

资源调用方法及装置

技术领域

本公开涉及移动通信技术领域，特别涉及一种资源调用方法及装置。

背景技术

用户感知的 API 访问 (Subscriber-aware Northbound API access, SNA) 安全性研究的目标之一是获得资源所有者的授权，相关技术中规定了允许用户设备 (User Equipment, UE) 提供/撤销对与第三方共享信息的许可。在这种情况下，UE 是资源所有者，而应用程序接口 (Application Programming Interface, API) 调用者在请求资源 (例如，特定 UE 的位置信息) 之前需要获得 UE 的授权。然而，在 API 调用场景中，并没有使 UE 能够授权 API 调用者请求其资源的机制。

发明内容

本公开提出了一种资源调用方法及装置，使 UE 能够授权 API 调用者在 API 调用场景中请求 UE 的资源。

本公开的第一方面实施例提供了一种资源调用方法，该方法由资源所有者执行，该方法包括：接收应用程序接口 API 调用者发送的资源授权请求和/或 API 授权请求，其中，资源授权请求用于请求、设置或修改资源所有者的资源；向第一实体发送授权码请求，授权码请求用于请求授权码；将从第一实体接收的授权码发送给 API 调用者。

在一些实施例中，该方法还包括：与 API 调用者进行相互认证；在认证通过的情况下，建立资源所有者与 API 调用者之间的第一连接，其中，第一连接为用于传输资源授权请求和/或 API 授权请求的安全连接。

在一些实施例中，与 API 调用者进行相互认证包括以下至少一项：当 API 调用者为用户设备 UE 时，基于证书与 API 调用者进行相互认证；当 API 调用者为应用功能 AF 时，通过基于 GBA 的认证机制、基于 AKMA 的认证机制或基于证书的认证机制进行相互认证。

在一些实施例中，接收 API 调用者发送的资源授权请求和/或 API 授权请求包括：当 API 调用者已经获得服务的授权，接收 API 调用者发送的资源授权请求；当 API 调用者未获得服务的授权，接收 API 调用者发送的资源授权请求和 API 授权请求，其中，资源授权请求中包括 API 调用者的标识、资源所有者的标识、目标资源标识中的至少一项，API 授权请求中包括服务标识符。

在一些实施例中，服务标识符包括以下至少一项：服务名称标识符、服务操作标识符、操作语义标识符、API 标识。

在一些实施例中，该方法还包括：与第一实体进行相互认证；在认证通过的情况下，建立资源所有者与第一实体之间的第二连接；其中，第二连接为用于传输授权码请求和响应的安全连接。

在一些实施例中，与第一实体进行相互认证包括：基于以下认证机制中的至少一项进行相互认证：基于证书的认证机制；基于 GBA 的认证机制；基于 AKMA 的认证机制；TLS-PSK；基于 OAuth 令牌的认证机制。

在一些实施例中，向第一实体发送授权码请求包括以下至少一项：实时同意资源授权请求以向第一实体发送授权码请求；根据资源所有者的本地策略异步同意资源授权请求以向第一实体发送授权码请求；向第一实体发送本地策略和/或授权码请求，本地策略用于辅助第一实体异步同意资源授权请求。

在一些实施例中，该方法还包括：当资源授权请求获得授权，且当 API 调用者已经获得服务的授权时，接收第一实体发送的授权码。

在一些实施例中，资源所有者为用户设备 UE，资源为 UE 的服务质量和/或位置信息。

本公开第二方面实施例提供了一种资源调用方法，该方法由第一实体执行，该方法包括：接收资源所有者发送的授权码请求，授权码请求用于请求授权码；向资源所有者发送授权码；接收 API 调用者发送的授权码；根据授权码生成令牌，并将令牌发送给 API 调用者。

在一些实施例中，该方法还包括：与资源所有者进行相互认证；在认证通过的情况下，建立资源所有者与第一实体之间的第二连接，其中，第二连接为用于传输授权码请求和响应的安全连接。

在一些实施例中，与资源所有者进行相互认证包括：基于以下认证机制中的至少一项进行相互认证：基于证书的认证机制；基于 GBA 的认证机制；基于 AKMA 的认证机制；TLS-PSK；基于 OAuth 令牌的认证机制。

在一些实施例中,接收资源所有者发送的授权码请求包括以下至少一项:根据资源所有者对资源授权请求的实时同意,接收授权码请求;根据资源所有者对资源授权请求的异步同意,接收授权码请求;接收资源所有者发送的本地策略和/或授权码请求,异步同意资源授权请求。

在一些实施例中,接收资源所有者发送的授权码请求还包括:当资源授权请求获得同意,且当 API 调用者已经获得服务的授权时,生成授权码。

在一些实施例中,当资源授权请求获得同意,且当 API 调用者已经获得服务的授权时,生成授权码包括:当资源授权请求获得同意,但 API 调用者未获得服务的授权时,根据预设策略,判断是否同意 API 调用者的服务授权请求;当同意 API 调用者的服务授权请求时,生成授权码。

在一些实施例中,该方法还包括:与 API 调用者进行相互认证;在认证通过的情况下,建立 API 调用者与第一实体之间的第三连接,其中,第三连接为用于传输授权码的安全连接。

在一些实施例中,与 API 调用者进行相互认证包括:基于以下认证机制中的至少一项进行相互认证:基于证书的认证机制;基于 GBA 的认证机制;基于 AKMA 的认证机制;TLS-PSK;基于 OAuth 令牌的认证机制。

在一些实施例中,根据授权码生成令牌,并将令牌发送给 API 调用者包括以下至少一项:向 API 调用者发送访问令牌和/或刷新令牌;接收 API 调用者发送的刷新令牌,基于刷新令牌向 API 调用者发送访问令牌。

在一些实施例中,第一实体为 CAPIF 核心功能或者授权功能。

本公开的第三方面实施例提供了一种资源调用方法,该方法由 API 调用者执行,该方法包括:向资源所有者发送资源授权请求和/或 API 授权请求,资源授权请求用于请求、设置或修改资源所有者的资源;接收资源所有者发送的授权码,并向第一实体发送授权码;接收第一实体基于授权码生成的令牌。

在一些实施例中,该方法还包括:与资源所有者进行相互认证;在认证通过的情况下,建立资源所有者与 API 调用者之间的第一连接,其中,第一连接为用于传输资源授权请求和/或 API 授权请求的安全连接。

在一些实施例中,与资源所有者进行相互认证包括以下至少一项:当 API 调用者为用户设备 UE 时,基于证书与资源所有者进行相互认证;当 API 调用者为应用功能 AF 时,通过基于 GBA 的认证机制、基于 AKMA 的认证机制或基于证书的认证机制与资源所有者进行相互认证。

在一些实施例中,向资源所有者发送资源授权请求和/或 API 授权请求包括:当 API 调用者已经获得服务的授权时,向资源所有者发送资源授权请求;当 API 调用者未获得服务的授权时,向资源所有者发送资源授权请求和 API 授权请求,其中,资源授权请求中包括 API 调用者的标识、资源所有者的标识、目标资源标识中的至少一项,API 授权请求中包括服务标识符。

在一些实施例中,当所述 API 调用者已经获得服务的授权,且所述 API 调用者向所述资源所有者发送的资源授权请求获得同意,所述第一实体基于所述授权码生成的令牌仅包括资源相关的授权信息。

在一些实施例中,该方法还包括:与第一实体进行相互认证;在认证通过的情况下,建立 API 调用者与第一实体之间的第三连接;其中,第三连接为用于传输授权码的安全连接。

在一些实施例中,接收第一实体基于授权码生成的令牌包括以下至少一项:接收第一实体发送的访问令牌和/或刷新令牌;向第一实体发送刷新令牌,并接收第一实体基于刷新令牌发送的访问令牌。

在一些实施例中,API 调用者为用户设备 UE 或者应用功能 AF,资源为资源所有者的服务质量和/或位置信息。

本公开的第四方面实施例提供了一种资源调用装置,该装置配置于资源所有者,该装置包括收发模块,收发模块用于:接收应用程序接口 API 调用者发送的资源授权请求和/或 API 授权请求,资源授权请求用于请求、设置或修改资源所有者的资源;向第一实体发送授权码请求,授权码请求用于请求授权码;将从第一实体接收的授权码发送给 API 调用者。

本公开的第五方面实施例提供了一种资源调用装置,该装置配置于第一实体,该装置包括收发模块,收发模块用于:接收资源所有者发送的授权码请求,授权码请求用于请求授权码;向资源所有者发送授权码;接收 API 调用者发送的授权码;根据授权码生成令牌,并将令牌发送给 API 调用者。

本公开的第六方面实施例提供了一种资源调用装置,该装置包括收发模块,收发模块用于:向资源所有者发送资源授权请求和/或 API 授权请求,资源授权请求用于请求、设置或修改资源所有者的资源;接收资源所有者发送的授权码,并向第一实体发送授权码;接收第一实体基于授权码生成的令牌。

本公开的第七方面实施例提供了一种通信系统,通信系统包括资源所有者、API 调用者、第一实体,其中:

资源所有者被配置为执行如上述第一方面实施例中任一项资源调用方法;

第一实体被配置为执行如上述第二方面实施例中任一项资源调用方法;

API 调用者被配置为执行如上述第三方面实施例中任一项资源调用方法。

本公开的第八方面实施例提供了一种通信设备，包括：收发器；存储器；处理器，分别与收发器及存储器连接，配置为通过执行存储器上的计算机可执行指令，控制收发器的无线信号收发，并能够实现上述第一方面实施例或第二方面实施例或第三方面实施例的资源调用方法。

本公开第九方面实施例提出了一种计算机存储介质，其中，计算机存储介质存储有计算机可执行指令；计算机可执行指令被处理器执行后，能够实现上述第一方面实施例或第二方面实施例或第三方面实施例的资源调用方法。

本公开实施例提供了一种资源调用方法及装置，资源所有者可以接收应用程序接口 API 调用者发送的资源授权请求和/或 API 授权请求，资源授权请求用于请求、设置或修改资源所有者的资源，并向第一实体发送授权码请求，其中授权码请求用于请求授权码，资源所有者可以将第一实体接收的授权码发送给 API 调用者。本公开提供的方案实现了在 API 调用场景中，UE 能够授权 API 调用者请求 UE 的资源，避免在授权过程中资源所有者对数据的篡改，避免在授权过程中资源所有者对数据的篡改。

本公开附加的方面和优点将在下面的描述中部分给出，部分将从下面的描述中变得明显，或通过本公开的实践了解到。

附图说明

本公开上述的和/或附加的方面和优点从下面结合附图对实施例的描述中将变得明显和容易理解，其中：

- 图 1 为根据本公开实施例的一种资源调用方法的流程示意图；
- 图 2 为根据本公开实施例的一种资源调用方法的流程示意图；
- 图 3 为根据本公开实施例的一种资源调用方法的流程示意图；
- 图 4 为根据本公开实施例的一种资源调用方法的流程示意图；
- 图 5 为根据本公开实施例的一种资源调用方法的流程示意图；
- 图 6 为根据本公开实施例的一种资源调用方法的流程示意图；
- 图 7 为根据本公开实施例的一种资源调用方法的交互示意图；
- 图 8 为根据本公开实施例的一种资源调用方法的交互示意图；
- 图 9 为根据本公开实施例的一种资源调用装置的框图；
- 图 10 为根据本公开实施例的一种资源调用装置的框图；
- 图 11 为根据本公开实施例的一种资源调用装置的框图；
- 图 12 为根据本公开实施例的一种资源调用装置的框图；
- 图 13 为根据本公开实施例的一种资源调用装置的框图；
- 图 14 为根据本公开实施例的一种资源调用装置的框图；
- 图 15 为根据本公开实施例的一种资源调用装置的框图；
- 图 16 为本公开实施例提供的一种通信装置的结构示意图；
- 图 17 为本公开实施例提供的一种芯片的结构示意图。

具体实施方式

下面详细描述本公开的实施例，实施例的示例在附图中示出，其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的，旨在用于解释本公开，而不能理解为对本公开的限制。

SNAAPP 安全性研究的目标之一是获得资源所有者的授权，在 TS 22.261 [1]第 6.10.2 条中规定了允许 UE 提供/撤销对与第三方共享的信息（例如位置信息、存在信息等）的许可。在这种情况下，UE 是资源所有者，而 API 调用者在请求资源（例如，特定 UE 的位置信息）之前需要获得 UE 的授权。然而，在 API 调用场景中，并没有使 UE 能够授权 API 调用者请求其资源的机制。

为此，本公开提出了一种资源调用方法及装置，使 UE 能够授权 API 调用者在 API 调用场景中请求 UE 的资源。

下面结合附图对本申请所提供的资源调用方法及装置进行详细地介绍。

图 1 示出了根据本公开实施例的一种资源调用方法的流程示意图。该方法可由资源所有者执行，具体地，资源所有者可以是 UE。如图 1 所示，该方法可以包括以下步骤。

S101，接收 API 调用者发送的资源授权请求和/或 API 授权请求，资源授权请求用于请求、设置或修改资源所有者的资源。

在本公开的实施例中，API调用者可以是UE或应用功能（Application Function，AF）。API调用者可以向资源请求者发送资源授权请求，以请求UE授权API调用者对资源的调用。其中，资源可以是资源所有者的位置信息和/或服务质量（Quality of Service，QoS）。

在本公开的一些实施例中，资源所有者还可以从API调用者接收API授权请求，该情况针对于API调用者尚未获得API授权的情况。

S102，向第一实体发送授权码请求，授权码请求用于请求授权码。

在本公开的实施例中，第一实体可以是通用API框架（Common API Framework，CAPIF）核心功能（CAPIF Core Function，CCF）或者授权功能（Authorization Function）。资源所有者可以向第一实体发送授权码请求，以向第一实体请求授权码。

可以理解的是，该授权码可以理解为授权API调用者在API调用场景中调用资源所有者的资源的凭证。

S103，将从第一实体接收的授权码发送给API调用者。

在本公开的实施例中，资源所有者可以从第一实体接收所请求的授权码，并将该授权码发送给API调用者，以供API调用者进行后续流程，例如兑换令牌。

应当理解，在UE授权API调用者请求其资源的过程中，有了令牌就可以访问资源，而不会做身份认证，如果资源所有者接触到令牌，资源所有者会冒充API调用者修改数据并诬陷该修改行为是API调用者所为。因此，本公开通过授权码隔离了资源所有者接触令牌，使得资源所有者无法接触不到授予API调用者进行资源调用的令牌，保证了UE授权API调用者请求其资源的可行性和安全性。

综上，根据本公开提供的资源调用方法，资源所有者可以接收应用程序接口API调用者发送的资源授权请求和/或API授权请求，资源授权请求用于请求、设置或修改资源所有者的资源，并向第一实体发送授权码请求，其中授权码请求用于请求授权码，资源所有者可以将第一实体接收的授权码发送给API调用者。本公开提供的方案实现了在API调用场景中，UE能够授权API调用者请求UE的资源，避免在授权过程中资源所有者对数据的篡改。

图2示出了根据本公开实施例的一种资源调用方法的流程示意图。该方法可由资源所有者执行，基于图1所示实施例，如图2所示，该方法可以包括以下步骤。

S201，与API调用者进行相互认证。

在一些可选实施例中，与API调用者进行相互认证可以通过如下方式进行。

在一种方式中，当API调用者为设备UE时，基于证书与API调用者进行相互认证。

在另一种方式中，当API调用者为应用功能AF时，通过基于GBA的认证机制、基于AKMA的认证机制或基于证书的认证机制进行相互认证。

具体地，API调用者和资源所有者可以进行相互认证。对于API调用者为UE的情况，可以基于证书实现相互认证。对于API调用者为A的情况，可以通过基于GBA的认证机制、基于AKMA的认证机制或基于证书的认证机制来实现相互认证。

S202，在认证通过的情况下，建立资源所有者与API调用者之间的第一连接。

本公开中，第一连接为用于传输资源授权请求和/或API授权请求的安全连接。

可以理解的是，API调用者和资源所有者之间的安全连接是在相互认证之后建立的。该安全连接可以是安全传输层（Transport Layer Security，TLS）连接，即，基于TLS协议建立的安全连接。

在本公开中，资源所有者与API调用者进行双向认证并建立安全连接的目的在于，资源调用者需要核对请求中的API调用者的身份信息是否和已经验证的信息一致，或者能被映射到已经验证的信息。例如，资源所有者已经验证的是API调用者的手机号，但是发来的请求中为对应的微信号，那么这个请求也可以被同意。

S203，接收应用程序接口API调用者发送的资源授权请求和/或API授权请求。

本公开的实施例中，资源授权请求用于请求、设置或修改资源所有者的资源。

在本公开中，针对API调用者是否获得API授权的不同情况，可进行不同的请求发送。

在一种示例中，当API调用者已经获得服务的授权，接收API调用者发送的资源授权请求。其中，资源授权请求中包括API调用者的标识、资源所有者的标识、目标资源标识中的至少一项。换言之，如果API调用者已经获得服务的授权，则API调用者向资源所有者发送的请求中包含API调用者的身份标识（例如GPSI、IMPI或应用层ID）、资源所有者（例如称为目标UE）的身份标识（例如GPSI、IMPI或应用层ID）、目标资源标识（例如，目标UE的位置、目标UE的QoS）。

在另一种示例中，当API调用者未获得服务的授权，接收API调用者发送的资源授权请求和API授权请求。其中，资源授权请求中包括API调用者的标识、资源所有者的标识、目标资源标识中的至

少一项，API 授权请求中包括服务标识符。换言之，如果 API 调用者未获得服务的授权，则 API 调用者向资源所有者发送的请求中除了包含 API 调用者的身份标识、目标 UE 的身份标识、目标资源标识之外，还包括服务标识符。

在本公开的实施例中，服务标识符包括以下至少一项：服务名称标识符（Service Name）、服务操作标识符（Service Operation）、操作语义标识符（Operation Semantics）、API 标识。

可以理解的是，当所述 API 调用者已经获得服务的授权，即，API 调用者仅发送资源授权请求时，并且所述 API 调用者向所述资源所有者发送的资源授权请求获得同意，则所述第一实体基于所述授权码生成的令牌仅包括资源相关的授权信息。

S204，与第一实体进行相互认证。

在本公开的实施例中，资源所有者可以基于以下认证机制中的至少一项与第一实体进行相互认证：基于证书的认证机制；基于 GBA 的认证机制；基于 AKMA 的认证机制；TLS-PSK；基于 OAuth 令牌的认证机制。

具体地，针对第一实体为 CCF 和 Authorization Function 的不同情况，可以采取不同的认证策略。对于第一实体为 CCF 的情况，资源所有者可以通过证书对 CCF 进行认证，然后 CCF 可以使用基于 GBA 的认证机制、基于 AKMA 的认证机制或基于证书的认证机制来认证资源所有者。CCF 还可以在认证后为资源所有者生成证书和 OAuth 2.0 令牌。对于第一实体为 Authorization Function 的情况，资源所有者可以通过证书对授权功能进行认证。然后 Authorization Function 可以使用 TLS-PSK、基于 OAuth 令牌的认证机制、基于 GBA 的认证机制、基于 AKMA 的认证机制或基于证书的认证机制来认证资源所有者，其中证书可以由 CCF 分配。

S205，在认证通过的情况下，建立资源所有者与第一实体之间的第二连接。

其中，第二连接为用于传输授权码请求和响应的安全连接。可以理解的是，资源所有者和 CCF/Authorization Function 之间的安全连接是在相互认证之后建立的。该安全连接可以是 TLS 连接，即，基于 TLS 协议建立的安全连接。

S206，向第一实体发送授权码请求。

在本公开的实施例中，资源所有者可以通过同步或异步的方式实现向第一实体发送授权码请求。

针对同步的情况，在一种示例中，资源所有者实时同意资源授权请求以向第一实体发送授权码请求。换言之，资源所有者可以及时、同步地授予对资源的授权请求。资源所有者向第一实体发送授权请求和授权信息，以请求授权码。

针对异步的情况，在另一种示例中，资源所有者根据资源所有者的本地策略异步同意资源授权请求以向第一实体发送授权码请求。换言之，资源所有者可以根据本地预先生成的配置文件，异步地授予对资源的授权请求，而无需实时响应。资源所有者向第一实体发送授权请求和授权信息，以请求授权码。

针对另一种异步的情况，在另一种示例中，资源所有者向第一实体发送本地策略和/或授权码请求，本地策略用于辅助第一实体异步同意资源授权请求。换言之，如果资源所有者之前将预先生成的配置文件发送给第一实体，则资源所有者向第一实体发送授权请求以请求授权码。第一实体可以根据预先生成的文件对资源的授权请求进行授权。可以理解的是，发送授权码请求和发送本地策略之间没有先后顺序或绑定关系，资源所有者可以在发送授权码请求之前或之后或同时发送本地策略，在本公开中不予限制。

S207，接收第一实体发送的授权码。

具体地，当资源授权请求获得授权，且当 API 调用者已经获得服务的授权时，资源所有者接收第一实体发送的授权码。

应当理解，是否发送授权码由第一实体决定，换言之，当资源访问和 API 授权均被同意，第一实体才生成并向资源所有者发送授权码。具体地，如果 API 调用者已经获得服务的授权，则第一实体在 API 调用者被授权请求资源时为 API 调用者生成授权码，也即，如果资源访问已经获得同意，且 API 调用者没有请求 API 相关的授权（在先已经获得 API 授权而无需再次请求），那么第一实体直接发送授权码进行资源请求。如果 API 调用者没有获得服务的授权，第一实体根据预先配置的策略检查 API 调用者是否被授权调用服务。如果 API 调用者被授权调用服务和资源，则第一实体为 API 生成授权码，也即，如果资源访问已经获得同意，但 API 调用者需要 API 授权，则第一实体可以根据运营商预设策略，判断 API 调用者是否可以访问该 API，如果可以，则第一实体生成并发送授权码，如果不可以，则不发。

S208，将授权码发送给 API 调用者。

本公开的实施例中，资源所有者接收到第一实体发送的授权码后，将授权码发送给 API 调用者，以用于后续兑换令牌。

应当理解的是,上述步骤 S201、S202、S204 以及 S205 为可选步骤。换言之,本公开中的请求和响应消息可以在没有身份认证及建立安全连接的条件下传递。

综上,根据本公开提供的资源调用方法,资源所有者可以与 API 调用者、第一实体进行双向认证,资源所有者可以接收应用程序接口 API 调用者发送的资源授权请求和/或 API 授权请求,并向第一实体发送授权码请求,其中授权码请求用于请求授权码,资源所有者可以将从第一实体接收的授权码发送给 API 调用者。本公开提供的方案实现了在 API 调用场景中,UE 能够授权 API 调用者请求 UE 的资源,避免在授权过程中资源所有者对数据的篡改。

图 3 示出了根据本公开实施例的一种资源调用方法的流程示意图。该方法可由第一实体执行,具体地,如上所述,第一实体可以是 CCF 或 Authorization Function。如图 3 所示,该方法可以包括以下步骤。

S301,接收资源所有者发送的授权码请求。

本公开中,授权码请求用于请求授权码。可以理解的是,该授权码可以理解为授权 API 调用者在 API 调用场景中调用资源所有者的资源的凭证。

S302,向资源所有者发送授权码。

在本公开的实施例中,当满足特定条件时,第一实体可以生成授权码并发送给资源所有者。其中,特定条件是指资源访问和 API 授权均被同意。

S303,接收 API 调用者发送的授权码。

在本公开的实施例中,授权码经发送给资源所有者后,由资源所有者发送给 API 调用者,第一实体从 API 调用者接收授权码,从而兑换令牌。

S304,根据授权码生成令牌,并将令牌发送给 API 调用者。

在本公开的实施例中,第一实体根据授权码生成令牌,并将令牌发送给 API 调用者,以使 API 调用者进行后续流程。

综上,根据本公开提供的资源调用方法,第一实体可以接收资源所有者发送的授权码请求,并响应该请求生成授权码并发送给资源所有者,接收 API 调用者发送的授权码,并根据该授权码生成令牌提供给 API 调用者。本公开提供的方案实现了在 API 调用场景中,UE 能够授权 API 调用者请求 UE 的资源,避免在授权过程中资源所有者对数据的篡改。

图 4 示出了根据本公开实施例的一种资源调用方法的流程示意图,该方法可由第一实体执行,基于图 3 的实施例,如图 4 所示,该方法可以包括以下步骤。

S401,与资源所有者进行相互认证。

在本公开的实施例中,第一实体可以基于以下认证机制中的至少一项与资源所有者进行相互认证:基于证书的认证机制;基于 GBA 的认证机制;基于 AKMA 的认证机制;TLS-PSK;基于 OAuth 令牌的认证机制。

具体地,针对第一实体为 CCF 和 Authorization Function 的不同情况,可以采取不同的认证策略。对于第一实体为 CCF 的情况,资源所有者可以通过证书对 CCF 进行认证,然后 CCF 可以使用基于 GBA 的认证机制、基于 AKMA 的认证机制或基于证书的认证机制来认证资源所有者。CCF 还可以在认证后为资源所有者生成证书和 OAuth 2.0 令牌。对于第一实体为 Authorization Function 的情况,资源所有者可以通过证书对授权功能进行认证。然后 Authorization Function 可以使用 TLS-PSK、基于 OAuth 令牌的认证机制、基于 GBA 的认证机制、基于 AKMA 的认证机制或基于证书的认证机制来认证资源所有者,其中证书可以由 CCF 分配。

S402,在认证通过的情况下,建立资源所有者与第一实体之间的第二连接。

其中,第二连接为用于传输授权码请求和响应的安全连接。可以理解的是,资源所有者和 CCF/Authorization Function 之间的安全连接是在相互认证之后建立的。可以通过 TLS 建立安全连接。该安全连接可以是 TLS 连接,即,基于 TLS 协议建立的安全连接。

S403,接收资源所有者发送的授权码请求。

在本公开的实施例中,资源所有者可以通过同步或异步的方式实现向第一实体发送授权码请求,换言之,资源所有者可以通过不同方式处理资源请求:

1. 资源所有者根据本地策略同意请求。

针对同步的情况,在一种示例中,第一实体根据资源所有者对资源授权请求的实时同意,接收授权码请求。资源所有者实时同意资源授权请求以向第一实体发送授权码请求。换言之,资源所有者可以及时、同步地授予对资源的授权请求。资源所有者向第一实体发送授权请求和授权信息,以请求授权码。

2. 资源所有者实时同意请求。

针对异步的情况，在另一种示例中，第一实体可以根据资源所有者对资源授权请求的异步同意，接收授权码请求。资源所有者根据资源所有者的本地策略异步同意资源授权请求以向第一实体发送授权码请求。换言之，资源所有者可以根据本地预先生成的配置文件，异步地授予对资源的授权请求，而无需实时响应。资源所有者向第一实体发送授权请求和授权信息，以请求授权码。

3. 资源所有者将策略发送至 CCF/Authorization Function，Authorization Function 根据策略来统一请求。

针对另一种异步的情况，在另一种示例中，第一实体接收资源所有者发送的本地策略和/或授权码请求，异步同意资源授权请求。资源所有者向第一实体发送本地策略和/或授权码请求，本地策略用于辅助第一实体异步同意资源授权请求。换言之，如果资源所有者之前将预生成的配置文件发送给第一实体，则资源所有者向第一实体发送授权请求以请求授权码。第一实体可以根据预先生成的文件对资源的授权请求进行授权。可以理解的是，发送授权码请求和发送本地策略之间没有先后顺序或绑定关系，资源所有者可以在发送授权码请求之前或之后或同时发送本地策略，在本公开中不予限制。

S404，当资源授权请求获得同意，且当 API 调用者已经获得服务的授权时，生成授权码。

具体地，当资源授权请求获得授权，且当 API 调用者已经获得服务的授权时，第一实体可以生成授权码。

应当理解，是否生成授权码由第一实体决定，换言之，当资源访问和 API 授权均被同意，第一实体才生成并向资源所有者发送授权码。具体地，如果 API 调用者已经获得服务的授权，则第一实体在 API 调用者被授权请求资源时为 API 调用者生成授权码，也即，如果资源访问已经获得同意，且 API 调用者没有请求 API 相关的授权（在先已经获得 API 授权而无需再次请求），那么第一实体直接发送授权码进行资源请求。

具体地，该步骤还包括：当资源授权请求获得同意，但 API 调用者未获得服务的授权时，根据预设策略，判断是否同意 API 调用者的服务授权请求；当同意 API 调用者的服务授权请求时，生成授权码。

换言之，如果 API 调用者没有获得服务的授权，第一实体根据预先配置的策略检查 API 调用者是否被授权调用服务。如果 API 调用者被授权调用服务和资源，则第一实体为 API 生成授权码，也即，如果资源访问已经获得同意，但 API 调用者需要 API 授权，则第一实体可以根据运营商预设策略，判断 API 调用者是否可以访问该 API，如果可以，则第一实体生成并发送授权码，如果不可以，则不发。

S405，向资源所有者发送授权码。

在本公开的实施例中，当满足特定条件时，第一实体可以生成授权码并发送给资源所有者。其中，如上一步骤所述，特定条件是指资源访问和 API 授权均被同意。

S406，与 API 调用者进行相互认证。

在本公开的实施例中，第一实体可以基于以下认证机制中的至少一项与 API 调用者进行相互认证：基于证书的认证机制；基于 GBA 的认证机制；基于 AKMA 的认证机制；TLS-PSK；基于 OAuth 令牌的认证机制。

具体地，针对第一实体为 CCF 和 Authorization Function 的不同情况，可以采取不同的认证策略。对于第一实体为 CCF 的情况，资源所有者可以通过证书对 CCF 进行认证，然后 CCF 可以使用基于 GBA 的认证机制、基于 AKMA 的认证机制或基于证书的认证机制来认证资源所有者。CCF 还可以在认证后为资源所有者生成证书和 OAuth 2.0 令牌。对于第一实体为 Authorization Function 的情况，资源所有者可以通过证书对授权功能进行认证。然后 Authorization Function 可以使用 TLS-PSK、基于 OAuth 令牌的认证机制、基于 GBA 的认证机制、基于 AKMA 的认证机制或基于证书的认证机制来认证资源所有者，其中证书可以由 CCF 分配。

S407，在认证通过的情况下，建立 API 调用者与第一实体之间的第三连接。

其中，第三连接为用于传输授权码的安全连接。可以理解的是，该安全连接是在相互认证之后建立的。该安全连接可以是 TLS 连接，即，基于 TLS 协议建立的安全连接。

S408，接收 API 调用者发送的授权码。

在本公开的实施例中，第一实体可以接收 API 调用者发送的授权码。可以理解的是，第一实体将授权码发送至资源所有者后，资源所有者将授权码发送给 API 调用者，API 调用者将授权码发送给第一实体，以用于后续兑换令牌。

S409，根据授权码生成令牌，并将令牌发送给 API 调用者。

在本公开的实施例中，第一实体可以通过如下方式生成并发送令牌给 API 调用者。

在一种示例中，第一实体向 API 调用者发送访问令牌和/或刷新令牌。

在另一种示例中，第一实体接收 API 调用者发送的刷新令牌，基于刷新令牌向 API 调用者发送访问令牌。

换言之，第一实体可以直接将刷新令牌/访问令牌发送给 API 调用者，或者，API 调用者可以将刷新令牌发送给第一实体以获取访问令牌。

在本公开的实施例中，访问令牌包括 CCF 身份标识（如 NF instance ID、NF ID）、Authorization Function 身份标识（如 NF instance ID、NF ID）、第二实体身份标识（如 NF instance ID、NF ID）、服务标识符、API 调用者身份标识（例如，GPSI、IMSI、应用层 ID）、资源所有者身份标识（例如，GPSI、IMSI、应用层 ID）、资源标识（例如，位置）、过期时间中的至少一项。其中，第二实体为 API 开放功能（API Exposing Function，AEF）。

应当理解的是，上述步骤 S401、S402、S406 以及 S407 为可选步骤。换言之，本公开中的请求和响应消息可以在没有身份认证及建立安全连接的条件上传递。

综上，根据本公开提供的资源调用方法，第一实体可以与资源所有者、API 调用者进行双向认证，第一实体可以接收资源所有者发送的授权码请求，并响应该请求生成授权码并发送给资源所有者，接收 API 和发送的授权码，并根据该授权码生成令牌提供给 API 调用者。本公开提供的方案实现了在 API 调用场景中，UE 能够授权 API 调用者请求 UE 的资源，避免在授权过程中资源所有者对数据的篡改。

图 5 示出了根据本公开实施例的一种资源调用方法的流程示意图。该方法可由 API 调用者执行，如上所述，API 调用者可以是 UE 或应用功能 AF。如图 5 所示，该方法可以包括以下步骤。

S501，向资源所有者发送资源授权请求和/或 API 授权请求。

本公开中，资源授权请求用于请求、设置或修改资源所有者的资源。其中，资源可以是资源所有者的位置信息和/或服务质量（Quality of Service，QoS）。

在本公开的实施例中，针对 API 调用者为不同实体的情况，所请求的资源可以包括不同内容。具体地，如果 API 调用者是 UE，所述资源包括 UE 在私人物联网（Personal IoT network，PIN）中的参数，例如 UE 作为具有管理功能的 PIN 单元（PIN elements with management capability）时，所述资源可以为 PEMC 的 QoS；UE 作为具有网关功能的 PIN 单元（PIN elements with gateway capability）时，所述资源可以为 PEGC 的 QoS；UE 作为 PEGC 时，所述资源也可以为 PEGC 下属 PIN 单元（PIN element）的 QoS，对此在本公开中不予限制。

在本公开的一些实施例中，API 调用者还可以向资源所有者发送 API 授权请求，该情况针对于 API 调用者尚未获得 API 授权的情况。

S502，接收资源所有者发送的授权码，并向第一实体发送授权码。

可以理解的是，该授权码可以理解为授权 API 调用者在 API 调用场景中调用资源所有者的资源的凭证。

在本公开的实施例中，当满足特定条件时，第一实体可以生成授权码并发送给资源所有者。其中，特定条件是指资源访问和 API 授权均被同意。随后，资源所有者将授权码发送给 API 调用者，API 调用者接收到该授权码后，可以将授权码发送至第一实体，以兑换令牌。

S503，接收第一实体基于授权码生成的令牌。

在本公开的实施例中，第一实体根据授权码生成令牌，并将令牌发送给 API 调用者，以使 API 调用者进行后续流程。

综上，根据本公开提供的资源调用方法，API 调用者可以向资源所有者发送资源授权请求和/或 API 授权请求，资源授权请求用于请求、设置或修改资源所有者的资源，接收资源所有者发送的授权码，并向第一实体发送授权码，并接收第一实体基于授权码生成的令牌。本公开提供的方案实现了在 API 调用场景中，UE 能够授权 API 调用者请求 UE 的资源，避免在授权过程中资源所有者对数据的篡改。

图 6 示出了根据本公开实施例的一种资源调用方法的流程示意图。基于图 5 的实施例，本方法由 API 调用者执行。如图 6 所示，该方法可以包括以下步骤。

S601，与资源所有者进行相互认证。

在本公开的实施例中，API 调用者与资源所有者进行相互认证可以通过如下方式进行。

在一种方式中，当 API 调用者为设备 UE 时，基于证书与 API 调用者进行相互认证。

在另一种方式中，当 API 调用者为应用功能 AF 时，通过基于 GBA 的认证机制、基于 AKMA 的认证机制或基于证书的认证机制进行相互认证。

具体地, API 调用者和资源所有者可以进行相互认证。对于 API 调用者为 UE 的情况, 可以基于证书实现相互认证。对于 API 调用者为 A 的情况, 可以通过基于 GBA 的认证机制、基于 AKMA 的认证机制或基于证书的认证机制来实现相互认证。

S602, 在认证通过的情况下, 建立资源所有者与 API 调用者之间的第一连接。

本公开中, 第一连接为用于传输资源授权请求和/或 API 授权请求的安全连接。

可以理解的是, API 调用者和资源所有者之间的安全连接是在相互认证之后建立的。该安全连接可以是 TLS 连接, 即, 基于 TLS 协议建立的安全连接。

在本公开中, 资源所有者与 API 调用者进行双向认证并建立安全连接的目的在于, 资源调用者需要核对请求中的 API 调用者的身份信息是否和已经验证的信息一致, 或者能被映射到已经验证的信息。例如, 资源所有者已经验证的是 API 调用者的手机号, 但是发来的请求中为对应的微信号, 那么这个请求也可以被同意。

S603, 向资源所有者发送资源授权请求和/或 API 授权请求。

本公开的实施例中, 资源授权请求用于请求、设置或修改资源所有者的资源。

在本公开中, 针对 API 调用者是否获得 API 授权的不同情况, 可进行不同的请求发送。

在一种示例中, 当 API 调用者已经获得服务的授权, 接收 API 调用者发送的资源授权请求。其中, 资源授权请求中包括 API 调用者的标识、资源所有者的标识、目标资源标识中的至少一项。换言之, 如果 API 调用者已经获得服务的授权, 则 API 调用者向资源所有者发送的请求中包含 API 调用者的身份标识 (例如 GPSI、IMPI 或应用层 ID)、资源所有者 (例如称为目标 UE) 的身份标识 (例如 GPSI、IMPI 或应用层 ID)、目标资源标识 (例如, 目标 UE 的位置、目标 UE 的 QoS)。

在另一种示例中, 当 API 调用者未获得服务的授权, 接收 API 调用者发送的资源授权请求和 API 授权请求。其中, 资源授权请求中包括 API 调用者的标识、资源所有者的标识、目标资源标识中的至少一项, API 授权请求中包括服务标识符。换言之, 如果 API 调用者未获得服务的授权, 则 API 调用者向资源所有者发送的请求中除了包含 API 调用者的身份标识、目标 UE 的身份标识、目标资源标识之外, 还包括服务标识符。

可以理解的是, 当所述 API 调用者已经获得服务的授权, 即, API 调用者仅发送资源授权请求时, 并且所述 API 调用者向所述资源所有者发送的资源授权请求获得同意, 则所述第一实体基于所述授权码生成的令牌仅包括资源相关的授权信息。S604, 接收资源所有者发送的授权码。

可以理解的是, 该授权码是第一实体在满足特定条件时生成并发送给资源所有者的, 其中特定条件指的是资源访问和 API 授权均被同意。资源所有者将授权码发送至 API 调用者, 以用于兑换令牌。

S605, 与第一实体进行相互认证。

在本公开的实施例中, 第一实体可以基于以下认证机制中的至少一项与 API 调用者进行相互认证: 基于证书的认证机制; 基于 GBA 的认证机制; 基于 AKMA 的认证机制; TLS-PSK; 基于 OAuth 令牌的认证机制。

具体地, 针对第一实体为 CCF 和 Authorization Function 的不同情况, 可以采取不同的认证策略。对于第一实体为 CCF 的情况, 资源所有者可以通过证书对 CCF 进行认证, 然后 CCF 可以使用基于 GBA 的认证机制、基于 AKMA 的认证机制或基于证书的认证机制来认证资源所有者。CCF 还可以在认证后为资源所有者生成证书和 OAuth 2.0 令牌。对于第一实体为 Authorization Function 的情况, 资源所有者可以通过证书对授权功能进行认证。然后 Authorization Function 可以使用 TLS-PSK、基于 OAuth 令牌的认证机制、基于 GBA 的认证机制、基于 AKMA 的认证机制或基于证书的认证机制来认证资源所有者, 其中证书可以由 CCF 分配。

S606, 在认证通过的情况下, 建立 API 调用者与第一实体之间的第三连接。

其中, 第三连接为用于传输授权码的安全连接。可以理解的是, 该安全连接是在相互认证之后建立的。该安全连接可以是 TLS 连接, 即, 基于 TLS 协议建立的安全连接。

S607, 向第一实体发送授权码。

在本公开的实施例中, 第一实体可以接收 API 调用者发送的授权码, 以用于兑换令牌。

S608, 接收第一实体基于授权码生成的令牌。

在本公开的实施例中, 第一实体可以通过如下方式生成并发送令牌给 API 调用者。

在一种示例中, 第一实体向 API 调用者发送访问令牌和/或刷新令牌。

在另一种示例中, 第一实体接收 API 调用者发送的刷新令牌, 基于刷新令牌向 API 调用者发送访问令牌。

换言之, 第一实体可以直接将刷新令牌/访问令牌发送给 API 调用者, 或者, API 调用者可以将刷新令牌发送给第一实体以获取访问令牌。

在本公开的实施例中，访问令牌包括 CCF 身份标识（如 NF instance ID、NF ID）、Authorization Function 身份标识（如 NF instance ID、NF ID）、第二实体身份标识（如 NF instance ID、NF ID）、服务标识符、API 调用者身份标识（例如，GPSI、IMSI、应用层 ID）、资源所有者身份标识（例如，GPSI、IMSI、应用层 ID）、资源标识（例如，位置）、过期时间中的至少一项。其中，第二实体为 AEF。

在之后的步骤中，API 调用者与第二实体进行交互：

S609，与第二实体进行相互认证。

在本公开的实施例中，API 调用者和 AEF 可以基于 TLS-PSK、基于 OAuth 令牌的认证机制、基于 GBA 的认证机制、基于 AKMA 的认证机制或基于证书的认证机制进行相互认证。

S610，在认证通过的情况下，建立 API 调用者与第二实体之间的第四连接。

可以理解的是，第四连接为 API 调用者和 AEF 之间的安全连接，该安全连接是在相互认证之后建立的。该安全连接可以是 TLS 连接，即，基于 TLS 协议建立的安全连接。

S611，向第二实体发送服务调用请求。

在本公开的实施例中，API 调用者向 AEF 发送的服务调用请求中包括：API 调用者的身份标识、资源所有者的身份标识、需要调用的服务的标识、API 调用者需要访问的用户资源标识和访问令牌。

S612，接收第二实体发送的授权响应。

在本公开的实施例中，AEF 可以根据令牌对请求进行授权，并向 API 调用者发送响应。

应当理解的是，上述步骤 S601、S602、S605、S606、S609、S610 为可选步骤。换言之，本公开中的请求和响应消息可以在没有身份认证及建立安全连接的条件上传递。

综上，根据本公开提供的资源调用方法，API 调用者可以与资源所有者、第一实体、第二实体进行双向认证，API 调用者可以向资源所有者发送资源授权请求和/或 API 授权请求，资源授权请求用于请求、设置或修改资源所有者的资源，接收资源所有者发送的授权码，并向第一实体发送授权码，并接收第一实体基于授权码生成的令牌。本公开提供的方案实现了在 API 调用场景中，UE 能够授权 API 调用者请求 UE 的资源，避免在授权过程中资源所有者对数据的篡改。

图 7 示出了根据本公开实施例的一种资源调用方法的交互示意图。该方法可由一种通信系统执行，该通信系统至少包括资源所有者、第一实体、API 调用者。如图 7 所示，且该方法可以包括以下步骤。

S701，第一实体向资源所有者发送资源授权请求和/或 API 授权请求。

S702，资源所有者向第一实体发送授权码请求。

S703，第一实体向资源所有者发送授权码。

S704，资源所有者向 API 调用者发送授权码。

S705，API 调用者向第一实体发送授权码。

S706，第一实体根据授权码生成令牌。

S707，第一实体将令牌发送给 API 调用者。

上述步骤的原理与图 1 至 6 所示实施例的原理相同，在此不再赘述。

综上，根据本公开提供的资源调用方法，通过 API 调用者、资源所有者、第一实体之间的交互，实现了在 API 调用场景中，UE 能够授权 API 调用者请求 UE 的资源，避免在授权过程中资源所有者对数据的篡改。

图 8 示出了根据本公开实施例的一种资源调用方法的交互示意图。该方法可由一种通信系统执行，基于图 7 所示的实施例，该通信系统至少包括资源所有者、第一实体、API 调用者、第二实体。如图 8 所示，该方法可以包括以下步骤。

S801，API 调用者与资源所有者之间进行相互认证，在认证通过的情况下，建立资源所有者与 API 调用者之间的第一连接。

S802，API 调用者向资源所有者发送资源授权请求和/或 API 授权请求。

S803，第一实体与资源所有者之间进行相互认证，在认证通过的情况下，建立资源所有者与第一实体之间的第二连接。

S804，资源所有者向第一实体发送授权码请求。

S805，第一实体生成授权码。

S806，第一实体将授权码发送给资源所有者。

S807，资源所有者将授权码发送给 API 调用者。

S808，API 调用者与第一实体之间进行相互认证，在认证通过的情况下，建立 API 调用者和第一实体之间的第三连接。

S809, API 调用者向第一实体发送授权码。

S810, 第一实体根据授权码生成令牌。

S811, 第一实体将令牌发送至 API 调用者。

S812, API 调用者与第二实体之间进行相互认证, 在认证通过的情况下, 建立 API 调用者和第二实体之间的第四连接。

S813, API 调用者向第二实体发送服务调用请求。

S814, 第二实体根据令牌对请求进行授权。

S815, 第二实体向 API 调用者发送授权响应。

上述步骤的原理与图 1 至 7 所示实施例的原理相同, 在此不再赘述。

应当理解的是, 上述步骤 S801、S803、S808 以及 S812 为可选步骤。换言之, 本公开中的请求和响应消息可以在没有身份认证及建立安全连接的条件下来传递。

综上, 根据本公开提供的资源调用方法, 通过 API 调用者、资源所有者、第一实体、第二实体之间的交互, 实现了在 API 调用场景中, UE 能够授权 API 调用者请求 UE 的资源, 避免在授权过程中资源所有者对数据的篡改。

上述本申请提供的实施例中, 分别从资源所有者、API 调用者、第一实体的角度对本申请实施例提供的方法进行了介绍。为了实现上述本申请实施例提供的方法中的各功能, 资源所有者和 API 调用者以及第一实体可以包括硬件结构、软件模块, 以硬件结构、软件模块、或硬件结构加软件模块的形式来实现上述各功能。上述各功能中的某个功能可以以硬件结构、软件模块、或者硬件结构加软件模块的方式来执行。

与上述几种实施例提供的资源调用方法相对应, 本公开还提供一种资源调用装置, 由于本公开实施例提供的资源调用装置与上述几种实施例提供的资源调用方法相对应, 因此资源调用方法的实施方式也适用于本实施例提供的资源调用装置, 在本实施例中不再详细描述。

图 9 为本公开实施例提供的一种资源调用装置 900 的结构示意图, 该资源调用装置 900 配置于资源所有者。

如图 9 所示, 装置 900 包括收发模块 910, 收发模块 910 用于: 接收应用程序接口 API 调用者发送的资源授权请求和/或 API 授权请求, 资源授权请求用于请求、设置或修改资源所有者的资源; 向第一实体发送授权码请求, 授权码请求用于请求授权码; 将从第一实体接收的授权码发送给 API 调用者。

根据本公开提供的资源调用装置, 资源所有者可以接收应用程序接口 API 调用者发送的资源授权请求和/或 API 授权请求, 资源授权请求用于请求、设置或修改资源所有者的资源, 并向第一实体发送授权码请求, 其中授权码请求用于请求授权码, 资源所有者可以将第一实体接收的授权码发送给 API 调用者。本公开提供的方案实现了在 API 调用场景中, UE 能够授权 API 调用者请求 UE 的资源, 避免在授权过程中资源所有者对数据的篡改。

在一些实施例中, 如图 10 所示, 该装置 900 还包括: 认证模块 920, 用于与 API 调用者进行相互认证; 在认证通过的情况下, 建立资源所有者与 API 调用者之间的第一连接。

在一些实施例中, 认证模块 920 还用于执行以下至少一项: 当 API 调用者为用户设备 UE 时, 基于证书与 API 调用者进行相互认证; 当 API 调用者为应用功能 AF 时, 通过基于 GBA 的认证机制、基于 AKMA 的认证机制或基于证书的认证机制进行相互认证。

在一些实施例中, 收发模块 910 还用于: 当 API 调用者已经获得服务的授权, 接收 API 调用者发送的资源授权请求; 当 API 调用者未获得服务的授权, 接收 API 调用者发送的资源授权请求和 API 授权请求, 其中, 资源授权请求中包括 API 调用者的标识、资源所有者的标识、目标资源标识中的至少一项, API 授权请求中包括服务标识符。

在一些实施例中, 认证模块 920 还用于: 与第一实体进行相互认证; 在认证通过的情况下, 建立资源所有者与第一实体之间的第二连接; 其中, 第二连接为用于传输授权码请求和响应的安全连接。

在一些实施例中, 认证模块 920 还用于: 基于以下认证机制中的至少一项进行相互认证: 基于证书的认证机制; 基于 GBA 的认证机制; 基于 AKMA 的认证机制; TLS-PSK; 基于 OAuth 令牌的认证机制。

在一些实施例中, 收发模块 910 还用于: 实时同意资源授权请求以向第一实体发送授权码请求; 根据资源所有者的本地策略异步同意资源授权请求以向第一实体发送授权码请求; 向第一实体发送本地策略和/或授权码请求, 本地策略用于辅助第一实体异步同意资源授权请求。

在一些实施例中, 收发模块 910 还用于: 当资源授权请求获得授权, 且当 API 调用者已经获得服务的授权时, 接收第一实体发送的授权码。

在一些实施例中，资源所有者为用户设备 UE，资源为 UE 的服务质量和/或位置信息。

综上，根据本公开提供的资源调用装置，资源所有者可以与 API 调用者、第一实体进行双向认证，资源所有者可以接收应用程序接口 API 调用者发送的资源授权请求和/或 API 授权请求，并向第一实体发送授权码请求，其中授权码请求用于请求授权码，资源所有者可以将从第一实体接收的授权码发送给 API 调用者。本公开提供的方案实现了在 API 调用场景中，UE 能够授权 API 调用者请求 UE 的资源，避免在授权过程中资源所有者对数据的篡改。

图 11 为本公开实施例提供的一种资源调用装置 1100 的结构示意图，该资源调用装置 1100 配置于第一实体。

如图 11 所示，装置 1100 包括收发模块 1110，收发模块 1110 用于：接收资源所有者发送的授权码请求，授权码请求用于请求授权码；向资源所有者发送授权码；接收 API 调用者发送的授权码；根据授权码生成令牌，并将令牌发送给 API 调用者。

根据本公开提供的资源调用装置，第一实体可以接收资源所有者发送的授权码请求，并响应该请求生成授权码并发送给资源所有者，接收 API 调用者发送的授权码，并根据该授权码生成令牌提供给 API 调用者。本公开提供的方案实现了在 API 调用场景中，UE 能够授权 API 调用者请求 UE 的资源，避免在授权过程中资源所有者对数据的篡改。

在一些实施例中，如图 12 所示，该装置 1100 还包括：认证模块 1120，用于与资源所有者进行相互认证；在认证通过的情况下，建立资源所有者与第一实体之间的第二连接，其中，第二连接为用于传输授权码请求和响应的安全连接。

在一些实施例中，认证模块 1120 还用于：基于以下认证机制中的至少一项进行相互认证：基于证书的认证机制；基于 GBA 的认证机制；基于 AKMA 的认证机制；TLS-PSK；基于 OAuth 令牌的认证机制。

在一些实施例中，收发模块 1110 还用于：根据资源所有者对资源授权请求的实时同意，接收授权码请求；根据资源所有者对资源授权请求的异步同意，接收授权码请求；接收资源所有者发送的本地策略和/或授权码请求，异步同意资源授权请求。

在一些实施例中，收发模块 1110 还用于：当资源授权请求获得同意，且当 API 调用者已经获得服务的授权时，生成授权码。

在一些实施例中，如图 13 所示，该装置 1100 还包括：授权模块 1130，用于当资源授权请求获得同意，但 API 调用者未获得服务的授权时，根据预设策略，判断是否同意 API 调用者的服务授权请求；当同意 API 调用者的服务授权请求时，生成授权码。

在一些实施例中，认证模块 1120 还用于：与 API 调用者进行相互认证；在认证通过的情况下，建立 API 调用者与第一实体之间的第三连接，其中，第三连接为用于传输授权码的安全连接。

在一些实施例中，认证模块 1120 还用于：基于以下认证机制中的至少一项进行相互认证：基于证书的认证机制；基于 GBA 的认证机制；基于 AKMA 的认证机制；TLS-PSK；基于 OAuth 令牌的认证机制。

在一些实施例中，收发模块 1110 还用于执行以下至少一项：向 API 调用者发送访问令牌和/或刷新令牌；接收 API 调用者发送的刷新令牌，基于刷新令牌向 API 调用者发送访问令牌。

在一些实施例中，第一实体为 CAPIF 核心功能或者授权功能。

根据本公开提供的资源调用装置，第一实体可以与资源所有者、API 调用者进行双向认证，第一实体可以接收资源所有者发送的授权码请求，并响应该请求生成授权码并发送给资源所有者，接收 API 调用者发送的授权码，并根据该授权码生成令牌提供给 API 调用者。本公开提供的方案实现了在 API 调用场景中，UE 能够授权 API 调用者请求 UE 的资源，避免在授权过程中资源所有者对数据的篡改。

图 14 为本公开实施例提供的一种资源调用装置 1400 的结构示意图，该资源调用装置 1400 配置于 API 调用者。

如图 14 所示，装置 1400 包括收发模块 1410，收发模块 1410 用于：向资源所有者发送资源授权请求和/或 API 授权请求，资源授权请求用于请求、设置或修改资源所有者的资源；接收资源所有者发送的授权码，并向第一实体发送授权码；接收第一实体基于授权码生成的令牌。

根据本公开提供的资源调用装置，API 调用者可以向资源所有者发送资源授权请求和/或 API 授权请求，资源授权请求用于请求、设置或修改资源所有者的资源，接收资源所有者发送的授权码，并向第一实体发送授权码，并接收第一实体基于授权码生成的令牌。本公开提供的方案实现了在 API 调用场景中，UE 能够授权 API 调用者请求 UE 的资源，避免在授权过程中资源所有者对数据的篡改。

在一些实施例中，如图 15 所示，该装置 1400 还包括：认证模块 1420，用于与资源所有者进行相互认证；在认证通过的情况下，建立资源所有者与 API 调用者之间的第一连接，其中，第一连接为用于传输资源授权请求和/或 API 授权请求的安全连接。

在一些实施例中，认证模块 1420 还用于执行以下至少一项：当 API 调用者为用户设备 UE 时，基于证书与资源所有者进行相互认证；当 API 调用者为应用功能 AF 时，通过基于 GBA 的认证机制、基于 AKMA 的认证机制或基于证书的认证机制与资源所有者进行相互认证。

在一些实施例中，收发模块 1410 还用于：当 API 调用者已经获得服务的授权时，向资源所有者发送资源授权请求；当 API 调用者未获得服务的授权时，向资源所有者发送资源授权请求和 API 授权请求，其中，资源授权请求中包括 API 调用者的标识、资源所有者的标识、目标资源标识中的至少一项，API 授权请求中包括服务标识符。

在一些实施例中，认证模块 1420 还用于：与第一实体进行相互认证；在认证通过的情况下，建立 API 调用者与第一实体之间的第三连接；其中，第三连接为用于传输授权码的安全连接。

在一些实施例中，收发模块 1410 还用于执行以下至少一项：接收第一实体发送的访问令牌和/或刷新令牌；向第一实体发送刷新令牌，并接收第一实体基于刷新令牌发送的访问令牌。

在一些实施例中，API 调用者为用户设备 UE 或者应用功能 AF，资源为资源所有者的服务质量和/或位置信息。

根据本公开提供的资源调用装置，API 调用者可以与资源所有者、第一实体、第二实体进行双向认证，API 调用者可以向资源所有者发送资源授权请求和/或 API 授权请求，资源授权请求用于请求、设置或修改资源所有者的资源，接收资源所有者发送的授权码，并向第一实体发送授权码，并接收第一实体基于授权码生成的令牌。本公开提供的方案实现了在 API 调用场景中，UE 能够授权 API 调用者请求 UE 的资源，避免在授权过程中资源所有者对数据的篡改。

本公开实施例还提供一种通信系统，该系统包括资源所有者、API 调用者、第一实体，其中：该系统包括前述图 9-15 实施例所示的资源调用装置，用于执行如图 1-8 实施例所示的资源调用方法。

请参见图 16，图 16 是本申请实施例提供的一种通信装置 1600 的结构示意图。通信装置 1600 可以是网络设备，也可以是用户设备，也可以是支持网络设备实现上述方法的芯片、芯片系统、或处理器等，还可以是支持用户设备实现上述方法的芯片、芯片系统、或处理器等。该装置可用于实现上述方法实施例中描述的方法，具体可以参见上述方法实施例中的说明。

通信装置 1600 可以包括一个或多个处理器 1601。处理器 1601 可以是通用处理器或者专用处理器等。例如可以是基带处理器或中央处理器。基带处理器可以用于对通信协议以及通信数据进行处理，中央处理器可以用于对通信装置（如，基站、基带芯片，终端设备、终端设备芯片，DU 或 CU 等）进行控制，执行计算机程序，处理计算机程序的数据。

可选的，通信装置 1600 中还可以包括一个或多个存储器 1602，其上可以存有计算机程序 1604，处理器 1601 执行计算机程序 1604，以使得通信装置 1600 执行上述方法实施例中描述的方法。可选的，存储器 1402 中还可以存储有数据。通信装置 1600 和存储器 1602 可以单独设置，也可以集成在一起。

可选的，通信装置 1600 还可以包括收发器 1605、天线 1606。收发器 1605 可以称为收发单元、收发机、或收发电路等，用于实现收发功能。收发器 1605 可以包括接收器和发送器，接收器可以称为接收机或接收电路等，用于实现接收功能；发送器可以称为发送机或发送电路等，用于实现发送功能。

可选的，通信装置 1600 中还可以包括一个或多个接口电路 1607。接口电路 1607 用于接收代码指令并传输至处理器 1601。处理器 1601 运行代码指令以使通信装置 1600 执行上述方法实施例中描述的方法。

在一种实现方式中，处理器 1601 中可以包括用于实现接收和发送功能的收发器。例如该收发器可以是收发电路，或者是接口，或者是接口电路。用于实现接收和发送功能的收发电路、接口或接口电路可以是分开的，也可以集成在一起。上述收发电路、接口或接口电路可以用于代码/数据的读写，或者，上述收发电路、接口或接口电路可以用于信号的传输或传递。

在一种实现方式中，处理器 1601 可以存有计算机程序 1603，计算机程序 1603 在处理器 1601 上运行，可使得通信装置 1600 执行上述方法实施例中描述的方法。计算机程序 1603 可能固化在处理器 1601 中，该种情况下，处理器 1601 可能由硬件实现。

在一种实现方式中，通信装置 1600 可以包括电路，电路可以实现前述方法实施例中发送或接收或者通信的功能。本申请中描述的处理器和收发器可实现在集成电路（integrated circuit, IC）、模拟 IC、射频集成电路 RFIC、混合信号 IC、专用集成电路（application specific integrated circuit, ASIC）、印刷

电路板 (printed circuit board, PCB)、电子设备等上。该处理器和收发器也可以用各种 IC 工艺技术来制造,例如互补金属氧化物半导体 (complementary metal oxide semiconductor, CMOS)、N 型金属氧化物半导体 (nMetal-oxide-semiconductor, NMOS)、P 型金属氧化物半导体 (positive channel metal oxide semiconductor, PMOS)、双极结型晶体管 (bipolar junction transistor, BJT)、双极 CMOS (BiCMOS)、硅锗 (SiGe)、砷化镓 (GaAs) 等。

以上实施例描述中的通信装置可以是网络设备或者用户设备,但本申请中描述的通信装置的范围并不限于此,而且通信装置的结构可以不受图 16 的限制。通信装置可以是独立的设备或者可以是较大设备的一部分。例如通信装置可以是:

- (1) 独立的集成电路 IC, 或芯片, 或, 芯片系统或子系统;
- (2) 具有一个或多个 IC 的集合, 可选的, 该 IC 集合也可以包括用于存储数据, 计算机程序的存储部件;
- (3) ASIC, 例如调制解调器 (Modem);
- (4) 可嵌入在其他设备内的模块;
- (5) 接收机、终端设备、智能终端设备、蜂窝电话、无线设备、手持机、移动单元、车载设备、网络设备、云设备、人工智能设备等等;
- (6) 其他等等。

对于通信装置可以是芯片或芯片系统的情况,可参见图 17 所示的芯片的结构示意图。图 17 所示的芯片包括处理器 1701 和接口 1702。其中,处理器 1701 的数量可以是一个或多个,接口 1702 的数量可以是多个。

可选的,芯片还包括存储器 1703,存储器 1703 用于存储必要的计算机程序和数据。

本领域技术人员还可以了解到本申请实施例列出的各种说明性逻辑块 (illustrative logical block) 和步骤 (step) 可以通过电子硬件、电脑软件,或两者的结合进行实现。这样的功能是通过硬件还是软件来实现取决于特定的应用和整个系统的设计要求。本领域技术人员可以对于每种特定的应用,可以使用各种方法实现的功能,但这种实现不应被理解为超出本申请实施例保护的范围。

本申请还提供一种可读存储介质,其上存储有指令,该指令被计算机执行时实现上述任一方法实施例的功能。

本申请还提供一种计算机程序产品,该计算机程序产品被计算机执行时实现上述任一方法实施例的功能。

在上述实施例中,可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时,可以全部或部分地以计算机程序产品的形式实现。计算机程序产品包括一个或多个计算机程序。在计算机上加载和执行计算机程序时,全部或部分地产生按照本申请实施例的流程或功能。计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。计算机程序可以存储在计算机可读存储介质中,或者从一个计算机可读存储介质向另一个计算机可读存储介质传输,例如,计算机程序可以从一个网站站点、计算机、服务器或数据中心通过有线 (例如同轴电缆、光纤、数字用户线 (digital subscriber line, DSL)) 或无线 (例如红外、无线、微波等) 方式向另一个网站站点、计算机、服务器或数据中心进行传输。计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。可用介质可以是磁性介质 (例如,软盘、硬盘、磁带)、光介质 (例如,高密度数字视频光盘 (digital video disc, DVD))、或者半导体介质 (例如,固态硬盘 (solid state disk, SSD)) 等。

本领域普通技术人员可以理解:本申请中涉及的第一、第二等各种数字编号仅为描述方便进行的区分,并不用来限制本申请实施例的范围,也表示先后顺序。

本申请中的至少一个还可以描述为一个或多个,多个可以是两个、三个、四个或者更多个,本申请不做限制。在本申请实施例中,对于一种技术特征,通过“第一”、“第二”、“第三”、“A”、“B”、“C”和“D”等区分该种技术特征中的技术特征,该“第一”、“第二”、“第三”、“A”、“B”、“C”和“D”描述的技术特征间无先后顺序或者大小顺序。

如本文使用的,术语“机器可读介质”和“计算机可读介质”指的是用于将机器指令和/或数据提供给可编程处理器的任何计算机程序产品、设备、和/或装置 (例如,磁盘、光盘、存储器、可编程逻辑装置 (PLD)),包括,接收作为机器可读信号的机器指令的机器可读介质。术语“机器可读信号”指的是用于将机器指令和/或数据提供给可编程处理器的任何信号。

可以将此处描述的系统和技术实施在包括后台部件的计算系统 (例如,作为数据服务器)、或者包括中间件部件的计算系统 (例如,应用服务器)、或者包括前端部件的计算系统 (例如,具有图形用户

界面或者网络浏览器的用户计算机,用户可以通过该图形用户界面或者该网络浏览器来与此处描述的系统和技术的实施方式交互)、或者包括这种后台部件、中间件部件、或者前端部件的任何组合的计算系统中。可以通过任何形式或者介质的数字数据通信(例如,通信网络)来将系统的部件相互连接。通信网络的示例包括:局域网(LAN)、广域网(WAN)和互联网。

计算机系统可以包括客户端和服务端。客户端和服务端一般远离彼此并且通常通过通信网络进行交互。通过在相应的计算机上运行并且彼此具有客户端-服务端关系的计算机程序来产生客户端和服务端的关系。

应该理解,可以使用上面所示的各种形式的流程,重新排序、增加或删除步骤。例如,本公开中记载的各步骤可以并行地执行也可以顺序地执行也可以不同的次序执行,只要能够实现本公开公开的技术方案所期望的结果,本文在此不进行限制。

此外,应该理解,本申请的各种实施例可以单独实施,也可以在方案允许的情况下与其他实施例组合实施。

本领域普通技术人员可以意识到,结合本文中所公开的实施例描述的各示例的单元及算法步骤,能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行,取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能,但是这种实现不应认为超出本申请的范围。

所属领域的技术人员可以清楚地了解到,为描述的方便和简洁,上述描述的系统、装置和单元的具体工作过程,可以参考前述方法实施例中的对应过程,在此不再赘述。

以上,仅为本申请的具体实施方式,但本申请的保护范围并不局限于此,任何熟悉本技术领域的技术人员在本申请揭露的技术范围内,可轻易想到变化或替换,都应涵盖在本申请的保护范围之内。因此,本申请的保护范围应以权利要求的保护范围为准。

权利要求书

- 1、一种资源调用方法，其特征在于，所述方法由资源所有者执行，所述方法包括：
接收应用程序接口 API 调用者发送的资源授权请求和/或 API 授权请求，其中，所述资源授权请求用于请求、设置或修改所述资源所有者的资源；
向第一实体发送授权码请求，所述授权码请求用于请求授权码；
将从所述第一实体接收到的所述授权码发送给所述 API 调用者。
- 2、根据权利要求 1 所述的方法，其特征在于，所述方法还包括：
与所述 API 调用者进行相互认证；以及
在认证通过的情况下，建立所述资源所有者与所述 API 调用者之间的第一连接，
其中，所述第一连接为用于传输所述资源授权请求和/或所述 API 授权请求的安全连接。
- 3、根据权利要求 2 所述的方法，其特征在于，所述与所述 API 调用者进行相互认证包括以下至少一项：
当所述 API 调用者为用户设备 UE 时，基于证书与所述 API 调用者进行相互认证；
当所述 API 调用者为应用功能 AF 时，通过基于 GBA 的认证机制、基于 AKMA 的认证机制或基于证书的认证机制进行相互认证。
- 4、根据权利要求 1 至 3 中任一项所述的方法，其特征在于，所述接收所述 API 调用者发送的资源授权请求和/或 API 授权请求包括：
当所述 API 调用者已经获得服务的授权时，接收所述 API 调用者发送的资源授权请求；
当所述 API 调用者未获得服务的授权时，接收所述 API 调用者发送的资源授权请求和 API 授权请求，
其中，所述资源授权请求中包括所述 API 调用者的标识、所述资源所有者的标识、目标资源标识中的至少一项，并且所述 API 授权请求中包括服务标识符。
- 5、根据权利要求 4 所述的方法，其特征在于，所述服务标识符包括以下至少一项：
服务名称标识符；
服务操作标识符；
操作语义标识符；
API 标识。
- 6、根据权利要求 1 至 5 中任一项所述的方法，其特征在于，所述方法还包括：
与所述第一实体进行相互认证；
在认证通过的情况下，建立所述资源所有者与所述第一实体之间的第二连接；
其中，所述第二连接为用于传输所述授权码请求和响应的安全连接。
- 7、根据权利要求 1 至 6 中任一项所述的方法，其特征在于，所述与第一实体进行相互认证包括：
基于以下认证机制中的至少一项进行相互认证：
基于证书的认证机制；
基于 GBA 的认证机制；
基于 AKMA 的认证机制；
TLS-PSK；
基于 OAuth 令牌的认证机制。
- 8、根据权利要求 1 至 7 中任一项所述的方法，其特征在于，所述向所述第一实体发送授权码请求包括以下至少一项：
实时同意所述资源授权请求以向所述第一实体发送授权码请求；
根据所述资源所有者的本地策略异步同意所述资源授权请求以向所述第一实体发送授权码请求；
向所述第一实体发送本地策略和/或所述授权码请求，所述本地策略用于辅助所述第一实体异步同意所述资源授权请求。
- 9、根据权利要求 1 至 8 中任一项所述的方法，其特征在于，所述方法还包括：
当所述资源授权请求获得授权且当所述 API 调用者已经获得服务的授权时，接收所述第一实体发送的授权码。
- 10、根据权利要求 1 至 9 中任一项所述的方法，其特征在于，所述资源所有者为用户设备 UE，所述资源为所述 UE 的服务质量和/或位置信息。
- 11、一种资源调用方法，其特征在于，所述方法由第一实体执行，所述方法包括：
接收资源所有者发送的授权码请求，所述授权码请求用于请求授权码；

- 向所述资源所有者发送授权码；
接收 API 调用者发送的授权码；
根据所述授权码生成令牌，并将所述令牌发送给所述 API 调用者。
- 12、根据权利要求 11 所述的方法，其特征在于，所述方法还包括：
与所述资源所有者进行相互认证；
在认证通过的情况下，建立所述资源所有者与所述第一实体之间的第二连接，
其中，所述第二连接为用于传输所述授权码请求和响应的安全连接。
- 13、根据权利要求 12 所述的方法，其特征在于，所述与所述资源所有者进行相互认证包括：
基于以下认证机制中的至少一项进行相互认证：
基于证书的认证机制；
基于 GBA 的认证机制；
基于 AKMA 的认证机制；
TLS-PSK；
基于 OAuth 令牌的认证机制。
- 14、根据权利要求 11 至 13 中任一项所述的方法，其特征在于，所述接收所述资源所有者发送的授权码请求包括以下至少一项：
根据所述资源所有者对资源授权请求的实时同意，接收所述授权码请求；
根据所述资源所有者对所述资源授权请求的异步同意，接收所述授权码请求；
接收所述资源所有者发送的本地策略和/或所述授权码请求，异步同意所述资源授权请求。
- 15、根据权利要求 10 至 14 中任一项所述的方法，其特征在于，所述接收所述资源所有者发送的授权码请求还包括：
当所述资源授权请求获得同意，且当所述 API 调用者已经获得服务的授权时，生成所述授权码。
- 16、根据权利要求 15 所述的方法，其特征在于，所述当所述资源授权请求获得同意，且当所述 API 调用者已经获得服务的授权时，生成所述授权码包括：
当所述资源授权请求获得同意，但所述 API 调用者未获得服务的授权时，根据预设策略，判断是否同意所述 API 调用者的服务授权请求；
当同意所述 API 调用者的服务授权请求时，生成所述授权码。
- 17、根据权利要求 11 至 16 中任一项所述的方法，其特征在于，所述方法还包括：
与所述 API 调用者进行相互认证；
在认证通过的情况下，建立所述 API 调用者与所述第一实体之间的第三连接，
其中，所述第三连接为用于传输授权码的安全连接。
- 18、根据权利要求 17 所述的方法，其特征在于，所述与所述 API 调用者进行相互认证包括：
基于以下认证机制中的至少一项进行相互认证：
基于证书的认证机制；
基于 GBA 的认证机制；
基于 AKMA 的认证机制；
TLS-PSK；
基于 OAuth 令牌的认证机制。
- 19、根据权利要求 11 至 18 中任一项所述的方法，其特征在于，所述根据所述授权码生成令牌，并将所述令牌发送给所述 API 调用者包括以下中的至少一项：
向所述 API 调用者发送访问令牌和/或刷新令牌；
接收所述 API 调用者发送的刷新令牌，基于所述刷新令牌向所述 API 调用者发送访问令牌。
- 20、根据权利要求 11 至 19 所述的方法，其特征在于，所述第一实体为 CAPIF 核心功能或者授权功能。
- 21、一种资源调用方法，其特征在于，所述方法由 API 调用者执行，所述方法包括：
向资源所有者发送资源授权请求和/或 API 授权请求，所述资源授权请求用于请求、设置或修改所述资源所有者的资源；
接收所述资源所有者发送的授权码，并向第一实体发送授权码；
接收所述第一实体基于所述授权码生成的令牌。
- 22、根据权利要求 21 所述的方法，其特征在于，所述方法还包括：
与所述资源所有者进行相互认证；
在认证通过的情况下，建立所述资源所有者与所述 API 调用者之间的第一连接，

其中，所述第一连接为用于传输所述资源授权请求和/或所述 API 授权请求的安全连接。

23、根据权利要求 22 所述的方法，其特征在于，所述与所述资源所有者进行相互认证包括以下中的至少一项：

当所述 API 调用者为用户设备 UE 时，基于证书与所述资源所有者进行相互认证；

当所述 API 调用者为应用功能 AF 时，通过基于 GBA 的认证机制、基于 AKMA 的认证机制或基于证书的认证机制与所述资源所有者进行相互认证。

24、根据权利要求 22 或 23 所述的方法，其特征在于，所述向所述资源所有者发送资源授权请求和/或 API 授权请求包括：

当所述 API 调用者已经获得服务的授权时，向所述资源所有者发送资源授权请求；

当所述 API 调用者未获得服务的授权时，向所述资源所有者发送资源授权请求和 API 授权请求，

其中，所述资源授权请求中包括所述 API 调用者的标识、所述资源所有者的标识、目标资源标识中的至少一项，所述 API 授权请求中包括服务标识符。

25、根据权利要求 24 所述的方法，其特征在于，当所述 API 调用者已经获得服务的授权，且所述 API 调用者向所述资源所有者发送的资源授权请求获得同意，所述第一实体基于所述授权码生成的令牌仅包括资源相关的授权信息。

26、根据权利要求 21 至 25 中任一项所述的方法，其特征在于，所述方法还包括：

与所述第一实体进行相互认证；

在认证通过的情况下，建立所述 API 调用者与所述第一实体之间的第三连接；

其中，所述第三连接为用于传输授权码的安全连接。

27、根据权利要求 21 至 26 中任一项所述的方法，其特征在于，所述接收所述第一实体基于所述授权码生成的令牌包括以下中的至少一项：

接收所述第一实体发送的访问令牌和/或刷新令牌；

向所述第一实体发送刷新令牌，并接收所述第一实体基于所述刷新令牌发送的访问令牌。

28、根据权利要求 21 至 27 中任一项所述的方法，其特征在于，所述 API 调用者为用户设备 UE 或者应用功能 AF，所述资源为所述资源所有者的服务质量和/或位置信息。

29、一种资源调用装置，其特征在于，所述装置配置于资源所有者，所述装置包括收发模块，所述收发模块用于：

接收应用程序接口 API 调用者发送的资源授权请求和/或 API 授权请求，所述资源授权请求用于请求、设置或修改所述资源所有者的资源；

向第一实体发送授权码请求，所述授权码请求用于请求授权码；

将从所述第一实体接收的所述授权码发送给所述 API 调用者。

30、一种资源调用装置，其特征在于，所述装置配置于第一实体，所述装置包括收发模块，所述收发模块用于：

接收资源所有者发送的授权码请求，所述授权码请求用于请求授权码；

向所述资源所有者发送授权码；

接收 API 调用者发送的授权码；

根据所述授权码生成令牌，并将所述令牌发送给所述 API 调用者。

31、一种资源调用装置，其特征在于，所述装置配置于 API 调用者，所述装置包括收发模块，所述收发模块用于：

向资源所有者发送资源授权请求和/或 API 授权请求，所述资源授权请求用于请求、设置或修改所述资源所有者的资源；

接收所述资源所有者发送的授权码，并向第一实体发送授权码；

接收所述第一实体基于所述授权码生成的令牌。

32、一种通信设备，其中，包括：收发器；存储器；处理器，分别与所述收发器及所述存储器连接，配置为通过执行所述存储器上的计算机可执行指令，控制所述收发器的无线信号收发，并能够实现权利要求 1-28 中任一项所述的方法。

33、一种计算机存储介质，其中，所述计算机存储介质存储有计算机可执行指令；所述计算机可执行指令被处理器执行后，能够实现权利要求 1-28 中任一项所述的方法。

34、一种通信系统，其特征在于，包括资源所有者、API 调用者、第一实体，其中：

所述资源所有者被配置为执行如权利要求 1-9 中任一项所述的方法；

所述第一实体被配置为执行如权利要求 10-19 中任一项所述的方法；

所述 API 调用者被配置为执行如权利要求 20-28 中任一项所述的方法。