(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
2019 年 5 月 23 日 (23.05.2019)

WIPO | PCT

(10) 国际公布号
WO 2019/095864 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01)

(21) 国际申请号: PCT/CN2018/107569

(22) 国际申请日: 2018 年 9 月 26 日 (26.09.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201711135547.2 2017年11月16日 (16.11.2017) CN

(71) 申请人: 阿里巴巴集团控股有限公司 (**ALIBABA GROUP HOLDING LIMITED**) [—/CN]; 开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。

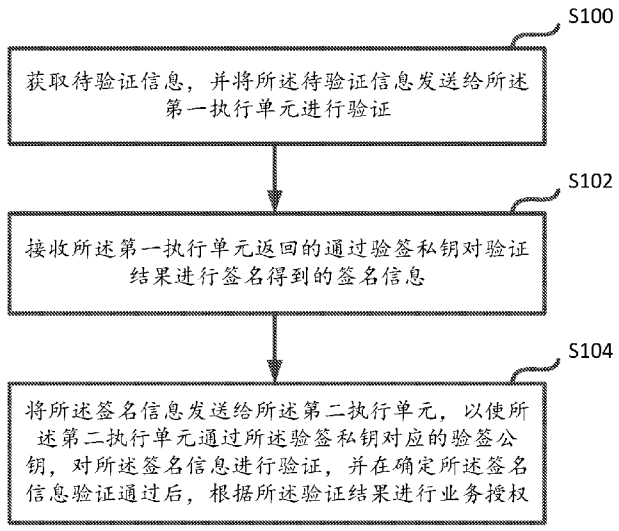
(72) 发明人: 孙曦 (**SUN, Xi**); 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 落红卫 (**LUO, Hongwei**); 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京博思佳知识产权代理有限公司 (**BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION**); 中国北京市海淀区上地三街 9 号嘉华大厦 B 座 409, Beijing 100085 (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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK,

(54) **Title:** SERVICE AUTHORIZATION METHOD, APPARATUS AND DEVICE

(54) 发明名称: 一种业务授权的方法、装置及设备



S100 ACQUIRE INFORMATION TO BE VERIFIED, AND SEND THE INFORMATION TO BE VERIFIED TO A FIRST EXECUTION UNIT FOR VERIFICATION

S102 RECEIVE SIGNATURE INFORMATION WHICH IS RETURNED BY THE FIRST EXECUTION UNIT AND OBTAINED BY SIGNING THE VERIFICATION RESULT BY MEANS OF A SIGNATURE VERIFICATION PRIVATE KEY

S104 SEND THE SIGNATURE INFORMATION TO A SECOND EXECUTION UNIT, SO THAT THE SECOND EXECUTION UNIT VERIFIES THE SIGNATURE INFORMATION BY MEANS OF A SIGNATURE VERIFICATION PUBLIC KEY CORRESPONDING TO THE VERIFICATION PRIVATE KEY, AND PERFORMS SERVICE AUTHORIZATION ACCORDING TO THE VERIFICATION RESULT AFTER IT IS DETERMINED THAT THE SIGNATURE INFORMATION PASSES THE VERIFICATION

图 1

(57) **Abstract:** Disclosed in the present description are a service authorization method, apparatus and device. In the method, after information to be verified is acquired, the information to be verified can be sent to a first execution unit, so that the first execution unit verifies the information to be verified, and signs the obtained verification result by means of a signature verification private key stored in the first execution unit, so as to obtain signature information. Then, a service application can obtain the signature information returned by the first execution unit, and then send the signature information to a second execution unit, so that the second execution unit verifies the signature information by means of a signature verification public key corresponding to the signature verification private key, and performs service authorization according to the verification result after it is determined that the signature information passes

WO 2019/095864 A1

[见续页]

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))。

the verification.

(57) 摘要：本说明书公开一种业务授权的方法、装置及设备，该方法中在获取到待验证信息后，可将该待验证信息发送至第一执行单元，以使该第一执行单元对该待验证信息进行验证，并将得到的验证结果通过该第一执行单元所保存的验签私钥进行签名，得到签名信息。而后，业务应用可以获取到该第一执行单元所返回的该签名信息，进而该将签名信息发送给第二执行单元，以使该第二执行单元通过该验签私钥所对应的验签公钥，对该签名信息进行验证，并在确定该签名信息验证通过后，根据该验证结果进行业务授权。

一种业务授权的方法、装置及设备

技术领域

[01]本说明书涉及计算机技术领域，尤其涉及一种业务授权的方法、装置及设备。

背景技术

[02]当前，传统基于密码的身份验证方式由于其存在易被遗忘、易被窃取、不便于输入等问题，已逐渐无法满足用户在进行身份验证时的便利性和安全性的需求，而基于指纹、声纹、面部识别等生物特征的身份验证方式由于其更为安全、更为便捷，已在各种场景中广泛应用。

[03]在实际应用中，设备运行的系统中通常包括两种环境，一种是可信执行环境（Trusted Execution Environment，TEE），一种为安全元件（Secure Element，SE）所提供的执行环境，其中，用于进行业务处理的业务应用通常运行在该 TEE 中。而用于对用户所要执行的业务进行授权的安全应用则运行在 SE 中。通常情况下，终端需要对用户输入的待验证生物特征信息进行验证，得到验证结果，该验证结果需要发送至该安全应用进行验证，而只有该安全应用确定该验证结果通过验证后，该安全应用才会对此次业务应用所执行的业务进行授权，进而使得业务应用执行该业务。

[04]然而，由于验证结果在从 TEE 传递至 SE 的过程中可能会存在被篡改的可能，所以，安全应用如何取信从 TEE 发来的验证结果则是一个值得考虑的问题。

[05]基于现有技术，需要更为有效的业务授权方式。

发明内容

[06]本说明书提供一种业务授权的方法，用以解决现有技术中一种安全环境所产生的身份验证的验证结果无法得到另一个安全环境授信认证的问题。

[07]本说明书提供了一种业务授权的方法，设备的系统中至少包括第一安全环境以及第二安全环境，第一执行单元在所述第一安全环境中运行，第二执行单元在所述第二安全环境中运行，所述方法包括：

[08]获取待验证信息，并将所述待验证信息发送给所述第一执行单元进行验证；

[09]接收所述第一执行单元返回的通过验签私钥对验证结果进行签名得到的签名信息；

[10]将所述签名信息发送给所述第二执行单元，以使所述第二执行单元通过所述验签私钥对应的验签公钥，对所述签名信息进行验证，并在确定所述签名信息验证通过后，根据所述验证结果进行业务授权。

[11]本说明书提供一种业务授权的装置，用以解决现有技术中一种安全环境所产生的身份验证的验证结果无法得到另一个安全环境授信认证的问题。

[12]本说明书提供了一种业务授权的装置，包含所述装置的设备的系统中至少包括第一安全环境以及第二安全环境，第一执行单元在所述第一安全环境中运行，第二执行单元在所述第二安全环境中运行，所述装置包括:

[13]获取模块，获取待验证信息，并将所述待验证信息发送给所述第一执行单元进行验证;

[14]接收模块，接收所述第一执行单元返回的通过验签私钥对验证结果进行签名得到的签名信息;

[15]发送模块，将所述签名信息发送给所述第二执行单元，以使所述第二执行单元通过所述验签私钥对应的验签公钥，对所述签名信息进行验证，并在确定所述签名信息验证通过后，根据所述验证结果进行业务授权。

[16]本说明书提供一种业务授权的设备，用以解决现有技术中一种安全环境所产生的身份验证的验证结果无法得到另一个安全环境授信认证的问题。

[17]本说明书提供了一种业务授权的设备，包括一个或多个存储器以及处理器，所述存储器存储程序，并且被配置成由所述一个或多个处理器执行以下步骤:

[18]获取待验证信息，并将所述待验证信息发送给第一执行单元进行验证，其中，所述第一执行单元在所述设备的系统包括的第一安全环境中运行;

[19]接收所述第一执行单元返回的通过验签私钥对验证结果进行签名得到的签名信息;

[20]将所述签名信息发送给第二执行单元，以使所述第二执行单元通过所述验签私钥对应的验签公钥，对所述签名信息进行验证，并在确定所述签名信息验证通过后，根据所述验证结果进行业务授权，其中，所述第二执行单元在所述设备的系统包括的第二安全环境中运行。

[21]本说明书提供一种业务授权的方法，用以解决现有技术中一种安全环境所产生的身份验证的验证结果无法得到另一个安全环境授信认证的问题。

[22]本说明书提供了一种业务授权的方法，设备的系统中至少包括第一安全环境以及第二安全环境，第一执行单元在所述第一安全环境中运行，第二执行单元在所述第二安全环境中运行，所述方法包括：

[23]所述第一执行单元接收业务应用发送的待验证信息；

[24]对所述待验证信息进行验证，并将得到的验证结果通过保存的验签私钥进行签名，得到签名信息；

[25]将所述签名信息通过所述业务应用发送给所述第二执行单元，以使所述第二执行单元通过所述验签私钥对应的验签公钥，对所述签名信息进行验证，并在所述签名信息验证通过后，根据所述验证结果进行业务授权。

[26]本说明书提供一种业务授权的装置，用以解决现有技术中一种安全环境所产生的身份验证的验证结果无法得到另一个安全环境授信认证的问题。

[27]本说明书提供了一种业务授权的装置，设备的系统中至少包括第一安全环境以及第二安全环境，所述装置在所述第一安全环境中运行，第二执行单元在所述第二安全环境中运行，所述装置包括：

[28]接收模块，接收业务应用发送的待验证信息；

[29]验证模块，对所述待验证信息进行验证，并将得到的验证结果通过保存的验签私钥进行签名，得到签名信息；

[30]发送模块，将所述签名信息通过所述业务应用发送给所述第二执行单元，以使所述第二执行单元通过所述验签私钥对应的验签公钥，对所述签名信息进行验证，并在所述签名信息验证通过后，根据所述验证结果进行业务授权。

[31]本说明书提供一种业务授权的设备，用以解决现有技术中一种安全环境所产生的身份验证的验证结果无法得到另一个安全环境授信认证的问题。

[32]本说明书提供了一种业务授权的设备，包括一个或多个存储器以及处理器，所述存储器存储程序，并且被配置成由所述一个或多个处理器执行以下步骤：

[33]第一执行单元接收业务应用发送的待验证信息，其中，所述第一执行单元在所述设备的系统包括的第一安全环境中运行；

[34]对所述待验证信息进行验证，并将得到的验证结果通过保存的验签私钥进行签名，得到签名信息；

[35]将所述签名信息通过所述业务应用发送给第二执行单元，以使所述第二执行单元通过所述验签私钥对应的验签公钥，对所述签名信息进行验证，并在所述签名信息验证通过后，根据所述验证结果进行业务授权，其中，所述第二执行单元在所述设备的系统包括的第二安全环境中运行。

[36]本说明书提供一种业务授权的方法，用以解决现有技术中一种安全环境所产生的身份验证的验证结果无法得到另一个安全环境授信认证的问题。

[37]本说明书提供了一种业务授权的方法，设备的系统中至少包括第一安全环境以及第二安全环境，第一执行单元在所述第一安全环境中运行，第二执行单元在所述第二安全环境中运行，所述方法包括:

[38]所述第二执行单元获取所述第一执行单元通过业务应用发送的签名信息，所述签名信息是所述第一执行单元通过验签私钥对验证结果进行签名后得到的，所述验证结果是所述第一执行单元对所述业务应用发送的待验证信息进行验证后得到的;

[39]通过所述验签私钥对应的验签公钥，对所述签名信息进行验证，并在确定所述签名信息通过验证后，根据从所述签名信息中解析出的所述验证结果进行业务授权。

[40]本说明书提供一种业务授权的装置，用以解决现有技术中一种安全环境所产生的身份验证的验证结果无法得到另一个安全环境授信认证的问题。

[41]本说明书提供了一种业务授权的装置，设备的系统中至少包括第一安全环境以及第二安全环境，第一执行单元在所述第一安全环境中运行，所述装置在所述第二安全环境中运行，所述装置包括:

[42]获取模块，获取所述第一执行单元通过业务应用发送的签名信息，所述签名信息是所述第一执行单元通过验签私钥对验证结果进行签名后得到的，所述验证结果是所述第一执行单元对所述业务应用发送的待验证信息进行验证后得到的;

[43]验证模块，通过所述验签私钥对应的验签公钥，对所述签名信息进行验证，并在确定所述签名信息通过验证后，根据从所述签名信息中解析出的所述验证结果进行业务授权。

[44]本说明书提供一种业务授权的设备，用以解决现有技术中一种安全环境所产生的身份验证的验证结果无法得到另一个安全环境授信认证的问题。

[45]本说明书提供了一种业务授权的设备，包括一个或多个存储器以及处理器，所述存

储器存储程序，并且被配置成由所述一个或多个处理器执行以下步骤：

[46]第二执行单元获取第一执行单元通过业务应用发送的签名信息，所述签名信息是所述第一执行单元通过验签私钥对验证结果进行签名后得到的，所述验证结果是所述第一执行单元对所述业务应用发送的待验证信息进行验证后得到的，其中，所述第一执行单元在所述设备的系统包括的第一安全环境中运行，所述第二执行单元在所述设备的系统包括的第二安全环境中运行；

[47]通过所述验签私钥对应的验签公钥，对所述签名信息进行验证，并在确定所述签名信息通过验证后，根据从所述签名信息中解析出的所述验证结果进行业务授权。

[48]本说明书采用的上述至少一个技术方案能够达到以下有益效果：

[49]在本说明书一个或多个实施例中，运行于第一安全环境中的第一执行单元可以对获取到的待验证信息进行验证，将得到的验证结果通过保存的验签私钥进行签名，进而将得到的签名信息通过业务应用发送给运行在第二安全环境中的第二执行单元，第二执行单元可以通过该验签私钥对应的验签公钥对该签名信息进行验证，并在确定该签名信息验证通过后，根据该验证结果进行业务授权。换句话说，利用非对称加密方式，可以使运行于第二安全环境中的第二执行单元对运行在第一安全环境中的第一执行单元所得到的验证结果进行授信认证，从而使得第二执行单元能够基于第一执行单元所得到的验证结果，确定是否对业务应用所执行的业务进行授权，进而向用户提供了更为安全、有效的身份验证方式。

附图说明

[50]此处所说明的附图用来提供对本说明书的进一步理解，构成本说明书的一部分，本说明书的示意性实施例及其说明用于解释本说明书，并不构成对本说明书的不当限定。在附图中：

[51]图 1 为本说明书提供的业务授权过程的示意图；

[52]图 2 为本说明书提供的业务应用通过第二执行单元发送的动态参数向第二执行单元申请业务授权的过程示意图；

[53]图 3 为本说明书提供的通过公钥证书对签名信息进行验证的示意图；

[54]图 4 为本说明书提供的一种业务授权的装置示意图；

[55] 图 5 为本说明书提供的一种业务授权的装置示意图;

[56] 图 6 为本说明书提供的一种业务授权的装置示意图;

[57] 图 7 为本说明书提供的一种业务授权的设备示意图;

[58] 图 8 为本说明书提供的一种业务授权的设备示意图;

[59] 图 9 为本说明书提供的一种业务授权的设备示意图。

具体实施方式

[60] 通常情况下，设备运行的系统中通常包括不同的安全环境，而在实际应用中，往往需要通过不同安全环境中执行单元或应用的相互协作，才能完成整个的业务执行过程。具体的，运行于第一安全环境中的业务应用，可以将设备获取到的待验证信息发送给运行在第一安全环境中的第一执行单元，第一执行单元可以对该待验证信息进行验证，并将得到的验证结果发送给运行于第二安全环境中的第二执行单元，第二执行单元可以通过该验证结果，确定是否对业务应用当前执行的业务进行授权。

[61] 由于第一执行单元和第二执行单元位于不同的安全环境中，所以，通常情况下，运行于第二安全环境的第二执行单元通常无法保证运行于第一安全环境的第一执行单元将对待验证信息进行验证后得到的验证结果发送至第二执行单元的过程中，该验证结果不会被篡改，所以，第二执行单元如何对第一执行单元所发送的验证结果进行取信，则是一个值得考虑的问题。

[62] 为此，本说明书提供了一种业务授权的方法，在获取到待验证信息后，可将该待验证信息发送至第一执行单元，以使该第一执行单元对该待验证信息进行验证，并将得到的验证结果通过该第一执行单元所保存的验签私钥进行签名，得到签名信息。而后，业务应用可以获取到该第一执行单元所返回的该签名信息，进而该将签名信息发送给第二执行单元，以使该第二执行单元通过该验签私钥所对应的验签公钥，对该签名信息进行验证，并在确定该签名信息验证通过后，根据该验证结果进行业务授权。

[63] 由于利用非对称加密方式，可以使运行于第二安全环境中的第二执行单元对运行于第一安全环境中的第一执行单元所得到的验证结果进行授信认证，从而使得第二执行单元能够基于第一执行单元所得到的验证结果，确定是否对业务应用所执行的业务进行授权，进而向用户提供了更为安全、有效的身份验证方式。

[64] 为了使本技术领域的人员更好地理解本说明书一个或多个实施例中的技术方案，下

面将结合本说明书一个或多个实施例中的附图，对本说明书一个或多个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说明书一部分实施例，而不是全部的实施例。基于本说明书中的实施例，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，都应当属于本说明书保护的范围。

[65]图 1 为本说明书提供的业务授权过程的示意图，具体包括以下步骤:

[66]S100: 获取待验证信息，并将所述待验证信息发送给所述第一执行单元进行验证。

[67]在本说明书中，用户在执行业务时，可以将需要进行身份验证的待验证信息输入到设备中业务应用，以使该业务应用通过该设备中的第一执行单元对该待验证信息进行验证。其中，这里提到的设备可以是诸如智能手机、平板电脑等移动终端设备。而这里提到的待验证信息可以是指诸如指纹、声纹、面部信息等待验证生物特征信息，也可以是指字符形式的待验证信息。当然，设备也可通过预设的接口，将采集到的待验证信息直接发送给第一执行单元。

[68]第一执行单元在获取到该待验证信息后，可以对其进行验证，并得到相应的验证结果。例如，第一执行单元在获取到待验证指纹后，可以将该待验证指纹与预先保存的用户的指纹信息进行匹配，并根据匹配结果，确定用户是否通过指纹验证。

[69]需要说明的是，在本说明书中，第一安全环境可以是指 TEE，运行于第一安全环境中的第一执行单元可以是指用于进行信息验证的模块，该模块可以是软件的形式，也可以是硬件的形式。第二安全环境可以是指 SE 所提供的执行环境，相应的，第二执行单元可以是指运行在 SE 中的安全应用。

[70]S102: 接收所述第一执行单元返回的通过验签私钥对验证结果进行签名得到的签名信息。

[71]第一执行单元对该待验证信息进行验证后，可将得到的验证结果通过自己所保存的验签私钥进行签名，得到的相应的签名信息，并在后续的过程中，将该签名信息返回给业务应用。

[72]在本说明书中，第一执行单元可以从该第一执行单元所对应的第一管理服务器获取到用于对验证结果进行签名的验签私钥。其中，该第一管理服务器可以针对该第一执行单元，生成唯一的一对验签私钥和验签公钥，并将该验签私钥下发至该第一执行单元中。而该验签公钥则可由该第一管理服务器发送给第二执行单元所对应的第二管理服务器中，以通过该第二管理服务器，将该验签公钥发送至第二执行单元，以在后续过程中，

使该第二执行单元通过该验签公钥对第一执行单元所生成的签名信息进行验证。

[73]在本说明书中，第一执行单元可以将得到的签名信息返回给该业务应用，以使该业务应用在后续将该签名信息发送给第二执行单元进行验证。其中，第一执行单元需要通过该业务应用将该签名信息发送给第二执行单元的原因在于，由于第一执行单元和第二执行单元位于不同的安全环境中，且，第二执行单元未对该第一执行单元进行访问授权，所以，通常情况下，第一执行单元是无法向运行于第二安全环境中的第二执行单元发送信息的。而由于第二执行单元需要对业务应用所执行的业务进行授权，所以，通常第二执行单元会对业务应用进行访问授权，允许业务应用向该第二执行单元进行访问。基于此，第一执行单元需要通过业务应用，将该签名信息发送给该第二执行单元。

[74]S104：将所述签名信息发送给所述第二执行单元，以使所述第二执行单元通过所述验签私钥对应的验签公钥，对所述签名信息进行验证，并在确定所述签名信息验证通过后，根据所述验证结果进行业务授权。

[75]业务应用可将第一执行单元返回的签名信息发送给运行于第二安全环境中的第二执行单元，该第二执行单元可以通过获取到的验签公钥，对该签名信息进行验证，进而在确定该签名信息通过验证后，可以通过解析出的验证结果，确定是否对该业务应用所执行的业务进行授权。

[76]从上述方法中可以看出，运行于第一安全环境中的第一执行单元可以对获取到的待验证信息进行验证，将得到的验证结果通过保存的验签私钥进行签名，进而将得到的签名信息通过业务应用发送给运行在第二安全环境中的第二执行单元，第二执行单元可以通过该验签私钥对应的验签公钥对该签名信息进行验证，并在确定该签名信息验证通过后，根据该验证结果进行业务授权。换句话说，利用非对称加密方式，可以使运行于第二安全环境中的第二执行单元对运行在第一安全环境中的第一执行单元所得到的验证结果进行授信认证，从而使得第二执行单元能够基于第一执行单元所得到的验证结果，确定是否对业务应用所执行的业务进行授权，进而向用户提供了更为安全、有效的身份验证方式。

[77]在上述说明的业务授权过程中，用户所使用的设备可能会面临重放攻击的可能，即，不法份子获取到验证通过的验证结果后，可以通过该验证结果不断的向第二执行单元申请业务授权，从而可能导致用户的信息或财产遭到损失。

[78]为了防止上述情况的发生，业务应用可以从该第二执行单元获取到由该第二执行单

元生成的动态参数，并将该动态参数发送给第一执行单元，以使该第一执行单元对该动态参数以及得到的验证结果一并进行签名，得到签名信息，如图 2 所示。

[79]图 2 为本说明书提供的业务应用通过第二执行单元发送的动态参数向第二执行单元申请业务授权的过程示意图。

[80]在图 2 中，业务应用可以访问运行于第二安全环境的第二执行单元，以获取到诸如随机数、时间信息等动态参数，其中，该动态参数可以由第二执行单元生成并在该第二执行单元中保存设定时间，在到达设定时间后，该第二执行单元可以将该动态参数删除。这里可以理解成，该第二执行单元对生成的动态参数设置了一个有效时间，即，业务应用只有在该有效时间内将第一执行单元对动态参数以及验证结果进行签名后得到的签名信息发送至第二执行单元中，第二执行单元才可以通过保存的动态参数对从该签名信息中解析出的动态参数进行验证，而一旦超过该有效时间，该动态参数将被作废，这样，从该签名信息中解析出的动态参数将无法通过第二执行单元的验证。

[81]第一执行单元可以对业务应用发送的待验证信息进行验证，得到相应的验证结果，并通过保存的验签私钥，对该验证结果以及获取到的动态参数进行签名，得到签名信息。

[82]第一执行单元可以将得到的签名信息返回给业务应用，由该业务应用将该签名信息发送给第二执行单元。第二执行单元可以通过从第二管理服务器获取到的验签公钥对该签名信息进行验证，并在确定该签名信息通过验证后，根据预先保存的动态参数对从该签名信息解析出的动态参数进行验证，即，对解析出的动态参数与保存的动态参数进行比对，确定两者是否一致，一致时，确定解析出的动态参数通过验证，不一致时，确定解析出的动态参数未通过验证。在确定该动态参数通过验证后，则可以根据从该签名信息中解析出的验证结果，确定是否对业务应用所执行的业务进行授权。

[83]其中，这里提到的验签公钥以及验签私钥是由第一执行单元所对应的第一管理服务器生成的，该第一管理服务器可以将生成的验签私钥发送给第一执行单元进行保存，并将该验签公钥通过第二执行单元所对应的第二管理服务器下发给第二执行单元。

[84]由于在每次业务执行过程中，业务应用向第二执行单元获取的动态参数均不相同，所以，即使不法份子利用某一次验证通过的验证结果，也无法通过重放攻击的方式，不断向第二执行单元申请业务授权，从而保证了用户的信息以及财产的安全。

[85]需要说明的是，第一管理服务器可以针对不同的第一执行单元，生成唯一的一对验签密钥对，也可以针对一个批次的第一执行单元，生成这一批次第一执行单元所需的验

签密钥对。换句话说，第一管理服务器可以针对每一个设备，生成唯一对应该设备的一对验签密钥对，也可以针对一批次的设备，生成对应这一批次设备的一对验签密钥对。

[86]在本说明书中，业务应用从第二执行单元获取上述动态参数的时机可以有很多，例如，业务应用可以先从第二执行单元中获取该动态参数，而后再将该动态参数和获取到的待验证信息发送给第一执行单元，也可以先将该待验证信息发送给第一执行单元，而后再从第二执行单元获取该动态参数并发送给第一执行单元。

[87]在本说明书中，第一管理服务器生成的验签公钥可以发送至证书授权（Certificate Authority，CA）中心进行公证，并得到相应的公钥证书，而后续第二执行单元可以通过该公钥证书，对业务应用发送的签名信息进行验证，如图 3 所示。

[88]图 3 为本说明书提供的通过公钥证书对签名信息进行验证的示意图。

[89]第一执行单元所对应的第一管理服务器在生成一对验签密钥对后，可以将该验签密钥对中的验签公钥发送至 CA 中心进行公证，该 CA 中心可以根据该验签公钥以及其他信息（如申请对该验签公钥进行公证的申请人的信息、时间信息等），生成被自己所保存的 CA 私钥进行签名的公钥证书。而后，CA 中心可以将该公钥证书通过第一管理服务器发送给第一执行单元进行保存，同时将该 CA 私钥所对应的 CA 公钥通过第二管理服务器发送给第二执行单元进行保存。

[90]这样一来，第一执行单元生成签名信息后，可以将该签名信息以及公钥证书通过业务应用发送给第二执行单元，第二执行单元可以通过获取到的 CA 公钥，对该公钥证书进行验证，并通过从该公钥证书解析出的验签公钥，对该签名信息进行验证。在确定该签名信息验证通过后，进一步对从该签名信息中解析出的动态参数进行验证，并在确定该动态参数通过验证后，根据从该签名信息解析出的验证结果，确定是否对业务应用当前所执行的业务进行授权。

[91]在本说明书中，第一执行单元可以在确定业务应用发送的待验证信息通过验证后，对获取到的动态参数进行签名，得到相应的签名信息。而第二执行单元通过业务应用接收到该签名信息时，则可以确定先前的待验证信息已通过第一执行单元的验证，进而在确定从该签名信息中解析出的动态参数通过验证时，可以对该业务应用当前所执行的业务进行授权。

[92]在本说明书中，业务应用可以通过该业务应用在第一安全环境中运行时所能提供的界面，将从第一执行单元获取到的签名信息等数据展示给用户。同理，第一执行单元也

可以通过该第一执行单元在第一安全环境中运行时所能提供的界面，将对该待验证信息进行验证后的验证结果进行展示，以使用户可以对该验证结果进行查看。

[93]从上述方法中可以看出，通过非对称加密方式，可以使运行于第二安全环境中的第二执行单元对运行在第一安全环境中的第一执行单元所得到的验证结果进行授信认证，从而使得第二执行单元能够基于第一执行单元所得到的验证结果，确定是否对业务应用所执行的业务进行授权。

[94]并且通过上述方式，第二执行单元可以授信第一执行单元所进行的生物识别验证，这样一来，对于需要两个不同安全环境相互协作完成的业务来说，用户可以通过生物识别这种简单、易操作的身份验证方式，进行身份验证，从而给用户在业务执行的过程中，带来了良好的用户体验。

[95]以上为本说明书的一个或多个实施例提供的业务授权方法，基于同样的思路，本说明书还提供了相应的业务授权的装置，如图 4、5、6 所示。

[96]图 4 为本说明书提供的一种业务授权的装置示意图，具体包括：

[97]获取模块 401，获取待验证信息，并将所述待验证信息发送给所述第一执行单元进行验证；

[98]接收模块 402，接收所述第一执行单元返回的通过验签私钥对验证结果进行签名得到的签名信息；

[99]发送模块 403，将所述签名信息发送给所述第二执行单元，以使所述第二执行单元通过所述验签私钥对应的验签公钥，对所述签名信息进行验证，并在确定所述签名信息验证通过后，根据所述验证结果进行业务授权。

[100] 所述第一安全环境包括：可信执行环境 TEE；所述第二安全环境包括：安全元件 SE 提供的执行环境。

[101] 所述待验证信息包括：待验证生物特征信息。

[102] 所述获取模块 401，获取所述第二执行单元发送的动态参数，所述动态参数包括：随机数、时间信息中的至少一种；将所述动态参数发送给所述第一执行单元，使所述第一执行单元通过所述验签私钥对所述验证结果和所述动态参数进行签名。

[103] 图 5 为本说明书提供的一种业务授权的装置示意图，具体包括：

[104] 接收模块 501，接收业务应用发送的待验证信息；

[105] 验证模块 502，对所述待验证信息进行验证，并将得到的验证结果通过保存的验签私钥进行签名，得到签名信息；

[106] 发送模块 503，将所述签名信息通过所述业务应用发送给所述第二执行单元，以使所述第二执行单元通过所述验签私钥对应的验签公钥，对所述签名信息进行验证，并在所述签名信息验证通过后，根据所述验证结果进行业务授权。

[107] 所述业务应用在所述第一安全环境中运行。

[108] 所述接收模块 501，接收所述第二执行单元通过所述业务应用发送的动态参数。

[109] 所述验证模块 502，将所述验证结果以及所述动态参数通过所述验签私钥进行签名，得到签名信息。

[110] 所述装置还包括：

[111] 获取模块 504，从所述装置对应的第一管理服务器，获取所述验签私钥。

[112] 所述获取模块 504，从所述第一管理服务器获取所述验签公钥的公钥证书，所述公钥证书是所述第一管理服务器从证书授权 CA 中心获取到的，所述公钥证书是所述 CA 中心根据保存的 CA 私钥对所述验签公钥进行认证后得到的。

[113] 所述发送模块 503，将所述公钥证书以及所述签名信息通过所述业务应用发送给所述第二执行单元，以使所述第二执行单元通过从所述 CA 中心获取到的 CA 公钥，对所述公钥证书进行验证，并在确定所述公钥证书验证通过后，通过从所述公钥证书中解析出的验签公钥，对所述签名信息进行验证。

[114] 图 6 为本说明书提供的一种业务授权的装置示意图，具体包括：

[115] 获取模块 601，获取所述第一执行单元通过业务应用发送的签名信息，所述签名信息是所述第一执行单元通过验签私钥对验证结果进行签名后得到的，所述验证结果是所述第一执行单元对所述业务应用发送的待验证信息进行验证后得到的；

[116] 验证模块 602，通过所述验签私钥对应的验签公钥，对所述签名信息进行验证，并在确定所述签名信息通过验证后，根据从所述签名信息中解析出的所述验证结果进行业务授权。

[117] 所述验签公钥是所述装置通过所述装置对应的第二管理服务器，从所述第一执行单元对应的第一管理服务器获取到的。

[118] 所述获取模块 601，通过所述装置对应的第二管理服务器，从证书授权 CA 中心

获取 CA 公钥。

[119] 所述验证模块 602，通过所述 CA 公钥，对从所述业务应用发送的公钥证书进行验证，所述公钥证书是所述 CA 中心根据所述 CA 公钥对应的 CA 私钥对所述验签公钥进行认证后得到的，所述公钥证书是所述业务应用从所述第一执行单元获取到的，所述公钥证书是所述第一执行单元通过所述第一执行单元对应的第一管理服务器从所述 CA 中心获取到的；当确定所述公钥证书通过验证后，通过从所述公钥证书中解析出的验签公钥，对所述签名信息进行验证，并在确定所述签名信息通过验证后，根据从所述签名信息中解析出的所述验证结果进行业务授权。

[120] 所述装置还包括：

[121] 发送模块 603，发送动态参数至所述业务应用，以使所述第一执行单元通过所述验签私钥，对所述验证结果以及从所述业务应用获取到的所述动态参数进行签名，得到签名信息。

[122] 所述验证模块 602，通过所述 CA 公钥，对所述公钥证书进行验证；当确定所述公钥证书通过验证后，通过从所述公钥证书中解析出的验签公钥，对所述签名信息进行验证；当确定所述签名信息通过验证后，对从所述签名信息中解析出的动态参数进行验证，并在确定所述动态参数通过验证后，根据从所述签名信息中解析出的所述验证结果进行业务授权。

[123] 基于上述说明的业务授权的方法，本说明书还对应提供了一种用于业务授权的设备，如图 7 所示。该设备包括一个或多个存储器以及处理器，所述存储器存储程序，并且被配置成由所述一个或多个处理器执行以下步骤：

[124] 获取待验证信息，并将所述待验证信息发送给第一执行单元进行验证，其中，所述第一执行单元在所述设备的系统包括的第一安全环境中运行；

[125] 接收所述第一执行单元返回的通过验签私钥对验证结果进行签名得到的签名信息；

[126] 将所述签名信息发送给第二执行单元，以使所述第二执行单元通过所述验签私钥对应的验签公钥，对所述签名信息进行验证，并在确定所述签名信息验证通过后，根据所述验证结果进行业务授权，其中，所述第二执行单元在所述设备的系统包括的第二安全环境中运行。

[127] 基于上述说明的业务授权的方法，本说明书还对应提供了一种用于业务授权的

设备，如图 8 所示。该设备包括一个或多个存储器以及处理器，所述存储器存储程序，并且被配置成由所述一个或多个处理器执行以下步骤：

[128] 第一执行单元接收业务应用发送的待验证信息，其中，所述第一执行单元在所述设备的系统包括的第一安全环境中运行；

[129] 对所述待验证信息进行验证，并将得到的验证结果通过保存的验签私钥进行签名，得到签名信息；

[130] 将所述签名信息通过所述业务应用发送给第二执行单元，以使所述第二执行单元通过所述验签私钥对应的验签公钥，对所述签名信息进行验证，并在所述签名信息验证通过后，根据所述验证结果进行业务授权，其中，所述第二执行单元在所述设备的系统包括的第二安全环境中运行。

[131] 基于上述说明的业务授权的方法，本说明书还对应提供了一种用于业务授权的设备，如图 9 所示。该设备包括一个或多个存储器以及处理器，所述存储器存储程序，并且被配置成由所述一个或多个处理器执行以下步骤：

[132] 第二执行单元获取第一执行单元通过业务应用发送的签名信息，所述签名信息是所述第一执行单元通过验签私钥对验证结果进行签名后得到的，所述验证结果是所述第一执行单元对所述业务应用发送的待验证信息进行验证后得到的，其中，所述第一执行单元在所述设备的系统包括的第一安全环境中运行，所述第二执行单元在所述设备的系统包括的第二安全环境中运行；

[133] 通过所述验签私钥对应的验签公钥，对所述签名信息进行验证，并在确定所述签名信息通过验证后，根据从所述签名信息中解析出的所述验证结果进行业务授权。

[134] 在本说明书的一个或多个实施例中，在获取到待验证信息后，可将该待验证信息发送至第一执行单元，以使该第一执行单元对该待验证信息进行验证，并将得到的验证结果通过该第一执行单元所保存的验签私钥进行签名，得到签名信息。而后，业务应用可以获取到该第一执行单元所返回的该签名信息，进而该将签名信息发送给第二执行单元，以使该第二执行单元通过该验签私钥所对应的验签公钥，对该签名信息进行验证，并在确定该签名信息验证通过后，根据该验证结果进行业务授权。

[135] 由于利用非对称加密方式，可以使运行于第二安全环境中的第二执行单元对运行于第一安全环境中的第一执行单元所得到的验证结果进行授信认证，从而使得第二执行单元能够基于第一执行单元所得到的验证结果，确定是否对业务应用所执行的业务进

行授权，进而向用户提供了更为安全、有效的身份验证方式。

[136] 在20世纪90年代，对于一个技术的改进可以很明显地区分是硬件上的改进（例如，对二极管、晶体管、开关等电路结构的改进）还是软件上的改进（对于方法流程的改进）。然而，随着技术的发展，当今的很多方法流程的改进已经可以视为硬件电路结构的直接改进。设计人员几乎都通过将改进的方法流程编程到硬件电路中来得到相应的硬件电路结构。因此，不能说一个方法流程的改进就不能用硬件实体模块来实现。例如，可编程逻辑器件（Programmable Logic Device，PLD）（例如现场可编程门阵列（Field Programmable Gate Array，FPGA））就是这样一种集成电路，其逻辑功能由用户对器件编程来确定。由设计人员自行编程来把一个数字系统“集成”在一片PLD上，而不需要请芯片制造厂商来设计和制作专用的集成电路芯片。而且，如今，取代手工地制作集成电路芯片，这种编程也多半改用“逻辑编译器（logic compiler）”软件来实现，它与程序开发撰写时所用的软件编译器相类似，而要编译之前的原始代码也得用特定的编程语言来撰写，此称之为硬件描述语言（Hardware Description Language，HDL），而HDL也并非仅有一种，而是有许多种，如ABEL（Advanced Boolean Expression Language）、AHDL（Altera Hardware Description Language）、Confluence、CUPL（Cornell University Programming Language）、HDCal、JHDL（Java Hardware Description Language）、Lava、Lola、MyHDL、PALASM、RHDL（Ruby Hardware Description Language）等，目前最普遍使用的是VHDL（Very-High-Speed Integrated Circuit Hardware Description Language）与Verilog。本领域技术人员也应该清楚，只需要将方法流程用上述几种硬件描述语言稍作逻辑编程并编程到集成电路中，就可以很容易得到实现该逻辑方法流程的硬件电路。

[137] 控制器可以按任何适当的方式实现，例如，控制器可以采取例如微处理器或处理器以及存储可由该（微）处理器执行的计算机可读程序代码（例如软件或固件）的计算机可读介质、逻辑门、开关、专用集成电路（Application Specific Integrated Circuit，ASIC）、可编程逻辑控制器和嵌入微控制器的形式，控制器的例子包括但不限于以下微控制器：ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20以及Silicone Labs C8051F320，存储器控制器还可以被实现为存储器的控制逻辑的一部分。本领域技术人员也知道，除了以纯计算机可读程序代码方式实现控制器以外，完全可以通过将方法步骤进行逻辑编程来使得控制器以逻辑门、开关、专用集成电路、可编程逻辑控制器和嵌入微控制器等的形式来实现相同功能。因此这种控制器可以被认为是一种硬件部件，而对其内包括的用于实现各种功能的装置也可以视为硬件部件内的结构。或者甚至，可以

将用于实现各种功能的装置视为既可以是实现方法的软件模块又可以是硬件部件内的结构。

[138] 上述实施例阐明的系统、装置、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机。具体的，计算机例如可以为个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任何设备的组合。

[139] 为了描述的方便，描述以上装置时以功能分为各种单元分别描述。当然，在实施本说明书时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

[140] 本领域内的技术人员应明白，本说明书的实施例可提供为方法、系统、或计算机程序产品。因此，本说明书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，本说明书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。

[141] 本说明书是参照根据本说明书一个或多个实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[142] 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。

[143] 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。

[144] 在一个典型的配置中，计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[145] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

[146] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体(transitory media)，如调制的数据信号和载波。

[147] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[148] 本说明书可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本说明书的一个或多个实施例，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

[149] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于系统实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[150] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

[151] 以上所述仅为本说明书的一个或多个实施例而已，并不用于限制本说明书。对于本领域技术人员来说，本说明书的一个或多个实施例可以有各种更改和变化。凡在本说明书的一个或多个实施例的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本说明书的权利要求范围之内。

权利要求书

1、一种业务授权的方法，设备的系统中至少包括第一安全环境以及第二安全环境，第一执行单元在所述第一安全环境中运行，第二执行单元在所述第二安全环境中运行，所述方法包括:

获取待验证信息，并将所述待验证信息发送给所述第一执行单元进行验证;

接收所述第一执行单元返回的通过验签私钥对验证结果进行签名得到的签名信息;

将所述签名信息发送给所述第二执行单元，以使所述第二执行单元通过所述验签私钥对应的验签公钥，对所述签名信息进行验证，并在确定所述签名信息验证通过后，根据所述验证结果进行业务授权。

2、如权利要求 1 所述的方法，所述第一安全环境包括：可信执行环境 TEE；所述第二安全环境包括：安全元件 SE 提供的执行环境。

3、如权利要求 1 或 2 所述的方法，所述待验证信息包括：待验证生物特征信息。

4、如权利要求 1 或 2 所述的方法，接收所述第一执行单元返回的通过验签私钥对验证结果进行签名得到的签名信息之前，所述方法还包括:

获取所述第二执行单元发送的动态参数，所述动态参数包括：随机数、时间信息中的至少一种;

将所述动态参数发送给所述第一执行单元，使所述第一执行单元通过所述验签私钥对所述验证结果和所述动态参数进行签名。

5、一种业务授权的方法，设备的系统中至少包括第一安全环境以及第二安全环境，第一执行单元在所述第一安全环境中运行，第二执行单元在所述第二安全环境中运行，所述方法包括:

所述第一执行单元接收业务应用发送的待验证信息;

对所述待验证信息进行验证，并将得到的验证结果通过保存的验签私钥进行签名，得到签名信息;

将所述签名信息通过所述业务应用发送给所述第二执行单元，以使所述第二执行单元通过所述验签私钥对应的验签公钥，对所述签名信息进行验证，并在所述签名信息验证通过后，根据所述验证结果进行业务授权。

6、如权利要求 5 所述的方法，所述业务应用在所述第一安全环境中运行。

7、如权利要求 5 所述的方法，将得到的验证结果通过保存的验签私钥进行签名，得到签名信息之前，所述方法还包括:

接收所述第二执行单元通过所述业务应用发送的动态参数。

8、如权利要求 7 所述的方法，将得到的验证结果通过保存的验签私钥进行签名，得到签名信息，具体包括:

将所述验证结果以及所述动态参数通过所述验签私钥进行签名，得到签名信息。

9、如权利要求 5 或 8 所述的方法，在接收业务应用发送的待验证信息之前，所述方法还包括:

从所述第一执行单元对应的第一管理服务器，获取所述验签私钥。

10、如权利要求 9 所述的方法，将所述签名信息通过业务应用发送给所述第二执行单元之前，所述方法还包括:

从所述第一管理服务器获取所述验签公钥的公钥证书，所述公钥证书是所述第一管理服务器从证书授权 CA 中心获取到的，所述公钥证书是所述 CA 中心根据保存的 CA 私钥对所述验签公钥进行认证后得到的。

11、如权利要求 10 所述的方法，将所述签名信息通过业务应用发送给所述第二执行单元，具体包括:

将所述公钥证书以及所述签名信息通过所述业务应用发送给所述第二执行单元，以使所述第二执行单元通过从所述 CA 中心获取到的 CA 公钥，对所述公钥证书进行验证，并在确定所述公钥证书验证通过后，通过从所述公钥证书中解析出的验签公钥，对所述签名信息进行验证。

12、一种业务授权的方法，设备的系统中至少包括第一安全环境以及第二安全环境，第一执行单元在所述第一安全环境中运行，第二执行单元在所述第二安全环境中运行，所述方法包括:

所述第二执行单元获取所述第一执行单元通过业务应用发送的签名信息，所述签名信息是所述第一执行单元通过验签私钥对验证结果进行签名后得到的，所述验证结果是所述第一执行单元对所述业务应用发送的待验证信息进行验证后得到的;

通过所述验签私钥对应的验签公钥，对所述签名信息进行验证，并在确定所述签名信息通过验证后，根据从所述签名信息中解析出的所述验证结果进行业务授权。

13、如权利要求 12 所述的方法，所述验签公钥是所述第二执行单元通过所述第二执行单元对应的第二管理服务器，从所述第一执行单元对应的第一管理服务器获取到的。

14、如权利要求 12 所述的方法，通过所述验签私钥对应的验签公钥，对所述签名信息进行验证之前，所述方法还包括:

通过所述第二执行单元对应的第二管理服务器，从证书授权 CA 中心获取 CA 公钥。

15、如权利要求 14 所述的方法，通过所述验签私钥对应的验签公钥，对所述签名信息进行验证，并在确定所述签名信息通过验证后，根据从所述签名信息中解析出的所述验证结果进行业务授权，具体包括:

通过所述 CA 公钥，对从所述业务应用发送的公钥证书进行验证，所述公钥证书是所述 CA 中心根据所述 CA 公钥对应的 CA 私钥对所述验签公钥进行认证后得到的，所述公钥证书是所述业务应用从所述第一执行单元获取到的，所述公钥证书是所述第一执行单元通过所述第一执行单元对应的第一管理服务器从所述 CA 中心获取到的;

当确定所述公钥证书通过验证后，通过从所述公钥证书中解析出的验签公钥，对所述签名信息进行验证，并在确定所述签名信息通过验证后，根据从所述签名信息中解析出的所述验证结果进行业务授权。

16、如权利要 15 所述的方法，获取所述第一执行单元通过业务应用发送的签名信息之前，所述方法还包括:

发送动态参数至所述业务应用，以使所述第一执行单元通过所述验签私钥，对所述验证结果以及从所述业务应用获取到的所述动态参数进行签名，得到签名信息。

17、如权利要求 16 所述的方法，通过所述验签私钥对应的验签公钥，对所述签名信息进行验证，并在确定所述签名信息通过验证后，根据从所述签名信息中解析出的所述验证结果进行业务授权，具体包括:

通过所述 CA 公钥，对所述公钥证书进行验证;

当确定所述公钥证书通过验证后，通过从所述公钥证书中解析出的验签公钥，对所述签名信息进行验证;

当确定所述签名信息通过验证后，对从所述签名信息中解析出的动态参数进行验证，并在确定所述动态参数通过验证后，根据从所述签名信息中解析出的所述验证结果进行业务授权。

18、一种业务授权的装置，包含所述装置的设备的系统中至少包括第一安全环境以及第二安全环境，第一执行单元在所述第一安全环境中运行，第二执行单元在所述第二安全环境中运行，所述装置包括:

获取模块，获取待验证信息，并将所述待验证信息发送给所述第一执行单元进行验证;

接收模块，接收所述第一执行单元返回的通过验签私钥对验证结果进行签名得到的签名信息;

发送模块，将所述签名信息发送给所述第二执行单元，以使所述第二执行单元通过

所述验签私钥对应的验签公钥，对所述签名信息进行验证，并在确定所述签名信息验证通过后，根据所述验证结果进行业务授权。

19、如权利要求 18 所述的装置，所述第一安全环境包括：可信执行环境 TEE；所述第二安全环境包括：安全元件 SE 提供的执行环境。

20、如权利要求 18 或 19 所述的装置，所述待验证信息包括：待验证生物特征信息。

21、如权利要求 18 或 19 所述的装置，所述获取模块，获取所述第二执行单元发送的动态参数，所述动态参数包括：随机数、时间信息中的至少一种；将所述动态参数发送给所述第一执行单元，使所述第一执行单元通过所述验签私钥对所述验证结果和所述动态参数进行签名。

22、一种业务授权的装置，设备的系统中至少包括第一安全环境以及第二安全环境，所述装置在所述第一安全环境中运行，第二执行单元在所述第二安全环境中运行，所述装置包括：

接收模块，接收业务应用发送的待验证信息；

验证模块，对所述待验证信息进行验证，并将得到的验证结果通过保存的验签私钥进行签名，得到签名信息；

发送模块，将所述签名信息通过所述业务应用发送给所述第二执行单元，以使所述第二执行单元通过所述验签私钥对应的验签公钥，对所述签名信息进行验证，并在所述签名信息验证通过后，根据所述验证结果进行业务授权。

23、如权利要求 22 所述的装置，所述业务应用在所述第一安全环境中运行。

24、如权利要求 22 所述的装置，所述接收模块，接收所述第二执行单元通过所述业务应用发送的动态参数。

25、如权利要求 24 所述的装置，所述验证模块，将所述验证结果以及所述动态参数通过所述验签私钥进行签名，得到签名信息。

26、如权利要求 22 或 25 所述的装置，所述装置还包括：

获取模块，从所述装置对应的第一管理服务器，获取所述验签私钥。

27、如权利要求 26 所述的装置，所述获取模块，从所述第一管理服务器获取所述验签公钥的公钥证书，所述公钥证书是所述第一管理服务器从证书授权 CA 中心获取到的，所述公钥证书是所述 CA 中心根据保存的 CA 私钥对所述验签公钥进行认证后得到的。

28、如权利要求 27 所述的装置，所述发送模块，将所述公钥证书以及所述签名信息通过所述业务应用发送给所述第二执行单元，以使所述第二执行单元通过从所述 CA

中心获取到的 CA 公钥，对所述公钥证书进行验证，并在确定所述公钥证书验证通过后，通过从所述公钥证书中解析出的验签公钥，对所述签名信息进行验证。

29、一种业务授权的装置，设备的系统中至少包括第一安全环境以及第二安全环境，第一执行单元在所述第一安全环境中运行，所述装置在所述第二安全环境中运行，所述装置包括：

获取模块，获取所述第一执行单元通过业务应用发送的签名信息，所述签名信息是所述第一执行单元通过验签私钥对验证结果进行签名后得到的，所述验证结果是所述第一执行单元对所述业务应用发送的待验证信息进行验证后得到的；

验证模块，通过所述验签私钥对应的验签公钥，对所述签名信息进行验证，并在确定所述签名信息通过验证后，根据从所述签名信息中解析出的所述验证结果进行业务授权。

30、如权利要求 29 所述的装置，所述验签公钥是所述装置通过所述装置对应的第二管理服务器，从所述第一执行单元对应的第一管理服务器获取到的。

31、如权利要求 29 所述的装置，所述获取模块，通过所述装置对应的第二管理服务器，从证书授权 CA 中心获取 CA 公钥。

32、如权利要求 31 所述的装置，所述验证模块，通过所述 CA 公钥，对从所述业务应用发送的公钥证书进行验证，所述公钥证书是所述 CA 中心根据所述 CA 公钥对应的 CA 私钥对所述验签公钥进行认证后得到的，所述公钥证书是所述业务应用从所述第一执行单元获取到的，所述公钥证书是所述第一执行单元通过所述第一执行单元对应的第一管理服务器从所述 CA 中心获取到的；当确定所述公钥证书通过验证后，通过从所述公钥证书中解析出的验签公钥，对所述签名信息进行验证，并在确定所述签名信息通过验证后，根据从所述签名信息中解析出的所述验证结果进行业务授权。

33、如权利要求 32 所述的装置，所述装置还包括：

发送模块，发送动态参数至所述业务应用，以使所述第一执行单元通过所述验签私钥，对所述验证结果以及从所述业务应用获取到的所述动态参数进行签名，得到签名信息。

34、如权利要求 33 所述的装置，所述验证模块，通过所述 CA 公钥，对所述公钥证书进行验证；当确定所述公钥证书通过验证后，通过从所述公钥证书中解析出的验签公钥，对所述签名信息进行验证；当确定所述签名信息通过验证后，对从所述签名信息中解析出的动态参数进行验证，并在确定所述动态参数通过验证后，根据从所述签名信息中解析出的所述验证结果进行业务授权。

35、一种业务授权的设备，包括一个或多个存储器以及处理器，所述存储器存储程序，并且被配置成由所述一个或多个处理器执行以下步骤：

获取待验证信息，并将所述待验证信息发送给第一执行单元进行验证，其中，所述第一执行单元在所述设备的系统包括的第一安全环境中运行；

接收所述第一执行单元返回的通过验签私钥对验证结果进行签名得到的签名信息；

将所述签名信息发送给第二执行单元，以使所述第二执行单元通过所述验签私钥对应的验签公钥，对所述签名信息进行验证，并在确定所述签名信息验证通过后，根据所述验证结果进行业务授权，其中，所述第二执行单元在所述设备的系统包括的第二安全环境中运行。

36、一种业务授权的设备，包括一个或多个存储器以及处理器，所述存储器存储程序，并且被配置成由所述一个或多个处理器执行以下步骤：

第一执行单元接收业务应用发送的待验证信息，其中，所述第一执行单元在所述设备的系统包括的第一安全环境中运行；

对所述待验证信息进行验证，并将得到的验证结果通过保存的验签私钥进行签名，得到签名信息；

将所述签名信息通过所述业务应用发送给第二执行单元，以使所述第二执行单元通过所述验签私钥对应的验签公钥，对所述签名信息进行验证，并在所述签名信息验证通过后，根据所述验证结果进行业务授权，其中，所述第二执行单元在所述设备的系统包括的第二安全环境中运行。

37、一种业务授权的设备，包括一个或多个存储器以及处理器，所述存储器存储程序，并且被配置成由所述一个或多个处理器执行以下步骤：

第二执行单元获取第一执行单元通过业务应用发送的签名信息，所述签名信息是所述第一执行单元通过验签私钥对验证结果进行签名后得到的，所述验证结果是所述第一执行单元对所述业务应用发送的待验证信息进行验证后得到的，其中，所述第一执行单元在所述设备的系统包括的第一安全环境中运行，所述第二执行单元在所述设备的系统包括的第二安全环境中运行；

通过所述验签私钥对应的验签公钥，对所述签名信息进行验证，并在确定所述签名信息通过验证后，根据从所述签名信息中解析出的所述验证结果进行业务授权。

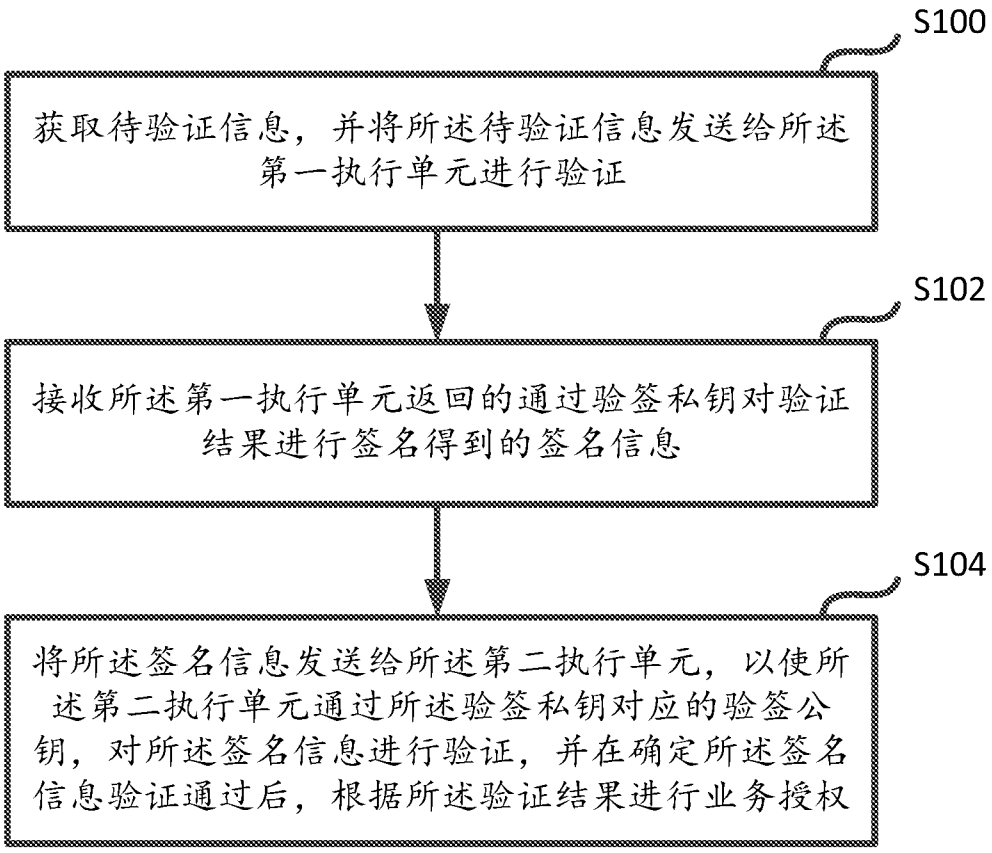

S100
获取待验证信息，并将所述待验证信息发送给所述第一执行单元进行验证
S102
接收所述第一执行单元返回的通过验签私钥对验证结果进行签名得到的签名信息
S104
将所述签名信息发送给所述第二执行单元，以使所述第二执行单元通过所述验签私钥对应的验签公钥，对所述签名信息进行验证，并在确定所述签名信息验证通过后，根据所述验证结果进行业务授权

图 1

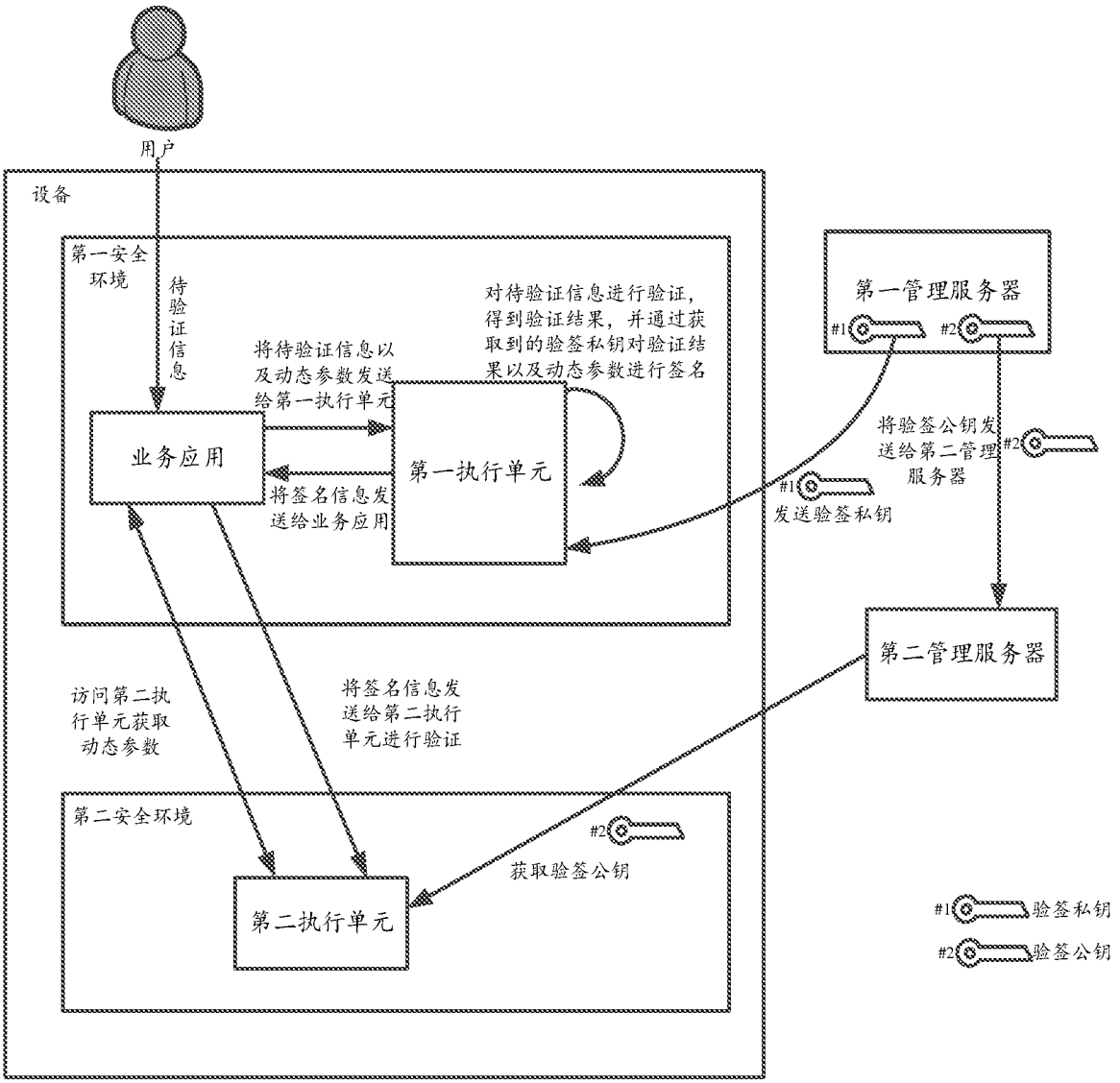

用户
设备
第一安全环境
待验证信息
业务应用
将待验证信息以及动态参数发送给第一执行单元
第一执行单元
对待验证信息进行验证，得到验证结果，并通过获取到的验签私钥对验证结果以及动态参数进行签名
将签名信息发送给业务应用
第一管理服务器
#1
#2
将验签公钥发送给第二管理服务器
#2
#1
发送验签私钥
第二管理服务器
访问第二执行单元获取动态参数
将签名信息发送给第二执行单元进行验证
第二安全环境
#2
获取验签公钥
第二执行单元
#1 验签私钥
#2 验签公钥

图 2

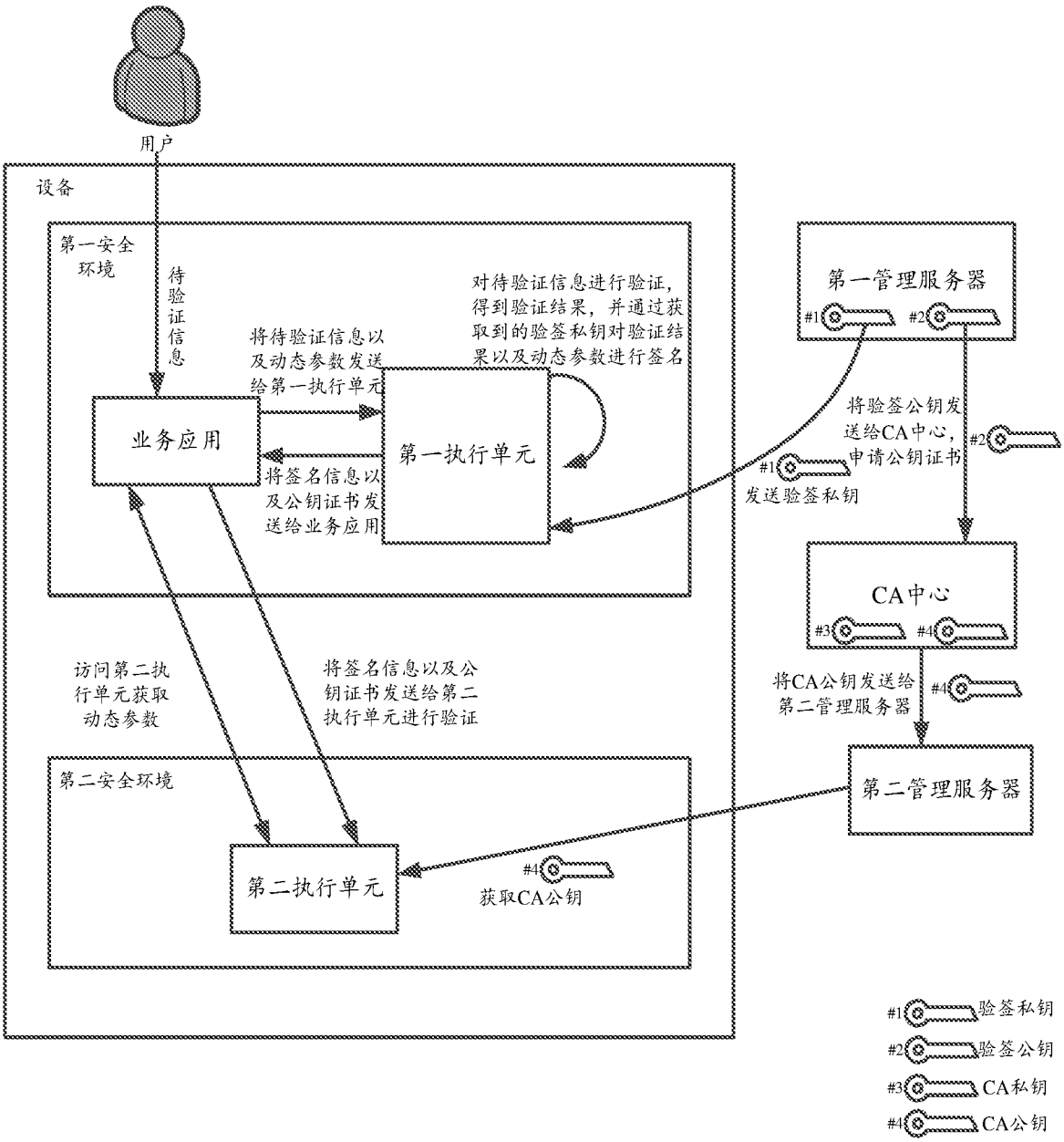

用户
设备
第一安全环境
待验证信息
将待验证信息以及动态参数发送给第一执行单元
对待验证信息进行验证，得到验证结果，并通过获取到的验签私钥对验证结果以及动态参数进行签名
业务应用
第一执行单元
将签名信息以及公钥证书发送给业务应用
第一管理服务器
#1
#2
将验签公钥发送给CA中心，申请公钥证书
#2
#1
发送验签私钥
CA中心
#3
#4
将CA公钥发送给第二管理服务器
#4
第二管理服务器
访问第二执行单元获取动态参数
将签名信息以及公钥证书发送给第二执行单元进行验证
第二安全环境
第二执行单元
#4
获取CA公钥
#1 验签私钥
#2 验签公钥
#3 CA私钥
#4 CA公钥

图 3

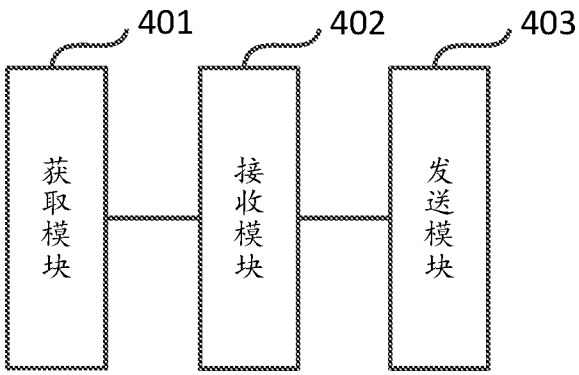

401
402
403
获取模块
接收模块
发送模块

图 4

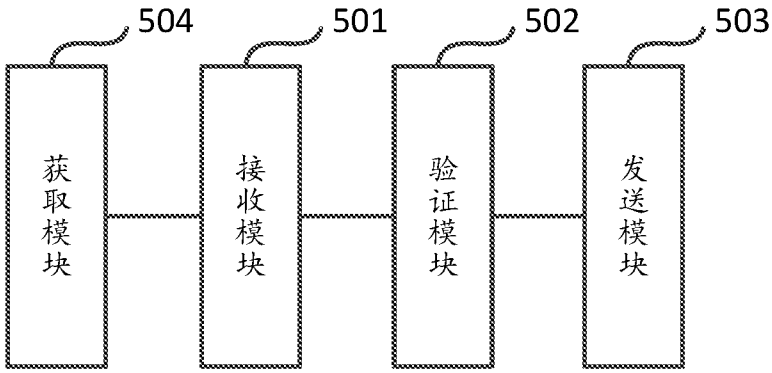


图 5

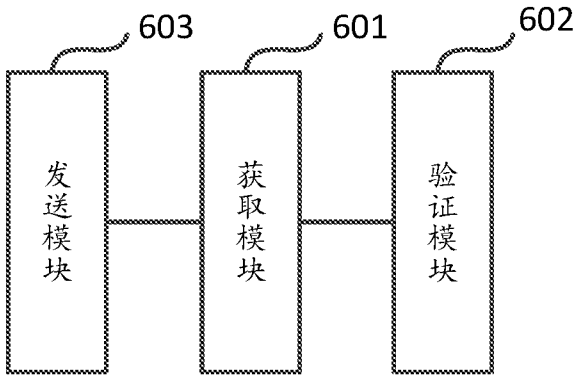


图 6

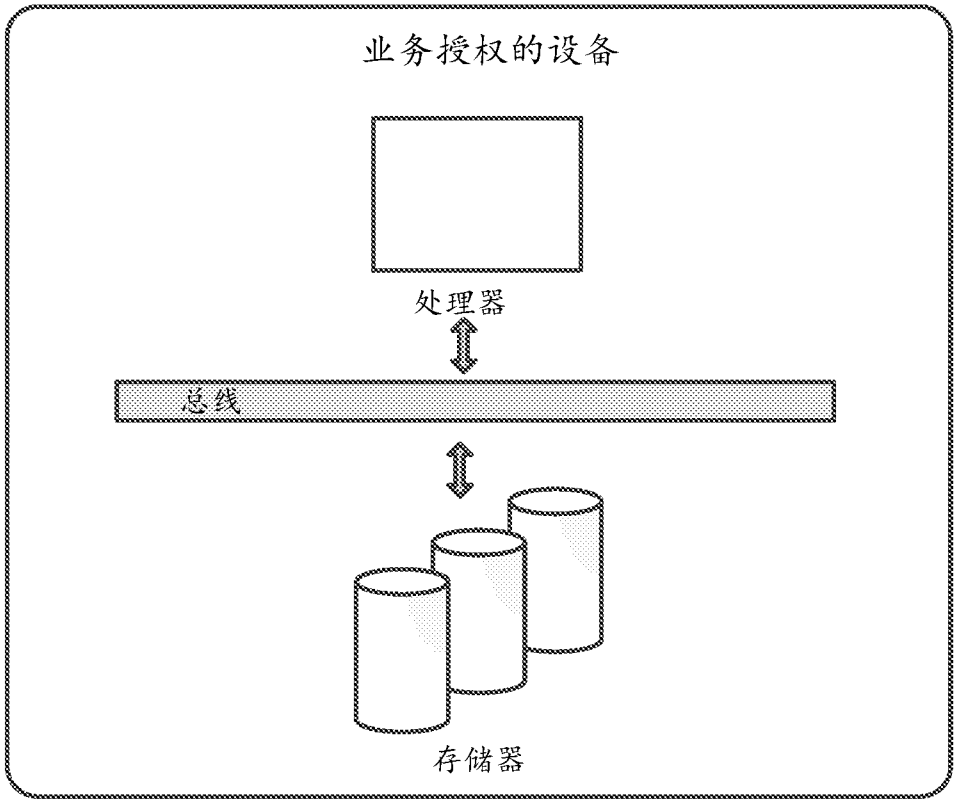


图 7

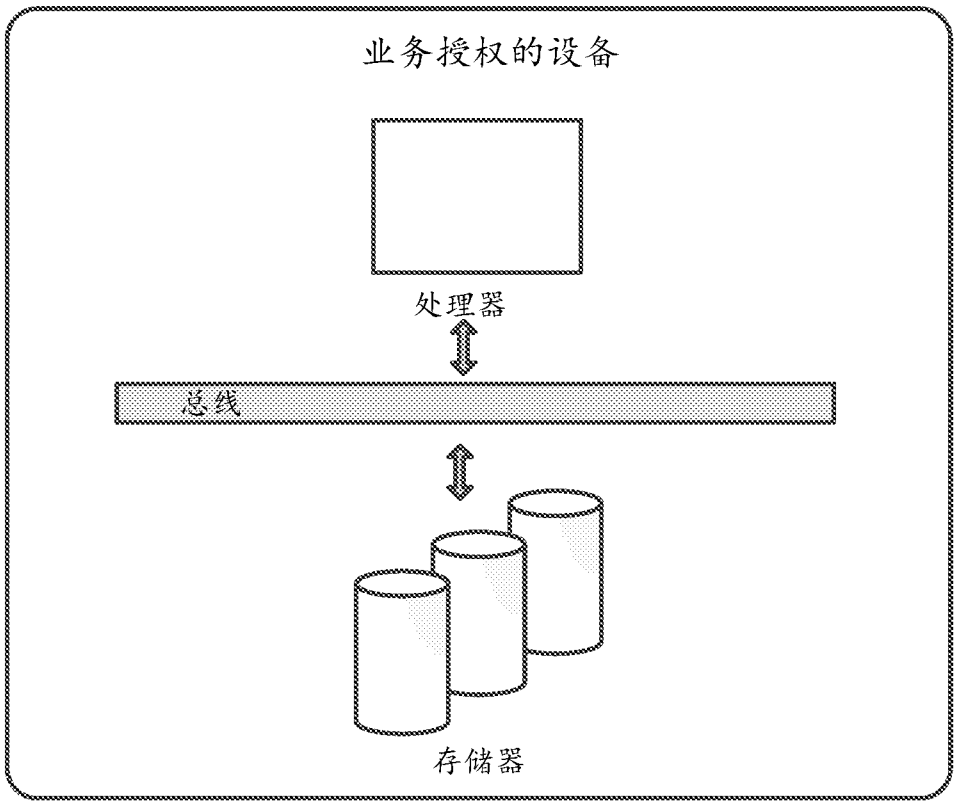


图 8

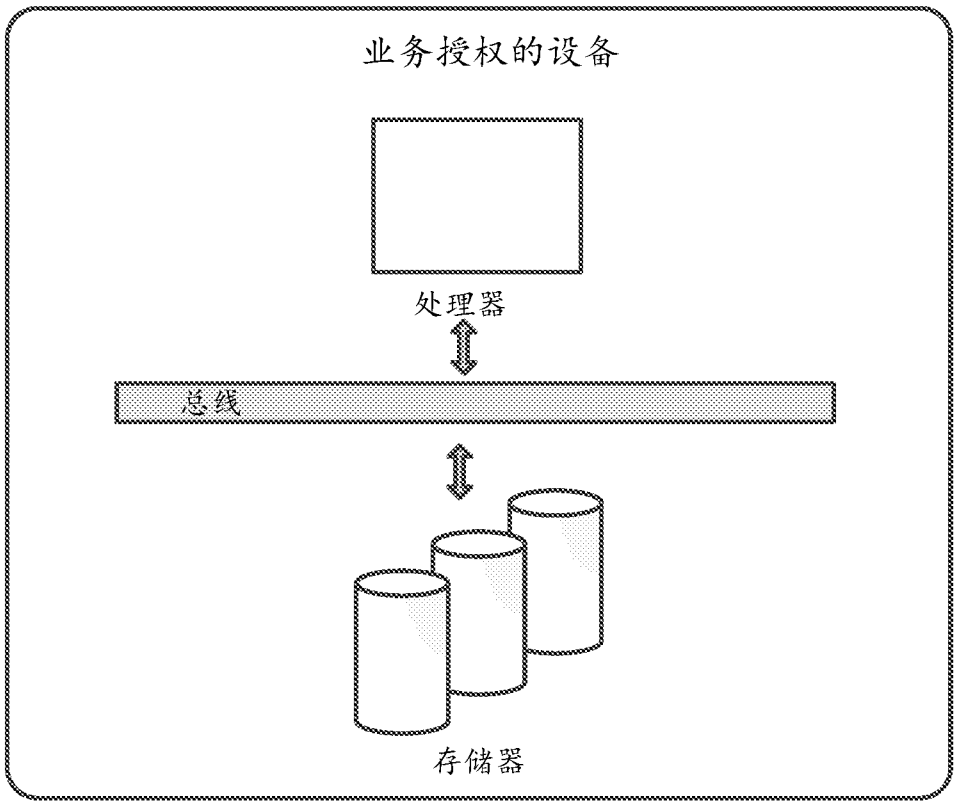


图 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/107569

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i

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)

H04L H04W H04B

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)

WPI, EPODOC, CNPAT, CNKI: 验证, TEE, SE, 可信执行环境, 安全元件, 私钥, 公钥, 签名, 授权, 时间, validate, trusted execution environment, secure element, private key, public key, signature, authoriz+, time

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 106850201 A (JINAN EASYSEC INFORMATION TECHNOLOGY CO., LTD.) 13 June 2017 (2017-06-13) description, paragraphs [0081]-[0087] and [0110]	1-37
X	CN 105490997 A (ALIBABA GROUP HOLDING LIMITED) 13 April 2016 (2016-04-13) description, paragraphs [0064]-[0092]	1-37
X	CN 106878280 A (ALIBABA GROUP HOLDING LIMITED) 20 June 2017 (2017-06-20) claims 1-5	1-37
PX	CN 108055132 A (ALIBABA GROUP HOLDING LIMITED) 18 May 2018 (2018-05-18) claims 1-37	1-37
A	WO 2016192774 A1 (HUAWEI TECHNOLOGIES CO., LTD.) 08 December 2016 (2016-12-08) entire document	1-37

☐ 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
19 November 2018	**07 January 2019**

Name and mailing address of the ISA/CN	Authorized officer
State Intellectual Property Office of the P. R. China **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/107569

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 106850201 A	13 June 2017	None	
CN 105490997 A	13 April 2016	US 2017222813 A1	03 August 2017
		WO 2016054990 A1	14 April 2016
		JP 2017531951 A	26 October 2017
		EP 3206329 A1	16 August 2017
		KR 20170066607 A	14 June 2017
		SG 11201702933 A1	29 June 2017
CN 106878280 A	20 June 2017	None	
CN 108055132 A	18 May 2018	None	
WO 2016192774 A1	08 December 2016	CN 107636672 A	26 January 2018
		EP 3298529 A1	28 March 2018

国际检索报告

国际申请号
PCT/CN2018/107569

A. 主题的分类

H04L 9/32(2006.01)i

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)

H04L H04W H04B

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））

WPI，EPODOC，CNPAT，CNKI：验证，TEE，SE，可信执行环境，安全元件，私钥，公钥，签名，授权，时间，validate，trusted execution environment，secure element，private key，public key，signature，autho-riz+，time

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 106850201 A (济南晟安信息技术有限公司) 2017年 6月 13日 (2017-06-13) 说明书第[0081]-[0087]、[0110]段	1-37
X	CN 105490997 A (阿里巴巴集团控股有限公司) 2016年 4月 13日 (2016-04-13) 说明书第[0064]-[0092]段	1-37
X	CN 106878280 A (阿里巴巴集团控股有限公司) 2017年 6月 20日 (2017-06-20) 权利要求1-5	1-37
PX	CN 108055132 A (阿里巴巴集团控股有限公司) 2018年 5月 18日 (2018-05-18) 权利要求1-37	1-37
A	WO 2016192774 A1 (HUAWEI TECHNOLOGIES CO., LTD.) 2016年 12月 8日 (2016-12-08) 全文	1-37

☐ 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
2018年 11月 19日	2019年 1月 7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 王欣 电话号码 86-(10)-53961617

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/107569

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	106850201	A	2017年 6月 13日	无			
CN	105490997	A	2016年 4月 13日	US	2017222813	A1	2017年 8月 3日
				WO	2016054990	A1	2016年 4月 14日
				JP	2017531951	A	2017年 10月 26日
				EP	3206329	A1	2017年 8月 16日
				KR	20170066607	A	2017年 6月 14日
				SG	11201702933	A1	2017年 6月 29日
CN	106878280	A	2017年 6月 20日	无			
CN	108055132	A	2018年 5月 18日	无			
WO	2016192774	A1	2016年 12月 8日	CN	107636672	A	2018年 1月 26日
				EP	3298529	A1	2018年 3月 28日