取客户端证书的私钥，并利用所述客户端证书的私钥对所述第一挑战码进行解密；所述第一生成模块404，用于根据解密后的第一挑战码以及所述字段信息生成第一数字签名；所述第一指示模块405，用于当确定所述第一数字签名与所述服务器中第二数字签名一致时，则指示允许所述虚

拟资源转移。

[120] 基于图4提供的虚拟资源数据的处理装置，还可以作出以下优选设置：

[121] 所述第一生成模块404具体用于：根据解密后的第一挑战码以及所述字段信息中的订单号字段，使用单向散列算法生成第一数字签名。

[122] 进一步优选的，所述装置还可以包括：第二发送模块，用于将所述第一数字签名以及所述字段信息发送至服务器；第一接收模块，用于接收所述服务器发送的比较结果，所述比较结果由服务器根据所述挑战码明文和所述字段信息生成第二数字签名，并将所述第一数字签名与所述第二数字签名进行比较而得到；基于此，所述第一指示模块405具体用于：当根据所述比较结果确定所述第一数字签名与所述第二数字签名一致时，则指示允许所述虚拟资源转移。

[123] 可以理解的是，在该实施例中没有详述的部分，可以参见上文第一和第三实施例中针对虚拟资源数据的处理方法的详细描述，此处不再赘述。

[124] 由上述可知，本实施例提供的虚拟资源数据的处理装置，服务器提前使用客户端证书中的公钥为用户生成挑战码；用户请求虚拟资源转移时使用客户端证书的私钥解密挑战码；然后根据将解密后的挑战码和请求相关的字段信息生成数字签名；服务器通过验证客户端生成的数字签名的正确性来确认该虚拟资源转移请求是否合法；由于攻击者没有用户的客户端证书，无法对公钥加密的挑战码进行解密，因此无法模仿用户的签名。生成的数字签名包含与对应支付请求的相关信息，且该签名只能用于本次交易，更能保证交易的安全性；并且，由于挑战码提前设置，大大降低了支付高峰时给服务器带来的负载压力，提高服务器的运行速率。

[125] 第五实施例

[126] 请参阅图5，图5为本发明实施例提供的虚拟资源数据的处理装置的结构示意图，其中名词的含义与上述第二实施例中的虚拟资源的处理的方法中相同，具体实现细节可以参考方法实施例中的说明。

[127] 优选的，所述虚拟资源数据的处理装置包括第二接收模块501、第三发送模块502、第三接收模块503以及第二指示模块504；

[128] 其中，所述第二接收模块501，用于接收虚拟资源数据的转移请求，所述转移

请求携带请求相关的字段信息；所述第三发送模块502，用于根据所述转移请求，向客户端发送预设的第一挑战码，所述第一挑战码利用客户端证书的公钥加密后生成；

[129] 所述第三接收模块503，用于接收客户端发送的第一数字签名，所述第一数字签名由所述客户端利用客户端证书的私钥对所述第一挑战码进行解密，并根据解密后的第一挑战码以及所述字段信息所生成；所述第二指示模块504，用于当确定所述第一数字签名与所述服务器中第二数字签名一致时，则指示允许所述虚拟资源转移。

[130] 进一步的，基于图5提供的虚拟资源数据的处理装置，还可以作出以下优选设置：

[131] 优选的，所述装置还可以包括：第四接收模块，用于接收用户信息；第二生成模块，用于根据所述用户信息，生成相对应的第二挑战码，所述第二挑战码携带对应的挑战码明文和挑战码密文；第二获取模块，用于获取所述用户信息指示的用户客户端证书的公钥；加密存储模块，用于利用所述客户端证书的公钥对所述挑战码进行加密，生成第一挑战码，并存储所述挑战码明文和挑战码密文。

[132] 进一步优选的，所述装置还可以包括：第五接收模块，用于接收所述客户端发送的所述第一数字签名以及所述字段信息；第三生成模块，用于使用所述挑战码明文和所述字段信息生成第二数字签名；比较模块，用于将所述第一数字签名与所述第二数字签名进行比较，得到比较结果；第四发送模块，用于将所述比较结果发送给客户端。

[133] 可以理解的是，在该实施例中没有详述的部分，可以参见上文第二和第三实施例中针对虚拟资源数据的处理方法的详细描述，此处不再赘述。

[134] 由上述可知，本实施例提供的虚拟资源数据的处理装置，服务器提前使用客户端证书中的公钥为用户生成挑战码；用户请求虚拟资源转移时使用客户端证书的私钥解密挑战码；然后根据将解密后的挑战码和请求相关的字段信息生成数字签名；服务器通过验证客户端生成的数字签名的正确性来确认该虚拟资源转移请求是否合法；由于攻击者没有用户的客户端证书，无法对公钥加密的挑战

码进行解密，因此无法模仿用户的签名。生成的数字签名包含与对应支付请求的相关信息，且该签名只能用于本次交易，更能保证交易的安全性；并且，由于挑战码提前设置，大大降低了支付高峰时给服务器带来的负载压力，提高服务器的运行速率。

[135] 第六实施例

[136] 请参阅图6，图6为本发明实施例提供的虚拟资源的处理系统的结构示意图，所述虚拟资源的处理系统包括：服务器601以及客户端602，其中，所述客户端602可具体为第四实施例所述的虚拟资源数据的处理装置，所述服务器601为第五实施例所述的虚拟资源数据的处理装置。

[137] 其中，所述客户端602用于发送虚拟资源数据的转移请求，所述转移请求携带请求相关的字段信息；根据所述转移请求，获取服务器预设的第一挑战码，所述第一挑战码利用客户端证书的公钥加密后生成；获取客户端证书的私钥，并利用所述客户端证书的私钥对所述第一挑战码进行解密；根据解密后的第一挑战码以及所述字段信息生成第一数字签名；当确定所述第一数字签名与所述服务器中第二数字签名一致时，则指示允许所述虚拟资源转移。

[138] 所述服务器601用于接收虚拟资源数据的转移请求，所述转移请求携带请求相关的字段信息；根据所述转移请求，向客户端发送预设的第一挑战码，所述第一挑战码利用客户端证书的公钥加密后生成；接收客户端发送的第一数字签名，所述第一数字签名由所述客户端利用客户端证书的私钥对所述第一挑战码进行解密，并根据解密后的第一挑战码以及所述字段信息所生成；当确定所述第一数字签名与所述服务器中第二数字签名一致时，则指示允许所述虚拟资源转移。

[139] 在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述的部分，可以参见上文针对虚拟资源数据的处理方法的详细描述，此处不再赘述。

[140] 本发明实施例提供的所述虚拟资源数据的处理装置，譬如为计算机、平板电脑、具有触摸功能的手机等等，所述虚拟资源数据的处理装置与上文实施例中的虚拟资源数据的处理方法属于同一构思，在所述虚拟资源数据的处理装置上可

以运行所述虚拟资源数据的处理方法实施例中提供的任一方法，其具体实现过程详见所述虚拟资源数据的处理方法实施例，此处不再赘述。

[141] 需要说明的是，对本发明所述虚拟资源数据的处理方法而言，本领域普通测试人员可以理解实现本发明实施例所述虚拟资源数据的处理方法的全部或部分流程，是可以通过计算机程序来控制相关的硬件来完成，所述计算机程序可存储于一计算机可读取存储介质中，如存储在终端的存储器中，并被该终端内的至少一个处理器执行，在执行过程中可包括如所述虚拟资源数据的处理方法的实施例的流程。其中，所述的存储介质可为磁碟、光盘、只读存储器（ROM，Read Only Memory）、随机存取记忆体（RAM，Random Access Memory）等。

[142] 对本发明实施例的所述虚拟资源数据的处理装置而言，其各功能模块可以集成在一个处理芯片中，也可以是各个模块单独物理存在，也可以两个或两个以上模块集成在一个模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。所述集成的模块如果以软件功能模块的形式实现并作为独立的产品销售或使用时，也可以存储在一个计算机可读取存储介质中，所述存储介质譬如为只读存储器，磁盘或光盘等。

[143] 以上对本发明实施例所提供的一种虚拟资源数据的处理方法及装置进行了详细介绍，本文中应用了具体个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。

权利要求书

[权利要求 1] 一种虚拟资源数据的处理方法，其特征在于，包括：

发送虚拟资源数据的转移请求，所述转移请求携带请求相关的字段信息；

根据所述转移请求，获取服务器预设的第一挑战码，所述第一挑战码利用客户端证书的公钥加密后生成；

获取客户端证书的私钥，并利用所述客户端证书的私钥对所述第一挑战码进行解密；

根据解密后的第一挑战码以及所述字段信息生成第一数字签名；

当确定所述第一数字签名与所述服务器中第二数字签名一致时，则指示允许所述虚拟资源转移。

[权利要求 2] 根据权利要求1所述的虚拟资源数据的处理方法，其特征在于，所述发送虚拟资源的转移请求之前，还包括：

发送用户信息，以使所述服务器根据所述用户信息进行处理以生成第一挑战码，所述处理包括：所述服务器根据所述用户信息相对应的第二挑战码，获取所述用户信息指示的客户端证书的公钥，所述服务器利用所述客户端证书的公钥对所述第二挑战码进行加密，生成第一挑战码。

[权利要求 3] 根据权利要求2所述的虚拟资源数据的处理方法，其特征在于，所述根据解密后的第一挑战码以及所述字段信息生成第一数字签名之后，还包括：

将所述第一数字签名以及所述字段信息发送至服务器；

接收所述服务器发送的比较结果，所述比较结果由服务器根据所述挑战码明文和所述字段信息生成第二数字签名，并将所述第一数字签名与所述第二数字签名进行比较而得到；

所述当确定所述第一数字签名与所述服务器中第二数字签名一致时，则指示允许所述虚拟资源转移，包括：当根据所述比较结果确定所述第一数字签名与所述第二数字签名一致时，则指示允许

所述虚拟资源转移。

[权利要求 4] 根据权利要求1所述的虚拟资源数据的处理方法，其特征在于，所述根据解密后的第一挑战码以及所述字段信息生成第一数字签名，包括：

根据解密后的第一挑战码以及所述字段信息中的订单号字段，使用单向散列算法生成第一数字签名。

[权利要求 5] 一种虚拟资源数据的处理方法，其特征在于，包括：

接收虚拟资源数据的转移请求，所述转移请求携带请求相关的字段信息；

根据所述转移请求，向客户端发送预设的第一挑战码，所述第一挑战码利用客户端证书的公钥加密后生成；

接收客户端发送的第一数字签名，所述第一数字签名由所述客户端利用客户端证书的私钥对所述第一挑战码进行解密，并根据解密后的第一挑战码以及所述字段信息所生成；

当确定所述第一数字签名与所述服务器中第二数字签名一致时，则指示允许所述虚拟资源转移。

[权利要求 6] 根据权利要求5所述的虚拟资源数据的处理方法，其特征在于，所述接收虚拟资源的转移请求之前，还包括：

接收用户信息；

根据所述用户信息，生成相对应的第二挑战码，所述第二挑战码携带对应的挑战码明文和挑战码密文；

获取所述用户信息指示的用户客户端证书的公钥；

利用所述客户端证书的公钥对所述挑战码进行加密，生成第一挑战码，并存储所述挑战码明文和挑战码密文。

[权利要求 7] 根据权利要求6所述的虚拟资源数据的处理方法，其特征在于，所述当确定所述第一数字签名与所述服务器中第二数字签名一致时，则指示允许所述虚拟资源转移之前，还包括：

接收所述客户端发送的所述第一数字签名以及所述字段信息；

使用所述挑战码明文和所述字段信息生成第二数字签名，并将所述第一数字签名与所述第二数字签名进行比较，得到比较结果；

将所述比较结果发送给客户端。

[权利要求 8] 一种虚拟资源数据的处理装置，其特征在于，包括处理器，所述处理器用于：

发送虚拟资源数据的转移请求，所述转移请求携带请求相关的字段信息；

根据所述转移请求，获取服务器预设的第一挑战码，所述第一挑战码利用客户端证书的公钥加密后生成；

获取客户端证书的私钥，并利用所述客户端证书的私钥对所述第一挑战码进行解密；

根据解密后的第一挑战码以及所述字段信息生成第一数字签名；

当确定所述第一数字签名与所述服务器中第二数字签名一致时，则指示允许所述虚拟资源转移。

[权利要求 9] 根据权利要求8所述的虚拟资源数据的处理装置，其特征在于，所述处理器用于：

将所述第一数字签名以及所述字段信息发送至服务器；

接收所述服务器发送的比较结果，所述比较结果由服务器根据所述挑战码明文和所述字段信息生成第二数字签名，并将所述第一数字签名与所述第二数字签名进行比较而得到；

当根据所述比较结果确定所述第一数字签名与所述第二数字签名一致时，则指示允许所述虚拟资源转移。

[权利要求 10] 根据权利要求8所述的虚拟资源数据的处理装置，其特征在于，所述处理器用于：根据解密后的第一挑战码以及所述字段信息中的订单号字段，使用单向散列算法生成第一数字签名。

[权利要求 11] 一种虚拟资源数据的处理装置，其特征在于，包括处理器，所述处理器用于：

接收虚拟资源数据的转移请求，所述转移请求携带请求相关的字

段信息；

根据所述转移请求，向客户端发送预设的第一挑战码，所述第一挑战码利用客户端证书的公钥加密后生成；

接收客户端发送的第一数字签名，所述第一数字签名由所述客户端利用客户端证书的私钥对所述第一挑战码进行解密，并根据解密后的第一挑战码以及所述字段信息所生成；

当确定所述第一数字签名与所述服务器中第二数字签名一致时，则指示允许所述虚拟资源转移。

[权利要求 12] 根据权利要求11所述的虚拟资源数据的处理装置，其特征在于，所述处理器用于：

接收用户信息；

根据所述用户信息，生成相对应的第二挑战码，所述第二挑战码携带对应的挑战码明文和挑战码密文；

获取所述用户信息指示的用户客户端证书的公钥；

利用所述客户端证书的公钥对所述挑战码进行加密，生成第一挑战码，并存储所述挑战码明文和挑战码密文。

[权利要求 13] 根据权利要求12所述的虚拟资源数据的处理装置，其特征在于，所述处理器用于：

接收所述客户端发送的所述第一数字签名以及所述字段信息；

使用所述挑战码明文和所述字段信息生成第二数字签名；

将所述第一数字签名与所述第二数字签名进行比较，得到比较结果；

将所述比较结果发送给客户端。

[权利要求 14] 一种存储介质，其内存储有处理器可执行指令，其中该处理器可执行指令用于让处理器完成以下操作：

发送虚拟资源数据的转移请求，所述转移请求携带请求相关的字段信息；

根据所述转移请求，获取服务器预设的第一挑战码，所述第一挑

战码利用客户端证书的公钥加密后生成；

获取客户端证书的私钥，并利用所述客户端证书的私钥对所述第一挑战码进行解密；

根据解密后的第一挑战码以及所述字段信息生成第一数字签名；

当确定所述第一数字签名与所述服务器中第二数字签名一致时，则指示允许所述虚拟资源转移。

[权利要求 15] 根据权利要求14所述的存储介质，其特征在于，所述处理器可执行指令用于让处理器完成以下操作：

发送用户信息，以使所述服务器根据所述用户信息进行处理以生成第一挑战码，所述处理包括：所述服务器根据所述用户信息相对应的第二挑战码，获取所述用户信息指示的客户端证书的公钥，所述服务器利用所述客户端证书的公钥对所述第二挑战码进行加密，生成第一挑战码。

[权利要求 16] 根据权利要求15所述的存储介质，其特征在于，所述处理器可执行指令用于让处理器完成以下操作：

将所述第一数字签名以及所述字段信息发送至服务器；

接收所述服务器发送的比较结果，所述比较结果由服务器根据所述挑战码明文和所述字段信息生成第二数字签名，并将所述第一数字签名与所述第二数字签名进行比较而得到；

所述当确定所述第一数字签名与所述服务器中第二数字签名一致时，则指示允许所述虚拟资源转移，包括：当根据所述比较结果确定所述第一数字签名与所述第二数字签名一致时，则指示允许所述虚拟资源转移。

[权利要求 17] 根据权利要求14所述的存储介质，其特征在于，所述处理器可执行指令用于让处理器完成以下操作：

根据解密后的第一挑战码以及所述字段信息中的订单号字段，使用单向散列算法生成第一数字签名。

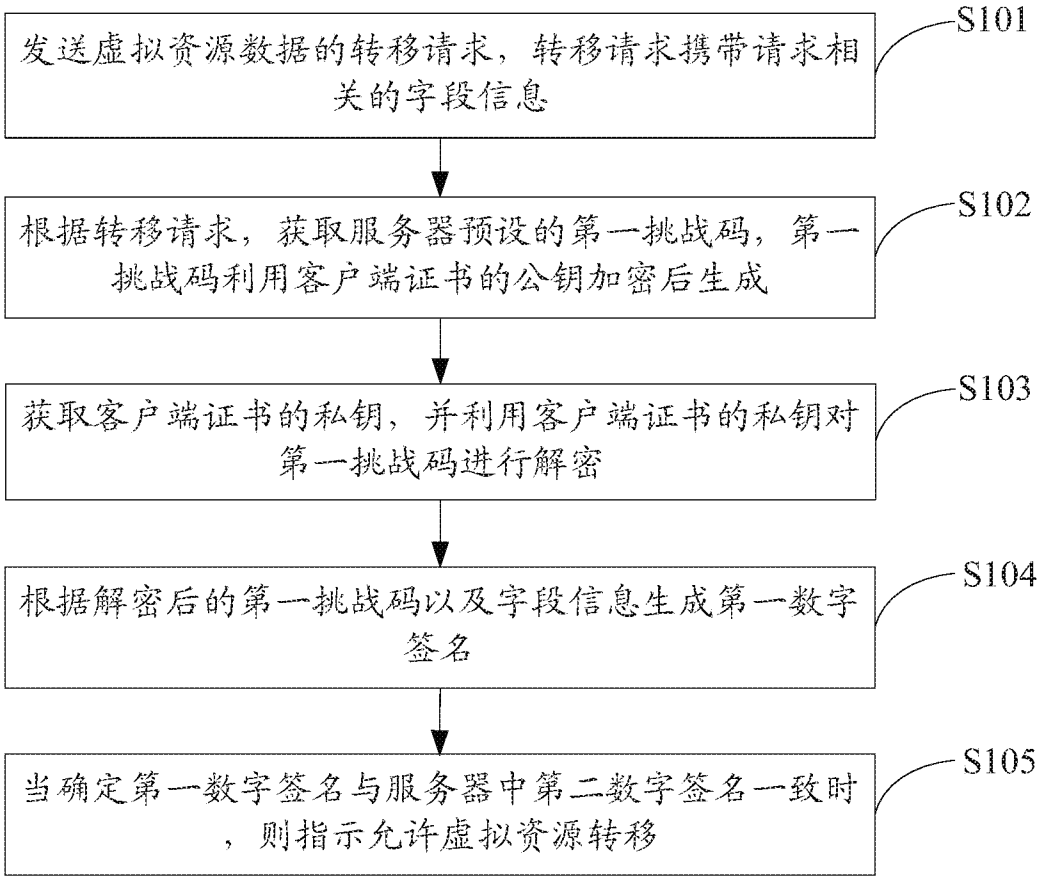
发送虚拟资源数据的转移请求，转移请求携带请求相关的字段信息
S101
根据转移请求，获取服务器预设的第一挑战码，第一挑战码利用客户端证书的公钥加密后生成
S102
获取客户端证书的私钥，并利用客户端证书的私钥对第一挑战码进行解密
S103
根据解密后的第一挑战码以及字段信息生成第一数字签名
S104
当确定第一数字签名与服务器中第二数字签名一致时，则指示允许虚拟资源转移
S105

图 1

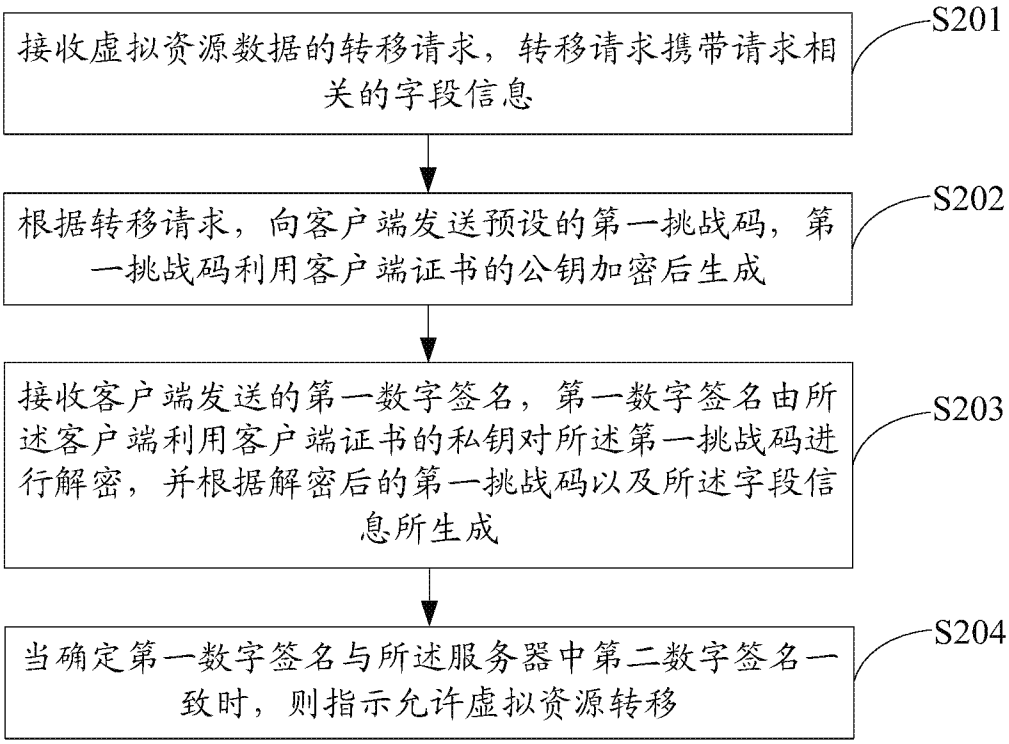
接收虚拟资源数据的转移请求，转移请求携带请求相关的字段信息
S201
根据转移请求，向客户端发送预设的第一挑战码，第一挑战码利用客户端证书的公钥加密后生成
S202
接收客户端发送的第一数字签名，第一数字签名由所述客户端利用客户端证书的私钥对所述第一挑战码进行解密，并根据解密后的第一挑战码以及所述字段信息所生成
S203
当确定第一数字签名与所述服务器中第二数字签名一致时，则指示允许虚拟资源转移
S204

图 2

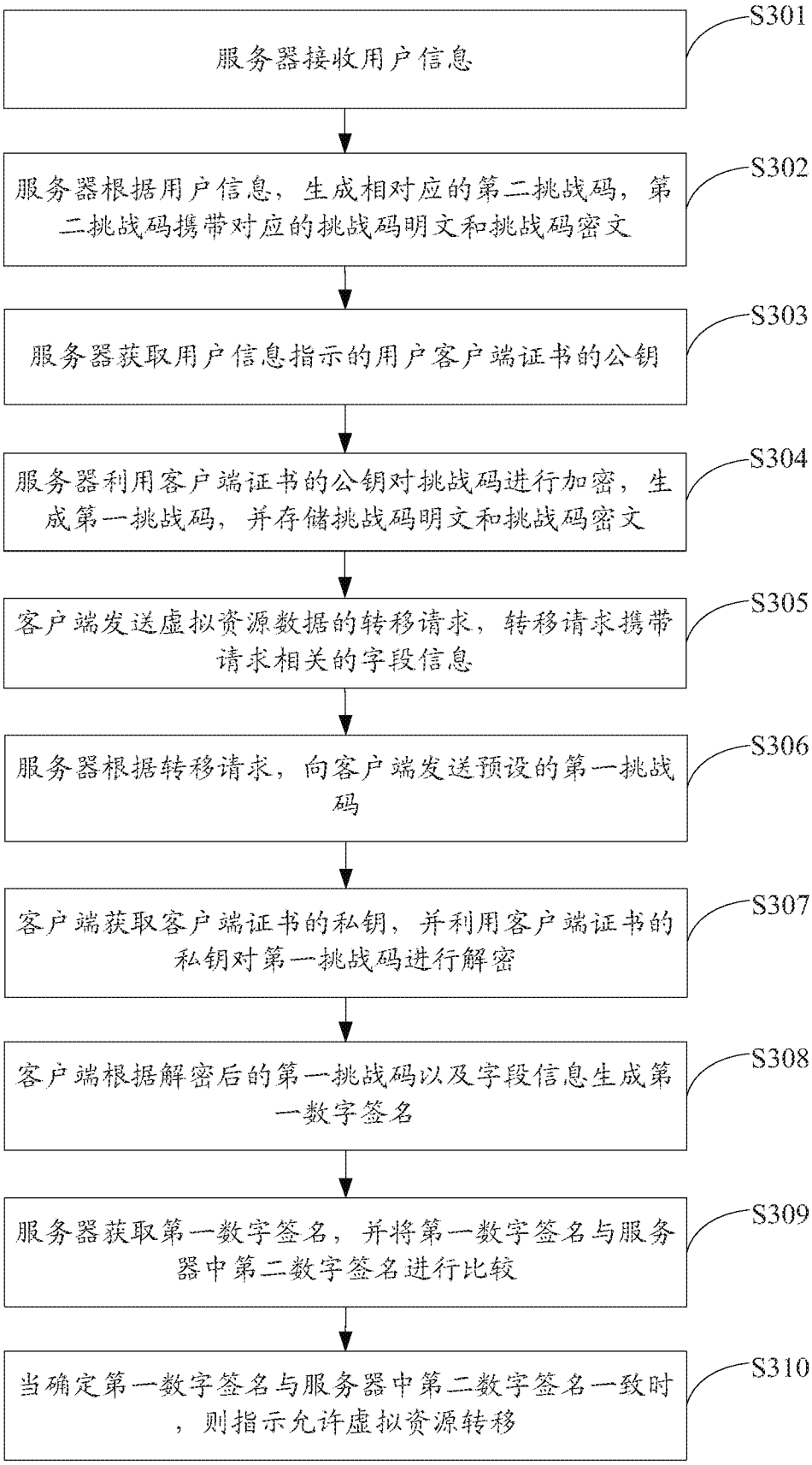
服务器接收用户信息
S301
服务器根据用户信息，生成相对应的第二挑战码，第二挑战码携带对应的挑战码明文和挑战码密文
S302
服务器获取用户信息指示的用户客户端证书的公钥
S303
服务器利用客户端证书的公钥对挑战码进行加密，生成第一挑战码，并存储挑战码明文和挑战码密文
S304
客户端发送虚拟资源数据的转移请求，转移请求携带请求相关的字段信息
S305
服务器根据转移请求，向客户端发送预设的第一挑战码
S306
客户端获取客户端证书的私钥，并利用客户端证书的私钥对第一挑战码进行解密
S307
客户端根据解密后的第一挑战码以及字段信息生成第一数字签名
S308
服务器获取第一数字签名，并将第一数字签名与服务器中第二数字签名进行比较
S309
当确定第一数字签名与服务器中第二数字签名一致时，则指示允许虚拟资源转移
S310

图 3

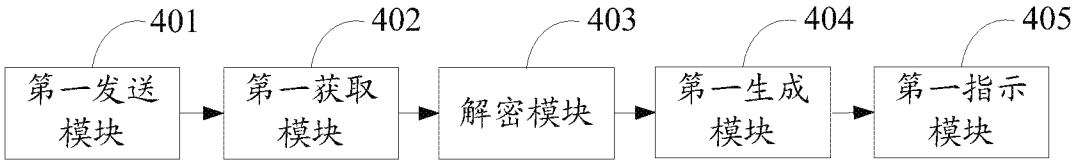
401
402
403
404
405
第一发送模块
第一获取模块
解密模块
第一生成模块
第一指示模块

图 4

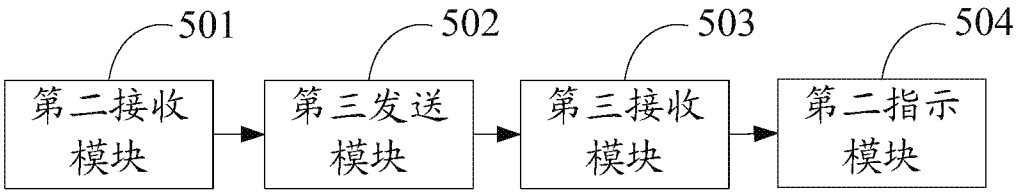
501
502
503
504
第二接收模块
第三发送模块
第三接收模块
第二指示模块

图 5

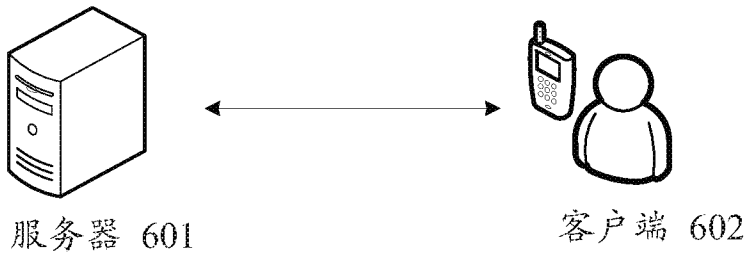
服务器 601
客户端 602

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/081565

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/00 (2006.01) i; G06Q 30/00 (2012.01) n

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q; H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT; WPI; EPODOC; CNKI: certificate, challenge password, pay, transaction, order, digital signature, transfer, challenge code, public W key, PKI, encrypt+, private W key, secret W key, decrypt+, signature, challenge

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 1477810 A (SHANGHAI KOAL SOFTWARE CO., LTD.), 25 February 2004 (25.02.2004), claims 1-4	1-17
X	CN 1859097 A (HUAWEI TECHNOLOGIES CO., LTD.), 08 November 2006 (08.11.2006), claims 1-5	1-17
A	CN 101083556 A (CAI, Shuiping), 05 December 2007 (05.12.2007), the whole document	1-17
A	WO 2004079985 A1 (TELECOM ITALIA MOBILE S.P.A.), 16 September 2004 (16.09.2004), the whole document	1-17

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
08 June 2016 (08.06.2016)	**26 July 2016 (26.07.2016)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **XU, Hongyan** Telephone No.: (86-10) **62413251**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/081565

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 1477810 A	25 February 2004	None	
CN 1859097 A	08 November 2006	None	
CN 101083556 A	05 December 2007	None	
WO 2004079985 A1	16 September 2004	JP 2006522514 A	28 September 2006
		US 2006189298 A1	24 August 2006
		CA 2518032 A1	16 September 2004
		EP 1602194 A1	07 December 2005
		CN 1757195 A	05 April 2006
		BR PI0408069 A	14 February 2006
		AT 402533 T	15 August 2008
		IT RM20030100 A1	07 September 2004
		DE 602004015259 E	04 September 2008

国际检索报告

国际申请号
PCT/CN2016/081565

A. 主题的分类

H04L 9/00(2006.01)i; G06Q 30/00(2012.01)n

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06Q; H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNPAT;WPI;EPODOC;CNKI:解密，私钥，证书，加密，挑战，挑战口令，支付，签名，交易，订单，数字签名，公钥，转账，挑战码,public W key, PKI,encrypt+, private W key,secret W key,decrypt+,signature,challenge

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 1477810 A (上海格尔软件股份有限公司) 2004年 2月 25日 (2004-02-25) 权利要求1-4	1-17
X	CN 1859097 A (华为技术有限公司) 2006年 11月 8日 (2006-11-08) 权利要求1-5	1-17
A	CN 101083556 A (蔡水平) 2007年 12月 5日 (2007-12-05) 全文	1-17
A	WO 2004079985 A1 (TELECOM ITALIA MOBILE S.P.A.) 2004年 9月 16日 (2004-09-16) 全文	1-17

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2016年 6月 8日	2016年 7月 26日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 许洪岩 电话号码 (86-10)62413251

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/081565

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	1477810	A	2004年 2月 25日	无			
CN	1859097	A	2006年 11月 8日	无			
CN	101083556	A	2007年 12月 5日	无			
WO	2004079985	A1	2004年 9月 16日	JP	2006522514	A	2006年 9月 28日
				US	2006189298	A1	2006年 8月 24日
				CA	2518032	A1	2004年 9月 16日
				EP	1602194	A1	2005年 12月 7日
				CN	1757195	A	2006年 4月 5日
				BR	PI0408069	A	2006年 2月 14日
				AT	402533	T	2008年 8月 15日
				IT	RM20030100	A1	2004年 9月 7日
				DE	602004015259	E	2008年 9月 4日