

(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
2016年7月7日 (07.07.2016)



(10) 国际公布号
WO 2016/107203 A1

- (51) 国际专利分类号:
H04L 29/06 (2006.01)
- (21) 国际申请号: PCT/CN2015/088636
- (22) 国际申请日: 2015年8月31日 (31.08.2015)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510003808.X 2015年1月4日 (04.01.2015) CN
- (71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。
- (72) 发明人: 王江胜 (WANG, Jiangsheng); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 林青春 (LIN, Qingchun); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。
- (74) 代理人: 北京同达信恒知识产权代理有限公司 (TDIP & PARTNERS); 中国北京市海淀区知春路7号致真大厦A1304-05室, Beijing 100191 (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, 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, KN, KP, KR, 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)。

[见续页]

(54) Title: IDENTITY AUTHENTICATION METHOD AND DEVICE

(54) 发明名称: 一种身份认证方法及装置

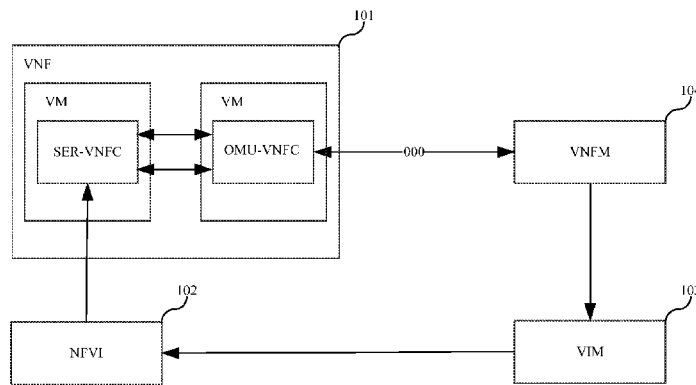


图 2 /Fig.2

(57) Abstract: Disclosed are an identity authentication method and device that are applied to a network function virtualization (NFV) system and can adapt to the dynamic change of the system. The NFV system comprises a virtual network function (VNF). The VNF comprises a first virtual network function component (VNFC) and a second VNFC. The authentication method comprises: generating a public key and a private key of a first VNFC and a public key and a private key of a second VNFC; writing or sending the private key of the first VNFC and the public key of the second VNFC into or to the first VNFC; and writing or sending the public key of the first VNFC and the private key of the second VNFC into or to the second VNFC, the public key and the private key of the first VNFC and the public key and the private key of the second VNFC being used for identity authentication of the first VNFC and the second VNFC.

(57) 摘要:

[见续页]



WO 2016/107203 A1



根据细则 4.17 的声明:

— 关于申请人有权申请并被授予专利(细则 4.17(ii))

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

本发明公开了一种身份认证方法及装置，应用于网络功能虚拟化 NFV 系统，能够适应系统的动态变化。该 NFV 系统包括虚拟网络功能 VNF，该 VNF 包括第一虚拟网络功能组成部分 VNFC 和第二 VNFC，该认证方法包括：生成第一 VNFC 的公钥和私钥，以及第二 VNFC 的公钥和私钥；将第一 VNFC 的私钥和第二 VNFC 的公钥写入或发送至第一 VNFC；以及将第一 VNFC 的公钥和第二 VNFC 的私钥写入或发送至第二 VNFC；其中，第一 VNFC 的公钥和私钥以及第二 VNFC 的公钥和私钥用于第一 VNFC 和第二 VNFC 进行身份认证。

一种身份认证方法及装置

技术领域

本发明涉及通信技术领域，尤其涉及一种应用于网络功能虚拟化（Network Function Virtualization, NFV）系统的身份认证方法及装置。

背景技术

虚拟网络功能（Virtual Network Function, VNF）为 NFV 系统的核心部分，每个 VNF 包括多个 VNF 组成部分（VNF Component, VNFC），各 VNFC 间通过内部虚拟网络实现通信。由于 VNF 中的各 VNFC 间通信通过了虚拟网络，为避免出现信息泄露、伪冒通信、篡改通信内容等安全风险，两个 VNFC 间初始建立通信时需要进行身份认证。

现有技术中，通常采用手工配置的方式在各 VNFC 上配置可信身份凭据，两个 VNFC 间初始建立通信时基于该手工配置的可信身份凭据进行身份认证。然而，NFV 系统中的 VNF 是动态变化的，手工配置可信身份凭据的方案效率较低，无法适应动态变化的 VNF。

发明内容

本发明实施例提供一种身份认证方法及装置，用以适应动态变化的 VNF。

第一方面，提供一种身份认证方法，应用于网络功能虚拟化 NFV 系统，所述 NFV 系统包括虚拟网络功能 VNF，所述 VNF 包括第一虚拟网络功能组成部分 VNFC 和第二 VNFC，所述方法包括：

生成所述第一 VNFC 的公钥和私钥，以及所述第二 VNFC 的公钥和私钥；
将所述第一 VNFC 的私钥和所述第二 VNFC 的公钥写入或发送至所述第一 VNFC；

将所述第一 VNFC 的公钥和所述第二 VNFC 的私钥写入或发送至所述第二 VNFC；其中，所述第一 VNFC 的公钥和私钥以及所述第二 VNFC 的公钥

和私钥用于所述第一 VNFC 和所述第二 VNFC 进行身份认证。

结合第一方面，在第一种可能的实现方式中，将所述第一 VNFC 的私钥和所述第二 VNFC 的公钥写入或发送至所述第一 VNFC，包括：

在生成所述第一 VNFC 时，将所述第一 VNFC 的私钥和所述第二 VNFC 的公钥写入所述第一 VNFC；或者

当所述第一 VNFC 为管理 VNFC 时，通过所述第一 VNFC 的管理通信通道，将所述第一 VNFC 的私钥和所述第二 VNFC 的公钥发送至所述第一 VNFC。

结合第一方面，或者结合第一方面的第一种可能的实现方式，在第二种可能的实现方式中，将所述第二 VNFC 的标识信息写入或发送至所述第一 VNFC；其中，所述第二 VNFC 的标识信息与所述第二 VNFC 的公钥的对应关系存储于所述第一 VNFC 中。

结合第一方面，第一方面的第一种可能的实现方式，或者第一方面的第二种可能的实现方式，在第三种可能的实现方式中，还包括：

将所述第一 VNFC 的标识信息写入或发送至所述第一 VNFC。

第二方面，提供一种身份认证方法，应用于网络功能虚拟化 NFV 系统，所述 NFV 系统包括虚拟网络功能 VNF，所述 VNF 包括第一虚拟网络功能组成部分 VNFC 和第二 VNFC，所述方法包括：

生成所述第一 VNFC 的专用密钥，以及所述第二 VNFC 的专用密钥；

将所述第一 VNFC 的专用密钥和所述第二 VNFC 的专用密钥写入或发送至所述第一 VNFC；

将所述第一 VNFC 的专用密钥和所述第二 VNFC 的专用密钥写入或发送至所述第二 VNFC；其中，所述第一 VNFC 的专用密钥以及所述第二 VNFC 的专用密钥用于所述第一 VNFC 和所述第二 VNFC 进行身份认证。

结合第二方面，在第一种可能的实现方式中，将所述第一 VNFC 的专用密钥和所述第二 VNFC 的专用密钥写入或发送至所述第一 VNFC，包括：

在生成所述第一 VNFC 时，将所述第一 VNFC 的专用密钥和所述第二

VNFC 的专用密钥写入所述第一 VNFC; 或者

当所述第一 VNFC 为管理 VNFC 时, 通过所述第一 VNFC 的管理通信通道, 将所述第一 VNFC 的专用密钥和所述第二 VNFC 的专用密钥发送至所述第一 VNFC。

结合第二方面, 或者结合第二方面的第一种可能的实现方式, 在第二种可能的实现方式中, 还包括:

将所述第二 VNFC 的标识信息写入或发送至所述第一 VNFC; 其中, 所述第二 VNFC 的标识信息与所述第二 VNFC 的专用密钥的对应关系存储于所述第一 VNFC 中。

结合第二方面, 第二方面的第一种可能的实现方式, 或者第二方面的第二种可能的实现方式, 在第三种可能的实现方式中, 还包括:

将所述第一 VNFC 的标识信息写入或发送至所述第一 VNFC。

第三方面, 提供一种身份认证装置, 应用于网络功能虚拟化 NFV 系统, 所述 NFV 系统包括虚拟网络功能 VNF, 所述 VNF 包括第一虚拟网络功能组成部分 VNFC 和第二 VNFC, 所述装置包括:

处理器, 用于生成所述第一 VNFC 的公钥和私钥, 以及所述第二 VNFC 的公钥和私钥;

输入输出接口, 用于将所述第一 VNFC 的私钥和所述第二 VNFC 的公钥写入或发送至所述第一 VNFC, 以及将所述第一 VNFC 的公钥和所述第二 VNFC 的私钥写入或发送至所述第二 VNFC; 其中, 所述第一 VNFC 的公钥和私钥以及所述第二 VNFC 的公钥和私钥用于所述第一 VNFC 和所述第二 VNFC 进行身份认证。

结合第三方面, 在第一种可能的实现方式中, 所述输入输出接口, 具体用于在生成所述第一 VNFC 时, 将所述第一 VNFC 的私钥和所述第二 VNFC 的公钥写入所述第一 VNFC; 或者当所述第一 VNFC 为管理 VNFC 时, 通过所述第一 VNFC 的管理通信通道, 将所述第一 VNFC 的私钥和所述第二 VNFC 的公钥发送至所述第一 VNFC。

结合第三方面，或者结合第三方面的第一种可能的实现方式，在第二种可能的实现方式中，所述输入输出接口，还用于将所述第二 VNFC 的标识信息写入或发送至所述第一 VNFC；其中，所述第二 VNFC 的标识信息与所述第二 VNFC 的公钥的对应关系存储于所述第一 VNFC 中。

结合第三方面，第三方面的第一种可能的实现方式，或者第三方面的第二种可能的实现方式，在第三种可能的实现方式中，所述输入输出接口，还用于将所述第一 VNFC 的标识信息写入或发送至所述第一 VNFC。

结合第三方面，第三方面的第一种可能的实现方式，第三方面的第二种可能的实现方式，或者第三方面的第三种可能的实现方式，在第四种可能的实现方式中，所述输入输出接口，包括写入器或发送器。

第四方面，提供一种身份认证装置，应用于网络功能虚拟化 NFV 系统，所述 NFV 系统包括虚拟网络功能 VNF，所述 VNF 包括第一虚拟网络功能组成部分 VNFC 和第二 VNFC，所述装置包括：

处理器，用于生成所述第一 VNFC 的专用密钥，以及所述第二 VNFC 的专用密钥；

输入输出接口，用于将所述第一 VNFC 的专用密钥和所述第二 VNFC 的专用密钥写入或发送至所述第一 VNFC，以及将所述第一 VNFC 的专用密钥和所述第二 VNFC 的专用密钥写入或发送至所述第二 VNFC；其中，所述第一 VNFC 的专用密钥以及所述第二 VNFC 的专用密钥用于所述第一 VNFC 和所述第二 VNFC 进行身份认证。

结合第四方面，在第一种可能的实现方式中，所述输入输出接口，具体用于在生成所述第一 VNFC 时，将所述第一 VNFC 的专用密钥和所述第二 VNFC 的专用密钥写入所述第一 VNFC；或者当所述第一 VNFC 为管理 VNFC 时，通过所述第一 VNFC 的管理通信通道，将所述第一 VNFC 的专用密钥和所述第二 VNFC 的专用密钥发送至所述第一 VNFC。

结合第四方面，或者结合第四方面的第一种可能的实现方式，在第二种可能的实现方式中，所述输入输出接口，还用于将所述第二 VNFC 的标识信

息写入或发送至所述第一 VNFC；其中，所述第二 VNFC 的标识信息与所述第二 VNFC 的对称密钥的对应关系存储于所述第一 VNFC 中。

结合第四方面，第四方面的第一种可能的实现方式，或者第四方面的第二种可能的实现方式，在第三种可能的实现方式中，所述输入输出接口，还用于将所述第一 VNFC 的标识信息写入或发送至所述第一 VNFC。

结合第四方面，第四方面的第一种可能的实现方式，第四方面的第二种可能的实现方式，或者第四方面的第三种可能的实现方式，在第四种可能的实现方式中，所述输入输出接口，包括写入器或发送器。

根据第一方面提供的身份认证方法，第二方面提供的身份认证方法，第三方面提供的身份认证装置，第四方面提供的身份认证装置，自动将身份凭据置入第一 VNFC 和第二 VNFC，基于置入的身份凭据，可以实现第一 VNFC 和第二 VNFC 间的身份认证，并且相比于现有技术，效率较高，能够适应动态变化的 VNF。

附图说明

附图用来提供对本发明的进一步理解，并且构成说明书的一部分，与本发明实施例一起用于解释本发明，并不构成对本发明的限制。在附图中：

图 1 为 NFV 系统架构的示意图；

图 2 为本发明实施例 1 提供的身份认证方案的示意图；

图 3 为本发明实施例 2 提供的身份认证方案的示意图；

图 4 为本发明实施例 3 提供的身份认证方案的示意图；

图 5 为本发明实施例 4 提供的身份认证方案的示意图；

图 6 为本发明实施例提供的身份认证方法的示意图之一；

图 7 为本发明实施例提供的身份认证流程的示意图之一；

图 8 为本发明实施例提供的身份认证方法的示意图之二；

图 9 为本发明实施例提供的身份认证流程的示意图之二；

图 10 为本发明实施例提供的身份认证装置的示意图之一；

图 11 为本发明实施例提供的身份认证装置的示意图之二。

具体实施方式

为了给出适应动态变化的 VNF 的身份认证方案，本发明实施例提供了一种身份认证方法及装置，以下结合说明书附图对本发明的优选实施例进行说明，应当理解，此处所描述的优选实施例仅用于说明和解释本发明，并不用于限定本发明。并且在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。

NFV 系统架构如图 1 所示，主要包括：

VNF 101，包括多个 VNFC，每个 VNFC 运行在一个虚拟机（Virtual Machine, VM）上；多个 VNFC 中，一个 VNFC 作为管理 VNFC（OMU-VNFC），其它 VNFC 均可以算作是业务 VNFC（SER-VNFC）；OMU-VNFC 统一对各 SER-VNFC 进行管理，通过管理通信通道 000 和 NFV 系统其它部分进行通信；

网络功能虚拟基础设施（Network Function Virtual Infrastructure, NFVI）102，包括虚拟计算资源、虚拟存储资源、虚拟网络资源等虚拟资源；

虚拟基础设施管理器（Virtual Infrastructure Manager, VIM）103，用于管理 NFVI，可以创建虚拟资源、VNF 以及 VNF 所需的网络连接；

VNF 管理器（VNF Manger, VNFM）104，用于对 VNF 的生命周期进行管理，例如 VNF 的建立、修改、销毁等，其中一些生命周期的管理操作例如 VNF 的建立需要通过 VIM 实现；

NFV 编排器（NFV Orchestra, NFVO）105，用于通过 VNFM 实现对 VNF 的管理，通过 VIM 实现对多个 VNF 的组网；

网元管理系统（Element Management System, EMS）106，用于将 VNF 作为网元进行管理，主要管理业务相关。

在本发明实施例中，VNF 至少包括第一 VNFC 和第二 VNFC，下面以第一 VNFC 与第二 VNFC 间的身份认证为例，用具体实施例对本发明实施例提供的身份认证方法进行详细描述。在下述具体实施例中，第一 VNFC 具体为

OMU-VNFC、第二 VNFC 具体为 SER-VNFC。

实施例 1:

在本发明实施例 1 中，VNF 的建立是由 VNFM 发起的，如图 2 所示，由 VNFM 生成建立 VNF 所需的全部配置信息，该配置信息中包括 OMU-VNFC 的公钥和私钥，以及 SER-VNFC 的公钥和私钥。

公钥和私钥是通过一种算法得到的一个密钥对，该密钥对的两个密钥中，非秘密的密钥称为公钥，秘密的密钥称为私钥。在使用该密钥对时，如果用公钥加密数据就必须用私钥解密，如果用私钥加密数据就必须用公钥解密，否则解密将不会成功。

VNFM 将 OMU-VNFC 的标识信息和私钥、SER-VNFC 的标识信息和公钥置入 OMU-VNFC，以及将 OMU-VNFC 的标识信息和公钥、SER-VNFC 的标识信息和私钥置入 SER-VNFC。

具体的，VNFM 可以将生成的建立 VNF 所需的全部配置信息下发给 VIM，并指示 VIM 在执行 OMU-VNFC 的生成时，将 OMU-VNFC 的标识信息和私钥、SER-VNFC 的标识信息和公钥写入至 OMU-VNFC；以及指示 VIM 在执行 SER-VNFC 的生成时，将 OMU-VNFC 的标识信息和公钥、SER-VNFC 的标识信息和私钥写入至 SER-VNFC。VIM 和 NFVI 配合实现 OMU-VNFC 的生成以及 SER-VNFC 的生成。

本领域技术人员可知晓，“写入”也可称为“注入”。

对于 OMU-VNFC，若 VNFM 与 OMU-VNFC 间的管理通信通道 000 已经建立，VNFM 也可以通过管理通信通道 000，将 OMU-VNFC 的标识信息和私钥、SER-VNFC 的标识信息和公钥发送至 OMU-VNFC，实现置入。

后续 OMU-VNFC 和 SER-VNFC 可以基于置入的公钥和私钥进行身份认证，具体的认证方式可参见后文图 7 的详述。

即在实施例 1 中，本发明实施例提供的身份认证方法的执行主体为 VNFM。

实施例 2:

在本发明实施例 2 中，VNF 的建立是由 EMS 发起的，如图 3 所示。

由 EMS 发起 VNF 的建立时，EMS 可以不参与公钥和私钥的生成，仍然由 VNFM 生成 OMU-VNFC 的公钥和私钥，以及 SER-VNFC 的公钥和私钥，后续置入步骤可参见上述实施例 1；此时，本发明实施例提供的身份认证方法的执行主体为 VNFM。

或者，EMS 也可以参与公钥和私钥的生成，即由 EMS 生成 OMU-VNFC 的公钥和私钥，以及 SER-VNFC 的公钥和私钥，EMS 将生成的 OMU-VNFC 的公钥和私钥，以及 SER-VNFC 的公钥和私钥再下发给 VNFM，并指示 VNFM 进行公钥和私钥的置入；此时，本发明实施例提供的身份认证方法的执行主体为 EMS。

实施例 3:

在本发明实施例 3 中，VNF 的建立是由 NFVO 发起的，如图 4 所示，NFVO 可以不参与公钥和私钥的生成，仍然由 VNFM 生成 OMU-VNFC 的公钥和私钥，以及 SER-VNFC 的公钥和私钥，后续置入步骤可参见上述实施例 1。

即在实施例 3 中，本发明实施例提供的身份认证方法的执行主体为 VNFM。

实施例 4:

在本发明实施例 4 中，VNF 的建立也是由 NFVO 发起的，如图 5 所示，由 NFVO 生成建立 VNF 所需的全部配置信息，该配置信息中包括 VNF 中 OMU-VNFC 的公钥和私钥，以及 SER-VNFC 的公钥和私钥。

NFVO 将 OMU-VNFC 的标识信息和私钥、SER-VNFC 的标识信息和公钥置入 OMU-VNFC，以及将 OMU-VNFC 的标识信息和公钥、SER-VNFC 的标识信息和私钥置入 SER-VNFC。

具体的，NFVO 将生成的建立 VNF 所需的全部配置信息下发给 VIM，并指示 VIM 在执行 OMU-VNFC 的生成时，将 OMU-VNFC 的标识信息和私钥、SER-VNFC 的标识信息和公钥写入 OMU-VNFC；以及指示 VIM 在执行 SER-VNFC 的生成时，将 OMU-VNFC 的标识信息和公钥、SER-VNFC 的标

识信息和私钥写入 OMU-VNFC。VIM 和 NFVI 配合实现 OMU-VNFC 的生成以及 SER-VNFC 的生成。

后续 OMU-VNFC 和 SER-VNFC 可以基于写入的公钥和私钥进行身份认证，具体的认证方式可参见后文图 7 的详述。

即在实施例 4 中，本发明实施例提供的身份认证方法的执行主体为 NFVO。

综上，本发明实施例提供了一种身份认证方法，应用于 NFV 系统，该 NFV 系统包括 VNF，该 VNF 包括第一 VNFC 和第二 VNFC，该身份认证方法如图 6 所示，具体可以包括如下步骤：

步骤 601、生成第一 VNFC 的公钥和私钥，以及第二 VNFC 的公钥和私钥；

步骤 602、将第一 VNFC 的私钥和第二 VNFC 的公钥写入或发送至第一 VNFC；

步骤 603、将第一 VNFC 的公钥和第二 VNFC 的私钥写入或发送至第二 VNFC；其中，第一 VNFC 的公钥和私钥以及第二 VNFC 的公钥和私钥用于第一 VNFC 和第二 VNFC 进行身份认证。

需要说明的是，上述步骤 602 和步骤 603 没有必然的先后执行顺序。

在一个具体实施例中，可以在生成第一 VNFC 时，将第一 VNFC 的私钥和第二 VNFC 的公钥写入第一 VNFC。在另一个具体实施例中，当第一 VNFC 为 OMU-VNFC 时，若第一 VNFC 的管理通信通道已经建立，也可以通过第一 VNFC 的管理通信通道，将第一 VNFC 的私钥和第二 VNFC 的公钥发送至第一 VNFC。

相应的，在一个具体实施例中，可以在生成第二 VNFC 时，将第一 VNFC 的公钥和第二 VNFC 的私钥写入第二 VNFC。在另一个具体实施例中，当第二 VNFC 为 OMU-VNFC 时，若第二 VNFC 的管理通信通道已经建立，也可以通过第二 VNFC 的管理通信通道，将第一 VNFC 的公钥和第二 VNFC 的私钥发送至第二 VNFC。

即在本发明实施例中，将第一 VNFC 的私钥和第二 VNFC 的公钥置入第一 VNFC、将第一 VNFC 的公钥和第二 VNFC 的私钥置入第二 VNFC，基于置入的公钥和私钥，第一 VNFC 和第二 VNFC 间可以基于非对称加密算法进行身份认证，具体方式本发明不做具体限定。

例如，在一个具体实施例中，在将第一 VNFC 的私钥和第二 VNFC 的公钥写入或发送至第一 VNFC 时，还可以将第一 VNFC 的标识信息一并写入或发送至第一 VNFC；在将第一 VNFC 的公钥和第二 VNFC 的私钥写入或发送至第二 VNFC 时，还可以将第二 VNFC 的标识信息一并写入或发送至第二 VNFC；然后第一 VNFC 和第二 VNFC 间可以采用图 7 所示的身份认证流程，具体包括如下步骤：

步骤 701、第一 VNFC 生成第一原始信息的第一摘要，并采用第一 VNFC 的私钥对第一原始信息的第一摘要进行加密，得到第一加密信息；其中，第一原始信息包含第一 VNFC 的标识信息，还可以包含第一 VNFC 向第二 VNFC 的通信连接请求。

步骤 702、第一 VNFC 将向第二 VNFC 发送携带第一原始信息和第一加密信息的认证请求。

步骤 703、第二 VNFC 接收第一 VNFC 发送的携带第一原始信息和第一加密信息的认证请求，之后，第二 VNFC 生成第一原始信息的第二摘要，以及采用第一 VNFC 的公钥对第一加密信息进行解密，得到第一解密信息。

步骤 704、判断第一原始信息的第二摘要和第一解密信息是否相同。

当第一原始信息的第二摘要和第一解密信息不相同，第二 VNFC 对第一 VNFC 身份认证失败，结束该认证流程，两个 VNFC 间不建立通信连接；

当第一原始信息的第二摘要和第一解密信息相同时，第二 VNFC 对第一 VNFC 身份认证通过，进入步骤 705。

步骤 705、第二 VNFC 生成第二原始信息的第一摘要，并采用第二 VNFC 的私钥对第二原始信息的第一摘要进行加密，得到第二加密信息；其中，第二原始信息包含第二 VNFC 的标识信息，还可以包含第二 VNFC 向第一 VNFC

的通信连接请求。

步骤 706、第二 VNFC 向第一 VNFC 发送携带第二原始信息和第二加密信息的认证请求。

步骤 707、第一 VNFC 接收第二 VNFC 发送的携带第二原始信息和第二加密信息的认证请求，之后，第一 VNFC 生成第二原始信息的第二摘要，以及采用第二 VNFC 的公钥对第二加密信息进行解密，得到第二解密信息。

步骤 708、判断第二原始信息的第二摘要和第二解密信息是否相同。

当第二原始信息的第二摘要和第二解密信息不相同，第一 VNFC 对第二 VNFC 身份认证失败，两个 VNFC 间不建立通信连接；

当第二原始信息的第二摘要和第二解密信息相同时，第一 VNFC 对第二 VNFC 身份认证通过。即此时，第一 VNFC 与第二 VNFC 间互相身份认证通过，两个 VNFC 间可以建立安全的通信连接。

较佳的，在将第一 VNFC 的私钥和第二 VNFC 的公钥写入或发送至第一 VNFC 时，还可以将第二 VNFC 的标识信息一并写入或发送至第一 VNFC，第二 VNFC 的标识信息与第二 VNFC 的公钥的对应关系存储于第一 VNFC 中，以便后续在接收到第二 VNFC 发送的认证请求时，根据第二原始信息中的第二 VNFC 的标识信息快速获取到第二 VNFC 的公钥。

相应的，在将第一 VNFC 的公钥和第二 VNFC 的私钥写入或发送至第二 VNFC 时，还可以将第一 VNFC 的标识信息一并写入或发送至第二 VNFC，第一 VNFC 的标识信息与第一 VNFC 的公钥的对应关系存储于第二 VNFC 中，以便后续在接收到第一 VNFC 发送的认证请求时，根据第一原始信息中的第一 VNFC 的标识信息快速获取到第一 VNFC 的公钥。

可见，采用本发明实施例提供的上述身份认证方法，可以在生成建立 VNF 所需的配置信息时，针对组成 VNF 的每个 VNFC，生成一对公钥和私钥，将该 VNFC 的私钥置入该 VNFC，将该 VNFC 的公钥置入需要与该 VNFC 进行通信的 VNFC，当然，需要与该 VNFC 进行通信的 VNFC 的数量可以为一个，也可以为多个。通过 VNFC 间校验公钥、私钥的匹配，可以实现 VNFC 间互

相的身份认证。

基于同一发明构思，本发明实施例还提供了一种身份认证方法，应用于NFV系统，该NFV系统包括VNF，该VNF包括第一VNFC和第二VNFC，该身份认证方法如图8所示，具体可以包括如下步骤：

步骤801、生成第一VNFC的专用密钥，以及第二VNFC的专用密钥；

专用密钥，又称为对称密钥，如果用专用密钥加密数据就必须用该专用密钥解密，否则解密将不会成功。

步骤802、将第一VNFC的专用密钥和第二VNFC的专用密钥写入或发送至第一VNFC；

步骤803、将第一VNFC的专用密钥和第二VNFC的专用密钥写入或发送至第二VNFC；其中，第一VNFC的专用密钥以及第二VNFC的专用密钥用于第一VNFC和第二VNFC进行身份认证。

需要说明的是，上述步骤802和步骤803没有必然的先后执行顺序。

在一个具体实施例中，可以在生成第一VNFC时，将第一VNFC的专用密钥和第二VNFC的专用密钥写入第一VNFC。在另一个具体实施例中，当第一VNFC为OMU-VNFC时，也可以通过第一VNFC的管理通信通道，将第一VNFC的专用密钥和第二VNFC的专用密钥发送至第一VNFC。

相应的，在一个具体实施例中，可以在生成第二VNFC时，将第一VNFC的专用密钥和第二VNFC的专用密钥写入第二VNFC。在另一个具体实施例中，当第二VNFC为OMU-VNFC时，也可以通过第二VNFC的管理通信通道，将第一VNFC的专用密钥和第二VNFC的专用密钥发送至第二VNFC。

即在本发明实施例中，将第一VNFC的专用密钥和第二VNFC的专用密钥置入第一VNFC、第二VNFC，基于置入的专用密钥，第一VNFC和第二VNFC间可以基于对称加密算法进行身份认证，具体方式本发明不做具体限定。

例如，在一个具体实施例中，在将第一VNFC的专用密钥和第二VNFC的专用密钥写入或发送至第一VNFC时，还可以将第一VNFC的标识信息一

并写入或发送至第一 VNFC；在将第一 VNFC 的专用密钥和第二 VNFC 的专用密钥写入或发送至第二 VNFC 时，还可以将第二 VNFC 的标识信息一并写入或发送至第二 VNFC；然后第一 VNFC 和第二 VNFC 间可以采用图 9 所示的身份认证流程，具体包括如下步骤：

步骤 901、第一 VNFC 生成第一原始信息的第一摘要，并采用第一 VNFC 的专用密钥对第一原始信息的第一摘要进行加密，得到第一加密信息；其中，第一原始信息包含第一 VNFC 的标识信息，还可以包含第一 VNFC 向第二 VNFC 的通信连接请求。

步骤 902、第一 VNFC 将向第二 VNFC 发送携带第一原始信息和第一加密信息的认证请求。

步骤 903、第二 VNFC 接收第一 VNFC 发送的携带第一原始信息和第一加密信息的认证请求，之后，第二 VNFC 生成第一原始信息的第二摘要，以及采用第一 VNFC 的专用密钥对第一加密信息进行解密，得到第一解密信息。

步骤 904、判断第一原始信息的第二摘要和第一解密信息是否相同。

当第一原始信息的第二摘要和第一解密信息不相同，第二 VNFC 对第一 VNFC 身份认证失败，结束该认证流程，两个 VNFC 间不建立通信连接；

当第一原始信息的第二摘要和第一解密信息相同时，第二 VNFC 对第一 VNFC 身份认证通过，进入步骤 905。

步骤 905、第二 VNFC 生成第二原始信息的第一摘要，并采用第二 VNFC 的专用密钥对第二原始信息的第一摘要进行加密，得到第二加密信息；其中，第二原始信息包含第二 VNFC 的标识信息，还可以包含第二 VNFC 向第一 VNFC 的通信连接请求。

步骤 906、第二 VNFC 向第一 VNFC 发送携带第二原始信息和第二加密信息的认证请求。

步骤 907、第一 VNFC 接收第二 VNFC 发送的携带第二原始信息和第二加密信息的认证请求，之后，第一 VNFC 生成第二原始信息的第二摘要，以及采用第二 VNFC 的专用密钥对第二加密信息进行解密，得到第二解密信息。

步骤 908、判断第二原始信息的第二摘要和第二解密信息是否相同。

当第二原始信息的第二摘要和第二解密信息不相同，第一 VNFC 对第二 VNFC 身份认证失败，两个 VNFC 间不建立通信连接；

当第二原始信息的第二摘要和第二解密信息相同时，第一 VNFC 对第二 VNFC 身份认证通过。即此时，第一 VNFC 与第二 VNFC 间互相身份认证通过，两个 VNFC 间可以建立安全的通信连接。

较佳的，在将第一 VNFC 的专用密钥和第二 VNFC 的专用密钥写入或发送至第一 VNFC 时，还可以将第二 VNFC 的标识信息一并写入或发送至第一 VNFC，第二 VNFC 的标识信息与第二 VNFC 的专用密钥的对应关系存储于第一 VNFC 中，以便后续在接收到第二 VNFC 发送的认证请求时，根据第二原始信息中的第二 VNFC 的标识信息快速获取到第二 VNFC 的专用密钥。

相应的，在将第一 VNFC 的专用密钥和第二 VNFC 的专用密钥写入或发送至第二 VNFC 时，还可以将第一 VNFC 的标识信息一并写入或发送至第二 VNFC，第一 VNFC 的标识信息与第一 VNFC 的专用密钥的对应关系存储于第二 VNFC 中，以便后续在接收到第一 VNFC 发送的认证请求时，根据第一原始信息中的第一 VNFC 的标识信息快速获取到第一 VNFC 的专用密钥。

可见，采用本发明实施例提供的上述身份认证方法，可以在生成建立 VNF 所需的配置信息时，针对组成 VNF 的每个 VNFC，生成专用密钥，将该 VNFC 的专用密钥置于该 VNFC 以及需要与该 VNFC 进行通信的 VNFC，当然，需要与该 VNFC 进行通信的 VNFC 的数量可以为一个，也可以为多个。通过 VNFC 间校验专用密钥匹配，可以实现 VNFC 间的身份认证。

图 8 所示的身份认证方法在 NFV 系统中的具体实现可以参见前述具体实施例 1-4，本发明在此不再赘述。

综上，采用本发明实施例提供的方法，可以实现身份凭据的自动置入，不需要通过手工配置来实现身份凭据的置入，因此，效率较高；并且，VNF 中 VNFC 间的通信关系是动态变化的，采用本发明实施例提供的方法，无论 VNFC 间的通信关系如何变化，均可以自动进行 VNFC 间的身份认证，因此

能够适应动态变化的 VNF，并且可以利用现有的 NFV 系统，易于实现。

基于同一发明构思，根据本发明上述实施例提供的身份认证方法，相应地，本发明另一实施例还提供了一种身份认证装置，应用于 NFV 系统，该 NFV 系统包括 VNF，该 VNF 包括第一 VNFC 和第二 VNFC。例如，在一个实施例中，第一 VNFC 为 OMU-VNFC，第二 VNFC 为 SER-VNFC；在另一个实施例中，第一 VNFC 为 SER-VNFC，第二 VNFC 为 OMU-VNFC；在另一个实施例中，第一 VNFC 为 SER-VNFC，第二 VNFC 为 SER-VNFC。本发明实施例提供的身份认证装置可以利用现有 NFV 系统中的 VNFM、EMS 或 NFVO 实现。该身份认证装置结构示意图如图 10 所示，具体包括：

生成单元 1001，用于生成第一 VNFC 的公钥和私钥，以及第二 VNFC 的公钥和私钥；

置入单元 1002，用于将第一 VNFC 的私钥和第二 VNFC 的公钥写入或发送至第一 VNFC，以及将第一 VNFC 的公钥和第二 VNFC 的私钥写入或发送至第二 VNFC；其中，第一 VNFC 的公钥和私钥以及第二 VNFC 的公钥和私钥用于第一 VNFC 和第二 VNFC 进行身份认证。

进一步的，置入单元 1002，具体用于在生成第一 VNFC 时，将第一 VNFC 的私钥和第二 VNFC 的公钥写入第一 VNFC；或者当第一 VNFC 为管理 VNFC 时，通过第一 VNFC 的管理通信通道，将第一 VNFC 的私钥和第二 VNFC 的公钥发送至第一 VNFC。

进一步的，置入单元 1002，具体用于在生成第二 VNFC 时，将第一 VNFC 的公钥和第二 VNFC 的私钥写入第二 VNFC；或者当第二 VNFC 为管理 VNFC 时，通过第二 VNFC 的管理通信通道，将第一 VNFC 的公钥和第二 VNFC 的私钥发送至第二 VNFC。

较佳的，置入单元 1002，还用于将第二 VNFC 的标识信息写入或发送至第一 VNFC；其中，第二 VNFC 的标识信息与第二 VNFC 的公钥的对应关系存储于第一 VNFC 中。

进一步的，置入单元 1002，还用于将第一 VNFC 的标识信息写入或发送

至第一 VNFC。

具体的，生成单元 1001 可以由处理器实现，置入单元 1002 可以由输入输出接口实现，该输入输出接口可以包括写入器或发送器。

基于同一发明构思，根据本发明上述实施例提供的身份认证方法，相应地，本发明另一实施例还提供了一种身份认证装置，应用于 NFV 系统，该 NFV 系统包括 VNF，该 VNF 包括第一 VNFC 和第二 VNFC，该身份认证装置结构示意图如图 11 所示，具体包括：

生成单元 1101，用于生成第一 VNFC 的专用密钥，以及第二 VNFC 的专用密钥；

置入单元 1102，用于将第一 VNFC 的专用密钥和第二 VNFC 的专用密钥写入或发送至第一 VNFC，以及将第一 VNFC 的专用密钥和第二 VNFC 的专用密钥写入或发送至第二 VNFC；其中，第一 VNFC 的专用密钥以及第二 VNFC 的专用密钥用于第一 VNFC 和第二 VNFC 进行身份认证。

进一步的，置入单元 1102，具体用于在生成第一 VNFC 时，将第一 VNFC 的专用密钥和第二 VNFC 的专用密钥写入第一 VNFC；或者当第一 VNFC 为管理 VNFC 时，通过第一 VNFC 的管理通信通道，将第一 VNFC 的专用密钥和第二 VNFC 的专用密钥发送至第一 VNFC。

进一步的，置入单元 1102，具体用于在生成第二 VNFC 时，将第一 VNFC 的专用密钥和第二 VNFC 的专用密钥写入第二 VNFC；或者当第二 VNFC 为管理 VNFC 时，通过第二 VNFC 的管理通信通道，将第一 VNFC 的专用密钥和第二 VNFC 的专用密钥发送至第二 VNFC。

较佳的，置入单元 1102，还用于将第二 VNFC 的标识信息写入或发送至第一 VNFC；其中，第二 VNFC 的标识信息与第二 VNFC 的对称密钥的对应关系存储于第一 VNFC 中。

进一步的，置入单元 1102，还用于将第一 VNFC 的标识信息写入或发送至第一 VNFC。

具体的，生成单元 1101 可以由处理器实现，置入单元 1102 可以由输入

输出接口实现，该输入输出接口可以包括写入器或发送器。

综上所述，本发明实施例提供的方案，相比于现有技术，能够自动实现VNFC间的身份认证，效率较高，能够适应动态变化的VNF。

本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中特定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中特定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中特定的功能的步骤。

尽管已描述了本发明的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权

利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

显然，本领域的技术人员可以对本发明实施例进行各种改动和变型而不脱离本发明实施例的精神和范围。这样，倘若本发明实施例的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

权利要求

1、一种身份认证方法，应用于网络功能虚拟化 NFV 系统，所述 NFV 系统包括虚拟网络功能 VNF，所述 VNF 包括第一虚拟网络功能组成部分 VNFC 和第二 VNFC，其特征在于，所述方法包括：

生成所述第一 VNFC 的公钥和私钥，以及所述第二 VNFC 的公钥和私钥；

将所述第一 VNFC 的私钥和所述第二 VNFC 的公钥写入或发送至所述第一 VNFC；

将所述第一 VNFC 的公钥和所述第二 VNFC 的私钥写入或发送至所述第二 VNFC；其中，所述第一 VNFC 的公钥和私钥以及所述第二 VNFC 的公钥和私钥用于所述第一 VNFC 和所述第二 VNFC 进行身份认证。

2、如权利要求 1 所述的方法，其特征在于，将所述第一 VNFC 的私钥和所述第二 VNFC 的公钥写入或发送至所述第一 VNFC，包括：

在生成所述第一 VNFC 时，将所述第一 VNFC 的私钥和所述第二 VNFC 的公钥写入所述第一 VNFC；或者

当所述第一 VNFC 为管理 VNFC 时，通过所述第一 VNFC 的管理通信通道，将所述第一 VNFC 的私钥和所述第二 VNFC 的公钥发送至所述第一 VNFC。

3、如权利要求 1 或 2 所述的方法，其特征在于，还包括：

将所述第二 VNFC 的标识信息写入或发送至所述第一 VNFC；其中，所述第二 VNFC 的标识信息与所述第二 VNFC 的公钥的对应关系存储于所述第一 VNFC 中。

4、如权利要求 1-3 任一所述的方法，其特征在于，还包括：

将所述第一 VNFC 的标识信息写入或发送至所述第一 VNFC。

5、一种身份认证方法，应用于网络功能虚拟化 NFV 系统，所述 NFV 系统包括虚拟网络功能 VNF，所述 VNF 包括第一虚拟网络功能组成部分 VNFC 和第二 VNFC，其特征在于，所述方法包括：

生成所述第一 VNFC 的专用密钥，以及所述第二 VNFC 的专用密钥；

将所述第一 VNFC 的专用密钥和所述第二 VNFC 的专用密钥写入或发送至所述第一 VNFC；

将所述第一 VNFC 的专用密钥和所述第二 VNFC 的专用密钥写入或发送至所述第二 VNFC；其中，所述第一 VNFC 的专用密钥以及所述第二 VNFC 的专用密钥用于所述第一 VNFC 和所述第二 VNFC 进行身份认证。

6、如权利要求 5 所述的方法，其特征在于，将所述第一 VNFC 的专用密钥和所述第二 VNFC 的专用密钥写入或发送至所述第一 VNFC，包括：

在生成所述第一 VNFC 时，将所述第一 VNFC 的专用密钥和所述第二 VNFC 的专用密钥写入所述第一 VNFC；或者

当所述第一 VNFC 为管理 VNFC 时，通过所述第一 VNFC 的管理通信通道，将所述第一 VNFC 的专用密钥和所述第二 VNFC 的专用密钥发送至所述第一 VNFC。

7、如权利要求 5 或 6 所述的方法，其特征在于，还包括：

将所述第二 VNFC 的标识信息写入或发送至所述第一 VNFC；其中，所述第二 VNFC 的标识信息与所述第二 VNFC 的专用密钥的对应关系存储于所述第一 VNFC 中。

8、如权利要求 5-7 任一所述的方法，其特征在于，还包括：

将所述第一 VNFC 的标识信息写入或发送至所述第一 VNFC。

9、一种身份认证装置，应用于网络功能虚拟化 NFV 系统，所述 NFV 系统包括虚拟网络功能 VNF，所述 VNF 包括第一虚拟网络功能组成部分 VNFC 和第二 VNFC，其特征在于，所述装置包括：

处理器，用于生成所述第一 VNFC 的公钥和私钥，以及所述第二 VNFC 的公钥和私钥；

输入输出接口，用于将所述第一 VNFC 的私钥和所述第二 VNFC 的公钥写入或发送至所述第一 VNFC，以及将所述第一 VNFC 的公钥和所述第二 VNFC 的私钥写入或发送至所述第二 VNFC；其中，所述第一 VNFC 的公钥

和私钥以及所述第二 VNFC 的公钥和私钥用于所述第一 VNFC 和所述第二 VNFC 进行身份认证。

10、如权利要求 9 所述的装置，其特征在于，所述输入输出接口，具体用于在生成所述第一 VNFC 时，将所述第一 VNFC 的私钥和所述第二 VNFC 的公钥写入所述第一 VNFC；或者当所述第一 VNFC 为管理 VNFC 时，通过所述第一 VNFC 的管理通信通道，将所述第一 VNFC 的私钥和所述第二 VNFC 的公钥发送至所述第一 VNFC。

11、如权利要求 9 或 10 所述的装置，其特征在于，所述输入输出接口，还用于将所述第二 VNFC 的标识信息写入或发送至所述第一 VNFC；其中，所述第二 VNFC 的标识信息与所述第二 VNFC 的公钥的对应关系存储于所述第一 VNFC 中。

12、如权利要求 9-11 任一所述的装置，其特征在于，所述输入输出接口，还用于将所述第一 VNFC 的标识信息写入或发送至所述第一 VNFC。

13、如权利要求 9-12 任一所述的装置，所述输入输出接口，包括写入器或发送器。

14、一种身份认证装置，应用于网络功能虚拟化 NFV 系统，所述 NFV 系统包括虚拟网络功能 VNF，所述 VNF 包括第一虚拟网络功能组成部分 VNFC 和第二 VNFC，其特征在于，所述装置包括：

处理器，用于生成所述第一 VNFC 的专用密钥，以及所述第二 VNFC 的专用密钥；

输入输出接口，用于将所述第一 VNFC 的专用密钥和所述第二 VNFC 的专用密钥写入或发送至所述第一 VNFC，以及将所述第一 VNFC 的专用密钥和所述第二 VNFC 的专用密钥写入或发送至所述第二 VNFC；其中，所述第一 VNFC 的专用密钥以及所述第二 VNFC 的专用密钥用于所述第一 VNFC 和所述第二 VNFC 进行身份认证。

15、如权利要求 14 所述的装置，其特征在于，所述输入输出接口，具体用于在生成所述第一 VNFC 时，将所述第一 VNFC 的专用密钥和所述第二

VNFC 的专用密钥写入所述第一 VNFC; 或者当所述第一 VNFC 为管理 VNFC 时, 通过所述第一 VNFC 的管理通信通道, 将所述第一 VNFC 的专用密钥和所述第二 VNFC 的专用密钥发送至所述第一 VNFC。

16、如权利要求 14 或 15 所述的装置, 其特征在于, 所述输入输出接口, 还用于将所述第二 VNFC 的标识信息写入或发送至所述第一 VNFC; 其中, 所述第二 VNFC 的标识信息与所述第二 VNFC 的对称密钥的对应关系存储于所述第一 VNFC 中。

17、如权利要求 14-16 任一所述的装置, 其特征在于, 所述输入输出接口, 还用于将所述第一 VNFC 的标识信息写入或发送至所述第一 VNFC。

18、如权利要求 14-17 任一所述的装置, 其特征在于, 所述输入输出接口, 包括写入器或发送器。

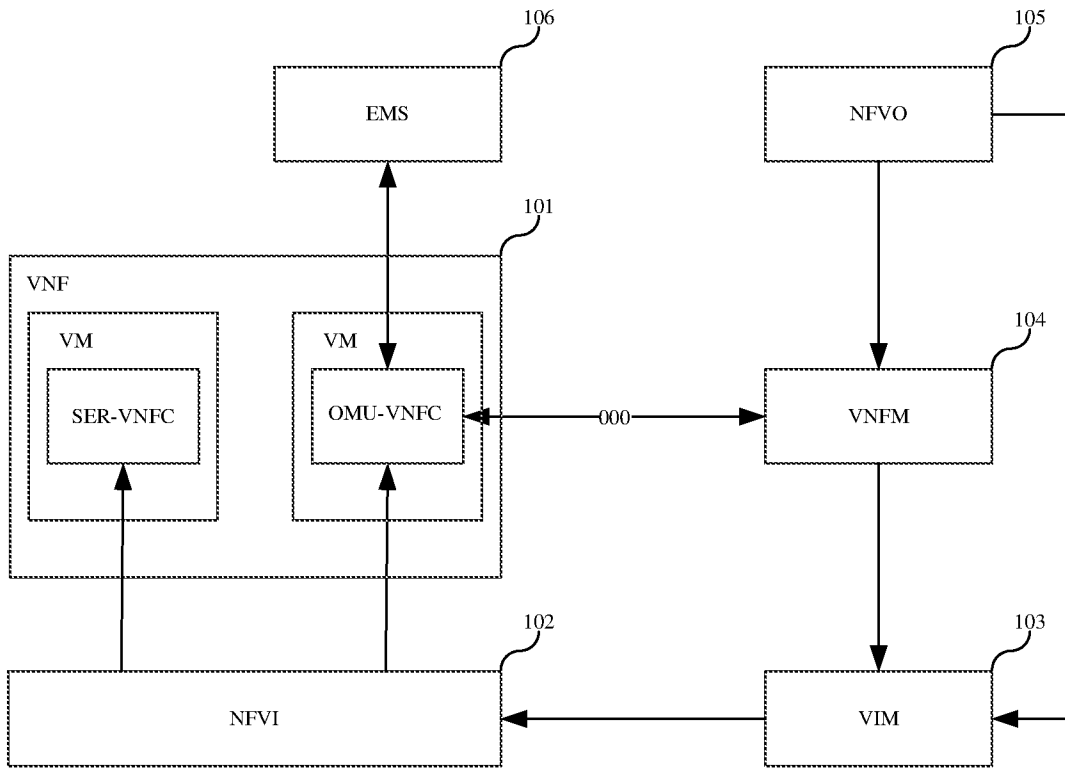


图 1

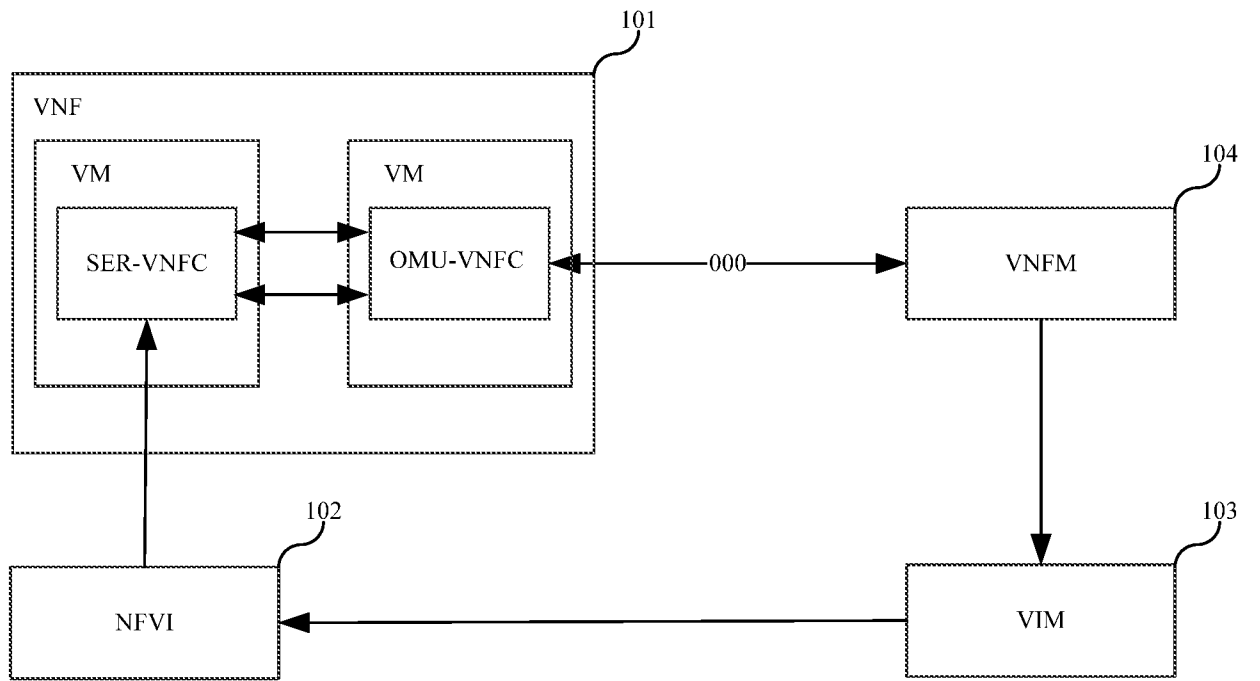


图 2

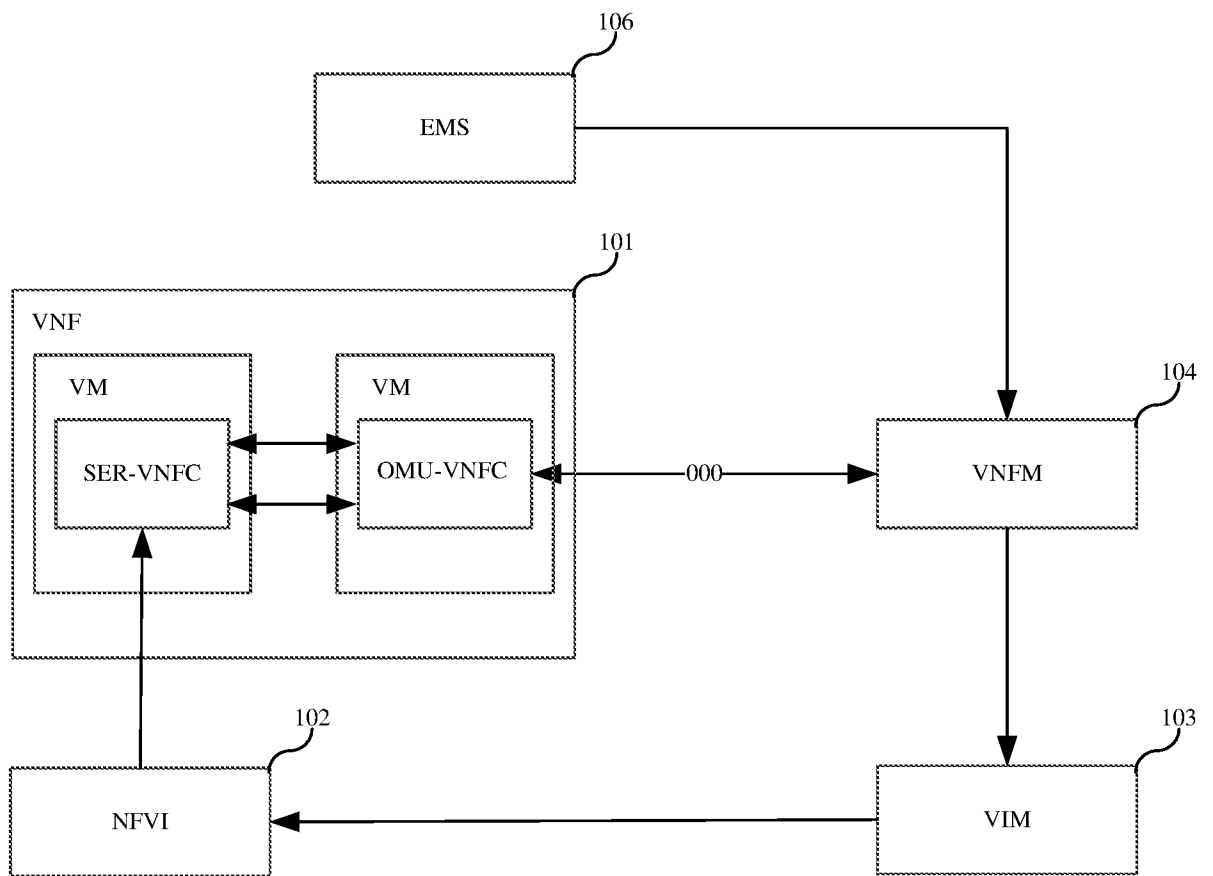


图 3

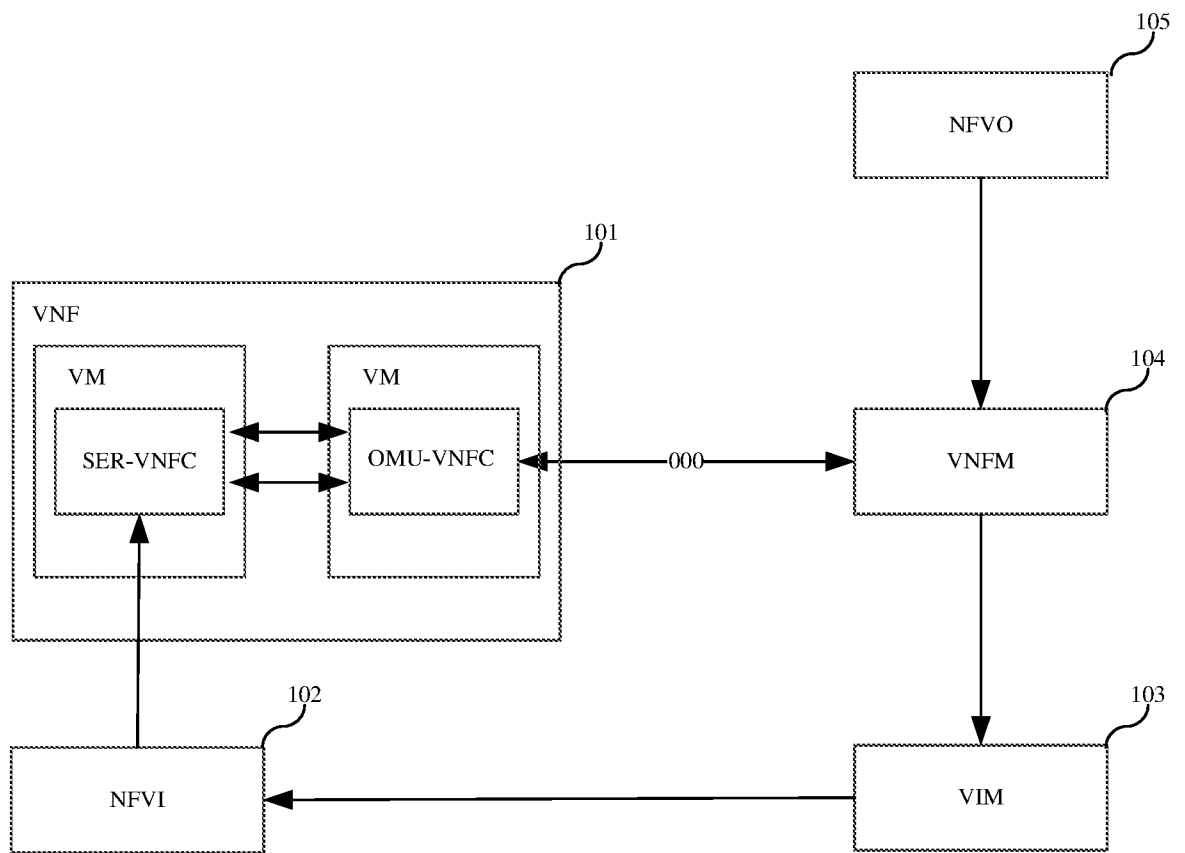


图 4

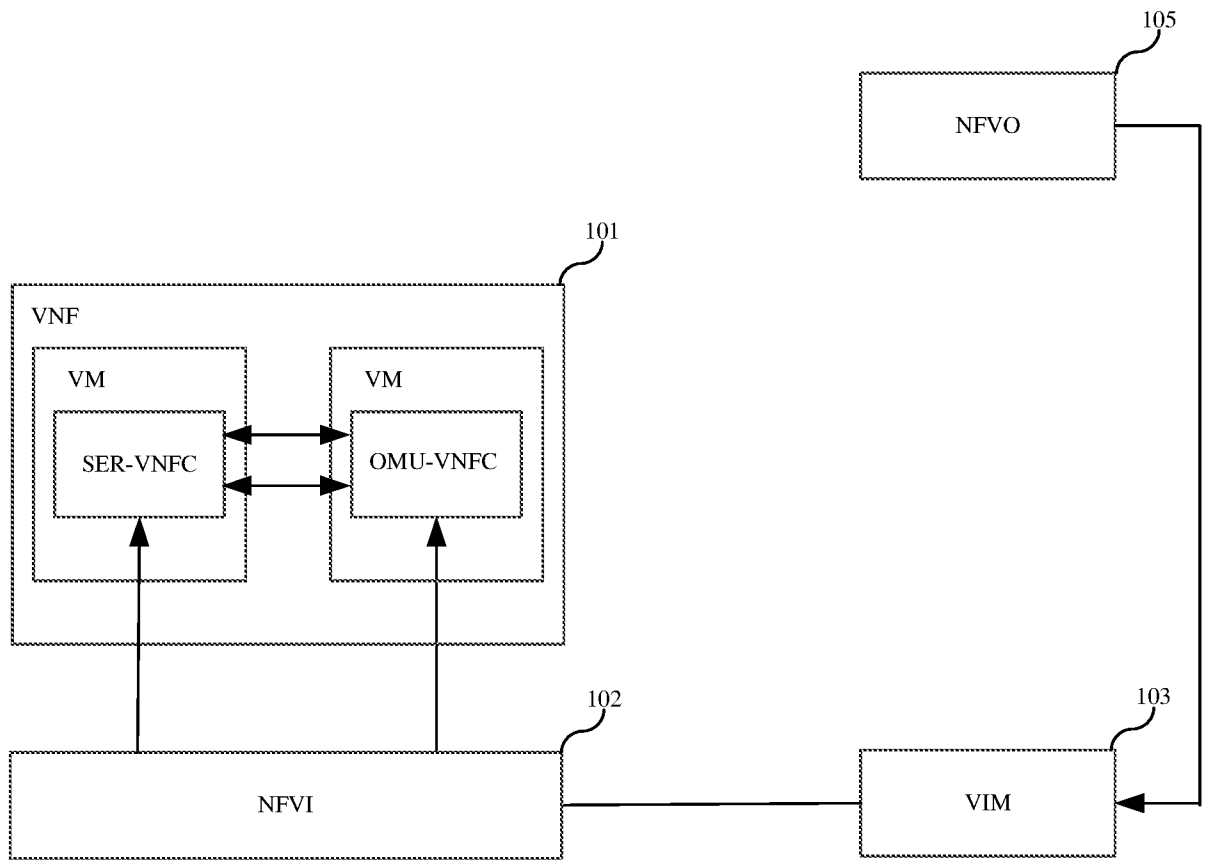


图 5

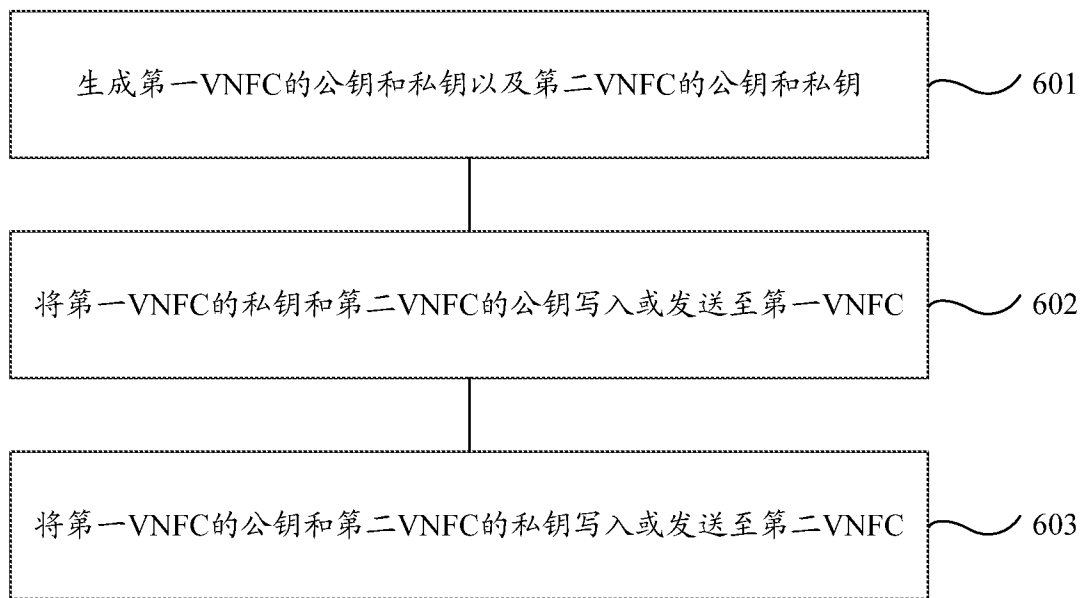


图 6

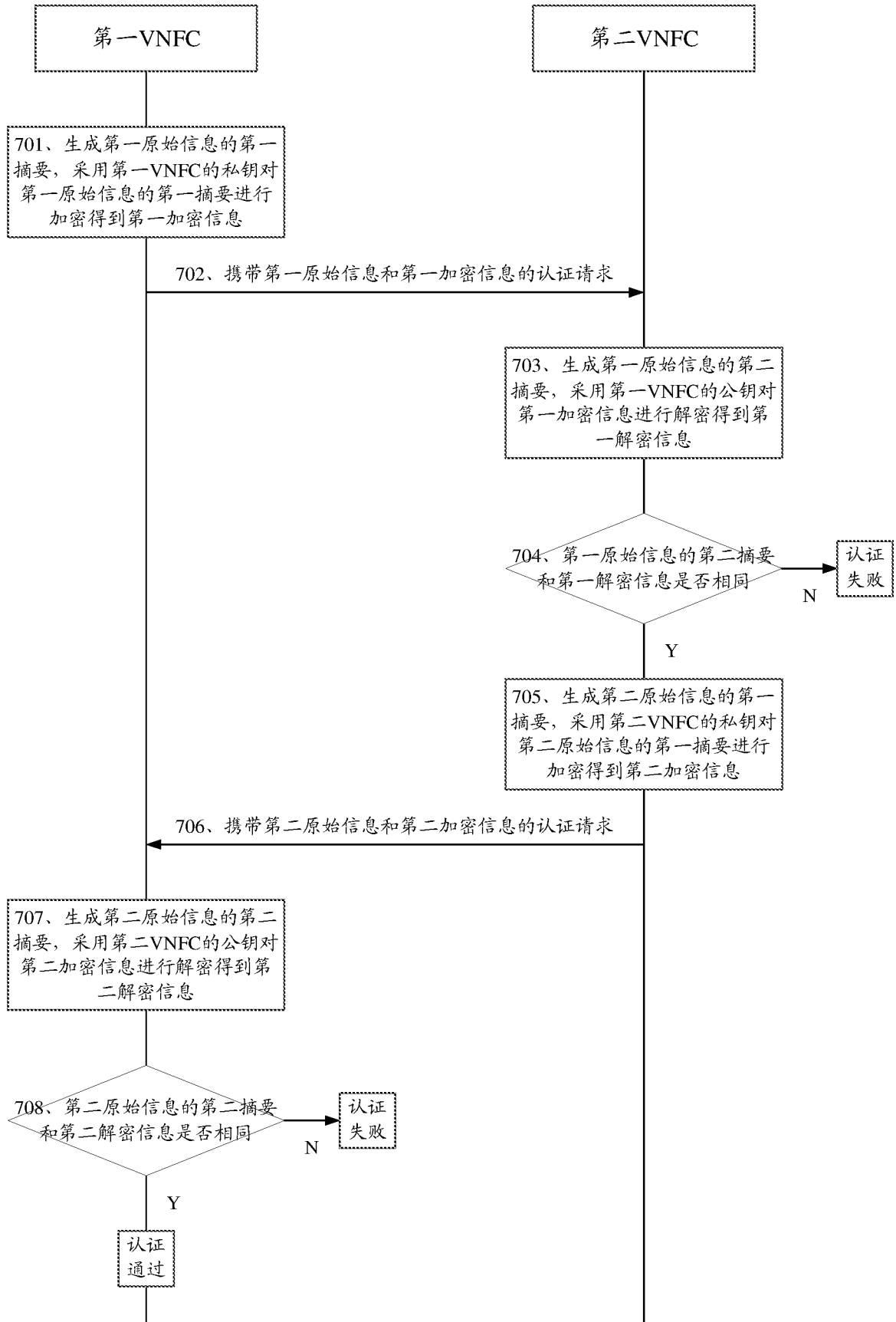


图 7

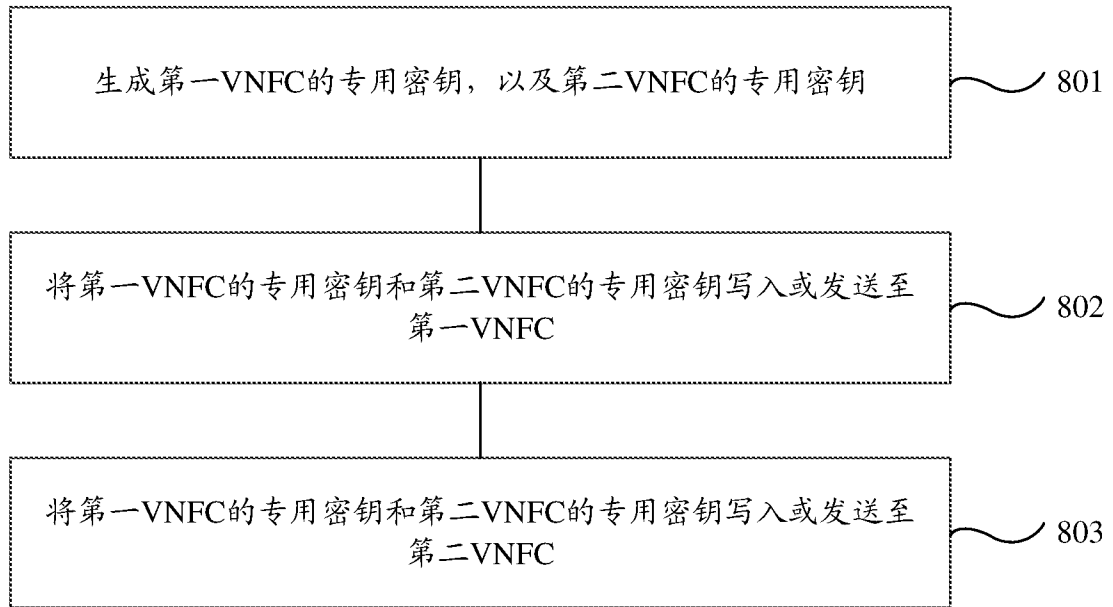


图 8

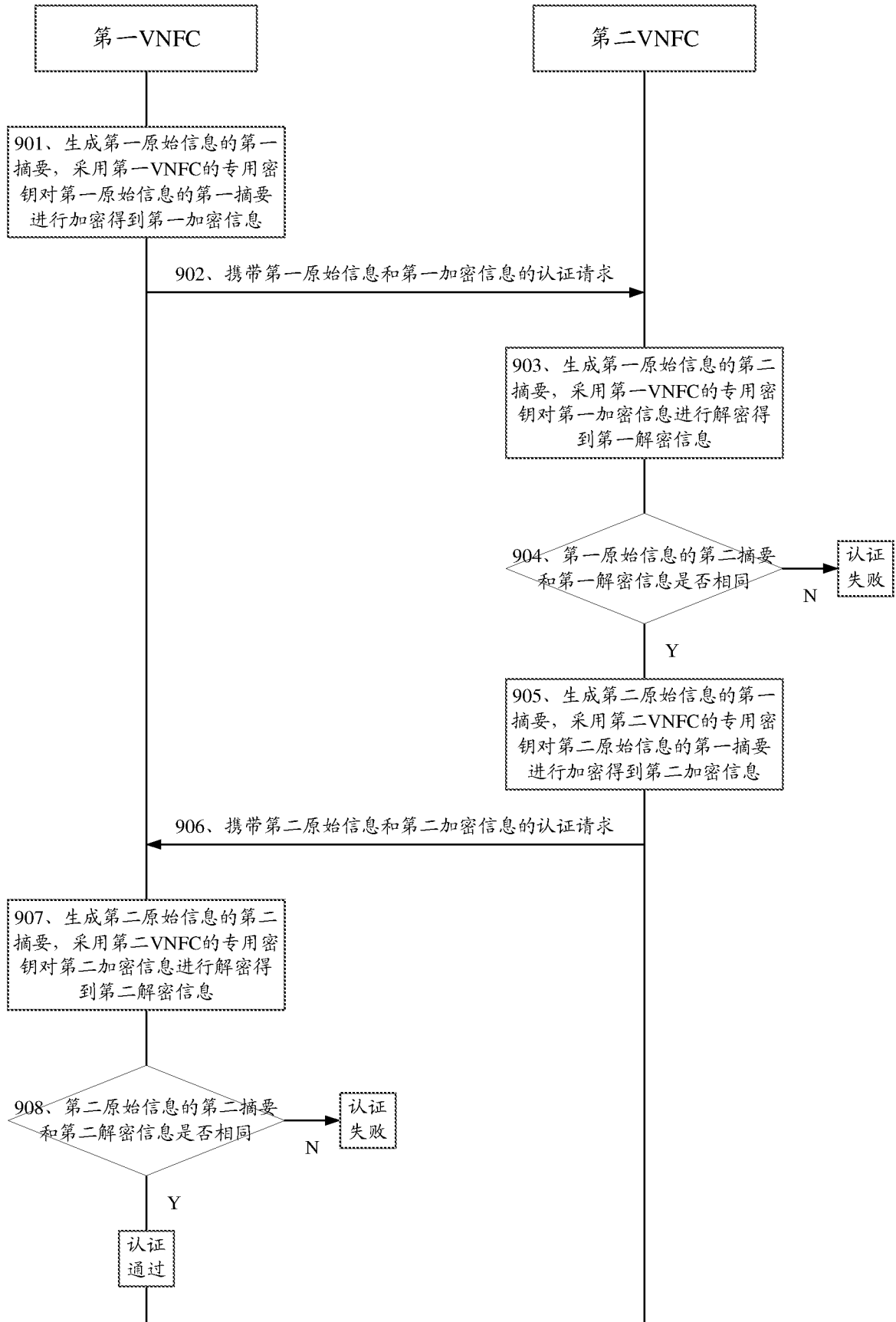


图 9

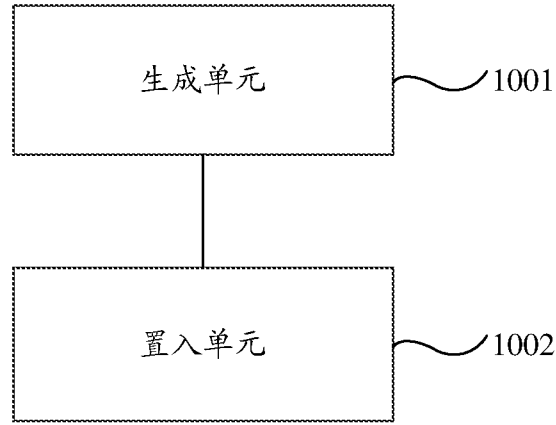


图 10

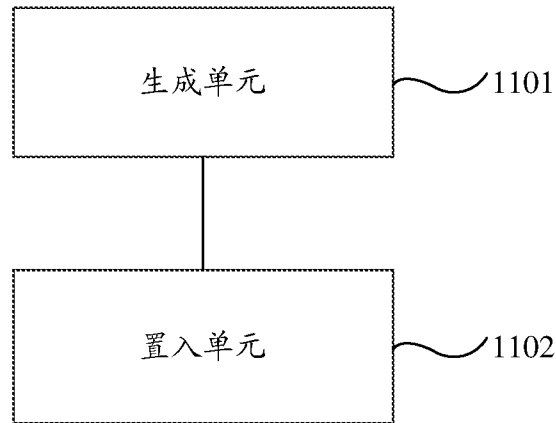


图 11

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2015/088636

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (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; H04Q; H04W; G06F

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: identity authentication, virtualization, secret key, asymmetric, identity, authentication, virtual, public w key, private w key, encrypt, encode, decipher, decode, symmetric, identifier, certificate, safety

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 104580208 A (HUAWEI TECHNOLOGIES CO., LTD.), 29 April 2015 (29.04.2015), claims 1-18	1-18
Y	CN 104134122 A (HUAWEI TECHNOLOGIES CO., LTD.), 05 November 2014 (05.11.2014), description, paragraphs 0094-0100	1-18
Y	CN 103888251 A (BEIJING UNIVERSITY OF TECHNOLOGY), 25 June 2014 (25.06.2014), description, paragraphs 40-46	1-18
A	WO 2012050419 A1 (MIMOS BHD.), 19 April 2012 (19.04.2012), the whole document	1-18

Further documents are listed in the continuation of Box C.

See patent family annex.

<p>* Special categories of cited documents:</p> <p>“A” document defining the general state of the art which is not considered to be of particular relevance</p> <p>“E” earlier application or patent but published on or after the international filing date</p> <p>“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)</p> <p>“O” document referring to an oral disclosure, use, exhibition or other means</p> <p>“P” document published prior to the international filing date but later than the priority date claimed</p>	<p>“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</p> <p>“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</p> <p>“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</p> <p>“&” document member of the same patent family</p>
---	---

Date of the actual completion of the international search
12 October 2015 (12.10.2015)

Date of mailing of the international search report
27 October 2015 (27.10.2015)

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
BAO, Xinxin
Telephone No.: (86-10) **82245278**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/088636

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104580208 A	29 April 2015	None	
CN 104134122 A	05 November 2014	None	
CN 103888251 A	25 June 2014	None	
WO 2012050419 A1	19 April 2012	MY 151311 A	15 May 2014

<p>A. 主题的分类</p> <p>H04L 29/06 (2006.01) i</p> <p>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</p>																	
<p>B. 检索领域</p> <p>检索的最低限度文献(标明分类系统和分类号)</p> <p>H04L; H04Q; H04W; G06F</p> <p>包含在检索领域中的除最低限度文献以外的检索文献</p> <p>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))</p> <p>CNPAT, CNKI, WPI, EPODOC: 身份认证, 虚拟化, 公钥, 私钥, 密钥, 加密, 解密, 对称, 非对称, 标识, 认证, 安全, 鉴权, identity, authentication, virtual, public w key, private w key, encrypt, encode, decipher, decode, symmetric, identifier, certificate, safety</p>																	
<p>C. 相关文件</p> <table border="1"> <thead> <tr> <th>类型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>PX</td> <td>CN 104580208 A (华为技术有限公司) 2015年 4月 29日 (2015 - 04 - 29) 权利要求1-18</td> <td>1-18</td> </tr> <tr> <td>Y</td> <td>CN 104134122 A (华为技术有限公司) 2014年 11月 5日 (2014 - 11 - 05) 说明书第0094段-0100段</td> <td>1-18</td> </tr> <tr> <td>Y</td> <td>CN 103888251 A (北京工业大学) 2014年 6月 25日 (2014 - 06 - 25) 说明书第40段-46段</td> <td>1-18</td> </tr> <tr> <td>A</td> <td>WO 2012050419 A1 (MIMOS BHD.) 2012年 4月 19日 (2012 - 04 - 19) 全文</td> <td>1-18</td> </tr> </tbody> </table>			类型*	引用文件, 必要时, 指明相关段落	相关的权利要求	PX	CN 104580208 A (华为技术有限公司) 2015年 4月 29日 (2015 - 04 - 29) 权利要求1-18	1-18	Y	CN 104134122 A (华为技术有限公司) 2014年 11月 5日 (2014 - 11 - 05) 说明书第0094段-0100段	1-18	Y	CN 103888251 A (北京工业大学) 2014年 6月 25日 (2014 - 06 - 25) 说明书第40段-46段	1-18	A	WO 2012050419 A1 (MIMOS BHD.) 2012年 4月 19日 (2012 - 04 - 19) 全文	1-18
类型*	引用文件, 必要时, 指明相关段落	相关的权利要求															
PX	CN 104580208 A (华为技术有限公司) 2015年 4月 29日 (2015 - 04 - 29) 权利要求1-18	1-18															
Y	CN 104134122 A (华为技术有限公司) 2014年 11月 5日 (2014 - 11 - 05) 说明书第0094段-0100段	1-18															
Y	CN 103888251 A (北京工业大学) 2014年 6月 25日 (2014 - 06 - 25) 说明书第40段-46段	1-18															
A	WO 2012050419 A1 (MIMOS BHD.) 2012年 4月 19日 (2012 - 04 - 19) 全文	1-18															
<p><input type="checkbox"/> 其余文件在C栏的续页中列出。</p> <p><input checked="" type="checkbox"/> 见同族专利附件。</p>																	
<p>* 引用文件的具体类型:</p> <table border="0"> <tr> <td>“A” 认为不特别相关的表示了现有技术一般状态的文件</td> <td>“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</td> </tr> <tr> <td>“E” 在国际申请日的当天或之后公布的在先申请或专利</td> <td>“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</td> </tr> <tr> <td>“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)</td> <td>“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</td> </tr> <tr> <td>“O” 涉及口头公开、使用、展览或其他方式公开的文件</td> <td>“&” 同族专利的文件</td> </tr> <tr> <td>“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</td> <td></td> </tr> </table>			“A” 认为不特别相关的表示了现有技术一般状态的文件	“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	“E” 在国际申请日的当天或之后公布的在先申请或专利	“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	“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)	“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	“O” 涉及口头公开、使用、展览或其他方式公开的文件	“&” 同族专利的文件	“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						
“A” 认为不特别相关的表示了现有技术一般状态的文件	“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																
“E” 在国际申请日的当天或之后公布的在先申请或专利	“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																
“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)	“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																
“O” 涉及口头公开、使用、展览或其他方式公开的文件	“&” 同族专利的文件																
“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																	
<p>国际检索实际完成的日期</p> <p>2015年 10月 12日</p>	<p>国际检索报告邮寄日期</p> <p>2015年 10月 27日</p>																
<p>ISA/CN的名称和邮寄地址</p> <p>中华人民共和国国家知识产权局(ISA/CN) 北京市海淀区蓟门桥西土城路6号 100088 中国</p> <p>传真号 (86-10)62019451</p>	<p>授权官员</p> <p>鲍欣欣</p> <p>电话号码 (86-10)82245278</p>																

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2015/088636

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	104580208	A	2015年 4月 29日	无			
CN	104134122	A	2014年 11月 5日	无			
CN	103888251	A	2014年 6月 25日	无			
WO	2012050419	A1	2012年 4月 19日	MY	151311	A	2014年 5月 15日