# (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 8 月 10 日 (10.08.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/133485 A1

(51) 国际专利分类号:
*H04L 9/08* (2006.01)

(21) 国际申请号: PCT/CN2017/071832

(22) 国际申请日: 2017 年 1 月 20 日 (20.01.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610072683.0 2016 年 2 月 2 日 (02.02.2016) CN



(71) 申请人: **阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED)** [—/CN]; 英属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: **刘敦俊 (LIU, Dunjun)**; 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)。 **董侃 (DONG, Kan)**; 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: **北京三友知识产权代理有限公司 (BEIJING SANYOU INTELLECTUAL PROPERTY AGENCY LTD.)**; 中国北京市金融街 35 号国际企业大厦 A 座 16 层, Beijing 100033 (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, JP, KE, KG, KH, KN, KP, KR, KW, 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,


[见续页]

(54) **Title**: METHOD OF ESTABLISHING COMMUNICATION BETWEEN APPARATUSES, DEVICE, AND SYSTEM

(54) **发明名称** : 一种建立设备间通信的方法、装置和系统

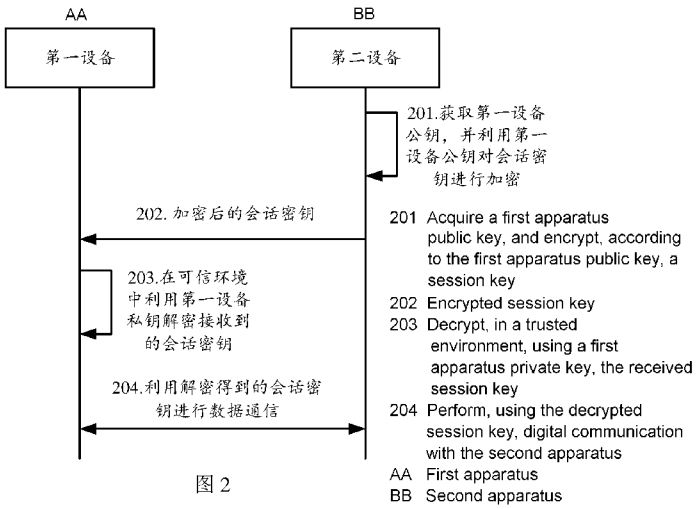



图 2


(57) **Abstract**: The present invention provides a method of establishing communication between apparatuses, device, and system. The method comprises: a second apparatus acquires a first apparatus public key, and encrypts, according to the first apparatus public key, a session key; the second apparatus transmits to the first apparatus the encrypted session key; the first apparatus decrypts, in a trusted environment, using a first apparatus private key, the received session key; and the first apparatus performs, using the decrypted session key, digital communication with the second apparatus. In the invention, the private key of the apparatus is used and the decryption of the session key is performed in a trusted environment, thereby preventing interception of the key and the session key owing to an OS security hole, and increasing security of communication between apparatuses.

(57) **摘要**: 本发明提供了一种建立设备间通信的方法、装置和系统，第二设备获取第一设备公钥，并利用第一设备公钥对会话密钥进行加密；第二设备将加密后的会话密钥发送给第一设备；第一设备在可信环境中利用第一设备私钥解密接收到的会话密钥；第一设备利用解密得到的会话密钥与第二设备之间进行数据通信。在本发明中，设备的私钥和对会话密钥的解密都在可信环境中执行，从而避免了因 OS 漏洞而引起密钥和会话密钥被截取，提高了设备间通信的安全性。


WO 2017/133485 A1

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))。

# 一种建立设备间通信的方法、装置和系统

本申请要求2016年02月02日递交的申请号为201610072683.0、发明名称为“一种建立设备间通信的方法、装置和系统”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

本发明涉及计算机应用技术领域，特别涉及一种建立设备间通信的方法、装置和系统。

## 背景技术

为了增强设备间通信的安全性，目前市面上存在一些加密通信，例如HTTPS（Hyper Text Transfer Protocol over Secure Socket Layer，基于安全的超文本传输协议）。HTTPS中，服务端与客户端之间通过预先约定的加密算法传递会话密钥，但由于客户端对会话密钥的处理过程均在通常的OS（Operating System，操作系统）中进行，所以会话密钥极易被截取，因此其安全等级会随着OS漏洞爆出而大打折扣，无法满足诸如金融等背景应用的安全需求。

## 发明内容

有鉴于此，本发明提供了一种建立设备间通信的方法、装置和设备，以便于提高设备间通信的安全性。

具体技术方案如下：

本发明提供了一种建立设备间通信的方法，该方法包括：

第一设备接收第二设备发送的加密后的会话密钥；

在可信环境中利用第一设备私钥解密所述加密后的会话密钥，并利用解密得到的会话密钥与所述第二设备进行数据通信。

根据本发明一优选实施方式，在所述第一设备接收第二设备发送的加密后的会话密钥之前，还包括：

所述第一设备将第一设备的标识信息发送给第二设备，以便所述第二设备确定与所述第一设备的标识信息对应的第一设备公钥，并向所述第一设备发送利用所述第一设备公钥加密后的会话密钥。

根据本发明一优选实施方式，所述第一设备的标识信息在所述可信环境中存储。

根据本发明一优选实施方式，所述第一设备的标识信息预先由标识服务设备分配和维护；

所述第一设备的标识信息对应的第一设备公钥预先由标识服务设备分配和维护，并供所述第二设备获取，且所述第一设备私钥预先写入所述第一设备的可信环境中。

根据本发明一优选实施方式，所述第一设备为客户端设备，所述第二设备为服务端设备。

根据本发明一优选实施方式，在所述第一设备接收第二设备发送的加密后的会话密钥之前，还包括：

所述第一设备发送第一设备公钥给所述第二设备，以便所述第二设备利用所述第一设备公钥加密会话密钥后返回给所述第一设备。

根据本发明一优选实施方式，所述第一设备公钥和第一设备私钥由标识服务设备生成并提供给所述第一设备，且所述第一设备私钥预先写入所述第一设备的可信环境中。

根据本发明一优选实施方式，所述第一设备和所述第二设备均为客户端设备。

根据本发明一优选实施方式，所述可信环境包括：

可信芯片，或者，

利用虚拟化机制隔离出的安全环境。

本发明还提供了一种建立设备间通信的方法，该方法包括：

第二设备获取第一设备公钥；

利用第一设备公钥对会话密钥进行加密后发送给第一设备；

利用所述会话密钥与所述第一设备进行数据通信。

根据本发明一优选实施方式，所述第二设备获取第一设备公钥包括：

所述第二设备接收所述第一设备的标识信息；

从标识服务设备获取所述第一设备的标识信息对应的第一设备公钥。

根据本发明一优选实施方式，该方法还包括：

若所述第二设备接收到所述标识服务设备发送的所述第一设备的标识信息不合法的响应，或者不存在所述第一设备的标识信息对应的第一设备公钥的响应，则向所述第一设备返回通信建立失败的响应。

根据本发明一优选实施方式，所述第一设备为客户端设备，所述第二设备为服务端设备。

根据本发明一优选实施方式，所述第二设备获取第一设备公钥包括：

所述第二设备接收所述第一设备发送的第一设备公钥。

根据本发明一优选实施方式，在所述利用第一设备公钥对会话密钥进行加密后发送给第一设备之前，还包括：

所述第二设备分配随机的会话密钥。

根据本发明一优选实施方式，所述第二设备在可信环境中执行所述分配随机的会话密钥以及对会话密钥进行加密的步骤。

本发明还提供了一种建立设备间通信的方法，该方法包括：

标识服务设备接收第二设备发送的第一设备的标识信息；

向所述第二设备返回所述第一设备的标识信息对应的第一设备公钥，以便所述第二设备利用第一设备公钥对会话密钥进行加密后发送给第一设备，所述会话密钥用于第一设备与第二设备之间的数据通信。

根据本发明一优选实施方式，该方法还包括：

所述标识服务设备维护预先为所述第一设备分配的标识信息，并维护预先针对所述第一设备生成的第一设备公钥和第一设备私钥。

根据本发明一优选实施方式，该方法还包括：

所述第一设备私钥预先写入所述第一设备的可信环境。

根据本发明一优选实施方式，该方法还包括：

若所述标识服务设备确定所述第一设备的标识信息不合法，则向所述第二设备返回所述第一设备的标识信息不合法的响应；或者，

若所述标识服务设备确定不存在所述第一设备的标识信息对应的第一设备公钥，则向所述第二设备返回不存在所述第一设备的标识信息的响应。

本发明还提供了一种建立设备间通信的装置，设置于第一设备，该装置包括：

密钥接收单元，用于接收第二设备发送的加密后的会话密钥；

可信执行单元，用于在可信环境中利用第一设备私钥解密所述加密后的会话密钥，并利用解密得到的会话密钥，进行所述第一设备与所述第二设备之间的数据通信。

根据本发明一优选实施方式，该装置还包括：

标识发送单元，用于将所述第一设备的标识信息发送给第二设备，以便所述第二设备确定与所述第一设备的标识信息对应的第一设备公钥，并向所述第一设备发送利用所述第一设备公钥加密后的会话密钥。

根据本发明一优选实施方式，可信执行单元请求并获取所述第一设备的标识信息；

所述可信执行单元，还用于应所述标识发送单元的请求，从安全存储区域获取所述第一设备的标识信息并返回给所述标识发送单元。

根据本发明一优选实施方式，所述第一设备的标识信息预先由标识服务设备分配和维护；

所述第一设备的标识信息对应的第一设备公钥预先由标识服务设备生成和维护，并供所述第二设备获取，且所述第一设备私钥预先写入所述第一设备的安全存储区域。

根据本发明一优选实施方式，所述第一设备为客户端设备，所述第二设备为服务端设备。

根据本发明一优选实施方式，该装置还包括：

公钥发送单元，用于发送第一设备公钥给所述第二设备，以便所述第二设备利用所述第一设备公钥加密会话密钥后返回给所述第一设备。

根据本发明一优选实施方式，所述第一设备公钥和第一设备私钥由标识服务设备生成并提供给所述第一设备，且所述第一设备私钥预先写入所述第一设备的安全存储区域中。

根据本发明一优选实施方式，所述第一设备和所述第二设备均为客户端设备。

根据本发明一优选实施方式，所述可信执行单元包括：

可信芯片，或者，

利用虚拟化机制隔离出的安全模块。

本发明还提供了一种建立设备间通信的装置，设置于第二设备，该装置包括：

公钥获取单元，用于获取第一设备公钥；

密钥处理单元，用于利用第一设备公钥对会话密钥进行加密后发送给第一设备；

数据通信单元，用于利用所述会话密钥，进行所述第二设备与所述第一设备之间的数据通信。

根据本发明一优选实施方式，所述公钥获取单元，具体用于：

接收所述第一设备的标识信息；

从标识服务设备获取所述第一设备的标识信息对应的第一设备公钥。

根据本发明一优选实施方式，该装置还包括：

响应发送单元，用于若所述公钥获取单元接收到所述标识服务设备发送的所述第一设备的标识信息不合法的响应，或者不存在所述第一设备的标识信息对应的第一设备公

钥的响应，则向所述第一设备返回通信建立失败的响应。

根据本发明一优选实施方式，所述第一设备为客户端设备，所述第二设备为服务端设备。

根据本发明一优选实施方式，所述公钥获取单元，具体用于接收所述第一设备发送的第一设备公钥。

根据本发明一优选实施方式，该装置还包括：

密钥生成单元，用于分配随机的会话密钥。

根据本发明一优选实施方式，所述密钥生成单元和所述密钥处理单元设置于可信环境中。

本发明还提供了一种建立设备间通信的装置，设置于标识服务设备，该装置包括：

接收单元，用于接收第二设备发送的第一设备的标识信息；

确定单元，用于确定所述第一设备的标识信息对应的第一设备公钥；

发送单元，用于向所述第二设备返回所述第一设备公钥，以便所述第二设备利用第一设备公钥对会话密钥进行加密后发送给第一设备，所述会话密钥用于第一设备与第二设备之间的数据通信。

根据本发明一优选实施方式，该装置还包括：

信息维护单元，用于维护预先为所述第一设备分配的标识信息，并维护预先针对所述第一设备生成的第一设备公钥和第一设备私钥。

根据本发明一优选实施方式，所述发送单元，还用于若所述确定单元确定所述第一设备的标识信息不合法，则向所述第二设备返回所述第一设备的标识信息不合法的响应；或者，

若所述确定单元确定不存在所述第一设备的标识信息对应的第一设备公钥，则向所述第二设备返回不存在所述第一设备的标识信息的响应。

本发明还提供了一种建立设备间通信的系统，该系统包括第一设备和第二设备。

根据本发明一优选实施方式，该系统还包括标识服务设备。

由以上技术方案可以看出，在本发明中，设备的私钥和对会话密钥的解密都在可信环境中执行，从而避免了因 OS 漏洞而引起密钥和会话密钥被截取，提高了设备间通信的安全性。

## 附图说明

图 1 为本发明所基于的系统架构图；

图 2 为本发明实施例提供的主要方法流程图；

图 3 为本发明实施例提供的客户端设备与服务端设备建立通信的方法流程图；

图 4 为本发明实施例提供的客户端设备之间建立通信的方法流程图；

图 5 为本发明实施例提供的与图 3 对应的具体实现方法流程图；

图 6 为本发明实施例提供的与图 4 对应的具体实现方法流程图；

图 7 为本发明实施例提供的第一种装置结构图；

图 8 为本发明实施例提供的第二种装置结构图；

图 9 为本发明实施例提供的第三种装置结构图；

图 10 为本发明实施例提供的一种应用场景示意图；

图 11 为本发明实施例提供的另一种应用场景示意图。

具体实施方式

为了使本发明的目的、技术方案和优点更加清楚，下面结合附图和具体实施例对本发明进行详细描述。

在本发明实施例中使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本发明。在本发明实施例和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。

应当理解，本文中使用的术语“和/或”仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系。

取决于语境，如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”或“响应于检测”。类似地，取决于语境，短语“如果确定”或“如果检测（陈述的条件或事件）”可以被解释成为“当确定时”或“响应于确定”或“当检测（陈述的条件或事件）时”或“响应于检测（陈述的条件或事件）”。

本发明所基于的系统架构如图 1 中所示，包括第一设备和第二设备。其中，第一设备可以为客户端设备，第二设备可以为服务端设备，即建立客户端设备和服务端设备之间的安全通信。或者，第一设备和第二设备均为客户端设备，即建立客户端设备之间的安全通信。

客户端设备可以包括但不限于：智能移动终端、智能家电设备、网络设备、可穿戴式设备、智能医疗设备、PC（个人计算机）等。其中智能移动设备可以包括诸如手机、平板电脑、笔记本电脑、PDA（个人数字助理）等。智能家电设备可以包括诸如智能电视、智能空调、智能热水器、智能冰箱、智能空气净化器等等。网络设备可以包括诸如交换机、无线 AP、服务器等。可穿戴式设备可以包括诸如智能手表、智能眼镜、智能手环等等。智能医疗设备可以包括诸如智能体温计、智能血压仪、智能血糖仪等等。服务端设备可以为服务器、交换机、路由器等。

这些客户端设备和服务端设备在架构上都可以包含一些基本组件，如总线、处理系统、存储系统、一个或多个输入/输出系统、和通信接口等。总线可以包括一个或多个导线，用来实现服务器或终端设备各组件之间的通信。处理系统包括各类型的用来执行指令、处理进程或线程的处理器或微处理器。存储系统可以包括存储动态信息的随机访问存储器（RAM）等动态存储器，和存储静态信息的只读存储器（ROM）等静态存储器，以及包括磁或光学记录介质与相应驱动的大容量存储器。输入系统供用户输入信息到服务端设备或客户端设备，如按键、键盘、鼠标、触摸式屏幕、手写笔、声音识别系统、或生物测定系统等。输出系统包括用来输出信息的显示器、打印机、扬声器等。通信接口用来使服务端设备或客户端设备与其它系统或系统进行通信。通信接口之间可通过有线连接、无线连接、或光连接连接到网络中。

图 2 为本发明实施例提供的主要方法流程图，如图 2 中所示，该方法可以主要包括以下步骤：

在 201 中，第二设备获取第一设备公钥，并利用第一设备公钥对会话密钥进行加密。

第二设备可以从服务器端获取第一设备公钥，例如第二设备可以利用第一设备的标识信息从标识服务设备获取第一设备公钥，这种情况可以适用于第二设备为服务端设备时。第二设备也可以从第一设备获取第一设备公钥，这种情况可以适用于第一设备为客户端设备时。具体将在后续实施例中详细描述。

其中会话密钥可以由第二设备生成或分配，但为了保证安全性，需要会话密钥具有一定的随机性，该会话密钥用于后续第一设备和第二设备之间的数据通信。

在 202 中，第二设备将加密后的会话密钥发送给第一设备。

在 203 中，第一设备在可信环境中利用第一设备私钥解密接收到的会话密钥。

第一设备私钥预先存储于第一设备的可信环境中，并在可信环境中执行对会话密钥的解密，从而保证会话密钥的安全性。在本发明实施例中，该可信环境可以是利用诸如

ARM TrustZone 或 Secure Element 或 TI M-Shield 等机制在硬件上隔离出的安全区域，也可以是利用虚拟化机制隔离出一个独立的安全环境。可信环境保证了存入的第一设备私钥不可篡改和擦除，以及会话密钥解密的私密性。

在 204 中，第一设备利用解密得到的会话密钥与第二设备之间进行数据通信。

后续第一设备与第二设备之间进行数据通信时，均采用该会话密钥进行数据的加解密。例如第一设备发送数据给第二设备时，采用该会话密钥对数据进行加密后发送给第二设备，第二设备利用该会话密钥对第一设备发送的数据进行解密。第二设备发送数据给第一设备时，也采用该会话密钥对数据进行加密后发送给第一设备，第一设备利用该会话密钥对第二设备发送的数据进行解密。

下面分别以客户端设备与服务端设备建立安全通信、客户端设备设备与客户端设备建立安全通信为例，对本发明提供的方法进行详细描述。

图 3 为本发明实施例提供的客户端设备与服务端设备建立通信的方法流程图，如图 3 中所示，该方法可以具体包括以下步骤：

在 301 中，客户端设备获取自身的 ID 信息。

在本发明实施例中，客户端设备的 ID 信息用于唯一标识客户端设备，可以采用但不限于：IMEI、MAC 地址等等。作为一种优选的实施方式，客户端设备的身份标识可以由标识服务设备分配，并提供给客户端设备，例如在客户端设备的出厂阶段提供给标识写入设备，由标识写入设备将客户端设备的 ID 写入客户端设备。

出于客户端设备 ID 信息安全性的考虑，客户端设备的 ID 信息可以存储于安全环境，例如安全存储区域，从而保证 ID 信息不被篡改。

本步骤可以在客户端设备需要与服务端设备建立通信连接时触发执行，可以由客户端设备触发执行。也可以由服务端设备触发执行，例如客户端设备接收到服务端设备的连接请求时，执行本步骤。

在 302 中，客户端设备将自身的 ID 信息发送给服务端设备。

在 303 中，服务端设备将客户端设备的 ID 信息发送给标识服务设备，以向标识服务设备请求客户端设备公钥。

在本实施例中，服务端设备利用客户端设备的 ID 信息，从标识服务设备获取客户端设备公钥。

在 304 中，标识服务设备确定客户端设备的 ID 信息对应的客户端设备公钥。

在本发明实施例中，标识服务设备可以负责统一维护客户端设备的 ID 信息与客户端

设备公钥之间的对应关系，该对应关系可以预先保存至标识服务设备。

作为一种优选的实施方式，合法客户端设备的 ID 信息可以由标识服务设备分配和维护，并在合法客户端设备的出厂阶段提供给标识写入设备，由标识写入设备写入合法客户端设备的可信环境中。

在本步骤中，标识服务设备可以首先对接收到的客户端设备的 ID 信息进行合法性判断，即判断接收到的客户端设备的 ID 信息是否为本地维护的 ID 信息，如果是，则确定该客户端设备的 ID 信息合法，可以继续确定该 ID 信息对应的客户端设备公钥；否则，确定该客户端设备的 ID 信息不合法，可以向服务端设备返回该客户端设备的 ID 信息不合法的响应，服务端设备确定通信建立失败，并可以向客户端设备返回通信建立失败的响应。

客户端设备公钥和客户端设备私钥是成对的密钥，可以由标识服务设备生成，并将客户端私钥提供给客户端设备维护，即写入客户端设备的可信环境（可以在客户端设备的出厂阶段执行，也可以在其他能够保证信息安全的阶段执行），标识服务设备在本地维护客户端设备的 ID 信息与客户端公钥之间的对应关系。

如果标识服务设备能够确定出客户端设备的 ID 信息对应的客户端设备公钥，则执行 305；如果本地没有维护该客户端设备的 ID 信息对应的客户端设备公钥，则可以向服务端设备返回不存在客户端设备公钥的响应，由服务端设备确定通信建立失败，并可以向客户端设备返回通信建立失败的响应。

在 305 中，标识服务设备将客户端设备公钥返回给服务端设备。

在 306 中，服务端设备生成会话密钥，并利用客户端设备公钥加密会话密钥。

会话密钥可以是依据一定算法产生的随机密钥，可以是对称式的密钥，也可以是非对称式的密钥。鉴于会话密钥的产生和利用已经是较为成熟的技术，在此不做详述，本步骤的重点在于利用客户端设备公钥加密会话密钥，以保证会话密钥能够安全私密地传递给客户端设备。

除了实时生成会话密钥的方式之外，也可以预先生成并维护一个会话密钥池，在本步骤中服务端设备从会话密钥池中随机分配一个会话密钥。通常会话密钥具有一定的有效期，当超过有效期之后，会话密钥失效，失效的会话密钥可以重新被分配给一个新的通信连接。后续实施例中会话密钥的分配方式也可以采用以上两种中的一种，后续不再赘述。

在 307 中，服务端设备将加密后的会话密钥发送给客户端设备。

由于服务端设备通常是单一业务类型的服务器，并不具备其他应用，因此服务端设备本身具有一定的安全级别，也可以看做服务端设备本身就是一个可信环境。

在 308 中，客户端设备在可信环境中获取客户端设备私钥，并利用客户端设备私钥解密会话密钥。

由于会话密钥是利用客户端设备公钥加密的，因此只有客户端私钥才能够对其解密，在本发明实施例中，客户端设备私钥只能从可信环境中获取，因此保证了该会话密钥仅能够由客户端设备解密得到，并且由于对会话密钥的解密也在可信环境中执行，因此保证了会话密钥不被其他设备获取和篡改。

在 309 中，客户端设备利用解密得到的会话密钥与服务端设备之间进行数据通信。

后续客户端设备与服务端设备之间的数据通信都采用会话密钥进行加密和解密。如果会话密钥是对称式密钥，那么客户端设备和服务端设备采用相同的密钥进行数据的加密和解密。如果会话密钥是非对称密钥，那么客户端设备和服务端设备采用密钥对中的一个进行数据的加密和解密。

客户端设备在利用会话密钥与服务端设备之间进行数据通信时，在可信环境下对数据进行加密和解密。

图 4 为本发明实施例提供的客户端设备之间建立通信的方法流程图，在本实施例中以设备 A 和设备 B 为例进行描述，如图 4 中所示，该方法可以具体包括以下步骤：

在 401 中，设备 A 发送设备 A 的公钥信息给设备 B。

本步骤可以在设备 A 需要与设备 B 建立通信连接时触发执行，即可以由设备 A 触发执行。也可以由设备 B 触发执行，例如设备 A 接收到设备 B 的连接请求时，执行本步骤。

与图 3 所示实施例类似地，本实施例中，设备 A 的公钥和私钥可以由标识服务设备预先生成并提供给设备 A，其中设备 A 的私钥预先写入设备 A 的可信环境中。

在 402 中，设备 B 在可信环境中生成会话密钥，并利用设备 A 的公钥信息对会话密钥进行加密。

同样，会话密钥可以是依据一定算法产生的随机密钥，可以是对称式的密钥，也可以是非对称式的密钥。

在 403 中，设备 B 将加密后的会话密钥发送给设备 A。

在 404 中，设备 A 在可信环境中利用设备 A 的私钥对会话密钥进行解密。

由于会话密钥是利用设备 A 公钥加密的，因此只有设备 A 的私钥才能够对其解密，在本发明实施例中，设备 A 的私钥只能从可信环境中获取，因此保证了该会话密钥仅能

够由设备 A 解密得到，并且由于对会话密钥的解密也在可信环境中执行，因此保证了会话密钥不被其他设备获取和篡改。

在 405 中，设备 A 利用解密得到的会话密钥与设备 B 之间进行数据通信。

后续设备 A 与设备 B 之间的数据通信都采用会话密钥进行加密和解密。如果会话密钥是对称式密钥，那么设备 A 和设备 B 采用相同的密钥进行数据的加密和解密。如果会话密钥是非对称密钥，那么设备 A 和设备 B 采用密钥对中的一个进行数据的加密和解密。

设备 A 在利用会话密钥与设备 B 之间进行数据通信时，在可信环境下对数据进行加密和解密。

下面通过两个实施例对图 3 和图 4 中客户端设备的具体实现方式进行描述。

图 5 为本发明实施例提供的与图 3 对应的具体实现方法流程图，客户端设备被细化为客户端、安全服务模块和可信环境模块。如图 5 中所示，该方法可以具体包括以下步骤：

在 501a 中，客户端向安全服务模块请求客户端设备的 ID 信息。

在 501b 中，安全服务模块解析该请求后，向可信环境模块请求客户端设备的 ID 信息。

在 501c 中，可信环境模块获取并向安全服务模块返回存储的客户端设备的 ID 信息。

客户端设备的 ID 信息预先存储于安全环境，由可信环境模块负责维护和处理。

在 501d 中，安全服务模块将客户端设备的 ID 信息返回给客户端。

上述步骤 501a~501d 对应于图 3 中的步骤 301。

在 502 中，由客户端将客户端设备的 ID 信息发送给服务端设备。

步骤 503~507 同图 3 中的 303~307。

在 508a 中，客户端接收服务端设备发送的加密后的会话密钥，并提供给安全服务模块。

在 508b 中，安全服务模块请求可信环境模块解密会话密钥。

在 508c 中，可信环境模块获取客户端设备私钥，并利用客户端设备私钥解密会话密钥。

上述步骤 508a~508c 对应于图 3 中的步骤 308。

在 509a 中，可信环境模块利用会话密钥加密数据。

在 509b 中，可信环境模块将加密后的数据发送给安全服务模块。

在 509c 中，安全服务模块将加密后的数据提供给客户端。

在 509d 中，由客户端将加密后的数据发送给服务端设备。

在 509e 中，服务端设备用会话密钥解密数据。

对于服务端设备利用会话密钥加密后的数据发送给客户端后，由客户端经由安全服务模块发送给可信环境模块，由可信环境模块利用会话密钥进行解密。该过程在图 5 中未示出。509a~509e 的过程对应于图 3 中的步骤 309。

图 6 为本发明实施例提供的与图 4 对应的具体实现方法流程图，客户端设备被细化为蓝牙应用和可信环境模块。如图 6 中所示，该方法可以具体包括以下步骤：

在 601 中，设备 A 的蓝牙应用向设备 B 的蓝牙应用发送设备 A 的公钥信息。

在 602a 中，设备 B 的蓝牙应用将设备 A 的公钥发送给设备 B 的可信环境模块。

在 602b 中，设备 B 的可信环境模块生成并存储会话密钥。

在 602c 中，设备 B 的可信环境模块利用设备 A 的公钥加密会话密钥。

602a~602c 的过程对应于图 4 中的步骤 402。

在 603a 中，设备 B 的可信环境模块将加密后的会话密钥发送给设备 B 的蓝牙应用。

在 603b 中，设备 B 的蓝牙应用将加密后的会话密钥发送给设备 A 的蓝牙应用。

在 603c 中，设备 A 的蓝牙应用将加密后的会话密钥发送给设备 A 的可信环境模块。

603a~603c 的过程对应于图 4 中的步骤 403。

在 604 中，设备 A 的可信环境模块利用设备 A 的私钥解密会话密钥。

在 605a 中，设备 A 的可信环境模块利用会话密钥加密数据。

在 605b 中，设备 A 的可信环境模块将加密后的数据发送给设备 A 的蓝牙应用。

在 605c 中，设备 A 的蓝牙应用将加密后的数据通过蓝牙发送给设备 B 的蓝牙应用。

在 605d 中，设备 B 的蓝牙应用将加密后的数据发送给设备 B 的可信环境模块。

在 605e 中，设备 B 的可信环境模块利用会话密钥解密加密后的数据。

后续设备 B 的可信环境模块利用会话密钥将发送给设备 A 的数据进行加密，将加密后的数据通过蓝牙应用发送给设备 A 的蓝牙应用，由设备 A 的蓝牙应用将机密后的数据提供给设备 A 的可信环境模块，设备 A 的可信环境模块利用会话密钥解密数据。该过程在图 6 中未示出。605a~605e 的过程对应于图 4 中的步骤 405。

以上是对本发明所提供方法进行的描述，下面结合实施例对本发明所提供的装置进行详细描述。

图 7 为本发明实施例提供的第一种装置结构图，该装置可以设置于上述实施例中的第一设备中，如图 7 中所示，该装置可以包括：密钥接收单元 01 和可信执行单元 02，

还可以包括：标识发送单元 03。各组成单元的主要功能如下：

密钥接收单元 01 负责接收第二设备发送的加密后的会话密钥。具体可以包括但不限于以下两种方式：

第一种方式：由标识发送单元 03 将第一设备的标识信息发送给第二设备，以便第二设备确定与第一设备的标识信息对应的第一设备公钥，并向第一设备发送利用第一设备公钥加密后的会话密钥。

其中，标识发送单元 03 可以向可信执行单元 02 请求并获取第一设备的标识信息；可信执行单元 02 应标识发送单元 03 的请求，从安全存储区域获取第一设备的标识信息并返回给标识发送单元 03。

第一设备的标识信息可以预先由标识服务设备分配和维护。例如在客户端设备的出厂阶段提供给标识写入设备，由标识写入设备将客户端设备的 ID 写入客户端设备。出于客户端设备 ID 信息安全性的考虑，客户端设备的 ID 信息可以存储于安全环境，例如安全存储区域，从而保证 ID 信息不被篡改。

第一设备的标识信息对应的第一设备公钥也可以预先由标识服务设备生成和维护，并供第二设备获取，且第一设备私钥预先写入第一设备的安全存储区域。

这种实现方式，可以应用于第一设备为客户端设备，第二设备为服务端设备的场景。

第二种方式：由公钥发送单元发送第一设备公钥给第二设备，以便第二设备利用第一设备公钥加密会话密钥后返回给第一设备，这种方式图中未示出。

同样，上述的第一设备公钥和第一设备私钥可以由标识服务设备生成并提供给第一设备，且第一设备私钥预先写入第一设备的安全存储区域中。

这种实现方式，可以应用于第一设备和第二设备均为客户端设备的场景。

可信执行单元 02 负责在可信环境中利用第一设备私钥解密加密后的会话密钥，并利用解密得到的会话密钥，进行第一设备与第二设备之间的数据通信。

其中可信执行单元 02 可以是利用诸如 ARM TrustZone 或 Secure Element 或 TI M-Shield 等机制在硬件上隔离出的安全区域，例如采用可信芯片的形式。也可以是利用虚拟化机制隔离出的安全模块。

图 8 为本发明实施例提供的第二种装置结构图，该装置可以设置于上述的第二设备，如图 8 中所示，该装置可以包括：公钥获取单元 11、密钥处理单元 12 和数据通信单元 13，还可以包括响应发送单元 14 和密钥生成单元 15。各组成单元的主要功能如下：

公钥获取单元 11 负责获取第一设备公钥。具体地，可以采用但不限于以下两种方式：

第一种方式：公钥获取单元 11 接收第一设备的标识信息，从标识服务设备获取第一设备的标识信息对应的第一设备公钥。

若公钥获取单元 11 接收到标识服务设备发送的第一设备的标识信息不合法的响应，或者不存在第一设备的标识信息对应的第一设备公钥的响应，则响应发送单元 14 可以向第一设备返回通信建立失败的响应。

这种情况可以适用于第一设备为客户端设备，第二设备为服务端设备的场景。

第二种方式，公钥获取单元 11 接收第一设备发送的第一设备公钥。

这种情况可以适用于第一设备和第二设备均为客户端设备的场景。

密钥处理单元 12 负责利用第一设备公钥对会话密钥进行加密后发送给第一设备。

数据通信单元 13 负责利用会话密钥，进行第二设备与第一设备之间的数据通信。

上述的会话密钥可以由密钥生成单元 15 负责生成，会话密钥可以是依据一定算法产生的随机密钥，可以是对称式的密钥，也可以是非对称式的密钥。

为了保证会话密钥的安全性，作为一种优选的实施方式，密钥生成单元 15 和密钥处理单元 12 可以设置于可信环境中。

图 9 为本发明实施例提供的第三种装置结构图，该装置可以设置于上述方法实施例中的标识服务设备，如图 9 中所示，该装置可以包括：接收单元 21、确定单元 22 和发送单元 23，还包括信息维护单元 24。各组成单元的主要功能如下：

接收单元 21 负责接收第二设备发送的第一设备的标识信息。

确定单元 22 负责确定第一设备的标识信息对应的第一设备公钥。

发送单元 23 负责向第二设备返回第一设备公钥，以便第二设备利用第一设备公钥对会话密钥进行加密后发送给第一设备，会话密钥用于第一设备与第二设备之间的数据通信。

信息维护单元 24 负责维护预先为第一设备分配的标识信息，并维护预先针对第一设备生成的第一设备公钥和第一设备私钥。其中第一设备的标识信息可以由该标识服务设备分配，并在第一设备的出厂阶段提供给标识写入设备，写入第一设备。第一设备公钥和第一设备私钥也可以由该标识服务设备生成，并在第一设备的出厂阶段提供给标识写入设备，写入第一设备的安全存储区域。

另外，若确定单元 22 确定第一设备的标识信息不合法，则发送单元 23 向第二设备返回第一设备的标识信息不合法的响应。若确定单元 22 确定不存在第一设备的标识信息对应的第一设备公钥，则发送单元 23 可以向第二设备返回不存在第一设备的标识信息的

响应。

下面列举几个具体的应用场景：

第一种应用场景：如图 10 所示，标识服务设备预先针对智能汽车生成智能汽车的 ID 信息，并针对智能汽车生成公钥-私钥对，将智能汽车的 ID 信息和私钥下发给标识写入设备，以便在该智能汽车出厂阶段，由标识写入设备将智能汽车的 ID 信息和私钥写入智能汽车的可信芯片中。

当智能汽车希望通过诸如物联网等与服务器端建立连接，从而享受业务服务器的服务时，诸如从业务服务器获取导航信息、路况信息、控制信息等等时，将该智能汽车的 ID 信息发送给业务服务器，业务服务器将该 ID 信息发送给标识服务设备，由标识服务设备将该智能汽车的 ID 信息对应的公钥发送给业务服务器。业务服务器利用智能汽车的公钥对生成的随机的会话密钥进行加密，将加密后的会话密钥发送给智能汽车。智能汽车接收到该会话密钥后提供给可信芯片，由可信芯片获取智能汽车的私钥后，利用私钥对接收到的加密后的会话密钥进行解密，后续就利用解密后得到的会话密钥与业务服务器进行数据通信。从而保证了智能汽车与业务服务器之间的数据通信安全。

第二种应用场景：如图 11 所示，标识服务设备预先针对智能手表生成智能手表的 ID 信息，并针对智能手表生成公钥-私钥对，将智能手表的 ID 信息和私钥下发给标识写入设备，以便在该智能手表出厂阶段，由标识写入设备将智能手表的 ID 信息和私钥写入智能手表的可信芯片中。

当智能手表要与手机建立连接从而进行数据交互时，将智能手表的公钥发送给手机，手机中的可信芯片利用该智能手表的公钥对生成的会话密钥进行加密后，发送给智能手表。

智能手表接收到加密后的会话密钥后，由可信芯片获取智能手表的私钥，并利用私钥对加密后的会话密钥进行解密。后续利用解密后得到的会话密钥与手机之间进行数据通信，从而保证智能手表与手机之间的数据通信安全。

除了上述应用场景之外，本发明还可以应用于其他应用场景，诸如智能电视与视频服务器之间的安全通信、智能手机与智能家电设备之间的安全通信，等等，在此不再一一穷举。

由以上描述可以看出，本发明提供的方法、装置和系统可以具备以下优点：

1）在本发明中，设备的私钥和对会话密钥的解密都在可信环境中执行，从而避免了因 OS 漏洞而引起密钥和会话密钥被截取，提高了设备间通信的安全性。

2）能够适用于客户端设备之间以及客户端与服务端设备之间等多种应用场景，灵活满足多种应用需求。

3）当进行客户端设备与服务端设备之间的安全通信时，通过标识服务设备对设备标识的合法性以及设备标识与设备公钥之间对应关系的合法性进行把控，更进一步增加了客户端设备与服务端设备之间通信的安全性。

在本发明所提供的几个实施例中，应该理解到，所揭露的系统，装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用硬件加软件功能单元的形式实现。

上述以软件功能单元的形式实现的集成的单元，可以存储在一个计算机可读取存储介质中。上述软件功能单元存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）或处理器（processor）执行本发明各个实施例所述方法的部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（Read-Only Memory，ROM）、随机存取存储器（Random Access Memory，RAM）、磁碟或者光盘等各种可以存储程序代码的介质。

以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明保护的范围之内。

# 权 利 要 求 书

1、一种建立设备间通信的方法，其特征在于，该方法包括：

第一设备接收第二设备发送的加密后的会话密钥；

在可信环境中利用第一设备私钥解密所述加密后的会话密钥，并利用解密得到的会话密钥与所述第二设备进行数据通信。

2、根据权利要求 1 所述的方法，其特征在于，在所述第一设备接收第二设备发送的加密后的会话密钥之前，还包括：

所述第一设备将第一设备的标识信息发送给第二设备，以便所述第二设备确定与所述第一设备的标识信息对应的第一设备公钥，并向所述第一设备发送利用所述第一设备公钥加密后的会话密钥。

3、根据权利要求 2 所述的方法，其特征在于，所述第一设备的标识信息在所述可信环境中存储。

4、根据权利要求 2 所述的方法，其特征在于，所述第一设备的标识信息预先由标识服务设备分配和维护；

所述第一设备的标识信息对应的第一设备公钥预先由标识服务设备分配和维护，并供所述第二设备获取，且所述第一设备私钥预先写入所述第一设备的可信环境中。

5、根据权利要求 2 所述的方法，其特征在于，所述第一设备为客户端设备，所述第二设备为服务端设备。

6、根据权利要求 1 所述的方法，其特征在于，在所述第一设备接收第二设备发送的加密后的会话密钥之前，还包括：

所述第一设备发送第一设备公钥给所述第二设备，以便所述第二设备利用所述第一设备公钥加密会话密钥后返回给所述第一设备。

7、根据权利要求 6 所述的方法，其特征在于，所述第一设备公钥和第一设备私钥由标识服务设备生成并提供给所述第一设备，且所述第一设备私钥预先写入所述第一设备的可信环境中。

8、根据权利要求 6 所述的方法，其特征在于，所述第一设备和所述第二设备均为客户端设备。

9、根据权利要求 1 至 8 任一权项所述的方法，其特征在于，所述可信环境包括：

可信芯片，或者，

利用虚拟化机制隔离出的安全环境。

10、一种建立设备间通信的方法，其特征在于，该方法包括：

第二设备获取第一设备公钥；

利用第一设备公钥对会话密钥进行加密后发送给第一设备；

利用所述会话密钥与所述第一设备进行数据通信。

11、根据权利要求 10 所述的方法，其特征在于，所述第二设备获取第一设备公钥包括：

所述第二设备接收所述第一设备的标识信息；

从标识服务设备获取所述第一设备的标识信息对应的第一设备公钥。

12、根据权利要求 11 所述的方法，其特征在于，该方法还包括：

若所述第二设备接收到所述标识服务设备发送的所述第一设备的标识信息不合法的响应，或者不存在所述第一设备的标识信息对应的第一设备公钥的响应，则向所述第一设备返回通信建立失败的响应。

13、根据权利要求 11 所述的方法，其特征在于，所述第一设备为客户端设备，所述第二设备为服务端设备。

14、根据权利要求 10 所述的方法，其特征在于，所述第二设备获取第一设备公钥包括：

所述第二设备接收所述第一设备发送的第一设备公钥。

15、根据权利要求 10 至 14 任一权项所述的方法，其特征在于，在所述利用第一设备公钥对会话密钥进行加密后发送给第一设备之前，还包括：

所述第二设备分配随机的会话密钥。

16、根据权利要求 15 所述的方法，其特征在于，所述第二设备在可信环境中执行所述分配随机的会话密钥以及对会话密钥进行加密的步骤。

17、一种建立设备间通信的方法，其特征在于，该方法包括：

标识服务设备接收第二设备发送的第一设备的标识信息；

向所述第二设备返回所述第一设备的标识信息对应的第一设备公钥，以便所述第二设备利用第一设备公钥对会话密钥进行加密后发送给第一设备，所述会话密钥用于第一设备与第二设备之间的数据通信。

18、根据权利要求 17 所述的方法，其特征在于，该方法还包括：

所述标识服务设备维护预先为所述第一设备分配的标识信息，并维护预先针对所述第一设备生成的第一设备公钥和第一设备私钥。

19、根据权利要求 18 所述的方法，其特征在于，该方法还包括：

所述第一设备私钥预先写入所述第一设备的可信环境。

20、根据权利要求 17 所述的方法，其特征在于，该方法还包括：

若所述标识服务设备确定所述第一设备的标识信息不合法，则向所述第二设备返回所述第一设备的标识信息不合法的响应；或者，

若所述标识服务设备确定不存在所述第一设备的标识信息对应的第一设备公钥，则向所述第二设备返回不存在所述第一设备的标识信息的响应。

21、一种建立设备间通信的装置，设置于第一设备，其特征在于，该装置包括：

密钥接收单元，用于接收第二设备发送的加密后的会话密钥；

可信执行单元，用于在可信环境中利用第一设备私钥解密所述加密后的会话密钥，并利用解密得到的会话密钥，进行所述第一设备与所述第二设备之间的数据通信。

22、根据权利要求 21 所述的装置，其特征在于，该装置还包括：

标识发送单元，用于将所述第一设备的标识信息发送给第二设备，以便所述第二设备确定与所述第一设备的标识信息对应的第一设备公钥，并向所述第一设备发送利用所述第一设备公钥加密后的会话密钥。

23、根据权利要求 22 所述的装置，其特征在于，所述标识发送单元向所述可信执行单元请求并获取所述第一设备的标识信息；

所述可信执行单元，还用于应所述标识发送单元的请求，从安全存储区域获取所述第一设备的标识信息并返回给所述标识发送单元。

24、根据权利要求 22 所述的装置，其特征在于，所述第一设备的标识信息预先由标识服务设备分配和维护；

所述第一设备的标识信息对应的第一设备公钥预先由标识服务设备生成和维护，并供所述第二设备获取，且所述第一设备私钥预先写入所述第一设备的安全存储区域。

25、根据权利要求 22 所述的装置，其特征在于，所述第一设备为客户端设备，所述第二设备为服务端设备。

26、根据权利要求 21 所述的装置，其特征在于，该装置还包括：

公钥发送单元，用于发送第一设备公钥给所述第二设备，以便所述第二设备利用所述第一设备公钥加密会话密钥后返回给所述第一设备。

27、根据权利要求 26 所述的装置，其特征在于，所述第一设备公钥和第一设备私钥由标识服务设备生成并提供给所述第一设备，且所述第一设备私钥预先写入所述第一

设备的安全存储区域中。

28、根据权利要求 26 所述的装置，其特征在于，所述第一设备和所述第二设备均为客户端设备。

29、根据权利要求 21 至 28 任一权项所述的装置，其特征在于，所述可信执行单元包括：

可信芯片，或者，

利用虚拟化机制隔离出的安全模块。

30、一种建立设备间通信的装置，设置于第二设备，其特征在于，该装置包括：

公钥获取单元，用于获取第一设备公钥；

密钥处理单元，用于利用第一设备公钥对会话密钥进行加密后发送给第一设备；

数据通信单元，用于利用所述会话密钥，进行所述第二设备与所述第一设备之间的数据通信。

31、根据权利要求 30 所述的装置，其特征在于，所述公钥获取单元，具体用于：

接收所述第一设备的标识信息；

从标识服务设备获取所述第一设备的标识信息对应的第一设备公钥。

32、根据权利要求 31 所述的装置，其特征在于，该装置还包括：

响应发送单元，用于若所述公钥获取单元接收到所述标识服务设备发送的所述第一设备的标识信息不合法的响应，或者不存在所述第一设备的标识信息对应的第一设备公钥的响应，则向所述第一设备返回通信建立失败的响应。

33、根据权利要求 31 所述的装置，其特征在于，所述第一设备为客户端设备，所述第二设备为服务端设备。

34、根据权利要求 30 所述的装置，其特征在于，所述公钥获取单元，具体用于接收所述第一设备发送的第一设备公钥。

35、根据权利要求 30 至 34 任一权项所述的装置，其特征在于，该装置还包括：

密钥生成单元，用于分配随机的会话密钥。

36、根据权利要求 35 所述的装置，其特征在于，所述密钥生成单元和所述密钥处理单元设置于可信环境中。

37、一种建立设备间通信的装置，设置于标识服务设备，其特征在于，该装置包括：

接收单元，用于接收第二设备发送的第一设备的标识信息；

确定单元，用于确定所述第一设备的标识信息对应的第一设备公钥；

发送单元，用于向所述第二设备返回所述第一设备公钥，以便所述第二设备利用第一设备公钥对会话密钥进行加密后发送给第一设备，所述会话密钥用于第一设备与第二设备之间的数据通信。

38、根据权利要求 37 所述的装置，其特征在于，该装置还包括：

信息维护单元，用于维护预先为所述第一设备分配的标识信息，并维护预先针对所述第一设备生成的第一设备公钥和第一设备私钥。

39、根据权利要求 37 所述的装置，其特征在于，所述发送单元，还用于若所述确定单元确定所述第一设备的标识信息不合法，则向所述第二设备返回所述第一设备的标识信息不合法的响应；或者，

若所述确定单元确定不存在所述第一设备的标识信息对应的第一设备公钥，则向所述第二设备返回不存在所述第一设备的标识信息的响应。

40、一种建立设备间通信的系统，其特征在于，该系统包括第一设备和第二设备；

所述第一设备包括如权利要求 21 至 28 任一权项所述的装置；

所述第二设备包括如权利要求 30 至 34 任一权项所述的装置。

41、根据权利要求 40 所述的系统，其特征在于，该系统还包括标识服务设备；

所述标识服务设备包括如权利要求 37 至 39 任一权项所述的装置。

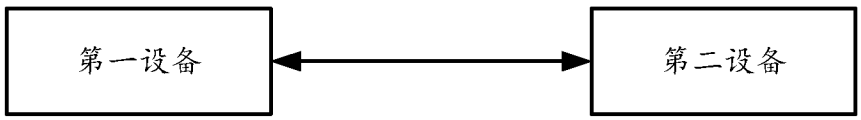

第一设备
第二设备

图 1

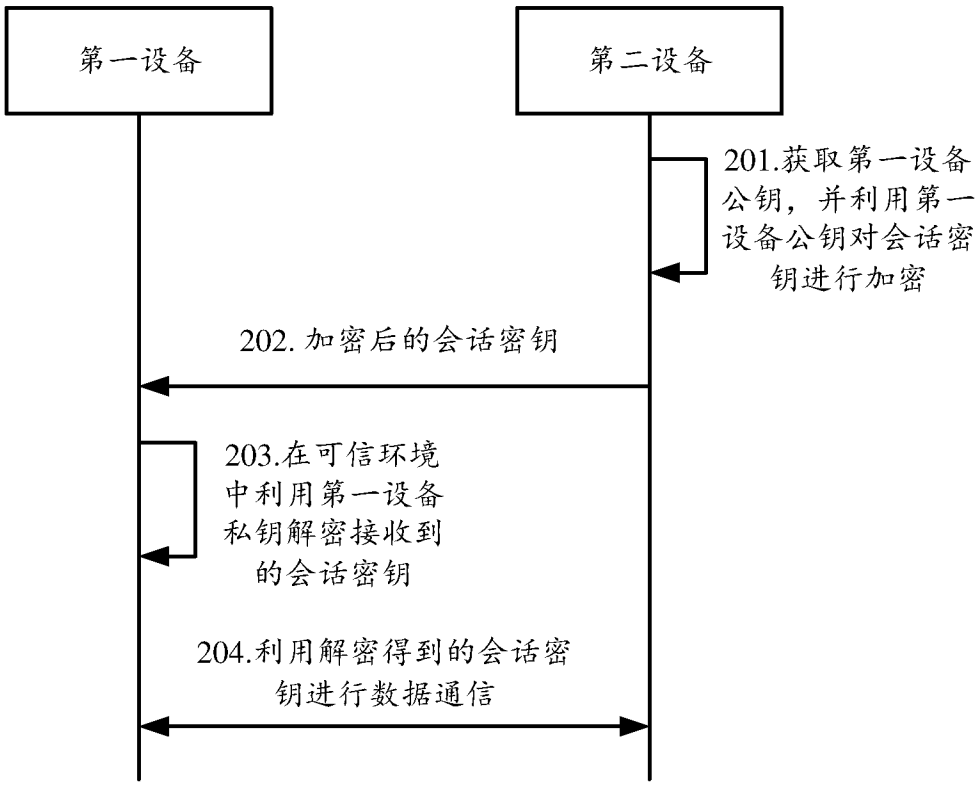

第一设备
第二设备
201.获取第一设备公钥，并利用第一设备公钥对会话密钥进行加密
202. 加密后的会话密钥
203.在可信环境中利用第一设备私钥解密接收到的会话密钥
204.利用解密得到的会话密钥进行数据通信

图 2

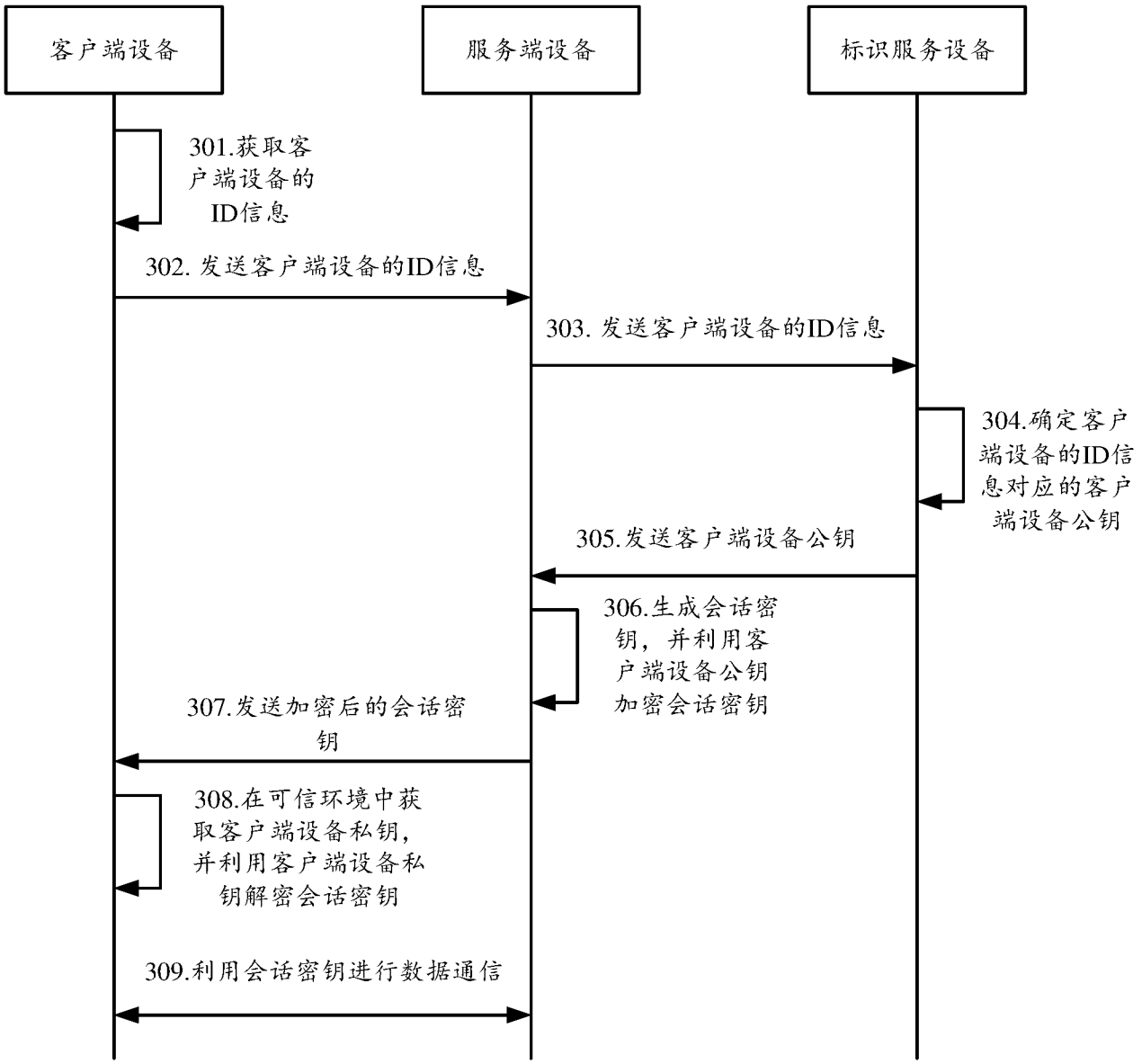

客户端设备
服务端设备
标识服务设备
301.获取客户端设备的ID信息
302. 发送客户端设备的ID信息
303. 发送客户端设备的ID信息
304.确定客户端设备的ID信息对应的客户端设备公钥
305.发送客户端设备公钥
306.生成会话密钥，并利用客户端设备公钥加密会话密钥
307.发送加密后的会话密钥
308.在可信环境中获取客户端设备私钥，并利用客户端设备私钥解密会话密钥
309.利用会话密钥进行数据通信

图 3

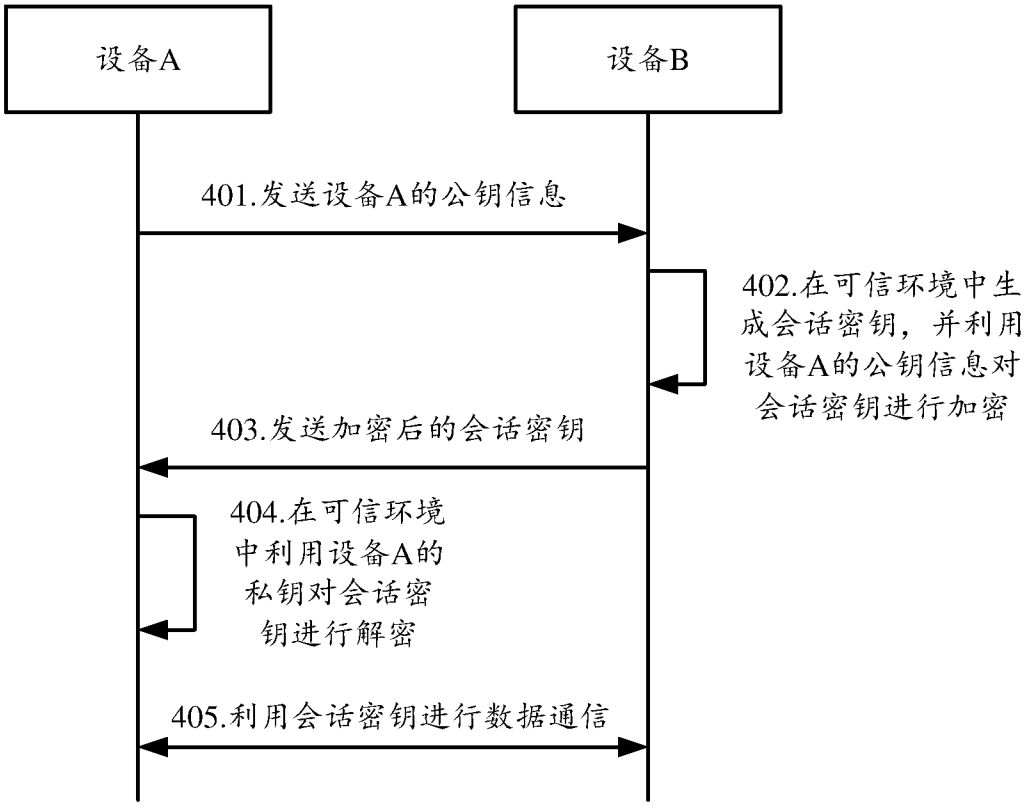

设备A
设备B
401.发送设备A的公钥信息
402.在可信环境中生成会话密钥，并利用设备A的公钥信息对会话密钥进行加密
403.发送加密后的会话密钥
404.在可信环境中利用设备A的私钥对会话密钥进行解密
405.利用会话密钥进行数据通信

图 4

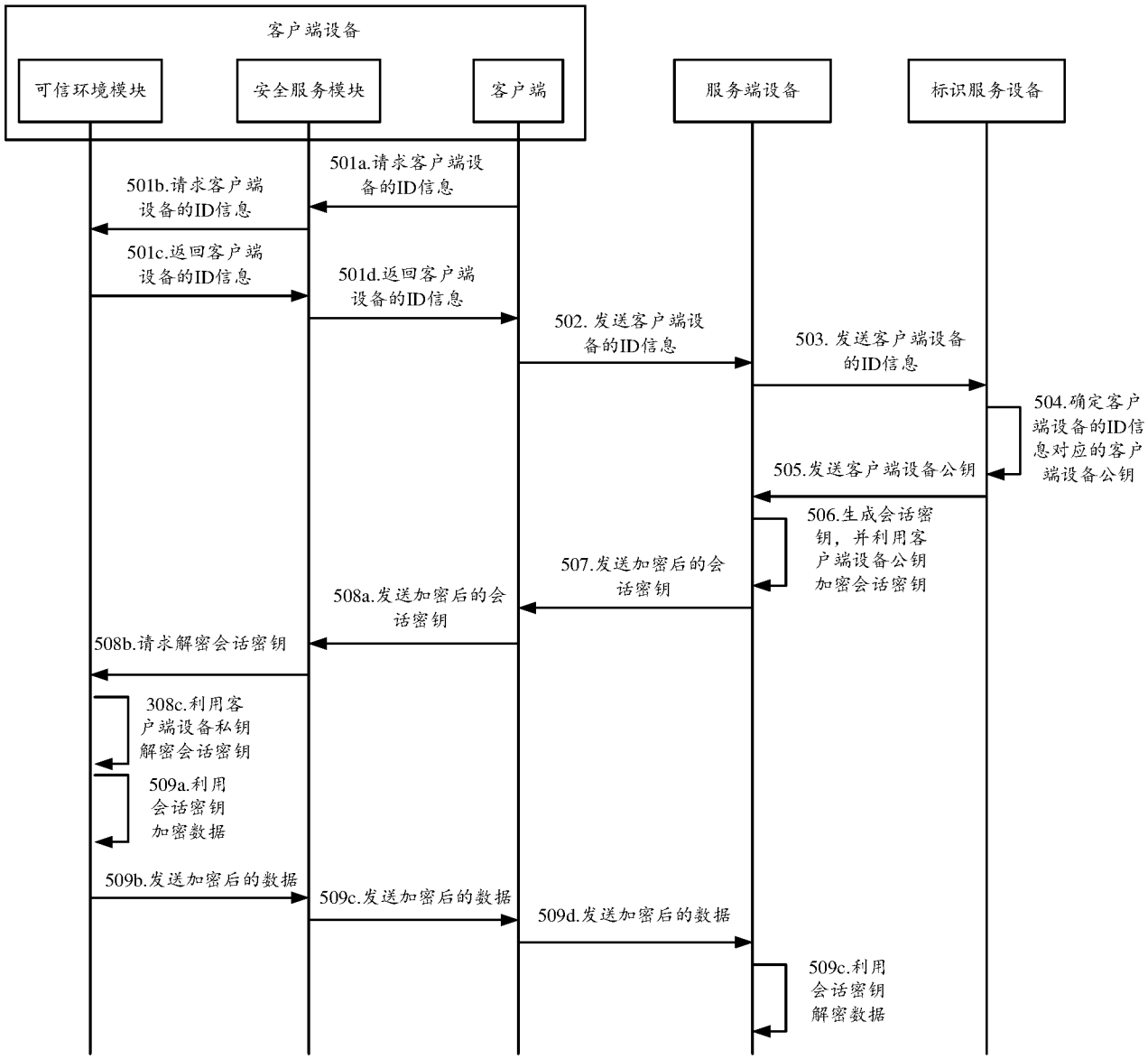

客户端设备
可信环境模块
安全服务模块
客户端
服务端设备
标识服务设备
501a.请求客户端设备的ID信息
501b.请求客户端设备的ID信息
501c.返回客户端设备的ID信息
501d.返回客户端设备的ID信息
502. 发送客户端设备的ID信息
503. 发送客户端设备的ID信息
504.确定客户端设备的ID信息对应的客户端设备公钥
505.发送客户端设备公钥
506.生成会话密钥，并利用客户端设备公钥加密会话密钥
507.发送加密后的会话密钥
508a.发送加密后的会话密钥
508b.请求解密会话密钥
308c.利用客户端设备私钥解密会话密钥
509a.利用会话密钥加密数据
509b.发送加密后的数据
509c.发送加密后的数据
509d.发送加密后的数据
509c.利用会话密钥解密数据

图 5

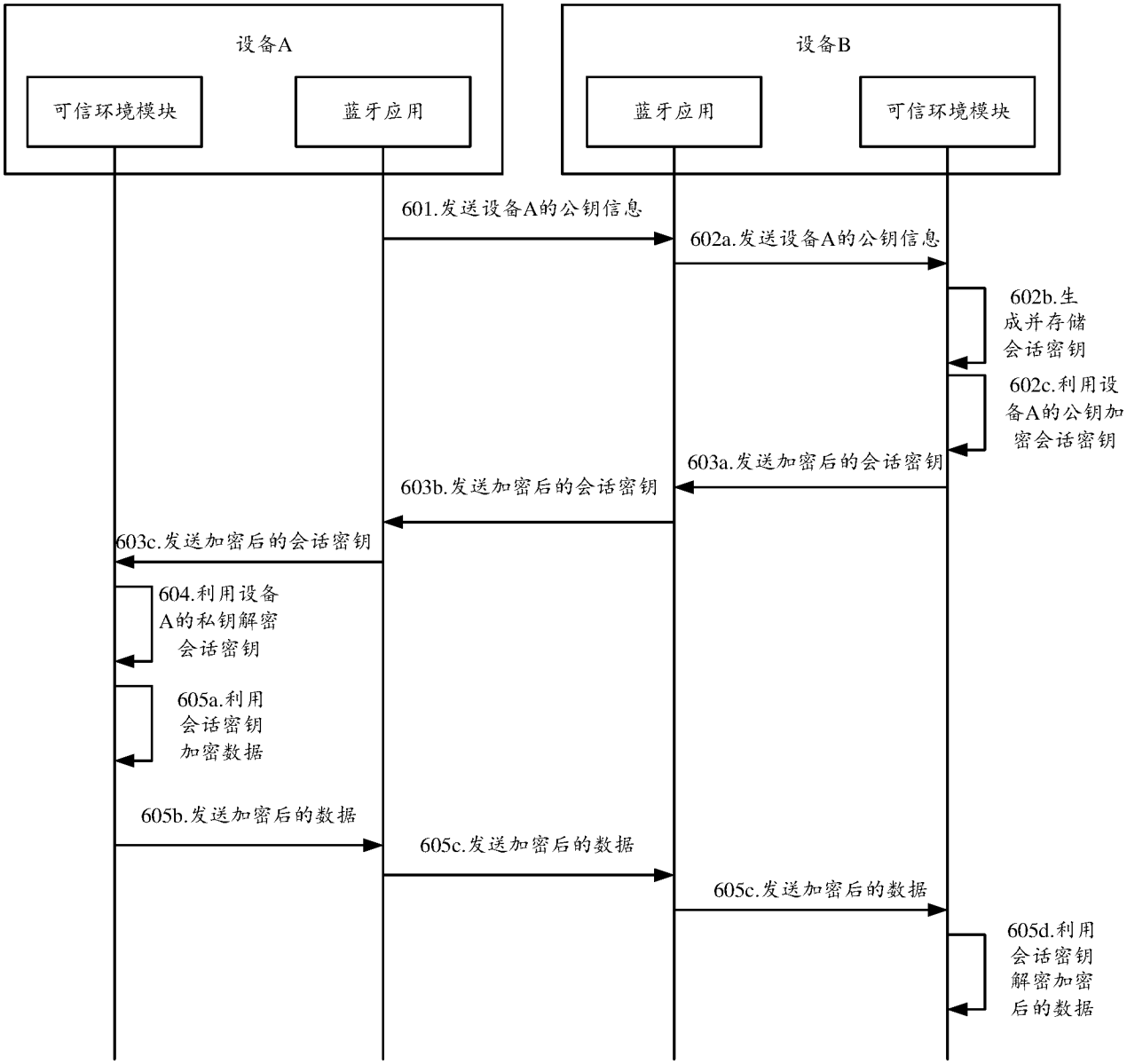

设备A
可信环境模块
蓝牙应用
设备B
蓝牙应用
可信环境模块
601.发送设备A的公钥信息
602a.发送设备A的公钥信息
602b.生成并存储会话密钥
602c.利用设备A的公钥加密会话密钥
603a.发送加密后的会话密钥
603b.发送加密后的会话密钥
603c.发送加密后的会话密钥
604.利用设备A的私钥解密会话密钥
605a.利用会话密钥加密数据
605b.发送加密后的数据
605c.发送加密后的数据
605c.发送加密后的数据
605d.利用会话密钥解密加密后的数据

图 6

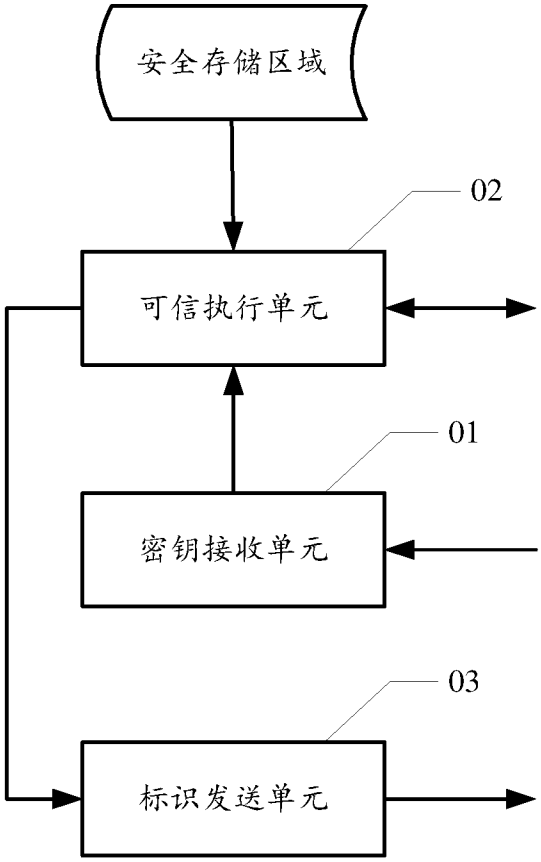



图 7

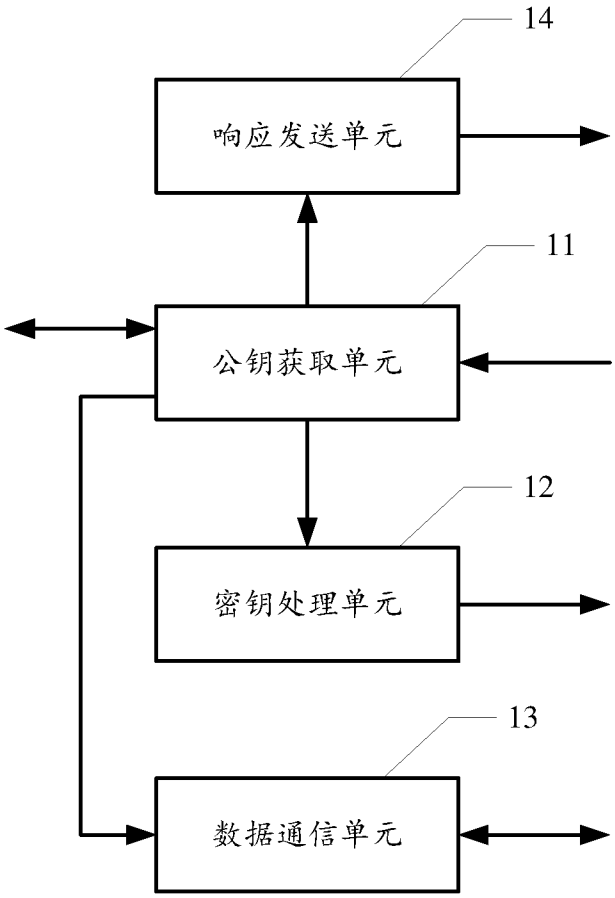

14
响应发送单元
11
公钥获取单元
12
密钥处理单元
13
数据通信单元

图 8

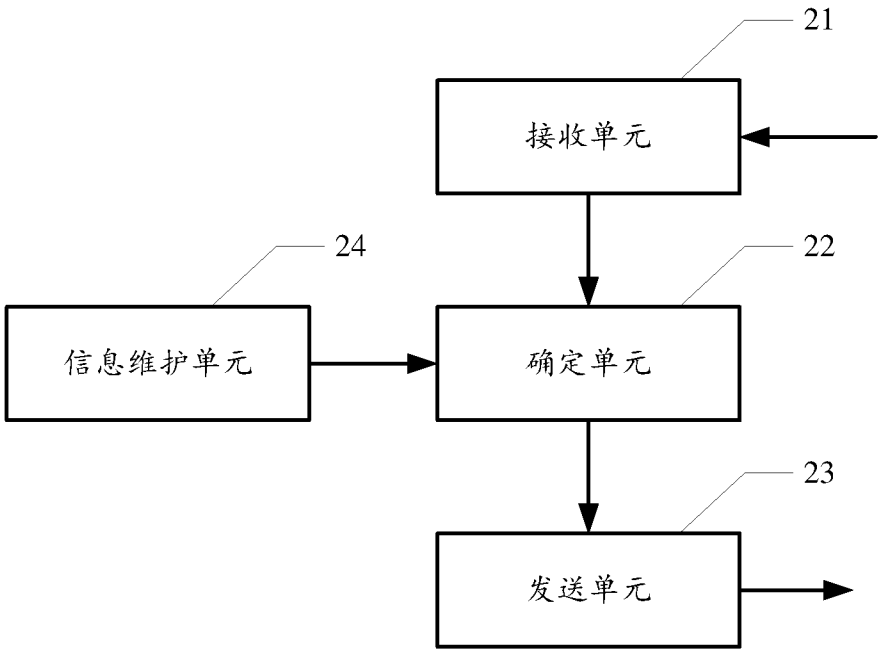

21
接收单元
24
22
信息维护单元
确定单元
23
发送单元

图 9

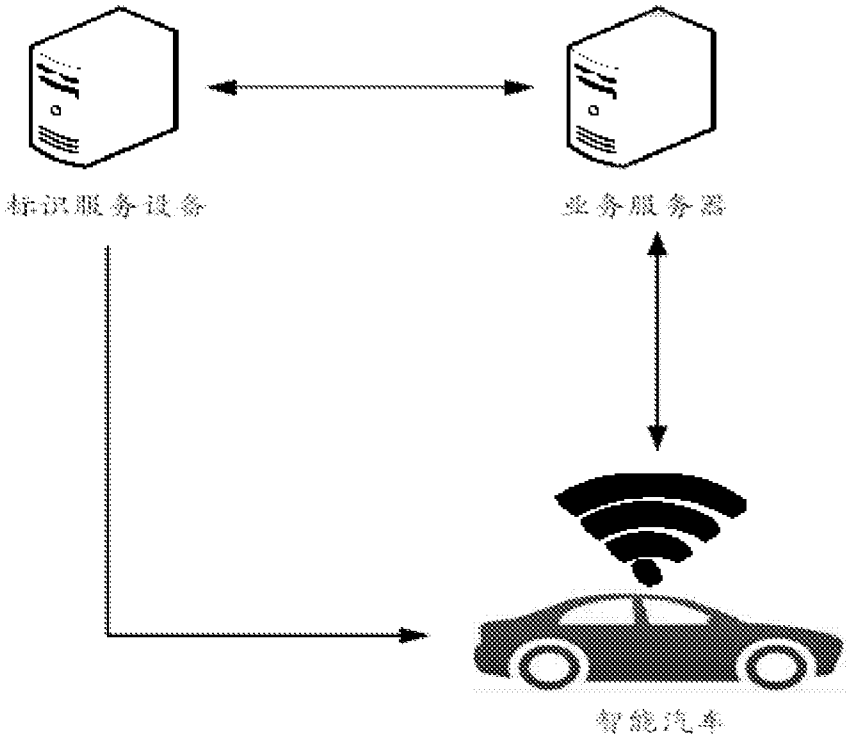



图 10

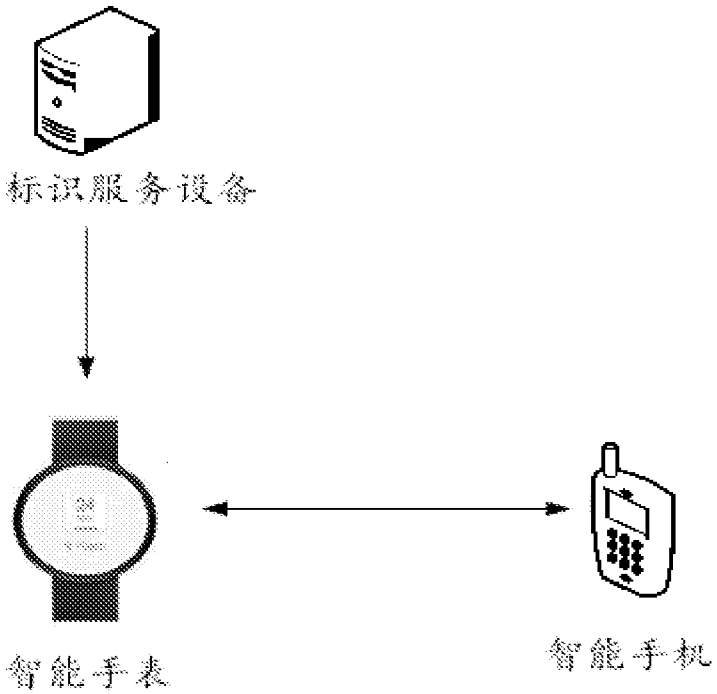



图 11

# INTERNATIONAL SEARCH REPORT

International application No.
**PCT/CN2017/071832**

**A. CLASSIFICATION OF SUBJECT MATTER**

H04L 9/08 (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; G06F

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)

CPRSABS; CNTXT; CNKI: TRUSTED, SESSION KEY, PRIVATE KEY, PUBLIC KEY

VEN: TRUST???, SESSION KEY, PRIVATE KEY, PUBLIC KEY

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | CN 102427449 A (BEIJING UNIVERSITY OF TECHNOLOGY), 25 April 2012 (25.04.2012), description, paragraphs [0051]-[0053] and [0102]-[0118] | 1, 6-10, 14-16, 21, 26-30, 34-36, 40 |
| Y | CN 102427449 A (BEIJING UNIVERSITY OF TECHNOLOGY), 25 April 2012 (25.04.2012), the same as above | 2-5, 11-13, 17-20, 22-25, 31-33, 37-39, 41 |
| Y | CN 101212293 A (POTEVIO INSTITUTE OF TECHNOLOGY CO., LTD.), 02 July 2008 (02.07.2008), description, page 6, line 9 to page 7, bottom line, and figure 2 | 2-5, 11-13, 17-20, 22-25, 31-33, 37-39, 41 |
| A | US 2008226065 A1 (ALADDIN EUROP GMBH), 18 September 2008 (18.09.2008), the whole document | 1-41 |
| A | CN 102143487 A (ZTE CORP.), 03 August 2011 (03.08.2011), the whole document | 1-41 |

☒ 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 |
|---|---|
| 10 March 2017 (10.03.2017) | **05 April 2017 (05.04.2017)** |
| Name and mailing address of the ISA/CN:<br>State Intellectual Property Office of the P. R. China<br>No. 6, Xitucheng Road, Jimenqiao<br>Haidian District, Beijing 100088, China<br>Facsimile No.: (86-10) 62019451 | Authorized officer<br>**WANG, Xiaoling**<br>Telephone No.: (86-10) **62089464** |

# INTERNATIONAL SEARCH REPORT

International application No.
**PCT/CN2017/071832**

**C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | US 2009024845 A1 (BENSHETLER, J.E. et al.), 22 January 2009 (22.01.2009), the whole document | 1-41 |
| A | CN 101479984 A (BOREN, S.L. et al.), 08 July 2009 (08.07.2009), the whole document | 1-41 |

# INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
**PCT/CN2017/071832**

| Patent Documents referred in the Report | Publication Date | Patent Family | Publication Date |
|---|---|---|---|
| CN 102427449 A | 25 April 2012 | CN 102427449 B | 09 April 2014 |
| CN 101212293 A | 02 July 2008 | CN 101212293 B | 14 April 2010 |
| US 2008226065 A1 | 18 September 2008 | US 2011029774 A1 | 03 February 2011 |
| | | US 7831051 B2 | 09 November 2010 |
| CN 102143487 A | 03 August 2011 | WO 2011095039 A1 | 11 August 2011 |
| | | CN 102143487 B | 10 June 2015 |
| US 2009024845 A1 | 22 January 2009 | US 2014195801 A1 | 10 July 2014 |
| | | US 8255684 B2 | 28 August 2012 |
| | | US 2012331289 A1 | 27 December 2012 |
| | | US 8694774 B2 | 08 April 2014 |
| | | US 9148421 B2 | 29 September 2015 |
| CN 101479984 A | 08 July 2009 | US 2009106551 A1 | 23 April 2009 |
| | | EP 2016701 A1 | 21 January 2009 |
| | | CN 101479984 B | 08 June 2011 |
| | | EP 2016701 A4 | 25 April 2012 |
| | | CA 2648780 C | 16 July 2013 |
| | | CA 2648780 A1 | 01 November 2007 |
| | | US 9166782 B2 | 20 October 2015 |
| | | WO 2007121587 A1 | 01 November 2007 |
| | | US 2013227286 A1 | 29 August 2013 |
| | | IN 200802526 P3 | 06 March 2009 |
| | | US 2017012949 A1 | 12 January 2017 |

# 国际检索报告

国际申请号
PCT/CN2017/071832

A. 主题的分类

H04L 9/08(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;G06F

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））

CPRSABS;CNTXT;CNKI:可信,会话密钥,私钥,公钥 VEN: TRUST???,SESSION KEY,PRIVATE KEY,PUBLIC KEY

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 102427449 A (北京工业大学) 2012年 4月 25日 (2012 - 04 - 25)<br>说明书第[0051]-[0053]段、第[0102]-[0118]段 | 1，6-10，14-16，21，26-30，34-36，40 |
| Y | CN 102427449 A (北京工业大学) 2012年 4月 25日 (2012 - 04 - 25)<br>同上 | 2-5，11-13，17-20，22-25，31-33，37-39，41 |
| Y | CN 101212293 A (普天信息技术研究院) 2008年 7月 2日 (2008 - 07 - 02)<br>说明书第6页第9行-第7页最后一行，图2 | 2-5，11-13，17-20，22-25，31-33，37-39，41 |
| A | US 2008226065 A1 (ALADDIN EUROP GMBH) 2008年 9月 18日 (2008 - 09 - 18)<br>全文 | 1-41 |
| A | CN 102143487 A (中兴通讯股份有限公司) 2011年 8月 3日 (2011 - 08 - 03)<br>全文 | 1-41 |

☑ 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 |
|---|---|
| 2017年 3月 10日 | 2017年 4月 5日 |
| ISA/CN的名称和邮寄地址<br>中华人民共和国国家知识产权局(ISA/CN)<br>中国北京市海淀区蓟门桥西土城路6号 100088<br>传真号 (86-10)62019451 | 受权官员<br>王晓玲<br>电话号码 (86-10)62089464 |

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 |
|---|---|---|
| A | US 2009024845 A1 (BENSHETLER JEFFERY E.等) 2009年 1月 22日 (2009-01-22)<br>全文 | 1-41 |
| A | CN 101479984 A (斯蒂芬 L. 博伦 等) 2009年 7月 8日 (2009-07-08)<br>全文 | 1-41 |

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2017/071832

| 检索报告引用的专利文件 | | | 公布日<br>(年/月/日) | 同族专利 | | | 公布日<br>(年/月/日) |
|---|---|---|---|---|---|---|---|
| CN | 102427449 | A | 2012年 4月 25日 | CN | 102427449 | B | 2014年 4月 9日 |
| CN | 101212293 | A | 2008年 7月 2日 | CN | 101212293 | B | 2010年 4月 14日 |
| US | 2008226065 | A1 | 2008年 9月 18日 | US | 2011029774 | A1 | 2011年 2月 3日 |
| | | | | US | 7831051 | B2 | 2010年 11月 9日 |
| CN | 102143487 | A | 2011年 8月 3日 | WO | 2011095039 | A1 | 2011年 8月 11日 |
| | | | | CN | 102143487 | B | 2015年 6月 10日 |
| US | 2009024845 | A1 | 2009年 1月 22日 | US | 2014195801 | A1 | 2014年 7月 10日 |
| | | | | US | 8255684 | B2 | 2012年 8月 28日 |
| | | | | US | 2012331289 | A1 | 2012年 12月 27日 |
| | | | | US | 8694774 | B2 | 2014年 4月 8日 |
| | | | | US | 9148421 | B2 | 2015年 9月 29日 |
| CN | 101479984 | A | 2009年 7月 8日 | US | 2009106551 | A1 | 2009年 4月 23日 |
| | | | | EP | 2016701 | A1 | 2009年 1月 21日 |
| | | | | CN | 101479984 | B | 2011年 6月 8日 |
| | | | | EP | 2016701 | A4 | 2012年 4月 25日 |
| | | | | CA | 2648780 | C | 2013年 7月 16日 |
| | | | | CA | 2648780 | A1 | 2007年 11月 1日 |
| | | | | US | 9166782 | B2 | 2015年 10月 20日 |
| | | | | WO | 2007121587 | A1 | 2007年 11月 1日 |
| | | | | US | 2013227286 | A1 | 2013年 8月 29日 |
| | | | | IN | 200802526 | P3 | 2009年 3月 6日 |
| | | | | US | 2017012949 | A1 | 2017年 1月 12日 |