(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 24 日 (24.08.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/140214 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01) *H04L 9/32* (2006.01)

(21) 国际申请号: PCT/CN2017/072879

(22) 国际申请日: 2017 年 2 月 4 日 (04.02.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610090043.2 2016 年 2 月 17 日 (17.02.2016) 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: **张黎黎 (ZHANG, Lili)**; 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)。 **陈航 (CHEN, Hang)**; 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, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

(54) **Title**: COMMUNICATION METHOD AND APPARATUS

(54) **发明名称** : 通讯方法及装置

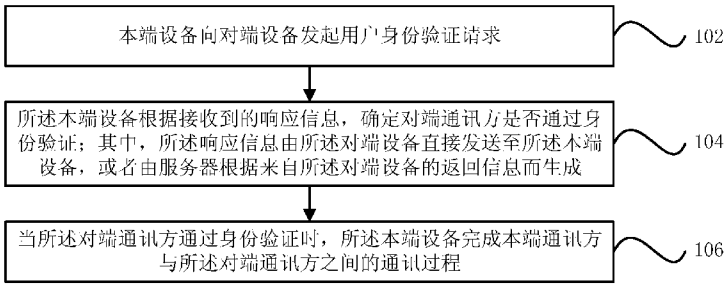

图 1

102 A LOCAL END DEVICE INITIATES A USER IDENTITY VERIFICATION REQUEST TO AN OPPOSITE END DEVICE

104 THE LOCAL END DEVICE DETERMINES WHETHER AN OPPOSITE END COMMUNICATION PARTY HAS PASSED IDENTITY VERIFICATION ACCORDING TO RECEIVED RESPONSE INFORMATION, WHEREIN THE RESPONSE INFORMATION IS DIRECTLY SENT TO THE LOCAL END DEVICE BY THE OPPOSITE END DEVICE, OR IS PRODUCED BY A SERVER ACCORDING TO RETURNED INFORMATION FROM THE OPPOSITE END DEVICE

106 WHEN THE OPPOSITE END COMMUNICATION PARTY HAS PASSED THE IDENTITY VERIFICATION, THE LOCAL END DEVICE COMPLETES A COMMUNICATION PROCESS BETWEEN A LOCAL END COMMUNICATION PARTY AND THE OPPOSITE END COMMUNICATION PARTY

(57) **Abstract**: Provided are a communication method and apparatus. The method may comprise: a local end device initiating a user identity verification request to an opposite end device; the local end device determining whether an opposite end communication party has passed identity verification according to received response information, wherein the response information is directly sent to the local end device by the opposite end device, or is produced by a server according to returned information from the opposite end device; and when the opposite end communication party has passed the identity verification, the local end device completes a communication process between a local end communication party and the opposite end communication party. Through the technical solution of the present invention, the communication security can be increased, and the benefits of the communication parties can be ensured.

(57) **摘要**: 本申请提供一种通讯方法及装置，该方法可以包括：本端设备向对端设备发起用户身份验证请求；所述本端设备根据接收到的响应信息，确定对端通讯方是否通过身份验证；其中，所述响应信息由所述对端设备直接发送至所述本端设备，或者由服务器根据来自所述对端设备的返回信息而生成；当所述对端通讯方通过身份验证时，所述本端设备完成本端通讯方与所述对端通讯方之间的通讯过程。通过本申请的技术方案，可以提升通讯安全性，保障通讯方的利益。

WO 2017/140214 A1

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

通讯方法及装置

本申请要求2016年02月17日递交的申请号为201610090043.2、发明名称为“通讯方法及装置”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

本申请涉及通讯技术领域，尤其涉及一种通讯方法及装置。

背景技术

当涉及到敏感内容时，各个通讯方往往需要确定通讯环境的安全性，以避免敏感内容泄露。在相关技术中，提出了对通讯消息进行加密，确保即便通讯消息泄露后，仍然能够保护其中的敏感内容不易被查看。

然而，在电子设备丢失或账号密码泄露等情况下，非法用户可能冒充相应用户，从其他用户处获得敏感内容，造成严重损失。

发明内容

有鉴于此，本申请提供一种通讯方法及装置，可以提升通讯安全性，保障通讯方的利益。

为实现上述目的，本申请提供技术方案如下：

根据本申请的第一方面，提出了一种通讯方法，包括：

本端设备向对端设备发起用户身份验证请求；

所述本端设备根据接收到的响应信息，确定对端通讯方是否通过身份验证；其中，所述响应信息由所述对端设备直接发送至所述本端设备，或者由服务器根据来自所述对端设备的返回信息而生成；

当所述对端通讯方通过身份验证时，所述本端设备完成本端通讯方与所述对端通讯方之间的通讯过程。

根据本申请的第二方面，提出了一种通讯方法，包括：

服务器将第一端设备发起的用户身份验证请求发送至第二端设备；

所述服务器根据所述第二端设备的返回信息，生成对所述用户身份验证请求的响应信息；

所述服务器将所述响应信息发送至所述第一端设备，以由所述第一端设备在确定第

二端通讯方通过身份验证时，完成第一端通讯方与所述第二端通讯方之间的通讯过程。

根据本申请的第三方面，提出了一种通讯装置，包括：

请求单元，使本端设备向对端设备发起用户身份验证请求；

验证单元，使所述本端设备根据接收到的响应信息，确定对端通讯方是否通过身份验证；其中，所述响应信息由所述对端设备直接发送至所述本端设备，或者由服务器根据来自所述对端设备的返回信息而生成；

通讯单元，当所述对端通讯方通过身份验证时，使所述本端设备完成本端通讯方与所述对端通讯方之间的通讯过程。

根据本申请的第四方面，提出了一种通讯装置，包括：

第一发送单元，使服务器将第一端设备发起的用户身份验证请求发送至第二端设备；

生成单元，使所述服务器根据所述第二端设备的返回信息，生成对所述用户身份验证请求的响应信息；

第二发送单元，使所述服务器将所述响应信息发送至所述第一端设备，以由所述第一端设备在确定第二端通讯方通过身份验证时，完成第一端通讯方与所述第二端通讯方之间的通讯过程。

由以上技术方案可见，本申请通过验证对端通讯方的用户身份，可以确保对端通讯方为授权用户，避免在电子设备丢失、账号密码泄露等情况下，由非法用户冒充该授权用户，有助于提升通讯安全性，保障通讯方的利益。

附图说明

图 1 是本申请一示例性实施例的一种基于验证发起方的通讯方法的流程图；

图 2 是本申请一示例性实施例的一种基于验证响应方的通讯方法的流程图；

图 3 是本申请一示例性实施例的一种基于服务器的通讯方法的流程图；

图 4 是本申请一示例性实施例的一种添加身份验证的通讯方法的流程图；

图 5A-5E 是本申请一示例性实施例的一种通讯界面的示意图；

图 6 是本申请一示例性实施例的另一种添加身份验证的通讯方法的流程图；

图 7 是本申请一示例性实施例的一种基于验证发起方的电子设备的结构示意图；

图 8 是本申请一示例性实施例的一种基于验证发起方的通讯装置的框图；

图 9 是本申请一示例性实施例的一种基于验证响应方的电子设备的结构示意图；

图 10 是本申请一示例性实施例的一种基于验证响应方的通讯装置的框图；

图 11 是本申请一示例性实施例的一种基于服务器的电子设备的结构示意图；

图 12 是本申请一示例性实施例的一种基于服务器的通讯装置的框图。

具体实施方式

为对本申请进行进一步说明，提供下列实施例：

图 1 是本申请一示例性实施例的一种基于验证发起方的通讯方法的流程图，如图 1 所示，该方法应用于验证发起方的电子设备中，可以包括以下步骤：

步骤 102，本端设备向对端设备发起用户身份验证请求。

步骤 104，所述本端设备根据接收到的响应信息，确定对端通讯方是否通过身份验证；其中，所述响应信息由所述对端设备直接发送至所述本端设备，或者由服务器根据来自所述对端设备的返回信息而生成。

步骤 106，当所述对端通讯方通过身份验证时，所述本端设备完成本端通讯方与所述对端通讯方之间的通讯过程。

在上述实施例中，本端设备与对端设备之间的身份验证过程，可以由本端设备与对端设备之间直接完成，比如采用本端设备与对端设备之间的端对端通讯，则本端设备可以直接接收到对端设备发送的响应信息，而无需服务器介入；或者，也可以由服务器协助本端设备与对端设备之间的身份验证过程，则本端设备可以接收到由服务器根据对端设备的返回信息生成的响应信息。

相应地，图 2 是本申请一示例性实施例的一种基于验证响应方的通讯方法的流程图，如图 2 所示，该方法应用于验证响应方的电子设备，可以包括以下步骤：

步骤 202，本端设备接收到对端设备发起的用户身份验证请求。

步骤 204，所述本端设备根据获取的本端通讯方的身份特征信息，生成对所述用户身份验证请求的响应信息。

步骤 206，所述本端设备将所述响应信息返回所述对端设备，以由所述对端设备在确定所述本端通讯方通过身份验证时，完成对端通讯方与所述本端通讯方之间的通讯过程。

当然，容易理解的是：图 1 所示的实施例以“验证发起方”的角度进行描述，因而“本端设备”即“验证发起方”使用的电子设备、“对端设备”即“验证响应方”使用的电子设备；而图 2 所示的实施例以“验证响应方”的角度进行描述，因而“本端设备”即“验证响应方”使用的电子设备、“对端设备”即“验证发起方”使用的电子设备。

相应地，当涉及到服务器的配合作用时，图 3 是本申请一示例性实施例的一种基于服务器的通讯方法的流程图，如图 3 所示，该方法应用于服务器中，可以包括以下步骤：

步骤 302，服务器将第一端设备发起的用户身份验证请求发送至第二端设备。

步骤 304，所述服务器根据所述第二端设备的返回信息，生成对所述用户身份验证请求的响应信息。

步骤 306，所述服务器将所述响应信息发送至所述第一端设备，以由所述第一端设备在确定第二端通讯方通过身份验证时，完成第一端通讯方与所述第二端通讯方之间的通讯过程。

由以上技术方案可见，本申请通过验证对端通讯方的用户身份，可以确保对端通讯方为授权用户，避免在电子设备丢失、账号密码泄露等情况下，由非法用户冒充该授权用户，有助于提升通讯安全性，保障通讯方的利益。

为了便于理解，下面结合通讯过程涉及的各方及其交互过程，对本申请的技术方案进行详细描述。

1、直接通讯

图 4 是本申请一示例性实施例的一种添加身份验证的通讯方法的流程图，如图 4 所示，假定用户 A 使用（比如登录相应的注册账号）设备 1、用户 B 使用（比如登录相应的注册账号）设备 2，则用户 A 与用户 B 通过设备 1、设备 2 实现直接通讯，并在通讯过程中实现身份验证；比如，当用户 A 为验证发起方、用户 B 为验证响应方时，该方法可以包括以下步骤：

步骤 402，设备 1 监测到通讯消息。

步骤 404，设备 1 确定通讯消息中是否包含敏感内容，若包含则转入步骤 406。

步骤 406，设备 1 向设备 2 发送用户身份验证请求。

在本实施例中，通讯消息可以为通讯过程中的任意消息，比如该通讯消息可以来自验证响应方，即图 4 中的用户 B（设备 2）。假定用户 A 为用户“小白”、用户 B 为用户“马总”，则图 5A 示出了用户“小白”使用的设备 1 的通讯界面；当设备 1 接收到来自用户“马总”的通讯消息“小白，把昨天张总的报价单发我一下……”时，如果“报价单”为预定义的敏感内容，则设备 1 通过对该通讯消息的自动识别和匹配后，可以自动转入步骤 406。其中，敏感内容可能由于用户的使用习惯、关心的方向和应用场景等的变化，而存在相应差异；而用户可以根据自身的实际需求，对敏感内容进行编辑，本申请并不对此进行限制。

如图 5A 所示，在设备 1 示出界面的右上角示出一开启的“锁”图标，表明此时尚未启动身份验证。如图 5B 所示，当设备 1 向设备 2 发起身份验证（即发送用户身份验证请求）时，在设备 1 示出界面的右上角的“锁”图标由开启状态切换至关闭状态，并且可以通过诸如图 5B 所示的“您已开启安全认证机制”的文字内容进行提示；当然，还可以采用其他的任意提示方式，本申请并不对此进行限制。

当然，通讯消息还可以来自验证发起方，比如图 4 所示实施例中的用户 A（设备 1）。举例而言，当用户“小白”在图 5A 所示的界面中进入信息输入时，比如通过界面下方的输入框进行手动输入，或者语音输入等，则设备 1 均可以对相应的输入内容进行识别和匹配，以确定其是否包含敏感内容。

需要说明的是：除了设备 1 基于内容监测而自动触发身份验证之外，用户还可以根据实际需求，手动触发身份验证。比如用户在任何认为需要执行身份验证的情况下，均可以通过诸如点击图 5A 所示界面右上角的“锁”图标，使其切换至图 5B 所示关闭状态的“锁”图标，从而手动启动身份验证。

步骤 408，设备 2 获取用户 B 的身份特征信息。

步骤 410，设备 2 生成响应信息。

步骤 412，设备 1 接收到设备 2 发送的响应信息。

步骤 414，设备 1 根据接收到的响应信息，执行身份验证操作。

在本实施例中，设备 2 获取作为验证响应方的用户 B 的身份特征信息，该身份特征信息可以包括以下至少之一：

1）对端通讯方的生理特征信息。比如，包含对端通讯方的预设生理特征的图像、视频等，比如该预设生理特征可以包括该对端通讯方的人脸特征，则包含对端通讯方的预设生理特征的图像可以为该对端通讯方的人脸图像、包含对端通讯方的预设生理特征的视频可以为该对端通讯方的人脸视频（包含人脸信息的视频）等；或者，生理特征信息还可以包括对端通讯方的指纹信息、声音片段、虹膜信息等。

2）对端通讯方的操作习惯信息。比如，对端通讯方的输入速度、按压力度、习惯性的错误输入（比如习惯于将“的”输入为“地”）等。

当然，所有能够用于身份识别的特征信息均可以应用于本申请的技术方案中，以上仅用于举例说明，本申请并不对此进行限制。

作为一示例性实施例，设备 2 在生成响应信息时，可以直接将身份特征信息添加至响应信息中，则设备 1 可以提取响应信息中包含的身份特征信息，并呈现于作为本端通

讯方的用户 A；比如图 5C 所示，当身份特征信息为人脸图像时，可以直接对该人脸图像进行展示，并由作为本端通讯方的用户 A 进行识别后，将识别结果告知设备 1，则设备 1 在识别结果为“通过验证”时认为对端通讯方通过身份验证，即当前用户确实为用户 B，以及设备 1 在识别结果为“不是机主”时认为对端通讯方未通过身份验证，即当前用户为其他用户伪装的用户 B。

当然，对于人脸图像、人脸视频等可视化的生理特征信息，以及习惯性的错误输入等可视化的操作习惯信息，设备 1 可以直接展示给本端通讯方；类似地，对于声音片段等可通过听觉识别的生理特征信息，设备 1 也可以直接播放给本端通讯方。而对于指纹信息、虹膜信息等生理特征信息，以及输入速度、按压力度等操作习惯信息，虽然无法通过视觉、听觉等进行呈现，但是设备 1 则可以将采集到的身份特征信息与预定义的标准特征信息（比如事先获取并存储有对端通讯方的身份特征信息）进行对比，并将对比数据呈现给本端通讯方，以供其查看和判断。

作为另一示例性实施例，设备 2 在生成响应信息时，可以根据采集到的身份特征信息验证作为对端通讯方的用户 B 的身份信息，并将验证结果添加至响应信息。那么，设备 1 可以提取响应信息中包含的身份验证结果，并据此确定对端通讯方是否通过身份验证，而无需该设备 1 执行具体的身份验证。

其中，设备 2 可以基于采集到的身份特征信息，并将该身份特征信息与预定义的标准特征信息进行比较后，自动完成身份验证，避免使用该设备 2 的非法用户冒充实际上的用户 B。

步骤 416，设备 1 与设备 2 之间实现通讯。

在本实施例中，当本端通讯方与对端通讯方之间执行了身份验证操作时，表明通讯内容可能涉及到敏感内容，因而可以本端通讯方与对端通讯方之间实现加密通讯过程，从而确保即便通讯内容被窃取后，也不会造成敏感内容的泄露。

需要说明的是：

（1）设备 1 在监测到通讯消息中包含敏感内容时，可以告知作为本端通讯方的用户 A，并由用户 A 确定是否需要执行身份验证。比如图 5D 所示，设备 1 可以向用户 A 展示诸如“涉及敏感内容，请验证对方身份”的提示信息，以及相应的选项；那么，当用户 A 选择“验证”时，设备 1 可以执行向对端通讯方的身份验证操作，而当用户 A 选择“不验证”时，即便通讯消息中包含敏感内容，也不会向对端通讯方执行身份验证操作。

（2）在上述实施例中，当设备 1 获得的身份特征信息为与对端通讯方相关的可视化

信息时，设备 1 可以将该身份特征信息展示于来自对端通讯方的通讯消息的关联区域。比如图 5E 所示，当身份特征信息为图 5C 所示的人脸图像时，可以将该人脸图像作为对端通讯方的实时头像，展示于该对端通讯方发送的通讯消息的关联区域，比如该关联区域可以为图 5E 中的用户“马总”发送的每条通讯消息的左侧。

（3）身份验证结果可以具有一定的时效性，则在每次确定对端通讯方通过身份验证后，可以启动相应的失效定时器，则该失效定时器对应的预设时长内均可以认为该对端通讯方的身份通过验证，那么即便该预设时长内存在触发身份验证操作的因素，比如设备 1 监测到包含敏感内容的通讯消息，仍然可以不触发该身份验证操作。而在该预设时长之后，即失效定时器超时后，设备 1 认为对端通讯方并未通过身份验证，因而在监测到敏感内容等可触发身份验证操作的因素时，设备 1 可以触发身份验证操作。

（4）身份验证操作可以在任意通讯界面发起，比如图 5A 所示的正常通讯界面；或者，可以限制该身份验证操作仅在诸如“澡堂”或“阅后即焚”等对端通讯方可能匿名的模式下，才允许执行身份验证；用户可以根据实际情况进行配置，本申请并不对此进行限制。

2、基于服务器

图 6 是本申请一示例性实施例的另一种添加身份验证的通讯方法的流程图，如图 6 所示，假定用户 A 使用设备 1、用户 B 使用设备 2，则用户 A 与用户 B 通过设备 1、设备 2 进行通讯时，需要由服务器进行消息转发等功能介入，并在通讯过程中协助完成身份验证；比如，当用户 A 为验证发起方、用户 B 为验证响应方时，该方法可以包括以下步骤：

步骤 602，设备 1 监测到通讯消息。

步骤 604，设备 1 确定通讯消息中是否包含敏感内容，若包含则转入步骤 606。

在本实施例中，步骤 602-604 可以参考图 4 所示的步骤 402-404，此处不再赘述。

步骤 606，设备 1 通过服务器向设备 2 发送用户身份验证请求。

在本实施例中，设备 1 可以将设备 2 标记为用户身份验证请求的目标方，并由服务器将设备 1 发出的用户身份验证请求转发至设备 2。当然，服务器可以对设备 1 发送的用户身份验证请求进行重新打包等处理，但并不会改变所需传递的内容。

步骤 608，设备 2 获取用户 B 的身份特征信息。

步骤 610，设备 2 生成响应信息。

步骤 612，设备 1 通过服务器接收到设备 2 发送的响应信息。

步骤 614，设备 1 根据接收到的响应信息，执行身份验证操作。

作为一示例性实施例，服务器在步骤 612 中，可以直接将设备 2 发送的信息转发至设备 1；其中，为了便于区分，假定设备 2 向服务器发送的信息为“返回信息”，而服务器向设备 1 发送的信息为“响应信息”，那么服务器在接收到返回信息后，可以提取返回信息中的内容，并直接将该内容添加至响应信息中，从而发送至设备 1。

那么，该响应信息中可能包含设备 2 采集到的身份特征信息，也可能包含设备 2 根据该身份特征信息生成的身份验证结果，则设备 1 可以采用类似于图 4 所示实施例的方式，执行身份验证操作，此处不再赘述。

作为另一示例性实施例，假定设备 2 向服务器发送的返回信息中包含其采集到的身份特征信息，则服务器可以提取该身份特征信息并执行身份验证，然后将得到的身份验证结果添加至响应信息中，并发送至设备 1；相应地，设备 1 可以根据该响应信息中的身份验证结果执行身份验证操作，此处不再赘述。其中，服务器基于设备 2 采集到的身份特征信息执行身份验证时，可以将该身份特征信息与预定义的标准特征信息进行比较后，自动完成身份验证；或者，服务器也可以采用其他方式实现身份验证，本申请并不对此进行限制。

步骤 616，设备 1 与设备 2 之间实现通讯；其中，通讯过程可以参考上述的步骤 416，此处不再赘述。

图 7 示出了根据本申请的一示例性实施例的基于验证发起方的电子设备的示意结构图。请参考图 7，在硬件层面，该电子设备包括处理器、内部总线、网络接口、内存以及非易失性存储器，当然还可能包括其他业务所需要的硬件。处理器从非易失性存储器中读取对应的计算机程序到内存中然后运行，在逻辑层面上形成通讯装置。当然，除了软件实现方式之外，本申请并不排除其他实现方式，比如逻辑器件抑或软硬件结合的方式等等，也就是说以下处理流程的执行主体并不限定于各个逻辑单元，也可以是硬件或逻辑器件。

请参考图 8，在软件实施方式中，该通讯装置可以包括请求单元、验证单元和通讯单元。其中：

请求单元，使本端设备向对端设备发起用户身份验证请求；

验证单元，使所述本端设备根据接收到的响应信息，确定对端通讯方是否通过身份验证；其中，所述响应信息由所述对端设备直接发送至所述本端设备，或者由服务器根据来自所述对端设备的返回信息而生成；

通讯单元，当所述对端通讯方通过身份验证时，使所述本端设备完成本端通讯方与所述对端通讯方之间的通讯过程。

可选的，所述请求单元具体用于：

使所述本端设备监测到通讯消息中包含预设敏感内容时，向对端设备发起用户身份验证请求。

可选的，所述验证单元具体用于：

使所述本端设备提取所述响应信息中包含的身份特征信息，并呈现于所述本端通讯方；

使所述本端设备根据接收到的所述本端通讯方对所述身份特征信息的识别结果，确定所述对端通讯方是否通过身份验证。

可选的，所述身份特征信息包括以下至少之一：

所述对端通讯方的生理特征信息、所述对端通讯方的操作习惯信息。

可选的，所述身份特征信息包括以下至少之一：

包含所述对端通讯方的预设生理特征的图像、包含所述对端通讯方的预设生理特征的视频。

可选的，还包括：

展示单元，当所述身份特征信息为与所述对端通讯方相关的可视化信息时，使所述本端设备将所述身份特征信息展示于来自所述对端通讯方的通讯消息的关联区域。

可选的，所述验证单元具体用于：

使所述本端设备提取所述响应信息中包含的身份验证结果，并据此确定所述对端通讯方是否通过身份验证；其中，所述身份验证结果由所述对端设备根据获得的所述对端通讯方的身份特征信息进行验证得到，或者所述身份验证结果由所述服务器根据所述返回信息中包含的身份特征信息进行验证得到。

可选的，所述通讯单元具体用于：

使所述本端设备在所述本端通讯方与所述对端通讯方之间实现加密通讯过程。

可选的，还包括：

启动单元，当所述对端通讯方通过身份验证时，启动相应的失效定时器；

失效单元，在所述失效定时器超时后，失效所述对端通讯方的身份验证结果。

图 9 示出了根据本申请的一示例性实施例的基于验证响应方的电子设备的示意结构图。请参考图 9，在硬件层面，该电子设备包括处理器、内部总线、网络接口、内存以

及非易失性存储器，当然还可能包括其他业务所需要的硬件。处理器从非易失性存储器中读取对应的计算机程序到内存中然后运行，在逻辑层面上形成通讯装置。当然，除了软件实现方式之外，本申请并不排除其他实现方式，比如逻辑器件抑或软硬件结合的方式等等，也就是说以下处理流程的执行主体并不限定于各个逻辑单元，也可以是硬件或逻辑器件。

请参考图 10，在软件实施方式中，该通讯装置可以包括接收单元、生成单元和返回单元。其中：

接收单元，使本端设备接收到对端设备发起的用户身份验证请求；

生成单元，使所述本端设备根据获取的本端通讯方的身份特征信息，生成对所述用户身份验证请求的响应信息；

返回单元，使所述本端设备将所述响应信息返回所述对端设备，以由所述对端设备在确定所述本端通讯方通过身份验证时，完成对端通讯方与所述本端通讯方之间的通讯过程。

可选的，所述生成单元具体用于：

使所述本端设备将所述身份特征信息添加至所述响应信息；

或者，使所述本端设备根据所述身份特征信息验证所述本端通讯方的身份信息，并将验证结果添加至所述响应信息。

可选的，所述身份特征信息包括以下至少之一：

所述对端通讯方的生理特征信息、所述对端通讯方的操作习惯信息。

可选的，所述身份特征信息包括以下至少之一：

包含所述对端通讯方的预设生理特征的图像、包含所述对端通讯方的预设生理特征的视频。

图 11 示出了根据本申请的一示例性实施例的基于服务器的电子设备的示意结构图。请参考图 11，在硬件层面，该电子设备包括处理器、内部总线、网络接口、内存以及非易失性存储器，当然还可能包括其他业务所需要的硬件。处理器从非易失性存储器中读取对应的计算机程序到内存中然后运行，在逻辑层面上形成通讯装置。当然，除了软件实现方式之外，本申请并不排除其他实现方式，比如逻辑器件抑或软硬件结合的方式等等，也就是说以下处理流程的执行主体并不限定于各个逻辑单元，也可以是硬件或逻辑器件。

请参考图 12，在软件实施方式中，该通讯装置可以包括第一发送单元、生成单元和

第二发送单元。其中：

第一发送单元，使服务器将第一端设备发起的用户身份验证请求发送至第二端设备；

生成单元，使所述服务器根据所述第二端设备的返回信息，生成对所述用户身份验证请求的响应信息；

第二发送单元，使所述服务器将所述响应信息发送至所述第一端设备，以由所述第一端设备在确定第二端通讯方通过身份验证时，完成第一端通讯方与所述第二端通讯方之间的通讯过程。

可选的，所述生成单元具体用于：

使所述服务器将所述返回信息中的内容添加至所述响应信息；

或者，使所述服务器提取所述返回信息中包含的所述第二端通讯方的身份特征信息，对所述身份特征信息进行验证，并将验证结果添加至所述响应信息。

可选的，所述身份特征信息包括以下至少之一：

所述第二端通讯方的生理特征信息、所述第二端通讯方的操作习惯信息。

可选的，所述身份特征信息包括以下至少之一：

包含所述第二端通讯方的预设生理特征的图像、包含所述第二端通讯方的预设生理特征的视频。

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

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

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

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

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

权 利 要 求 书

1．一种通讯方法，其特征在于，包括：

本端设备向对端设备发起用户身份验证请求；

所述本端设备根据接收到的响应信息，确定对端通讯方是否通过身份验证；其中，所述响应信息由所述对端设备直接发送至所述本端设备，或者由服务器根据来自所述对端设备的返回信息而生成；

当所述对端通讯方通过身份验证时，所述本端设备完成本端通讯方与所述对端通讯方之间的通讯过程。

2．根据权利要求 1 所述的方法，其特征在于，所述本端设备向对端设备发起用户身份验证请求，包括：

所述本端设备监测到通讯消息中包含预设敏感内容时，向对端设备发起用户身份验证请求。

3．根据权利要求 1 所述的方法，其特征在于，所述本端设备根据接收到的响应信息，确定对端通讯方是否通过身份验证，包括：

所述本端设备提取所述响应信息中包含的身份特征信息，并呈现于所述本端通讯方；

所述本端设备根据接收到的所述本端通讯方对所述身份特征信息的识别结果，确定所述对端通讯方是否通过身份验证。

4．根据权利要求 3 所述的方法，其特征在于，所述身份特征信息包括以下至少之一：

所述对端通讯方的生理特征信息、所述对端通讯方的操作习惯信息。

5．根据权利要求 3 所述的方法，其特征在于，所述身份特征信息包括以下至少之一：

包含所述对端通讯方的预设生理特征的图像、包含所述对端通讯方的预设生理特征的视频。

6．根据权利要求 3 所述的方法，其特征在于，还包括：

当所述身份特征信息为与所述对端通讯方相关的可视化信息时，所述本端设备将所述身份特征信息展示于来自所述对端通讯方的通讯消息的关联区域。

7．根据权利要求 1 所述的方法，其特征在于，所述本端设备根据接收到的响应信息，确定对端通讯方是否通过身份验证，包括：

所述本端设备提取所述响应信息中包含的身份验证结果，并据此确定所述对端通讯方是否通过身份验证；其中，所述身份验证结果由所述对端设备根据获得的所述对端通讯方的身份特征信息进行验证得到，或者所述身份验证结果由所述服务器根据所述返回信息中包含的身份特征信息进行验证得到。

8．根据权利要求 1 所述的方法，其特征在于，所述本端设备完成本端通讯方与所述对端通讯方之间的通讯过程，包括：

所述本端设备在所述本端通讯方与所述对端通讯方之间实现加密通讯过程。

9．根据权利要求 1 所述的方法，其特征在于，还包括：

当所述对端通讯方通过身份验证时，启动相应的失效定时器；

在所述失效定时器超时后，失效所述对端通讯方的身份验证结果。

10．一种通讯方法，其特征在于，包括：

服务器将第一端设备发起的用户身份验证请求发送至第二端设备；

所述服务器根据所述第二端设备的返回信息，生成对所述用户身份验证请求的响应信息；

所述服务器将所述响应信息发送至所述第一端设备，以由所述第一端设备在确定第二端通讯方通过身份验证时，完成第一端通讯方与所述第二端通讯方之间的通讯过程。

11．根据权利要求 10 所述的方法，其特征在于，所述服务器根据所述第二端设备的返回信息，生成对所述用户身份验证请求的响应信息，包括：

所述服务器将所述返回信息中的内容添加至所述响应信息；

或者，所述服务器提取所述返回信息中包含的所述第二端通讯方的身份特征信息，对所述身份特征信息进行验证，并将验证结果添加至所述响应信息。

12．根据权利要求 11 所述的方法，其特征在于，所述身份特征信息包括以下至少之一：

所述第二端通讯方的生理特征信息、所述第二端通讯方的操作习惯信息。

13．根据权利要求 11 所述的方法，其特征在于，所述身份特征信息包括以下至少之一：

包含所述第二端通讯方的预设生理特征的图像、包含所述第二端通讯方的预设生理特征的视频。

14．一种通讯装置，其特征在于，包括：

请求单元，使本端设备向对端设备发起用户身份验证请求；

验证单元，使所述本端设备根据接收到的响应信息，确定对端通讯方是否通过身份验证；其中，所述响应信息由所述对端设备直接发送至所述本端设备，或者由服务器根据来自所述对端设备的返回信息而生成；

通讯单元，当所述对端通讯方通过身份验证时，使所述本端设备完成本端通讯方与所述对端通讯方之间的通讯过程。

15．根据权利要求 14 所述的装置，其特征在于，所述请求单元具体用于：

使所述本端设备监测到通讯消息中包含预设敏感内容时，向对端设备发起用户身份验证请求。

16．根据权利要求 14 所述的装置，其特征在于，所述验证单元具体用于：

使所述本端设备提取所述响应信息中包含的身份特征信息，并呈现于所述本端通讯方；

使所述本端设备根据接收到的所述本端通讯方对所述身份特征信息的识别结果，确定所述对端通讯方是否通过身份验证。

17．根据权利要求 16 所述的装置，其特征在于，所述身份特征信息包括以下至少之一：

所述对端通讯方的生理特征信息、所述对端通讯方的操作习惯信息。

18．根据权利要求 16 所述的装置，其特征在于，所述身份特征信息包括以下至少之一：

包含所述对端通讯方的预设生理特征的图像、包含所述对端通讯方的预设生理特征的视频。

19．根据权利要求 16 所述的装置，其特征在于，还包括：

展示单元，当所述身份特征信息为与所述对端通讯方相关的可视化信息时，使所述本端设备将所述身份特征信息展示于来自所述对端通讯方的通讯消息的关联区域。

20．根据权利要求 14 所述的装置，其特征在于，所述验证单元具体用于：

使所述本端设备提取所述响应信息中包含的身份验证结果，并据此确定所述对端通讯方是否通过身份验证；其中，所述身份验证结果由所述对端设备根据获得的所述对端通讯方的身份特征信息进行验证得到，或者所述身份验证结果由所述服务器根据所述返回信息中包含的身份特征信息进行验证得到。

21．根据权利要求 14 所述的装置，其特征在于，所述通讯单元具体用于：

使所述本端设备在所述本端通讯方与所述对端通讯方之间实现加密通讯过程。

22．根据权利要求 14 所述的装置，其特征在于，还包括：

启动单元，当所述对端通讯方通过身份验证时，启动相应的失效定时器；

失效单元，在所述失效定时器超时后，失效所述对端通讯方的身份验证结果。

23．一种通讯装置，其特征在于，包括：

第一发送单元，使服务器将第一端设备发起的用户身份验证请求发送至第二端设备；

生成单元，使所述服务器根据所述第二端设备的返回信息，生成对所述用户身份验证请求的响应信息；

第二发送单元，使所述服务器将所述响应信息发送至所述第一端设备，以由所述第一端设备在确定第二端通讯方通过身份验证时，完成第一端通讯方与所述第二端通讯方之间的通讯过程。

24．根据权利要求 23 所述的装置，其特征在于，所述生成单元具体用于：

使所述服务器将所述返回信息中的内容添加至所述响应信息；

或者，使所述服务器提取所述返回信息中包含的所述第二端通讯方的身份特征信息，对所述身份特征信息进行验证，并将验证结果添加至所述响应信息。

25．根据权利要求 24 所述的装置，其特征在于，所述身份特征信息包括以下至少之一：

所述第二端通讯方的生理特征信息、所述第二端通讯方的操作习惯信息。

26．根据权利要求 24 所述的装置，其特征在于，所述身份特征信息包括以下至少之一：

包含所述第二端通讯方的预设生理特征的图像、包含所述第二端通讯方的预设生理特征的视频。

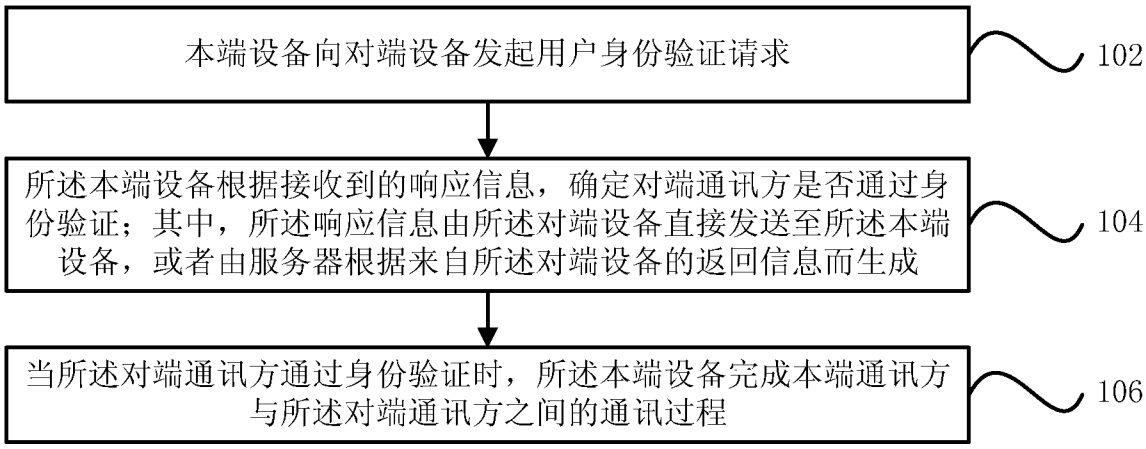
本端设备向对端设备发起用户身份验证请求
102
所述本端设备根据接收到的响应信息，确定对端通讯方是否通过身份验证；其中，所述响应信息由所述对端设备直接发送至所述本端设备，或者由服务器根据来自所述对端设备的返回信息而生成
104
当所述对端通讯方通过身份验证时，所述本端设备完成本端通讯方与所述对端通讯方之间的通讯过程
106

图 1

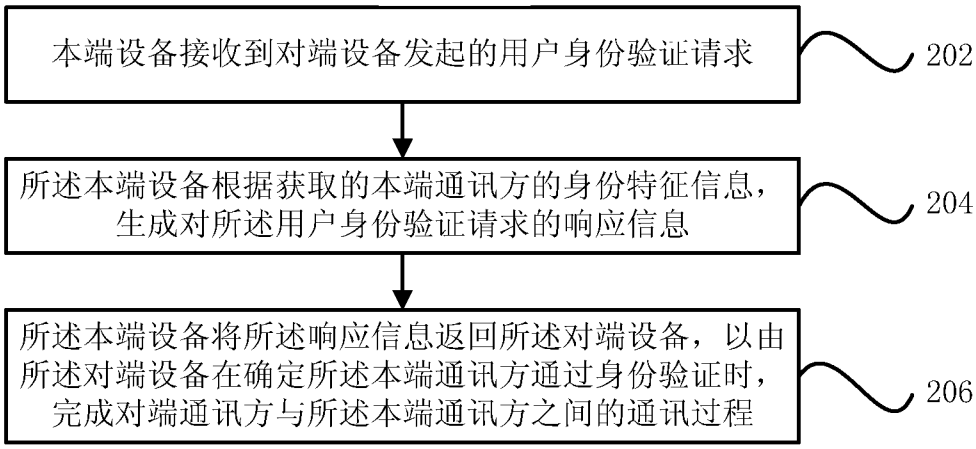
本端设备接收到对端设备发起的用户身份验证请求
202
所述本端设备根据获取的本端通讯方的身份特征信息，生成对所述用户身份验证请求的响应信息
204
所述本端设备将所述响应信息返回所述对端设备，以由所述对端设备在确定所述本端通讯方通过身份验证时，完成对端通讯方与所述本端通讯方之间的通讯过程
206

图 2

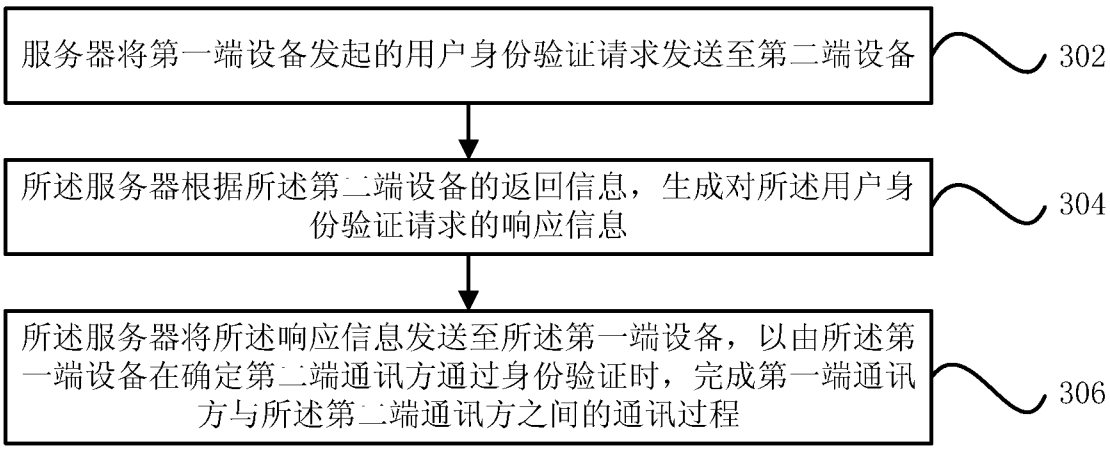
服务器将第一端设备发起的用户身份验证请求发送至第二端设备
302
所述服务器根据所述第二端设备的返回信息，生成对所述用户身份验证请求的响应信息
304
所述服务器将所述响应信息发送至所述第一端设备，以由所述第一端设备在确定第二端通讯方通过身份验证时，完成第一端通讯方与所述第二端通讯方之间的通讯过程
306

图 3

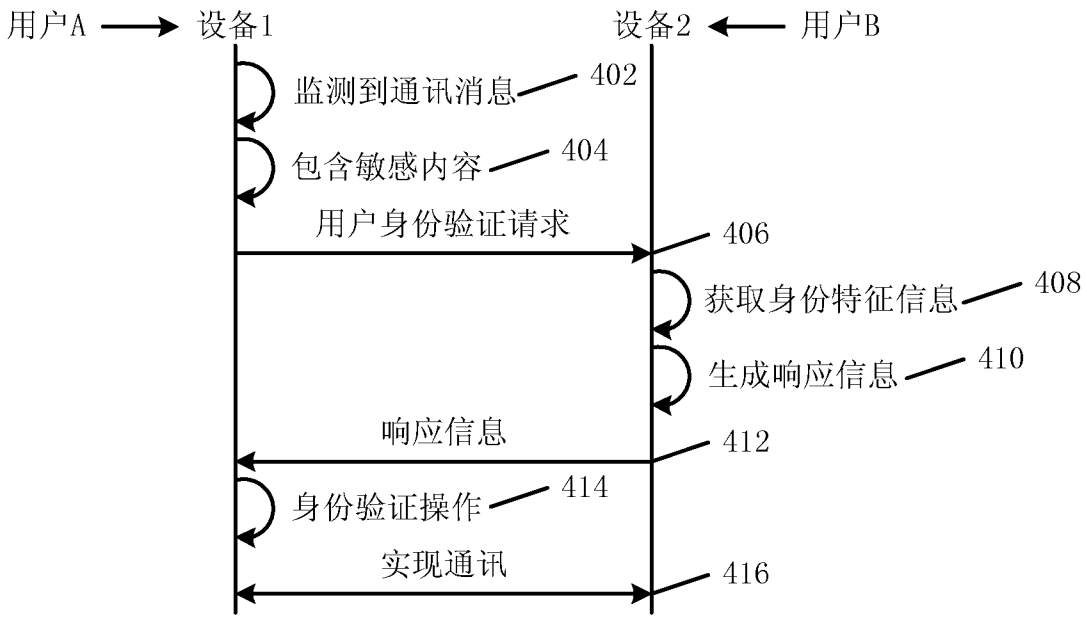
用户A
设备1
设备2
用户B
监测到通讯消息
402
包含敏感内容
404
用户身份验证请求
406
获取身份特征信息
408
生成响应信息
410
响应信息
412
身份验证操作
414
实现通讯
416

图 4

图 5A

图 5B

图 5C


10:45
马总
20:20
好的~
以上为历史消息
小白，把昨天张总的报价单发我一下。
10:45
涉及敏感内容，请验证对方身份
验证
不验证

图 5D


10:45
马总
以上为历史消息
小白，把昨天张总的报价单发我一下。
10:45
您已开启安全认证机制
已通过安全认证
20:20
马总，请稍等！

图 5E

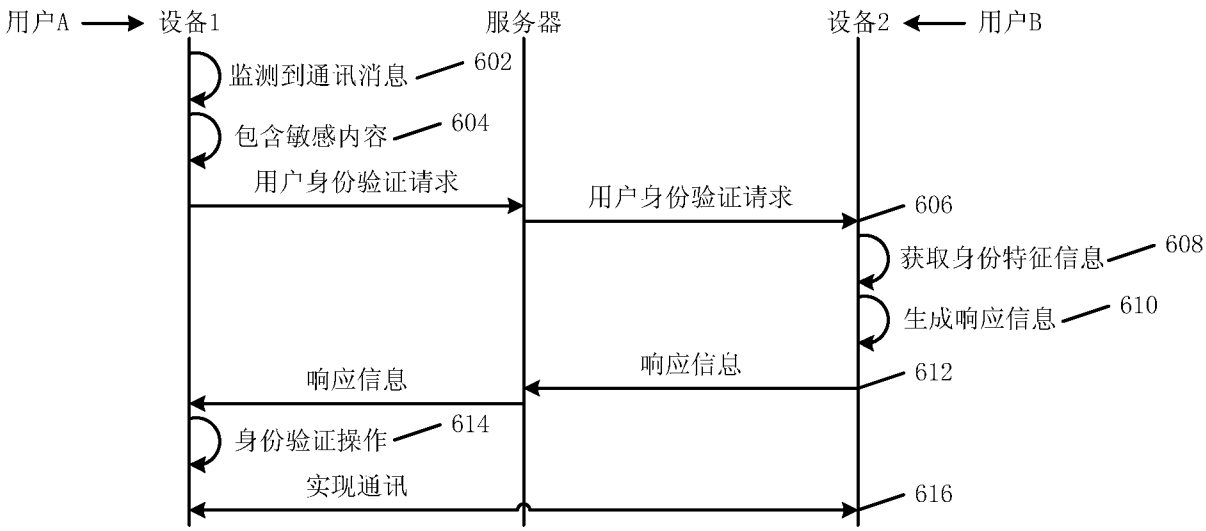
用户A
设备1
服务器
设备2
用户B
监测到通讯消息
602
包含敏感内容
604
用户身份验证请求
用户身份验证请求
606
获取身份特征信息
608
生成响应信息
610
响应信息
响应信息
612
身份验证操作
614
实现通讯
616

图 6

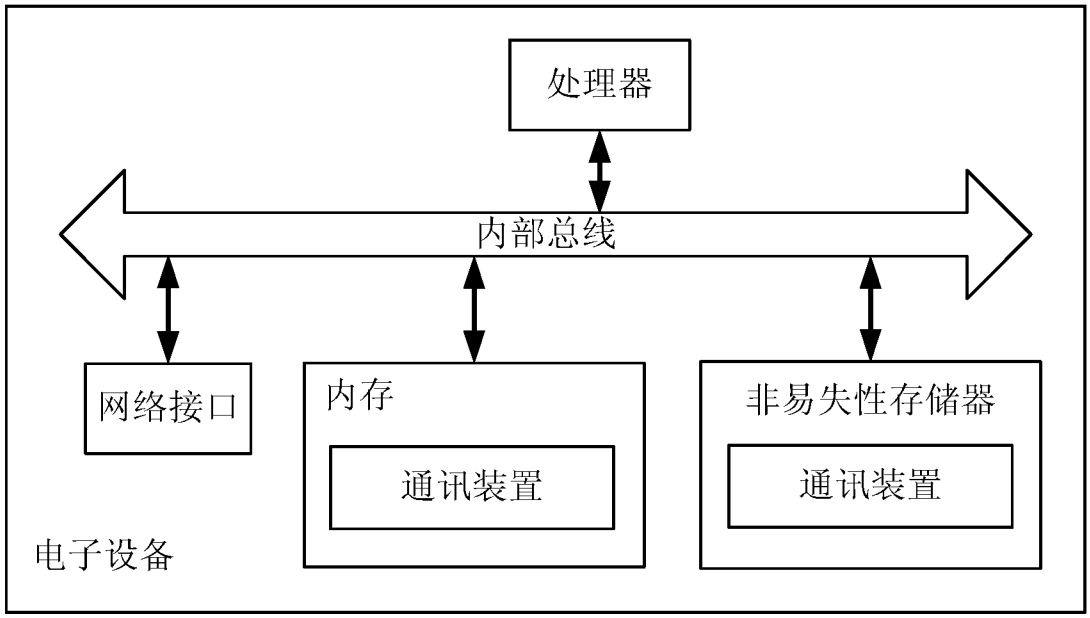
处理器
内部总线
网络接口
内存
通讯装置
非易失性存储器
通讯装置
电子设备

图 7

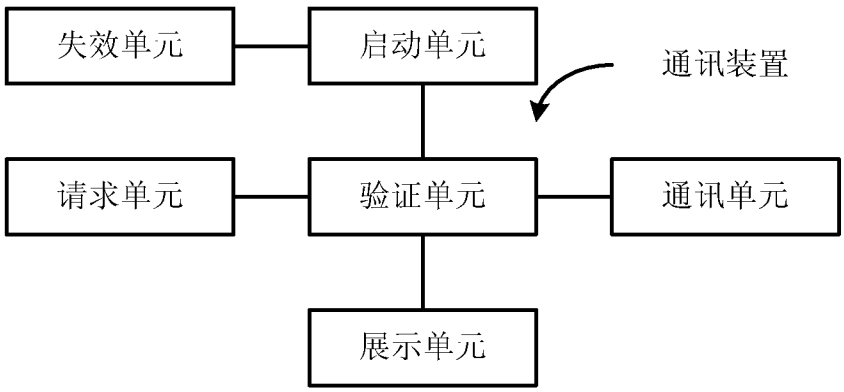
失效单元
启动单元
通讯装置
请求单元
验证单元
通讯单元
展示单元

图 8

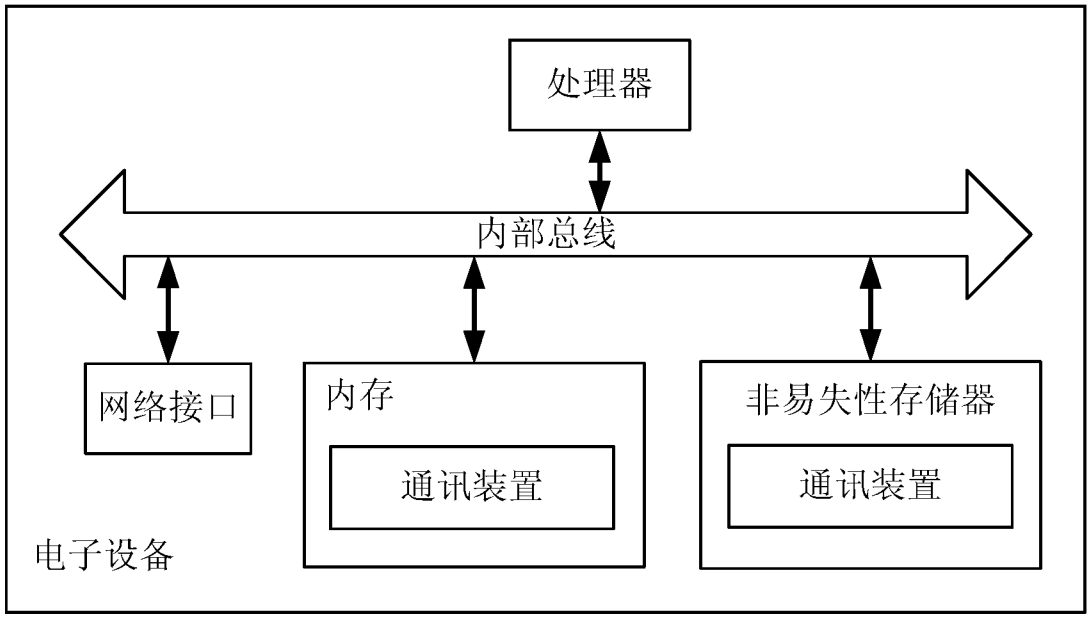
处理器
内部总线
网络接口
内存
通讯装置
非易失性存储器
通讯装置
电子设备

图 9

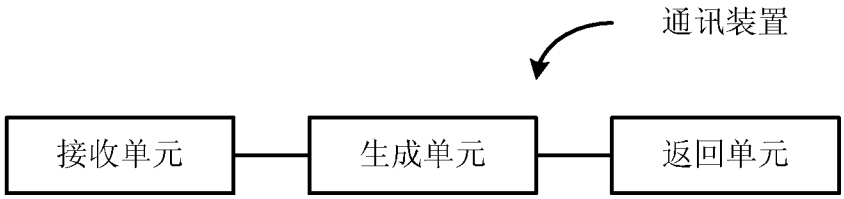
通讯装置
接收单元
生成单元
返回单元

图 10

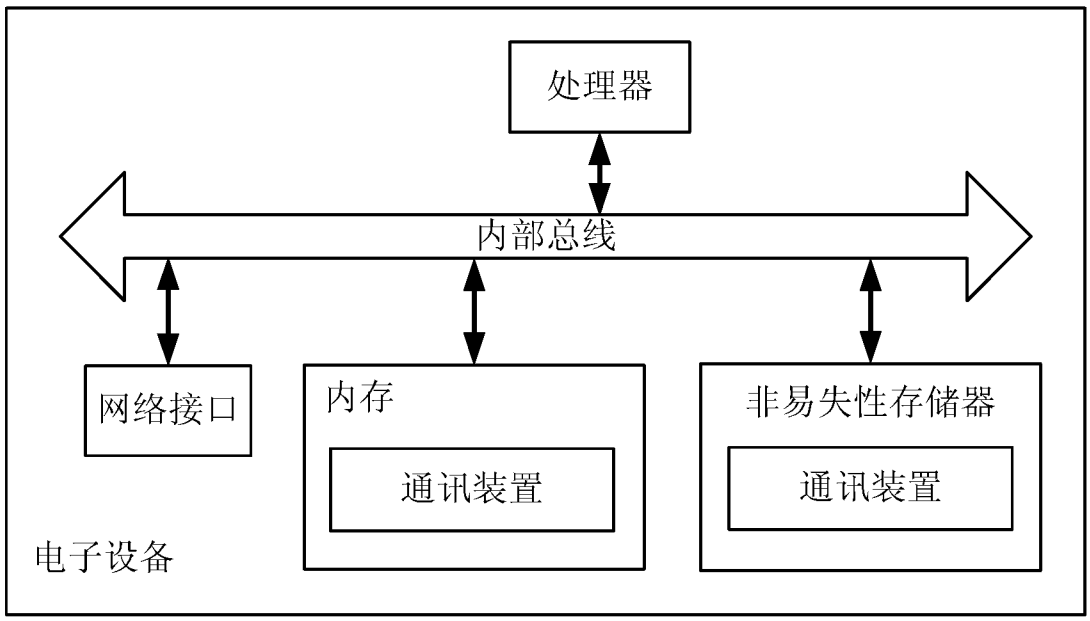
处理器
内部总线
网络接口
内存
通讯装置
非易失性存储器
通讯装置
电子设备

图 11

图 12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/072879

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i; H04L 9/32 (2006.01) i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L G06F H04M

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

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

CNPAT, CNKI, WPI, EPODOC: direct connection, identi+, authentication, verify, server, terminal, direct, communication, link, biological, physiology, habit, image, video, picture, security

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 105721468 A (ALIBABA GROUP HOLDING LIMITED), 29 June 2016 (29.06.2016), the whole document	1-26
PX	CN 105656871 A (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.), 08 June 2016 (08.06.2016), description, paragraphs [0047]-[0096]	1-26
X	CN 104580117 A (TENCENT INC.), 29 April 2015 (29.04.2015), description, paragraphs [0034]-[0050]	1-26
X	CN 105007167 A (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.), 28 October 2015 (28.10.2015), description, paragraphs [0034]-[0044]	1-26
X	CN 104660814 A (GUANG DONG OPPO MOBILE TELECOMMUNICATIONS CO., LTD.), 27 May 2015 (27.05.2015), description, paragraphs [0042]-[0053]	1-9, 14-22
A	CN 104298908 A (LENOVO (BEIJING) CO., LTD.), 21 January 2015 (21.01.2015), the whole document	1-26

☒ 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
01 March 2017 (01.03.2017)	**30 March 2017 (30.03.2017)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **JIANG, Li** Telephone No.: (86-10) **61648235**

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/072879

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2015070032 A1 (TEAMBLIND INC.), 14 May 2015 (14.05.2015), the whole document	1-26

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/072879

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 105721468 A	29 June 2016	None	
CN 105656871 A	08 June 2016	WO 2017000606 A1	05 January 2017
CN 104580117 A	29 April 2015	None	
CN 105007167 A	28 October 2015	None	
CN 104660814 A	27 May 2015	None	
CN 104298908 A	21 January 2015	None	
WO 2015070032 A1	14 May 2015	JP 2016508259 A	17 March 2016
		US 2015304849 A1	22 October 2015
		KR 20150053701 A	18 May 2015

国际检索报告

国际申请号
PCT/CN2017/072879

A. 主题的分类

H04L 29/06(2006.01)i; H04L 9/32(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L G06F H04M

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNPAT,CNKI,WPI,EPODOC:身份，认证，验证，服务器，终端，直接，直连，通信，通讯，生物，生理，习惯，图像，图片，视频，安全，identi+，authentication，verify，server，terminal，direct，communication，link，biological，physiology，habit，image，video，picture，security

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	CN 105721468 A (阿里巴巴集团控股有限公司) 2016年 6月 29日 (2016-06-29) 全文	1-26
PX	CN 105656871 A (宇龙计算机通信科技深圳有限公司) 2016年 6月 8日 (2016-06-08) 说明书第[0047]-[0096]段	1-26
X	CN 104580117 A (深圳市腾讯计算机系统有限公司) 2015年 4月 29日 (2015-04-29) 说明书第[0034]-[0050]段	1-26
X	CN 105007167 A (宇龙计算机通信科技深圳有限公司) 2015年 10月 28日 (2015-10-28) 说明书第[0034]-[0044]段	1-26
X	CN 104660814 A (广东欧珀移动通信有限公司) 2015年 5月 27日 (2015-05-27) 说明书第[0042]-[0053]段	1-9，14-22
A	CN 104298908 A (联想北京有限公司) 2015年 1月 21日 (2015-01-21) 全文	1-26

☑ 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 1日	2017年 3月 30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	蒋莉
传真号 (86-10)62019451	电话号码 (86-10)61648235

国际检索报告

国际申请号
PCT/CN2017/072879

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	WO 2015070032 A1 (TEAMBLIND INC.) 2015年 5月 14日 (2015 - 05 - 14) 全文	1-26

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2017/072879

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	105721468	A	2016年 6月 29日		无		
CN	105656871	A	2016年 6月 8日	WO	2017000606	A1	2017年 1月 5日
CN	104580117	A	2015年 4月 29日		无		
CN	105007167	A	2015年 10月 28日		无		
CN	104660814	A	2015年 5月 27日		无		
CN	104298908	A	2015年 1月 21日		无		
WO	2015070032	A1	2015年 5月 14日	JP	2016508259	A	2016年 3月 17日
				US	2015304849	A1	2015年 10月 22日
				KR	20150053701	A	2015年 5月 18日