

终端信息的传递方法及相关产品

技术领域

本申请涉及通信技术领域，尤其涉及一种终端信息的传递方法及相关产品。

5

背景技术

新空口技术中，终端与网络侧进行初始注册的过程中，网络设备与终端之间传递的策略选择相关信息是明文的，此种机制存在暴露终端的隐私信息的风险。

发明内容

本申请的实施例提供一种终端信息的传递方法及相关产品，可以提高终端策略的查询过程中网络侧与终端信息交互过程的安全性。

第一方面，本申请实施例提供一种终端信息的传递方法，应用于网络设备，所述网络设备包括第一网元，所述方法包括：

15 所述第一网元接收来自终端的第一信息，所述第一信息用于指示终端存储的终端策略，且该第一信息包括非明文呈现的内容。

所述第一网元根据所述第一信息查询所述终端策略。

第二方面，本申请实施例提供一种终端信息的传递方法，应用于终端，所述方法包括：

20 所述终端接收来自第一网元的第二信息，所述第二信息用于指示终端存储的终端策略，且该第二信息包括非明文呈现的内容。

所述终端根据所述第二信息查询所述终端策略。

第三方面，本申请实施例提供一种网络设备，该网络设备具有实现上述方法设计中第一网络设备的行为的功能。所述功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。所述硬件或软件包括一个或多个与上述功能相对应的模块。在一个可能的设计中，网络设备包括处理器，所述处理器被配置为支持网络设备执行上述方法中相应的功能。进一步的，网络设备还可以包括收发器，所述收发器用于支持网络设备与终端之间的通信。进一步的，网络设备还可以包括存储器，所述存储器用于与处理器耦合，其保存网络设备必要的程序指令和数据。

25 第四方面，本申请实施例提供一种终端，该终端具有实现上述方法设计中第一终端的行为的功能。所述功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。所述硬件或软件包括一个或多个与上述功能相对应的模块。在一个可能的设计中，终端包括处理器，所述处理器被配置为支持终端执行上述方法中相应的功能。进一步的，终端还可以包括收发器，所述收发器用于支持终端与网络设备之间的通信。进一步的，终端还可以包括存储器，所述存储器用于与处理器耦合，其保存终端必要的程序指令和数据。

30 第五方面，本申请实施例提供一种网络设备，包括处理器、存储器、收发器以及一个或多个程序，其中，所述一个或多个程序被存储在所述存储器中，并且被配置由所述处理器执行，所述程序包括用于执行本申请实施例第一方面任一方法中的步骤的指令。

35 第六方面，本申请实施例提供一种终端，包括处理器、存储器、通信接口以及一个或多个程序，其中，所述一个或多个程序被存储在所述存储器中，并且被配置由所述处理器执行，所述程序包括用于执行本申请实施例第二方面任一方法中的步骤的指令。

40 第七方面，本申请实施例提供了一种计算机可读存储介质，其中，所述计算机可读存储介质存储用于电子数据交换的计算机程序，其中，所述计算机程序使得计算机执行如本申请实施例第一方面任一方法中所描述的部分或全部步骤。

-2-

第八方面，本申请实施例提供了一种计算机可读存储介质，其中，所述计算机可读存储介质存储用于电子数据交换的计算机程序，其中，所述计算机程序使得计算机执行如本申请实施例第二方面任一方法中所描述的部分或全部步骤。

第九方面，本申请实施例提供了一种计算机程序产品，其中，所述计算机程序产品包括存储了计算机程序的非瞬时性计算机可读存储介质，所述计算机程序可操作来使计算机执行如本申请实施例第一方面任一方法中所描述的部分或全部步骤。该计算机程序产品可以为一个软件安装包。

第十方面，本申请实施例提供了一种计算机程序产品，其中，所述计算机程序产品包括存储了计算机程序的非瞬时性计算机可读存储介质，所述计算机程序可操作来使计算机执行如本申请实施例第二方面任一方法中所描述的部分或全部步骤。该计算机程序产品可以为一个软件安装包。

可以看出，本申请实施例，网络设备的第一网元首先接收来自终端的第一信息，其次，根据所述第一信息查询所述终端策略，由于该第一信息是为非明文呈现的内容，故而可以避免第一网元与终端之间在传输该第一信息的过程中，该第一信息被非法窃取并直接利用，有利于提高终端策略的查询过程中网络侧与终端信息交互过程的安全性。

附图说明

下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍。

图 1A 是本申请实施例提供的一种可能的通信系统的网络架构图；

图 1B 是本申请实施例提供的一种终端策略与 PSI 参数之间的关系示例图；

图 2A 是本申请实施例提供的一种终端信息的传递方法的流程示意图；

图 2B 是本申请实施例提供的一种用于标识 UE policy 的 PSI 参数的示例格式；

图 2C 是本申请实施例提供的另一种用于标识 UE policy 的 PSI 参数的示例格式；

图 2D 是本申请实施例提供的另一种用于标识 UE policy 的 PSI 参数的示例格式；

图 2E 是本申请实施例提供的一种第一信息的示例格式；

图 2F 是本申请实施例提供的另一种第一信息的示例格式；

图 2G 是本申请实施例提供的一种在注册请求消息中进行加密发送的处理过程的示例图；

图 3A 是本申请实施例提供的一种终端信息的传递方法的流程示意图；

图 3B 是本申请实施例提供的一种终端信息的传递方法的流程示意图；

图 3C 是本申请实施例提供的一种终端信息的传递方法的流程示意图；

图 4A 是本申请实施例提供的一种终端信息的传递方法的流程示意图；

图 4A1 是本申请实施例提供的一种用户标识与 PSI 参数之间的对应关系的示意图；

图 4A2 是本申请实施例提供的另一种用户标识与 PSI 参数之间的对应关系的示意图；

图 4B 是本申请实施例提供的另一种终端信息的传递方法的流程示意图；

图 4C 是本申请实施例提供的另一种终端信息的传递方法的流程示意图；

图 4D 是本申请实施例提供的另一种终端信息的传递方法的流程示意图；

图 5 是本申请实施例提供的一种网络设备的结构示意图；

图 6 是本申请实施例提供的一种终端的结构示意图；

图 7 是本申请实施例提供的一种网络设备的结构示意图；

图 8 是本申请实施例提供的一种终端的结构示意图。

具体实施方式

下面将结合附图对本申请实施例中的技术方案进行描述。

示例的，图 1A 示出了本申请涉及的无线通信系统。该无线通信系统 100 可以工作在高频频段上，不限于长期演进（Long Term Evolution, LTE）系统，还可以是未来演进的第五代移动通信（the 5th

Generation, 5G) 系统、新空口(NR)系统, 机器与机器通信 (Machine to Machine, M2M) 系统等。该无线通信系统100可包括: 一个或多个网络设备101, 一个或多个终端103, 以及核心网设备105。其中: 网络设备101可以为基站, 基站可以用于与一个或多个终端进行通信, 也可以用于与一个或多个具有部分终端功能的基站进行通信 (比如宏基站与微基站)。基站可以是时分同步码分多址 (Time Division Synchronous Code Division Multiple Access, TD-SCDMA) 系统中的基站收发台 (Base Transceiver Station, BTS), 也可以是LTE系统中的演进型基站 (Evolutional Node B, eNB), 以及5G系统、新空口(NR)系统中的基站。另外, 基站也可以为接入点 (Access Point, AP)、传输节点 (Trans TRP)、中心单元 (Central Unit, CU) 或其他网络实体, 并且可以包括以上网络实体的功能中的一些或所有功能。核心网设备105包括接入和移动管理功能 (Access and Mobility Management Function, AMF) 实体, 用户面功能 (User Plane Function, UPF) 实体和会话管理功能 (Session Management Function, SMF) 等核心网侧的设备。终端103可以分布在整个无线通信系统100中, 可以是静止的, 也可以是移动的。在本申请的一些实施例中, 终端103可以是移动设备 (如智能手机)、移动台 (mobile station)、移动单元 (mobile unit)、M2M终端、无线单元、远程单元、用户代理、移动客户端等等。

需要说明的, 图1A示出的无线通信系统100仅仅是为了更加清楚的说明本申请的技术方案, 并不构成对本申请的限定, 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。

下面对本申请涉及的相关技术进行介绍。

目前, 终端策略又称为用户设备策略UE Policy, 该终端策略包括接入网络发现与选择策略 (access network discovery and selection policy, ANDSP) 以及用户设备路径选择策略 (UE Route Selection Policy, URSP), ANDSP是用于选择无线局域网WLAN接入的服务集标识 (Service Set Identifier, SSID) 的策略, 用户路径选择策略 (UE route selection poplcy, URSP) 是用于选择不同分组协议单元会话PDU Session的策略。目前, 对于UE Policy已经制定了策略分段标识 (policy section identifier, PSI) 参数, 来灵活的划分UE Policy。下面给出协议中WLANSP策略和URSP策略的示例。

1. WLANSP策略举例

无线局域网选择策略规则1WLANSP rule 1:

Priority 1、Validity Conditions (PLMN 1)、Group of Selection Criteria with priority 1: PreferredSSIDList = Priority 1: myoperator1, Priority 2: myoperator2、MinimumBackhaulThreshold = 2Mbps in the downlink、Group of Selection Criteria with priority 2、PreferredSSIDList = Priority 1: myoperator3;

WLANSP rule 2:

Priority 2、Validity Conditions (PLMN 1)、Group of Selection Criteria with priority 1: PreferredRoamingPartnerList = Priority 1: partner1.com, Priority 2: partner2.com、MaximumBSSLoad = 60。

2. URSP策略举例

URSP规则1URSP rule 1:

Priority:1、Traffic filter: App=DummyApp、Direct offload: Prohibited、Slice Info: S-NSSAI-a、Continuity Types: SSC Mode 3、DNNs: internet、Access Type: 3GPP access;

URSP规则2URSP rule 2:

Priority:2、Traffic filter: App=App1, App2、Direct offload: Permitted、Slice Info: S-NSSAI-a、Access Type: Non-3GPP access。

目前, 对于URSP策略已经制定了相关的内容, 如表1和表2所示。

表1: 用户路径选择规则UE Route Selection Policy Rule

Information name	Description	Category	PCF permitted to modify in a UE context	Scope
------------------	-------------	----------	---	-------

-4-

Rule Precedence	Determines the order the URSP rule is enforced in the UE.	Mandatory (NOTE 1)	Yes	UE context
Traffic descriptor	This part defines the traffic descriptors for the policy			
Application identifiers	Application identifier(s)	Optional	Yes	UE context
IP descriptors	IP 3 tuple(s) (destination IP address or IPv6 network prefix, destination port number, protocol ID of the protocol above IP)	Optional	Yes	UE context
Non-IP descriptors	Descriptor(s) for non-IP traffic	Optional	Yes	UE context
List of Route Selection Descriptors	A list of Route Selection Descriptors. The components of a Route Selection Descriptor are described in table 6.6.2-2.	Mandatory		
NOTE 1: Rules in a URSP shall have different precedence values.				

表2: 路径选择描述符

Information name	Description	Category	PCF permitted to modify in a UE context	Scope
Route Selection Descriptor Precedence	Determines the order in which the Route Selection Descriptors are to be applied.	Mandatory (NOTE 1)	Yes	UE context
Route selection components	This part defines the route selection components	Mandatory (NOTE 2)		
SSC Mode Selection	One single value of SSC mode.	Optional	Yes	UE context
Network Slice Selection	Either one single value or a list of values of S-NSSAI(s).	Optional	Yes	UE context
DNN Selection	Either one single value or a list of values of DNN(s).	Optional	Yes	UE context
Non-seamless Offload indication	Indicates if the traffic of the matching application is to be offloaded to non-3GPP access outside of a PDU Session.	Optional (NOTE 3)	Yes	UE context
Access Type preference	Indicates the preferred Access Type (3GPP or non-3GPP) when the UE establishes a PDU Session for the matching application.	Optional	Yes	UE context
NOTE 1: Every Route Selection Descriptors in the list shall have a different precedence value.				
NOTE 2: At least one of the route selection component shall be present.				
NOTE 3: If this indication is present in a Route Selection Descriptor, no other components shall be included in the Route Selection Descriptor.				

举例来说,如图1B所示,其中,USRP规则1-N表示UE policy第一部分,对应policy ID: PSI1, USRP规则1-M表示UE policy第二部分,对应policy ID: PSI2, ANDSP表示UE policy第三部分,对应policy ID: PSI3。因此在网络侧通常是一个SUPI对应一个或多个PSI。对于PSI的使用,是在初始注册Initial registration

请求消息中，将终端现有保存的策略分段标识PSI加入进来，传送给分组控制功能PCF网元，这样分组控制功能PCF网元可以知道当前终端存储的PSI是什么，然后按需进行UE Policy的调整。由于PSI添加在初始注册请求消息中是明文的，很容易被对方截获，就会带来如下安全问题：暴露终端的隐私信息，攻击者可能使用该信息进行非法行为。

5 针对上述问题，本申请实施例提出以下实施例，下面结合附图进行详细描述。

请参阅图2A，图2A是本申请实施例提供的一种终端信息的传递方法，应用于上述示例通信系统中的网络设备，所述网络设备包括第一网元，该方法包括：

在201部分，所述第一网元接收来自终端的第一信息。

10 其中，所述第一网元可以为策略控制功能PCF网元。所述第一信息可以由所述终端经接入网RAN设备和接入及移动性管理功能AMF网元透传至所述PCF网元的。

其中，所述第一信息用于指示终端存储的终端策略，且该第一信息包括非明文呈现的内容。其中，所述非明文呈现的内容具体是指该第一信息中所包含的用于指示终端的设备标识（对应用户ID）的内容是非明文标识信息，该非明文标识信息具体可以是加密信息（包括加密成SUCI形式或由其他秘钥如第一秘钥加密和/或第二秘钥进行完整性保护的情况）或者与终端策略有直接对应关系的不直接包含用户ID（如SUPI）的其他格式的标识信息。

15 在202部分，所述第一网元根据所述第一信息查询所述终端策略。

可以看出，本申请实施例中，网络设备的第一网元首先接收来自终端的第一信息，其次，根据所述第一信息查询所述终端策略，由于该第一信息是为非明文呈现的内容，故而可以避免第一网元与终端之间在传输该第一信息的过程中，该第一信息被非法窃取并直接利用，有利于提高终端策略的查询过程中网络侧与终端信息交互过程的安全性。

20 在一个可能的示例中，所述第一信息用于指示所述终端存储的终端策略；所述第一网元接收来自终端的第一信息之后，所述方法还包括：

所述第一网元根据所述第一信息查询所述终端策略。

25 在一个可能的示例中，所述第一信息包括一个策略分段标识PSI列表，所述PSI列表中的每个PSI参数由用户身份标识ID和特征ID表示。

举例来说，假设终端包括4个UE policy，分别为UE policy第一部分、UE policy第二部分、UE policy第三部分以及UE policy第四部分，其中UE policy第一部分用PSI1标识，UE policy第二部分用PSI2标识，UE policy第三部分用PSI3标识，UE policy第四部分用PSI4来标识，则如表3所示，第一信息可以包括一个如表3所示的PSI列表。

30

表3

终端的UE policy	PSI参数
UE policy第一部分	PSI1
UE policy第二部分	PSI2
UE policy第三部分	PSI3
UE policy第四部分	PSI4

其中，如图2B所示的用于标识UE policy的PSI参数的一种示例格式中，包括身份ID和特征ID两部分，该身份ID可以是SUPI或SUCI或MSISDN或Domain Name，该特征ID1则可以是UE policy的排序编号，如UE policy第一部分对应的特征ID为1，如UE policy第三部分对应的特征ID为3。

35 其中，如图2C所示的用于标识UE policy的PSI参数的另一种示例格式中，包括公共陆地移动网络PLMN和特征ID两部分，该PLMN+特征ID来唯一标识对应的UE policy的全球唯一性，该特征ID的bit数会非常大（数以亿计），且一个SUPI下面可以携带多个PSI ID，对于网络侧的影响较大。

在一个可能的示例中，所述第一信息包括一个用户ID和一个PSI列表，所述PSI列表中的每个PSI参数由特征ID表示。

举例来说，假设终端包括4个UE policy，分别为UE policy第一部分、UE policy第二部分、UE policy

第三部分以及UE policy第四部分，其中UE policy第一部分用特征ID1标识，UE policy第二部分用特征ID2标识，UE policy第三部分用特征ID3标识，UE policy第四部分用特征ID4标识，则如表4所示，第一信息可以包括一个如表4所示的PSI列表。

表4

终端的UE policy	PSI参数
UE policy第一部分	特征ID1
UE policy第二部分	特征ID2
UE policy第三部分	特征ID 3
UE policy第四部分	特征ID 4

- 5
- 其中，所述特征ID为网络侧（如第一网元）生成的特征码，该特征码与PSI对应的内容是一一对应的关系，网络侧可以根据该特征码索引到PSI对应的内容。
- 举例来说，如图2D所示，假设针对终端的4个PSI参数，具体包括PSI 1、PSI 2、PSI 3、PSI 4，网络侧针对每个PSI参数均随机生成一个特征码，具体包括特征ID1、特征ID2、特征ID3、特征ID4，则该4个特征码与4个PSI参数之间的对应关系可以是PSI 1对应特征ID1，PSI2对应特征ID2，PSI3对应特征ID3，PSI4对应特征ID4。
- 10
- 在一个可能的示例中，所述第一信息包括一个PLMN ID和一个PSI列表，所述PSI列表中的每个PSI参数由特征ID表示。
- 举例来说，假设终端包括4个UE policy，分别为UE policy第一部分、UE policy第二部分、UE policy第三部分以及UE policy第四部分，其中UE policy第一部分用特征ID1标识，UE policy第二部分用特征ID2标识，UE policy第三部分用特征ID3标识，UE policy第四部分用特征ID4标识，则如图2E所示，第一信息可以包括PLMN ID和PSI列表。
- 15
- 在一个可能的示例中，所述第一信息包括一个PSI列表，所述PSI列表中的每个PSI参数由PLMN ID和特征ID表示。
- 举例来说，假设终端包括4个UE policy，分别为UE policy第一部分、UE policy第二部分、UE policy第三部分以及UE policy第四部分，其中UE policy第一部分用PLMN ID+特征ID1标识，UE policy第二部分用PLMN ID+特征ID2标识，UE policy第三部分用PLMN ID+特征ID3标识，UE policy第四部分用PLMN ID+特征ID4标识，则如图2F所示，第一信息可以包括一个如图2F所示的PSI列表。
- 20
- 在一个可能的示例中，所述PSI列表中的PSI参数是全球唯一的；或者，所述PSI列表中的PSI参数是PLMN内唯一的。
- 25
- 在一个可能的示例中，所述用户ID或所述PSI参数包括以下任意一种：签约用户永久标识SUPI、签约用户加密标识SUCI、移动台国际用户识别码MSISDN、域名Domain Name。
- 其中，所述特征ID用于指示用户ID约束下的预设数量个终端策略中的任意一个策略，在所述用户ID为SUPI或SUCI时，所述预设数量小于预设阈值，所述预设阈值可以是10。
- 30
- 在一个可能的示例中，当所述用户ID不是SUPI时，所述方法还包括：
所述第一网元向第二网元查询所述用户ID对应的SUPI值。
- 在一个可能的示例中，所述第二网元具备签约标识去隐藏功能SIDE。
- 在一个可能的示例中，所述第一网元根据所述第一信息查询所述终端策略，包括：
所述第一网元使用所述SUPI和/或所述特征ID向第三网元查询所述终端策略
- 35
- 在一个可能的示例中，所述第一网元根据所述第一信息查询所述终端策略，包括：
所述第一网元使用所述终端上报的所述第一信息中的PSI参数直接向所述第三网元查询所述终端策略。
- 在一个可能的示例中，所述第三网元为核心网数据存储网元。
- 在一个可能的示例中，所述第一信息为终端向所述第一网元传送的数据，所述数据的部分或全部信息通过第一秘钥加密和/或第二秘钥进行完整性保护。

在一个可能的示例中,所述方法还包括:所述第一网元根据所述第一信息解密和/或检查完整性以得到第一内容。

在一个可能的示例中,所述方法还包括:所述第一网元根据所述第一内容查询所述终端策略。

在一个可能的示例中,所述第一秘钥或所述第二秘钥由第三秘钥经过预设算法生成。

5 在一个可能的示例中,所述第三秘钥由第四网元发送到所述终端。

在一个可能的示例中,所述第四网元为网络侧的鉴权服务功能AUSF网元。

下面结合图2G,对PSI列表在注册请求消息中进行加密发送的处理过程进行示例描述。

用户设备UE首先向基站发送初始请求消息(如注册请求消息);

基站接收到初始请求消息后,将该初始请求消息转发给核心网网元;

10 核心网网元接收到该初始请求消息后,与UE完成秘钥协商过程和算法协商过程;

UE使用秘钥和算法对PSI列表进行加密和/或完整性保护,通过上行非接入层NAS消息向核心网网元发送加密和/或完整性保护的PSI列表及相关内容;

核心网网元接收到NAS消息后,对PSI列表及相关内容进行解密和/或完整性校验,最后通过特定接口(如N7接口)将解密的PSI列表及其相关内容发送给PCF网元。

15 在一个可能的示例中,所述第一秘钥在所述第一网元和所述终端预先配置。

与图2A所示实施例一致的,请参阅图3A,图3A是本申请实施例提供的另一种终端信息的传递方法,应用于上述示例通信系统的网络设备,所述网络设备包括第一网元,该方法包括:

在3A01部分,所述第一网元接收来自终端的第一信息。

20 其中,所述第一信息包括一个策略分段标识PSI列表,所述PSI列表中的每个PSI参数由用户身份标识ID和特征ID表示。或者,所述第一信息包括一个用户ID和一个PSI列表,所述PSI列表中的每个PSI参数由特征ID表示。且所述PSI列表中的PSI参数是全球唯一的;或者,所述PSI列表中的PSI参数是PLMN内唯一的。

25 其中,所述用户ID或所述PSI参数包括以下任意一种:签约用户永久标识SUPI、签约用户加密标识SUCI、移动台国际用户识别码MSISDN、域名Domain Name、第一网元生成的编号和/或字符串,所述编号和/或字符串与用户ID或所述PSI参数内容是一一对应的。

其中,所述用户ID不是SUPI。

在3A02部分,所述第一网元向第二网元查询所述用户ID对应的SUPI值。

30 其中,所述第二网元具备签约标识去隐藏功能(subscription identifier de-concealing function, SIDF)。该第二网元例如可以是会话管理功能(Session Management Function, SMF)网元,此处不做唯一限定。

在3A03部分,所述第一网元使用所述SUPI和/或所述特征ID向第三网元查询所述终端策略。

其中,所述第三网元为核心网数据存储网元。

35 可以看出,本申请实施例中,网络设备的第一网元首先接收来自终端的第一信息,其次,向第二网元查询该第一信息中的用户ID对应的SUPI值,最后,使用所述SUPI和/或所述特征ID向第三网元查询所述终端策略,可见,由于第一网元与终端传输的第一信息并不直接包含用于指示终端的身份标识的SUPI,如此可以避免该第一信息在传输过程中被窃取并直接利用,有利于提高终端策略的查询过程中网络侧与终端信息交互过程的安全性。

与图2A和图3A实施例一致的,请参阅图3B,图3B是本申请实施例提供的一种终端信息的传递方法,应用于上述示例通信系统的网络设备,所述网络设备包括第一网元,该方法包括:

40 在3B01部分,所述第一网元接收来自终端的第一信息。

其中,所述第一信息包括一个策略分段标识PSI列表,所述PSI列表中的每个PSI参数由用户身份标识ID和特征ID表示。或者,所述第一信息包括一个用户ID和一个PSI列表,所述PSI列表中的每个PSI参数由特征ID表示。且所述PSI列表中的PSI参数是全球唯一的;或者,所述PSI列表中的PSI参数是PLMN内唯一的。

-8-

其中, 所述用户ID或所述PSI参数包括以下任意一种: 签约用户永久标识SUPI、签约用户加密标识SUCI、移动台国际用户识别码MSISDN、域名Domain Name、第一网元生成的编号和/或字符串, 所述编号和/或字符串与用户ID或所述PSI参数内容是一一对应的。

其中, 所述用户ID不是SUPI。

5 在3B02部分, 所述第一网元使用所述终端上报的所述第一信息中的PSI参数直接向第三网元查询所述终端策略。

其中, 所述第三网元为核心网数据存储网元。

10 可以看出, 本申请实施例中, 网络设备的第一网元首先接收来自终端的第一信息, 其次, 使用终端上报的所述第一信息中的PSI参数直接向第三网元查询所述终端策略。可见, 由于第一信息中的PSI参数不直接包含SUPI, 如此可以避免该第一信息在传输过程中被窃取并直接利用, 有利于提高终端策略的查询过程中网络侧与终端信息交互过程的安全性。

与图2A和图3A实施例一致的, 请参阅图3C, 图3C是本申请实施例提供的一种终端信息的传递方法, 应用于上述示例通信系统的网络设备, 所述网络设备包括第一网元, 该方法包括:

15 在3C01部分, 所述第一网元接收来自终端的第一信息。

其中, 所述第一信息为终端向所述第一网元传送的数据, 所述数据的部分或全部信息通过第一密钥加密。

在3C02部分, 所述第一网元根据所述第一信息解密和/或检查完整性以得到第一内容。

20 其中, 所述第一内容包括PSI相关信息, 或者, 可以包括UE policy的具体内容, 此处以包括PSI相关信息为例进行说明。

在3C03部分, 所述第一网元根据所述第一内容查询所述终端策略。

其中, 所述第一密钥或所述第二密钥由第三密钥经过预设算法生成。所述第三密钥由第四网元发送到所述终端。所述第四网元为网络侧的鉴权服务功能AUSF网元。

25 其中, 所述第一密钥在所述第一网元和所述终端预先配置。或者, 所述第一网元为策略控制功能PCF网元。

可以看出, 本申请实施例中, 网络设备的第一网元首先接收来自终端的第一信息, 其次, 根据所述第一密钥解密所述第一信息以得到相关信息, 最后, 根据所述相关信息查询所述终端的终端策略, 可见, 由于第一信息通过第一密钥加密, 如此可以避免该第一信息在传输过程中被窃取并直接利用, 有利于提高终端策略的查询过程中网络侧与终端信息交互过程的安全性。

30 与图2A、图3A-3C实施例一致的, 请参阅图4A, 图4A是本申请实施例提供的一种终端信息的传递方法, 应用于上述示例通信系统中的终端, 该方法包括:

在4A01部分, 所述终端接收来自第一网元的第二信息。

其中, 所述第一网元为网络设备中的网元。

35 其中, 所述第二信息用于指示终端存储的终端策略, 且该第二信息包括非明文呈现的内容。其中, 所述非明文呈现的内容具体是指该第二信息中所包含的用于指示终端的设备标识(对应用户ID)的内容是非明文标识信息, 该非明文标识信息具体可以是加密信息(包括加密成SUCI形式或由其他密钥如第一密钥加密和/或第二密钥进行完整性保护的情况)或者与终端策略有直接对应关系的不直接包含用户ID(如SUPI)的其他格式的标识信息。

40 在4A02部分, 所述终端根据所述第二信息查询所述终端策略。

可见, 本申请实施例中, 终端首先接收来自网络设备的第一网元的第一信息, 其次, 根据所述第二信息查询所述终端策略, 由于该第二信息是为非明文呈现的内容, 故而可以避免网络设备与终端之间在传输该第二信息的过程中, 该第二信息被非法窃取并直接利用, 有利于提高终端策略的查询过程中网络侧与终端信息交互过程的安全性。

在一个可能的示例中,所述第二信息包括一个策略分段标识PSI列表,所述PSI列表中的每个PSI参数由用户身份标识ID和特征ID表示。

在一个可能的示例中,所述第二信息包括一个PSI列表,所述PSI列表中的每个PSI参数由PLMN ID和特征ID表示。

5 在一个可能的示例中,所述第二信息包括一个用户ID和一个PSI列表,所述PSI列表中的每个PSI参数由特征ID表示。

在本可能的示例中,所述终端根据PLMN ID和PSI的对应关系来存储所述终端策略。

其中,在漫游场景下,回归属地的hPCF将策略发给vPCF,其中包含回归属地的PLMN ID和对应的PSI列表,同时vPCF自行添加拜访地的策略,形成拜访地的PLMN ID和对应的PSI列表,然后vPCF将两
10 组PLMN ID和对应的PSI列表在一条消息中发送给终端。

在一个可能的示例中,所述PSI列表中的PSI参数是全球唯一的;或者,所述PSI列表中的PSI参数是PLMN内唯一的。

在一个可能的示例中,所述用户ID或所述PSI参数包括以下任意一种:签约用户永久标识SUPI、签约用户加密标识SUCI、移动台国际用户识别码MSISDN、域名Domain Name、第一网元生成的编号和/或字符串,所述编号和/或字符串与用户ID或所述PSI参数内容是一一对应的。
15

在一个可能的示例中,当所述用户ID不是SUPI时,所述方法还包括:所述终端向第二网元查询所述用户ID对应的SUPI值。

在一个可能的示例中,所述第二网元具备标识去隐藏功能。

在一个可能的示例中,所述终端根据所述第二信息查询所述终端策略,包括:所述终端使用所述SUPI和/或所述特征ID向第三网元查询所述终端策略。
20

在一个可能的示例中,所述终端根据所述第二信息查询所述终端策略,包括:所述终端使用所述第一网元下发的所述第二信息中的PSI参数直接向第三网元查询所述终端策略。

在一个可能的示例中,所述第三网元为核心网数据存储网元。

在一个可能的示例中,所述第二信息为所述第一网元向所述终端传送的数据,所述数据的部分或全部信息通过第一密钥加密和/或第二密钥进行完整性保护。
25

在一个可能的示例中,所述方法还包括:所述终端根据所述第二信息解密和/或检查完整性以得到第二内容。

在一个可能的示例中,所述方法还包括:所述终端根据所述第二内容查询所述终端策略。

在一个可能的示例中,所述第一密钥或所述第二密钥由第三密钥经过预设算法生成。

30 在一个可能的示例中,所述第三密钥由第四网元发送到所述终端。

在一个可能的示例中,所述第四网元为网络侧的鉴权服务功能AUSF网元。

在一个可能的示例中,所述第一密钥在所述第一网元和所述终端预先配置。

在一个可能的示例中,所述第一网元为策略控制功能PCF网元。

在一个可能的示例中,所述终端接收来自第一网元的第二信息,包括:所述终端接收来自第一网元根据映射关系信息发送的第二信息,所述映射关系信息包括用户标识和PSI参数之间的对应关系。
35

在一个可能的示例中,所述映射关系信息中的每一个用户标识对应至少一个PSI参数。

在一个可能的示例中,所述映射关系信息中的一个PSI参数只对应于一个用户标识。

举例来说,如图4A1所示,假设用户标识包括3个,分别为User-1、User-2、User-3,PSI参数包括10个,分别为PSI1、PSI2、PSI3、PSI4、PSI5、PSI6、PSI7、PSI8、PSI9,其中,PSI1用于指示UE policy的内容1,PSI2用于指示UE policy的内容2,PSI3用于指示UE policy的内容3,PSI4用于指示UE policy的内容3,PSI5用于指示UE policy的内容4,PSI6用于指示UE policy的内容5,PSI7用于指示UE policy的内容10,PSI8用于指示UE policy的内容9,PSI9用于指示UE policy的内容10,则上述用户标识与PSI参数之间的映射关系可以是User-1对应PSI1、PSI2、PSI3,User-2对应PSI4、PSI5、PSI6、PSI7,User-3对应PSI8、PSI9。
40

其中, 上述用户标识与PSI参数之间的对应关系可以是网络侧存储。

在一个可能的示例中, 所述映射关系信息中的一个PSI参数至少对应于一个用户标识。

5 举例来说, 如图4A2所示, 假设用户标识包括3个, 分别为User-1、User-2、User-3, PSI参数包括n个(n为正整数), 分别为PSI1、PSI2、PSI3、.....PSIn, 其中, 其中PSI1用于指示UE policy的内容1, PSI2用于指示UE policy的内容2, PSI3用于指示UE policy的内容3, PSI4用于指示UE policy的内容3, 以此类推, PSIn用于指示UE policy的内容n, 则上述用户标识与PSI参数之间的对应关系可以是User-1对应PSI1、PSI3、PSI5, User-2对应PSI2、PSI3, User-3对应PSI4、PSI5、PSIn。

其中, 上述用户标识与PSI参数之间的对应关系可以是网络侧存储。

10 与图2A、图3A-3C、图4A实施例一致的, 请参阅图4B, 图4B是本申请实施例提供的一种终端信息的传递方法, 应用于上述示例通信系统的终端, 该方法包括:

在4B01部分, 所述终端接收来自第一网元的第二信息。

15 其中, 所述第二信息包括一个策略分段标识PSI列表, 所述PSI列表中的每个PSI参数由用户身份标识ID和特征ID表示。或者, 所述第二信息包括一个用户ID和一个PSI列表, 所述PSI列表中的每个PSI参数由特征ID表示。且所述PSI列表中的PSI参数是全球唯一的; 或者, 所述PSI列表中的PSI参数是PLMN内唯一的。

其中, 所述用户ID或所述PSI参数包括以下任意一种: 签约用户永久标识SUPI、签约用户加密标识SUCI、移动台国际用户识别码MSISDN、域名Domain Name、第一网元生成的编号和/或字符串, 所述编号和/或字符串与用户ID或所述PSI参数内容是一一对应的。

20 其中, 所述用户ID不是SUPI。

在4B02部分, 所述终端向第二网元查询所述用户ID对应的SUPI值。

其中, 所述第二网元具备签约标识去隐藏功能(subscription identifier de-concealing function, SIDF)。该第二网元例如可以是会话管理功能(Session Management Function, SMF)网元, 此处不做唯一限定。

在4B03部分, 所述终端使用所述SUPI和/或所述特征ID向第三网元查询所述终端策略。

25 其中, 所述第三网元为核心网数据存储服务网元。

可见, 本申请实施例中, 终端首先接收来自网络设备的第二信息, 其次, 向第二网元查询该第二信息中的用户ID对应的SUPI值, 最后, 使用所述SUPI和/或所述特征ID向第三网元查询终端策略, 可见, 由于终端与网络设备之间传输的第二信息并不直接包含用于指示终端的身份标识的SUPI, 如此可以避免该第二信息在传输过程中被窃取并直接利用, 有利于提高终端策略的查询过程中网络侧与终端信息交互过程的安全性。

30 与图2A、图3A-3C、图4A、图4B实施例一致的, 请参阅图4C, 图4C是本申请实施例提供的一种终端信息的传递方法, 应用于上述示例通信系统的终端, 该方法包括:

在4C01部分, 所述终端接收来自第一网元的第二信息。

其中, 所述第一网元为网络设备中的网元。

35 其中, 所述第二信息包括一个策略分段标识PSI列表, 所述PSI列表中的每个PSI参数由用户身份标识ID和特征ID表示。或者, 所述第二信息包括一个用户ID和一个PSI列表, 所述PSI列表中的每个PSI参数由特征ID表示。且所述PSI列表中的PSI参数是全球唯一的; 或者, 所述PSI列表中的PSI参数是PLMN内唯一的。

40 其中, 所述用户ID或所述PSI参数包括以下任意一种: 签约用户永久标识SUPI、签约用户加密标识SUCI、移动台国际用户识别码MSISDN、域名Domain Name、第一网元生成的编号和/或字符串, 所述编号和/或字符串与用户ID或所述PSI参数内容是一一对应的。

其中, 所述用户ID不是SUPI。

在4C02部分, 所述终端使用所述网络设备下发的所述第二信息中的PSI参数直接向第三网元查询所述终端策略。

其中，所述第三网元为核心网数据存储网元。

可见，本申请实施例中，终端首先接收来自网络设备下发的第二信息，其次，使用该第二信息中的PSI参数直接向第三网元查询所述终端策略。可见，由于第二信息中的PSI参数不直接包含SUPI，如此可以避免该第二信息在传输过程中被窃取并直接利用，有利于提高终端策略的查询过程中网络侧与终端信息交互过程的安全性。

与图2A、图3A-3C、图4A-4C实施例一致的，请参阅图4D，图4D是本申请实施例提供的一种终端信息的传递方法，应用于上述示例通信系统的终端，该方法包括：

在4D01部分，所述终端接收来自网络设备的第二信息。

其中，所述第二信息为终端向所述第一网元传送的数据，所述数据的部分或全部信息通过第一密钥加密。

其中，所述第一密钥或所述第二密钥由第三密钥经过预设算法生成。所述第三密钥由第四网元发送到所述终端。所述第四网元为网络侧的鉴权服务功能AUSF网元。

其中，所述第一密钥在所述第一网元和所述终端预先配置。或者，所述第一网元为策略控制功能PCF网元。

在4D02部分，所述终端根据所述第二信息解密和/或检查完整性以得到第二内容。

其中，所述第一内容包括PSI相关信息，或者，可以包括UE policy的具体内容，此处以包括PSI相关信息为例进行说明。

在4D03部分，所述终端根据所述第二内容查询所述终端策略。

可见，本申请实施例中，终端首先接收来自网络设备的第二信息，其次，根据所述第二信息解密和/或检查完整性以得到第二内容，最后，根据所述第二内容查询所述终端策略。由于第二信息必须通过解密和/或检查完整性才能够得到明文第二内容，从而查询到终端策略，如此可以避免该第二信息在传输过程中被窃取并直接利用，有利于提高终端策略的查询过程中网络侧与终端信息交互过程的安全性。

与上述实施例一致的，请参阅图5，图5是本申请实施例提供的一种网络设备的结构示意图，如图所示，该网络设备包括处理器、存储器、通信接口以及一个或多个程序，其中，所述一个或多个程序被存储在所述存储器中，并且被配置由所述处理器执行，所述程序包括用于执行以下步骤的指令；

接收来自终端的第一信息；所述第一信息用于指示终端存储的终端策略，且该第一信息为非明文呈现的内容。所述非明文呈现的内容具体是指该第一信息中所包含的用于指示终端的设备标识（对应用户ID）的内容是非明文标识信息，该非明文标识信息具体可以是加密信息（包括加密成SUCI形式或由其他密钥如第一密钥加密的情况）或者与终端策略有直接对应关系的不直接包含用户ID（如SUPI）的标识信息。

根据所述第一信息查询所述终端策略。

可以看出，本申请实施例中，网络设备的第一网元首先接收来自终端的第一信息，其次，根据所述第一信息查询所述终端策略，由于该第一信息是为非明文呈现的内容，故而可以避免第一网元与终端之间在传输该第一信息的过程中，该第一信息被非法窃取并直接利用，有利于提高终端策略的查询过程中网络侧与终端信息交互过程的安全性。

在一个可能的示例中，所述第一信息包括一个策略分段标识PSI列表，所述PSI列表中的每个PSI参数由用户身份标识ID和特征ID表示。

在一个可能的示例中，所述第一信息包括一个用户ID和一个PSI列表，所述PSI列表中的每个PSI参数由特征ID表示。

在一个可能的示例中，所述PSI列表中的PSI参数是全球唯一的；或者，所述PSI列表中的PSI参数是PLMN内唯一的。

在一个可能的示例中，所述用户ID或所述PSI参数包括以下任意一种：签约用户永久标识SUPI、签约用户加密标识SUCI、移动台国际用户识别码MSISDN、域名Domain Name、第一网元生成的编号和

/或字符串,所述编号和/或字符串与用户ID或所述PSI参数内容是一一对应的。

在一个可能的示例中,当所述用户ID不是SUPI时,所述程序还包括用于执行以下操作的指令:向第二网元查询所述用户ID对应的SUPI值。

在一个可能的示例中,所述第二网元具备签约标识去隐藏功能SIDF。

5 在一个可能的示例中,在所述第一网元根据所述第一信息查询所述终端策略方面,所述程序中的指令具体用于执行以下操作:使用所述SUPI和/或所述特征ID向第三网元查询所述终端策略。

在一个可能的示例中,当所述用户ID不是SUPI时,在所述第一网元根据所述第一信息查询所述终端策略方面,所述程序中的指令具体用于执行以下操作:使用所述终端上报的所述第一信息中的PSI参数直接向第三网元查询所述终端策略。

10 在一个可能的示例中,所述第三网元为核心网数据存储网元。

在一个可能的示例中,所述第一信息为终端向所述第一网元传送的数据,所述数据的部分或全部信息通过第一密钥加密;在所述根据所述第一信息查询所述终端策略方面,所述程序中的指令具体用于执行以下操作:根据所述第一密钥解密所述第一信息以得到相关信息;以及用于根据所述相关信息查询所述终端的终端策略。

15 在一个可能的示例中,所述第一密钥由第二密钥经过预设算法生成。

在一个可能的示例中,所述第二密钥由第四网元提供并经接入及移动性管理功能AMF网元发送到所述终端,所述第四网元为网络侧的鉴权服务功能AUSF网元。

在一个可能的示例中,所述第一密钥由网络侧预先配置给所述终端。

在一个可能的示例中,所述第一网元为策略控制功能PCF网元。

20

与上述实施例一致的,请参阅图6,图6是本申请实施例提供的一种终端的结构示意图,如图所示,该终端包括处理器、存储器、通信接口以及一个或多个程序,其中,所述一个或多个程序被存储在所述存储器中,并且被配置由所述处理器执行,所述程序包括用于执行以下步骤的指令;

25 接收来自网络设备的第二信息。所述第二信息用于指示终端存储的终端策略,且该第二信息为非明文呈现的内容。所述非明文呈现的内容具体是指该第二信息中所包含的用于指示终端的设备标识(对应用户ID)的内容是非明文标识信息,该非明文标识信息具体可以是加密信息(包括加密成SUCI形式或由其他密钥如第一密钥加密和/或第二密钥进行完整性保护的情况)或者与终端策略有直接对应关系的不直接包含用户ID(如SUPI)的标识信息。

根据所述第二信息查询所述终端策略。

30 可以看出,本申请实施例中,终端首先接收来自网络设备的第二信息,其次,根据所述第二信息查询所述终端策略,由于该第二信息是为非明文呈现的内容,故而可以避免第一网元与终端之间在传输该第二信息的过程中,该第二信息被非法窃取并直接利用,有利于提高终端策略的查询过程中网络侧与终端信息交互过程的安全性。

35 在一个可能的示例中,所述第二信息包括一个策略分段标识PSI列表,所述PSI列表中的每个PSI参数由用户身份标识ID和特征ID表示。

在一个可能的示例中,所述第二信息包括一个用户ID和一个PSI列表,所述PSI列表中的每个PSI参数由特征ID表示。

在一个可能的示例中,所述PSI列表中的PSI参数是全球唯一的;或者,所述PSI列表中的PSI参数是PLMN内唯一的。

40 在一个可能的示例中,所述用户ID或所述PSI参数包括以下任意一种:签约用户永久标识SUPI、签约用户加密标识SUCI、移动台国际用户识别码MSISDN、域名Domain Name、第一网元生成的编号和/或字符串,所述编号和/或字符串与用户ID或所述PSI参数内容是一一对应的。

在一个可能的示例中,当所述用户ID不是SUPI时,所述程序还包括用于执行以下操作的指令:向第二网元查询所述用户ID对应的SUPI值。

在一个可能的示例中, 所述第二网元具备标识去隐藏功能。

在一个可能的示例中, 在所述根据所述第二信息查询所述终端策略方面, 所述程序中的指令具体用于执行以下操作: 使用所述SUPI和/或所述特征ID向第三网元查询所述终端策略。

5 在一个可能的示例中, 在所述根据所述第二信息查询所述终端策略方面, 所述程序中的指令具体用于执行以下操作: 使用所述第一网元下发的所述第二信息中的PSI参数直接向第三网元查询所述终端策略。

在一个可能的示例中, 所述第三网元为核心网数据存储网元。

在一个可能的示例中, 所述第二信息为所述第一网元向所述终端传送的数据, 所述数据的部分或全部信息通过第一秘钥加密和/或第二秘钥进行完整性保护。

10 在一个可能的示例中, 所述程序还包括用于执行以下操作的指令: 根据所述第二信息解密和/或检查完整性以得到第二内容。

在一个可能的示例中, 所述程序还包括用于执行以下操作的指令: 根据所述第二内容查询所述终端策略。

在一个可能的示例中, 所述第一秘钥或所述第二秘钥由第三秘钥经过预设算法生成。

15 在一个可能的示例中, 所述第三秘钥由第四网元发送到所述终端。

在一个可能的示例中, 所述第四网元为网络侧的鉴权服务功能AUSF网元。

在一个可能的示例中, 所述第一秘钥在所述第一网元和所述终端预先配置。

在一个可能的示例中, 所述第一网元为策略控制功能PCF网元。

20 上述主要从各个网元之间交互的角度对本申请实施例的方案进行了介绍。可以理解的是, 终端和网络设备为了实现上述功能, 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使用不同方法来实现所述的功能, 但是这种实现不应认为超出本申请的范围。

25 本申请实施例可以根据上述方法示例对终端和网络设备进行功能单元的划分, 例如, 可以对应各个功能划分各个功能单元, 也可以将两个或两个以上的功能集成在一个处理单元中。上述集成的单元既可以采用硬件的形式实现, 也可以采用软件程序模块的形式实现。需要说明的是, 本申请实施例中对单元的划分是示意性的, 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。

30 在采用集成的单元的情况下, 图7示出了上述实施例中所涉及的网络设备的一种可能的功能单元组成框图。网络设备700包括: 处理单元702和通信单元703。处理单元702用于对网络设备的动作进行控制管理, 例如, 处理单元702用于支持网络设备执行图2A中的步骤201、202, 图3A中的步骤3A01、3A02、3A03, 图3B中的步骤3B01、3B02、图3C中的步骤3C01至3C03和/或用于本文所描述的技术的其它过程。通信单元703用于支持网络设备与其他设备的通信, 例如与图3C中示出的终端之间的通信。网络设备还可以包括存储单元701, 用于存储网络设备的程序代码和数据。

35 其中, 处理单元702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), 现场可编程门阵列(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。所述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。通信单元703可以是收发器、收发电路等, 存储单元701可以是存储器。

40 其中, 所述处理单元702用于通过所述通信单元703接收来自终端的第一信息。其中, 所述第一信息用于指示终端存储的终端策略, 且该第一信息为非明文呈现的内容。所述非明文呈现的内容具体是指

该第一信息中所包含的用于指示终端的设备标识（对应用户ID）的内容是非明文标识信息，该非明文标识信息具体可以是加密信息（包括加密成SUCI形式或由其他秘钥如第一秘钥加密的情况）或者与终端策略有直接对应关系的不直接包含用户ID（如SUPI）的标识信息。以及用于根据所述第一信息查询所述终端策略。

5 可见，本示例中，网络设备的第一网元首先接收来自终端的第一信息，其次，根据所述第一信息查询所述终端策略，由于该第一信息是为非明文呈现的内容，故而可以避免第一网元与终端之间在传输该第一信息的过程中，该第一信息被非法窃取并直接利用，有利于提高终端策略的查询过程中网络侧与终端信息交互过程的安全性。

10 在一个可能的示例中，所述第一信息包括一个策略分段标识PSI列表，所述PSI列表中的每个PSI参数由用户身份标识ID和特征ID表示。

在一个可能的示例中，所述第一信息包括一个用户ID和一个PSI列表，所述PSI列表中的每个PSI参数由特征ID表示。

在一个可能的示例中，所述PSI列表中的PSI参数是全球唯一的；或者，所述PSI列表中的PSI参数是PLMN内唯一的。

15 在一个可能的示例中，所述用户ID或所述PSI参数包括以下任意一种：签约用户永久标识SUPI、签约用户加密标识SUCI、移动台国际用户识别码MSISDN、域名Domain Name、第一网元生成的编号和/或字符串，所述编号和/或字符串与用户ID或所述PSI参数内容是一一对应的。

在一个可能的示例中，当所述用户ID不是SUPI时，所述处理单元702还用于：通过所述通信单元703向第二网元查询所述用户ID对应的SUPI值。

20 在一个可能的示例中，所述第二网元具备签约标识去隐藏功能SIDF。

在一个可能的示例中，在所述根据所述第一信息查询所述终端策略，所述处理单元702具体用于：使用所述SUPI和/或所述特征ID通过所述通信单元703向第三网元查询所述终端策略。

25 在一个可能的示例中，当所述用户ID不是SUPI时，在所述根据所述第一信息查询所述终端策略方面，所述处理单元702具体用于：使用所述终端上报的所述第一信息中的PSI参数直接向第三网元查询所述终端策略。

在一个可能的示例中，所述第三网元为核心网数据存储网元。

30 在一个可能的示例中，所述第一信息为终端向所述第一网元传送的数据，所述数据的部分或全部信息通过第一秘钥加密；在所述根据所述第一信息查询所述终端策略方面，所述处理单元702具体用于：根据所述第一秘钥解密所述第一信息以得到相关信息；以及用于根据所述相关信息查询所述终端的终端策略。

在一个可能的示例中，所述第一秘钥由第二秘钥经过预设算法生成。

在一个可能的示例中，所述第二秘钥由第四网元提供并经接入及移动性管理功能AMF网元发送到所述终端，所述第四网元为网络侧的鉴权服务功能AUSF网元。

在一个可能的示例中，所述第一秘钥由网络侧预先配置给所述终端。

35 在一个可能的示例中，所述第一网元为策略控制功能PCF网元。

当处理单元702为处理器，通信单元703为通信接口，存储单元701为存储器时，本申请实施例所涉及的网络设备可以为图5所示的网络设备。

40 在采用集成的单元的情况下，图8示出了上述实施例中所涉及的终端的一种可能的功能单元组成框图。终端800包括：处理单元802和通信单元803。处理单元802用于对终端的动作进行控制管理，例如，处理单元802用于支持终端执行图4A中的步骤4A01、4A02，图4B中的步骤4B01-4B03、图4C中的4C01、4C02、图4D中的4D01至4D03和/或用于本文所描述的技术的其它过程。通信单元803用于支持终端与其他设备的通信，例如与图5中示出的网络设备之间的通信。终端还可以包括存储单元801，用于存储终端的程序代码和数据。

其中,处理单元 802 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),现场可编程门阵列(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。所述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。通信单元 803 可以是收发器、收发电路等,存储单元 801 可以是存储器。

其中,所述处理单元802用于通过所述通信单元803接收来自网络设备的第二信息。所述第二信息用于指示终端存储的终端策略,且该第二信息为非明文呈现的内容。所述非明文呈现的内容具体是指该第二信息中所包含的用于指示终端的设备标识(对应用户ID)的内容是非明文标识信息,该非明文标识信息具体可以是加密信息(包括加密成SUCI形式或由其他秘钥如第一秘钥加密和/或第二秘钥进行完整性保护的情况)或者与终端策略有直接对应关系的不直接包含用户ID(如SUPI)的标识信息。以及用于通过所述通信单元803根据所述第二信息查询所述终端策略。

可见,本示例中,终端首先接收来自网络设备的第二信息,其次,根据所述第二信息查询所述终端策略,由于该第二信息是为非明文呈现的内容,故而可以避免第一网元与终端之间在传输该第二信息的过程中,该第二信息被非法窃取并直接利用,有利于提高终端策略的查询过程中网络侧与终端信息交互过程的安全性。

在一个可能的示例中,所述第二信息包括一个策略分段标识PSI列表,所述PSI列表中的每个PSI参数由用户身份标识ID和特征ID表示。

在一个可能的示例中,所述第二信息包括一个用户ID和一个PSI列表,所述PSI列表中的每个PSI参数由特征ID表示。

在一个可能的示例中,所述PSI列表中的PSI参数是全球唯一的;或者,所述PSI列表中的PSI参数是PLMN内唯一的。

在一个可能的示例中,所述用户ID或所述PSI参数包括以下任意一种:签约用户永久标识SUPI、签约用户加密标识SUCI、移动台国际用户识别码MSISDN、域名Domain Name、第一网元生成的编号和/或字符串,所述编号和/或字符串与用户ID或所述PSI参数内容是一一对应的。

在一个可能的示例中,当所述用户ID不是SUPI时,所述处理单元820还用于:通过所述通信单元803向第二网元查询所述用户ID对应的SUPI值。

在一个可能的示例中,所述第二网元具备标识去隐藏功能。

在一个可能的示例中,在所述根据所述第二信息查询所述终端策略方面,所述处理单元803具体用于:使用所述SUPI和/或所述特征ID通过所述通信单元803向第三网元查询所述终端策略。

在一个可能的示例中,在所述根据所述第二信息查询所述终端策略方面,所述处理单元802具体用于:使用所述第一网元下发的所述第二信息中的PSI参数直接通过所述通信单元803向第三网元查询所述终端策略。

在一个可能的示例中,所述第三网元为核心网数据存储网元。

在一个可能的示例中,所述第二信息为所述第一网元向所述终端传送的数据,所述数据的部分或全部信息通过第一秘钥加密和/或第二秘钥进行完整性保护。

在一个可能的示例中,所述处理单元802还用于:根据所述第二信息解密和/或检查完整性以得到第二内容。

在一个可能的示例中,所述处理单元802还用于:根据所述第二内容查询所述终端策略。

在一个可能的示例中,所述第一秘钥或所述第二秘钥由第三秘钥经过预设算法生成。

在一个可能的示例中,所述第三秘钥由第四网元发送到所述终端。

在一个可能的示例中,所述第四网元为网络侧的鉴权服务功能AUSF网元。

在一个可能的示例中,所述第一秘钥在所述第一网元和所述终端预先配置。

在一个可能的示例中, 所述第一网元为策略控制功能 PCF 网元。

当处理单元 802 为处理器, 通信单元 803 为通信接口, 存储单元 801 为存储器时, 本申请实施例所涉及的终端可以为图 6 所示的终端。

本申请实施例还提供了一种计算机可读存储介质, 其中, 所述计算机可读存储介质存储用于电子数
5 据交换的计算机程序, 其中, 所述计算机程序使得计算机执行如上述方法实施例中终端所描述的部分或全部步骤。

本申请实施例还提供了一种计算机可读存储介质, 其中, 所述计算机可读存储介质存储用于电子数
据交换的计算机程序, 其中, 所述计算机程序使得计算机执行如上述方法实施例中网络设备所描述的部分或全部步骤。

10 本申请实施例还提供了一种计算机程序产品, 其中, 所述计算机程序产品包括存储了计算机程序的非瞬时性计算机可读存储介质, 所述计算机程序可操作来使计算机执行如上述方法实施例中终端所描述的部分或全部步骤。该计算机程序产品可以为一个软件安装包。

本申请实施例还提供了一种计算机程序产品, 其中, 所述计算机程序产品包括存储了计算机程序的非瞬时性计算机可读存储介质, 所述计算机程序可操作来使计算机执行如上述方法中网络设备所描述的部分或全部步骤。该计算机程序产品可以为一个软件安装包。

15 本申请实施例所描述的方法或者算法的步骤可以以硬件的方式来实现, 也可以是由处理器执行软件指令的方式来实现。软件指令可以由相应的软件模块组成, 软件模块可以被存放于随机存取存储器 (Random Access Memory, RAM)、闪存、只读存储器 (Read Only Memory, ROM)、可擦除可编程只读存储器 (Erasable Programmable ROM, EPROM)、电可擦可编程只读存储器 (Electrically EPROM, EEPROM)、寄存器、硬盘、移动硬盘、只读光盘 (CD-ROM) 或者本领域熟知的任何其它形式的存储介质中。一种示例性的存储介质耦合至处理器, 从而使处理器能够从该存储介质读取信息, 且可向该存储介质写入信息。当然, 存储介质也可以是处理器的组成部分。处理器和存储介质可以位于 ASIC 中。另外, 该 ASIC 可以位于接入网设备、目标网络设备或核心网设备中。当然, 处理器和存储介质也可以作为分立组件存在于接入网设备、目标网络设备或核心网设备中。

20 本领域技术人员应该可以意识到, 在上述一个或多个示例中, 本申请实施例所描述的功能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或功能。所述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。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、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。所述可用介质可以是磁性介质 (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。

25 以上所述的具体实施方式, 对本申请实施例的目的、技术方案和有益效果进行了进一步详细说明, 所应理解的是, 以上所述仅为本申请实施例的具体实施方式而已, 并不用于限定本申请实施例的保护范围, 凡在本申请实施例的技术方案的基础之上, 所做的任何修改、等同替换、改进等, 均应包括在本申请实施例的保护范围之内。