(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
2018 年 10 月 11 日 (11.10.2018)

WIPO | PCT

(10) 国际公布号
WO 2018/184433 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01) *H04L 12/58* (2006.01)

(21) 国际申请号: PCT/CN2018/077527

(22) 国际申请日: 2018 年 2 月 28 日 (28.02.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201710223657.8 2017年4月7日 (07.04.2017) CN

(71) 申请人: 中兴通讯股份有限公司 (ZTE CORPORATION) [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(72) 发明人: 陈安地 (CHEN, Andi); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(74) 代理人: 北京天昊联合知识产权代理有限公司 (TEE&HOWE INTELLECTUAL PROPERTY ATTORNEYS); 中国北京市东城区建国门内大街 28 号民生金融中心 D 座 10 层盛博, Beijing 100005 (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:** INTERNET-OF-THINGS AUTHENTICATION SYSTEM AND INTERNET-OF-THINGS AUTHENTICATION METHOD

(54) **发明名称**: 一种物联网认证系统和物联网认证方法

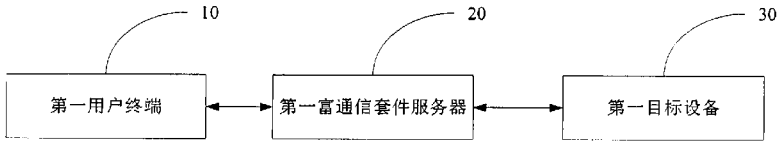

图 1

10 First user terminal
20 First rich communications kit server
30 First destination device

(57) **Abstract:** The present disclosure provides an Internet-of-Things authentication system and Internet-of-Things authentication method. The Internet-of-Things authentication system comprises a first user terminal used for receiving an interaction communications request from a user and generating a remote authentication request message carrying second binding relationship information, and sending the remote authentication request message to a first destination device; a first rich communications kit server used, during a process of a first user terminal and/or rich communications account establishing a binding relationship with a first destination device and authenticating the binding relationship, for achieving message forwarding between the first user and the first destination device; the first destination device is used for storing first binding relationship information, receiving a remote authentication request message, and detecting whether the second binding relationship information is consistent with the first binding relationship information; if it is consistent, then authentication is successful, and the first destination device receives the interaction communications request of the first user.

(57) **摘要**: 本公开提出了一种物联网认证系统和物联网认证方法。所述物联网认证系统包括第一用户终端, 用于接受用户的交互通信请求, 生成携带第二绑定关系信息的远程认证请求消息, 并将远程认证请求消息发送至第一目标设备; 第一富通信套件服务器, 用于在第一用户终端和/或富通信账号与第一目标设备建立绑定关系以及认证绑定关系的过程中, 实现第一用户终端和第一目标设备之间的消息转发; 第一目标设备, 用于存储第一绑定关系信息, 接收远程认证请求消息, 检测第二绑定关系信息与第一绑定关系信息是否一致, 其中, 如果一致, 则认证通过, 第一目标设备接受第一用户终端的交互通信请求。

WO 2018/184433 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))。

一种物联网认证系统和物联网认证方法

技术领域

本公开涉及移动通信与物联网技术领域，特别涉及一种物联网认证系统和物联网认证方法。

背景技术

随着社会的发展、科学技术水平的不断提高，物联网得到了广泛的发展。物联网的迅速崛起，使得通过人与物、物与物之间的互联交互，来实现各种远程业务或是远程设备管理的场景也日益增加。但是，随之而来的用户身份认证以及远程身份认证中存在的安全性和易用性问题，也逐渐暴露。

在一种情况中，采用生物识别技术的认证方法可以快速、安全、准确地进行身份的认证。例如，利用指纹、脸形、虹膜等生物特征的身份认证已经广泛第应用于智能移动终端。但是，尚未提出在物联网环境下的用户与设备间的有效的远程认证系统和方法。

发明内容

本公开提供了一种物联网认证系统和物联网认证方法。

本公开实施例提供的物联网认证系统，包括第一用户终端、第一富通信套件服务器和第一目标设备，其中，所述第一用户终端用于接受用户的交互通信请求，生成携带第二绑定关系信息的远程认证请求消息，并将所述远程认证请求消息发送至所述第一目标设备；所述第一富通信套件服务器用于在第一用户终端和/或富通信账号与所述第一目标设备建立绑定关系以及认证绑定关系过程中，实现所述第一用户终端与所述第一目标设备之间的消息转发；所述第一目标设备用于存储所述第一用户终端和/或富通信账号与所述第一目标设备之间的第一绑定关系信息，接收所述远程认证请求消息，并且检测所述远程认证请求消息中的所述第二绑定关系信息与所述第一绑定关系信息是否一致，其中，如果所述远程认证请求消息中的第二绑定关系信息与所述

第一绑定关系信息一致，则认证通过，并且所述第一目标设备接受所述第一用户终端的交互通信请求。

在一个示例性实施例中，所述远程认证请求消息中携带时间戳信息；并且所述第一目标设备还用于在验证所述远程认证请求消息中的绑定关系信息与所述存储的绑定关系信息是否一致时，检测所述时间戳是否超时，其中，如果所述远程认证请求消息中的第二绑定关系信息与所述第二绑定关系信息一致且时间戳不超时，则认证通过。

在一个示例性实施例中，所述第一用户终端还用于在生成所述远程认证请求消息之前，要求用户输入生物信息认证。

在一个示例性实施例中，所述生物信息认证为指纹识别、面部识别或语音识别中的至少一者。

本公开实施例还提供了一种物联网认证系统，包括第二用户终端、第二富通信套件服务器、第二目标设备和第三方服务器，其中，所述第二用户终端用于接受用户的交互通信请求，生成携带第二绑定关系信息的远程认证请求消息，并将所述远程认证请求消息发送至所述第二目标设备；所述第二富通信套件服务器用于在所述第二用户终端和/或富通信账号与所述第二目标设备建立绑定关系以及认证绑定关系过程中，实现所述第二用户终端与所述第三方服务器之间的消息转发；所述第三方服务器用于存储所述第二用户终端和/或富通信账号与所述第二目标设备之间的第一绑定关系信息；接收所述远程认证请求消息，验证远程认证请求消息中的所述第二绑定关系信息与所述第一绑定关系信息是否一致，其中，如果远程认证请求消息中的所述第二绑定关系信息与所述第一绑定关系信息一致，将所述远程认证请求消息转发至所述第二目标设备；所述第二目标设备，用于接收所述远程认证请求消息，检测所述远程认证请求消息中的目标设备信息与本地信息是否一致，如果与本地信息一致，则认证通过，接受第二用户终端的交互通信请求。

本公开实施例还提供了一种物联网认证方法，包括：通过第一富通信套件服务器转发消息以使第一用户终端和/或富通信账号与第一目标设备绑定，并将第一绑定关系信息存储在所述第一目标设备中；通

过所述第一用户终端请求发出与所述第一目标设备进行交互通信的请求，通过所述第一用户终端生成携带第二绑定关系信息的远程认证请求消息，并将所述远程认证请求消息发送至第一目标设备；以及通过所述第一目标设备接收所述远程认证请求消息，验证所述远程认证请求消息中的第二绑定关系信息与所述第一绑定关系信息是否一致，如果所述远程认证请求消息中的第二绑定关系信息与所述第一绑定关系信息一致，则认证通过，并且所述第一目标设备接受第一用户终端的交互通信请求。

在一个示例性实施例中，在将所述远程认证请求消息发送至所述第一目标设备时，所述远程认证请求消息中携带时间戳信息，并且所述方法还包括：在验证所述远程认证请求消息中的第二绑定关系信息与所述第一绑定关系信息是否一致时，检测所述时间戳是否超时，其中，如果所述远程认证请求消息中的第二绑定关系信息与所述第一绑定关系信息一致且时间戳不超时，则认证通过。

在一个示例性实施例中，所述方法还包括：在将所述远程认证请求消息发送至所述第一目标设备时，对所述远程认证请求消息进行加密处理。

在一个示例性实施例中，在通过所述第一富通信套件服务器发出与所述第一目标设备进行交互通信的请求时，所述第一用户终端要求用户输入生物信息认证，其中，如果生物信息认证成功，则所述第一用户终端生成所述远程认证请求消息。

本公开实施例还提供了一种物联网认证方法，包括：通过第二富通信套件服务器转发消息以使第二用户终端和/或富通信账号与第二目标设备的绑定，并将所述第一绑定关系信息存储在第三方服务器中；通过第二用户终端发出与第二目标设备进行交互通信的请求，通过所述第二用户终端生成携带第二绑定关系信息的远程认证请求消息，并将所述远程认证请求消息发送至第三方服务器；通过所述第三方服务器接收所述远程认证请求消息，验证所述远程认证请求消息中的第二绑定关系信息与所述第一绑定关系信息是否一致，其中，如果所述远程认证请求消息中的第二绑定关系信息与所述第一绑定关系信息一致，

将所述远程认证请求消息转发至所述第二目标设备；通过所述第二目标设备接收远程认证请求消息，检测所述远程认证请求消息中的目标设备信息与本地信息是否一致，其中，如果所述远程认证请求消息中的目标设备信息与本地信息一致，则认证通过，并且述第二目标设备接受第二用户终端的交互通信请求。

附图说明

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

图 1 为根据本公开第一实施例的物联网认证系统的结构示意图；

图 2 为根据本公开第二实施例的物联网认证系统的结构示意图；

图 3 为根据本公开第一实施例的物联网认证方法的流程示意图；

图 4 为根据本公开第二实施例的物联网认证方法的流程示意图；

图 5 为根据本公开第三实施例的物联网认证方法的流程示意图；

图 6 为根据本公开第三实施例的物联网认证方法中的绑定步骤的流程示意图；

图 7 为根据本公开第三实施例的物联网认证方法中的信令流程示意图；

图 8 为根据本公开第三实施例的物联网认证系统的结构示意图；以及

图 9 为根据本公开第四实施例的物联网认证系统的结构示意图。

具体实施方式

为使本公开的目的、技术方案和优点更加清楚明白，下文中将结合附图对本公开的实施例进行详细说明。需要说明的是，在不冲突的情况下，本公开中的实施例及实施例中的特征可以相互任意组合。

富通信套件(Rich Communication Suite)是由全球移动通信联盟（GSMA）推进的、构建在 IMS（IP Multimedia Subsystem）网络之上的、具有统一业务集定义的技术标准。RCS 基于手机电话号码簿实现

语音、消息、状态呈现等多媒体业务。用户通过智能终端上的软件客户端来使用 RCS 业务。在一些情况下，RCS 业务可以类似于互联网的 QQ、微信等即时通信业务并且可以直接使用手机上保存的电话号码来自动显示用户的在线状态，从而实时地进行语音、图片、视频等多种方式的沟通。除非另有所指，根据本公开实施例的物联网认证系统和物联网认证方法基于 RCS 实现。

需要说明的是，使用本公开提供的物联网认证方法之前，用户需要成为运营商实名认证机制认证成功的 RCS 用户。用户使用自己的 RCS 用户账户作为物联网账户登录 RCS 终端。本公开中涉及的消息交互均使用 RCS 环境中的信令通道。RCS 具有较高信息整合能力和及时性，同时也具有更好的多媒体呈现能力和极佳的用户体验。RCS 通信还具有较好安全性，用户注册 RCS 平台需要通过运营商网络国家实名制认证。在 RCS 平台下的用户登录场景中，通过会话初始协议(Session Initiation Protocol，SIP)中的注册（REGISTER）信令系列流程来确认 SIP 设备并认证 SIP 代理，从而有效地建立一个安全的信令交互通道。

如图 1 所示，本公开提供了一种物联网认证系统，包括第一用户终端 10、第一富通信套件服务器 20 和第一目标设备 30，其中，第一用户终端 10 用于接受用户的交互通信请求，生成携带第二绑定关系信息的远程认证请求消息，并将远程认证请求消息发送至第一目标设备 30；第一富通信套件服务器 20 用于在第一用户终端 10 和/或富通信账号与第一目标设备 30 建立绑定关系并且在认证绑定关系过程中，实现第一用户终端 10 和第一目标设备 30 之间的消息转发；第一目标设备 30 用于存储第一用户终端 10 和/或富通信账号与第一目标设备 30 之间的第一绑定关系信息，接收远程认证请求消息，并且检测远程认证请求消息中的第二绑定关系信息与存储的第一绑定关系信息是否一致，其中，如果检测远程认证请求消息中的第二绑定关系信息与第一绑定关系信息一致，则认证通过并且所述第一目标设备接受第一用户终端 10 的交互通信请求。

在一个示例性实施例中，所述第一富通信套件服务器 20 还用于预先建立第一用户终端 10 与富通信账号之间的绑定关系。

在一个示例性实施例中，所述远程认证请求消息中携带时间戳信息；并且所述第一目标设备 30 还用于在验证所述远程认证请求消息中的第二绑定关系信息与所述第一绑定关系信息是否一致时，检测所述时间戳是否超时，其中，如果所述远程认证请求消息中的第二绑定关系信息与所述第二绑定关系信息一致且所述时间戳不超时，则认证通过。

需要说明的是，在所述远程认证请求消息中携带时间戳信息的情况下，所述时间戳设定的超时时间可以较短，以确保操作的时效性，同时增强消息的防伪能力。

在一个示例性实施例中，所述第一用户终端 10 还用于在生成所述远程认证请求消息之前，要求用户输入生物信息认证。

需要说明的是，生物识别技术是一种便捷并且安全的认证方式。用于生物识别的生物特征可以包括手形、指纹、脸形、虹膜、视网膜、脉搏、耳廓等。行为特征可以包括签字、声音、按键力度等。在一个示例性实施例中，所述生物信息认证包括但不限于指纹识别、面部识别和语音识别。

在一个示例性实施例中，所述远程认证请求消息发送时进行加密处理。

在一个示例性实施例中，所述在第一用户终端和/或富通信账号与第一目标设备之间建立的绑定关系可以在接受用户的交互通信请求前预先单独建立，也可以在接受用户的交互通信请求时建立。

所述第一用户终端 10 和/或富通信账号与第一目标设备 30 建立绑定关系的过程包括：第一用户终端 10 生成携带目标设备识别码的第二绑定请求消息，并经由第一富通信套件服务器 20 将第二绑定请求消息发送至第一目标设备 30；第一目标设备 30 接收第二绑定请求消息，检测第二绑定请求消息中的目标设备识别码信息与本地信息是否一致，其中，如果第二绑定请求消息中的目标设备识别码信息与本地信息一致，则绑定成功，接受第一用户终端 10 的绑定请求。

如图 2 所示，本公开还提供了一种物联网认证系统，包括第二用户终端 40、第二富通信套件服务器 50、第二目标设备 70 和第三方服

务器 60，其中，

所述第二用户终端 40 用于接受用户的交互通信请求，生成携带第二绑定关系信息的远程认证请求消息，并将远程认证请求消息发送至所述第二目标设备 70；

所述第二富通信套件服务器 50 用于在第二用户终端和/或富通信账号与第二目标设备建立绑定关系以及认证绑定关系过程中，在第二用户终端 40 和第三方服务器 60 之间进行消息转发；

所述第三方服务器 60 用于存储第二用户终端 40 和/或富通信账号与第二目标设备 70 之间的第一绑定关系信息，接收远程认证请求消息，验证远程认证请求消息中的第二绑定关系信息与第一绑定关系信息是否一致，其中，如果远程认证请求消息中的第二绑定关系信息与第一绑定关系信息一致，将所述远程认证请求消息转发至所述第二目标设备 70；

所述第二目标设备 70 用于接收远程认证请求消息，检测远程认证请求消息中的目标设备信息与本地信息是否一致，其中，如果远程认证请求消息中的目标设备信息与本地信息一致，则认证通过并且所述第二目标设备接受第二用户终端 40 的交互通信请求。

在一个示例性实施例中，所述第二富通信套件服务器 50 还用于预先建立第二用户终端 40 与富通信账号之间的绑定关系。

在一个示例性实施例中，所述远程认证请求消息中携带时间戳信息；所述第三方服务器 60 还用于在验证所述远程认证请求消息中的第二绑定关系信息与所述第一绑定关系信息是否一致时，检测所述时间戳是否超时，其中，如果所述远程认证请求消息中的第二绑定关系信息与所述第一绑定关系信息一致且时间戳不超时，则将所述远程认证请求消息转发至所述第二目标设备 70；所述第二目标设备 70 还用于在检测远程认证请求消息中的目标设备信息与本地信息是否一致时，检测所述时间戳是否超时，其中，如果远程认证请求消息中的目标设备信息与本地信息一致且时间戳不超时，则认证通过。

在一个示例性实施例中，所述第二用户终端 40 还用于在生成所述远程认证请求消息前，要求用户输入生物信息认证。

在一个示例性实施例中，所述生物信息认证包括但不限于指纹识别、面部识别和语音识别。

在一个示例性实施例中，所述远程认证请求消息发送时进行加密处理。

在一个示例性实施例中，所述第三方服务器 60 可以为 RCS 公众号服务器。

在一个示例性实施例中，所述在第二用户终端和/或富通信账号与第二目标设备之间建立的绑定关系可以在接受用户的交互通信请求前预先单独建立，也可以在接受用户的交互通信请求时建立。

所述第二用户终端 40 和/或富通信账号与第二目标设备 70 建立绑定关系的过程包括：第二用户终端 40 生成携带第二目标设备 70 的目标设备识别码的绑定请求消息，并经由第二富通信套件服务器 50 将绑定请求消息发送至第三方服务器 60；第三方服务器 60 接收绑定请求消息，检测是否预先存储有第二目标设备 70 的信息，其中，如果预先存储有第二目标设备 70 的信息，则将绑定请求消息发送至第二目标设备 70；第二目标设备 70 接收绑定请求消息，检测绑定请求消息中的目标设备识别码信息与本地信息是否一致，其中，如果绑定请求消息中的目标设备识别码信息与本地信息一致，则绑定成功并且第二目标设备 70 接受第二用户终端 40 的绑定请求。

如图 3 所示，根据本公开实施例的一种物联网认证方法，包括如下步骤：

步骤 301：通过第一富通信套件服务器转发消息以使第一用户终端和/或富通信账号与第一目标设备绑定，并将第一绑定关系信息存储在所述第一目标设备中；

步骤 302：通过所述第一用户终端发出与所述第一目标设备进行交互通信的请求，通过所述第一用户终端生成携带第二绑定关系信息的远程认证请求消息，并通过第一富通信套件服务器将所述远程认证请求消息发送至所述第一目标设备；以及

步骤 303：通过所述第一目标设备接收所述远程认证请求消息，验证所述远程认证请求消息中的第二绑定关系信息与所述第一绑定关

系信息是否一致，其中，如果所述远程认证请求消息中的第二绑定关系信息与所述第一绑定关系信息一致，则认证通过，并且所述第一目标设备接受第一用户终端的交互通信请求；如果所述远程认证请求消息中的第二绑定关系信息与所述第一绑定关系信息不一致，则认证失败，所述第一目标设备拒绝所述第一用户终端的交互通信请求。

在一个示例性实施例中，在步骤 301 之前，用户可以通过第一富通信套件服务器，预先建立第一用户终端和富通信账号之间的绑定关系。

在一个示例性实施例中，在将所述远程认证请求消息发送至所述第一目标设备时，所述远程认证请求消息中携带有时间戳信息。在一个示例性实施例中，所述第一目标设备在验证所述远程认证请求消息中的第二绑定关系信息与所述第一绑定关系信息是否一致时，检测所述时间戳是否超时，其中，如果所述远程认证请求消息中的第二绑定关系信息与所述第一绑定关系信息一致且时间戳不超时，则认证通过；如果所述远程认证请求消息中的第二绑定关系信息与所述第一绑定关系信息不一致或时间戳超时，则认证失败。

需要说明的是，当所述远程认证请求消息中携带时间戳信息时，所述时间戳设定的超时时间应当较短，以确保操作时效性，同时增强消息的防伪能力。在一个示例性实施例中，步骤 302 还包括：在将所述远程认证请求消息发送至所述第一目标设备时，对所述远程认证请求消息进行加密处理。

在一个示例性实施例中，在通过所述第一富通信套件服务器发出与所述第一目标设备进行交互通信的请求时，所述第一用户终端要求用户输入生物信息认证，其中，如果生物信息认证成功，则所述第一用户终端生成所述远程认证请求消息。在一个示例性实施例中，所述生物信息认证包括但不限于指纹识别、面部识别和语音识别。

在一个示例性实施例中，在第一用户终端和/或富通信账号与第一目标设备之间建立的所述绑定关系可以在接受用户的交互通信请求前预先单独建立，也可以在接受用户的交互通信请求时建立。

所述通过第一富通信套件转发消息以使第一用户终端和/或富通

信账号与第一目标设备的绑定的步骤包括：通过所述第一用户终端生成携带目标设备识别码的第二绑定请求消息，并经由第一富通信套件服务器将所述第二绑定请求消息发送至所述第一目标设备；以及通过所述第一目标设备接收所述第二绑定请求消息，检测所述第二绑定请求消息中的目标设备识别码信息与本地信息是否一致，如果所述第二绑定请求消息中的目标设备识别码信息与本地信息一致，则绑定成功，并且所述第一目标设备接受第一用户终端的绑定请求。

在一个示例性实施例中，如图 4 所示，根据本公开实施例的一种物联网认证方法，包括：

步骤 401：通过第二富通信套件服务器转发消息以使第二用户终端和/或富通信账号与第二目标设备的绑定，并将第一绑定关系信息存储在第三方服务器中；

步骤 402：通过第二用户终端发出与第二目标设备进行交互通信的请求，通过所述第二用户终端生成携带第二绑定关系信息的远程认证请求消息，并通过所述第二富通信套件服务器将所述远程认证请求消息发送至所述第三方服务器；

步骤 403：通过所述第三方服务器接收所述远程认证请求消息，验证远程认证请求消息中的第二绑定关系信息与所述第一绑定关系信息是否一致，其中，如果远程认证请求消息中的第二绑定关系信息与所述第一绑定关系信息一致，则将所述远程认证请求消息转发至所述第二目标设备；如果远程认证请求消息中的第二绑定关系信息与所述第一绑定关系信息不一致，则认证失败，并且所述第三方服务器拒绝第二用户终端的交互通信请求；

步骤 404：通过所述第二目标设备接收远程认证请求消息，检测远程认证请求消息中的目标设备信息与本地信息是否一致，其中，如果所述远程认证请求消息中的目标设备信息与本地信息一致，则认证通过，并且述第二目标设备接受第二用户终端的交互通信请求；如果所述远程认证请求消息中的目标设备信息与本地信息不一致，则认证失败，并且述第二目标设备拒绝第二用户终端的交互通信请求。

在一个示例性实施例中，在步骤 401 之前，用户通过第二富通信

套件服务器，预先建立第二用户终端和富通信账号之间的绑定关系。

在一个示例性实施例中，在将所述远程认证请求消息发送至所述第三方服务器或第二目标设备时，所述远程认证请求消息中携带时间戳信息。在一个示例性实施例中，步骤 403 还包括：在通过所述第三方服务器验证所述远程认证请求消息中的第二绑定关系信息与所述第一绑定关系信息是否一致时，检测所述时间戳是否超时，其中，如果所述远程认证请求消息中的第二绑定关系信息与所述第一绑定关系信息一致且时间戳不超时，则将所述远程认证请求消息转发至所述第二目标设备；如果所述远程认证请求消息中的第二绑定关系信息与所述第一绑定关系信息不一致或时间戳超时，则认证失败，并且所述第三方服务器拒绝第二用户终端的交互通信请求；在一个示例性实施例中，步骤 404 还包括：在通过所述第二目标设备检测远程认证请求消息中的目标设备信息与本地信息是否一致时，检测所述时间戳是否超时，其中，如果远程认证请求消息中的目标设备信息与本地信息一致且时间戳不超时，则认证通过，并且所述第二目标设备接受第二用户终端的交互通信请求；如果远程认证请求消息中的目标设备信息与本地信息不一致或时间戳超时，则认证失败，所述第二目标设备拒绝第二用户终端的交互通信请求。

在一个示例性实施例中，所述方法还包括：在将所述远程认证请求消息发送至所述第三方服务器或第二目标设备时，对所述远程认证请求消息进行加密处理。

在一个示例性实施例中，在通过所述第二用户终端请求与所述第二目标设备进行交互通信时，所述第二用户终端要求用户输入生物信息认证，其中，如果生物信息认证成功，所述第二用户终端生成所述远程认证请求消息。

在一个示例性实施例中，所述生物信息认证包括但不限于指纹识别、面部识别或语音识别。

在一个示例性实施例中，在第二用户终端和/或富通信账号与第二目标设备之间建立的绑定关系可以在接受用户的交互通信请求前预先单独建立，也可以在接受用户的交互通信请求时建立。

所述第二用户终端和/或富通信账号与第二目标设备建立绑定关系的过程包括：第二用户终端生成携带目标设备识别码的第二绑定请求消息，并经由第二富通信套件服务器将所述第二绑定请求消息发送至第三方服务器；第三方服务器接收绑定请求消息，检测是否预先存储有第二目标设备的信息，其中，如果预先存储有第二目标设备的信息，则将所述第二绑定请求消息发送至第二目标设备；第二目标设备接收绑定请求消息，检测所述第二绑定请求消息中的目标设备识别码信息与本地信息是否一致，其中，如果所述第二绑定请求消息中的目标设备识别码信息与本地信息一致，则绑定成功，并且第二目标设备接受第二用户终端的绑定请求。

在本公开的一个示例性实施例中，如图 5 所示，所述物联网认证方法，包括如下步骤：

步骤 501：使用 RCS 账户登录 RCS 终端，通过富通信套件服务器转发消息以使用户终端、RCS 账户与目标设备之间绑定，并将绑定关系信息存储在目标设备或第三方服务器中；

步骤 502：通过 RCS 终端发出与目标设备进行交互通信的请求；

步骤 503：通过 RCS 终端生成加密的远程认证请求消息，所述远程认证请求消息包括 RCS 账户信息、用户终端识别码、目标设备识别码和时间戳信息，其中，如果所述绑定关系信息存储在第三方服务器中，转到步骤 504；如果所述绑定关系信息存储在目标设备中，转到步骤 506；

步骤 504：通过 RCS 终端将所述远程认证请求消息发送至第三方服务器，第三方服务器接收并解析远程认证请求消息，检测远程认证请求消息中的 RCS 账户信息、用户终端识别码和目标设备识别码与预先存储的绑定关系信息是否一致以及时间戳信息是否超时，其中，如果远程认证请求消息中的 RCS 账户信息、用户终端识别码和目标设备识别码与预先存储的绑定关系信息一致且时间戳不超时，转到步骤 505；如果远程认证请求消息中的 RCS 账户信息、用户终端识别码和目标设备识别码与预先存储的绑定关系信息不完全一致或者时间戳超时，转到步骤 508；

步骤 505：通过所述第三方服务器将携带时间戳信息的远程认证请求消息发送至目标设备，目标设备接收并解析远程认证请求消息，检测远程认证请求消息中的目标设备识别码与本地识别码是否一致以及时间戳信息是否超时，其中，如果远程认证请求消息中的目标设备识别码与本地识别码一致且时间戳不超时，转到步骤 507；如果远程认证请求消息中的目标设备识别码与本地识别码不一致或时间戳信息超时，转到步骤 508；

步骤 506：通过 RCS 终端将所述远程认证请求消息发送至目标设备，目标设备接收并解析远程认证请求消息，检测远程认证请求消息中的 RCS 账户信息、用户终端识别码和目标设备识别码与预先存储的绑定信息是否一致以及时间戳信息是否超时，其中，如果远程认证请求消息中的 RCS 账户信息、用户终端识别码和目标设备识别码与预先存储的绑定信息一致且时间戳不超时，转到步骤 507；如果远程认证请求消息中的 RCS 账户信息、用户终端识别码和目标设备识别码与预先存储的绑定信息不完全一致或时间戳信息超时，转到步骤 508；

步骤 507：确定认证通过，使得所述目标设备接受用户的交互通信请求；以及

步骤 508：确定认证失败，使得所述目标设备拒绝用户的交互通信请求。

在一个示例性实施例中，如图 6 所示，所述通过富通信套件服务器转发消息以使用户终端、RCS 账户与目标设备之间绑定的步骤包括：

步骤 5011：通过 RCS 终端请求绑定目标设备以使 RCS 终端生成绑定请求信息，所述绑定请求信息包括用户终端识别码、RCS 账户、目标设备识别码，其中，如果通过第三方服务器进行绑定，转到步骤 5012；如果通过目标设备进行绑定，转到步骤 5014；

步骤 5012：通过 RCS 服务器将绑定请求信息发送至第三方服务器，第三方服务器接收绑定请求信息并解析，验证是否预先存储有目标设备信息，其中，如果预先存储有目标设备信息，转到步骤 5013；如果没有预先存储目标设备信息，转到步骤 5016；

步骤 5013：通过所述第三方服务器将绑定请求信息发送至目标设

备，目标设备接收绑定请求信息，验证绑定请求信息中的目标设备识别码与本地识别码是否一致，其中，如果绑定请求信息中的目标设备识别码与本地识别码一致，提示用户是否接受绑定，如果用户接受绑定，返回确认绑定以使第三方服务器存储绑定映射，并且转到步骤 5015；如果绑定请求信息中的目标设备识别码与本地识别码不一致或用户拒绝绑定，转到步骤 5016；

步骤 5014：通过 RCS 服务器将绑定请求信息发送至目标设备，目标设备接收并解析绑定请求信息，验证绑定请求信息中的目标设备识别码与本地识别码是否一致，其中，如果绑定请求信息中的目标设备识别码与本地识别码一致，提示用户是否接受绑定，如果用户接受绑定，返回确认绑定以使目标设备存储绑定映射，并且转到步骤 5015；如果绑定请求信息中的目标设备识别码与本地识别码不一致或用户拒绝绑定，转到步骤 5016；

步骤 5015：确定绑定成功；以及

步骤 5016：确定绑定失败。

在一个示例性实施例中，如果目标设备为 RCS 终端，目标设备可以要求用户输入生物信息认证。如果生物信息认证成功，提示用户是否接受绑定。如果生物信息认证失败，转到步骤 5016。

在一个示例性实施例中，例如，所述目标设备识别码或用户终端识别码可以为目标设备或用户终端的介质访问控制（Medium Access Control，MAC）地址、通用唯一识别码（Universally Unique Identifier，UUID）、移动用户国际号码（Mobile Station International SDN，MSISDN）或国际用户识别码（International Mobile Subscriber Identification Number，IMSI）。

在本实施例中的各个网元模块间的信令流程如图 7 所示。在图 7 中，当用户发起绑定目标设备的指令时，用户输入目标设备唯一标识。RCS 终端生成绑定 RCS 账户和目标设备的绑定请求消息，并通过 RCS 服务器转发至第三方服务器或目标设备。当用户发起远程操作目标设备的请求时，RCS 终端接受用户的远程操作请求，生成携带绑定关系信息的远程操作请求指令。如果所述绑定关系信息存储在目标设备中，

RCS 终端通过 RCS 服务器将远程操作请求指令发送至目标设备。目标设备接收到所述远程操作请求指令后，对其中的绑定关系信息进行验证。如果验证通过，则接受用户的远程操作指令。如果所述绑定关系信息存储在第三方服务器中，RCS 终端通过 RCS 服务器将远程操作请求指令发送至第三方服务器。第三方服务器接收到所述远程操作请求指令后，对其中的绑定关系信息进行验证，如果验证通过，则将远程操作指令发送至目标设备。目标设备验证目标设备识别码与本地识别码是否一致。如果目标设备识别码与本地识别码一致，则目标设备接受用户的远程操作指令。

值得说明的是，本公开所述的用户终端包括但不限于具有 RCS 应用的手机、平板电脑（PAD）等移动通讯设备。所述的目标设备至少具有联网解析 SIP 信令的能力。所述的 RCS 服务器可承载多种公共账号业务，提供包括但不限于以 SIP 信令为基础的消息收发、消息查询、修改能力。所述的第三方服务器具有独立的存储和逻辑处理能力，和 RCS 服务器互联，进而可以和 RCS 用户进行交互。

本公开还提供了几个优选的实施例对本公开进行进一步解释，但是值得注意的是，该优选实施例只是为了更好的描述本公开，并不构成对本公开不当的限定。下面的各个实施例可以独立存在，且不同实施例中的技术特点可以组合在一个实施例中一起使用。

在一个实例中，如图 8 所示，用户终端 A 带有指纹识别系统（如常见智能手机）。用户终端 A 上安装有 RCS 终端软件。用户为 RCS 用户。用户需要通过用户终端 A 远程启动车机系统设备 B，车机系统设备 B 能简单解析 SIP 信令，并设有用于存储绑定信息的数据库。用户终端 A 和车机系统设备 B 可以通过 RCS 平台实现信息交互。

（1）用户登录用户终端 A 的 RCS 系统以发起绑定请求。

（2）用户终端 A 提示用户认证指纹并输入设备 B 的唯一识别码（如发动机号），其中，如果指纹认证通过，则用户终端 A 通过 RCS 服务器的转发将携带用户终端 A 唯一识别码（如手机 UUID 或 ISDN 等）、设备 B 唯一识别码、用户 RCS 账户的加密绑定指令发送至设备 B，转到步骤（3）；如果指纹认证失败，提示用户身份有问题，结束

流程。

（3）设备 B 收到加密绑定指令并解密，显示用户终端 A 和用户 RCS 账户信息，提示用户是否接受绑定；用户操作设备 B 进行绑定确认，使得设备 B 绑定用户 RCS 帐号、用户终端 A 的唯一识别码和设备 B 的唯一识别码。

（4）在绑定完成后，发送绑定完成消息到用户终端 A；此时，用户可通过用户终端 A 远程认证模块发起启动设备 B 指令。

（5）用户终端 A 请求用户输入指纹进行身份认证。

（6）如果身份认证通过，则用户终端 A 通过 RCS 服务器的转发将携带时间戳、用户 RCS 账户、用户终端 A 唯一识别码的加密启动请求发送到设备 B，转到步骤（7）；如果身份认证失败，用户终端 A 提示用户身份异常并结束流程。

（7）设备 B 解密启动请求，核对时间戳未超时，校验用户 RCS 帐号、用户终端 A 的唯一识别码和设备 B 的唯一识别码与存储的绑定信息是否一致；如果校验通过，设备 B 启动车机发动机；如果校验失败，设备 B 忽略该请求。

在一个实例中，如图 9 所示，用户终端 C 带有指纹识别系统。用户终端 C 上安装有 RCS 终端软件。用户为 RCS 用户。用户需要通过用户终端 C 远程打开门禁设备 D，门禁系统设备 D 能简单解析 SIP 信令。

（a）用户登录用户终端 C 上的 RCS 系统，并进入门禁设备 D 的 RCS 公众号服务器。

（b）用户发起绑定请求，用户终端 C 提示用户进行指纹认证；用户输入门禁设备 D 的唯一识别码（如网络模块 MAC 地址）以发起绑定；如果认证通过，则用户终端 C 通过 RCS 服务器的转发将发起绑定指令发送至 RCS 公众号服务器，转到步骤（c）；如果认证失败，用户终端 C 提示用户身份异常并结束流程。

（c）RCS 公众号服务器解密信息，确认是否存在门禁设备 D；如果存在门禁设备 D，向门禁设备 D 发起确认信息；门禁设备 D 提示用户是否接受绑定，以使用户操作门禁设备 D 进行绑定确认；用户确认后，公众号系统绑定用户 RCS 帐号、用户终端 C 的唯一识别码和门禁

设备 D 的唯一识别码，转到步骤（d）；如果不存在设备 D 或用户拒绝绑定设备 D，用户终端 C 流程结束。

（d）绑定完成后，用户通过用户终端 C 远程认证模块发起解锁指令。

（e）用户终端 C 请求用户输入指纹进行身份认证。

（f）如果身份认证通过，用户终端 C 通过 RCS 服务器的转发将携带时间戳、用户 RCS 账户、用户终端 C 唯一识别码和门禁设备 D 的唯一识别码的加密解锁请求发送到 RCS 公众号服务器，转到步骤（g）；如果身份认证失败，用户终端 C 提示用户身份异常并结束流程。

（g）RCS 公众号服务器解密解锁请求，核对时间戳未超时，校验用户 RCS 账户、用户终端 C 唯一识别码和门禁设备 D 的唯一识别码与存储的绑定信息是否一致，如果一致，将携带时间戳和门禁设备 D 唯一识别码的加密解锁指令发送到门禁设备 D，转到步骤（h）；如果校验不一致或者时间戳超时，用户终端 C 提示用户身份异常并结束流程。

（h）门禁设备 D 解密解锁请求后，核对时间戳未超时，校验解锁指令中的唯一识别码与本设备唯一识别码是否一致；如果一致，门禁设备 D 解锁；如果不一致，忽略该请求。

在一个实例中，用户终端 E 带有指纹识别系统。用户终端 E 上安装有 RCS 终端软件。用户为 RCS 用户。用户需要通过用户终端 E 远程解锁终端设备 F。终端设备 F 上预装 RCS 软件客户端且登录 RCS 账户。

（ⅰ）用户终端 E 登录 RCS 系统，并与终端设备 F 进行绑定。

（ⅱ）用户终端 E 提示用户进行指纹认证；如果指纹认证通过，用户终端 E 通过 RCS 服务器的转发将携带用户终端 E 的用户 RCS 账户的加密绑定指令发送至终端设备 F；如果指纹认证失败，用户终端 E 提示用户身份异常并结束流程。

（ⅲ）终端设备 F 收到绑定指令并解密，显示用户终端 E 的绑定指令，并提示用户是否接受绑定。

（ⅳ）终端设备 F 请求用户输入指纹验证身份；如果身份验证通过且接受绑定，终端设备 F 发送绑定回执信息至用户终端 E，记录用户终端 E 的授权用户信息，转到步骤（ⅴ）；如果身份验证失败或拒

绝绑定，用户终端 E 流程结束。

（ v ）用户终端 E 通过绑定回执信息来记录终端设备 F 的绑定信息，其中，用户在解锁设备列表中可见终端设备 F；用户通过用户终端 E 远程认证模块发起启动指令至终端设备 F。

（ vi ）用户终端 E 请求用户输入指纹进行身份认证。

（vii）如果身份认证通过，通过 RCS 服务器的转发，用户终端 E 发送携带时间戳、用户终端 E 的用户 RCS 账户的加密启动请求到终端设备 F，转到步骤（viii）；如果身份认证失败，提示用户身份有问题，流程结束。

（viii）终端设备 F 解密启动请求，核对时间戳未超时，检验启动请求中的用户信息是否为授权用户，如果校验通过，解锁终端设备 F；如果校验失败，则忽略该启动请求。

本公开提供的物联网认证系统和物联网认证方法，通过 RCS 账户发起远程认证指令，利用富通信套件（Rich Communication Suite，RCS）服务器进行远程认证。指令防伪基于 RCS 安全信令通道，通过检测发起方设备、对端设备、RCS 账户信息进行远程认证。借助 RCS 服务的实时性、安全性、规范性，便捷有效地实现物联网环境中用户和设备、设备和设备间的安全交互。

本公开有效地将传统生物识别和新的 RCS 富通信方式结合，充分发挥生物识别系统和 RCS 富通信的优势，可有效避免服务器生物信息算法分析，减少服务器认证压力。一方面，将生物认证方式运用于物联网中，降低用户学习成本，有效实现人与物、物与物的安全认证。另一方面，采用统一的信令交互方式透传认证信息，统一交互方案，实现一个统一的远程认证模块，促使各个设备厂商低开发成本，高效部署安全认证环境。同时，通过对 RCS 模块功能的扩充，大大提高用户粘度。

本领域普通技术人员可以理解上述方法中的全部或部分步骤可通过程序来指令相关硬件完成，所述程序可以存储于计算机可读存储介质中，如只读存储器、磁盘或光盘等。上述实施例的全部或部分步骤也可以使用一个或多个集成电路来实现，相应地，上述实施例中的各

模块/单元可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。本公开不限制于任何特定形式的硬件和软件的结合。

以上所述仅为本公开的优选实施例而已，并不用于限制本公开，对于本领域的技术人员来说，本公开可以有各种更改和变化。凡在本公开的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本公开的保护范围之内。

权 利 要 求

1. 一种物联网认证系统，包括第一用户终端、第一富通信套件服务器和第一目标设备，其中，

所述第一用户终端用于接受用户的交互通信请求，生成携带第二绑定关系信息的远程认证请求消息，并将所述远程认证请求消息发送至所述第一目标设备；

所述第一富通信套件服务器用于在第一用户终端和/或富通信账号与所述第一目标设备建立绑定关系以及认证绑定关系过程中，实现所述第一用户终端与所述第一目标设备之间的消息转发；

所述第一目标设备用于存储所述第一用户终端和/或富通信账号与所述第一目标设备之间的第一绑定关系信息，接收所述远程认证请求消息，并且检测所述远程认证请求消息中的所述第二绑定关系信息与所述第一绑定关系信息是否一致，其中，如果所述远程认证请求消息中的第二绑定关系信息与所述第一绑定关系信息一致，则认证通过并且所述第一目标设备接受所述第一用户终端的交互通信请求。

2. 根据权利要求 1 所述的物联网认证系统，其中，所述远程认证请求消息中携带时间戳信息；并且

所述第一目标设备还用于在验证所述远程认证请求消息中的绑定关系信息与所述存储的绑定关系信息是否一致时，检测所述时间戳是否超时，其中，如果所述远程认证请求消息中的第二绑定关系信息与所述第二绑定关系信息一致且时间戳不超时，则认证通过。

3. 根据权利要求 1 所述的物联网认证系统，其中，所述第一用户终端还用于在生成所述远程认证请求消息之前，要求用户输入生物信息认证。

4. 根据权利要求 3 所述的物联网认证系统，其中，所述生物信息认证包括指纹识别、面部识别和语音识别中的至少一者。

5. 一种物联网认证系统，包括第二用户终端、第二富通信套件服务器、第二目标设备和第三方服务器，其中，

所述第二用户终端用于接受用户的交互通信请求，生成携带第二绑定关系信息的远程认证请求消息，并将所述远程认证请求消息发送至所述第二目标设备；

所述第二富通信套件服务器用于在所述第二用户终端和/或富通信账号与所述第二目标设备建立绑定关系以及认证绑定关系过程中，实现所述第二用户终端与所述第三方服务器之间的消息转发；

所述第三方服务器用于存储所述第二用户终端和/或富通信账号与第二目标设备之间的第一绑定关系信息，接收所述远程认证请求消息，验证远程认证请求消息中的所述第二绑定关系信息与所述第一绑定关系信息是否一致，其中，如果远程认证请求消息中的所述第二绑定关系信息与所述第一绑定关系信息一致，将所述远程认证请求消息转发至所述第二目标设备；

所述第二目标设备用于接收远程认证请求消息，检测远程认证请求消息中的目标设备信息与本地信息是否一致，其中，如果远程认证请求消息中的目标设备信息与本地信息一致，则认证通过并且所述第二目标设备接受所述第二用户终端的交互通信请求。

6. 根据权利要求 5 所述的物联网认证系统，其中，所述远程认证请求消息中携带时间戳信息；

所述第三方服务器还用于在验证所述远程认证请求消息中的第二绑定关系信息与所述第一绑定关系信息是否一致时，检测所述时间戳是否超时，其中，如果所述远程认证请求消息中的第二绑定关系信息与所述第一绑定关系信息一致且时间戳不超时，则将所述远程认证请求消息转发至所述第二目标设备；

所述第二目标设备还用于在检测远程认证请求消息中的目标设备信息与本地信息是否一致时，检测所述时间戳是否超时，其中，如果远程认证请求消息中的目标设备信息与本地信息一致且时间戳不超时，

则认证通过。

7. 一种物联网认证方法，包括：

通过第一富通信套件服务器转发消息以使第一用户终端和/或富通信账号与第一目标设备绑定，并将第一绑定关系信息存储在所述第一目标设备中；

通过所述第一用户终端发出与所述第一目标设备进行交互通信的请求，通过所述第一用户终端生成携带第二绑定关系信息的远程认证请求消息，并将所述远程认证请求消息发送至所述第一目标设备；以及

通过所述第一目标设备接收所述远程认证请求消息，验证所述远程认证请求消息中的第二绑定关系信息与所述第一绑定关系信息是否一致，如果所述远程认证请求消息中的第二绑定关系信息与所述第一绑定关系信息一致，则认证通过，并且所述第一目标设备接受第一用户终端的交互通信请求。

8. 根据权利要求 7 所述的物联网认证方法，其中，

在将所述远程认证请求消息发送至所述第一目标设备时，所述远程认证请求消息中携带时间戳信息，并且

所述方法还包括：在验证所述远程认证请求消息中的第二绑定关系信息与所述第一绑定关系信息是否一致时，检测所述时间戳是否超时，其中，如果所述远程认证请求消息中的第二绑定关系信息与所述第一绑定关系信息一致且时间戳不超时，则认证通过。

9. 根据权利要求 7 所述的物联网认证方法，还包括：在将所述远程认证请求消息发送至所述第一目标设备时，对所述远程认证请求消息进行加密处理。

10. 根据权利要求 7 所述的物联网认证方法，其中，在通过所述第一富通信套件服务器发出与所述第一目标设备进行交互通信的请求

时，所述第一用户终端要求用户输入生物信息认证，其中，如果生物信息认证成功，则所述第一用户终端生成所述远程认证请求消息。

11. 一种物联网认证方法，包括：

通过第二富通信套件服务器转发消息以使第二用户终端和/或富通信账号与第二目标设备的绑定，并将第一绑定关系信息存储在第三方服务器中；

通过第二用户终端发出与第二目标设备进行交互通信的请求，通过所述第二用户终端生成携带第二绑定关系信息的远程认证请求消息，并将所述远程认证请求消息发送至所述第三方服务器；

通过所述第三方服务器接收所述远程认证请求消息，验证所述远程认证请求消息中的第二绑定关系信息与所述第一绑定关系信息是否一致，其中，如果所述远程认证请求消息中的第二绑定关系信息与所述第一绑定关系信息一致，将所述远程认证请求消息转发至所述第二目标设备；

通过所述第二目标设备接收远程认证请求消息，检测所述远程认证请求消息中的目标设备信息与本地信息是否一致，其中，如果所述远程认证请求消息中的目标设备信息与本地信息一致，则认证通过，并且述第二目标设备接受第二用户终端的交互通信请求。

12. 根据权利要求 11 所述的物联网认证方法，其中，在将所述远程认证请求消息发送至所述第三方服务器时，所述远程认证请求消息中携带时间戳信息，

所述方法还包括：在通过所述第三方设备验证所述远程认证请求消息中的第二绑定关系信息与所述第一绑定关系信息是否一致时，检测所述时间戳是否超时，其中，如果所述远程认证请求消息中的第二绑定关系信息与所述第一绑定关系信息一致且时间戳不超时，则认证通过；以及

在通过所述第二目标设备检测远程认证请求消息中的目标设备信息与本地信息是否一致时，检测所述时间戳是否超时，其中，如果远

程认证请求消息中的目标设备信息与本地信息一致且时间戳不超时，则认证通过，并且所述第二目标设备接受第二用户终端的交互通信请求。

13. 根据权利要求 11 所述的物联网认证方法，还包括：在将所述远程认证请求消息发送至所述第三方服务器时，对所述远程认证请求消息进行加密处理。

14. 根据权利要求 11 所述的物联网认证方法，其中，在通过所述第二富通信套件服务器请求与所述第三方设备进行交互通信时，所述第二用户终端要求用户输入生物信息认证，其中，如果生物信息认证成功，所述第二用户终端生成所述远程认证请求消息。

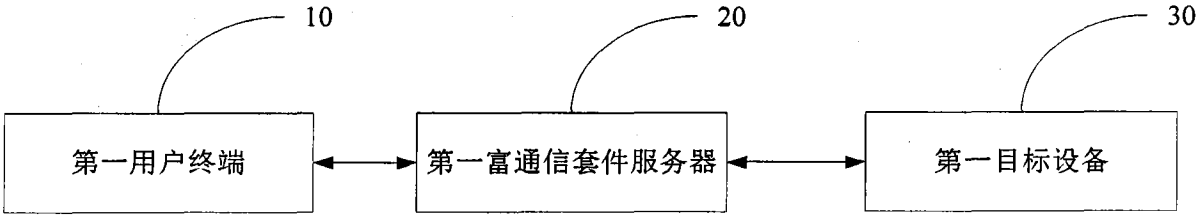

图 1

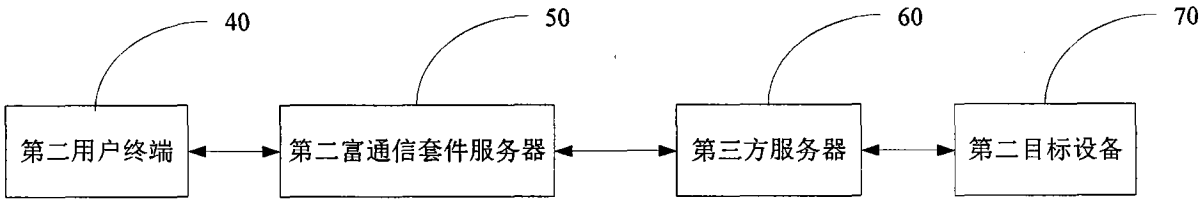

图 2

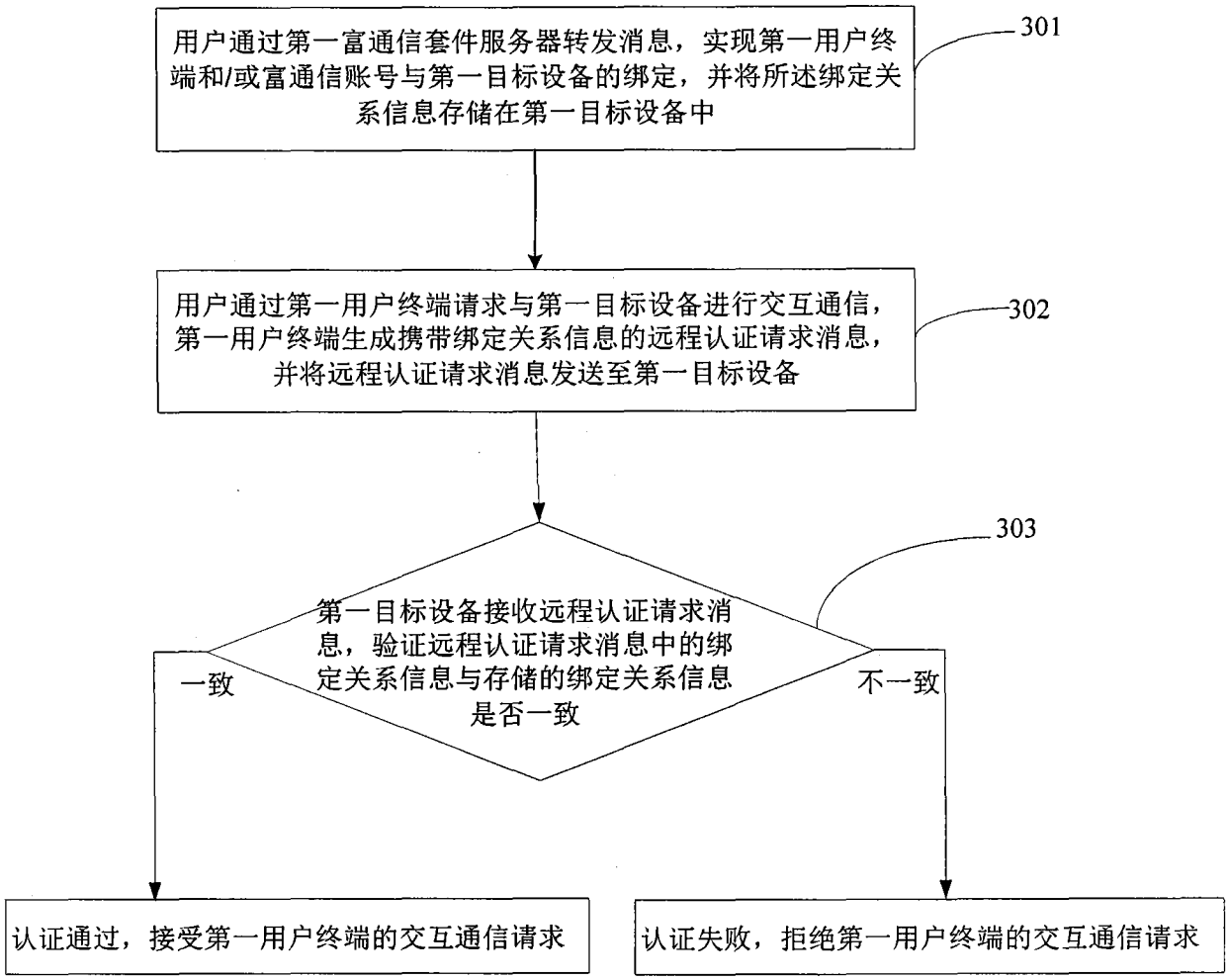

图 3

替换页（细则第26条）

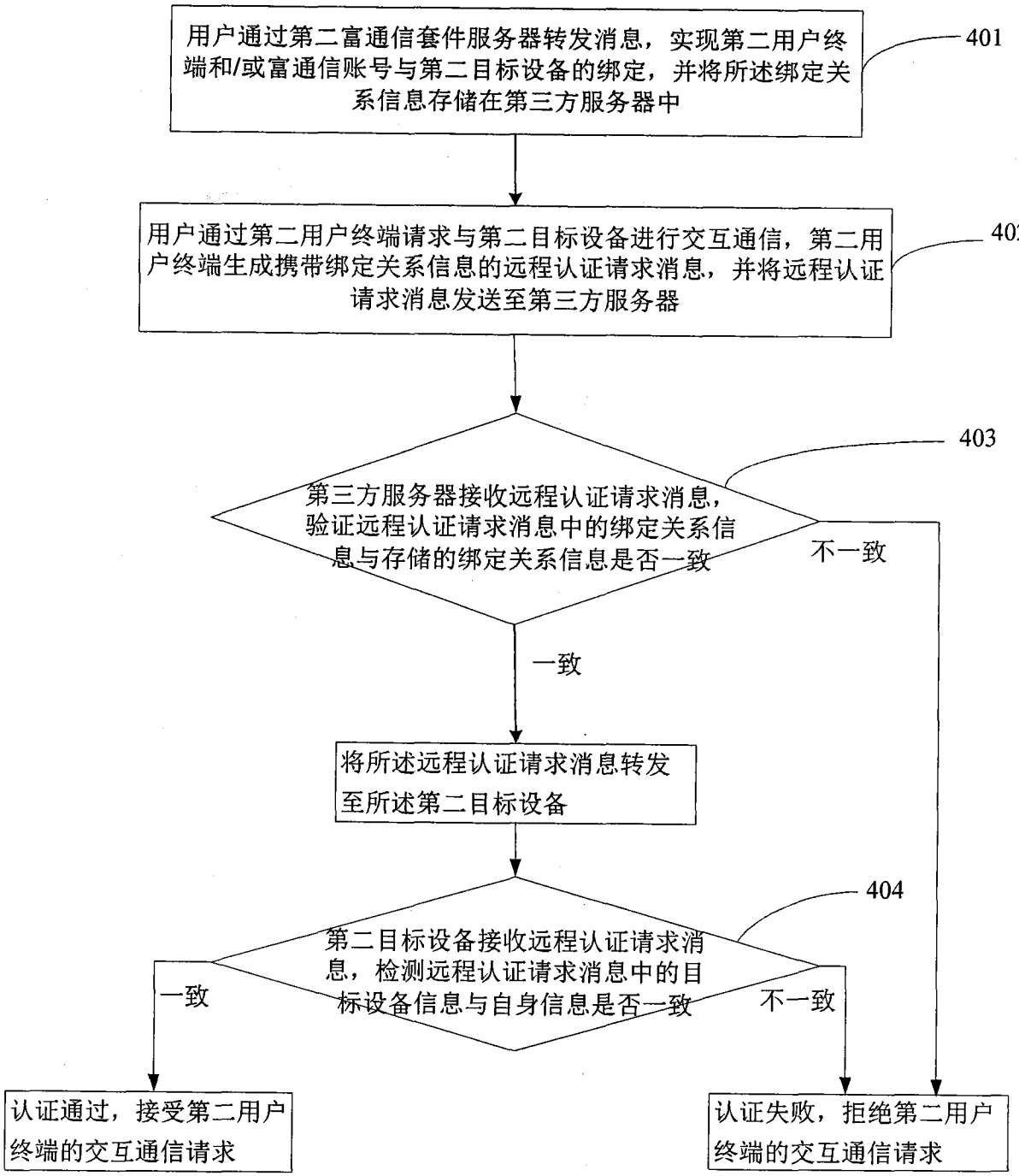
用户通过第二富通信套件服务器转发消息，实现第二用户终端和/或富通信账号与第二目标设备的绑定，并将所述绑定关系信息存储在第三方服务器中
401
用户通过第二用户终端请求与第二目标设备进行交互通信，第二用户终端生成携带绑定关系信息的远程认证请求消息，并将远程认证请求消息发送至第三方服务器
402
第三方服务器接收远程认证请求消息，验证远程认证请求消息中的绑定关系信息与存储的绑定关系信息是否一致
403
不一致
一致
将所述远程认证请求消息转发至所述第二目标设备
第二目标设备接收远程认证请求消息，检测远程认证请求消息中的目标设备信息与自身信息是否一致
404
一致
不一致
认证通过，接受第二用户终端的交互通信请求
认证失败，拒绝第二用户终端的交互通信请求

图 4

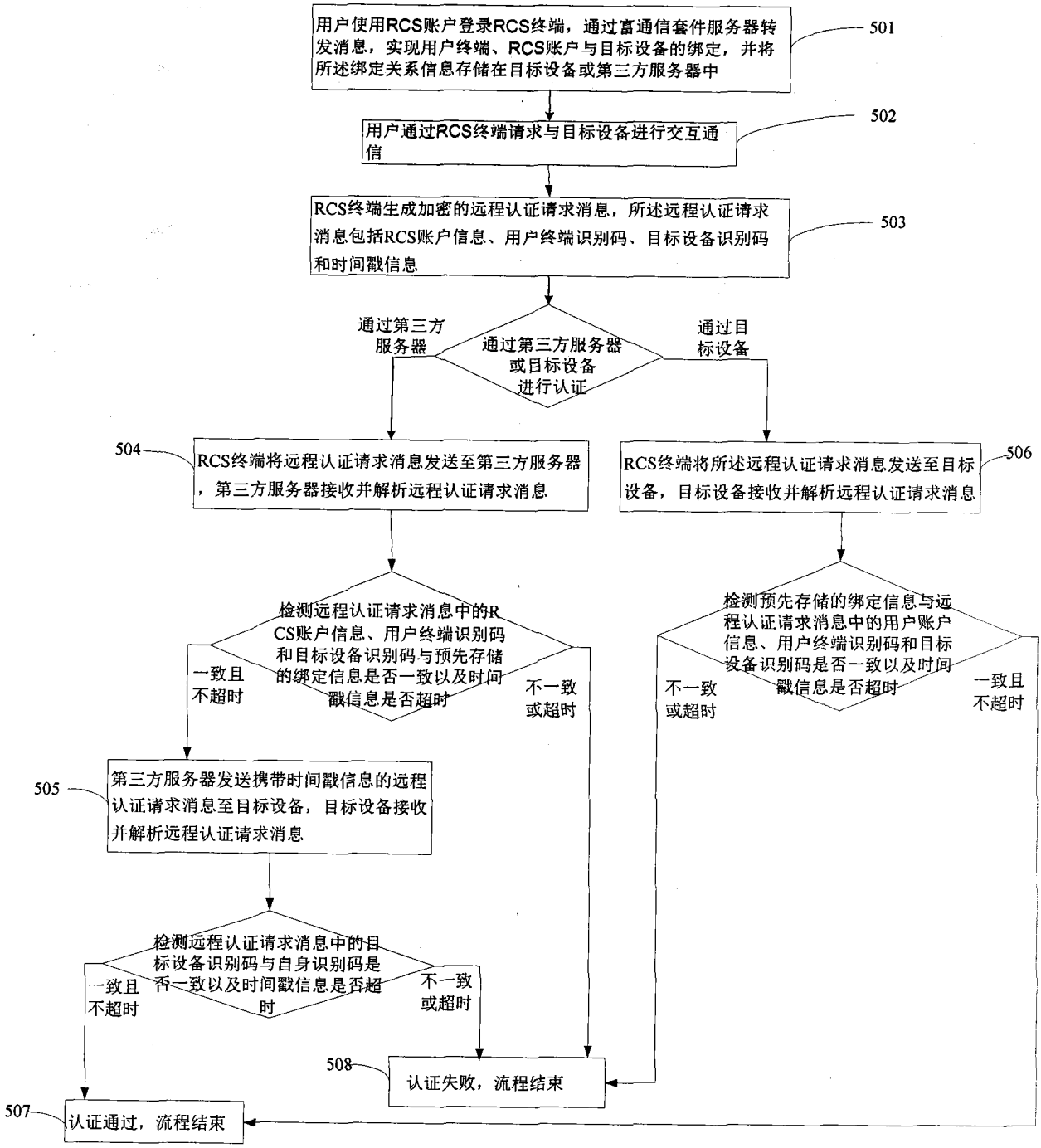
用户使用RCS账户登录RCS终端，通过富通信套件服务器转发消息，实现用户终端、RCS账户与目标设备的绑定，并将所述绑定关系信息存储在目标设备或第三方服务器中
501
用户通过RCS终端请求与目标设备进行交互通信
502
RCS终端生成加密的远程认证请求消息，所述远程认证请求消息包括RCS账户信息、用户终端识别码、目标设备识别码和时间戳信息
503
通过第三方服务器或目标设备进行认证
通过第三方服务器
通过目标设备
504
RCS终端将远程认证请求消息发送至第三方服务器，第三方服务器接收并解析远程认证请求消息
506
RCS终端将所述远程认证请求消息发送至目标设备，目标设备接收并解析远程认证请求消息
检测远程认证请求消息中的RCS账户信息、用户终端识别码和目标设备识别码与预先存储的绑定信息是否一致以及时间戳信息是否超时
一致且不超时
不一致或超时
检测预先存储的绑定信息与远程认证请求消息中的用户账户信息、用户终端识别码和目标设备识别码是否一致以及时间戳信息是否超时
不一致或超时
一致且不超时
505
第三方服务器发送携带时间戳信息的远程认证请求消息至目标设备，目标设备接收并解析远程认证请求消息
检测远程认证请求消息中的目标设备识别码与自身识别码是否一致以及时间戳信息是否超时
一致且不超时
不一致或超时
508
认证失败，流程结束
507
认证通过，流程结束

图 5

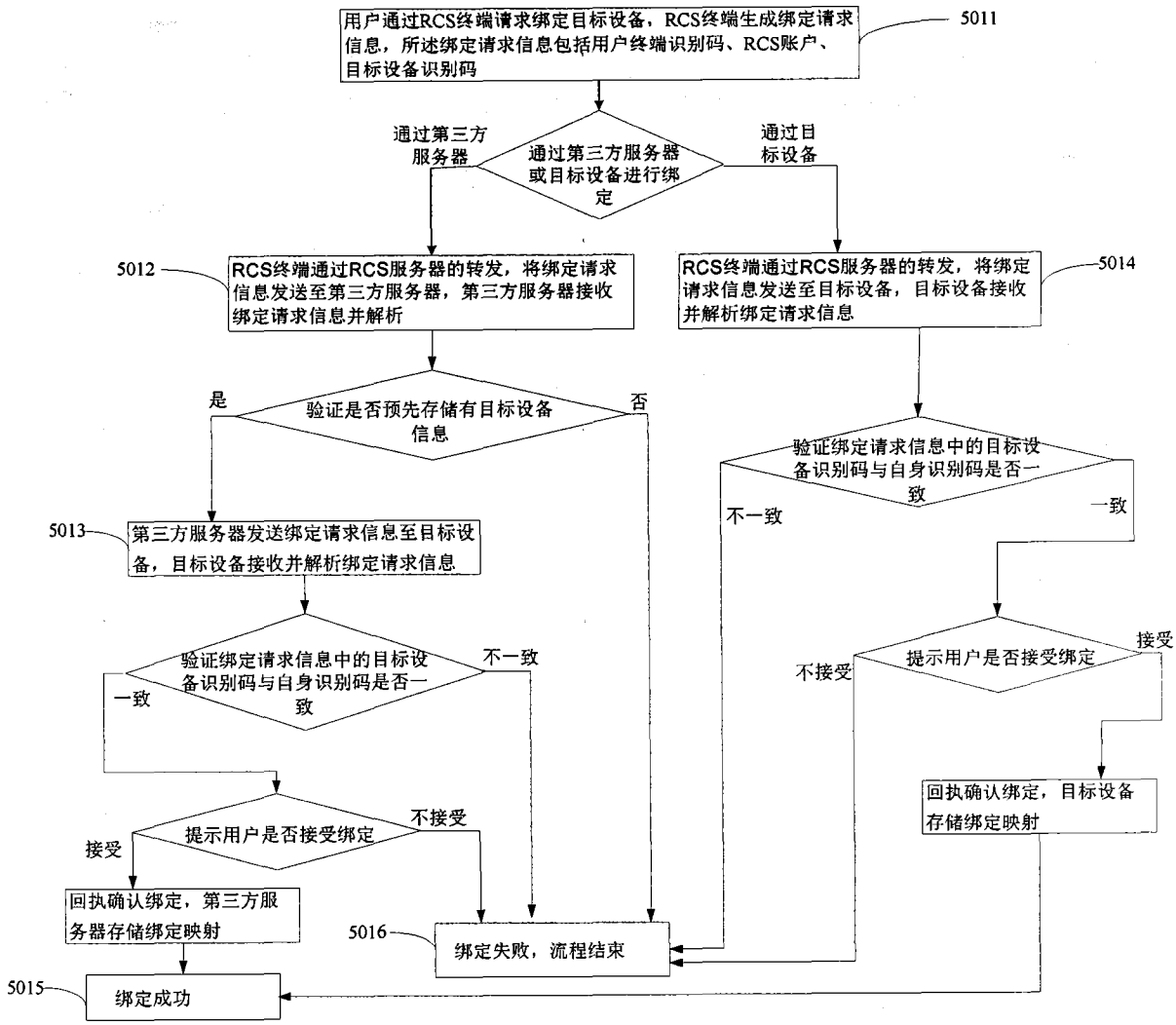

图 6

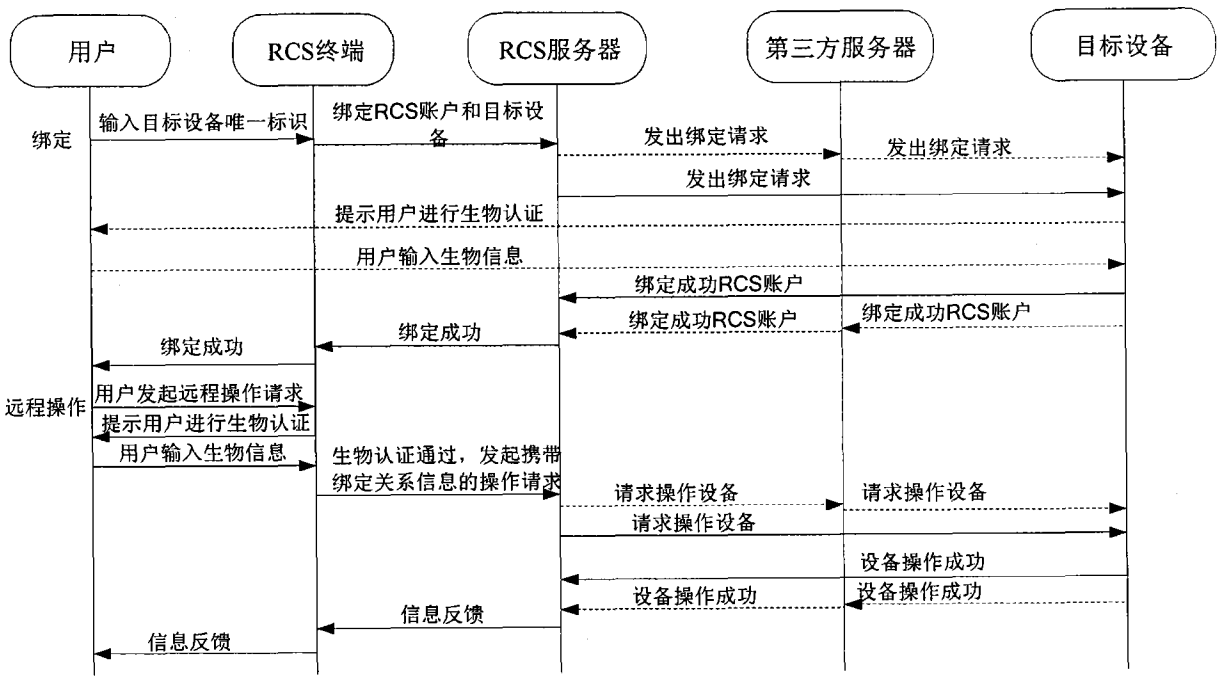

图 7

替换页（细则第26条）

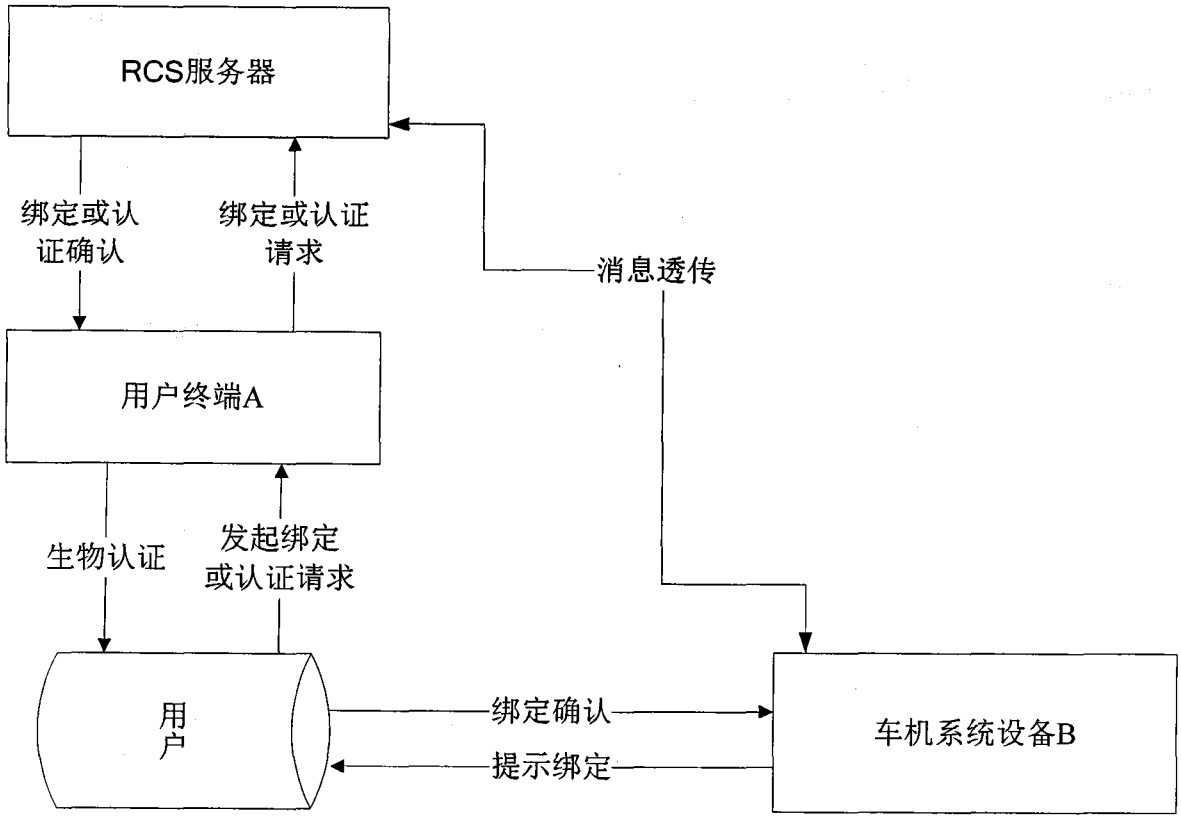

图 8

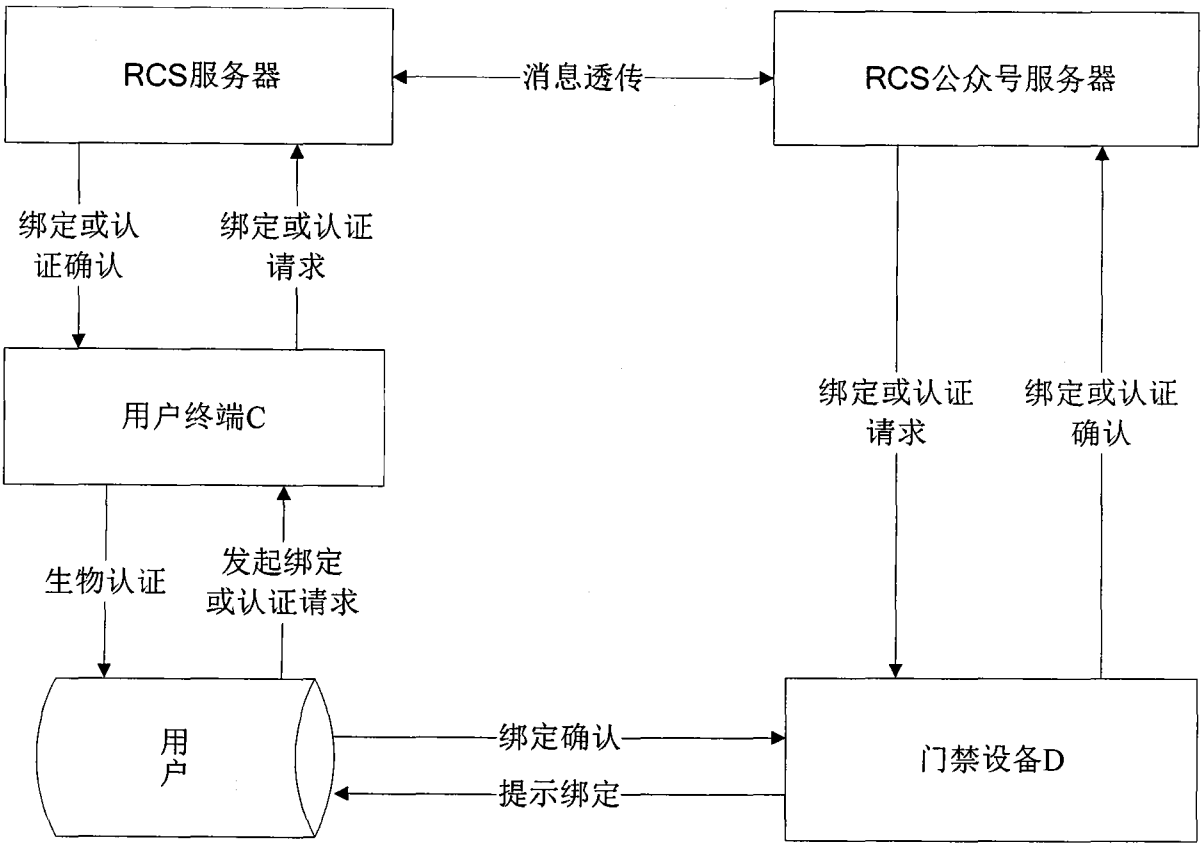

图 9

替换页（细则第26条）

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/077527

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i; H04L 12/58 (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

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)

CNABS, CNTXT, CNKI, VEN, WOTXT, USTXT: 富通信套件, 富通信, 融合通信, RCS, 物联网, 远程, 认证, 验证, 服务器, 终端, 客户端, 绑定, 识别码, MAC 地址, UUID, ISDN, IMSI, 第三方, Rich Communication Suite, Internet of things, remote, authenticate, server, terminal, client, UE, bind, identification code, ID, MAC address? third party

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 103475713 A (BEIJING SI-TECH INFORMATION TECHNOLOGY CO., LTD.) 25 December 2013 (25.12.2013), see claim 1; description, paragraphs [0002], [0070]-[0077], [0090]-[0100] and [0108]; and figures 1 and 4	1-14
A	CN 103999429 A (ORANAGE, PARIS) 20 August 2014 (20.08.2014), see entire document	1-14
A	CN 104468145 A (HUAWEI TECHNOLOGIES CO., LTD.) 25 March 2015 (25.03.2015), see entire document	1-14
A	EP 2161962 B1 (TELIASONERA AB) 20 February 2013 (20.02.2013), see entire document	1-14

☐ 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
11 May 2018	22 May 2018

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

Authorized officer
WU, Xu
Telephone No. (86-10) 62089859

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/077527

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103475713 A	25 December 2013	None	
CN 103999429 A	20 August 2014	EP 2769526 A1	27 August 2014
		FR 2981818 A1	26 April 2013
		WO 2013057437 A1	25 April 2013
		US 2014226657 A1	14 August 2014
CN 104468145 A	25 March 2015	CN 104468145 B	16 March 2018
		WO 2016086817 A8	09 September 2016
		WO 2016086817 A1	09 June 2016
EP 2161962 B1	20 February 2013	EP 2161962 A1	10 March 2010

国际检索报告

国际申请号
PCT/CN2018/077527

A. 主题的分类

H04L 29/06(2006.01)i; H04L 12/58(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

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）)

CNABS,CNTXT,CNKI,VEN,WOTXT,USTXT:富通信套件，富通信，融合通信，RCS，物联网，远程，认证，验证，服务器，终端，客户端，绑定，识别码，MAC地址，UUID，ISDN，IMSI，第三方，Rich Communication Suite，Internet of things，remote，authenticate，server，terminal，client，UE，bind，identification code，ID，MAC address，third party

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 103475713 A (北京思特奇信息技术股份有限公司) 2013年 12月 25日 (2013-12-25) 参见权利要求1；说明书第0002、0070-0077、0090-0100和0108段；图1和4	1-14
A	CN 103999429 A (橙公司) 2014年 8月 20日 (2014-08-20) 参见全文	1-14
A	CN 104468145 A (华为技术有限公司) 2015年 3月 25日 (2015-03-25) 参见全文	1-14
A	EP 2161962 B1 (TELIASONERA AB) 2013年 2月 20日 (2013-02-20) 参见全文	1-14

☐ 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 5月 11日	2018年 5月 22日

ISA/CN的名称和邮寄地址	受权官员
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	吴旭
传真号 (86-10)62019451	电话号码 86-010-62089859

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/077527

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	103475713	A	2013年 12月 25日	无			
CN	103999429	A	2014年 8月 20日	EP	2769526	A1	2014年 8月 27日
				FR	2981818	A1	2013年 4月 26日
				WO	2013057437	A1	2013年 4月 25日
				US	2014226657	A1	2014年 8月 14日
CN	104468145	A	2015年 3月 25日	CN	104468145	B	2018年 3月 16日
				WO	2016086817	A8	2016年 9月 9日
				WO	2016086817	A1	2016年 6月 9日
EP	2161962	B1	2013年 2月 20日	EP	2161962	A1	2010年 3月 10日