

(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
2023 年 4 月 6 日 (06.04.2023)



(10) 国际公布号
WO 2023/051679 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01) H04W 8/24 (2009.01)

中国广东省深圳市龙岗区坂田华为总部
办公楼, Guangdong 518129 (CN)。

(21) 国际申请号: PCT/CN2022/122530

(22) 国际申请日: 2022 年 9 月 29 日 (29.09.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202111166679.8 2021 年 9 月 30 日 (30.09.2021) CN

(71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: 左俊 (ZUO, Jun); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 郭晓龙 (GUO, Xiaolong); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 林宏达 (LIN, Hongda);

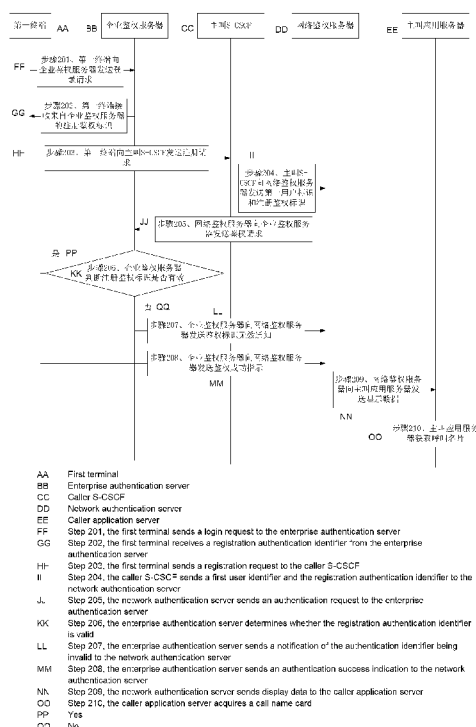
(74) 代理人: 深圳市深佳知识产权代理事务所 (普通合伙) (SHENPAT INTELLECTUAL PROPERTY AGENCY); 中国广东省深圳市罗湖区南湖街道春风路庐山大厦 B 座 18C2、18D、18E、18E2, Guangdong 518001 (CN)。

(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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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,

(54) Title: CALL PROCESSING METHOD, AND RELATED DEVICE AND STORAGE MEDIUM

(54) 发明名称: 一种呼叫处理的方法、相关设备以及存储介质



(57) Abstract: Disclosed in the embodiments of the present invention are a call processing method, and a related device and a storage medium, by means of which secure data to be displayed is sent to a second user during the process of a first user calling the second user, and the amount of information comprised in said data can be effectively increased. The method comprises: a first calling device acquiring a signature key; the first calling device acquiring data to be displayed of a first user; the first calling device signing said data by means of the signature key, so as to acquire first verification signature information; and the first calling device sending said data and the first verification signature information to a second calling device by means of a media channel between the first calling device and the second calling device, wherein the first verification signature information is used for verifying the security of said data.

(57) 摘要: 本发明实施例公开了一种呼叫处理的方法、相关设备以及存储介质, 用于在第一用户呼叫第二用户的过程中, 向第二用户发送安全的待显示数据, 且能够有效地提高待显示数据所包括的信息量。方法包括: 第一呼叫设备获取签名密钥; 第一呼叫设备获取第一用户的待显示数据; 第一呼叫设备通过签名密钥对待显示数据进行签名以获取第一验证签名信息; 第一呼叫设备通过第一呼叫设备和第二呼叫设备之间的媒体通道, 向第二呼叫设备发送待显示数据以及第一验证签名信息, 第一验证签名信息用于验证待显示数据的安全性。

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))。

— 1 —

一种呼叫处理的方法、相关设备以及存储介质

本申请要求于 2021 年 09 月 30 日提交中国专利局、申请号为 202111166679.8、发明名称为“一种呼叫处理的方法、相关设备以及存储介质”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。

5

技术领域

本申请涉及通信领域，尤其涉及一种呼叫处理的方法、相关设备以及通信系统。

背景技术

IP 多媒体子系统(IP multimedia subsystem, IMS)是一种全新的多媒体业务形式，它能够

10 能够满足更新颖、更多样化多媒体业务的需求。IMS 是解决移动与固网融合，引入语音、数据、视频三重融合等差异化业务的重要方式。

基于 IMS，在第一用户向第二用户呼叫的过程中，会出现第一用户为仿冒或篡改的情况，为此，主叫侧可通过安全电话身份重访(secure telephony identity revisited, STIR)或使用令牌对声明信息进行基于签名的处理方案(signature-based handling of asserted

15 information using toKENS, SHAKEN)技术对第一用户的呼叫请求消息的相关信息签名以生成签名信息，该相关信息可为主叫号码、被叫号码、时间戳、信誉度等级和呼叫源地址等。被叫侧根据公钥对签名信息进行验证。

STIR 或 SHAKEN 技术仅能做到对第一用户的号码进行认证，无法对第一用户的多种身份信息

20 信息进行认证。认证过程不涉及对企业信息的认证。而且 STIR/SHAKEN 技术仅涉及对信令层面的信息的加密与认证过程。

发明内容

本发明提供了一种呼叫处理的方法、相关设备以及存储介质，其用于在第一用户呼叫第二用户的过程中，向第二用户发送安全的待显示数据，且能够有效地提高待显示数据所

25 包括的信息量。

本发明实施例第一方面提供了一种呼叫处理的方法，所述方法包括：所述第一呼叫设备获取签名密钥；所述第一呼叫设备获取第一用户的待显示数据，所述第一用户通过所述

30 第一呼叫设备呼叫第二呼叫设备，所述待显示数据包括与所述第一用户对应的信息和/或与所述第一用户所属的企业对应的信息；所述第一呼叫设备通过所述签名密钥对所述待显示数据进行签名以获取第一验证签名信息；所述第一呼叫设备通过所述第一呼叫设备和所述

第二呼叫设备之间的媒体通道，向所述第二呼叫设备发送所述待显示数据以及所述第一验证签名信息，所述第一验证签名信息用于验证所述待显示数据的安全性。

本方面所示的第一呼叫设备可为第一用户所使用的第一终端，或，该第一呼叫设备可

35 为主叫运营商网络所包括的至少一个设备，例如，第一呼叫设备可为主叫运营商网络所包括的主叫媒体服务器，主叫应用服务器 AS，主叫服务-呼叫会话控制功能 S-CSCF，主叫代理-呼叫会话控制功能 P-CSCF 或主叫互通会话边界控制器 I-SBC。

可见，在第一用户呼叫第二用户的过程中，第一呼叫设备向第二呼叫设备所发送的第

—2—

一验证签名信息是待显示数据进行签名以获取的，第二呼叫设备接收到待显示数据以及所述第一验证签名信息后，能够根据第一验证签名信息对待显示数据的安全性进行验证，第二用户所使用的第二终端即可在呼叫的过程中，显示该待显示数据，以便于第二用户确定所显示的待显示数据是否经过篡改或泄漏。而且因该待显示数据是经由所述第一呼叫设备

5 和所述第二呼叫设备之间的媒体通道传输，有效地提高了待显示数据所传输的数据量。

基于第一方面，一种可选地实现方式中，所述第一呼叫设备通过所述签名密钥对所述待显示数据进行签名以获取第一验证签名信息之前，所述方法还包括：所述第一呼叫设备向所述第二呼叫设备发送第一指示消息，所述第一指示消息用于指示所述第一呼叫设备支持对所述待显示数据签名的能力；所述第一呼叫设备接收来自所述第二呼叫设备的第二指示消息，所述第二指示消息用于指示所述第二呼叫设备支持验证所述待显示数据安全性的能力。

10

可见，第一呼叫设备和第二呼叫设备之间，可通过该第一指示消息和第二指示消息进行协商，在第二呼叫设备接收到该第一指示消息的情况下，确定所述第一呼叫设备支持对所述待显示数据签名的能力，第二呼叫设备即可向第一呼叫设备返回第二指示消息，第二

15 呼叫设备根据该第二指示消息确定第二呼叫设备支持验证所述待显示数据安全性的能力，那么，第一呼叫设备能够向第二呼叫设备发送所述待显示数据以及第一验证签名信息，以确保第二呼叫设备能够根据该第一验证签名信息验证待显示数据的安全性。

基于第一方面，一种可选地实现方式中，所述第一呼叫设备获取第一用户的待显示数据包括：所述第一呼叫设备接收呼叫请求消息，所述呼叫请求消息携带所述待显示数据。

20 可见，第一呼叫设备为主叫运营商网络所包括的设备，该第一呼叫设备能够接收来自第一终端的呼叫请求消息，该呼叫请求消息携带该待显示数据，第一呼叫设备接收到该呼叫请求消息后，即可获取到该待显示数据。

基于第一方面，一种可选地实现方式中，所述第一呼叫设备获取第一用户的待显示数据包括：所述第一呼叫设备接收呼叫请求消息；所述第一呼叫设备获取与所述呼叫请求消息对应的所述待显示数据。

25

可见，第一呼叫设备为主叫运营商网络所包括的设备，第一呼叫设备可预先存储该待显示数据，第一呼叫设备接收到来自第一终端的呼叫请求消息后，即可获取与该呼叫请求消息对应的待显示数据。

基于第一方面，一种可选地实现方式中，所述第一呼叫设备获取签名密钥包括：所述第一呼叫设备向所述第二呼叫设备发送呼叫请求消息，所述呼叫请求消息用于请求获取所述签名密钥；所述第一呼叫设备接收来自所述第二呼叫设备的主密钥和主盐密钥，所述主密钥和所述主盐密钥用于安全实时传输协议 SRTP；所述第一呼叫设备根据所述主密钥和所述主盐密钥，生成所述签名密钥。

30

可见，第一呼叫设备通过该呼叫请求消息向第二呼叫设备请求获取主密钥和主盐密钥，第一呼叫设备基于安全实时传输协议 SRTP，能够根据该主密钥和主盐密钥推导出签名密钥，本方面所示的第一呼叫设备能够基于安全实时传输协议 SRTP 获取该签名密钥，以实现对待显示数据的签名。

35

— 3 —

基于第一方面，一种可选地实现方式中，所述第一呼叫设备接收来自所述第二呼叫设备的主密钥和主盐密钥包括：所述第一呼叫设备接收来自所述第二呼叫设备的签名信息，所述签名信息包括通过公钥签名的所述主密钥和所述主盐密钥；所述第一呼叫设备通过私钥验证所述签名信息以获取所述主密钥和所述主盐密钥。

5 为提高待显示数据的安全性，需要保证第一呼叫设备所获取到的主密钥和主盐密钥的安全性，若主密钥和主盐密钥出现泄露或篡改，那么，将导致待显示数据会出现泄露或篡改的情况，为此，第一呼叫设备所接收到的签名信息包括通过公钥签名的所述主密钥和所述主盐密钥，有效地避免了主密钥和主盐密钥出现泄露或篡改的情况，提高了待显示数据的安全性。

10 基于第一方面，一种可选地实现方式中，与所述第一用户对应的信息包括如下所示的至少一项：所述第一用户的名称，所述第一用户的工号，所述第一用户的头像，所述第一用户的职位信息，与所述第一用户相关的音视频文件，或所述第一用户所属的协会的信息；

与所述第一用户所属的企业对应的信息包括如下所示的至少一项：所述企业名称，所述企业的商标，与所述企业相关的音视频文件，或所述企业所属的协会的信息。

15 本发明实施例第二方面提供了一种呼叫处理的方法，所述方法包括：第二呼叫设备接收来自第一呼叫设备的待显示数据以及第一验证签名信息，所述第一验证签名信息为通过签名密钥对所述待显示数据进行签名以获取，所述待显示数据和所述第一验证签名信息通过所述第一呼叫设备和所述第二呼叫设备之间的媒体通道传输，所述待显示数据包括与所述第一用户对应的信息和/或与所述第一用户所属的企业对应的信息；所述第二呼叫设备通过所述签名密钥对所述待显示数据进行签名以获取第二验证签名信息；若所述第二呼叫设备确定所述第一验证签名信息和所述第二验证签名信息相同，确定所述待显示数据通过安全
20 性验证，使所述待显示数据显示。

本方面所示的第二呼叫设备可为第二用户所使用的第二终端，或，该第二呼叫设备可为被叫运营商网络所包括的至少一个设备，例如，第二呼叫设备可为被叫运营商网络所包括的被叫媒体服务器，被叫应用服务器 AS，被叫服务-呼叫会话控制功能 S-CSCF，被叫代理-呼叫会话控制功能 P-CSCF 或被叫互通会话边界控制器 I-SBC。
25

本方面所示的有益效果，请参见第一方面所示，具体不做赘述。

基于第二方面，一种可选地实现方式中，所述第二呼叫设备接收来自第一呼叫设备的待显示数据以及第一验证签名信息之前，所述方法还包括：所述第二呼叫设备接收来自所述
30 所述第一呼叫设备的第一指示消息，所述第一指示消息用于指示所述第一呼叫设备支持对所述待显示数据签名的能力；所述第二呼叫设备向所述第一呼叫设备发送第二指示消息，所述第二指示消息用于指示所述第二呼叫设备支持验证所述待显示数据安全性的能力。

基于第二方面，一种可选地实现方式中，所述若所述第二呼叫设备确定所述第一验证签名信息和所述第二验证签名信息相同，确定所述待显示数据通过安全性验证之后，所述
35 方法还包括：所述第二呼叫设备向第二终端发送所述待显示数据，所述第二终端为第二用户所使用的终端，所述第二终端用于显示所述待显示数据。

基于第二方面，一种可选地实现方式中，所述第二呼叫设备为第二终端，所述第二终

—4—

端为第二用户所使用的终端，所述若所述第二呼叫设备确定所述第一验证签名信息和所述第二验证签名信息相同，确定所述待显示数据通过安全性验证之后，所述方法还包括：所述第二呼叫设备显示所述待显示数据。

基于第二方面，一种可选地实现方式中，所述若所述第二呼叫设备确定所述第一验证签名信息和所述第二验证签名信息相同，确定所述待显示数据通过安全性验证之后，所述方法还包括：所述第二呼叫设备向所述第二终端发送通知消息，所述通知消息用于指示所述待显示数据通过安全性验证。

可见，在所述第二呼叫设备确定待显示数据通过安全性验证，向所述第二终端发送用于指示待显示数据通过安全性验证的通知信息，所述第二终端接收到该通知信息后，即可显示用于指示待显示数据通过安全性验证的通知信息，以保证第二用户根据第二终端已显示的通知信息，确定所显示的待显示数据是安全的。

基于第二方面，一种可选地实现方式中，所述第二呼叫设备接收来自第一呼叫设备的待显示数据以及第一验证签名信息之前，所述方法还包括：所述第二呼叫设备接收来自所述第一呼叫设备的呼叫请求消息，所述呼叫请求消息用于请求获取所述签名密钥；所述第二呼叫设备根据所述呼叫请求消息向所述第一呼叫设备发送主密钥和主盐密钥，所述主密钥和所述主盐密钥用于安全实时传输协议 SRTP，所述主密钥和所述主盐密钥用于生成所述验证签名。

基于第二方面，一种可选地实现方式中，所述第二呼叫设备根据所述呼叫请求消息向所述第一呼叫设备发送主密钥和主盐密钥包括：所述第二呼叫设备通过公钥对所述主密钥和所述主盐密钥签名以获取签名信息；所述第二呼叫设备向所述第一呼叫设备发送所述签名信息。

基于第二方面，一种可选地实现方式中，所述第二呼叫设备接收来自第一呼叫设备的待显示数据以及第一验证签名信息之前，所述方法还包括：所述第二呼叫设备接收来自所述第一呼叫设备的呼叫请求消息；所述第二呼叫设备根据所述呼叫请求消息向所述第一呼叫设备发送所述签名密钥。

基于第二方面，一种可选地实现方式中，与所述第一用户对应的信息包括如下所示的至少一项：所述第一用户的名称，所述第一用户的工号，所述第一用户的头像，所述第一用户的职位信息，与所述第一用户相关的音视频文件，或所述第一用户所属的协会的信息；

所述第一用户所属的企业对应的信息包括如下所示的至少一项：所述企业名称，所述企业的商标，与所述企业相关的音视频文件，或所述企业所属的协会的信息。

本发明实施例第三方面提供了一种呼叫设备，包括：第一获取模块，用于获取签名密钥；第二获取模块，用于获取第一用户的待显示数据，所述第一用户为与所述呼叫设备对应的用户，所述待显示数据包括与所述第一用户对应的信息和/或与所述第一用户所属的企业对应的信息；签名模块，用于通过所述签名密钥对所述待显示数据进行签名以获取第一验证签名信息；发送模块，用于通过所述呼叫设备和另一呼叫设备之间的媒体通道，向所述另一呼叫设备发送所述待显示数据以及所述第一验证签名信息，所述第一验证签名信息用于验证所述待显示数据的安全性。

—5—

本方面有益效果的说明，请参见上述第一方面所示，具体不做赘述。

基于第三方面，一种可选地实现方式中，所述发送模块还用于，向所述另一呼叫设备发送第一指示消息，所述第一指示消息用于指示所述呼叫设备支持对所述待显示数据签名的能力；所述呼叫设备还包括接收模块，所述接收模块用于接收来自所述另一呼叫设备的第二指示消息，所述第二指示消息用于指示所述另一呼叫设备支持验证所述待显示数据安全性的能力。

基于第三方面，一种可选地实现方式中，所述第二获取模块具体用于，接收呼叫请求消息，所述呼叫请求消息携带所述待显示数据。

基于第三方面，一种可选地实现方式中，所述第二获取模块具体用于，接收呼叫请求消息；获取与所述呼叫请求消息对应的所述待显示数据。

基于第三方面，一种可选地实现方式中，所述第一获取模块具体用于，向所述另一呼叫设备发送呼叫请求消息，所述呼叫请求消息用于请求获取所述签名密钥；接收来自所述另一呼叫设备的主密钥和主盐密钥，所述主密钥和所述主盐密钥用于安全实时传输协议SRTP；根据所述主密钥和所述主盐密钥，生成所述签名密钥。

基于第三方面，一种可选地实现方式中，所述第一获取模块具体用于，接收来自所述另一呼叫设备的签名信息，所述签名信息包括通过公钥签名的所述主密钥和所述主盐密钥；通过私钥验证所述签名信息以获取所述主密钥和所述主盐密钥。

基于第三方面，一种可选地实现方式中，与所述第一用户对应的信息包括如下所示的至少一项：

所述第一用户的名称，所述第一用户的工号，所述第一用户的头像，所述第一用户的职位信息，与所述第一用户相关的音视频文件，或所述第一用户所属的协会的信息；

与所述第一用户所属的企业对应的信息包括如下所示的至少一项：

所述企业名称，所述企业的商标，与所述企业相关的音视频文件，或所述企业所属的协会的信息。

本发明实施例第四方面提供了一种呼叫设备，包括：接收模块，用于接收来自另一呼叫设备的待显示数据以及第一验证签名信息，所述第一验证签名信息为通过签名密钥对所述待显示数据进行签名以获取，所述待显示数据和所述第一验证签名信息通过所述另一呼叫设备和呼叫设备之间的媒体通道传输，所述待显示数据包括与第一用户对应的信息和/或与所述第一用户所属的企业对应的信息，所述第一用户为与所述另一呼叫设备对应的用户；签名模块，用于通过所述签名密钥对所述待显示数据进行签名以获取第二验证签名信息；验证模块，用于若确定所述第一验证签名信息和所述第二验证签名信息相同，确定所述待显示数据通过安全性验证，使所述待显示数据显示。

本方面有益效果的说明，请参见上述第二方面所示，具体不做赘述。

基于第四方面，一种可选地实现方式中，所述接收模块还用于，接收来自所述另一呼叫设备的第一指示消息，所述第一指示消息用于指示所述另一呼叫设备支持对所述待显示数据签名的能力；向所述另一呼叫设备发送第二指示消息，所述第二指示消息用于指示所述呼叫设备支持验证所述待显示数据安全性的能力。

基于第四方面，一种可选地实现方式中，所述呼叫设备还包括发送模块，用于向第二终端发送所述待显示数据，所述第二终端为第二用户所使用的终端，所述第二终端用于显示所述待显示数据。

5 基于第四方面，一种可选地实现方式中，所述呼叫设备为第二终端，所述第二终端为第二用户所使用的终端，所述呼叫设备还包括显示模块，所述显示模块用于显示所述待显示数据。

基于第四方面，一种可选地实现方式中，所述发送模块还用于向所述第二终端发送通知消息，所述通知消息用于指示所述待显示数据通过安全性验证。

10 基于第四方面，一种可选地实现方式中，所述接收模块还用于，接收来自所述另一呼叫设备的呼叫请求消息，所述呼叫请求消息用于请求获取所述签名密钥；所述发送模块还用于，根据所述呼叫请求消息向所述另一呼叫设备发送主密钥和主盐密钥，所述主密钥和所述主盐密钥用于安全实时传输协议 SRTP，所述主密钥和所述主盐密钥用于生成所述验证签名。

15 基于第四方面，一种可选地实现方式中，所述发送模块具体用于：通过公钥对所述主密钥和所述主盐密钥签名以获取签名信息；向所述另一呼叫设备发送所述签名信息。

基于第四方面，一种可选地实现方式中，所述接收模块还用于，接收来自所述另一呼叫设备的呼叫请求消息；所述发送模块还用于，根据所述呼叫请求消息向所述另一呼叫设备发送所述签名密钥。

20 本发明实施例第五方面提供了一种呼叫设备，包括相互耦合的处理器和存储器，所述存储器中存储了计算机程序代码，所述处理器调用并执行所述存储器中的计算机程序代码，使得所述呼叫设备执行如上述第一方面任一项所述的方法。

本发明实施例第六方面提供了一种呼叫设备，包括相互耦合的处理器和存储器，所述存储器中存储了计算机程序代码，所述处理器调用并执行所述存储器中的计算机程序代码，使得所述呼叫设备执行如上述第二方面任一项所述的方法。

25 本发明实施例第七方面提供了一种计算机可读存储介质，所述存储介质存储有计算机程序，所述计算机程序包括程序指令，所述程序指令当被处理器执行时使所述处理器执行如上述第一方面至第二方面任一项所述的方法。

30 本发明实施例第八方面提供了一种通信系统，包括第一终端，如上述第五方面所示的呼叫设备，如上述第六方面所示的呼叫设备以及第二终端，所述第一终端为第一用户所使用的终端，上述第五方面所示的呼叫设备为主叫运营商网络所包括的设备，上述第六方面所示的呼叫设备为被叫运营商网络所包括的设备，所述第二终端为第二用户所使用的终端，所述第一用户呼叫第二用户。

35 本发明实施例第九方面提供了一种通信系统，包括如上述第五方面所示的呼叫设备，主叫运营商网络，被叫运营商网络以及如上述第六方面所示的呼叫设备，如上述第五方面所示的呼叫设备为第一用户所使用的设备，如上述第六方面所示的呼叫设备为第二用户所使用的设备。

附图说明

图 1 为本申请所提供的主叫通信系统的一种实施例结构示意图；
图 2 为本申请所提供的主叫通信系统执行注册的过程的一种实施例步骤流程图；
图 3 为本申请所提供的主叫通信系统执行呼叫的一种实施例步骤流程图；
5 图 4 为本申请所提供的主叫通信系统执行呼叫的另一种实施例步骤流程图；
图 5 为本申请所提供的主叫通信系统执行呼叫的另一种实施例步骤流程图；
图 6 为本申请所提供的主叫通信系统执行呼叫的另一种实施例步骤流程图；
图 7 为本申请所提供的主叫通信系统执行呼叫的另一种实施例步骤流程图；
图 8 为本申请所提供的第一呼叫设备的一种实施例结构示意图；
10 图 9 为本申请所提供的第二呼叫设备的一种实施例结构示意图；
图 10 为本申请所提供的呼叫设备的一种实施例结构示意图。

具体实施方式

下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地
15 描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本
发明中的实施例，本领域技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，
都属于本发明保护的范围。

本申请提供了一种呼叫处理的方法，为更好的理解本申请所提供的呼叫处理的方法，
以下首先结合图 1 所示对本申请所示的方法所应用的主叫通信系统的结构进行说明：第一
20 用户基于该主叫通信系统能够实现向第二用户的呼叫。

图 1 为本申请所提供的主叫通信系统的一种实施例结构示意图。

本实施例所示的主叫通信系统包括依次连接的运营商管理设备 111、主叫运营商网络
120 以及企业网络 130，本实施例对主叫运营商网络 120 的具体网络类型不做限定，例如，
该主叫运营商网络 120 的网络类型为 IMS、第三代合作伙伴计划（3rd generation
25 partnership project, 3GPP）或中国通信标准化协会（china communications standards
association, CCSA），以及未来出现的任意网络架构。以下本申请各实施例以主叫运营商
网络 120 为 IMS 为例。

以下对该主叫运营商网络 120 所包括的各个设备进行说明，需明确的是，本实施例对
各个设备类型的说明为可选地示例性，不做限定，本实施例所示的设备还可称为网元。

30 本实施例所示的主叫运营商网络 120 包括网络鉴权服务器 121，本实施例所示的网络
鉴权服务器还可称之为第三方账号管理（thirdparty account management, TAM）设备。

主叫运营商网络 120 包括主叫媒体服务器 122，所述主叫媒体服务器 122 可集成多媒
体资源功能处理器（multimedia resource function processor, MRFP）以及多媒体资源
功能控制器（multimedia resource function controller, MRFC）。主叫运营商网络 120
35 还包括主叫应用服务器（application server, AS）123 以及主叫服务-呼叫会话控制功能
（serving-call session control function, S-CSCF）124，该主叫 S-CSCF124 还集成查
询-呼叫会话控制功能（interrogating-call session control function, I-CSCF）。其中，

—8—

网络鉴权服务器 121 分别与主叫媒体服务器 122、主叫 AS123 以及主叫 S-CSCF124 连接，主叫媒体服务器 122 与主叫 AS123 连接，主叫 AS123 与主叫 S-CSCF124 连接。

主叫 S-CSCF124 分别连接主叫代理-呼叫会话控制功能 (proxy-call session control function, P-CSCF) 以及主叫互通会话边界控制器 (interconnect-session border controller, I-SBC) 125，其中，主叫 P-CSCF126 还集成接入会话边界控制器 (access-session border controller, A-SBC)。

以下对本实施例所示的企业网络 130 的结构进行说明，需明确的是，本实施例对该企业网络 130 的说明为可选地示例，不做限定。

该企业网络 130 具体包括企业鉴权服务器 131、企业接入代理设备 132 以及第一终端 133。其中，企业鉴权服务器 131 分别与网络鉴权服务器 121、企业接入代理设备 132 以及第一终端 133 连接。该企业接入代理设备 132 与主叫 I-SBC125 或主叫 P-CSCF 连接，该第一终端 133 与主叫 P-CSCF126 连接。其中，企业接入代理设备 132 也可能是企业话音中继设备。

其中，第一用户（也可称之为主叫用户）所使用的第一终端 133 可为智能终端、计算机中的任一设备。该第一终端内置 IMS 软件开发工具包 (software development kit, SDK)，以实现本申请所示的呼叫处理流程。

以下对本申请所提供的呼叫处理的方法的各个实施例进行说明，为更好的理解本申请所示的各个实施例，首先对本申请所示的呼叫处理的方法所要实现的目的进行概述性说明：

本申请所示的呼叫处理的方法，第一用户在对第二用户进行呼叫的时候，可向第二用户发送呼叫名片，第二用户（也可称之为被叫用户）所使用的第二终端在振铃的时候，即可显示该呼叫名片。该呼叫名片包括按照预设排版方式排版后的待显示数据，该待显示数据包括如下所示的至少一项：

与第一用户对应的信息，或与第一用户所属的企业对应的信息。

其中，第一用户对应的信息可包括如下所示的一项或多项：

第一用户的名称，第一用户的工号，第一用户的头像、第一用户的职位信息，与第一用户相关的音视频文件或第一用户所属的协会的信息等，其中，该第一用户的名称可为第一用户的姓名，也可为第一用户的昵称等，具体在本实施例中不做限定。

第一用户所属的企业对应的信息可包括如下所示的一项或多项：

企业名称，企业商标 (LOGO)，与企业相关的图片，与企业相关的音视频文件，或企业所属的协会的信息。

其中，协会的信息可为协会的名称、协会的 LOGO、协会的相关图片、与协会相关的音视频文件等。

本申请对呼叫名片所包括的待显示数据的具体内容以及待显示数据的具体排版方式不做限定。本申请能够保证在第一用户呼叫第二用户的过程中，向第二用户发送的该呼叫名片是安全的，还能够有效地避免呼叫名片被篡改或被仿冒的可能，避免第二用户接收到不安全的数据。

以下结合各个实施例对本实施例所示的呼叫处理的方法的执行过程进行说明：

实施例一

本实施例所示企业内部的第一用户为向企业外部的第二用户呼叫时，先执行注册处理流程，基于该注册处理流程，将待显示数据发送至主叫运营商网络，由主叫运营商网络根据来自第一用户的待显示数据生成呼叫名片。

5 可知，在注册阶段，主叫运营商网络已成功获取到呼叫名片，在后续的主叫运营商网络呼叫第二用户时，主叫运营商网络无需在呼叫过程中获取呼叫名片，而是直接将已在注册阶段获取到的呼叫名片发送至第二用户，节省了呼叫过程中主叫运营商网络与企业鉴权服务器之间所交互的信息量，缩短了呼叫接续时延，提高了呼叫效率，具体参见图 2 所示，

图 2 为本申请所提供的主叫通信系统执行注册的过程的一种实施例步骤流程图。

10 步骤 201、第一终端向企业鉴权服务器发送登录请求。

本实施例以第一终端向企业鉴权服务器发送登录请求为例进行示例性说明，在其他示例中，也可由企业接入代理设备向企业鉴权服务器发送登录请求，不做限定。该第一终端可运行企业应用程序（APP），该第一终端通过该企业 APP 能够实现本申请所示的呼叫处理的方法中，由第一终端执行的流程。

15 第一用户对企业外部的第二用户进行呼叫时，可通过第一终端向企业鉴权服务器发送该登录请求，该登录请求包括该第一用户的第一用户标识。

本实施例所示的第一用户标识（也可称之为 UserID）可为该第一用户的邮箱地址，例如，zhangsan@xxx.com。本实施例所示的第一用户标识有别于现有的 E.164 号码，可见，该第一用户标识对主叫运营商网络而言属于异构标识，本申请所示的第一用户向第二用户
20 进行呼叫的过程，所使用的不是 E.164 号码，而是本实施例所提供的作为异构标识的第一用户标识（即第一用户的邮箱地址）。

步骤 202、第一终端接收来自企业鉴权服务器的注册鉴权标识。

本实施例所示的企业鉴权服务器接收到该第一用户标识，即可为该第一用户标识分配注册鉴权标识，该注册鉴权标识用于注册至主叫运营商网络。

25 本实施例对注册鉴权标识不做限定，本实施例以该注册鉴权标识为令牌（token）为例进行示例性说明。

步骤 203、第一终端向主叫 S-CSCF 发送注册请求。

其中，所述注册请求包括所述第一用户的第一用户标识和所述注册鉴权标识。

30 本实施例所示的注册请求为会话发起协议（session initiation protocol, SIP）注册（REGISTER）消息，该注册请求需要携带第一用户的第一用户标识和所述注册鉴权标识。

本实施例所示的 token 可使用基于 64 个可打印字符来表示二进制数据（Base64）的编码格式，该 token 可通过授权（Authorization）头域和扩展的鉴权方式（如 Bearer）携带，如消息格式可为：Authorization: Bearer <Base64(<token>>)>。

例如，该 SIP REGISTER 消息具体可为如下所示：

35 SIP REGISTER: 2b.ims.<operator>.com
From/To: SIP zhangsan%40xxx.com@2b.ims.<operator>.com
Authorization: Bearer <Base64(<token>>)>

以下对第一终端向主叫 S-CSCF 发送注册请求的过程进行说明：

参见图 1 所示，第一终端 133 向主叫 P-CSCF126 发送该注册请求，主叫 P-CSCF 再转发该注册请求至主叫 S-CSCF124，其中，主叫 P-CSCF 按照 SIP 用户注册的标准流程（参见 3GPP TS 24.229）处理 SIP REGISTER 消息后转发给主叫 S-CSCF。

5 步骤 204、主叫 S-CSCF 向网络鉴权服务器发送第一用户标识和注册鉴权标识。

主叫 S-CSCF 判断注册请求使用 Bearer 的鉴权方式时，向网络鉴权服务器发送第一用户标识和注册鉴权标识，以请求网络鉴权服务器利用注册鉴权标识对第一用户进行鉴权。

步骤 205、网络鉴权服务器向企业鉴权服务器发送鉴权请求。

10 本实施例所示的网络鉴权服务器接收到该第一用户标识的情况下，即可根据该第一用户标识确定出对应的企业鉴权服务器。

由上述示例可知，本实施例所示的第一用户标识为用户的邮箱地址（例如，zhangsan@xxx.com），则网络鉴权服务器即可在第一用户标识中获得企业域名（例如 xxx.com）。网络鉴权服务器根据该企业域名即可查询出企业鉴权服务器的地址。

15 具体地，由上述所示可知，网络鉴权服务器从主叫 S-CSCF 接收到的第一用户标识为 zhangsan%40xxx.com，本步骤所示的网络鉴权服务器在根据第一用户标识确定对应的企业鉴权服务器的过程中，企业鉴权服务器对被转义的第一用户标识（zhangsan%40xxx.com）进行恢复以获取到恢复转义后的第一用户标识（zhangsan@xxx.com）。可见，网络鉴权服务器即可根据恢复转义后的第一用户标识查询出对应的企业鉴权服务器的地址。

20 本实施例所示的网络鉴权服务器向所述企业鉴权服务器所发送的鉴权请求包括注册鉴权标识。可选地，本实施例所示可通过超文本传输安全协议（hyper text transfer protocol over securesocket layer, HTTPS）发送所述鉴权请求。

步骤 206、企业鉴权服务器判断注册鉴权标识是否有效，若否，则执行步骤 207，若是，则执行步骤 208。

25 本实施例所示的注册鉴权标识为 token，则企业鉴权服务器即可判断该 token 是否位于有效期内，该有效期可为绝对有效期，例如，该有效期的起始时刻为 A1，该有效期的终止时刻为 A2，该 A1 时刻和 A2 时刻可为任意互不相同的两个时刻。若企业鉴权服务器判断出该 token 位于该有效期内，则企业鉴权服务器确定该 token 有效，若企业鉴权服务器判断出该 token 位于该有效期之外，则企业鉴权服务器确定该 token 无效。

30 又如，该有效期可为剩余有效时长，可见，若注册鉴权标识对应的剩余有效时长还有剩余时间，则企业鉴权服务器判断该 token 有效，若注册鉴权标识对应的剩余有效时长已无剩余时间，则企业鉴权服务器判断该 token 无效。

步骤 207、企业鉴权服务器向网络鉴权服务器发送鉴权标识无效通知。

35 具体地，本实施例所示的企业鉴权服务器向网络鉴权服务器发送该鉴权标识无效通知，该鉴权标识无效通知用于指示该注册鉴权标识（token）无效。网络鉴权服务器接收到该鉴权标识无效通知的情况下，则不再执行与第一用户注册的相关流程。

步骤 208、企业鉴权服务器向网络鉴权服务器发送鉴权成功指示。

本实施例所示的鉴权成功指示包括鉴权标识有效通知，该鉴权标识有效通知用于指示

该注册鉴权标识 (token) 有效。

本实施例所示的鉴权成功指示还包括第二用户标识，具体地，企业鉴权服务器预先创建不同的用户标识和不同的鉴权标识的对应关系，在企业鉴权服务器确定该注册鉴权标识有效的情况下，企业鉴权服务器即可将该有效的注册鉴权标识对应的第二用户标识发送至网络鉴权服务器。

可选地，本实施例所示的鉴权成功指示可包括如下所示的至少一项：

用于指示注册鉴权标识的有效期的消息，第一用户的名称（例如，zhangsan），第一用户的头像的下载地址，用于指示该第一用户是否具有外呼权限的消息等。

步骤 209、网络鉴权服务器向主叫应用服务器发送待显示数据。

本实施例中，在网络鉴权服务器确定第一用户通过鉴权的情况下，网络鉴权服务器即可将已获取到的待显示数据向主叫应用服务器发送。

本实施例以所述待显示数据包括与第一用户对应的信息和/或与第一用户所属的企业对应的信息，具体说明请参见图 1 相关的说明，具体不做赘述。

网络鉴权服务器获取待显示数据的方式可为，在企业鉴权服务器判断注册鉴权标识有效的情况下，企业鉴权服务器向网络鉴权服务器发送该待显示数据。又如，网络鉴权服务器在企业开户阶段获取该待显示数据。又如，网络鉴权服务器从企业鉴权服务器获取一部分的待显示数据（如与第一用户相关的信息），网络鉴权服务器在企业开户阶段获取另一部分待显示数据（如与第一用户所属的企业相关的信息）等，具体在本实施例中不做限定。

本实施例所示的网络鉴权服务器确定第一用户通过鉴权的方式有可选地两种：

方式 1：

由网络鉴权服务器负责对第一用户鉴权，具体地，所述网络鉴权服务器确定通过鉴权的条件有两个，一个条件是根据已接收到鉴权标识有效通知。另一个条件是该网络鉴权服务器确定第一用户标识和第二用户标识相同。

方式 2：

由企业鉴权服务器负责对第一用户鉴权，企业鉴权服务器再将鉴权结果向网络鉴权服务器通知，具体地，所述网络鉴权服务器向企业鉴权服务器发送的鉴权请求包括所述第一用户标识，所述企业鉴权服务器在判断所述注册鉴权标识有效且所述第一用户标识和所述第二用户标识相同，则向网络鉴权服务器发送注册鉴权成功指示，网络鉴权服务器根据该注册鉴权成功指示以确定第一用户通过鉴权。

步骤 210、主叫应用服务器获取呼叫名片。

本实施例所示的以主叫应用服务器用于获取呼叫名片为例进行示例性说明，在其他示例中，用于获取呼叫名片的设备可为主叫运营商网络所包括的任一设备。本实施例所示的主叫应用服务器获取呼叫名片的几种可选地方式为：

方式 1

本实施例所示的主叫应用服务器能够接收到来自网络鉴权服务器的待显示数据，主叫应用服务器即可按照呼叫名片的排版方式，对待显示数据进行排版以获取呼叫名片。其中，该呼叫名片的排版方式可在企业开户阶段向网络鉴权服务器发送的，又如，该呼叫名片的

排版方式可在步骤 209 的过程中由网络鉴权服务器向主叫应用服务器发送的，即，网络鉴权服务器在确定第一用户通过鉴权的情况下，网络鉴权服务器即可将该呼叫名片的排版方式向主叫应用服务器发送。

该呼叫名片的排版方式是指，所生成的呼叫名片中，第一用户对应的信息和/或第一用户所属的企业对应的信息中，各信息的显示方式以及显示位置。

例如，第一用户的名称，第一用户的工号，第一用户的头像、第一用户的职位信息，与第一用户相关的音视频文件，第一用户所属的协会的信息，企业名称，企业商标，与企业相关的图片，与企业相关的音视频文件以及企业所属的协会的信息等，在呼叫名片中的显示方式以及显示位置。

本方式以呼叫名片存储于主叫应用服务器为例进行示例性说明，在其他示例中，在主叫应用服务器获取到呼叫名片后，主叫应用服务器将已生成的呼叫名片发送至文件服务器进行存储，并本地记录该呼叫名片的存储地址。

方式 2

主叫应用服务器接收来自网络鉴权服务器的所述待显示数据以及呼叫名片的排版方式的情况下，网络鉴权服务器将待显示数据以及呼叫名片的排版方式转发给主叫媒体服务器 122。主叫媒体服务器 122 按照呼叫名片的排版方式对待显示数据进行排版以获取呼叫名片。

主叫媒体服务器 122 将已生成的呼叫名片发送至文件服务器进行存储，并将呼叫名片的存储地址发送给主叫应用服务器。

方式 3:

本方式中，网络鉴权服务器获取到待显示数据以及呼叫名片的排版方式的情况下，网络鉴权服务器按照呼叫名片的排版方式对待显示数据进行排版以生成呼叫名片。然后，网络鉴权服务器将该呼叫名片发送给主叫应用服务器。其中，网络鉴权服务器向主叫应用服务器发送该呼叫名片方式可为，网络鉴权服务器将所述呼叫名片存储至文件服务器，网络鉴权服务器将呼叫名片的存储地址发送给主叫应用服务器，所述主叫应用服务器即可根据该地址从文件服务器下载该呼叫名片。

采用本实施例所示的方法，企业内部的第一用户向企业外部的第二用户呼叫时，先执行注册处理流程，基于该注册处理流程，主叫应用服务器能够成功地获取到呼叫名片，以便于后续第一用户呼叫第二用户时，主叫应用服务器能够将该呼叫名片发送至第二用户，无需在呼叫的过程中执行生成呼叫名片的步骤，缩短了呼叫处理的时延，提高了呼叫效率，以使在第一用户呼叫第二用户的过程中，该呼叫名片能够显示于第二终端上。

而且基于本实施例所示的方法，在第一终端执行注册处理流程的过程中，实现了信任安全联盟所示的企业鉴权第一用户的过程。其中，为保证第一用户向第二用户所发送的呼叫名片的安全性，则本申请所示能够创建信任安全联盟，该信任安全联盟是指，主叫运营商网络鉴权企业，企业鉴权第一用户（可以理解，该第一用户为该企业的员工），可见，若企业被主叫运营商网络鉴权通过，第一用户被企业鉴权通过，那么，主叫运营商网络可信任来自企业的数据，企业可信任来自第一用户的数据，主叫运营商网络基于可信任的来自企业的数据即可构造可信任的呼叫名片，从而保证主叫运营商网络向第二用户所发送的呼

叫名片的可信性。

需明确的是，上述对信任安全联盟所包括的对象的说明为可选地示例，不做限定，例如，该信任安全联盟还可指，主叫运营商网络鉴权第三方网络，第三方网络鉴权企业，企业鉴权第一用户，其中，该第三方网络可为企业租用的用于执行呼叫相关业务的网络，例如，该第三方网络可为软件即服务（software-as-a-service SaaS）平台。可见，若第三方网络被主叫运营商网络鉴权通过，企业被第三方网络鉴权通过，第一用户被企业鉴权通过，那么，主叫运营商网络可信任来自第三方网络的数据，第三方网络可信任来自企业的数据，企业可信任来自第一用户的数据，主叫运营商网络基于可信任的来自第三方网络的数据即可构造可信任的呼叫名片，从而保证主叫运营商网络向第二用户所发送的呼叫名片的可信性。

而且本实施例所示的方法，因主叫运营商网络鉴权企业，那么，网络鉴权服务器信任来自企业鉴权服务器的数据（如部分或全部待显示数据），那么，无需第一用户在主叫运营商网络开户的情况下，即可使用主叫运营商网络提供的呼叫第二用户的业务，可见，本实施例所示的方法，第一用户能够在免开户的情况下实现对第二用户的呼叫，解决企业租用主叫运营商网络存在的企业员工（即第一用户）开户问题，从而避免了第一用户在主叫运营商网络开户所导致的第一用户上线慢，第一用户的个人隐私信息暴露的问题。

实施例二

本实施例说明基于图 2 所示的方法，在第一用户已注册至主叫运营商网络的情况下，第一用户如何使用第一终端实现对第二终端的呼叫。具体参见图 3 所示。

图 3 为本申请所提供的主叫通信系统执行呼叫的一种实施例步骤流程图。

步骤 301、第一终端向第一呼叫设备发送第一呼叫请求消息。

本实施例所示的第一呼叫设备用于对该第一呼叫请求消息进行主叫侧验证，第一呼叫设备能够根据已通过主叫侧验证的第一呼叫请求消息触发第一用户对第二用户的呼叫。

本实施例所示的第一呼叫设备为主叫运营商网络所包括的主叫 S-CSCF 为例进行示例性说明，在其他示例中，该第一呼叫设备可为主叫运营商网络所包括的任一设备，或，该第一呼叫设备所执行的功能，可由主叫运营商网络所包括的至少两个设备执行，具体在本实施例中不做限定。

所述第一呼叫请求消息为 SIP INVITE 消息，该第一呼叫请求消息基于控制面传输，其中，第一呼叫请求消息基于控制面传输是指，该第一呼叫请求消息为通过 SIP 协议传输的信令流。

该 SIP INVITE 消息包括所述第一用户的第一用户标识和呼叫鉴权标识，对第一用户标识和呼叫鉴权标识的说明，请参见实施例一所示的对第一用户的用户标识和注册鉴权标识的说明，具体不做赘述。

以下对第一终端向主叫 S-CSCF 发送第一呼叫请求消息的过程进行说明：

第一终端向主叫 P-CSCF 发送该 SIP INVITE 消息，主叫 P-CSCF 按照 SIP 用户始发呼叫的标准流程（参见 3GPP TS 24.229 和 3GPP TS 26.114）处理该 SIP INVITE 消息后转发给

主叫 S-CSCF。

本实施例所示的 SIP INVITE 消息的格式示例可参见如下所示：

INVITE tel:+86139XXXXXXXXX

From: <sip: zhangsan%40xxx.com@2b.ims.<operator>.com>

5 To: <tel:+86139XXXXXXXXX>

Authorization: Bearer <Base64(<token>)>

其中，“+86139XXXXXXXXX”为第二用户的号码。本实施例所示的第一用户标识 UserID 以 zhangsan@xxx.com 为例，本示例通过 SIP 用户标识携带第一用户标识，该 SIP 用户标识可为 zhangsan@xxx.com@2b.ims.<operator>.com，其中，2b.ims.<operator>.com 为主
10 叫运营商网络为基于异构标识（即第一用户标识）接入主叫运营商网络的统一定义的固定域名。

因 SIP 协议所规定的消息中不能够包括两个“@”，则第一终端可对 UserID（如 zhangsan@xxx.com）中的“@”进行转义，本实施例对转义的具体规则的说明为可选地示例，不做限定，例如，第一终端将 UserID 中的“@”转义为“%40”。

15 本实施例所示的 token 可使用基于 64 个可打印字符来表示二进制数据（Base64）的编码格式，该 token 可通过授权（Authorization）头域和扩展的鉴权方式（如 Bearer）携带，如消息格式可为：Authorization: Bearer <Base64(<token>)>。

步骤 302、第一呼叫设备判断呼叫鉴权标识是否满足预设条件，若否，则执行步骤 303，若是，则执行步骤 304。

20 本实施例所示以第一呼叫设备为主叫运营商网络所包括的主叫 S-CSCF 执行步骤 302 为例进行示例性说明，在其他示例中，也可由主叫运营商网络所包括的其他任一设备执行本实施例所示的步骤 302，对执行主体的说明，请参见上述步骤 301 所示，具体不做赘述。

本实施例所示的预设条件为所述呼叫鉴权标识和目标鉴权标识相同，且所述目标鉴权标识有效，可知，在主叫 S-CSCF 判断出呼叫鉴权标识满足预设条件的情况下，主叫 S-CSCF
25 即可确定该第一呼叫请求消息通过主叫侧验证。其中，该目标鉴权标识为所述主叫 S-CSCF 在实施例一所示的注册阶段所缓存的注册鉴权标识。

若所述主叫 S-CSCF 判断呼叫鉴权标识和目标鉴权标识相同，且所述目标鉴权标识有效，确定该呼叫鉴权标识满足该预设条件。

步骤 303、第一呼叫设备拒绝第一呼叫请求消息所请求的呼叫。

30 执行步骤 303 的第一呼叫设备的说明，请参见步骤 302 所示，具体不做赘述。

在所述主叫 S-CSCF 拒绝第一呼叫请求消息所请求的呼叫的情况下，所述第一用户无法基于该第一呼叫请求消息实现对第二用户的呼叫。

步骤 304、第一呼叫设备向第二呼叫设备发送第一呼叫请求消息。

本实施例所示的第一呼叫设备在确定第一呼叫请求消息经过主叫侧验证后，即可对该
35 第一呼叫请求消息进行处理，并将处理后的第一呼叫请求消息发送给第二呼叫设备，该第二呼叫设备为被叫运营商网络所包括的任一设备或该第二呼叫设备可为被叫运营商网络所包括的至少两个设备实现，具体不做限定。执行本实施例所示的步骤 304 的第一呼叫设备

可为主叫运营商网络所包括的主叫 S-CSCF 等任一设备，对执行主体的说明，可参见上述步骤所示，具体不做赘述。

以下对第一呼叫设备向第二呼叫设备发送第一呼叫请求消息的具体过程进行说明：

可知，在步骤 303 中，作为第一呼叫设备的主叫 S-CSCF 已确定第一呼叫请求消息经过主叫侧验证后，主叫 S-CSCF 对该第一呼叫请求消息进行处理，主叫 S-CSCF 可将处理后的第一呼叫请求消息发送至第二呼叫设备。

其中，主叫 S-CSCF 对该第一呼叫请求消息进行处理具体处理过程如下：

本实施例中，主叫 S-CSCF 可从安全密钥存储 (secure key store, SKS) 获取私钥。主叫 S-CSCF 获取第一呼叫请求消息的呼叫数据，并基于该私钥对呼叫数据进行签名以获取第一签名信息，其中，呼叫数据可包括第一用户的标识，第二用户的标识，第一终端的网际互连协议 (internet protocol, IP) 地址和端口号等，该呼叫数据用于创建第一呼叫设备和第二呼叫设备之间的媒体通道。本实施例所示的主叫 S-CSCF 可将该第一签名信息设置在第一呼叫请求消息的头消息中。

具体地，创建第一呼叫设备和第二呼叫设备之间的媒体通道是指，第一呼叫设备通过该第一呼叫请求消息向第二呼叫设备发送用于创建媒体通道的第一终端的网际互连协议 (internet protocol, IP) 地址和端口号。第二呼叫设备根据该第一呼叫请求消息，向第一呼叫设备返回用于创建媒体通道的第二终端的 IP 地址和端口号，基于第一终端的 IP 地址和端口号，以及第二终端的 IP 地址和端口号，能够创建第一呼叫设备和第二呼叫设备之间的媒体通道，即该媒体通道的一端为第一呼叫设备的 IP 地址和端口号，媒体通道的另一端为第二呼叫设备的 IP 地址和端口号，基于该媒体通道实现第一呼叫设备和第二呼叫设备之间的媒体面信息的传输。

其中，该媒体面信息是指采用媒体面协议封装的报文，该媒体面协议可为安全实时传输协议 (securereal-time transport protocol, SRTP) 或实时传输协议 (real-time transport protocol, RTP) 等。

本实施例所示的主叫 S-CSCF 还可在第一呼叫请求消息中设置第一指示消息，该第一指示消息用于请求签名密钥，该签名密钥为用于对呼叫名片进行签名的密钥。

可选地，本实施例所述的第一指示消息还可用于指示所述第一呼叫设备支持对呼叫名片签名的能力。例如，本实施例所示的第一指示消息可为 “Supported: early-media-authentication-with-shaken”。在第二呼叫设备接收到该第一指示消息的情况下，即可根据该第一指示消息确定第一呼叫设备向第二呼叫设备请求签名密钥，而且第一呼叫设备支持对呼叫名片签名的能力。

可选地，本实施例所示的第一呼叫请求消息还包括认证等级信息，本实施例所示的主叫 S-CSCF 预先创建第一用户的标识与认证等级信息的对应关系，在主叫 S-CSCF 接收到第一用户的标识的情况下，即可确定对应的认证等级信息。其中，认证等级信息可包括 A 级等级信息，B 级等级信息以及 C 级等级信息，其中，A 级等级信息，B 级等级信息以及 C 级等级信息表示第一用户的可信度依次降低。

以下对第一呼叫设备向第二呼叫设备发送该处理后的第一呼叫请求消息的过程进行示

例性说明：

本实施例中，主叫 S-CSCF 将第一呼叫请求消息的目的 IP 地址设置为第二呼叫设备的 IP 地址，将第一呼叫请求消息的目的端口号设置有第二呼叫设备的端口号，主叫 S-CSCF 根据第一呼叫请求消息所携带的目的 IP 地址和目的端口号向第二呼叫设备发送第一呼叫请求消息，以实现第一呼叫设备向第二呼叫设备发送第一呼叫请求消息的目的。

步骤 305、第二呼叫设备向第二终端发送第一呼叫请求消息。

本实施例中，在第二呼叫设备确定第一呼叫请求消息经过被叫侧验证后，再将该经过被叫侧验证的第一呼叫请求消息发送至第二终端。本实施例所示的第二呼叫设备可为被叫运营商网络所包括的任一设备，例如，该第二呼叫设备可为被叫运营商网络所包括的被叫 S-CSCF、被叫应用服务器或被叫 P-CSCF 等任一设备，对被叫运营商网络的结构说明，可参见图 1 所示的对主叫运营商网络的结构说明，具体不做赘述。

本实施例以第二呼叫设备为被叫 S-CSCF 为例进行示例性说明，以下对被叫 S-CSCF 实现对第一呼叫请求消息的被叫侧验证的过程进行说明：

被叫 S-CSCF 接收该第一呼叫请求消息后，被叫 S-CSCF 根据已获取的公钥对第一呼叫请求消息所包括的第一签名信息进行签名验证，该公钥为经过证书中心（certificate authority, CA）认证后的公钥。

若被叫 S-CSCF 确定该第一签名信息通过签名验证，则被叫 S-CSCF 确定所述第一呼叫请求消息经过被叫侧验证。在被叫 S-CSCF 确定该第一签名信息通过签名验证后，说明该呼叫数据为未经篡改而且完整的数据。

被叫 S-CSCF 确定第一呼叫请求消息经过被叫侧验证后，被叫 S-CSCF 通过被叫 P-CSCF 向第二终端发送所述第一呼叫请求消息。

具体地，被叫 S-CSCF 将第一呼叫请求消息的 IP 地址设置为被叫 P-CSCF 的 IP 地址，再将目的端口号设置为被叫 P-CSCF 的端口号，被叫 S-CSCF 根据第一呼叫请求消息所携带的目的 IP 地址和目的端口号向被叫 P-CSCF 发送第一呼叫请求消息。该第一呼叫请求消息携带第二终端的标识，被叫 P-CSCF 根据第二终端的标识获取对应的第二终端的 IP 地址和端口号，被叫 P-CSCF 将第一呼叫请求消息的目的 IP 地址设置为第二终端的 IP 地址，再将第一呼叫请求消息的目的端口号修改为第二终端的端口号，被叫 P-CSCF 根据第一呼叫请求消息所携带的目的 IP 地址和目的端口号，向第二终端发送该第一呼叫请求消息。

步骤 306、第二终端向第二呼叫设备发送 180 振铃消息。

在第二终端已成功接收到第一呼叫请求消息的情况下，该第二终端可根据该第一呼叫请求消息振铃，第二终端成功振铃的情况下，可向第二呼叫设备发送 180 振铃消息，以通知该第二终端已振铃。

第二终端向第二呼叫设备发送 180 振铃消息的过程，可参见第二呼叫设备向第二终端发送第一呼叫请求消息的过程，具体不做赘述。

本实施例中，在第一呼叫请求消息已携带认证等级信息的情况下，则第二终端可显示该认证等级信息。例如，若第一呼叫请求消息携带 A 级等级信息，那么，第二终端可在振铃的同时显示该 A 级等级信息。

本实施例所示的 180 振铃消息还携带第二终端的 IP 地址和端口号，以实现第一呼叫设备和第二呼叫设备之间的媒体通道的创建。

步骤 307、第二呼叫设备向第一呼叫设备发送 180 振铃消息。

5 本实施例所示的第二呼叫设备接收到该 180 振铃消息后，可对该 180 振铃消息进行处理，并将处理后的 180 振铃消息转发给第一呼叫设备。

具体地，第二呼叫设备将主密钥（S-key）和主盐密钥（S-salt）设置于 180 振铃消息中。本实施例所示的所述主密钥和所述主盐密钥为用于 SRTP 所需要的密钥。

10 本实施例中，第二呼叫设备可在本步骤 307 所示的，在第二呼叫设备接收到 180 振铃消息的情况下获取该主密钥和主盐密钥，或者，第二呼叫设备可在接收到来自第一呼叫设备的第一呼叫请求消息的情况下，获取该主密钥和主盐密钥，具体在本实施例中不做限定，本实施例以第二呼叫设备在接收到第一呼叫请求消息的情况下获取该主密钥和主盐密钥为例，以下对第二呼叫设备获取该主密钥和主盐密钥的过程进行说明：

15 首先，第二呼叫设备确定第一呼叫请求消息已携带该第一指示消息，由步骤 304 所示可知，该第一指示消息用于请求签名密钥。第二呼叫设备根据该第一呼叫请求消息确定需要获取用于 SRTP 的主密钥和主盐密钥。

其次，第二呼叫设备基于 SRTP 密钥管理算法获取对应的主密钥和主盐密钥。

本实施例所示的第二呼叫设备为保证向第一呼叫设备所传输的主密钥和主盐密钥的安全，第二呼叫设备可基于已存储的公钥对主密钥和主盐密钥进行签名以获取第二签名信息。第二呼叫设备将该第二签名信息设置于 180 振铃消息中。

20 本实施例所示的第二呼叫设备还可在 180 振铃消息中设置第二指示消息，其中，所述第二指示消息用于指示第二呼叫设备支持验证所述待显示数据安全性的能力。可知，第一呼叫设备在接收到该第二指示消息的情况下，即可将签名后的呼叫名片发送给第二呼叫设备。第一呼叫设备和第二呼叫设备基于该第一指示消息和第二指示消息的协商，能够实现第二终端显示经由第一呼叫设备签名和经由第二呼叫设备对呼叫名片进行签名验证的目的。

25 本实施例所示的第二呼叫设备还可在 180 振铃消息中设置第二呼叫设备的地址，其中，该第二呼叫设备的地址包括第二呼叫设备的 IP 地址以及端口号。

30 本实施例中，在第二呼叫设备接收到来自第一呼叫设备的第一呼叫请求消息的情况下，第二呼叫设备能够获取第一呼叫请求消息所携带的第一终端的 IP 地址和端口号。在第一呼叫设备接收到该 180 振铃消息的情况下，第一呼叫设备能够获取第二终端的 IP 地址和端口号，基于第一终端的 IP 地址和端口号，以及第二终端的 IP 地址和端口号，能够创建第一呼叫设备和第二呼叫设备之间的媒体通道。

步骤 308、第一呼叫设备向第一终端发送 180 振铃消息。

35 所述第一呼叫设备接收到该 180 振铃消息后，即可向第一终端发送该 180 振铃消息，第一呼叫设备向第一终端发送 180 振铃消息的过程，可参见第二呼叫设备向第二终端发送第一呼叫请求消息的过程，具体不做赘述。本实施例所示的 180 振铃消息可携带第一用户的标识，以保证第一呼叫设备能够基于该第一用户的标识获取第一终端的 IP 地址和端口号，以向第一终端发送该 180 振铃消息。第一终端根据该 180 振铃消息确定第二终端已成功接

收到第一呼叫请求消息，且该第二终端已振铃。

步骤 309、第一呼叫设备获取签名密钥。

具体地，第一呼叫设备接收到 180 振铃消息后，从 180 振铃消息中提取出第二签名信息。第一呼叫设备基于私钥对第二签名信息进行签名验证以获取所述第二签名信息所携带的所述主密钥和所述主盐密钥。第一呼叫设备通过密钥推导函数对所述主密钥和所述主盐密钥进行计算以获取签名密钥。

步骤 310、第一呼叫设备向第二呼叫设备发送 SRTP 协议报文。

本实施例所示的第一呼叫设备能够获取呼叫名片，具体说明请参见实施例一所示，具体不做赘述。

为更好地理解，以下结合表 1 所示对 SRTP 协议报文的结构进行说明：

表 1

V	P	X	CC	M	PT	序 列 号
时间戳						
同步信源标识符 (synchronizing source identifier, SSRC)						
特约信源标识符 (contributing source identifiers, CSRC)						
载荷 (payload)						
身份验证标签 (authentication tag)						
.....						

其中，V 表示版本号，P 表示填充位，X 表示扩展位，CC 表示特约信源 (CSRC) 标识符的数目，M 表示用于指示不同有效载荷含义的标记，PT 表示有效载荷类型。

本实施例所示的 SRTP 协议报文的 payload 携带呼叫名片，第一呼叫设备基于签名密钥对 payload 进行签名以获取第一验证签名信息，该第一验证签名信息作为表 1 所示的身份验证标签 (authentication tag)。

上述所示的 180 振铃消息已携带第二呼叫设备的地址，第一呼叫设备根据第二呼叫设备的地址，向第二呼叫设备发送该 SRTP 协议报文。可知，由于本实施例所示的 SRTP 协议报文是基于 SRTP 协议传输的报文，该 SRTP 协议报文在第一呼叫设备和第二呼叫设备之间基于媒体通道传输。

步骤 311、第二呼叫设备向第二终端发送呼叫名片。

第二呼叫设备将来自第一呼叫设备的 SRTP 协议报文转发给第二呼叫设备，第二呼叫设备可从 SRTP 协议报文中获取第二终端的 IP 地址和端口号，第二呼叫根据 SRTP 协议报文所携带的第二终端的 IP 地址和端口号，向第二终端发送呼叫名片。

步骤 312、第二终端显示该呼叫名片。

可知，本实施例所示的第二终端能够在振铃的过程中，且在第二终端支持视频通话功能的情况下，所述第二终端显示该呼叫名片。

步骤 313、第二呼叫设备判断呼叫名片是否通过安全性验证，若是，则执行步骤 314，若否，则执行步骤 315。

所述第二呼叫设备从 SRTP 协议报文中获取到呼叫名片后，所述第二呼叫设备判断该呼叫名片是否通过安全性验证，以下对所述第二呼叫设备如何判断该呼叫名片是否通过安全性验证的过程进行说明：

所述第二呼叫设备通过该签名密钥对呼叫名片进行签名以获取第二验证签名信息，若
5 所述第二呼叫设备判断 SRTP 协议报文所携带的第一验证签名信息和第二验证签名信息相同，则确定呼叫名片通过安全性验证，则执行步骤 314。若所述第二呼叫设备判断 SRTP 协议报文所携带的第一验证签名信息和第二验证签名信息不相同，则确定呼叫名片未通过安全性验证，则执行步骤 315。

步骤 314、第二呼叫设备向第二终端发送第一通知信息。

10 在所述第二呼叫设备确定呼叫名片通过安全性验证，则向第二终端发送用于指示呼叫名片通过安全性验证的第一通知信息，第二终端接收到该第一通知信息后，即可显示该第一通知信息，以保证第二用户根据第二终端已显示的第一通知信息，确定所显示的呼叫名片是安全的。

本实施例对第一通知信息的类型不做限定，该第一通知信息的类型可为文本信息，语
15 音信息，或视频信息等，具体不做限定。

步骤 315、第二呼叫设备向第二终端发送第二通知信息。

在所述第二呼叫设备确定呼叫名片未通过安全性验证，则向第二终端发送用于指示呼
20 叫名片未通过安全性验证的第二通知信息，第二终端接收到该第二通知信息后，即可显示该第二通知信息，以保证第二用户根据第二终端已显示的第二通知信息，确定所显示的呼
叫名片是不安全的。

本实施例对步骤 311 和步骤 312 之间的执行时序不做限定。本实施例以先执行步骤 311，
在执行步骤 313 为例进行示例性说明，即第二呼叫设备先向第二终端发送呼叫名片，再判
断呼叫名片是否通过安全性验证。可知，第二终端先对呼叫名片进行显示，而后再接收来
自第二呼叫设备的第一通知信息或第二通知信息，以确定已显示的呼叫名片是否安全。

25 在其他示例中，也可先执行步骤 313，再执行步骤 311，即第二呼叫设备先判断呼叫名片是否通过安全性验证，在第二呼叫设备确定呼叫名片已通过安全性验证的情况下，再将
呼叫名片发送至第二终端，可知，此示例下的第二终端所接收到的呼叫名片为安全的。

本实施例中，在呼叫处理的过程中，因第一用户无需直接在主叫运营商网络开户，则
30 避免第一用户的个人隐私信息在主叫运营商网络处暴露。本实施例所示的第二终端所显示
的呼叫名片所包括的各个信息全部来自企业鉴权服务器和/或网络鉴权服务器，而非第一用
户，避免了呼叫名片存在造假的情况。

而且第二终端所显示的呼叫名片是经过第一呼叫设备签名，第二呼叫设备的签名验证
的，提高了呼叫名片的安全性，避免了呼叫名片出现篡改和泄漏的情况，提高了呼叫名片
的安全和可信。

35 因本实施例所示的呼叫名片基于媒体通道传输，有效地提高了呼叫名片所传输的待显
示数据的数据量，基于媒体通道传输能够实现第一用户跨运营商实现对第二用户呼叫的目
的。

实施例三

实施例二所示的第一用户呼叫第二用户的过程中，需要第一用户预先注册至主叫运营商网络，注册过程如实施例一所示。以下结合图 4 所示对第一用户无需预先注册至主叫运营商网络的情况下，直接实现第一用户呼叫第二用户的过程进行说明。

图 4 为本申请所提供的主叫通信系统执行呼叫的另一种实施例步骤流程图。

步骤 401、第一终端向第一呼叫设备发送第二呼叫请求消息。

在第一用户确定需要呼叫第二用户时，所述第一用户即可通过该第一终端向第一呼叫设备发送第二呼叫请求消息，以触发第一用户对第二用户的呼叫。所述第二呼叫请求消息可为 SIP INVITE 消息，该 SIP INVITE 消息包括所述第一用户的第一用户标识和呼叫鉴权标识，对第一用户标识和呼叫鉴权标识的说明，请参见实施例二所示的对第一用户的第一用户标识和呼叫鉴权标识的说明，具体不做赘述。对第一呼叫设备的具体说明，请参见实施例二所示，具体不做赘述。

步骤 402、第一呼叫设备向企业鉴权服务器发送呼叫鉴权请求。

本实施例以第一呼叫设备为主叫 S-CSCF 为例，主叫 S-CSCF 向主叫应用服务器发送第二呼叫请求消息。其中，若主叫 S-CSCF 确定该第二呼叫请求消息所包括的呼叫鉴权标识与目标鉴权标识相同，而且主叫 S-CSCF 判断第二呼叫请求消息使用 Bearer 的鉴权方式时，所述主叫 S-CSCF 向网络鉴权服务器发送包括第一用户标识和呼叫鉴权标识的第二呼叫请求消息，以请求网络鉴权服务器利用呼叫鉴权标识对第一用户进行鉴权。对呼叫鉴权标识和 Bearer 的鉴权方式的具体说明，请详见实施例二所示，具体不做赘述。

本实施例所示的网络鉴权服务器接收到来自主叫 S-CSCF 的第一用户标识和呼叫鉴权请求后，向企业鉴权服务器发送鉴权请求的过程的说明，请参见实施例一的步骤 205 所示，具体不做赘述。

步骤 403、企业鉴权服务器判断呼叫鉴权标识是否有效，若否，则执行步骤 404，若是，则执行步骤 405。

本实施例所示的步骤 504 的具体执行过程，请参见实施例二的步骤 206 所示，具体不做赘述。

步骤 404、企业鉴权服务器向第一呼叫设备发送呼叫鉴权标识无效通知。

具体地，本实施例所示的企业鉴权服务器可向第一呼叫设备发送该呼叫鉴权标识无效通知，具体执行过程的说明，可参加实施例一的步骤 207 所示，具体不做赘述。

步骤 405、企业鉴权服务器向第一呼叫设备发送呼叫鉴权成功指示。

具体地，本实施例所示的企业鉴权服务器可向第一呼叫设备发送该呼叫鉴权成功指示，具体执行过程的说明，可参加实施例一的步骤 208 所示，具体不做赘述。

步骤 406、第一呼叫设备获取待显示数据。

本实施例所示的第一呼叫设备获取该待显示数据的过程，可参加实施例一所示的步骤 209 至步骤 210 所示，具体不做赘述。

步骤 407、第一呼叫设备向第二呼叫设备发送第二呼叫请求消息。

- 21 -

步骤 408、第二呼叫设备向第二终端发送第二呼叫请求消息。

步骤 409、第二终端向第二呼叫设备发送 180 振铃消息。

步骤 410、第二呼叫设备向第一呼叫设备发送 180 振铃消息。

步骤 411、第一呼叫设备向第一终端发送 180 振铃消息。

5 步骤 412、第一呼叫设备获取签名密钥。

步骤 413、第一呼叫设备向第二呼叫设备发送 SRTP 协议报文。

步骤 414、第二呼叫设备向第二终端发送呼叫名片。

步骤 415、第二终端显示该呼叫名片。

10 步骤 416、第二呼叫设备判断呼叫名片是否通过安全性验证，若是，则执行步骤 417，
若否，则执行步骤 418。

步骤 417、第二呼叫设备向第二终端发送第一通知信息。

步骤 418、第二呼叫设备向第二终端发送第二通知信息。

本实施例所示的步骤 407 至步骤 418 的执行过程，请参见实施例二所示的步骤 304 至步骤 315 所示，具体不做赘述。

15 本实施例中，第一用户在对第二用户进行呼叫的过程中，第一用户无需预先注册至运营商网络，避免在第一用户呼叫第二用户的过程中，需要预先进行注册的步骤，提高了第一用户呼叫第二用户的效率，同时减少了注册相关资源的消耗。

20 而且在主叫运营商网络、企业、企业员工（第一用户）之间建立信任安全联盟，可保证第二终端振铃时，所显示的呼叫名片的信息是安全的，而且呼叫名片满足呼叫名片的排版方式，以保证呼叫名片所呈现的各项信息能够符合企业定制的需求，且呼叫名片的风格统一。

25 在呼叫处理的过程中，因第一用户无需直接在运营商网络开户，则避免第一用户的个人隐私信息在主叫运营商处暴露，而且在对第二用户进行呼叫的过程中，呼叫名片所显示的信息也可不涉及第一用户的个人隐私信息，有效地保证了第一用户的个人隐私信息的安全。

本实施例所示的第二终端所显示的呼叫名片所包括的各个信息全部来自企业鉴权服务器和/或网络鉴权服务器，而非第一用户，如果呼叫名片存在造假的问题，则可以基于信任安全联盟形成的信任链进行溯源和追责。

30 实施例四

实施例二所示的第一呼叫设备通过向第二呼叫设备发送 SRTP 协议报文的方式，以使第二终端显示呼叫名片。而本实施例所示的第一呼叫可不基于 SRTP 协议，实现呼叫名片的传输，本实施例所示的方法基于图 2 所示的方法，在第一用户已注册至主叫运营商网络的情况下，第一用户如何使用第一终端实现对第二终端的呼叫。具体参见图 5 所示。

35 图 5 为本申请所提供的主叫通信系统执行呼叫的另一种实施例步骤流程图。

步骤 501、第一终端向第一呼叫设备发送第一呼叫请求消息。

步骤 502、第一呼叫设备判断呼叫鉴权标识是否满足预设条件，若否，则执行步骤 503，

— 22 —

若是，则执行步骤 504。

步骤 503、第一呼叫设备拒绝第一呼叫请求消息所请求的呼叫。

步骤 504、第一呼叫设备向第二呼叫设备发送第一呼叫请求消息。

步骤 505、第二呼叫设备向第二终端发送第一呼叫请求消息。

5 步骤 506、第二终端向第二呼叫设备发送 180 振铃消息。

步骤 507、第二呼叫设备向第一呼叫设备发送 180 振铃消息。

步骤 508、第一呼叫设备向第一终端发送 180 振铃消息。

本实施例所示的步骤 501 至步骤 508 的执行过程的说明，请参见实施例二所示的步骤 301 至步骤 308 所示，具体执行过程不做赘述。

10 步骤 509、第一呼叫设备获取签名密钥。

本实施例所示的验证签名可参见实施例二所示的步骤 309 所示，可选地，本实施例所示的签名密钥还可为主叫运营商网络根据预先选定的安全散列算法（secure hash algorithm, SHA）所包括的任一算法导出，例如，本实施例所示的签名密钥为主叫运营商网络根据预先选定的算法 SHA1 导出。

15 步骤 510、第一呼叫设备向第二呼叫设备发送媒体报文。

本实施例所示的媒体报文可采用实时传输协议（real-time transport protocol, RTP）。RTP 协议为语音、图像、传真等多种多媒体数据提供端到端的实时传输服务。本实施例所示的媒体报文可包括呼叫名片，主叫运营商网络（如主叫运营商网络所包括的主叫媒体服务器）基于签名密钥对呼叫名片进行签名以获取第一验证签名信息，并将该第一验证签名信息设置于媒体报文中。本实施例以 RTP 协议为例进行示例性说明，不做限定，在其他示

20 例中，可采用任一媒体面协议传输呼叫名片和签名。

步骤 511、第二呼叫设备向第二终端发送呼叫名片。

步骤 512、第二终端显示该呼叫名片。

步骤 513、第二呼叫设备判断呼叫名片是否通过安全性验证，若是，则执行步骤 514，

25 若否，则执行步骤 515。

步骤 514、第二呼叫设备向第二终端发送第一通知信息。

步骤 515、第二呼叫设备向第二终端发送第二通知信息。

本实施例所示的步骤 511 至步骤 515 的执行过程的说明，请参见步骤 311 至步骤 315 所示，具体不做赘述。

30 本申请所示的第一用户也可无需预先注册至主叫运营商网络的情况下，直接实现第一用户呼叫第二用户的过程，具体执行过程可参见实施例三所示，实施例三所示的签名密钥可为本实施例所示的 SHA 所包括的任一算法，具体过程不做赘述。

实施例五

35 上述实施例中，以第一呼叫设备为主叫运营商网络所包括的设备，第二呼叫设备为被叫运营商网络所包括的设备为例，说明第一用户向第二用户呼叫的过程。本实施例结合图 6 所示以第一呼叫设备为第一用户所使用的第一终端，第二呼叫设备为第二用户所使用的

第二终端为例，说明第一终端实现对呼叫名片的签名过程，以第二终端实现呼叫名片的签名验证过程，以实现第一用户呼叫第二用户为例进行示例性说明：

图 6 为本申请所提供的主叫通信系统执行呼叫的另一种实施例步骤流程图。

步骤 601、第一终端向主叫运营商网络发送第三呼叫请求消息。

5 本实施例所示的第三呼叫请求消息的具体说明，可参见实施例二的步骤 301 所示，具体不做赘述，本实施例所示的第三呼叫请求消息还包括第一签名信息，该第一签名消息的具体说明可如下所示：

10 第一终端可获取私钥。第一终端获取呼叫数据，并基于该私钥对呼叫数据进行签名以获取第一签名信息，其中，呼叫数据可包括第一用户的标识，第二用户的标识等，该呼叫数据用于创建第一终端和第二终端之间的媒体通道传输。本实施例所示的第一终端可将该第一签名信息设置在第三呼叫请求消息的头消息中。对获取该第一签名消息的具体说明，也可参见实施例一的步骤 304 所示，具体不做赘述。

15 本实施例所示的第三呼叫请求消息还包括第一指示消息，该第一指示消息用于请求签名密钥，该签名密钥为用于对呼叫名片进行签名的密钥，对第一指示消息的具体说明，可参见实施例一的步骤 304 所示，具体不做赘述。

步骤 602、主叫运营商网络判断呼叫鉴权标识是否满足预设条件，若否，则执行步骤 603，若是，则执行步骤 604。

步骤 603、主叫运营商网络拒绝第三呼叫请求消息所请求的呼叫。

步骤 604、主叫运营商网络向被叫运营商网络发送第三呼叫请求消息。

20 本实施例所示的步骤 602 至步骤 604 的执行过程的说明，请参见实施例二的步骤 302 至步骤 304 所示，具体不做赘述。

步骤 605、被叫运营商网络向第二终端发送第三呼叫请求消息。

步骤 606、第二终端确定第三呼叫请求消息通过被叫侧验证后，向被叫运营商网络发送 180 振铃消息。

25 本实施例所述的第二终端接收到第三呼叫请求消息后，对第三呼叫请求消息进行被叫侧验证，在确定第三呼叫请求消息通过被叫侧验证后，向被叫运营商网络发送 180 振铃消息。以下对第二终端如何实现对第三呼叫请求消息进行被叫侧验证的过程进行说明：

30 第二终端根据已获取的公钥对第三呼叫请求消息所包括的第一签名信息进行签名验证，该公钥的说明可参见实施例二所示，具体不做赘述。若第二终端第一签名信息通过签名验证后，第二终端确定第三呼叫请求消息所携带的呼叫数据为未经篡改而且完整的数据。

本实施例所示的 180 振铃消息的具体说明，请参见实施例二的步骤 306 所示，具体不做赘述。

步骤 607、被叫运营商网络向主叫运营商网络发送 180 振铃消息。

步骤 608、主叫运营商网络向第一终端发送 180 振铃消息。

35 步骤 609、第一终端获取签名密钥。

本实施例所示的第一终端获取签名密钥的过程，可参见实施例二的步骤 309 所示的主叫运营商网络获取签名密钥的过程，具体不做赘述。

— 24 —

步骤 610、第一终端向主叫运营商网络发送 SRTP 协议报文。

具体地，本实施例所示的第一终端获取呼叫名片，第一终端通过该 SRTP 协议报文携带该呼叫名片。本实施例所示的第一终端获取 SRTP 协议报文的具体过程，可参见实施例二的步骤 310 所示的主叫运营商网络获取该 SRTP 协议报文的过程，具体不做赘述。

5 步骤 611、主叫运营商网络向被叫运营商网络发送 SRTP 协议报文。

步骤 612、被叫运营商网络向第二终端发送呼叫名片。

步骤 613、第二终端显示该呼叫名片。

本实施例所示的步骤 613 的执行过程的说明，请参见实施例二所示的步骤 312 所示，具体不做赘述。

10 步骤 614、第二终端判断呼叫名片是否通过安全性验证，若是，则执行步骤 615，若否，则执行步骤 616。

本实施例所示的第二终端判断呼叫名片是否通过安全性验证的过程，请参见实施例二的步骤 313 所示的被叫运营商服务器判断呼叫名片是否通过安全性验证的过程，具体不做赘述。

15 步骤 615、第二终端显示第一通知信息。

步骤 616、第二终端显示第二通知信息。

本实施例所示的第一通知信息和第二通知信息的说明，请分别参见实施例二的步骤 314 和步骤 315 所示，具体不做赘述。

20 可知，本实施例所示的第一终端负责对呼叫名片进行签名，而第二终端负责对呼叫名片进行签名验证并进行显示，可减少主叫运营商网络和被叫运营商网络的算力资源。而且因本实施例由第一终端和第二终端执行呼叫名片的签名和签名验证过程，则使得第一终端和第二终端可应用至任意类型的运营商网络中，降低了对运营商网络类型的限制。

实施例六

25 实施例五所示的第一用户呼叫第二用户的过程中，需要第一用户预先注册至主叫运营商网络，注册过程如实施例一所示。以下结合图 7 所示对第一用户无需预先注册至主叫运营商网络的情况下，直接实现第一用户呼叫第二用户的过程进行说明，本实施例所示以第一呼叫设备为第一用户所使用的第一终端，第二呼叫设备为第二用户所使用的第二终端为例，具体说明请参见实施例五所示：

30 图 7 为本申请所提供的主叫通信系统执行呼叫的另一种实施例步骤流程图。

步骤 701、第一终端向主叫运营商网络发送第四呼叫请求消息。

35 在第一用户确定需要呼叫第二用户时，所述第一用户即可通过该第一终端向主叫运营商网络发送第四呼叫请求消息，以触发第一用户对第二用户的呼叫。所述第四呼叫请求消息可为 SIP INVITE 消息，该 SIP INVITE 消息包括所述第一用户的第一用户标识和呼叫鉴权标识，对第一用户标识和呼叫鉴权标识的说明，请参见实施例二所示的对第一用户的第一用户标识和呼叫鉴权标识的说明，具体不做赘述。

本实施例所示的第四呼叫请求消息还包括第一签名信息，可选地，该第四呼叫请求消

— 25 —

息还包括第一指示消息，对第一签名消息和第一指示消息的说明，请参见实施例五的步骤 601 所示，具体不做赘述。

步骤 702、主叫运营商网络向企业鉴权服务器发送呼叫鉴权请求。

步骤 703、企业鉴权服务器判断呼叫鉴权标识是否有效，若否，则执行步骤 704，若是，
5 则执行步骤 705。

步骤 704、企业鉴权服务器向第一终端发送呼叫鉴权标识无效通知。

步骤 705、企业鉴权服务器向第一终端发送呼叫鉴权成功指示。

步骤 706、第一终端获取待显示数据。

本实施例所示的第一终端获取该待显示数据的过程，可参见实施例一所示的步骤 209
10 至步骤 210 所示，具体不做赘述。

步骤 707、主叫运营商网络向被叫运营商网络发送第四呼叫请求消息。

步骤 708、被叫运营商网络向第二终端发送第四呼叫请求消息。

步骤 709、第二终端向被叫运营商网络发送 180 振铃消息。

步骤 710、被叫运营商网络向主叫运营商网络发送 180 振铃消息。

15 步骤 711、主叫运营商网络向第一终端发送 180 振铃消息。

步骤 712、第一终端获取签名密钥。

步骤 713、第一终端向主叫运营商网络发送 SRTP 协议报文。

步骤 714、主叫运营商网络向被叫运营商网络发送 SRTP 协议报文。

步骤 715、被叫运营商网络向第二终端发送呼叫名片。

20 步骤 716、第二终端显示该呼叫名片。

步骤 717、第二终端判断呼叫名片是否通过安全性验证，若是，则执行步骤 718，若否，
则执行步骤 719。

步骤 718、第二终端显示第一通知信息。

步骤 719、第二终端显示第二通知信息。

25 本实施例所示的步骤 707 至步骤 719 的执行过程，请参见实施例五所示的步骤 604 至
步骤 616 所示，具体不做赘述。

本实施例中，第一用户在对第二用户进行呼叫的过程中，第一用户无需预先注册至运营商网络，避免在第一用户呼叫第二用户的过程中，需要预先进行注册的步骤，提高了第一用户呼叫第二用户的效率，同时减少了注册相关资源的消耗。而且本实施例所示的第一
30 终端负责对呼叫名片进行签名，而第二终端负责对签名后的呼叫名片进行签名验证并进行显示，可减少主叫运营商网络和被叫运营商网络的算力资源。本实施例由第一终端和第二终端执行呼叫名片的签名和签名验证过程，则使得第一终端和第二终端可应用至任意类型的运营商网络中，降低了对运营商网络类型的限制。

本申请中，实施例五和实施例六所示的呼叫名片也可不基于 SRTP 协议，实现呼叫名片
35 的传输，具体说明可参见实施例四所示，具体不做赘述。

本申请中，对呼叫名片的签名过程，可由第一终端执行，具体说明请参见实施例五和实施例六所示，而对签名后的呼叫名片签名验证的过程，可由第二呼叫设备执行，具体说

明可参见实施例一至实施例四任一实施例所示。又如，对呼叫名片的签名过程，可由第一呼叫设备执行，具体说明可参见实施例一至实施例四任一实施例所示，而对签名后的呼叫名片签名验证的过程，可由第二终端执行，具体说明可参见实施例五或实施例六所示，具体不做赘述。

- 5 需明确的是，在实施例一至实施例六中，运营商网络以 IMS 网络为例，本申请对运营商网络的具体网络类型不做限定，例如，本实施例所示的运营商网络可适用于任意架构的电信网络，具体网络类型在本实施例中不做限定。

实施例七

- 10 本实施例结合图 8 所示对用于执行上述方法实施例的第一呼叫设备的结构进行说明：图 8 为本申请所提供的第一呼叫设备的一种实施例结构示意图。

所述第一呼叫设备包括：

第一获取模块 801，用于获取签名密钥；

- 15 第二获取模块 802，用于获取第一用户的待显示数据，所述第一用户用于所述第一呼叫设备呼叫第二呼叫设备，所述待显示数据包括与所述第一用户对应的信息和/或与所述第一用户所属的企业对应的信息；

签名模块 803，用于通过所述签名密钥对所述待显示数据进行签名以获取第一验证签名信息；

- 20 发送模块 804，用于通过所述第一呼叫设备和所述第二呼叫设备之间的媒体通道，向所述第二呼叫设备发送所述待显示数据以及所述第一验证签名信息，所述第一验证签名信息用于验证所述待显示数据的安全性。

其中，所述签名模块 803 分别与第一获取模块 801 以及第二获取模块 802 连接，且所述签名模块 803 还与发送模块 804 连接。

- 25 可选地，若本实施例所示的第一呼叫设备应用于实施例二中，本实施例所示的第一呼叫设备还包括判断模块 800，所述判断模块 800 用于执行步骤 302 以及步骤 303。其中，所述判断模块 800 与发送模块 804 连接。所述发送模块 804 用于执行步骤 304 以及步骤 308，所述第一获取模块 801 用于执行步骤 309，所述签名模块 803 用于根据来自所述第一获取模块 801 的签名密钥以及来自第二获取模块 802 的待显示数据获取第一验证签名信息，具体说明请参见步骤 310 所示，所述发送模块 804 用于执行步骤 310。

- 30 可选地，若本实施例所示的第一呼叫设备应用于实施例三中，所述发送模块 804 还用于执行步骤 402，所述第二获取模块 802 用于执行步骤 406，所述发送模块 804 用于执行步骤 407 以及步骤 411，所述第一获取模块 801 用于执行步骤 412，所述签名模块 803 用于根据来自所述第一获取模块 801 的签名密钥以及来自第二获取模块 802 的待显示数据获取第一验证签名信息，具体说明请参见步骤 413 所示，所述发送模块 804 用于执行步骤 413。

- 35 可选地，若本实施例所示的第一呼叫设备应用于实施例四中，所述判断模块 800 用于执行步骤 502 以及步骤 503，所述发送模块 804 用于执行步骤 504 以及步骤 508，所述第一获取模块 801 用于执行步骤 509，所述签名模块 803 用于根据来自所述第一获取模块 801

的签名密钥以及来自第二获取模块 802 的待显示数据获取第一验证签名信息，具体说明请参见步骤 510 所示，所述发送模块 804 用于执行步骤 510。

可选地，若本实施例所示的第一呼叫设备应用于实施例五中，所述发送模块 804 用于执行步骤 601，所述第一获取模块 801 用于执行步骤 609，所述签名模块 803 用于根据来自
5 所述第一获取模块 801 的签名密钥以及来自第二获取模块 802 的待显示数据获取第一验证签名信息，具体说明请参见步骤 610 所示，所述发送模块 804 用于执行步骤 610。

可选地，若本实施例所示的第一呼叫设备应用于实施例六中，所述发送模块 804 用于执行步骤 701，所述第一获取模块 801 用于执行步骤 712，所述签名模块 803 用于根据来自
10 所述第一获取模块 801 的签名密钥以及来自第二获取模块 802 的待显示数据获取第一验证签名信息，具体说明请参见步骤 713 所示，所述发送模块 804 用于执行步骤 713。

实施例八

本实施例结合图 9 所示对用于执行上述方法实施例的第二呼叫设备的结构进行说明：

图 9 为本申请所提供的第二呼叫设备的一种实施例结构示意图。

15 所述第二呼叫设备包括：

接收模块 901，用于接收来自第一呼叫设备的待显示数据以及第一验证签名信息，所述第一验证签名信息为通过签名密钥对所述待显示数据进行签名以获取，所述待显示数据和所述第一验证签名信息通过所述第一呼叫设备和所述第二呼叫设备之间的媒体通道传输，所述待显示数据包括与所述第一用户对应的信息和/或与所述第一用户所属的企业对应的
20 信息；

签名模块 902，用于通过所述签名密钥对所述待显示数据进行签名以获取第二验证签名信息；

验证模块 903，用于若确定所述第一验证签名信息和所述第二验证签名信息相同，确定所述待显示数据通过安全性验证，使所述待显示数据显示。

25 其中，所述接收模块 901 分别与所述签名模块 902 和所述验证模块 903 连接。

可选地，若本实施例所示的第二呼叫设备应用于实施例二中，所述第二呼叫设备还包括发送模块 900，所述发送模块 900 可与接收模块 901 连接。所述发送模块 900 用于执行步骤 305 以及步骤 307，所述接收模块 901 用于通过发送模块 900，将已接收的待显示数据发送至第二终端，具体过程请参见步骤 311 所示，所述签名模块 902 和所述验证模块 903，
30 共同用于执行步骤 313，所述发送模块 900 用于执行步骤 314 至步骤 315。

可选地，若本实施例所示的第二呼叫设备应用于实施例三中，所述第二呼叫设备还包括发送模块 900，所述发送模块 900 用于执行步骤 408 以及步骤 410，所述接收模块 901 用于通过发送模块 900，将已接收的待显示数据发送至第二终端，具体过程请参见步骤 414 所示，所述签名模块 902 和所述验证模块 903，共同用于执行步骤 416，所述发送模块 900
35 用于执行步骤 417 至步骤 418。

可选地，若本实施例所示的第二呼叫设备应用于实施例四中，所述第二呼叫设备还包括发送模块 900，所述发送模块 900 用于执行步骤 505 以及步骤 507，所述接收模块 901 用

于通过发送模块 900，将已接收的待显示数据发送至第二终端，具体过程请参见步骤 511 所示，所述签名模块 902 和所述验证模块 903，共同用于执行步骤 513，所述发送模块 900 用于执行步骤 514 至步骤 515。

可选地，若本实施例所示的第二呼叫设备应用于实施例五中，所述第二呼叫设备还包括发送模块 900，所述发送模块 900 用于执行步骤 606，所述接收模块 901 用于接收来自被叫运营商网络的待显示数据，具体执行过程请参见步骤 612 所示，所述签名模块 902 和所述验证模块 903，共同用于执行步骤 614，所述发送模块 900 用于执行步骤 615 至步骤 616。

可选地，若本实施例所示的第二呼叫设备应用于实施例六中，所述第二呼叫设备还包括发送模块 900，所述发送模块 900 用于执行步骤 709，所述接收模块 901 用于接收来自被叫运营商网络的待显示数据，具体执行过程请参见步骤 715 所示，所述签名模块 902 和所述验证模块 903，共同用于执行步骤 717，所述发送模块 900 用于执行步骤 718 至步骤 719。

实施例九

本实施例结合图 10 所示，从实体硬件的角度对用于执行上述方法实施例的呼叫设备的结构进行说明：本实施例所示的呼叫设备可为上述所示的第一呼叫设备或第二呼叫设备。

图 10 为本申请所提供的呼叫设备的一种实施例结构示意图。

呼叫设备 1000 具体包括：处理器 1001、存储器 1002、总线 1003、收发器 1004 以及网络接口 1006。

具体的，存储器 1002 可以包括以易失性和 / 或非易失性存储器形式的计算机存储媒体，如只读存储器和 / 或随机存取存储器。存储器 1002 可以存储操作系统、应用程序、其他程序模块、可执行代码和程序数据。

收发器 1004 可以用于向呼叫设备输入命令和信息，该收发器 1004 可以通过总线 1003 连接至处理器 1001。收发器 1004 还可以用于呼叫设备输出信息，例如所选定的占位服务器和 / 或占位虚拟机。

呼叫设备可以通过网络接口 1006 连接到通信网络中，在联网环境下，呼叫设备中存储的计算机执行指令可以存储在远程存储设备中，而限于在本地存储。

当呼叫设备中的处理器 1001 执行存储器 1002 中存储的可执行代码或应用程序时，呼叫设备可以执行以上任一方法实施例由呼叫设备执行的操作，具体执行过程参见上述方法实施例，在此不再赘述。

本申请还提供了一种通信系统，该通信系统包括主叫通信系统以及被叫通信系统。

其中，主叫通信系统的具体说明，请详见图 1 所示，被叫通信系统的说明，请参见图 1 所示，具体不做赘述。本实施例所示的通信系统用于执行上述各方法实施例，具体执行过程，不做赘述。

以上所述，以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的范围。

— 29 —

权 利 要 求

1. 一种呼叫处理的方法，其特征在于，所述方法包括：

第一呼叫设备获取签名密钥；

5 所述第一呼叫设备获取第一用户的待显示数据，所述待显示数据包括与所述第一用户对应的信息和/或与所述第一用户所属的企业对应的信息；

所述第一呼叫设备通过所述签名密钥对所述待显示数据进行签名以获取第一验证签名信息；

10 所述第一呼叫设备通过所述第一呼叫设备和第二呼叫设备之间的媒体通道，向所述第二呼叫设备发送所述待显示数据以及所述第一验证签名信息，所述第一验证签名信息用于验证所述待显示数据的安全性。

2. 根据权利要求 1 所述的方法，其特征在于，所述第一呼叫设备通过所述签名密钥对所述待显示数据进行签名以获取第一验证签名信息之前，所述方法还包括：

15 所述第一呼叫设备向所述第二呼叫设备发送第一指示消息，所述第一指示消息用于指示所述第一呼叫设备支持对所述待显示数据签名的能力；

所述第一呼叫设备接收来自所述第二呼叫设备的第二指示消息，所述第二指示消息用于指示所述第二呼叫设备支持验证所述待显示数据安全性的能力。

20 3. 根据权利要求 1 或 2 所述的方法，其特征在于，所述第一呼叫设备获取第一用户的待显示数据包括：

所述第一呼叫设备接收呼叫请求消息，所述呼叫请求消息携带所述待显示数据。

4. 根据权利要求 1 或 2 所述的方法，其特征在于，所述第一呼叫设备获取第一用户的待显示数据包括：

25 所述第一呼叫设备接收呼叫请求消息；

所述第一呼叫设备获取与所述呼叫请求消息对应的所述待显示数据。

5. 根据权利要求 1 至 4 任一项所述的方法，其特征在于，所述第一呼叫设备获取签名密钥包括：

30 所述第一呼叫设备向所述第二呼叫设备发送呼叫请求消息，所述呼叫请求消息用于请求获取所述签名密钥；

所述第一呼叫设备接收来自所述第二呼叫设备的主密钥和主盐密钥，所述主密钥和所述主盐密钥用于安全实时传输协议 SRTP；

所述第一呼叫设备根据所述主密钥和所述主盐密钥，生成所述签名密钥。

35

6. 根据权利要求 5 所述的方法，其特征在于，所述第一呼叫设备接收来自所述第二呼叫设备的主密钥和主盐密钥包括：

— 30 —

所述第一呼叫设备接收来自所述第二呼叫设备的签名信息，所述签名信息包括通过公钥签名的所述主密钥和所述主盐密钥；

所述第一呼叫设备通过私钥验证所述签名信息以获取所述主密钥和所述主盐密钥。

5 7. 根据权利要求 1 至 6 任一项所述的方法，与所述第一用户对应的信息包括如下所示的至少一项：

所述第一用户的名称，所述第一用户的工号，所述第一用户的头像，所述第一用户的职位信息，与所述第一用户相关的音视频文件，或所述第一用户所属的协会的信息；

与所述第一用户所属的企业对应的信息包括如下所示的至少一项：

10 所述企业名称，所述企业的商标，与所述企业相关的音视频文件，或所述企业所属的协会的信息。

8. 一种呼叫处理的方法，其特征在于，所述方法包括：

15 第二呼叫设备接收来自第一呼叫设备的待显示数据以及第一验证签名信息，所述第一验证签名信息为通过签名密钥对所述待显示数据进行签名以获取，所述待显示数据和所述第一验证签名信息通过所述第一呼叫设备和所述第二呼叫设备之间的媒体通道传输，所述待显示数据包括与所述第一用户对应的信息和/或与所述第一用户所属的企业对应的信息；

所述第二呼叫设备通过所述签名密钥对所述待显示数据进行签名以获取第二验证签名信息；

20 若所述第二呼叫设备确定所述第一验证签名信息和所述第二验证签名信息相同，确定所述待显示数据通过安全性验证，使所述待显示数据显示。

9. 根据权利要求 8 所述的方法，其特征在于，所述第二呼叫设备接收来自第一呼叫设备的待显示数据以及第一验证签名信息之前，所述方法还包括：

25 所述第二呼叫设备接收来自所述第一呼叫设备的第一指示消息，所述第一指示消息用于指示所述第一呼叫设备支持对所述待显示数据签名的能力；

所述第二呼叫设备向所述第一呼叫设备发送第二指示消息，所述第二指示消息用于指示所述第二呼叫设备支持验证所述待显示数据安全性的能力。

30 10. 根据权利要求 8 或 9 所述的方法，其特征在于，所述若所述第二呼叫设备确定所述第一验证签名信息和所述第二验证签名信息相同，确定所述待显示数据通过安全性验证之后，所述方法还包括：

所述第二呼叫设备向第二终端发送所述待显示数据，所述第二终端为第二用户所使用的终端，所述第二终端用于显示所述待显示数据。

35

11. 根据权利要求 8 或 9 所述的方法，其特征在于，所述第二呼叫设备为第二终端，所述第二终端为第二用户所使用的终端，所述若所述第二呼叫设备确定所述第一验证签名信

— 31 —

息和所述第二验证签名信息相同，确定所述待显示数据通过安全性验证之后，所述方法还包括：

所述第二呼叫设备显示所述待显示数据。

- 5 12. 根据权利要求 10 所述的方法，其特征在于，所述若所述第二呼叫设备确定所述第一验证签名信息和所述第二验证签名信息相同，确定所述待显示数据通过安全性验证之后，所述方法还包括：

所述第二呼叫设备向所述第二终端发送通知消息，所述通知消息用于指示所述待显示数据通过安全性验证。

10

13. 根据权利要求 8 至 12 任一项所述的方法，其特征在于，所述第二呼叫设备接收来自第一呼叫设备的待显示数据以及第一验证签名信息之前，所述方法还包括：

所述第二呼叫设备接收来自所述第一呼叫设备的呼叫请求消息，所述呼叫请求消息用于请求获取所述签名密钥；

15

所述第二呼叫设备根据所述呼叫请求消息向所述第一呼叫设备发送主密钥和主盐密钥，所述主密钥和所述主盐密钥用于安全实时传输协议 SRTP，所述主密钥和所述主盐密钥用于生成所述验证签名。

20

14. 根据权利要求 13 所述的方法，其特征在于，所述第二呼叫设备根据所述呼叫请求消息向所述第一呼叫设备发送主密钥和主盐密钥包括：

所述第二呼叫设备通过公钥对所述主密钥和所述主盐密钥签名以获取签名信息；

所述第二呼叫设备向所述第一呼叫设备发送所述签名信息。

25

15. 根据权利要求 8 至 14 任一项所述的方法，其特征在于，所述第二呼叫设备接收来自第一呼叫设备的待显示数据以及第一验证签名信息之前，所述方法还包括：

所述第二呼叫设备接收来自所述第一呼叫设备的呼叫请求消息；

所述第二呼叫设备根据所述呼叫请求消息向所述第一呼叫设备发送所述签名密钥。

30

16. 根据权利要求 8 至 14 任一项所述的方法，其特征在于，与所述第一用户对应的信息包括如下所示的至少一项：

所述第一用户的名称，所述第一用户的工号，所述第一用户的头像，所述第一用户的职位信息，与所述第一用户相关的音视频文件，或所述第一用户所属的协会的信息；

与所述第一用户所属的企业对应的信息包括如下所示的至少一项：

35

所述企业名称，所述企业的商标，与所述企业相关的音视频文件，或所述企业所属的协会的信息。

17. 一种呼叫设备，其特征在于，包括：

— 32 —

第一获取模块，用于获取签名密钥；

第二获取模块，用于获取第一用户的待显示数据，所述第一用户为与所述呼叫设备对应的用户，所述待显示数据包括与所述第一用户对应的信息和/或与所述第一用户所属的企业对应的信息；

5 签名模块，用于通过所述签名密钥对所述待显示数据进行签名以获取第一验证签名信息；

发送模块，用于通过所述呼叫设备和另一呼叫设备之间的媒体通道，向所述另一呼叫设备发送所述待显示数据以及所述第一验证签名信息，所述第一验证签名信息用于验证所述待显示数据的安全性。

10

18. 一种呼叫设备，其特征在于，包括：

接收模块，用于接收来自另一呼叫设备的待显示数据以及第一验证签名信息，所述第一验证签名信息为通过签名密钥对所述待显示数据进行签名以获取，所述待显示数据和所述第一验证签名信息通过所述另一呼叫设备和呼叫设备之间的媒体通道传输，所述待显示数据包括与第一用户对应的信息和/或与所述第一用户所属的企业对应的信息，所述第一用户为与所述另一呼叫设备对应的用户；

15

签名模块，用于通过所述签名密钥对所述待显示数据进行签名以获取第二验证签名信息；

验证模块，用于若确定所述第一验证签名信息和所述第二验证签名信息相同，确定所述待显示数据通过安全性验证，使所述待显示数据显示。

20

19. 一种呼叫设备，其特征在于，包括相互耦合的处理器和存储器，所述存储器中存储了计算机程序代码，所述处理器调用并执行所述存储器中的计算机程序代码，使得所述呼叫设备执行如权利要求 1-7 任一项所述的方法。

25

20. 一种呼叫设备，其特征在于，包括相互耦合的处理器和存储器，所述存储器中存储了计算机程序代码，所述处理器调用并执行所述存储器中的计算机程序代码，使得所述呼叫设备执行如权利要求 8-16 任一项所述的方法。

30

21. 一种通信系统，其特征在于，包括如权利要求 19 所述的呼叫设备以及如权利要求 20 所述的呼叫设备。

22. 一种计算机可读的存储介质，其特征在于，所述存储介质存储有计算机程序，所述计算机程序包括程序指令，所述程序指令当被处理器执行时使所述处理器执行如权利要求 1 至 16 任一项所述的方法。

35

23. 一种呼叫处理的方法，其特征在于，所述方法包括：

第一呼叫设备获取签名密钥；

所述第一呼叫设备获取第一用户的待显示数据，所述待显示数据包括与所述第一用户对应的信息和/或与所述第一用户所属的企业对应的信息；

5 所述第一呼叫设备通过所述签名密钥对所述待显示数据进行签名以获取第一验证签名信息；

所述第一呼叫设备通过所述第一呼叫设备和第二呼叫设备之间的媒体通道，向所述第二呼叫设备发送所述待显示数据以及所述第一验证签名信息；

所述第二呼叫设备接收来自所述第一呼叫设备的所述待显示数据以及所述第一验证签名信息；

10 所述第二呼叫设备通过所述签名密钥对所述待显示数据进行签名以获取第二验证签名信息；

若所述第二呼叫设备确定所述第一验证签名信息和所述第二验证签名信息相同，确定所述待显示数据通过安全性验证，使所述待显示数据显示。

15 24. 根据权利要求 23 所述的方法，其特征在于，所述第一呼叫设备通过所述签名密钥对所述待显示数据进行签名以获取第一验证签名信息之前，所述方法还包括：

所述第一呼叫设备向所述第二呼叫设备发送第一指示消息，所述第一指示消息用于指示所述第一呼叫设备支持对所述待显示数据签名的能力；

20 所述第二呼叫设备接收来自所述第一呼叫设备的所述待显示数据以及所述第一验证签名信息之前，所述方法还包括：

所述第二呼叫设备向所述第一呼叫设备发送第二指示消息，所述第二指示消息用于指示所述第二呼叫设备支持验证所述待显示数据安全性的能力。

25 25. 根据权利要求 23 或 24 所述的方法，其特征在于，所述第一呼叫设备获取第一用户的待显示数据包括：

所述第一呼叫设备接收呼叫请求消息，所述呼叫请求消息携带所述待显示数据。

26. 根据权利要求 23 或 24 所述的方法，其特征在于，所述第一呼叫设备获取第一用户的待显示数据包括：

30 所述第一呼叫设备接收呼叫请求消息；

所述第一呼叫设备获取与所述呼叫请求消息对应的所述待显示数据。

27. 根据权利要求 23 至 26 任一项所述的方法，其特征在于，所述第一呼叫设备获取签名密钥之前，所述方法还包括：

35 所述第一呼叫设备向所述第二呼叫设备发送呼叫请求消息，所述呼叫请求消息用于请求获取所述签名密钥；

所述第二呼叫设备接收来自所述第一呼叫设备的所述待显示数据以及所述第一验证签

— 34 —

名信息之前，所述方法还包括：

所述第二呼叫设备根据所述呼叫请求消息向所述第一呼叫设备发送主密钥和主盐密钥，所述主密钥和所述主盐密钥用于安全实时传输协议 SRTP；

所述第一呼叫设备获取签名密钥包括：

- 5 所述第一呼叫设备接收来自所述第二呼叫设备的所述主密钥和所述主盐密钥；
 所述第一呼叫设备根据所述主密钥和所述主盐密钥，生成所述签名密钥。

28. 根据权利要求 27 所述的方法，其特征在于，所述第二呼叫设备根据所述呼叫请求消息向所述第一呼叫设备发送主密钥和主盐密钥包括：

- 10 所述第二呼叫设备通过公钥对所述主密钥和所述主盐密钥签名以获取签名信息；
 所述第二呼叫设备向所述第一呼叫设备发送所述签名信息。

29. 根据权利要求 23 至 28 任一项所述的方法，其特征在于，与所述第一用户对应的信息包括如下所示的至少一项：

- 15 所述第一用户的名称，所述第一用户的工号，所述第一用户的头像，所述第一用户的职位信息，与所述第一用户相关的音视频文件，或所述第一用户所属的协会的信息；
 与所述第一用户所属的企业对应的信息包括如下所示的至少一项：
 所述企业名称，所述企业的商标，与所述企业相关的音视频文件，或所述企业所属的协会的信息。

20

25

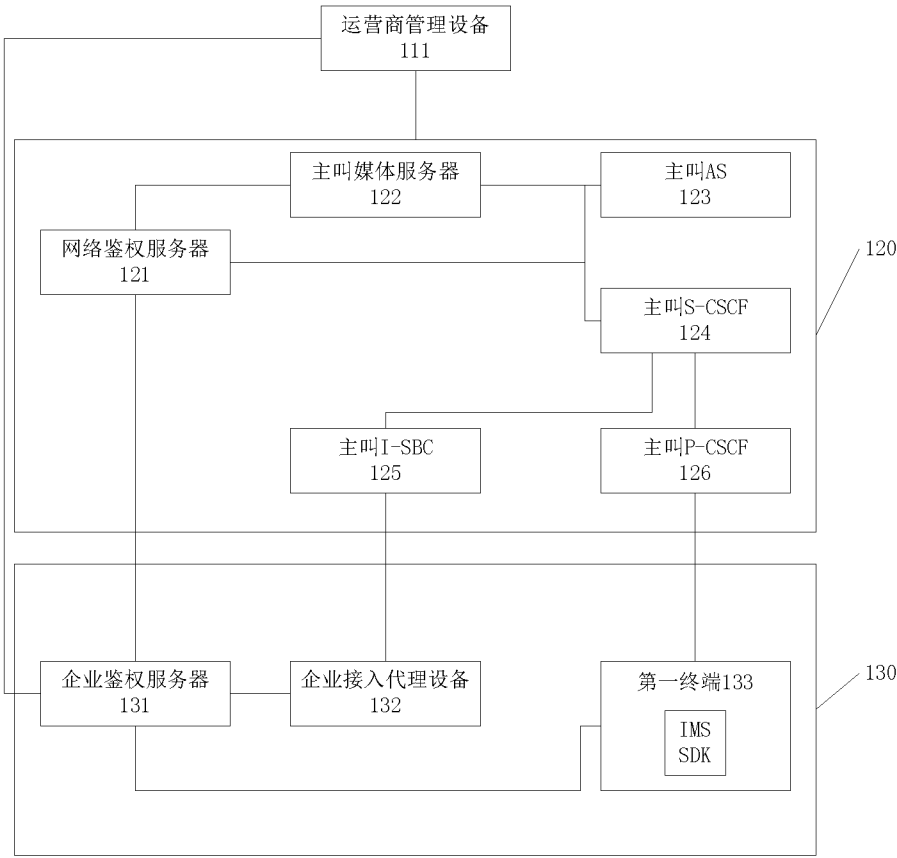


图 1

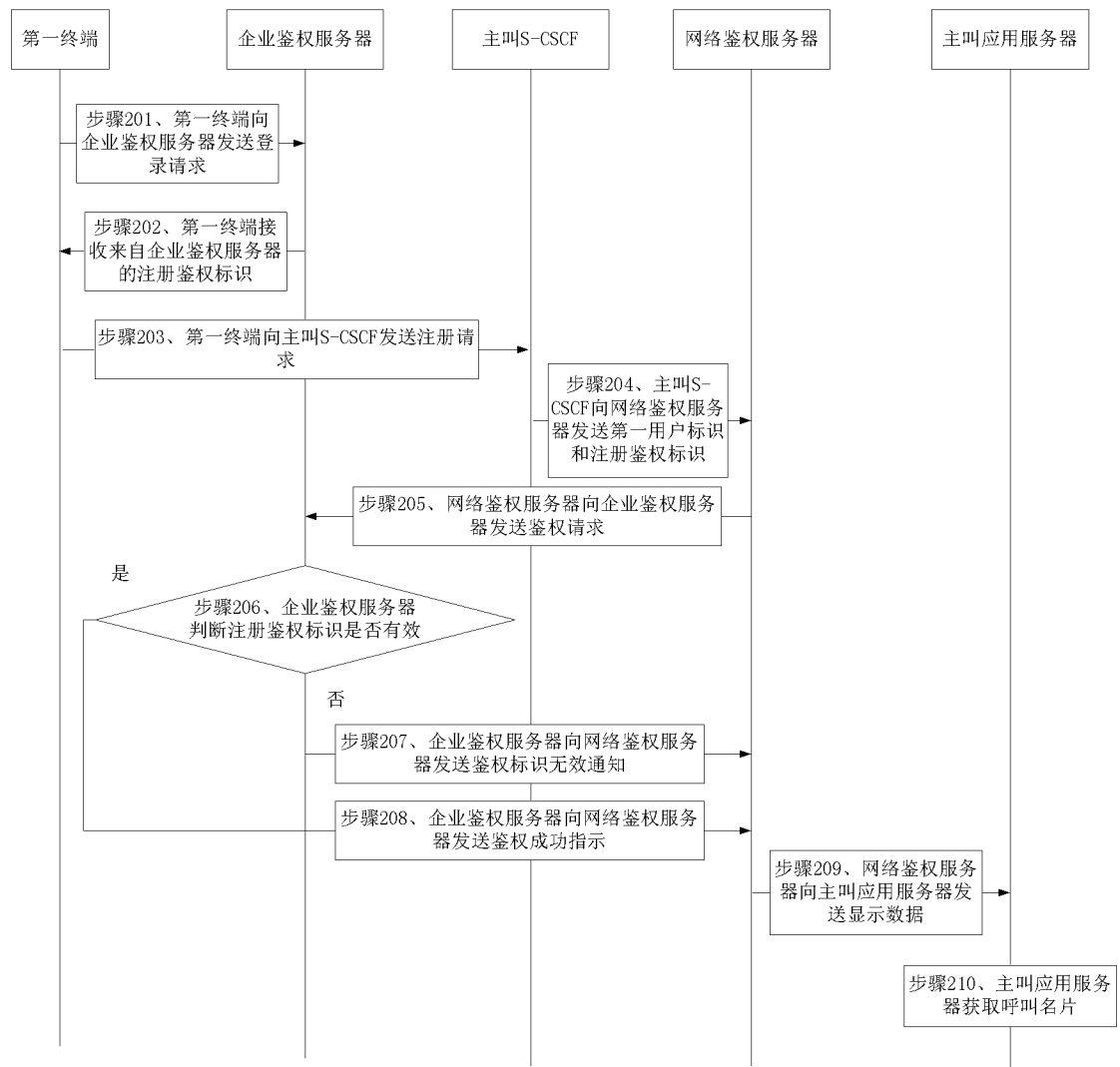


图 2

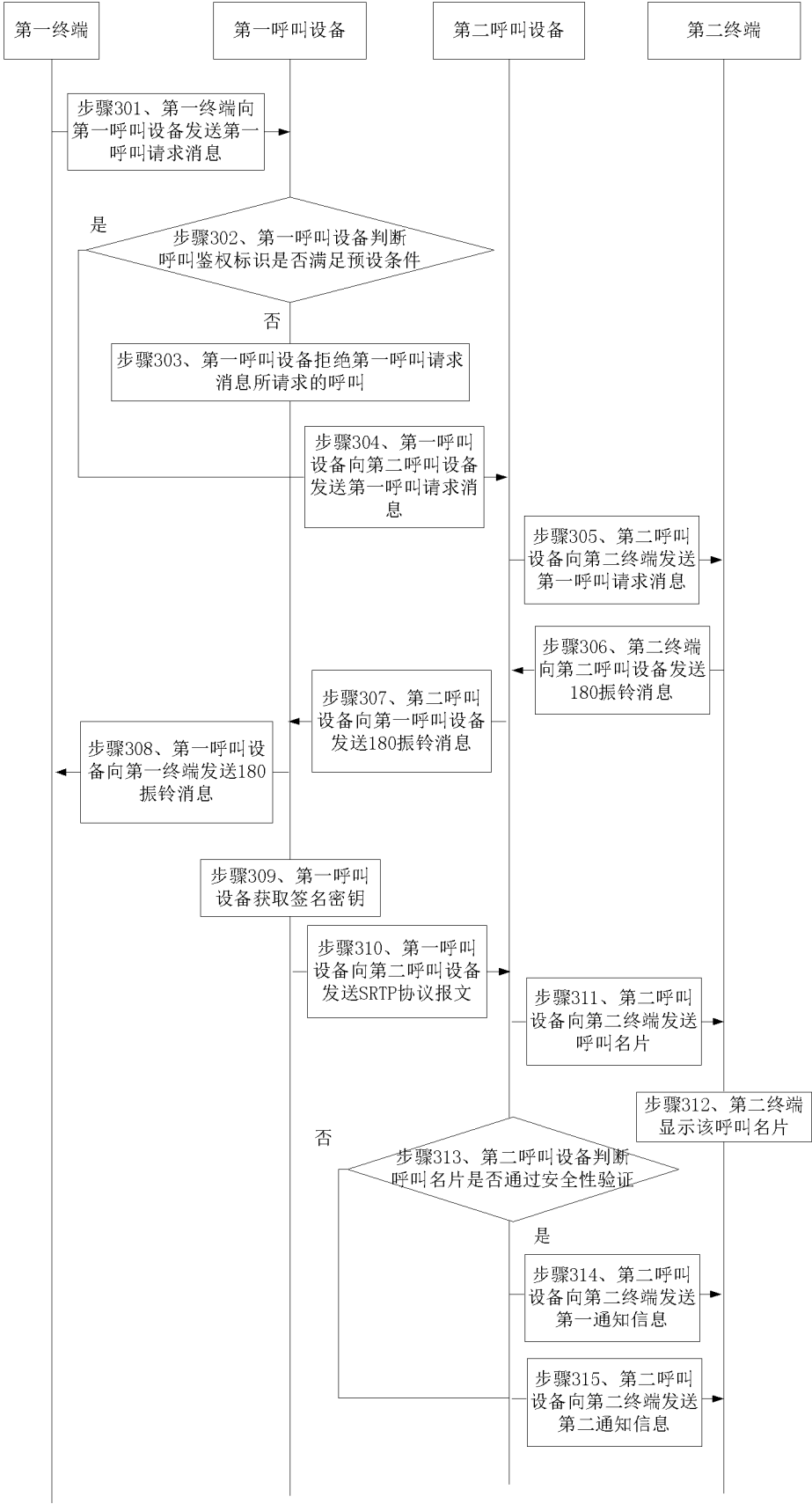


图 3

—4/8—

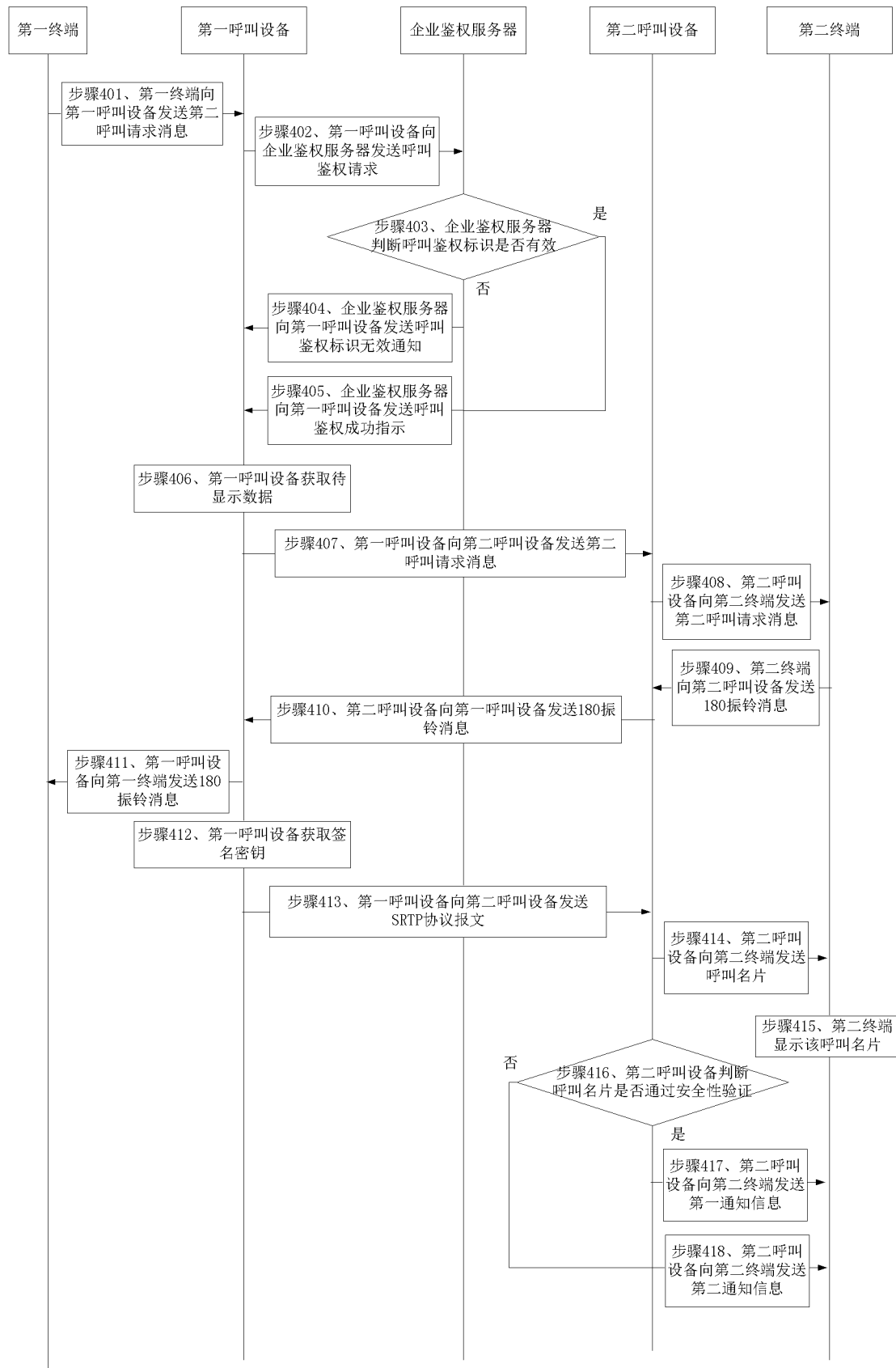


图 4

— 5/8 —

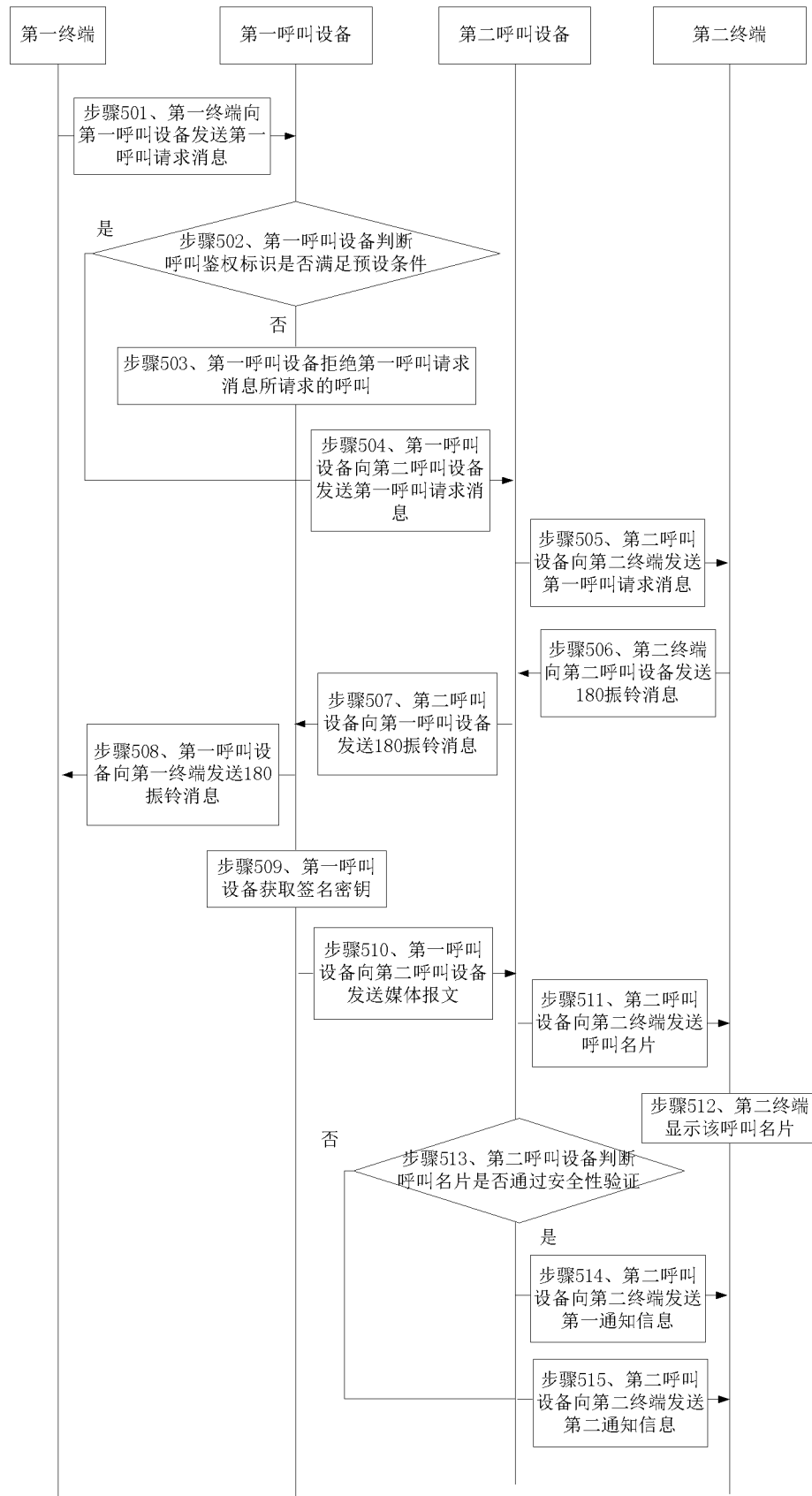


图 5

—6/8—

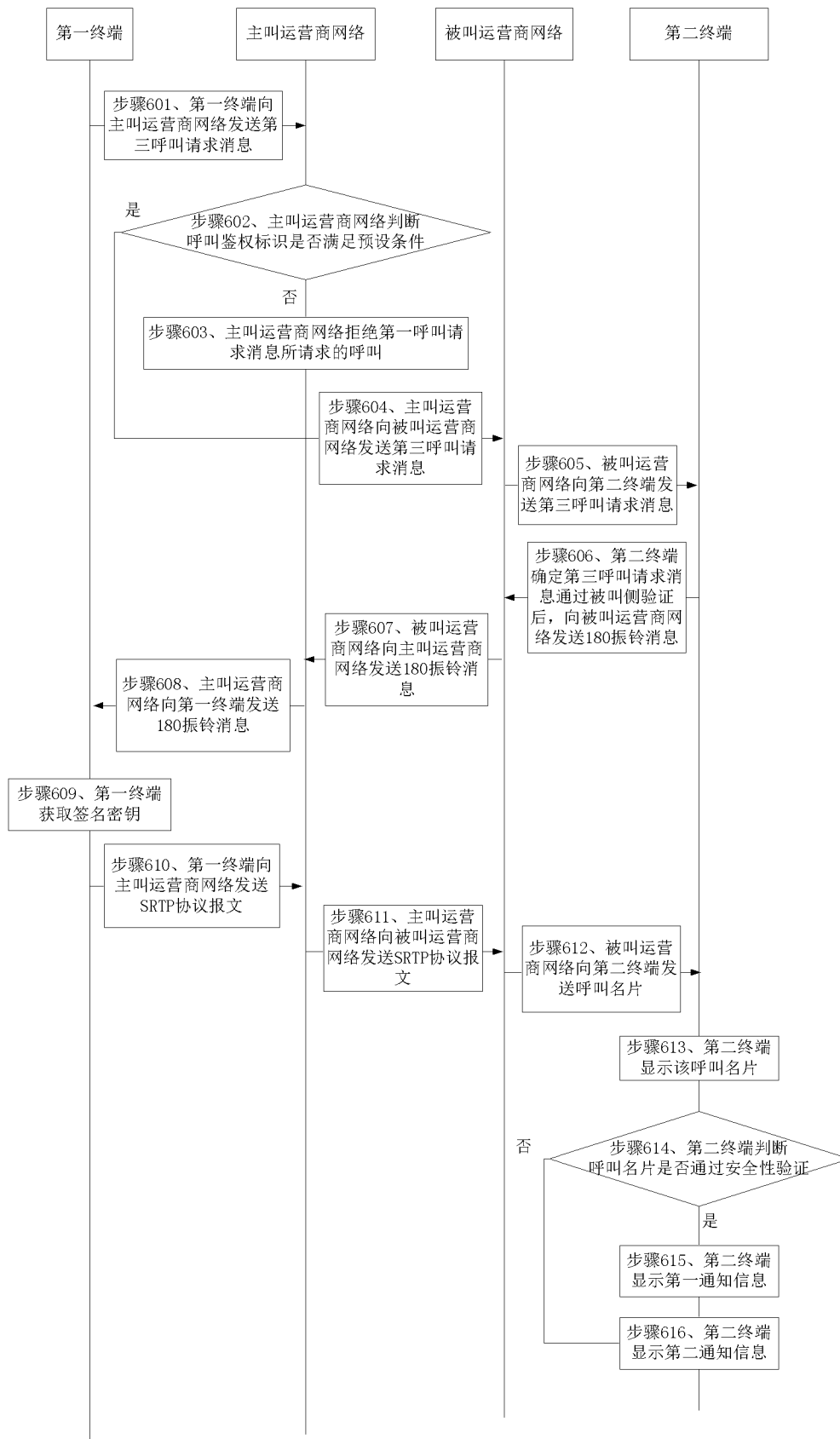


图 6

— 7/8 —

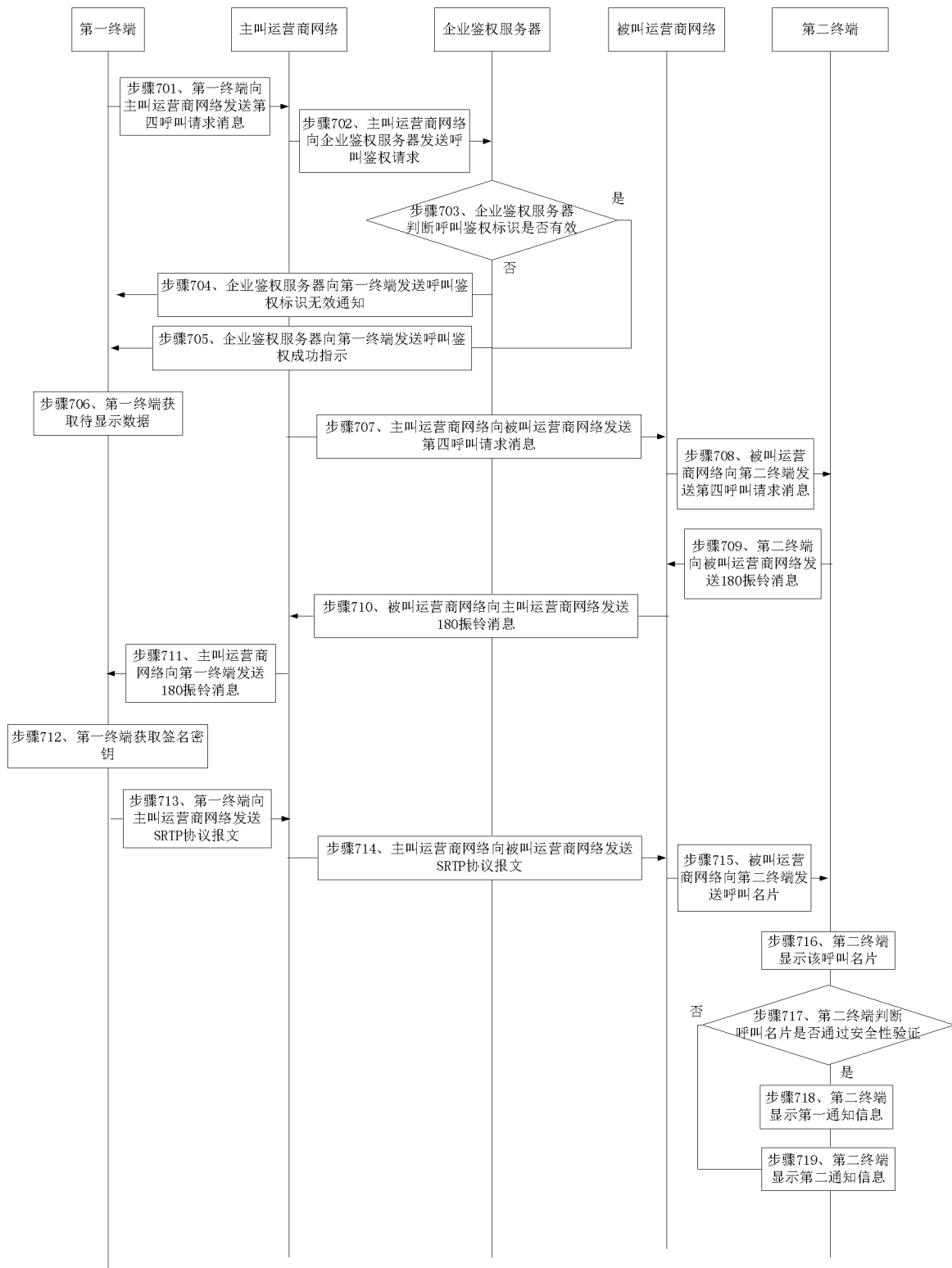


图 7

— 8/8 —

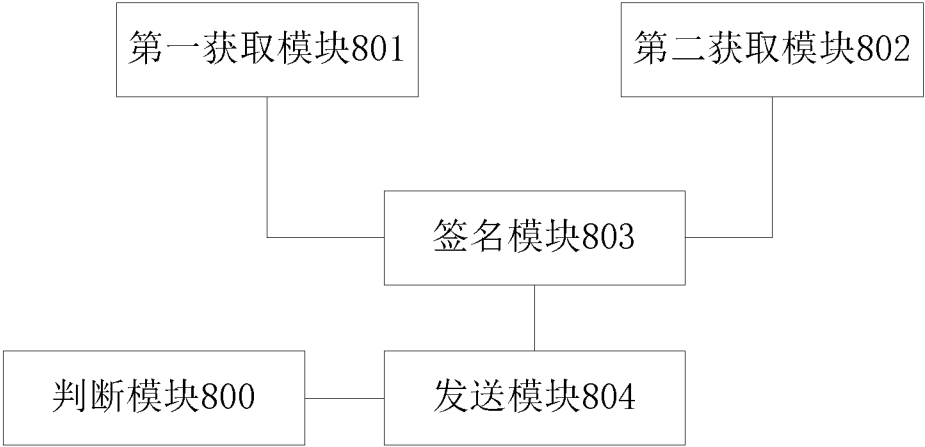


图 8

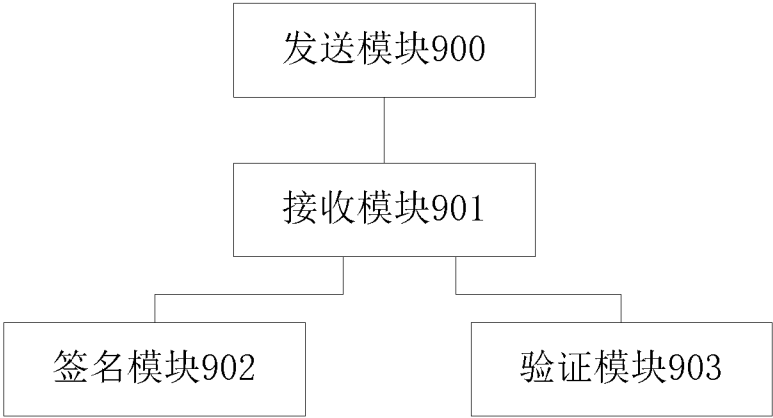


图 9

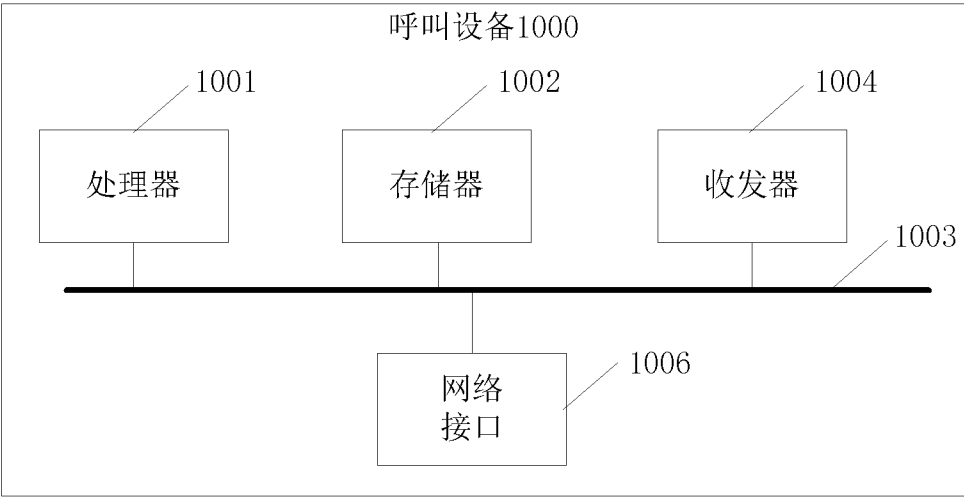


图 10

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2022/122530

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i; H04W 8/24(2009.01)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)

H04L9/-; H04W8/-

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)

CNTEXT; CNABS; CNKI: 呼叫, 主叫方, 被叫方, 安全, 验证, 认证, 签名, 加密, 用户, 名称, 工号, 协会, 职位, 头像, 个人信息, 私人, 企业, 密钥, 私钥, 公钥, +RTP, SIP, +INVITE, +CSCF; VEN; USTXT; EPTXT; WOTXT; 3GPP; IETF: call+, security, verif+, authent+, sign+, encrypt+, user, name, job, association, position, avatar, personal, corporation, enterprise, +key, private, public, +RTP, SIP, +INVITE, +CSCF

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	US 2022086276 A1 (DOUGLAS RANALLI) 17 March 2022 (2022-03-17) description, paragraphs [0059]-[0097]	1-29
Y	US 2020336314 A1 (VERIZON PATENT AND LICENSING INC.) 22 October 2020 (2020-10-22) description, paragraphs [0012]-[0063] and [0082]-[0088]	1-29
Y	US 10154136 B1 (SYMANTEC CORP.) 11 December 2018 (2018-12-11) description, column 4, line 63-column 8, line 10	1-29
Y	US 2020028690 A1 (VERIZON PATENT AND LICENSING INC.) 23 January 2020 (2020-01-23) description, paragraphs [0015]-[0093]	1-29
A	US 2020053136 A1 (T-MOBILE USA, INC.) 13 February 2020 (2020-02-13) entire document	1-29
A	CN 108886520 A (BLACKBERRY LTD.) 23 November 2018 (2018-11-23) entire document	1-29



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

12 December 2022

Date of mailing of the international search report

21 December 2022

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing
100088, China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2022/122530

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
US	2022086276	A1	17 March 2022	WO	2022060705	A1	24 March 2022
US	2020336314	A1	22 October 2020	US	2021409228	A1	30 December 2021
				US	11133938	B2	28 September 2021
US	10154136	B1	11 December 2018	None			
US	2020028690	A1	23 January 2020	US	2021281424	A1	09 September 2021
				US	11018872	B2	25 May 2021
US	2020053136	A1	13 February 2020	WO	2020037007	A1	20 February 2020
				US	11063990	B2	13 July 2021
CN	108886520	A	23 November 2018	KR	20180107776	A	02 October 2018
				EP	3408993	A1	05 December 2018
				CA	3011821	A1	03 August 2017
				WO	2017132277	A1	03 August 2017
				US	2017134444	A1	11 May 2017
				HK	1261456	A0	03 January 2020
				EP	3408993	B1	04 November 2020
				CN	108886520	B	30 March 2021
				US	11297111	B2	05 April 2022

国际检索报告

国际申请号

PCT/CN2022/122530

A. 主题的分类

H04L 9/32 (2006.01) i; H04W 8/24 (2009.01) 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)

H04L9/-; H04W8/-

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))

CNXTX;CNABS;CNKI:呼叫, 主叫方, 被叫方, 安全, 验证, 认证, 签名, 加密, 用户, 名称, 工号, 协会, 职位, 头像, 个人信息, 私人, 企业, 密钥, 私钥, 公钥, +RTP, SIP, +INVITE, +CSCF; VEN;USTXT;EPTXT;WOTXT;3GPP;IETF:call+, security, verif+, authent+, sign+, encrypt+, user, name, job, association, position, avatar, personal, corporation, enterprise, +key, private, public, +RTP, SIP, +INVITE, +CSCF

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
PX	US 2022086276 A1 (DOUGLAS RANALLI) 2022年3月17日 (2022 - 03 - 17) 说明书第[0059]-[0097]段	1-29
Y	US 2020336314 A1 (VERIZON PATENT AND LICENSING INC.) 2020年10月22日 (2020 - 10 - 22) 说明书第[0012]-[0063]、[0082]-[0088]段	1-29
Y	US 10154136 B1 (SYMANTEC CORPORATION) 2018年12月11日 (2018 - 12 - 11) 说明书第4栏第63行-第8栏第10行	1-29
Y	US 2020028690 A1 (VERIZON PATENT AND LICENSING INC.) 2020年1月23日 (2020 - 01 - 23) 说明书第[0015]-[0093]段	1-29
A	US 2020053136 A1 (T-MOBILE USA, INC.) 2020年2月13日 (2020 - 02 - 13) 全文	1-29
A	CN 108886520 A (黑莓有限公司) 2018年11月23日 (2018 - 11 - 23) 全文	1-29

☐ 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

2022年12月12日

国际检索报告邮寄日期

2022年12月21日

ISA/CN的名称和邮寄地址

中国国家知识产权局 (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

授权官员

王璐

电话号码 (86-28)62969272

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2022/122530

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)
US	2022086276	A1	2022年3月17日	WO	2022060705	A1	2022年3月24日
US	2020336314	A1	2020年10月22日	US	2021409228	A1	2021年12月30日
				US	11133938	B2	2021年9月28日
US	10154136	B1	2018年12月11日	无			
US	2020028690	A1	2020年1月23日	US	2021281424	A1	2021年9月9日
				US	11018872	B2	2021年5月25日
US	2020053136	A1	2020年2月13日	WO	2020037007	A1	2020年2月20日
				US	11063990	B2	2021年7月13日
CN	108886520	A	2018年11月23日	KR	20180107776	A	2018年10月2日
				EP	3408993	A1	2018年12月5日
				CA	3011821	A1	2017年8月3日
				WO	2017132277	A1	2017年8月3日
				US	2017134444	A1	2017年5月11日
				HK	1261456	A0	2020年1月3日
				EP	3408993	B1	2020年11月4日
				CN	108886520	B	2021年3月30日
				US	11297111	B2	2022年4月5日