

认证方法及通信装置

5 本申请要求于 2021 年 01 月 22 日提交国家知识产权局、申请号为 202110090637.4、申请名称为“认证方法及通信装置”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

本申请涉及通信技术领域，尤其涉及一种认证方法及通信装置。

背景技术

10 目前，互联网协议多媒体子系统（internet protocol multimedia subsystem，IMS）通常采用会话发起协议（session initiation protocol，SIP）摘要（digest）认证方式来认证终端设备。服务呼叫会话控制功能（serving call session control function，S-CSCF）网元为终端设备指示安全算法为消息摘要第五版（message digest 5，MD5）算法。终端设备采用 MD5 算法进行计算，以得到认证响应。之后，终端设备向 S-CSCF 网元发送认证响应，以使 S-CSCF 网元基于该认证响应对终端设备进行认证。由于 MD5 算法是不安全的算法，所以，
15 一种方案是考虑让部分终端设备支持新的安全算法，如安全散列算法（secure hash algorithm，SHA）256 或 SHA512，通过 SHA256 或 SHA512 计算的认证响应完成认证。

显然，这种方案会导致如下情况：一些终端设备支持 SHA256 或 SHA512，因此需要使用 SHA256 或 SHA512 计算认证响应，而另一些终端设备不支持 SHA256 和 SHA512，仍沿用 MD5 算法计算认证响应。此种情况下，如何使得支持不同安全算法的终端设备完
20 成认证，是亟待解决的问题。

发明内容

本申请实施例提供一种认证方法及通信装置，能够认证支持不同安全算法的终端设备。

第一方面，本申请实施例提供一种认证方法，该方法的执行主体可以是终端设备，也可以是应用于终端设备中的芯片。下面以执行主体是终端设备为例进行描述。该方法包括：
25 终端设备向服务呼叫会话控制功能网元发送第一注册请求消息。其中，第一注册请求消息携带终端设备能够支持的安全算法的信息，安全算法包括以下至少一项：第一安全算法或第二安全算法。终端设备接收来自服务呼叫会话控制功能网元的认证挑战消息。其中，认证挑战消息包括第三安全算法的信息，第三安全算法为终端设备能够支持的安全算法中的一个。终端设备根据第三安全算法计算安全参数的哈希值，终端设备根据第三安全算法和
30 哈希值计算认证响应，终端设备向服务呼叫会话控制功能网元发送第二注册请求消息。其中，第二注册请求消息携带认证响应，认证响应用于认证终端设备。

如此，对于支持新的安全算法（如第一安全算法和/或第二安全算法）的终端设备而言，终端设备在第一注册请求消息中携带安全算法的信息，以向服务呼叫会话控制功能网元指示自身支持的安全算法，使得终端设备和服务呼叫会话控制功能网元基于相同的安全算法
35 计算认证响应，从而能够认证支持“第一安全算法和/或第二安全算法”的终端设备。并且，对于不支持新的安全算法（如第一安全算法和/或第二安全算法）的终端设备而言，终端设

备在第一注册请求消息中无需携带安全算法的信息。此种情况下，服务呼叫会话控制功能网元即可确定安全算法为 MD5 算法，从而使用 MD5 算法计算认证响应，以认证不支持新的安全算法（如第一安全算法和/或第二安全算法）的终端设备。

在一种可能的设计中，第一安全算法为安全散列算法 SHA256，第二安全算法为安全散列算法 SHA512。其中，SHA256 和 SHA512 是新的安全算法，所以，使用 SHA256 或 SHA512 认证终端设备的情况下，认证过程的安全性能得到了提升。

第二方面，本申请实施例提供一种认证方法，该方法的执行主体可以是服务呼叫会话控制功能网元，也可以是应用于服务呼叫会话控制功能网元中的芯片。下面以执行主体是服务呼叫会话控制功能网元为例进行描述。该方法包括：服务呼叫会话控制功能网元接收来自终端设备的第一注册请求消息。其中，第一注册请求消息包括终端设备能够支持的安全算法的信息，安全算法包括以下至少一项：第一安全算法或第二安全算法。服务呼叫会话控制功能网元向归属签约用户服务器发送认证向量请求消息。其中，认证向量请求消息包括终端设备能够支持的安全算法的信息。服务呼叫会话控制功能网元接收归属签约用户服务器返回的认证向量请求响应。其中，认证向量请求响应包括哈希值以及第三安全算法的信息，哈希值是基于第三安全算法计算得到的，第三安全算法为终端设备能够支持的安全算法中的一个。服务呼叫会话控制功能网元向终端设备发送认证挑战消息。其中，认证挑战消息包括第三安全算法的信息。服务呼叫会话控制功能网元接收来自终端设备的第二注册请求消息。其中，第二注册请求消息携带第一认证响应。服务呼叫会话控制功能网元根据第三安全算法和哈希值，计算第二认证响应。服务呼叫会话控制功能网元使用第二认证响应检验第一认证响应，得到终端设备的认证结果。

如此，对于支持新的安全算法（如第一安全算法和/或第二安全算法）的终端设备而言，服务呼叫会话控制功能网元能够通过第一注册请求消息获知终端设备支持的安全算法。然后，服务呼叫会话控制功能网元向归属签约用户服务器提供终端设备支持的安全算法的信息，以从归属签约用户服务器中获取第三安全算法的信息和第三安全算法计算的哈希值。然后，服务呼叫会话控制功能网元根据认证向量请求响应中的信息，确定第二认证响应，从而第二认证响应来校验第一认证响应，以认证支持“第一安全算法和/或第二安全算法”的终端设备。并且，对于不支持新的安全算法（如第一安全算法和/或第二安全算法）的终端设备而言，终端设备在第一注册请求消息中无需携带安全算法的信息，此种情况下，服务呼叫会话控制功能网元即可确定安全算法为 MD5 算法，从而使用 MD5 算法计算认证响应，以认证不支持新的安全算法（如第一安全算法和/或第二安全算法）的终端设备。

在一种可能的设计中，第一安全算法为安全散列算法 SHA256，第二安全算法为安全散列算法 SHA512。

第三方面，本申请实施例提供一种认证方法，该方法的执行主体可以是归属签约用户服务器，也可以是应用于归属签约用户服务器中的芯片。下面以执行主体是归属签约用户服务器为例进行描述。该方法包括：归属签约用户服务器接收来自服务呼叫会话控制功能网元的认证向量请求消息。其中，认证向量请求消息包括终端设备能够支持的安全算法的信息，安全算法包括以下至少一项：第一安全算法或第二安全算法。归属签约用户服务器根据第三安全算法计算安全参数的哈希值，其中，第三安全算法为终端设备能够支持的安全算法中的一个。归属签约用户服务器向服务呼叫会话控制功能网元返回认证向量请求响

应，其中，认证向量请求响应携带哈希值以及第三安全算法的信息。

也就是说，归属签约用户服务器通过认证向量请求消息获知终端设备支持的安全算法，然后，归属签约用户服务器从终端设备支持的安全算法中确定一个安全算法作为第三安全算法，通过认证向量请求响应向服务呼叫会话控制功能网元提供第三安全算法的信息和第三安全算法计算的哈希值，以使服务呼叫会话控制功能网元计算第二认证响应，从而能够认证支持“第一安全算法和/或第二安全算法”的终端设备。并且，对于不支持新的安全算法（如第一安全算法和/或第二安全算法）的终端设备而言，认证向量请求消息不携带终端设备支持的安全算法的信息，归属签约用户服务器仍向服务呼叫会话控制功能网元提供 MD5 算法计算的哈希值，以使服务呼叫会话控制功能网元使用 MD5 算法计算认证响应，以认证不支持新的安全算法（如第一安全算法和/或第二安全算法）的终端设备。

在一种可能的设计中，第一安全算法为安全散列算法 SHA256，第二安全算法为安全散列算法 SHA512。

第四方面，本申请实施例提供一种认证方法，该方法的执行主体可以是归属签约用户服务器，也可以是应用于归属签约用户服务器中的芯片。下面以执行主体是归属签约用户服务器为例进行描述。该方法包括：归属签约用户服务器接收来自服务呼叫会话控制功能网元的认证向量请求消息，归属签约用户服务器根据第一安全算法计算安全参数的第一哈希值，归属签约用户服务器根据第二安全算法计算安全参数的第二哈希值。归属签约用户服务器向服务呼叫会话控制功能网元返回认证向量请求响应。其中，认证向量请求响应携带第一哈希值和第二哈希值。

也就是说，归属签约用户服务器至少计算两种安全算法的哈希值，如归属签约用户服务器使用第一安全算法计算的第一哈希值，以及使用第二安全算法计算的第二哈希值。然后，归属签约用户服务器通过认证向量请求响应向服务呼叫会话控制功能网元提供上述安全算法确定的哈希值，以使服务呼叫会话控制功能网元获知终端设备支持的安全算法之后，能够从认证向量请求响应提供的多个哈希值中选择一个哈希值，计算第二认证响应，从而能够认证终端设备。

在一种可能的设计中，认证向量请求响应包括按照预设顺序携带的第一哈希值和第二哈希值，且预设顺序是基于第一安全算法的优先级和第二安全算法的优先级确定的，以使服务呼叫会话控制功能网元能够根据预设顺序区分第一哈希值和第二哈希值。

在一种可能的设计中，认证向量请求响应还携带第一安全算法的信息和第二安全算法的信息。其中，第一安全算法的信息与第一哈希值之间存在对应关系，第二安全算法的信息与第二哈希值之间存在对应关系，以使服务呼叫会话控制功能网元能够根据上述对应关系区分第一哈希值和第二哈希值。

在一种可能的设计中，第一安全算法为安全散列算法 SHA256 或 SHA512，第二安全算法为消息摘要 MD5 算法。也就是说，无论终端设备支持 SHA256、SHA512 或 MD5 算法中哪一安全算法，本申请实施例认证方法均能够认证该终端设备。

在一种可能的设计中，第一安全算法为 SHA256，第二安全算法为 SHA512。

在一种可能的设计中，本申请实施例认证方法还包括：归属签约用户服务器根据第四安全算法计算安全参数的第三哈希值。其中，认证向量请求响应还携带第三哈希值。第四安全算法为 MD5 算法。

也就是说，在第一安全算法为 SHA256，第二安全算法为 SHA512 的情况下，归属签约用户服务器还使用第四安全算法计算安全参数的第三哈希值，以向服务呼叫会话控制功能网元提供第四安全算法计算的哈希值。无论终端设备支持第一安全算法、第二安全算法和第四安全算法中的哪一安全算法，终端设备和服务呼叫会话控制功能网元均能够基于同一安全算法（即第三安全算法）计算认证响应，以认证终端设备。

第五方面，本申请实施例提供一种认证方法，该方法的执行主体可以是服务呼叫会话控制功能网元，也可以是应用于服务呼叫会话控制功能网元中的芯片。下面以执行主体是服务呼叫会话控制功能网元为例进行描述。该方法包括：服务呼叫会话控制功能网元接收来自终端设备的第一注册请求消息。服务呼叫会话控制功能网元向归属签约用户服务器发送认证向量请求消息。服务呼叫会话控制功能网元接收归属签约用户服务器返回的认证向量请求响应。其中，认证向量请求响应携带第一哈希值和第二哈希值，第一哈希值是基于第一安全算法计算的，第二哈希值是基于第二安全算法计算的。服务呼叫会话控制功能网元向终端设备发送认证挑战请求消息。其中，认证挑战请求消息携带第一安全算法的信息和第二安全算法的信息。服务呼叫会话控制功能网元接收来自终端设备的第二注册请求消息。其中，第二注册请求消息包括第一认证响应和第三安全算法的信息，第一认证响应是基于第三安全算法计算的，第三安全算法是第一安全算法或第二安全算法。服务呼叫会话控制功能网元从第一哈希值和第二哈希值中选择第三安全算法对应的哈希值。服务呼叫会话控制功能网元根据第三安全算法和第三安全算法对应的哈希值计算第二认证响应。服务呼叫会话控制功能网元使用第二认证响应校验第一认证响应，得到终端设备的认证结果。

也就是说，服务呼叫会话控制功能网元能够通过认证向量请求响应从归属签约用户服务器中获取至少两种安全算法计算的哈希值，如第一安全算法计算的第一哈希值，以及第二安全算法计算的第二哈希值。然后，服务呼叫会话控制功能网元通过认证挑战请求消息携带第一安全算法的信息和第二安全算法的信息，以使终端设备能够从认证挑战请求消息的安全算法中确定一个安全算法（即第三安全算法）。服务呼叫会话控制功能网元通过第二注册请求消息获知终端设备支持的一个安全算法，即第三安全算法，然后使用第三安全算法，从认证向量请求响应提供的哈希值中确定第三安全算法对应的哈希值，根据第三安全算法和第三安全算法对应的哈希值计算第二认证响应，从而能够认证终端设备。对于服务呼叫会话控制功能网元而言，服务呼叫会话控制功能网元无需识别终端设备是否支持新的安全算法（如 SHA256 和/或 SHA512），简化了处理过程。

在一种可能的设计中，认证向量请求响应包括按照预设顺序携带的第一哈希值和第二哈希值，且预设顺序是基于第一安全算法的优先级和第二安全算法的优先级确定的。服务呼叫会话控制功能网元从第一哈希值和第二哈希值中选择第三安全算法对应的哈希值，包括：服务呼叫会话控制功能网元根据预设顺序，从第一哈希值和第二哈希值中选择第三安全算法对应的哈希值。

也就是说，服务呼叫会话控制功能网元能够根据上述预设顺序，从认证向量请求响应提供的多个哈希值中，确定第三安全算法对应的哈希值，以基于第三安全算法对应的哈希值计算第二认证响应。

在一种可能的设计中，认证向量请求响应还携带第一安全算法的信息和第二安全算法的信息，其中，第一安全算法的信息与第一哈希值之间存在对应关系，第二安全算法的信

息与第二哈希值之间存在对应关系。服务呼叫会话控制功能网元从第一哈希值和第二哈希值中选择第三安全算法对应的哈希值，包括：服务呼叫会话控制功能网元根据对应关系，从第一哈希值和第二哈希值中选择第三安全算法对应的哈希值。

也就是说，服务呼叫会话控制功能网元能够根据上述对应关系，从认证向量请求响应提供的多个哈希值中，确定第三安全算法对应的哈希值，以基于第三安全算法对应的哈希值计算第二认证响应。

在一种可能的设计中，认证挑战请求消息包括按照预设顺序携带的第一安全算法的信息和第二安全算法的信息，且预设顺序是基于第一安全算法的优先级和第二安全算法的优先级确定的。在第一安全算法的优先级高于第二安全算法的优先级的情况下，第一安全算法的信息在第二安全算法的信息之前，以使终端设备优先读取到优先级较高的安全算法的信息。

在一种可能的设计中，第一安全算法为安全散列算法 SHA256 或 SHA512，第二安全算法为消息摘要 MD5 算法。

在一种可能的设计中，第一安全算法为 SHA256，第二安全算法为 SHA512。

在一种可能的设计中，认证向量请求响应还携带第三哈希值，第三哈希值是基于第四安全算法计算的。第四安全算法为 MD5 算法。服务呼叫会话控制功能网元从第一哈希值和第二哈希值中选择第三安全算法对应的哈希值，包括：服务呼叫会话控制功能网元从第一哈希值、第二哈希值和第三哈希值中选择第三安全算法对应的哈希值。其中，认证挑战请求消息还携带第四安全算法的信息，第三安全算法是第一安全算法、第二安全算法或第四安全算法。

也就是说，在第一安全算法为 SHA256，第二安全算法为 SHA512 的情况下，服务呼叫会话控制功能网元还能够通过认证挑战请求消息向终端设备提供第四安全算法的信息，以使终端设备从第一安全算法、第二安全算法和第四安全算法中确定一个安全算法，作为第三安全算法。服务呼叫会话控制功能网元还能够通过认证向量请求响应从归属签约用户服务器中获取第四安全算法计算的第三哈希值。在服务呼叫会话控制功能网元确定第三安全算法之后，从第一哈希值、第二哈希值和第三哈希值中确定第三安全算法对应的哈希值，以使用第三安全算法和第三安全算法对应的哈希值计算第二认证响应。也就是说，无论终端设备支持第一安全算法、第二安全算法和第四安全算法中的哪一安全算法，终端设备和服务呼叫会话控制功能网元均能够基于同一安全算法（即第三安全算法）计算认证响应，以认证终端设备。

第六方面，本申请实施例提供一种认证方法，该方法的执行主体可以是终端设备，也可以是应用于终端设备中的芯片。下面以执行主体是终端设备为例进行描述。该方法包括：终端设备接收来自服务呼叫会话控制功能网元的认证挑战请求消息。其中，认证挑战请求消息携带第一安全算法的信息和第二安全算法的信息。终端设备确定第三安全算法，其中，第三安全算法为第一安全算法或第二安全算法。终端设备根据第三安全算法计算安全参数的哈希值。终端设备根据第三安全算法和哈希值计算认证响应。终端设备向服务呼叫会话控制功能网元发送注册请求消息。其中，注册请求消息携带认证响应，认证响应用于认证终端设备。

也就是说，终端设备能够从认证挑战请求消息的安全算法的信息中确定一个安全算法，

即第三安全算法。然后，终端设备通过第二注册请求消息向服务呼叫会话控制功能网元指示自身支持的安全算法，即第三安全算法，以使服务呼叫会话控制功能网元使用第三安全算法计算第二认证响应，从而能够认证终端设备。

5 在一种可能的设计中，认证挑战请求消息包括按照预设顺序携带的第一安全算法的信息和第二安全算法的信息，且预设顺序是基于第一安全算法的优先级和第二安全算法的优先级确定的。

在一种可能的设计中，终端设备确定第三安全算法，包括：终端设备确定认证挑战请求消息中自身能够识别的首个安全算法为第三安全算法。

10 由于认证挑战请求消息是按照预设顺序携带安全算法的信息，终端设备优先识别到的是优先级较高的安全算法的信息，保证终端设备使用自身支持的且优先级较高的安全算法计算认证响应，从而保证认证过程的安全性能。

在一种可能的设计中，终端设备确定第三安全算法，包括：终端设备确定第一安全算法和第二安全算法中优先级较高的安全算法为第三安全算法。也就是说，终端设备根据认证挑战请求消息中各个安全算法的优先级，从认证挑战请求消息的各个安全算法中确定一个安全算法，即第三安全算法。由于安全算法的优先级在一定程度上影响认证过程的安全性能，终端设备结合安全算法的优先级来确定第三安全算法，能够保证认证过程的安全性能。

在一种可能的设计中，第一安全算法为安全散列算法 SHA256 或 SHA512，第二安全算法为消息摘要 MD5 算法。

20 在一种可能的设计中，第一安全算法为 SHA256，第二安全算法为 SHA512。

在一种可能的设计中，认证挑战请求消息携带第一安全算法的信息、第二安全算法的信息和第四安全算法的信息。终端设备确定第三安全算法，包括：终端设备从第一安全算法、第二安全算法和第四安全算法中确定第三安全算法。其中，第三安全算法为第一安全算法、第二安全算法或第四安全算法。

25 也就是说，在第一安全算法为 SHA256，第二安全算法为 SHA512 的情况下，服务呼叫会话控制功能网元还能够通过认证挑战请求消息向终端设备提供第四安全算法的信息，以使终端设备从第一安全算法、第二安全算法和第四安全算法中确定一个安全算法，作为第三安全算法。也就是说，无论终端设备支持第一安全算法、第二安全算法和第四安全算法中的哪一安全算法，终端设备和服务呼叫会话控制功能网元均能够基于同一安全算法
30 （即第三安全算法）计算认证响应，以实现终端设备的认证过程。

第七方面，本申请实施例提供一种通信装置，该通信装置可以为上述第一方面或第一方面任一种可能的设计中的终端设备，或者为设置于上述终端设备内的装置，或者实现上述终端设备功能的芯片；所述通信装置包括实现上述方法相应的模块、单元、或手段
35 （means），该模块、单元、或 means 可以通过硬件实现，软件实现，或者通过硬件执行相应的软件实现。该硬件或软件包括一个或多个与上述功能相对应的模块或单元。

该通信装置包括发送单元、接收单元和处理单元。其中，发送单元，用于向服务呼叫会话控制功能网元发送第一注册请求消息。其中，第一注册请求消息携带通信装置能够支持的安全算法的信息，安全算法包括以下至少一项：第一安全算法或第二安全算法。接收单元，用于接收来自服务呼叫会话控制功能网元的认证挑战消息。其中，认证挑战消息包

括第三安全算法的信息，第三安全算法为通信装置能够支持的安全算法中的一个。处理单元，用于根据第三安全算法计算安全参数的哈希值。处理单元，还用于根据第三安全算法和哈希值计算认证响应。发送单元，还用于向服务呼叫会话控制功能网元发送第二注册请求消息。其中，第二注册请求消息携带认证响应，认证响应用于认证通信装置。

- 5 在一种可能的设计中，第一安全算法为安全散列算法 SHA256，第二安全算法为安全散列算法 SHA512。

第八方面，本申请实施例提供一种通信装置，该通信装置可以为上述第二方面或第二方面任一种可能的设计中的服务呼叫会话控制功能网元，或者为设置于上述服务呼叫会话控制功能网元内的装置，或者实现上述服务呼叫会话控制功能网元功能的芯片；所述通信
10 装置包括实现上述方法相应的模块、单元、或手段（means），该模块、单元、或 means 可以通过硬件实现，软件实现，或者通过硬件执行相应的软件实现。该硬件或软件包括一个或多个与上述功能相对应的模块或单元。

该通信装置包括发送单元、接收单元和处理单元。其中，接收单元，用于接收来自终端设备的第一注册请求消息。其中，第一注册请求消息包括终端设备能够支持的安全算法
15 的信息，安全算法包括以下至少一项：第一安全算法或第二安全算法。发送单元，用于向归属签约用户服务器发送认证向量请求消息。其中，认证向量请求消息包括终端设备能够支持的安全算法的信息。接收单元，还用于接收归属签约用户服务器返回的认证向量请求响应。其中，认证向量请求响应包括哈希值以及第三安全算法的信息，哈希值是基于第三安全算法计算得到的，第三安全算法为终端设备能够支持的安全算法中的一个。发送单元，
20 还用于向终端设备发送认证挑战消息，其中，认证挑战消息包括第三安全算法的信息。接收单元，还用于接收来自终端设备的第二注册请求消息，其中，第二注册请求消息携带第一认证响应。处理单元，用于根据第三安全算法和哈希值，计算第二认证响应。处理单元，还用于使用第二认证响应检验第一认证响应，得到终端设备的认证结果。

- 25 在一种可能的设计中，第一安全算法为安全散列算法 SHA256，第二安全算法为安全散列算法 SHA512。

第九方面，本申请实施例提供一种通信装置，该通信装置可以为上述第三方面或第三方面任一种可能的设计中的归属签约用户服务器，或者为设置于上述归属签约用户服务器内的装置，或者实现上述归属签约用户服务器功能的芯片；所述通信装置包括实现上述方法相应的模块、单元、或手段（means），该模块、单元、或 means 可以通过硬件实现，软
30 件实现，或者通过硬件执行相应的软件实现。该硬件或软件包括一个或多个与上述功能相对应的模块或单元。

该通信装置包括发送单元、接收单元和处理单元。其中，接收单元，用于接收来自服务呼叫会话控制功能网元的认证向量请求消息。其中，认证向量请求消息包括终端设备能够支持的安全算法的信息，安全算法包括以下至少一项：第一安全算法或第二安全算法。
35 处理单元，用于根据第三安全算法计算安全参数的哈希值，其中，第三安全算法为终端设备能够支持的安全算法中的一个。发送单元，用于向服务呼叫会话控制功能网元返回认证向量请求响应，其中，认证向量请求响应携带哈希值以及第三安全算法的信息。

在一种可能的设计中，第一安全算法为安全散列算法 SHA256，第二安全算法为安全散列算法 SHA512。

第十方面，本申请实施例提供一种通信装置，该通信装置可以为上述第四方面或第四方面任一种可能的设计中的归属签约用户服务器，或者为设置于上述归属签约用户服务器内的装置，或者实现上述归属签约用户服务器功能的芯片；所述通信装置包括实现上述方法相应的模块、单元、或手段（means），该模块、单元、或 means 可以通过硬件实现，软件实现，或者通过硬件执行相应的软件实现。该硬件或软件包括一个或多个与上述功能相对应的模块或单元。

该通信装置包括发送单元、接收单元和处理单元。其中，接收单元，用于接收来自服务呼叫会话控制功能网元的认证向量请求消息。处理单元，用于根据第一安全算法计算安全参数的第一哈希值。处理单元，还用于根据第二安全算法计算安全参数的第二哈希值。发送单元，用于向服务呼叫会话控制功能网元返回认证向量请求响应，其中，认证向量请求响应携带第一哈希值和第二哈希值。

在一种可能的设计中，认证向量请求响应包括按照预设顺序携带的第一哈希值和第二哈希值，且预设顺序是基于第一安全算法的优先级和第二安全算法的优先级确定的。

在一种可能的设计中，第一安全算法为安全散列算法 SHA256 或安全散列算法 SHA512，第二安全算法为消息摘要 MD5 算法。

第十一方面，本申请实施例提供一种通信装置，该通信装置可以为上述第五方面或第五方面任一种可能的设计中的服务呼叫会话控制功能网元，或者为设置于上述服务呼叫会话控制功能网元内的装置，或者实现上述服务呼叫会话控制功能网元功能的芯片；所述通信装置包括实现上述方法相应的模块、单元、或手段（means），该模块、单元、或 means 可以通过硬件实现，软件实现，或者通过硬件执行相应的软件实现。该硬件或软件包括一个或多个与上述功能相对应的模块或单元。

该通信装置包括发送单元、接收单元和处理单元。其中，接收单元，用于接收来自终端设备的第一注册请求消息。发送单元，用于向归属签约用户服务器发送认证向量请求消息。接收单元，还用于接收归属签约用户服务器返回的认证向量请求响应，其中，认证向量请求响应携带第一哈希值和第二哈希值，第一哈希值是基于第一安全算法计算的，第二哈希值是基于第二安全算法计算的。发送单元，还用于向终端设备发送认证挑战请求消息，其中，认证挑战请求消息携带第一安全算法的信息和第二安全算法的信息。接收单元，还用于接收来自终端设备的第二注册请求消息，其中，第二注册请求消息包括第一认证响应和第三安全算法的信息，第一认证响应是基于第三安全算法计算的，第三安全算法是第一安全算法或第二安全算法。处理单元，用于从第一哈希值和第二哈希值中选择第三安全算法对应的哈希值。处理单元，还用于根据第三安全算法和第三安全算法对应的哈希值计算第二认证响应。处理单元，还用于使用第二认证响应校验第一认证响应，得到终端设备的认证结果。

在一种可能的设计中，认证向量请求响应包括按照预设顺序携带的第一哈希值和第二哈希值，且预设顺序是基于第一安全算法的优先级和第二安全算法的优先级确定的；处理单元，具体用于：根据预设顺序，从第一哈希值和第二哈希值中选择第三安全算法对应的哈希值。

在一种可能的设计中，认证挑战请求消息包括按照预设顺序携带的第一安全算法的信息和第二安全算法的信息，且预设顺序是基于第一安全算法的优先级和第二安全算法的优

先级确定的。

在一种可能的设计中,第一安全算法为安全散列算法 SHA256 或安全散列算法 SHA512,第二安全算法为消息摘要 MD5 算法。

第十二方面,本申请实施例提供一种通信装置,该通信装置可以为上述第六方面或第六方面任一种可能的设计中的终端设备,或者为设置于上述终端设备内的装置,或者实现上述终端设备功能的芯片;所述通信装置包括实现上述方法相应的模块、单元、或手段(means),该模块、单元、或 means 可以通过硬件实现,软件实现,或者通过硬件执行相应的软件实现。该硬件或软件包括一个或多个与上述功能相对应的模块或单元。

该通信装置包括发送单元、接收单元和处理单元。其中,接收单元,用于接收来自服务呼叫会话控制功能网元的认证挑战请求消息,其中,认证挑战请求消息携带第一安全算法的信息和第二安全算法的信息。处理单元,用于确定第三安全算法,其中,第三安全算法为第一安全算法或第二安全算法。处理单元,还用于根据第三安全算法计算安全参数的哈希值。处理单元,还用于根据第三安全算法和哈希值计算认证响应。发送单元,用于向服务呼叫会话控制功能网元发送注册请求消息,其中,注册请求消息携带认证响应,认证响应用于认证通信装置。

在一种可能的设计中,认证挑战请求消息包括按照预设顺序携带的第一安全算法的信息和第二安全算法的信息,且预设顺序是基于第一安全算法的优先级和第二安全算法的优先级确定的。

在一种可能的设计中,处理单元,具体用于:确定认证挑战请求消息中自身能够识别的首个安全算法为第三安全算法。

在一种可能的设计中,第一安全算法为安全散列算法 SHA256 或安全散列算法 SHA512,第二安全算法为消息摘要 MD5 算法。

第十三方面,本申请实施例提供了一种通信装置,包括:处理器和存储器;该存储器用于存储计算机指令,当该处理器执行该指令时,使得该通信装置执行上述任一方面或任一方面任一种可能的设计中终端设备所执行的方法。该通信装置可以为上述第一方面或第一方面任一种可能的设计中的终端设备,或者实现上述终端设备功能的芯片;或者,该通信装置可以为上述第六方面或第六方面任一种可能的设计中的终端设备,或者实现上述终端设备功能的芯片。

第十四方面,本申请实施例提供了一种通信装置,包括:处理器;所述处理器与存储器耦合,用于读取存储器中的指令并执行,以使该通信装置执行如上述任一方面或任一方面任一种可能的设计中的终端设备所执行的方法。该通信装置可以为上述第一方面或第一方面任一种可能的设计中的终端设备,或者实现上述终端设备功能的芯片;或者,该通信装置可以为上述第六方面或第六方面任一种可能的设计中的终端设备,或者实现上述终端设备功能的芯片。

第十五方面,本申请实施例提供一种芯片,包括逻辑电路和输入输出接口。其中,输入输出接口用于与芯片之外的模块通信,例如,该芯片可以为实现上述第一方面或第一方面任一种可能的设计中的终端设备功能的芯片。输入输出接口输出第一注册请求消息、第二注册请求消息。输入输出接口输入认证挑战请求消息。逻辑电路用于运行计算机程序或指令,以实现以上第一方面或第一方面任一种可能的设计中的方法。或者,该芯片可以为

实现上述第六方面或第六方面任一种可能的设计中的终端设备功能的芯片。输入输出接口输出注册请求消息，输入输出接口输入认证挑起请求消息。逻辑电路用于运行计算机程序或指令，以实现以上第六方面或第六方面任一种可能的设计中的方法。

第十六方面，本申请实施例提供了一种通信装置，包括：处理器和存储器；该存储器
5 用于存储计算机指令，当该处理器执行该指令时，使得该通信装置执行上述任一方面或任一方面任一种可能的设计中服务呼叫会话控制功能网元所执行的方法。该通信装置可以为上述第二方面或第二方面任一种可能的设计中的服务呼叫会话控制功能网元，或者实现上述服务呼叫会话控制功能网元功能的芯片；或者，该通信装置可以为上述第五方面或第五方面任一种可能的设计中的服务呼叫会话控制功能网元，或者实现上述服务呼叫会话控制
10 功能网元功能的芯片。

第十七方面，本申请实施例提供了一种通信装置，包括：处理器；所述处理器与存储器耦合，用于读取存储器中的指令并执行，以使该通信装置执行如上述任一方面或任一方面任一种可能的设计中的服务呼叫会话控制功能网元所执行的方法。该通信装置可以为上述第二方面或第二方面任一种可能的设计中的服务呼叫会话控制功能网元，或者实现上述
15 服务呼叫会话控制功能网元功能的芯片；或者，该通信装置可以为上述第五方面或第五方面任一种可能的设计中的服务呼叫会话控制功能网元，或者实现上述服务呼叫会话控制功能网元功能的芯片。

第十八方面，本申请实施例提供一种芯片，包括逻辑电路和输入输出接口。其中，输入输出接口用于与芯片之外的模块通信，例如，该芯片可以为实现上述第二方面或第二方面任一种可能的设计中的服务呼叫会话控制功能网元功能的芯片。输入输出接口输入第一注册请求消息、认证向量请求响应、第二注册请求消息。输入输出接口输出认证向量请求消息、认证挑战请求消息。逻辑电路用于运行计算机程序或指令，以实现以上第二方面或第二方面任一种可能的设计中的方法。或者，该芯片可以为实现上述第五方面或第五方面任一种可能的设计中的服务呼叫会话控制功能网元功能的芯片。输入输出接口输入第一注册请求消息、认证向量请求响应、第二注册请求消息，输入输出接口输出认证向量请求消息、认证挑起请求消息。逻辑电路用于运行计算机程序或指令，以实现以上第五方面或第五方面任一种可能的设计中的方法。
20 25

第十九方面，本申请实施例提供了一种通信装置，包括：处理器和存储器；该存储器用于存储计算机指令，当该处理器执行该指令时，使得该通信装置执行上述任一方面或任一方面任一种可能的设计中归属签约用户服务器所执行的方法。该通信装置可以为上述第三方面或第三方面任一种可能的设计中的归属签约用户服务器，或者实现上述归属签约用户服务器功能的芯片；或者，该通信装置可以为上述第四方面或第四方面任一种可能的设计中的归属签约用户服务器，或者实现上述归属签约用户服务器功能的芯片。
30

第二十方面，本申请实施例提供了一种通信装置，包括：处理器；所述处理器与存储器耦合，用于读取存储器中的指令并执行，以使该通信装置执行如上述任一方面或任一方面任一种可能的设计中的归属签约用户服务器所执行的方法。该通信装置可以为上述第三方面或第三方面任一种可能的设计中的归属签约用户服务器，或者实现上述归属签约用户服务器功能的芯片；或者，该通信装置可以为上述第四方面或第四方面任一种可能的设计中的归属签约用户服务器，或者实现上述归属签约用户服务器功能的芯片。
35

第二十一方面，本申请实施例提供一种芯片，包括逻辑电路和输入输出接口。其中，输入输出接口用于与芯片之外的模块通信，例如，该芯片可以为实现上述第三方面或第三方面任一种可能的设计中的归属签约用户服务器功能的芯片。输入输出接口输出认证向量请求响应。输入输出接口输入认证向量请求消息。逻辑电路用于运行计算机程序或指令，
5 以实现以上第三方面或第三方面任一种可能的设计中的方法。或者，该芯片可以为实现上述第四方面或第四方面任一种可能的设计中的归属签约用户服务器功能的芯片。输入输出接口输出认证向量请求响应，输入输出接口输入认证向量请求消息。逻辑电路用于运行计算机程序或指令，以实现以上第四方面或第四方面任一种可能的设计中的方法。

第二十二方面，本申请实施例提供一种计算机可读存储介质，该计算机可读存储介质
10 中存储有指令，当其在计算机上运行时，使得计算机可以执行上述任一方面中任一项的认证方法。

第二十三方面，本申请实施例提供一种包含指令的计算机程序产品，当其在计算机上运行时，使得计算机可以执行上述任一方面中任一项的认证方法。

第二十四方面，本申请实施例提供一种电路系统，电路系统包括处理电路，处理电路
15 被配置为执行如上述任一方面中任一项的认证方法。

第二十五方面，本申请实施例提供一种通信系统，该通信系统包括上述各个方面中任一项中的终端设备、服务呼叫会话控制功能网元和归属签约用户服务器。

其中，第二方面至第二十五方面中任一种设计所带来的技术效果可参考上文所提供的对应的方法中的有益效果，此处不再赘述。

20 **附图说明**

- 图 1 为本申请实施例提供的一种认证方法的流程示意图；
- 图 2 为本申请实施例提供的一种网络架构的示意图；
- 图 3 为本申请实施例提供的再一种认证方法的流程示意图；
- 图 4a 为本申请实施例提供的又一种认证方法的流程示意图；
- 25 图 4b 为本申请实施例提供的又一种认证方法的流程示意图；
- 图 5 为本申请实施例提供的又一种认证方法的流程示意图；
- 图 6 为本申请实施例提供的一种通信装置的结构示意图；
- 图 7 为本申请实施例提供的再一种通信装置的结构示意图。

具体实施方式

30 本申请的说明书以及附图中的术语“第一”和“第二”等是用于区别不同的对象，或者用于区别对同一对象的不同处理，而不是用于描述对象的特定顺序。此外，本申请的描述中所提到的术语“包括”和“具有”以及它们的任何变形，意图在于覆盖不排他的包含。例如包含了一系列步骤或单元的过程、方法、系统、产品或设备没有限定于已列出的步骤或单元，而是可选地还包括其他没有列出的步骤或单元，或可选地还包括对于这些过程、
35 方法、产品或设备固有的其它步骤或单元。本申请实施例中，“多个”包括两个或两个以上。本申请实施例中，“示例性的”或者“例如”等词用于表示作例子、例证或说明。本申请实施例中被描述为“示例性的”或者“例如”的任何实施例或设计方案不应被解释为比其它实施例或设计方案更优选或更具优势。确切而言，使用“示例性的”或者“例如”

等词旨在以具体方式呈现相关概念。在本申请实施例中，“传输”包括“发送”或“接收”。

首先，介绍本申请中所涉及的协议（session initiation protocol, SIP）摘要（digest）认证方式。

5 协议摘要认证方式是互联网协议多媒体子系统（internet protocol multimedia subsystem, IMS）通常采用的认证终端设备的方式。图 1 示出了一种协议摘要认证方式的处理步骤：

S111、终端设备向代理呼叫会话控制功能（proxy call session control function, P-CSCF）网元发送第一注册请求消息。相应的，代理呼叫会话控制功能（proxy call session control function, P-CSCF）网元接收来自终端设备的第一注册请求消息。

10 其中，第一注册请求消息包括终端设备的标识，如 IP 多媒体私有标识（IP multimedia private identity, IMPI）。

S112、P-CSCF 网元向查询呼叫会话控制功能（interrogating call session control function, I-CSCF）网元发送第一注册请求消息。相应的，I-CSCF 网元接收来自 P-CSCF 网元的第一注册请求消息。

15 S113、I-CSCF 网元向服务呼叫会话控制功能（serving call session control function, S-CSCF）网元发送第一注册请求消息。相应的，S-CSCF 网元接收来自 I-CSCF 网元的第一注册请求消息。

其中，S-CSCF 网元是 HSS 确定的一个网元。例如，I-CSCF 网元执行 S112 之后，I-CSCF 网元向归属签约用户服务器（home subscriber server, HSS）发出请求，以请求 HSS 确定哪一 S-CSCF 网元处理该第一注册请求消息。HSS 接收来自 I-CSCF 网元的请求之后，HSS 20 确定由哪个 S-CSCF 网元处理该第一注册请求消息。然后，HSS 向 I-CSCF 网元发送 Cx 选择信息（Cx-Selection-Info）消息。相应的，I-CSCF 网元接收来自 HSS 的 Cx-Selection-Info 消息。其中，Cx-Selection-Info 消息指示处理上述第一注册请求消息的 S-CSCF 网元。

S121、S-CSCF 网元向 HSS 发送认证向量请求消息。相应的，HSS 接收来自 S-CSCF 网元的认证向量请求消息。

25 其中，认证向量请求消息包括终端设备的标识，如 IMPI。

S122、HSS 向 S-CSCF 网元发送认证向量请求响应。相应的，S-CSCF 网元接收来自 HSS 的认证向量请求响应。

其中，认证向量请求响应可以包括但不限于以下参数：

第一项、IMPI。IMPI 用于标识终端设备。

30 第二项、域（realm）信息。域信息用于表示终端进行认证的域的信息。

第三项、安全算法（algorithm），如消息摘要第五版（message digest 5, MD5）算法的名称、或 MD5 算法的标识。

第四项、qop。qop 的取值为“auth”的情况下，表明仅用于用户认证，qop 的取值为“auth-int”的情况下，指示同时做用户认证和消息体完整性保护。

35 第五项、哈希值 HA1。哈希值 HA1 是采用上述 MD5 算法对用户名称（username）、域信息和密码（password）进行计算之后的哈希值。示例性的，哈希值 HA1 是下述三个参数拼接之后的哈希值：

HA1=username:realm:password 的 MD5 值

其中，HA1 表示哈希值，username 表示用户名称，realm 表示域信息，password 表示

密码,“:”表示拼接。也就是说,先确定用户名称(username)、域信息和密码(password)三个参数的拼接,再确定拼接之后整体参数的哈希值。

S131、S-CSCF 网元向 I-CSCF 网元发送认证挑战请求消息。相应的, I-CSCF 网元接收来自 S-CSCF 网元的认证挑战请求消息。

5 其中,认证挑战请求消息可以包括但不限于以下参数:

第一项、IMPI。IMPI 用于标识终端设备。

第二项、域信息,与 S122 中的“域信息”相同。

第三项、安全算法(algorithm),如 MD5 算法的名称、或 MD5 算法的标识。

第四项、qop,与 S122 中的“qop”相同。

10 第五项、nonce。nonce 是 S-CSCF 网元产生的一个随机数。

S132、I-CSCF 网元向 P-CSCF 网元发送认证挑战请求消息。相应的, P-CSCF 网元接收来自 I-CSCF 网元的认证挑战请求消息。

S133、P-CSCF 网元向终端设备发送认证挑战请求消息。相应的,终端设备接收来自 P-CSCF 网元的认证挑战请求消息。

15 S141、终端设备向 P-CSCF 网元发送第二注册请求消息。相应的, P-CSCF 网元接收来自终端设备的第二注册请求消息。

其中,第二注册请求消息至少包括认证响应(response)。认证响应用于认证终端设备。认证响应是采用 MD5 算法对用户名称、域信息、密码、nonce 和 digest-uri 等参数进行计算之后的数值。认证响应是如下参数拼接之后的哈希值:

20 response=HA1:nonce:n-c:cnonce:qop:HA2 的 MD5 值

其中, response 表示认证响应, HA1 表示对用户名称、域信息和密码进行 MD5 计算之后的哈希值, nonce 表示 S-CSCF 网元产生的一个随机数, n-c 表示 nonce-count, 即终端设备使用相同 nonce 发送第二注册请求消息的计数器的计数值, cnonce 是终端设备产生的一个随机数, qop 的取值表示仅用于认证还是用于认证和消息体的完整性保护。哈希值 HA2 是采用 MD5 算法对 method 和 digest-uri 进行计算之后的哈希值。也就是说,先确定 HA1、nonce、n-c、cnonce、qop 和 HA2 的拼接,再确定拼接之后整体参数的哈希值。其中, 哈希值 HA2 是如下参数拼接之后的哈希值:

HA2=method:digest-uri 的 MD5 值

30 其中, method 表示超文本传输协议(hyper text transfer protocol, HTTP)请求的方法, digest-uri 表示统一资源标识符(uniform resource identifier, URI)的信息,“:”表示拼接。

可选的,第二注册请求消息还包括以下参数中的一项或多项:

第一项、IMPI。IMPI 用于标识终端设备。

第二项、域信息,与 S122 中的“域信息”相同。

第三项、安全算法(algorithm),如 MD5 算法的名称、或 MD5 算法的标识。

35 第四项、qop,与 S122 中的“qop”相同。

第五项、nonce,与 S131 中的“nonce”相同。

第六项、cnonce。cnonce 是终端设备产生的一个随机数。

第七项、nonce-count。表示终端设备使用相同 nonce 发送第二注册请求消息的计数器的计数值。

第八项、digest-uri。表示 URI 的信息。

S142、P-CSCF 网元向 I-CSCF 网元发送第二注册请求消息。相应的，I-CSCF 网元接收来自 P-CSCF 网元的第二注册请求消息。

5 S143、I-CSCF 网元向 S-CSCF 网元发送第二注册请求消息。相应的，S-CSCF 网元接收来自 I-CSCF 网元的第二注册请求消息。

其中，S-CSCF 网元接收第二注册请求消息之后，S-CSCF 网元基于认证向量请求响应中的哈希值 HA1 和安全算法，计算认证响应。在 S-CSCF 网元确定自身计算的认证响应与第二注册请求消息中的认证响应不同的情况下，S-CSCF 网元确认认证失败。反之，在 S-CSCF 网元确定自身计算的认证响应与第二注册请求消息中的认证响应相同的情况下，
10 S-CSCF 网元确认认证成功，执行 S151：

S151、S-CSCF 网元向 I-CSCF 网元发送认证成功消息。相应的，S-CSCF 网元接收来自 I-CSCF 网元的认证成功消息。

S152、I-CSCF 网元向 P-CSCF 网元发送认证成功消息。相应的，P-CSCF 网元接收来自 I-CSCF 网元的认证成功消息。

15 S153、P-CSCF 网元向终端设备发送认证成功消息。相应的，终端设备接收来自 P-CSCF 网元的认证成功消息。

由于 MD5 算法是不安全的算法，所以，一种方案是考虑让部分终端设备支持新的安全算法，如安全散列算法（secure hash algorithm, SHA）256 或 SHA512，通过 SHA256 或 SHA512 计算的认证响应完成认证。

20 显然，这种方案会导致如下情况：一些终端设备支持 SHA256 或 SHA512，因此需要使用 SHA256 或 SHA512 计算认证响应，而另一些终端设备不支持 SHA256 和 SHA512，仍沿用 MD5 算法计算认证响应。此种情况下，如何使得支持不同安全算法的终端设备完成认证，是亟待解决的问题。

鉴于此，本申请实施例提供一种认证方法，本申请实施例认证方法可以适用于 IMS
25 网络，如图 2 所示，该通信系统可以包括终端设备 20 和网络设备 21。终端设备 20 和网络设备 21 通信连接。图 2 仅为示意图，并不构成对本申请实施例认证方法的适用场景的限制。

其中，终端设备 20，也可以称为用户设备（user equipment, UE），如手机、电脑，还可以为蜂窝电话、无绳电话、会话启动协议（session initiation protocol, SIP）电话、无线
30 本地环路（wireless local loop, WLL）站、个人数字处理（personal digital assistant, PDA）设备、膝上型计算机、手持式通信设备、手持式计算设备、卫星无线设备、无线调制解调器卡、电视机顶盒（set top box, STB）、用户驻地设备（customer premise equipment, CPE）和/或用于在无线系统上进行通信的其他设备。

其中，网络设备 21 包括如下网元：P-CSCF 网元、I-CSCF 网元、S-CSCF 网元连接、
35 HSS 和应用服务器（application server, AS）。各网元之间的连接关系如下：终端设备通过 P-CSCF 网元、I-CSCF 网元与 S-CSCF 网元连接，S-CSCF 网元还分别与 HSS 和 AS 连接，I-CSCF 网元还与 HSS 连接，如图 2 所示。P-CSCF 网元用于完成终端设备的接入，也就是说，终端设备通过 P-CSCF 网元接入 IMS。I-CSCF 网元用于选择 S-CSCF 网元，不同运营商或不同局域网络之间的互通，实现网络屏蔽等功能。S-CSCF 网元用于提供会话控制和

路由等核心功能。上述 P-CSCF 网元、I-CSCF 网元和 S-CSCF 网元实现呼叫会话控制功能 (call session control function, CSCF), 以完成呼叫和会话时的控制和路由等功能。HSS 用于保存终端设备的安全算法, 如签约数据和配置数据等。AS 是指为终端设备提供应用服务的服务器。

5 需要说明的是, 图 2 所示的终端设备可以通过第四代(4th generation, 4G)网络接入 IMS, 也可以通过第五代 (5th generation, 5G) 网络接入 IMS, 本申请实施例对此不作限定。此外, 图 2 仅为示例性框架图, 除图 2 所示的功能网元外, 该 IMS 还可以包括其他功能网元, 本申请实施例对此不作限制。

10 本申请实施例描述的通信系统以及业务场景是为了更加清楚的说明本申请实施例的技术方案, 并不构成对于本申请实施例提供的技术方案的限定。本领域普通技术人员可知, 随着网络架构的演变和新业务场景的出现, 本申请实施例提供的技术方案对于类似的技术问题, 同样适用。

下面对本申请实施例提供的认证方法进行具体阐述。

15 需要说明的是, 本申请下述实施例中各个网元之间的消息名字或消息中各参数的名字等只是一个示例, 具体实现中也可以是其他的名字。在本申请实施例中, 第 X 安全算法的信息, 可以但不限于如下其中一项: 第 X 安全算法的名称、或第 X 安全算法的标识等。其中, 第 X 安全算法可以是指第一安全算法、第二安全算法、第三安全算法、或第四安全算法等。在此统一说明, 以下不再赘述。

20 本申请实施例提供一种认证方法 300, 该认证方法 300 应用在认证过程中。参见图 3, 该认证方法 300 包括如下步骤:

S301、终端设备向 S-CSCF 网元发送第一注册请求消息。相应的, S-CSCF 网元接收来自终端设备的第一注册请求消息。

其中, 第一注册请求消息包括终端设备的标识 (如 IMPI)。并且, 第一注册请求消息还可以包括以下信息中的至少一项:

25 第一项、终端设备能够支持的安全算法的信息。安全算法的信息包括安全算法的名称、或安全算法的标识等。安全算法包括以下至少一项: 第一安全算法或第二安全算法。其中, 第一安全算法为 SHA256, 第二安全算法为 SHA512。示例性的, 安全算法的信息可以承载于第一注册请求消息中的“能力信息 (capability informatio)”字段中。

30 第二项、指示信息。其中, 指示信息可以是以下至少一项: 指示“已废除 MD5 算法”的信息、指示“不支持 MD5 算法”的信息、指示“支持新的安全算法”的信息、或指示“终端设备是新版本的终端设备”等。其中, 新版本的终端设备是指, 支持第一安全算法和/或第二安全算法的终端设备。如此, S-CSCF 网元即可明确获知终端设备支持新的安全算法, 如第一安全算法、或第二安全算法。

其中, S301 的具体实现过程可以参见 S111、S112 和 S113 的相关说明, 此处不再赘述。

35 S302、S-CSCF 网元向 HSS 发送认证向量请求消息。相应的, HSS 接收来自 S-CSCF 网元的认证向量请求消息。

其中, 认证向量请求消息包括终端设备的标识 (IMPI)。并且, 认证向量请求消息还包括以下至少一项: 终端设备能够支持的安全算法的信息、指示信息。其中, S302 中的指示信息与 S301 中的指示信息相同。在认证向量请求消息包括“终端设备能够支持的安全

算法的信息”的情况下，认证向量请求消息中安全算法的信息与第一注册请求消息中安全算法的信息一致。例如，在第一注册请求消息包括 SHA256 的标识的情况下，认证向量请求消息包括 SHA256 的标识。在第一注册请求消息包括 SHA512 的标识的情况下，认证向量请求消息包括 SHA512 的标识。在第一注册请求消息包括 SHA256 的标识和 SHA512 的标识的情况下，认证向量请求消息包括 SHA256 的标识和 SHA512 的标识。

S303、HSS 根据第三安全算法计算安全参数的哈希值 HA1。

其中，第三安全算法为终端设备能够支持的安全算法中的一个。

若 HSS 收到的认证向量请求消息包括“终端设备能够支持的安全算法的信息”，则 HSS 确定第三安全算法的过程如下：在认证向量请求消息包括 SHA256 的标识的情况下，第三安全算法为 SHA256。在认证向量请求消息包括 SHA512 的标识的情况下，第三安全算法为 SHA512。在认证向量请求消息包括 SHA256 的标识和 SHA512 的标识的情况下，HSS 从 SHA256 和 SHA512 中确定一个算法作为第三安全算法，如，HSS 根据本地配置的 SHA256 的优先级和 SHA512 的优先级选择优先级高的安全算法，作为第三安全算法。

若 HSS 收到的认证向量请求消息包括“指示信息”，则 HSS 确定第三安全算法的过程如下：HSS 根据指示信息确定第三安全算法。例如，HSS 根据指示信息获知终端设备支持新的安全算法，之后，HSS 从 SHA256 和 SHA512 中确定一个算法作为第三安全算法。或者，HSS 配置有 SHA256，且未配置 SHA512 的情况下，HSS 将 SHA256 作为第三安全算法。或者，HSS 未配置 SHA256，且配置有 SHA512 的情况下，HSS 将 SHA512 作为第三安全算法。

其中，安全参数是 IMPI 所标识的终端设备的配置参数。例如，安全参数包括上述终端设备上登录的用户名称、密码和域名。

示例性的，HSS 采用第三安全算法对用户名称、密码和域信息三个参数进行计算，以得到第三安全算法对应的哈希值 HA1。以第三安全算法实现为 SHA256 为例，哈希值 HA1 是如下参数拼接之后的哈希值：

HA1=username:realm:password 的 SHA256 值

其中，HA1 表示第三安全算法对应的哈希值，username 表示用户名称，realm 表示域信息，password 表示密码。“:”表示拼接。

S304、HSS 向 S-CSCF 网元发送认证向量请求响应。相应的，S-CSCF 网元接收来自 HSS 的认证向量请求响应。

其中，认证向量请求响应携带哈希值 HA1 以及第三安全算法的信息。HA1 是 S303 中 HSS 计算得到的数值。第三安全算法是 S303 中 HSS 计算哈希值 HA1 的安全算法，第三安全算法的信息包括第三安全算法的名称、或第三安全算法的标识等。当然，认证向量请求响应中还可以包括其他参数，详见 S122 的相关说明，此处不再赘述。

S305、S-CSCF 网元向终端设备发送认证挑战请求消息。相应的，终端设备接收来自 S-CSCF 网元的认证挑战请求消息。

其中，认证挑战请求消息包括第三安全算法的信息，如第三安全算法的名称、第三安全算法的标识等。认证挑战请求消息中的第三安全算法与认证向量请求响应中的第三安全算法一致。例如，在认证向量请求响应包括 SHA256 的标识的情况下，认证挑战请求消息包括 SHA256 的标识。当然，认证挑战请求消息还可以包括其他参数，详见 S131 的相关

说明，此处不再赘述。

其中，S305的实现过程可以参见S131、S132和S133的相关说明，此处不再赘述。

- 需要说明的是，在终端设备支持一种安全算法（如SHA256或SHA512）的情况下，认证挑战请求消息可以不携带第三安全算法的信息。由于终端设备支持的安全算法是一种，所以，终端设备能够确定采用哪一安全算法计算哈希值HA1，无需S-CSCF网元通过认证挑战请求消息指示安全算法，以节省信令开销。

S306、终端设备根据第三安全算法计算安全参数的哈希值HA1。

- 其中，第三安全算法是认证挑战请求消息指示的安全算法。例如，在认证挑战请求消息包括SHA256的标识的情况下，第三安全算法为SHA256。或者，第三安全安全算法是终端设备通过终端设备能够支持的安全算法确定的。例如，终端设备只支持SHA256的情况下，则第三安全算法为SHA256。

其中，安全参数是终端设备的配置参数。安全参数包括上述终端设备上登录的用户名称、密码和域信息。

- 示例性的，终端设备采用SHA256（即第三安全算法）对用户名称、密码和域信息三个参数进行计算，以得到SHA256（即第三安全算法）对应的哈希值HA1。

S307、终端设备根据第三安全算法和哈希值HA1计算第一认证响应。

示例性的，仍以第三安全算法为SHA256为例，第一认证响应的计算过程如下：

首先，终端设备采用SHA256对method和digest-uri进行计算，以得到哈希值HA2。示例性的，哈希值HA2是如下参数拼接之后的哈希值：

- HA2=method:digest-uri的SHA256值

其中，method表示HTTP请求的方法，digest-uri表示URI的信息，“:”表示拼接。

然后，终端设备采用SHA256对HA1、nonce、n-c、cnonce、qop、HA2进行计算，以得到第一认证响应。示例性的，第一认证响应是如下参数拼接之后的哈希值：

response=HA1:nonce:n-c:cnonce:qop:HA2的SHA256值

- 其中，response表示第一认证响应，HA1表示对用户名称、域信息和密码进行SHA256计算之后的哈希值，nonce表示S-CSCF网元产生的一个随机数，n-c表示nonce-count，即终端设备使用相同nonce发送第二注册请求消息的计数器的计数值，cnonce是终端设备产生的一个随机数，qop的取值表示仅用于认证还是用于认证和消息体的完整性保护。哈希值HA2是采用SHA256算法对method和digest-uri进行计算之后的哈希值。哈希值HA2是如下参数拼接之后的哈希值：

HA2=method:digest-uri的SHA256值

其中，method表示HTTP请求的方法，digest-uri表示URI的信息，“:”表示拼接。

S308、终端设备向S-CSCF网元发送第二注册请求消息。相应的，S-CSCF网元接收来自终端设备的第二注册请求消息。

- 其中，第二注册请求消息携带第一认证响应。第二注册请求消息中携带的第一认证响应是S307中终端设备计算得到的认证响应。当然，第二注册请求消息还可以包括其他参数，详见S141的相关说明，此处不再赘述。

其中，S308的实现过程可以参见S141、S142和S143的相关说明，此处不再赘述。

S309、S-CSCF网元根据第三安全算法和哈希值HA1，计算第二认证响应。

其中,第三安全算法是 S-CSCF 网元基于 S303 中认证向量请求响应确定的,与认证向量请求响应中的安全算法一致。哈希值 HA1 是 S303 中认证向量请求响应中携带的哈希值。第三安全算法也可以是 S-CSCF 网元基于 S308 中第二注册请求消息确定的,与第二注册请求消息中终端设备携带的安全算法一致。

5 示例性的,仍以第三安全算法为 SHA256 为例,第二认证响应的计算过程如下:

首先,S-CSCF 网元采用 SHA256 对 method 和 digest-uri 进行计算,以得到哈希值 HA2。

然后,S-CSCF 网元采用 SHA256 对 HA1、nonce、n-c、cnonce、qop、HA2 进行计算,以得到第二认证响应。

S310、S-CSCF 网元使用第二认证响应检验第一认证响应,得到终端设备的认证结果。

10 其中,第一认证响应是 S308 中第二注册请求消息携带的第一认证响应。第二认证响应是 S309 中 S-CSCF 网元计算得到的第二认证响应。

示例性的,在 S-CSCF 网元确定第一认证响应与第二认证响应不同的情况下,S-CSCF 网元确定终端设备认证失败。反之,在 S-CSCF 网元确定第一认证响应与第二认证响应相同的情况下,S-CSCF 网元确定终端设备认证成功,S-CSCF 网元向终端设备发送认证成功消息,详见 S151、S152 和 S153 的相关说明,此处不再赘述。

15 需要说明的是,对于支持 MD5 算法的终端设备而言,执行图 1 所示的处理流程,即可完成终端设备的认证过程。对于 S-CSCF 网元而言,S-CSCF 网元确定第一注册请求消息中不携带安全算法的信息,所以,S-CSCF 网元即可确定该终端设备是不支持新的安全算法,如第一安全算法、第二安全算法,S-CSCF 网元仍采用图 1 所示的处理流程对终端设备进行认证。S-CSCF 网元与 HSS 之间的交互过程仍参见图 1 所示。

20 如此,对于支持新的安全算法(如第一安全算法和/或第二安全算法)的终端设备而言,终端设备在第一注册请求消息中携带安全算法的信息,以向 S-CSCF 网元指示自身支持的安全算法。终端设备和 S-CSCF 网元即可基于相同的安全算法计算认证响应,如终端设备基于第三安全算法计算第一认证响应,S-CSCF 网元基于第三安全算法计算第二认证响应。
25 然后,S-CSCF 网元采用第二认证响应来校验第一认证响应,从而能够认证支持“第一安全算法和/或第二安全算法”的终端设备,避免由于终端设备和 S-CSCF 网元采用不同的安全算法,所导致的认证失败的现象。并且,对于不支持第一安全算法和第二安全算法的终端设备而言,终端设备在第一注册请求消息中无需携带安全算法的信息,此种情况下,S-CSCF 网元即可确定安全算法为 MD5 算法,从而采用 MD5 算法计算认证响应,以实现
30 终端设备的认证过程。

本申请实施例提供一种认证方法 400,该认证方法 400 应用在认证过程中。参见图 4a 和图 4b,该认证方法 400 包括如下步骤:

S401、终端设备向 S-CSCF 网元发送第一注册请求消息。相应的,S-CSCF 网元接收来自终端设备的第一注册请求消息。

35 其中,第一注册请求消息的介绍可以参见 S111 中关于“第一注册请求消息”的相关说明,此处不再赘述。S401 的实现过程可以参见 S111、S112 和 S113 的相关说明,此处不再赘述。

S402、S-CSCF 网元向 HSS 发送认证向量请求消息。相应的,HSS 接收来自 S-CSCF 网元的认证向量请求消息。

其中，认证向量请求消息可以参见 S121 中关于“认证向量请求消息”的相关说明，此处不再赘述。S402 的实现过程可以参见 S121 的相关说明，此处不再赘述。

对于 HSS 而言，根据 HSS 配置的安全算法的数量，通过两种情况对本申请实施例认证方法 400 进行介绍：

- 5 第一种情况，HSS 配置第一安全算法和第二安全算法的情况下，HSS 执行如图 4a 所示的 S403a：

S403a、HSS 根据第一安全算法计算安全参数的第一哈希值 HA1，以及根据第二安全算法计算安全参数的第二哈希值 HA1。

- 10 其中，第一安全算法为 SHA256，第二安全算法为 MD5 算法。或者，第一安全算法为 SHA512，第二安全算法为 MD5 算法。或者，第一安全算法为 SHA256，第二安全算法为 SHA512。

其中，安全参数包括上述终端设备上登录的用户名称、密码和域信息。

- 15 示例性的，在第一安全算法为 SHA256，且第二安全算法为 MD5 算法的情况下，HSS 采用 SHA256（即第一安全算法）对用户名称、密码和域信息三个参数进行计算，以得到 SHA256（即第一安全算法）对应的第一哈希值 HA1。HSS 采用 MD5 算法（即第二安全算法）对用户名称、密码和域信息三个参数进行计算，以得到 MD5 算法（即第二安全算法）对应的第二哈希值 HA1。

第二种情况，HSS 配置第一安全算法、第二安全算法和第四安全算法的情况下，HSS 执行如图 4b 所示的 S403b：

- 20 S403b、HSS 根据第一安全算法计算安全参数的第一哈希值 HA1，根据第二安全算法计算安全参数的第二哈希值 HA1，且根据第四安全算法计算安全参数的第三哈希值 HA1。

其中，第一安全算法为 SHA256，第二安全算法为 SHA512，第四安全算法为 MD5 算法。

- 25 其中，第一哈希值 HA1 和第二哈希值 HA1 的计算过程可以参见 S403a，第三哈希值 HA1 的计算过程可以参见 S122 的相关说明，此处不再赘述。

S404、HSS 向 S-CSCF 网元发送认证向量请求响应。相应的，S-CSCF 网元接收来自 HSS 的认证向量请求响应。

其中，通过两种情况对认证向量请求响应进行介绍：

- 30 第一种情况，在 HSS 执行 S403a 的情况下，认证向量请求响应携带第一哈希值 HA1 和第二哈希值 HA1。第一哈希值 HA1 是 S403a 中 HSS 计算的第一哈希值 HA1，第二哈希值 HA1 是 S403a 中 HSS 计算的第二哈希值 HA1。当然，认证向量请求响应中还可以包括其他参数，详见 S122 的相关说明，此处不再赘述。

- 35 在一些实施方式中，以认证向量请求响应携带两个哈希值为例，认证向量请求响应按照预设顺序携带第一哈希值 HA1 和第二哈希值 HA1。其中，预设顺序是基于第一安全算法的优先级和第二安全算法的优先级确定的。例如，第一安全算法的优先级高于第二安全算法的优先级，此时，认证向量请求响应中的第一哈希值 HA1 位于第二哈希值 HA1 之前。反之，第一安全算法的优先级低于第二安全算法的优先级，此时，认证向量请求响应中的第一哈希值 HA1 位于第二哈希值 HA1 之后。如此，S-CSCF 网元即可按照预设顺序区分第一哈希值 HA1 和第二哈希值 HA1。

需要说明的是，上述预设顺序仅是以“算法的优先级”这一指标为例进行介绍的。当然，预设顺序还可以是按照其他指标确定的，本申请实施例对此不作限定。

在一些实施方式中，以认证向量请求响应携带两个哈希值为例，认证向量请求响应还携带第一安全算法的信息、第二安全算法的信息。其中，第一安全算法的信息与第一哈希值 HA1 之间存在对应关系，第二安全算法的信息与第二哈希值 HA1 之间存在对应关系。示例性的，仍以第一安全算法为 SHA256，第二安全算法为 SHA512 为例，认证向量请求响应还携带 SHA256 的标识和 SHA512 的标识。其中，第一安全算法的信息与第一哈希值 HA1 之间存在的对应关系，可以体现为：SHA256 的标识和第一哈希值 HA1 在认证向量请求响应中的位置关系，例如，SHA256 的标识在第一哈希值 HA1 之后（或之前）。第二安全算法的信息与第二哈希值 HA1 之间存在的对应关系，可以体现为：SHA512 的标识和第二哈希值 HA1 在认证向量请求响应中的位置关系，例如，SHA512 的标识在第二哈希值 HA1 之后（或之前）。由于 S-CSCF 网元能够根据安全算法的信息区分第一安全算法和第二安全算法，S-CSCF 网元再结合上述对应关系也就能够区分第一哈希值 HA1 和第二哈希值 HA2。

第二种情况，在 HSS 执行 S403b 的情况下，认证向量请求响应携带第一哈希值 HA1、第二哈希值 HA1 和第三哈希值 HA1。第一哈希值 HA1 是 S403b 中 HSS 计算的第一哈希值 HA1，第二哈希值 HA1 是 S403b 中 HSS 计算的第二个哈希值 HA1，第三哈希值 HA1 是 S403b 中 HSS 计算的第三个哈希值 HA1。当然，认证向量请求响应中还可以包括其他参数，详见 S122 的相关说明，此处不再赘述。

在一些实施方式中，以认证向量请求响应携带三个哈希值为例，认证向量请求响应按照预设顺序携带第一哈希值 HA1、第二哈希值 HA1 和第三哈希值 HA1。其中，预设顺序是基于第一安全算法的优先级、第二安全算法的优先级和第四安全算法的优先级确定的。

在一些实施方式中，以认证向量请求响应携带三个哈希值为例，认证向量请求响应还携带第一安全算法的信息、第二安全算法的信息和第四安全算法的信息。其中，第一安全算法的信息与第一哈希值 HA1 之间存在对应关系，第二安全算法的信息与第二哈希值 HA1 之间存在对应关系，第四安全算法的信息与第三哈希值 HA1 之间存在对应关系。

S405、S-CSCF 网元向终端设备发送认证挑战请求消息。相应的，终端设备接收来自 S-CSCF 网元的认证挑战请求消息。

其中，S405 的实现过程可以参见 S131、S132 和 S133 的相关说明，此处不再赘述。下面，通过两种情况对认证挑战请求消息进行介绍：

第一种情况，以认证向量请求响应携带两个哈希值为例，认证挑战请求消息携带第一安全算法的信息和第二安全算法的信息。认证挑战请求消息中的第一安全算法，与 S404 的第一种情况中计算第一哈希值 HA1 的安全算法一致。认证挑战请求消息中的第二安全算法，与 S404 的第一种情况中计算第二哈希值 HA1 的安全算法一致。当然，认证挑战请求消息还可以包括其他参数，详见 S131 的相关说明，此处不再赘述。

在一些实施方式中，认证挑战请求消息按照预设顺序携带第一安全算法的信息和第二安全算法的信息。其中，预设顺序是基于第一安全算法的优先级和第二安全算法的优先级确定的。例如，第一安全算法的优先级高于第二安全算法的优先级，此时，认证挑战请求消息中的第一安全算法的信息位于第二安全算法的信息之前。反之，第一安全算法的优先

级低于第二安全算法的优先级，此时，认证挑战请求消息中的第一安全算法的信息位于第二安全算法的信息之后。如此，终端设备即可按照预设顺序优先识别出优先级较高的安全算法。

第二种情况，以认证向量请求响应携带三个哈希值为例，认证挑战请求消息携带第一安全算法的信息、第二安全算法的信息和第四安全算法的信息。认证挑战请求消息中的第一安全算法，与 S404 的第二种情况中计算第一哈希值 HA1 的安全算法一致。认证挑战请求消息中的第二安全算法，与 S404 的第二种情况中计算第二哈希值 HA1 的安全算法一致。认证挑战请求消息中的第四安全算法，与 S404 的第二种情况中计算第三哈希值 HA1 的安全算法一致。当然，认证挑战请求消息还可以包括其他参数，详见 S131 的相关说明，此处不再赘述。

在一些实施方式中，认证挑战请求消息按照预设顺序携带第一安全算法的信息、第二安全算法的信息和第四安全算法的信息。其中，预设顺序是基于第一安全算法的优先级、第二安全算法的优先级和第四安全算法的优先级确定的，以使终端设备按照预设顺序优先识别出优先级较高的安全算法。

需要说明的是，上述预设顺序仅是以“算法的优先级”这一指标为例进行介绍的。当然，预设顺序还可以是按照其他指标确定的，本申请实施例对此不作限定。

S406、终端设备确定第三安全算法。

其中，S406 的实现过程可以但不限于如下两种情况：

第一种情况，在“认证挑战请求消息携带两个安全算法的信息（即第一安全算法的信息和第二安全算法的信息）”的情况下，第三安全算法为第一安全算法，或第三安全算法为第二安全算法。其中，S406 的实现过程可以但不限于如下两种方式：

第一种方式，首先，终端设备根据认证挑战请求消息确定第一安全算法和第二安全算法。然后，终端设备根据第一安全算法的优先级和第二安全算法的优先级，从第一安全算法和第二安全算法中选择一个优先级较高的安全算法，作为第三安全算法。

第二种方式，在“认证挑战请求消息按照预设顺序携带第一安全算法的信息和第二安全算法的信息”的情况下，终端设备逐个识别认证挑战请求消息中安全算法的信息，直至识别出自身支持的安全算法的信息。此种情况下，终端设备识别出的安全算法为第三安全算法。也就是说，第三安全算法是在预设顺序中终端设备支持的首个安全算法。例如，认证挑战请求消息按照预设顺序携带 SHA256 的标识（即第一安全算法的信息）和 MD5 的标识（即第二安全算法的信息），终端设备支持 SHA256 的情况下，终端设备识别出认证挑战请求消息中 SHA256 的信息之后，将 SHA256 作为第三安全算法。

第二种情况，在“认证挑战请求消息携带三个安全算法的信息（即第一安全算法的信息、第二安全算法的信息和第四安全算法的信息）”的情况下，第三安全算法为第一安全算法，或第三安全算法为第二安全算法，或第三安全算法为第四安全算法。其中，S406 的实现过程可以但不限于如下两种方式：

第一种方式，首先，终端设备根据认证挑战请求消息确定第一安全算法、第二安全算法和第四安全算法。然后，终端设备根据第一安全算法的优先级、第二安全算法的优先级和第四安全算法的优先级，从第一安全算法、第二安全算法和第四安全算法中选择一个优先级较高的安全算法，作为第三安全算法。

第二种方式，在“认证挑战请求消息按照预设顺序携带第一安全算法的信息、第二安全算法的信息和第四安全算法的信息”的情况下，终端设备逐个识别认证挑战请求消息中安全算法的信息，直至识别出自身支持的安全算法的信息。此种情况下，终端设备识别出的安全算法为第三安全算法。

5 S407、终端设备根据第三安全算法计算安全参数的哈希值 HA1。

其中，第三安全算法是 S406 中终端设备确定的安全算法。例如，第三安全算法为 SHA256。

其中，安全参数是终端设备的配置参数。安全参数包括上述终端设备上登录的用户名称、密码和域信息。

10 示例性的，终端设备采用 SHA256（即第三安全算法）对用户名称、密码和域信息三个参数进行计算，以得到 SHA256（即第三安全算法）对应的 HA1。

S408、终端设备根据第三安全算法和哈希值 HA1 计算第一认证响应。

示例性的，仍以第三安全算法为 SHA256 为例，第一认证响应的计算过程如下：

首先，终端设备采用 SHA256 对 method 和 digest-uri 进行计算，以得到哈希值 HA2。

15 示例性的，哈希值 HA2 是如下参数拼接之后的哈希值：

HA2=method:digest-uri 的 SHA256 值

其中，method 表示 HTTP 请求的方法，digest-uri 表示 URI 的信息，“:”表示拼接。

然后，终端设备采用 SHA256 对 HA1、nonce、n-c、cnonce、qop、HA2 进行计算，以得到第一认证响应。其中，第一认证响应是如下参数拼接之后的哈希值：

20 response=HA1:nonce:n-c:cnonce:qop:HA2 的 SHA256 值

其中，response 表示第一认证响应，HA1 表示对用户名称、域信息和密码进行 SHA256 计算之后的哈希值，nonce 表示 S-CSCF 网元产生的一个随机数，n-c 表示 nonce-count，即终端设备使用相同 nonce 发送第二注册请求消息的计数器的计数值，cnonce 是终端设备产生的一个随机数，qop 的取值表示仅用于认证还是用于认证和消息体的完整性保护。哈希值 HA2 是采用 SHA256 算法对 method 和 digest-uri 进行拼接之后的哈希值：

HA2=method:digest-uri 的 SHA256 值

其中，method 表示 HTTP 请求的方法，digest-uri 表示 URI 的信息，“:”表示拼接。

S409、终端设备向 S-CSCF 网元发送第二注册请求消息。相应的，S-CSCF 网元接收来自终端设备的第二注册请求消息。

30 其中，第二注册请求消息包括第一认证响应和第三安全算法的信息。第二注册请求消息中携带的第一认证响应是 S408 中终端设备计算得到的第一认证响应。第三安全算法是 S407 中终端设备确定的第三安全算法。当然，第二注册请求消息还可以包括其他参数，详见 S141 的相关说明，此处不再赘述。

其中，S409 的实现过程可以参见 S141、S142 和 S143 的相关说明，此处不再赘述。

35 对于 S-CSCF 网元而言，分两种情况对该 S-CSCF 网元的执行过程进行介绍：

第一种情况，在 S404 的认证向量请求响应携带两个哈希值的情况下，S-CSCF 网元执行如图 4a 所示的 S410a：

S410a、S-CSCF 网元从第一哈希值 HA1 和第二哈希值 HA1 中选择第三安全算法对应的哈希值 HA1。

其中,第一哈希值 HA1 和第二哈希值 HA1 是 S404 的认证向量请求响应携带的哈希值。第三安全算法是 S-CSCF 网元基于 S409 中第二注册请求消息确定的安全算法。

其中, S410a 的实现过程可以但不限于如下两种方式:

5 第一种方式,在“认证向量请求响应按照预设顺序携带第一哈希值 HA1 和第二哈希值 HA1”的情况下, S-CSCF 网元根据预设顺序区分第一哈希值 HA1 和第二哈希值 HA1。S-CSCF 网元从第一哈希值 HA1 和第二哈希值 HA1 中选择第三安全算法对应的哈希值 HA1。具体地,若第三安全算法实现为第一安全算法,则 S-CSCF 网元确定第三安全算法对应的哈希值为第一哈希值 HA1。若第三安全算法实现为第二安全算法,则 S-CSCF 网元确定第三安全算法对应的哈希值为第二哈希值 HA1。

10 第二种方式,在“认证向量请求响应还携带第一安全算法的信息和第二安全算法的信息,且第一安全算法的信息与第一哈希值 HA1 之间存在对应关系,第二安全算法的信息与第二哈希值 HA1 之间存在对应关系”的情况下, S-CSCF 网元根据认证向量请求响应中的对应关系,从第一哈希值 HA1 和第二哈希值 HA1 中选择第三安全算法对应的哈希值 HA1。具体地,由于 S-CSCF 网元能够根据安全算法的信息区分第一安全算法和第二安全算法, S-CSCF 网元再结合上述对应关系也就能区分第一哈希值 HA1 和第二哈希值 HA1。若第三安全算法实现为第一安全算法,则 S-CSCF 网元确定第三安全算法对应的哈希值为第一哈希值 HA1。若第三安全算法实现为第二安全算法,则 S-CSCF 网元确定第三安全算法对应的哈希值为第二哈希值 HA1。

20 第二种情况,在 S404 的认证向量请求响应携带三个哈希值的情况下, S-CSCF 网元执行如图 4b 所示的 S410b:

S410b、S-CSCF 网元从第一哈希值 HA1、第二哈希值 HA1 和第三哈希值 HA1 中选择第三安全算法对应的哈希值 HA1。

25 其中,第一哈希值 HA1、第二哈希值 HA1 和第三哈希值 HA1 是 S404 的认证向量请求响应携带的哈希值。第三安全算法是 S-CSCF 网元基于 S409 中第二注册请求消息确定的安全算法。

其中, S410b 的实现过程可以但不限于如下两种方式:

30 第一种方式,在“认证向量请求响应按照预设顺序携带第一哈希值 HA1、第二哈希值 HA1 和第三哈希值 HA1”的情况下, S-CSCF 网元根据预设顺序区分第一哈希值 HA1、第二哈希值 HA1 和第三哈希值 HA1。S-CSCF 网元从第一哈希值 HA1、第二哈希值 HA1 和第三哈希值 HA1 中选择第三安全算法对应的哈希值 HA1,具体可以参见 S410a 的介绍,此处不再赘述。

35 第二种方式,在“认证向量请求响应还携带第一安全算法的信息、第二安全算法的信息和第四安全算法的信息,且第一安全算法的信息与第一哈希值 HA1 之间存在对应关系,第二安全算法的信息与第二哈希值 HA1 之间存在对应关系,第四安全算法的信息与第三哈希值 HA1 之间存在对应关系”的情况下, S-CSCF 网元根据认证向量请求响应中的对应关系,从第一哈希值 HA1 和第二哈希值 HA1 中选择第三安全算法对应的哈希值 HA1,具体可以参见 S41a 的介绍,此处不再赘述。

S411、S-CSCF 网元根据第三安全算法和第三安全算法对应的哈希值 HA1,计算第二认证响应。

其中，第三安全算法是 S-CSCF 网元基于 S409 中第二注册请求消息确定的安全算法，与第二注册请求消息中的第三安全算法一致。第三安全算法对应的哈希值 HA1 是 S-CSCF 网元基于 S410 中确定的哈希值。

示例性的，仍以第三安全算法为 SHA256 为例，第二认证响应的计算过程如下：

5 首先，S-CSCF 网元采用 SHA256 对 method 和 digest-uri 进行计算，以得到哈希值 HA2。

然后，S-CSCF 网元采用 SHA256 对 HA1、nonce、n-c、cnonce、qop、HA2 进行计算，以得到第二认证响应。

S412、S-CSCF 网元使用第二认证响应检验第一认证响应，得到终端设备的认证结果。

10 其中，第一认证响应是 S409 中第二注册请求消息携带的第一认证响应。第二认证响应是 S411 中 S-CSCF 网元计算得到的第二认证响应。

示例性的，在 S-CSCF 网元确定第一认证响应与第二认证响应不同的情况下，S-CSCF 网元确定终端设备认证失败。反之，在 S-CSCF 网元确定第一认证响应与第二认证响应相同的情况下，S-CSCF 网元确定终端设备认证成功，S-CSCF 网元向终端设备发送认证成功消息，详见 S151、S152 和 S153 的相关说明，此处不再赘述。

15 也就是说，终端设备能够结合认证挑战请求消息中的安全算法的信息，以及自身支持的安全算法，来确定一个安全算法，即第三安全算法，终端设备通过第三安全算法来计算第一认证响应。并且终端设备在第二注册请求消息中携带第三安全算法的信息，以向 S-CSCF 网元指示自身支持的安全算法。终端设备和 S-CSCF 网元即可基于相同的安全算法计算认证响应，S-CSCF 网元采用第二认证响应来校验第一认证响应，从而能够认证终端设备，避免由于终端设备和 S-CSCF 网元采用不同的安全算法，所导致的认证失败的现象。对于网络侧（如 S-CSCF 网元、HSS）而言，网络侧无需识别终端设备是否支持新的安全算法，统一采用上述图 4a 或图 4b 所示的方法即可，简化了网络侧的实现过程。

本申请实施例提供一种认证方法 500，该认证方法 500 应用在认证过程中。参见图 5，该认证方法 500 包括如下步骤：

25 S501、终端设备向 S-CSCF 网元发送第一注册请求消息。相应的，S-CSCF 网元接收来自终端设备的第一注册请求消息。

其中，第一注册请求消息的介绍可以参见 S111 中关于“第一注册请求消息”的相关说明，此处不再赘述。S501 的实现过程可以参见 S111、S112 和 S113 的相关说明，此处不再赘述。

30 S502、S-CSCF 网元向终端设备发送认证挑战请求消息。相应的，终端设备接收来自 S-CSCF 网元的认证挑战请求消息。

其中，S502 的实现过程可以参见 S131、S132 和 S133 的相关说明，此处不再赘述。

其中，通过两种情况对认证挑战请求消息进行介绍：

35 第一种情况，认证挑战请求消息携带两个安全算法，即第一安全算法的信息和第二安全算法的信息。其中，第一安全算法为 SHA256，第二安全算法为 MD5 算法。或者，第一安全算法为 SHA512，第二安全算法为 MD5 算法。或者，第一安全算法为 SHA256，第二安全算法为 SHA512。当然，认证挑战请求消息还可以包括其他参数，详见 S131 的相关说明，此处不再赘述。在一些实施方式中，认证挑战请求消息按照预设顺序携带第一安全算法的信息和第二安全算法的信息，具体可以参见方法 400 中 S405 第一种情况的介绍，此

处不再赘述。

第二种情况，认证挑战请求消息携带三个安全算法，即第一安全算法的信息、第二安全算法的信息和第四安全算法的信息。例如，第一安全算法为 SHA256，第二安全算法为 SHA512，第四安全算法为 MD5 算法。在一些实施方式中，认证挑战请求消息按照预设顺序携带第一安全算法的信息、第二安全算法的信息和第四安全算法，具体可以参见方法 400 中 S405 第二种情况的介绍，此处不再赘述。

S503、终端设备确定第三安全算法。

其中，S503 的实现过程可以但不限于如下两种情况：

第一种情况，在“认证挑战请求消息携带两个安全算法的信息（即第一安全算法的信息和第二安全算法的信息）”的情况下，第三安全算法为第一安全算法，或第三安全算法为第二安全算法。其中，S503 的具体实现过程可以参见 S406 中第一种情况的介绍，此处不再赘述。

第二种情况，在“认证挑战请求消息携带三个安全算法的信息（即第一安全算法的信息、第二安全算法的信息和第四安全算法的信息）”的情况下，第三安全算法为第一安全算法，或第三安全算法为第二安全算法，或第三安全算法为第四安全算法。其中，S503 的具体实现过程可以参见 S406 中第一种情况的介绍，此处不再赘述。

S504、终端设备根据第三安全算法计算安全参数的哈希值 HA1。

其中，第三安全算法是 S503 中终端设备确定的安全算法。例如，第三安全算法为 SHA256。

其中，安全参数是终端设备的配置参数。安全参数包括上述终端设备上登录的用户名称、密码和域信息。

示例性的，终端设备采用 SHA256（即第三安全算法）对用户名称、密码和域信息三个参数进行计算，以得到 SHA256（即第三安全算法）对应的 HA1。

S505、终端设备根据第三安全算法和哈希值 HA1 计算第一认证响应。

示例性的，仍以第三安全算法为 SHA256 为例，第一认证响应的计算过程如下：

首先，终端设备采用 SHA256 对 method 和 digest-uri 进行计算，以得到哈希值 HA2。

然后，终端设备采用 SHA256 对 HA1、nonce、n-c、cnonce、qop、HA2 进行计算，以得到第一认证响应。

S506、终端设备向 S-CSCF 网元发送第二注册请求消息。相应的，S-CSCF 网元接收来自终端设备的第二注册请求消息。

其中，第二注册请求消息包括第一认证响应和第三安全算法的信息。第二注册请求消息中携带的第一认证响应是 S505 中终端设备计算得到的第一认证响应。第三安全算法是 S503 中终端设备确定的第三安全算法。当然，第二注册请求消息还可以包括其他参数，详见 S141 的相关说明，此处不再赘述。

其中，S506 的实现过程可以参见 S141、S142 和 S143 的相关说明，此处不再赘述。

S507、S-CSCF 网元向 HSS 发送认证向量请求消息。相应的，HSS 接收来自 S-CSCF 网元的认证向量请求消息。

其中，认证向量请求消息包括第三安全算法的信息。第三安全算法与 S506 中第二注册请求消息中的第三安全算法一致。

其中，S507 的实现过程可以参见 S121 的相关说明，此处不再赘述。

S508、HSS 根据第三安全算法计算安全参数的哈希值 HA1。

其中，第三安全算法是 HSS 基于 S507 中认证向量请求消息确定的，与认证向量请求消息中的第三安全算法一致。

5 其中，安全参数包括上述终端设备上登录的用户名称、密码和域信息。

示例性的，在第三安全算法为 SHA256 的情况下，HSS 采用 SHA256（即第三安全算法）对用户名称、密码和域信息三个参数进行计算，以得到 SHA256（即第三安全算法）对应的哈希值 HA1。

10 S509、HSS 向 S-CSCF 网元发送认证向量请求响应。相应的，S-CSCF 网元接收来自 HSS 的认证向量请求响应。

其中，认证向量请求响应携带哈希值 HA1。哈希值 HA1 是 S508 中 HSS 计算得到的哈希值 HA1。当然，认证向量请求响应中还可以包括其他参数，详见 S122 的相关说明，此处不再赘述。

15 S510、S-CSCF 网元根据第三安全算法和第三安全算法对应的哈希值 HA1，计算第二认证响应。

其中，第三安全算法是 S-CSCF 网元基于 S506 中第二注册请求消息确定的安全算法，与第二注册请求消息中的第三安全算法一致。

示例性的，仍以第三安全算法为 SHA256 为例，第二认证响应的计算过程如下：

首先，S-CSCF 网元采用 SHA256 对 method 和 digest-uri 进行计算，以得到哈希值 HA2。

20 然后，S-CSCF 网元采用 SHA256 对 HA1、nonce、n-c、cnonce、qop、HA2 进行计算，以得到第二认证响应。

S511、S-CSCF 网元使用第二认证响应检验第一认证响应，得到终端设备的认证结果。

其中，第一认证响应是 S509 中第二注册请求消息携带的第一认证响应。第二认证响应是 S510 中 S-CSCF 网元计算得到的第二认证响应。

25 示例性的，在 S-CSCF 网元确定第一认证响应与第二认证响应不同的情况下，S-CSCF 网元确定终端设备认证失败。反之，在 S-CSCF 网元确定第一认证响应与第二认证响应相同的情况下，S-CSCF 网元确定终端设备认证成功，S-CSCF 网元向终端设备发送认证成功消息，详见 S151、S152 和 S153 的相关说明，此处不再赘述。

30 也就是说，终端设备能够结合认证挑战请求消息中的安全算法的信息，以及自身支持的安全算法，来确定一个安全算法，即第三安全算法，终端设备通过第三安全算法来计算第一认证响应。并且终端设备在第二注册请求消息中携带第三安全算法的信息，以向 S-CSCF 网元指示自身支持的安全算法。终端设备和 S-CSCF 网元即可基于相同的安全算法计算认证响应，S-CSCF 网元采用第二认证响应来校验第一认证响应，从而能够认证终端设备，避免由于终端设备和 S-CSCF 网元采用不同的安全算法，所导致的认证失败的现象。

35 对于 S-CSCF 网元和 HSS 之间的交互过程而言，认证向量请求消息中携带了终端设备支持的安全算法，即第三安全算法，所以，HSS 也就能向 S-CSCF 网元提供第三安全算法对应的哈希值 HA1，以使 S-CSCF 网元基于 HSS 网元提供的第三安全算法的 HA1 计算第二认证响应。对于网络侧（如 S-CSCF 网元、HSS）而言，网络侧无需识别终端设备是否支持新的安全算法，统一采用上述图 5 所示的方法即可，简化了网络侧的实现过程。

上述主要从各个网元之间交互的角度对本申请实施例提供的方案进行了介绍。相应的,本申请实施例还提供了通信装置,该通信装置可以为上述方法实施例中的网元,或者包含上述网元的装置,或者为可用于网元的部件。可以理解的是,该通信装置为了实现上述功能,其包含了执行各个功能相应的硬件结构和/或软件模块。本领域技术人员应该很容易意识到,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,本申请能够以硬件或硬件和计算机软件的结合形式来实现。某个功能究竟以硬件还是计算机软件驱动硬件的方式来执行,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。

10 本申请实施例提供一种芯片,该芯片包括逻辑电路和输入输出接口。其中,输入输出接口用于与芯片之外的模块通信,逻辑电路用于执行上述方法实施例中终端设备上除了收发操作之外的其他操作。

比如,以芯片实现为上述方法实施例图 3 的终端设备的功能为例,输入输出接口可以用于执行本申请实施例中终端设备侧的 S301、S305、S308,和/或输入输出接口还用于执行本申请实施例中终端设备侧的其他收发步骤。逻辑电路可以用于执行本申请实施例中终端设备侧的 S306、S307,和/或逻辑电路还用于执行本申请实施例中终端设备侧的其他处理步骤。

再如,以芯片实现为上述方法实施例图中图 4a(或图 4b)的终端设备的功能为例,输入输出接口可以用于执行终端设备侧的 S401、S405、S409,和/或输入输出接口还用于执行本申请实施例中终端设备侧的其他收发步骤。逻辑电路可以用于执行终端设备侧中的 S406、S407、S408,和/或逻辑电路还用于执行本申请实施例中终端设备侧的其他处理步骤。

又如,以芯片实现为上述方法实施例图中图 5 的终端设备的功能为例,输入输出接口可以用于执行终端设备侧的 S501、S502、S506,和/或输入输出接口还用于执行本申请实施例中终端设备侧的其他收发步骤。逻辑电路可以用于执行终端设备侧中的 S503、S504、S505,和/或逻辑电路还用于执行本申请实施例中终端设备侧的其他处理步骤。

比如,以芯片实现为上述方法实施例图 3 的服务呼叫会话控制功能网元的功能为例,输入输出接口可以用于执行本申请实施例中服务呼叫会话控制功能网元侧的 S301、S302、S304、S305、S308,和/或输入输出接口还用于执行本申请实施例中服务呼叫会话控制功能网元侧的其他收发步骤。逻辑电路可以用于执行本申请实施例中服务呼叫会话控制功能网元侧的 S309、S310,和/或逻辑电路还用于执行本申请实施例中服务呼叫会话控制功能网元侧的其他处理步骤。

再如,以芯片实现为上述方法实施例图中图 4a 的服务呼叫会话控制功能网元的功能为例,输入输出接口可以用于执行服务呼叫会话控制功能网元侧的 S401、S402、S404、S405、S409,和/或输入输出接口还用于执行本申请实施例中服务呼叫会话控制功能网元侧的其他收发步骤。逻辑电路可以用于执行服务呼叫会话控制功能网元侧中的 S410a、S411、S412,和/或逻辑电路还用于执行本申请实施例中服务呼叫会话控制功能网元侧的其他处理步骤。

又如，以芯片实现为上述方法实施例图中 4b 的服务呼叫会话控制功能网元的功能为例，输入输出接口可以用于执行服务呼叫会话控制功能网元侧的 S401、S402、S404、S405、S409，和/或输入输出接口还用于执行本申请实施例中服务呼叫会话控制功能网元侧的其他收发步骤。逻辑电路可以用于执行服务呼叫会话控制功能网元侧中的 S410b、S411、S412，和/或逻辑电路还用于执行本申请实施例中服务呼叫会话控制功能网元侧的其他处理步骤。

又如，以芯片实现为上述方法实施例图中 5 的服务呼叫会话控制功能网元的功能为例，输入输出接口可以用于执行服务呼叫会话控制功能网元侧的 S501、S502、S506、S507、S509，和/或输入输出接口还用于执行本申请实施例中服务呼叫会话控制功能网元侧的其他收发步骤。逻辑电路可以用于执行服务呼叫会话控制功能网元侧中的 S510、S511，和/或逻辑电路还用于执行本申请实施例中服务呼叫会话控制功能网元侧的其他处理步骤。

比如，以芯片实现为上述方法实施例图 3 的归属签约用户服务器的功能为例，输入输出接口可以用于执行本申请实施例中归属签约用户服务器侧的 S302、S304，和/或输入输出接口还用于执行本申请实施例中归属签约用户服务器侧的其他收发步骤。逻辑电路可以用于执行本申请实施例中归属签约用户服务器侧的 S303，和/或逻辑电路还用于执行本申请实施例中归属签约用户服务器侧的其他处理步骤。

再如，以芯片实现为上述方法实施例图中 4a 的归属签约用户服务器的功能为例，输入输出接口可以用于执行归属签约用户服务器侧的 S402、S404，和/或输入输出接口还用于执行本申请实施例中归属签约用户服务器侧的其他收发步骤。逻辑电路可以用于执行归属签约用户服务器侧中的 S403a，和/或逻辑电路还用于执行本申请实施例中归属签约用户服务器侧的其他处理步骤。

又如，以芯片实现为上述方法实施例图中 4b 的归属签约用户服务器的功能为例，输入输出接口可以用于执行归属签约用户服务器侧的 S402、S404，和/或输入输出接口还用于执行本申请实施例中归属签约用户服务器侧的其他收发步骤。逻辑电路可以用于执行归属签约用户服务器侧中的 S403b，和/或逻辑电路还用于执行本申请实施例中归属签约用户服务器侧的其他处理步骤。

又如，以芯片实现为上述方法实施例图中 5 的归属签约用户服务器的功能为例，输入输出接口可以用于执行归属签约用户服务器侧的 S507、S509，和/或输入输出接口还用于执行本申请实施例中归属签约用户服务器侧的其他收发步骤。逻辑电路可以用于执行归属签约用户服务器侧中的 S508，和/或逻辑电路还用于执行本申请实施例中归属签约用户服务器侧的其他处理步骤。

图 6 示出了一种通信装置 600 的结构示意图。该通信装置 600 可以以软件的形式存在，也可以为设备，或者设备中的组件。

该通信装置 600 包括处理单元 602、发送单元 603 和接收单元 604。

发送单元 603 是该通信装置 600 的一种接口电路，用于向其它装置发送信号。例如，当该通信装置 600 以芯片的方式实现时，该发送单元 603 是该芯片用于向其它芯片或装置发送信号的接口电路。

接收单元 604 是该通信装置 600 的一种接口电路，用于从其它装置接收信号。例

如，当该通信装置 600 以芯片的方式实现时，该接收单元 604 是该芯片用于从其它芯片或装置接收信号的接口电路。

比如，当通信装置 600 用于实现上述终端设备的功能时，示例性的，以图 3 为例，处理单元 602 可以用于支持通信装置 600 执行图 3 中的 S306、S307，和/或用于本文所描述的方案的其它过程。发送单元 603 用于支持通信装置 600 和其他网元之间的通信。比如，发送单元 603 用于支持通信装置 600 执行图 3 所示的 S301、S308，和/或用于本文所描述的方案的其它过程。接收单元 604 用于支持通信装置 600 和其他网元之间的通信。比如，接收单元 604 用于支持通信装置 600 执行图 3 所示的 S305，和/或用于本文所描述的方案的其它过程。

以图 4a（或图 4b）为例，处理单元 602 可以用于支持通信装置 600 执行图 4a（或图 4b）中的 S406、S407、S408，和/或用于本文所描述的方案的其它过程。发送单元 603 用于支持通信装置 600 和其他网元之间的通信。比如，发送单元 603 用于支持通信装置 600 执行图 4a（或图 4b）所示的 S401、S409，和/或用于本文所描述的方案的其它过程。接收单元 604 用于支持通信装置 600 和其他网元之间的通信。比如，接收单元 604 用于支持通信装置 600 执行图 4a（或图 4b）所示的 S405，和/或用于本文所描述的方案的其它过程。

以图 5 为例，处理单元 602 可以用于支持通信装置 600 执行图 5 中的 S503、S504、S505，和/或用于本文所描述的方案的其它过程。发送单元 603 用于支持通信装置 600 和其他网元之间的通信。比如，发送单元 603 用于支持通信装置 600 执行图 5 所示的 S501、S506，和/或用于本文所描述的方案的其它过程。接收单元 604 用于支持通信装置 600 和其他网元之间的通信。比如，接收单元 604 用于支持通信装置 600 执行图 5 所示的 S502，和/或用于本文所描述的方案的其它过程。

比如，当通信装置 600 用于实现上述服务呼叫会话控制功能网元的功能时，示例性的，以图 3 为例，处理单元 602 可以用于支持通信装置 600 执行图 3 中的 S309、S310，和/或用于本文所描述的方案的其它过程。发送单元 603 用于支持通信装置 600 和其他网元之间的通信。比如，发送单元 603 用于支持通信装置 600 执行图 3 所示的 S302，和/或用于本文所描述的方案的其它过程。接收单元 604 用于支持通信装置 600 和其他网元之间的通信。比如，接收单元 604 用于支持通信装置 600 执行图 3 所示的 S301、S304、S308，和/或用于本文所描述的方案的其它过程。

以图 4a 为例，处理单元 602 可以用于支持通信装置 600 执行图 4a 中的 S410a、S411、S412，和/或用于本文所描述的方案的其它过程。发送单元 603 用于支持通信装置 600 和其他网元之间的通信。比如，发送单元 603 用于支持通信装置 600 执行图 4a 所示的 S402，和/或用于本文所描述的方案的其它过程。接收单元 604 用于支持通信装置 600 和其他网元之间的通信。比如，接收单元 604 用于支持通信装置 600 执行图 4a 所示的 S401、S404、S409，和/或用于本文所描述的方案的其它过程。

以图 4b 为例，处理单元 602 可以用于支持通信装置 600 执行图 4b 中的 S410b、S411、S412，和/或用于本文所描述的方案的其它过程。发送单元 603 用于支持通信装置 600 和其他网元之间的通信。比如，发送单元 603 用于支持通信装置 600 执行图 4b 所示的 S402，和/或用于本文所描述的方案的其它过程。接收单元 604 用于支持通信装

置 600 和其他网元之间的通信。比如，接收单元 604 用于支持通信装置 600 执行图 4b 所示的 S401、S404、S409，和/或用于本文所描述的方案的其它过程。

以图 5 为例，处理单元 602 可以用于支持通信装置 600 执行图 5 中的 S510、S511，和/或用于本文所描述的方案的其它过程。发送单元 603 用于支持通信装置 600 和其他网元之间的通信。比如，发送单元 603 用于支持通信装置 600 执行图 5 所示的 S502、S507，和/或用于本文所描述的方案的其它过程。接收单元 604 用于支持通信装置 600 和其他网元之间的通信。比如，接收单元 604 用于支持通信装置 600 执行图 5 所示的 S501、S506、S509，和/或用于本文所描述的方案的其它过程。

比如，当通信装置 600 用于实现上述归属签约用户服务器的功能时，示例性的，以图 3 为例，处理单元 602 可以用于支持通信装置 600 执行图 3 中的 S303，和/或用于本文所描述的方案的其它过程。发送单元 603 用于支持通信装置 600 和其他网元之间的通信。比如，发送单元 603 用于支持通信装置 600 执行图 3 所示的 S304，和/或用于本文所描述的方案的其它过程。接收单元 604 用于支持通信装置 600 和其他网元之间的通信。比如，接收单元 604 用于支持通信装置 600 执行图 3 所示的 S302，和/或用于本文所描述的方案的其它过程。

以图 4a 为例，处理单元 602 可以用于支持通信装置 600 执行图 4a 中的 S403a，和/或用于本文所描述的方案的其它过程。发送单元 603 用于支持通信装置 600 和其他网元之间的通信。比如，发送单元 603 用于支持通信装置 600 执行图 4a 所示的 S404，和/或用于本文所描述的方案的其它过程。接收单元 604 用于支持通信装置 600 和其他网元之间的通信。比如，接收单元 604 用于支持通信装置 600 执行图 4a 所示的 S402，和/或用于本文所描述的方案的其它过程。

以图 4b 为例，处理单元 602 可以用于支持通信装置 600 执行图 4b 中的 S403b，和/或用于本文所描述的方案的其它过程。发送单元 603 用于支持通信装置 600 和其他网元之间的通信。比如，发送单元 603 用于支持通信装置 600 执行图 4b 所示的 S404，和/或用于本文所描述的方案的其它过程。接收单元 604 用于支持通信装置 600 和其他网元之间的通信。比如，接收单元 604 用于支持通信装置 600 执行图 4b 所示的 S402，和/或用于本文所描述的方案的其它过程。

以图 5 为例，处理单元 602 可以用于支持通信装置 600 执行图 5 中的 S508，和/或用于本文所描述的方案的其它过程。发送单元 603 用于支持通信装置 600 和其他网元之间的通信。比如，发送单元 603 用于支持通信装置 600 执行图 5 所示的 S509，和/或用于本文所描述的方案的其它过程。接收单元 604 用于支持通信装置 600 和其他网元之间的通信。比如，接收单元 604 用于支持通信装置 600 执行图 5 所示的 S507，和/或用于本文所描述的方案的其它过程。

可选的，通信装置 600 还可以包括存储单元 601，用于存储通信装置 600 的程序代码和数据，数据可以包括不限于原始数据或者中间数据等。

其中，处理单元 602 可以是处理器或控制器，例如可以是中央处理器（central processing unit, CPU），通用处理器，数字信号处理器（digital signal processor, DSP），专用集成电路（application specific integrated circuit, ASIC），现成可编程门阵列（field programmable gate array, FPGA）或者其他可编程逻辑器件、晶体管逻辑器件、硬件

部件或者其任意组合。其可以实现或执行结合本申请公开内容所描述的各种示例性的逻辑方框，模块和电路。处理器也可以是实现计算功能的组合，例如包含一个或多个微处理器组合，DSP和微处理器的组合等等。

发送单元 603 和接收单元 604 可以是通信接口、收发器或收发电路等，其中，该
5 通信接口是统称，在具体实现中，该通信接口可以包括多个接口。

存储单元 601 可以是存储器。

当处理单元 602 包括处理器，发送单元 603 和接收单元 604 包括通信接口，存储
单元 601 包括存储器时，本申请实施例所涉及的通信装置 700 可以为图 7 所示。

参阅图 7 所示，该通信装置 700 包括：至少一个处理器 702、收发器 703、存储器
10 701。

其中，收发器 703 可以为独立设置的发送器，该发送器可用于向其他设备发送信息，该收发器也可以为独立设置的接收器，用于从其他设备接收信息。该收发器也可以是将发送、接收信息功能集成在一起的部件，本申请实施例对收发器的具体实现不做限制。

15 可选的，通信装置 700 还可以包括总线 704。其中，收发器 703、处理器 702 以及存储器 701 可以通过总线 704 相互连接；总线 704 可以包括外设部件互连标准（peripheral component interconnect, PCI）总线或扩展工业标准结构（extended industry standard architecture, EISA）总线等。所述总线 704 可以分为地址总线、数据总线、控制总线等。为便于表示，图 7 中仅用一条粗线表示，但并不表示仅有一根总线或一
20 种类型的总线。

本领域普通技术人员可以理解：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。所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机程序指令时，全部或部分地产生按照本申请实施例所述的流程
25 或功能。所述计算机可以包括通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令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，所述计算机指令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、
30 计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以包括计算机能够存取的任何可用介质或者是包括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。所述可用介质可以包括磁性介质，（例如，软盘、硬盘、磁带）、光介质（例如，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。

35 在本申请所提供的几个实施例中，应该理解到，所揭露的系统，装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些

接口，装置或单元的间接耦合或通信连接，可以是电性或其它的形式。

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

另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个功能单元独立存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用硬件加软件功能单元的形式实现。

通过以上的实施方式的描述，所属领域的技术人员可以清楚地了解到本申请可借助软件加必需的通用硬件的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在可读取的存储介质中，如计算机的软盘，硬盘或光盘等，包括若干指令用以使得一台计算机设备（可以包括个人计算机，服务器，或者网络设备等等）执行本申请各个实施例所述的方法。

以上所述，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，在本申请揭露的技术范围内的变化或替换，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所述权利要求的保护范围为准。

1.一种认证方法，其特征在于，包括：

归属签约用户服务器接收来自服务呼叫会话控制功能网元的认证向量请求消息；

所述归属签约用户服务器根据第一安全算法计算安全参数的第一哈希值；

5 所述归属签约用户服务器根据第二安全算法计算安全参数的第二哈希值；

所述归属签约用户服务器向所述服务呼叫会话控制功能网元返回认证向量请求响应，其中，所述认证向量请求响应携带所述第一哈希值和所述第二哈希值。

2.根据权利要求1所述的方法，其特征在于，所述认证向量请求响应包括按照预设顺序携带的所述第一哈希值和所述第二哈希值，且所述预设顺序是基于所述第一安全算法的
10 优先级和所述第二安全算法的优先级确定的。

3.一种认证方法，其特征在于，包括：

服务呼叫会话控制功能网元接收来自终端设备的第一注册请求消息；

所述服务呼叫会话控制功能网元向归属签约用户服务器发送认证向量请求消息；

15 所述服务呼叫会话控制功能网元接收所述归属签约用户服务器返回的认证向量请求响应，其中，所述认证向量请求响应携带第一哈希值和第二哈希值，所述第一哈希值是基于第一安全算法计算的，所述第二哈希值是基于第二安全算法计算的；

所述服务呼叫会话控制功能网元向所述终端设备发送认证挑战请求消息，其中，所述认证挑战请求消息携带所述第一安全算法的信息和所述第二安全算法的信息；

20 所述服务呼叫会话控制功能网元接收来自所述终端设备的第二注册请求消息，其中，所述第二注册请求消息包括第一认证响应和第三安全算法的信息，所述第一认证响应是基于所述第三安全算法计算的，所述第三安全算法是所述第一安全算法或所述第二安全算法；

所述服务呼叫会话控制功能网元从所述第一哈希值和所述第二哈希值中选择所述第三安全算法对应的哈希值；

25 所述服务呼叫会话控制功能网元根据所述第三安全算法和所述第三安全算法对应的哈希值计算第二认证响应；

所述服务呼叫会话控制功能网元使用所述第二认证响应校验所述第一认证响应，得到所述终端设备的认证结果。

4.根据权利要求3所述的方法，其特征在于，所述认证向量请求响应包括按照预设顺序携带的所述第一哈希值和所述第二哈希值，且所述预设顺序是基于所述第一安全算法的
30 优先级和所述第二安全算法的优先级确定的；

所述服务呼叫会话控制功能网元从所述第一哈希值和所述第二哈希值中选择所述第三安全算法对应的哈希值，包括：所述服务呼叫会话控制功能网元根据所述预设顺序，从所述第一哈希值和所述第二哈希值中选择所述第三安全算法对应的哈希值。

35 5.根据权利要求3或4所述的方法，其特征在于，所述认证挑战请求消息包括按照预设顺序携带的所述第一安全算法的信息和所述第二安全算法的信息，且所述预设顺序是基于所述第一安全算法的优先级和所述第二安全算法的优先级确定的。

6.一种认证方法，其特征在于，包括：

终端设备接收来自服务呼叫会话控制功能网元的认证挑战请求消息，其中，所述认证挑战请求消息携带第一安全算法的信息和第二安全算法的信息；

所述终端设备确定第三安全算法，其中，所述第三安全算法为所述第一安全算法或所述第二安全算法；

所述终端设备根据所述第三安全算法计算安全参数的哈希值；

所述终端设备根据所述第三安全算法和所述哈希值计算认证响应；

- 5 所述终端设备向所述服务呼叫会话控制功能网元发送注册请求消息，其中，所述注册请求消息携带所述认证响应，所述认证响应用于认证所述终端设备。

7.根据权利要求6所述的方法，其特征在于，所述认证挑战请求消息包括按照预设顺序携带的所述第一安全算法的信息和所述第二安全算法的信息，且所述预设顺序是基于所述第一安全算法的优先级和所述第二安全算法的优先级确定的。

- 10 8.根据权利要求6或7所述的方法，其特征在于，所述终端设备确定第三安全算法，包括：所述终端设备确定所述认证挑战请求消息中自身能够识别的首个安全算法为所述第三安全算法。

9.一种通信装置，其特征在于，包括：

接收单元，用于接收来自服务呼叫会话控制功能网元的认证向量请求消息；

- 15 处理单元，用于根据第一安全算法计算安全参数的第一哈希值；

所述处理单元，还用于根据第二安全算法计算安全参数的第二哈希值；

发送单元，用于向所述服务呼叫会话控制功能网元返回认证向量请求响应，其中，所述认证向量请求响应携带所述第一哈希值和所述第二哈希值。

- 20 10.根据权利要求9所述的装置，其特征在于，所述认证向量请求响应包括按照预设顺序携带的所述第一哈希值和所述第二哈希值，且所述预设顺序是基于所述第一安全算法的优先级和所述第二安全算法的优先级确定的。

11.一种通信装置，其特征在于，包括：

接收单元，用于接收来自终端设备的第一注册请求消息；

发送单元，用于向归属签约用户服务器发送认证向量请求消息；

- 25 所述接收单元，还用于接收所述归属签约用户服务器返回的认证向量请求响应，其中，所述认证向量请求响应携带第一哈希值和第二哈希值，所述第一哈希值是基于第一安全算法计算的，所述第二哈希值是基于第二安全算法计算的；

所述发送单元，还用于向所述终端设备发送认证挑战请求消息，其中，所述认证挑战请求消息携带所述第一安全算法的信息和所述第二安全算法的信息；

- 30 所述接收单元，还用于接收来自所述终端设备的第二注册请求消息，其中，所述第二注册请求消息包括第一认证响应和第三安全算法的信息，所述第一认证响应是基于所述第三安全算法计算的，所述第三安全算法是所述第一安全算法或所述第二安全算法；

处理单元，用于从所述第一哈希值和所述第二哈希值中选择所述第三安全算法对应的哈希值；

- 35 所述处理单元，还用于根据所述第三安全算法和所述第三安全算法对应的哈希值计算第二认证响应；

所述处理单元，还用于使用所述第二认证响应校验所述第一认证响应，得到所述终端设备的认证结果。

12.根据权利要求11所述的装置，其特征在于，所述认证向量请求响应包括按照预设

顺序携带的所述第一哈希值和所述第二哈希值，且所述预设顺序是基于所述第一安全算法的优先级和所述第二安全算法的优先级确定的；所述处理单元，具体用于：根据所述预设顺序，从所述第一哈希值和所述第二哈希值中选择所述第三安全算法对应的哈希值。

- 5 13.根据权利要求 11 或 12 所述的装置，其特征在于，所述认证挑战请求消息包括按照预设顺序携带的所述第一安全算法的信息和所述第二安全算法的信息，且所述预设顺序是基于所述第一安全算法的优先级和所述第二安全算法的优先级确定的。

14.一种通信装置，其特征在于，包括：

接收单元，用于接收来自服务呼叫会话控制功能网元的认证挑战请求消息，其中，所述认证挑战请求消息携带第一安全算法的信息和第二安全算法的信息；

- 10 处理单元，用于确定第三安全算法，其中，所述第三安全算法为所述第一安全算法或所述第二安全算法；

所述处理单元，还用于根据所述第三安全算法计算安全参数的哈希值；

所述处理单元，还用于根据所述第三安全算法和所述哈希值计算认证响应；

- 15 发送单元，用于向所述服务呼叫会话控制功能网元发送注册请求消息，其中，所述注册请求消息携带所述认证响应，所述认证响应用于认证所述通信装置。

15.根据权利要求 14 所述的装置，其特征在于，所述认证挑战请求消息包括按照预设顺序携带的所述第一安全算法的信息和所述第二安全算法的信息，且所述预设顺序是基于所述第一安全算法的优先级和所述第二安全算法的优先级确定的。

- 20 16.根据权利要求 14 或 15 所述的装置，其特征在于，所述处理单元，具体用于：确定所述认证挑战请求消息中自身能够识别的首个安全算法为所述第三安全算法。

17.根据权利要求 1 至 8 任一项所述的方法，或者，根据权利要求 9 至 16 任一项所述的装置，其特征在于，所述第一安全算法为安全散列算法 SHA256 或安全散列算法 SHA512；所述第二安全算法为消息摘要 MD5 算法。

18.一种认证方法，其特征在于，包括：

- 25 终端设备向服务呼叫会话控制功能网元发送第一注册请求消息，其中，所述第一注册请求消息携带所述终端设备能够支持的安全算法的信息；所述安全算法包括以下至少一项：第一安全算法或第二安全算法；

- 30 所述终端设备接收来自所述服务呼叫会话控制功能网元的认证挑战消息，其中，所述认证挑战消息包括第三安全算法的信息，所述第三安全算法为所述终端设备能够支持的安全算法中的一个；

所述终端设备根据所述第三安全算法计算安全参数的哈希值；

所述终端设备根据所述第三安全算法和所述哈希值计算认证响应；

所述终端设备向所述服务呼叫会话控制功能网元发送第二注册请求消息，其中，所述第二注册请求消息携带所述认证响应，所述认证响应用于认证所述终端设备。

- 35 19.一种认证方法，其特征在于，包括：

服务呼叫会话控制功能网元接收来自终端设备的第一注册请求消息，其中，所述第一注册请求消息包括所述终端设备能够支持的安全算法的信息；所述安全算法包括以下至少一项：第一安全算法或第二安全算法；

所述服务呼叫会话控制功能网元向归属签约用户服务器发送认证向量请求消息，其中，

所述认证向量请求消息包括所述终端设备能够支持的安全算法的信息；

所述服务呼叫会话控制功能网元接收所述归属签约用户服务器返回的认证向量请求响应，其中，所述认证向量请求响应包括哈希值以及第三安全算法的信息，所述哈希值是基于所述第三安全算法计算得到的，所述第三安全算法为所述终端设备能够支持的安全算法中的一个；

所述服务呼叫会话控制功能网元向所述终端设备发送认证挑战消息，其中，所述认证挑战消息包括所述第三安全算法的信息；

所述服务呼叫会话控制功能网元接收来自所述终端设备的第二注册请求消息，其中，所述第二注册请求消息携带第一认证响应；

所述服务呼叫会话控制功能网元根据所述第三安全算法和所述哈希值，计算第二认证响应；

所述服务呼叫会话控制功能网元使用所述第二认证响应检验所述第一认证响应，得到所述终端设备的认证结果。

20.一种认证方法，其特征在于，包括：

归属签约用户服务器接收来自服务呼叫会话控制功能网元的认证向量请求消息，其中，所述认证向量请求消息包括终端设备能够支持的安全算法的信息；所述安全算法包括以下至少一项：第一安全算法或第二安全算法；

所述归属签约用户服务器根据第三安全算法计算安全参数的哈希值，其中，所述第三安全算法为所述终端设备能够支持的安全算法中的一个；

所述归属签约用户服务器向所述服务呼叫会话控制功能网元返回认证向量请求响应，其中，所述认证向量请求响应携带所述哈希值以及所述第三安全算法的信息。

21.一种通信装置，其特征在于，包括：

发送单元，用于向服务呼叫会话控制功能网元发送第一注册请求消息，其中，所述第一注册请求消息携带所述通信装置能够支持的安全算法的信息；所述安全算法包括以下至少一项：第一安全算法或第二安全算法；

接收单元，用于接收来自所述服务呼叫会话控制功能网元的认证挑战消息，其中，所述认证挑战消息包括第三安全算法的信息，所述第三安全算法为所述通信装置能够支持的安全算法中的一个；

处理单元，用于根据所述第三安全算法计算安全参数的哈希值；

所述处理单元，还用于根据所述第三安全算法和所述哈希值计算认证响应；

所述发送单元，还用于向所述服务呼叫会话控制功能网元发送第二注册请求消息，其中，所述第二注册请求消息携带所述认证响应，所述认证响应用于认证所述通信装置。

22.一种通信装置，其特征在于，包括：

接收单元，用于接收来自终端设备的第一注册请求消息，其中，所述第一注册请求消息包括所述终端设备能够支持的安全算法的信息；所述安全算法包括以下至少一项：第一安全算法或第二安全算法；

发送单元，用于向归属签约用户服务器发送认证向量请求消息，其中，所述认证向量请求消息包括所述终端设备能够支持的安全算法的信息；

所述接收单元，还用于接收所述归属签约用户服务器返回的认证向量请求响应，其中，

所述认证向量请求响应包括哈希值以及第三安全算法的信息，所述哈希值是基于所述第三安全算法计算得到的，所述第三安全算法为所述终端设备能够支持的安全算法中的一个；

所述发送单元，还用于向所述终端设备发送认证挑战消息，其中，所述认证挑战消息包括所述第三安全算法的信息；

- 5 所述接收单元，还用于接收来自所述终端设备的第二注册请求消息，其中，所述第二注册请求消息携带第一认证响应；

处理单元，用于根据所述第三安全算法和所述哈希值，计算第二认证响应；

所述处理单元，还用于使用所述第二认证响应检验所述第一认证响应，得到所述终端设备的认证结果。

- 10 23.一种通信装置，其特征在于，包括：

接收单元，用于接收来自服务呼叫会话控制功能网元的认证向量请求消息，其中，所述认证向量请求消息包括终端设备能够支持的安全算法的信息；所述安全算法包括以下至少一项：第一安全算法或第二安全算法；

- 15 处理单元，用于根据第三安全算法计算安全参数的哈希值，其中，所述第三安全算法为所述终端设备能够支持的安全算法中的一个；

发送单元，用于向所述服务呼叫会话控制功能网元返回认证向量请求响应，其中，所述认证向量请求响应携带所述哈希值以及所述第三安全算法的信息。

- 20 24.根据权利要求18至20任一项所述的方法，或者，根据权利要求21至23任一项所述的装置，其特征在于，所述第一安全算法为安全散列算法 SHA256，所述第二安全算法为安全散列算法 SHA512。

25 25.一种通信装置，其特征在于，包括处理器和收发器，所述处理器用于执行权利要求1至8中任一项方法中的处理操作，所述收发器用于执行权利要求1至8中任一项方法中的通信操作；或者，所述处理器用于执行权利要求18至20中任一项方法中的处理操作，所述收发器用于执行权利要求18至20中任一项方法中的通信操作。

- 25 26.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质存储计算机指令，当所述计算机指令在计算机上运行时，使得所述计算机执行权利要求1至8任一项所述的方法，或使得所述计算机执行权利要求18至20任一项所述的方法。

- 30 27.一种计算机程序产品，其特征在于，当所述计算机程序产品在计算机上运行时，使得所述计算机执行权利要求1至8任一项所述的方法，或使得所述计算机执行权利要求18至20任一项所述的方法。

28.一种芯片，其特征在于，所述芯片包括处理电路和收发管脚；所述处理电路用于执行权利要求1至8中任一项方法中的处理操作，所述收发管脚用于执行权利要求1至8中任一项方法中的通信操作；或者，所述处理电路用于执行权利要求18至20中任一项方法中的处理操作，所述收发管脚用于执行权利要求18至20中任一项方法中的通信操作。

35