

ICS 33.040.01

M 10

**YD**

# 中华人民共和国通信行业标准

YD/T 2911-2015

---

## 下一代网络移动性安全框架

Mobility security framework in NGN

(ITU-T Y.2760 Mobility Security Framework in NGN, MOD)

2015-07-14 发布

2015-10-01 实施

---

中华人民共和国工业和信息化部 发布

## 目 次

前 言	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	2
5 网络架构	3
5.1 安全威胁	4
5.2 安全需求	4
6 支持安全能力的相关功能实体	5
7 密钥管理与认证	5
7.1 密钥管理框架	5
7.2 认证	6
8 安全上下文建立	11
8.1 服务AM-FE与目标AM-FE间安全上下文传输	11
8.2 服务AR-FE与目标AR-FE间安全上下文传输	12
8.3 UE和HDC-FE间安全上下文传输	12
9 IP移动性安全	13
9.1 主机移动性安全	13
9.2 网络移动性安全	14
10 UE和HDC-FE间的安全	14
10.1 主机发起的UE与HDC-FE间安全联盟的建立	14
10.2 网络发起的UE与HDC-FE间的安全关联建立	15
11 传输功能层的安全	15
11.1 UE与接入节点功能模块的安全	15
11.2 UE与L3HEF（层3切换执行功能）	15
附录A（资料性附录） 若干实例	17
参考文献	20

## 前 言

本标准修改采用ITU-T Y.2760, 与ITU-T Y.2760相比主要差异如下:

——ITU-T Y.2760 中第 5 章“下一代网络的安全要求”, 在本标准中修改为第 5 章“网络架构”。

——ITU-T Y.2760 中第 11 章“UE 与 NID-FE 之间的安全”, 在本标准中没有包括。

本标准按照 GB/T 1.1-2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由中国通信标准化协会提出并归口。

本标准起草单位: 中兴通信股份有限公司、华为技术有限公司、中国移动通信集团公司。

本标准主要起草人: 韦银星、王鸿彦。

# 下一代网络移动性安全框架

## 1 范围

本标准描述下一代网络(NGN)传输层移动性安全框架,内容包括认证和密钥管理,安全上下文建立,IP移动性安全,传输层中移动性管理、控制和传输的安全。本标准涉及的场景包括相同和不同接入技术间的移动性,域内和域间的移动性。

本标准适用于下一代网络(NGN)传输层的移动性安全。

## 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅所注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

ITU-T Y. 2011 (2004)	下一代网络一般原理和通用参考模型
ITU-T Y.2012 (2010)	下一代网络的功能需求和架构
ITU-T Y.2014 (2010)	下一代网络中网络附着功能
ITU-T Y.2018 (2009)	下一代网络移动性管理和控制功能
ITU-T Q.1706 /Y.2801(2006)	下一代网络移动性管理需求
ITU-T Y.2701 (2007)	下一代网络版本1的安全需求
ITU-T Y.2704 (2010)	下一代网络的安全安全机制和过程
ITU-T Y.2000 增补 7(2008)	下一代网络版本 2 范围的补充
ITU-R M.1645 (2003)	IMT- 2000 和超 IMT2000 系统未来发展的框架和总体目标。
ITU-T X.805 (2003)	提供端到端通信系统的安全架构

## 3 术语和定义

下列术语和定义适用于本文件。

### 3.1

切换 Handover

给移动体移动期间和移动以后提供业务的能力,但对它们的业务级协议有某些影响。

### 3.2

移动性 Mobility

用户或其它移动实体不因其位置或技术环境的改变而进行传递和接入业务的能力。

### 3.3

水平移动性 Horizontal Mobility

相同层次上的移动性。一般它被称为在相同接入技术内的移动性。

### 3.4

垂直移动性 Vertical Mobility

不同层次之间的移动性。一般它被称为不同接入技术之间的移动性。

### 3.5

下一代网络传输层 NGN Transport Stratum

NGN的一部分, 为用户提供传输数据的功能, 在终结实体之间控制和管理传输资源来传输这些数据。

### 3.6

信任 Trust

实体X信任实体Y是指当且仅当实体X信赖实体Y以某种特定的方式执行一组活动。

### 3.7

安全上下文 Security Context

一组安全参数, 包括标识符、密钥材料、密码算法等。

## 4 缩略语

下列缩略语适用于本文件。

3G	3rd Generation	第三代
ABG-FE	Access Border Gateway Functional Entity	接入边界网关功能实体
AE	Authentication Extension	认证扩展
AKA	Authentication and Key Agreement	认证和密钥协商
AM-FE	Access Management Functional Entity	接入管理功能实体
AN-FE	Access Node Functional Entity	接入节点功能实体
ANI	Application to Network Interface	应用到网络接口
AR-FE	Access Relay Functional Entity	接入中继功能实体
DDoS	Distributed Deny of Service	分布式拒绝服务
EAP	Extensible Authentication Protocol	扩展认证协议
EN-FE	Edge Node Functional Entity	边界节点功能实体
FA	Foreign Agent	外部代理
HA	Home Agent	家乡代理
HDC-FE	Handover Decision and Control Functional Entity	切换决策与控制功能实体
IP	Internet Protocol	互联网协议
L3HEF	Layer 3 Handover Execution Function	层3切换执行功能
MIP	Mobile IP	移动IP
MIPv4	Mobile IP for IP version 4.	移动IP第四版
MIPv6	Mobile IP for IP version 6.	移动IP第六版
MLM-FE	Mobile Location Management Function	移动位置管理功能
MMCF	Mobility Management Control Functions	移动管理控制功能
MN	Mobile Node	移动节点
MOBIKE	IKEv2 Mobility and Multihoming Protocol	互联网密钥交换第二版移动和多穴协议
NACF	Network Attachment Control Functions	网络附着控制功能
NGN	Next Generation Network	下一代网络

NID-FE	Network Information Distribution Functional Entity	网络信息分发功能实体
NNI	Network to Network Interface	网络到网络接口
PKI	Public Key Infrastructure	公钥基础设施
PMIPv6	Proxy Mobile IPv6	代理移动IP第六版
RAN	Radio Access Network	无线接入网
RRP	Registration Reply	注册响应
RRQ	Registration Request	注册请求
TAA-FE	Transport Authentication and Authorization Functional Entity	传输认证和授权功能实体
TLM-FE	Transport Location Management Functional Entity	传输位置管理功能实体
TLS	Transport Layer Security	传输层安全
TTLS	Tunneled Transport Layer Security	隧道传输层安全
TUP-FE	Transport User Profile Functional Entity	传输用户属性功能实体
UE	User Equipment	用户设备
UNI	User to Network Interface	用户到网络接口
WiMax	Worldwide Interoperability for Microwave Access	全球互操作性微波接入
WLAN	Wireless LAN	无线局域网

## 5 网络架构

下一代网络 (NGN) 支持多种接入技术, 如 WLAN、WiMax 和 3G RAN 等。支持移动性是 NGN 的一个特性, 包括游牧和切换。在 NGN 版本 2 中, 切换覆盖不同接入技术网络和相同接入技术的场景。NGN 支持以下特性:

(1) 信任模型: NGN 安全信任模型定义了三个安全域: 信任、信任但脆弱的、不信任的。接入网在接入核心网前要通过安全网关。

(2) 支持多种接入技术。

(3) 支持多种移动性协议: MIPv4, MIPv6, DSMIPv6, PMIPv6, MOBIKE。

(4) 终端支持多模 UE: 如 WLAN, WiMax, 3G RAN 等。

(5) 支持业务连续性: 在异构接入系统间切换时保持业务连续性。

根据 NGN 框架, 定义五个安全特性组, 如图 1 所示。

(I): 最终用户功能与传输层间的安全: 保护最终用户功能和传输功能的接入网络实体之间的物理或逻辑安全; 包括最终用户功能和传输功能间 UNI 接口的安全。

(II): 最终用户功能与传输控制功能间的安全: 包括传输功能和传输控制功能接口间控制消息的安全; 关注最终用户功能和传输控制功能间 UNI 接口的安全。

(III): 最终用户功能与业务层间的安全: 包括传输控制功能实体与业务层间控制消息接口的安全; 关注最终用户功能与业务层间 UNI 接口的安全。

(IV): 业务层与应用实体间的安全: 包括最终用户功能与业务功能间 ANI 接口的安全。

(V): NGN 与其他网络间的安全: 包括 NGN 与其他网络间 NNI 接口的安全。

X.805 原理适用于本标准中提出的安全威胁和安全需求。

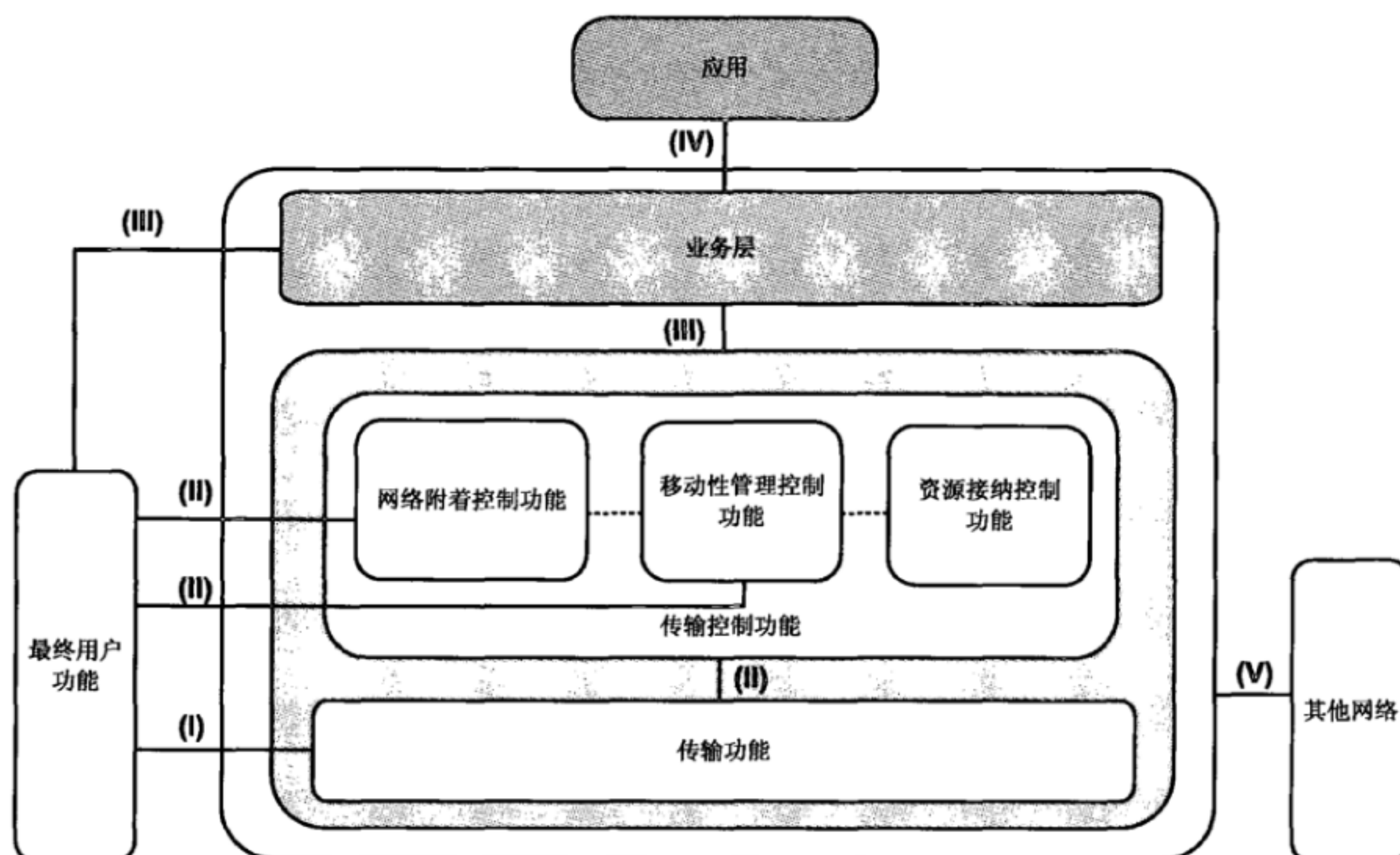


图 1 下一代网络移动性安全框架

### 5.1 安全威胁

下列安全威胁在ITU-T Y.2018中定义。

威胁 1: UE 未经授权向 MLM-FE 发起移动性信令。

威胁 2: 移动性信令可能被攻击者篡改。

威胁 3: MLM-FE 可能被假冒，这样可能会提供假信息给 UE。

威胁 4: UE 的位置可能被攻击者窃听。

威胁 5: 流量重定向攻击可能会发生。

威胁 6: 攻击者通过中间人攻击在路径上插入信息

威胁 7: DDoS 攻击可能消耗大量的网络资源

威胁 8: UE 可能未经授权来获取来自 HDC-FE 或 NID-FE 的信息

威胁 9: HDC-FE 或 NID-FE 可能被假冒，发送错误的信息给 UE。

威胁 10: UE 和 HDC-FE 或 NID-FE 间的信令可能被修改或窃听。

威胁 11: 用户面数据可能被窃听或修改。

### 5.2 安全需求

下列安全需求在ITU-T Y.2018中定义。

需求 1: UE 和 NID-FE 需要相互认证。

需求 2: UE 和 MLM-FE 间信令需要完整性和机密性保护。

需求 3: UE 和 MLM-FE 间的信令需要防止重放攻击。

需求 4: 网络需要提供对 UE 位置的隐私保护。

需求 5: UE 和 HDC-FE 需要相互认证。

需求 6: UE 和 HDC-FE 间的信令需要完整性和机密性保护。

需求 7: UE 和 HDC-FE 间的信令需要防止重放攻击。

需求 8: 网络需要提供低延迟的认证和信令保护。

需求 9: 安全上下文的传递需要被优化。

需求 10: 支持介质无关的移动性安全。

需求 11: 在 UE 和 EN-FE 间需要保护用户面流量。

需求 12: 支持多连接安全。

## 6 支持安全能力的相关功能实体

NGN中下列功能实体与移动性安全相关。

传输用户属性功能实体 (TUP-FE)

TUP-FE存储用户认证数据, 如密钥材料、认证方法和用户签约信息等。TUP-FE的详细功能描述见 ITU-T Y.2014。

传输认证授权功能实体 (TAA-FE)

TAA-FE从TUP-FE中提取认证数据和接入授权信息。TAA-FE也作为一个代理。详细的模式见 ITU-T Y.2014。

移动位置管理功能实体 (MLM-FE)

MLM-FE从NACF中获取认证、授权和记账信息, 和UE进行双向认证, 在UE与MLM-FE间创建安全关联。详细的模式描述见ITU-T Y.2018。

切换决策控制功能实体 (HDC-FE)

HDC-FE需要与UE建立安全关联, 经过TLM-FE从TAA-FE中获取安全密钥。详细的模式描述见ITU-T Y.2018。

网络信息分发功能实体 (NID-FE)

NID-FE需要和UE建立安全关联来保护网络选择之类的信息。NID-FE通过TLM-FE从TAA-FE中获取安全信息。详细的模式描述见ITU-T Y.2018。

接入管理功能实体 (AM-FE)

AM-FE转发网络接入请求至TAA-FE来认证用户、授权或拒绝网络接入、提取用户特定接入配置参数。AM-FE可以重用网络注册/认证数据来快速恢复而不需要反复地执行完整的注册/认证/配置过程。详细的模式描述见ITU-T Y.2014。

层3切换执行功能 (L3HEF)

L3HEF需要和UE建立安全关联来保护两者之间的流量。详细的模式描述见ITU-T Y.2018。

注: L3HEF的安全表达了UE和EN-FE之间用户面流量保护的安全需求。

接入节点功能实体 (AN-FE)

AN-FE需要和UE建立安全关联, 通过AM-FE从TAA-FE获取密钥材料。详细的模式描述见ITU-T Y.2018。

## 7 密钥管理与认证

### 7.1 密钥管理框架

NGN 移动性安全使用分层密钥派生机制。NGN 中有几类密钥材料, 如根密钥、会话密钥等。根密

钥是一种长期安全存储的凭据（例如，共享密钥或密码）。会话密钥是一种短期的由根密钥产生的密钥材料。在 NGN 中 UE 和认证实体（例如 TAA-FE/TUP-FE）存储共享的根密钥。

通常会话密钥材料是通过根密钥和其他密钥产生参数（如认证过程中协商信息）来产生的。会话密钥材料用于保护信令流量和用户流量。会话密钥可以进一步派生。密钥的推导机制依赖于特定的加密算法或协议。

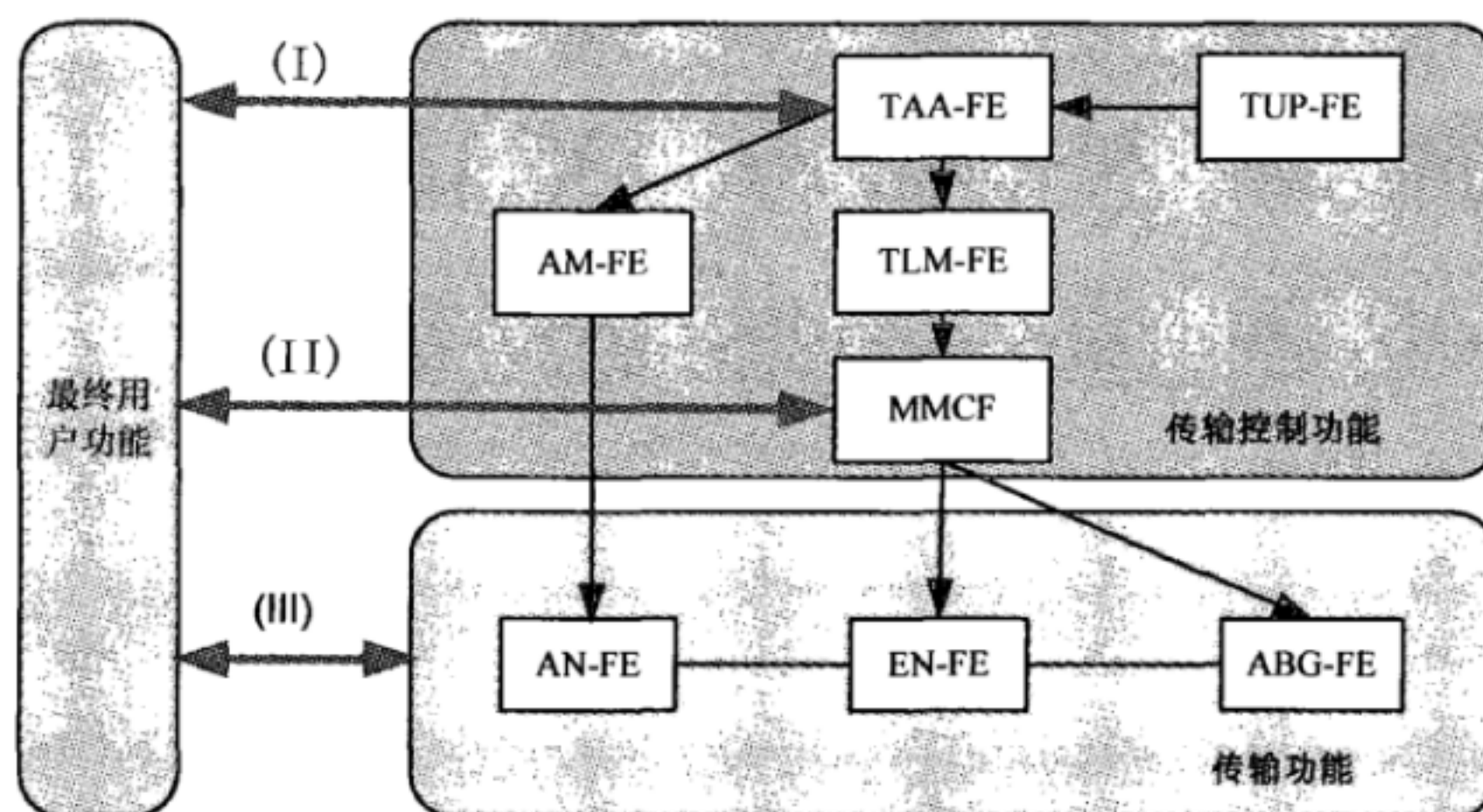


图2 下一代网络中移动性安全通用密钥框架

在图 2 中, 下一代网络中移动性安全通用密钥框架描述如下。

(I) UE 与 NGN 中功能实体执行相互认证的过程。在认证过程中, TUP-FE 基于根密钥材料产生认证矢量并发送这些认证矢量至 TAA-FE。双向认证过程成功结束后, TAA-FE 和 UE 生成会话密钥材料。会话密钥材料可用于生成子会话密钥材料。会话密钥材料传递到功能实体如 AM-FE、MMCF。AM-FE 和 MMCF 根据收到的会话密钥材料生成子会话密钥材料。

(II) UE 与 MMCF 间的安全关联是基于通过 TLM-FE 从 TAA-FE 获得的密钥材料。该会话密钥根据 TAA-FE 中会话密钥产生或推导。

(III) UE 与 NGN 传输层的安全关联基于共享密钥。该共享密钥由 TAA-FE、AM-FE 或 MMCF 中的会话密钥材料产生。AN-FE 通过 AM-FE 从 TAA-FE 中接收会话密钥。如果 AM-FE 有推导会话密钥材料的能力, AN-FE 直接从 AM-FE 中获取会话密钥材料。EN-FE 和 ABG-FE 通过 TLM-FE 和 MMCF 从 TAA-FE 中接收密钥材料。如果 MMCF 可以产生会话密钥, EN-FE 和 ABG-FE 可以直接从 MMCF 中获取密钥材料。

认证过程是基于挑战—响应协议。

## 7.2 认证

### 7.2.1 通用认证流程

在假设 UE 和 TAA-FE 均有快速再认证能力的前提下, 执行下列步骤, 如图 3 所示。

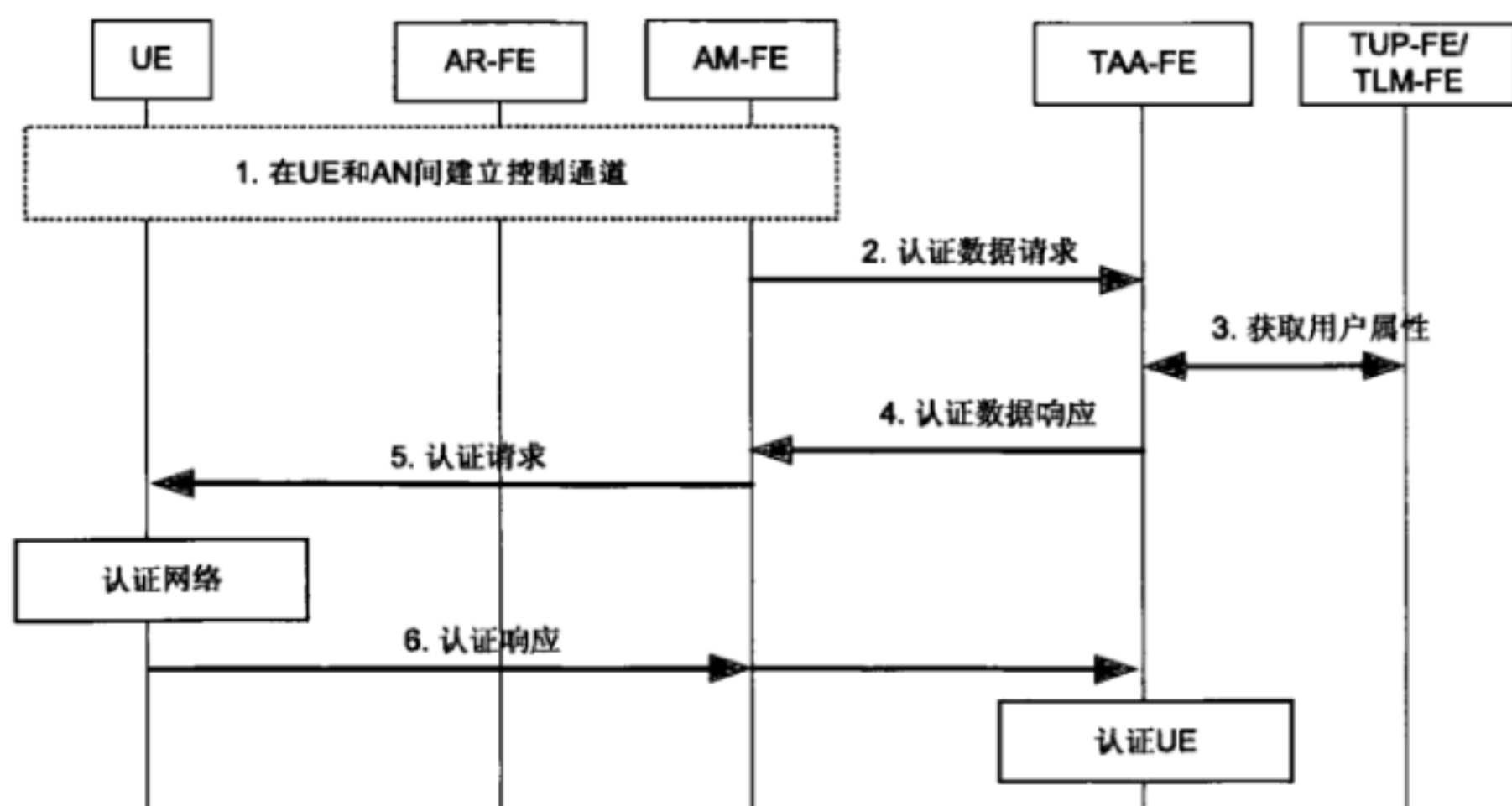


图3 通用认证流程

(1) UE 与接入网功能间建立控制通道（该过程不在本标准的范围内）。

(2) AM-FE 向 TAA-FE 发送 UE 的信息来请求认证数据。

(3) TAA-FE 从认证请求中获取认证信息，与 TUP-FE/TLM-FE 交互获取用户属性和包括认证令牌和会话密钥材料的认证矢量，其中认证信息包括用户 ID 和接入网信息。

(4) TAA-FE 发送包含认证令牌的认证数据响应到 AM-FE。

(5) AM-FE 发送认证请求至 UE。UE 从认证请求中获取认证令牌，产生本地认证矢量，该认证矢量包括基于认证令牌和根密钥的会话密钥材料。UE 通过验证收到的认证令牌来认证网络。

(6) UE 发送认证响应至 AM-FE，该响应包含 UE 产生的认证令牌。AM-FE 转发该信息到 TAA-FE。TAA-FE 获取认证令牌，TAA-FE 检查收到的认证令牌的有效性来认证 UE。

### 7.2.2 快速重认证流程

快速重认证用来减少切换时延。TUP-FE/TLM-FE 不参与快速重新认证过程，这使得认证过程速度更快，并减少 TUP-FE/TLM-FE 负载。推荐 UE 和 NGN 中的认证实体支持通用快速重认证。

假设 UE 和 TAA-FE 具备快速重认证能力的情况下执行下述步骤，如图 4 所示。

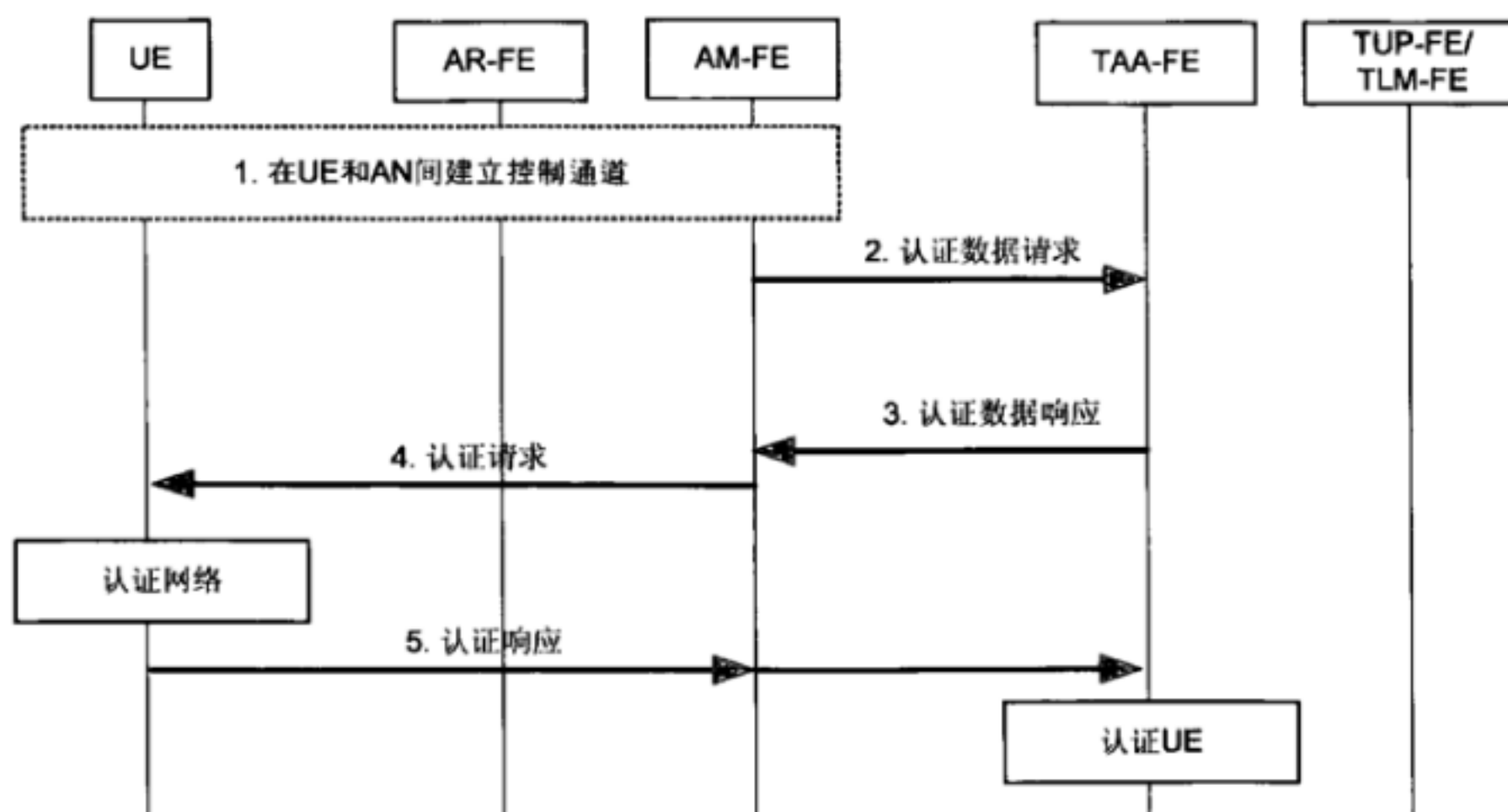


图4 通用快速重认证流程

(1) UE 与接入网功能间建立控制通道（该过程不在本标准的范围内）。

- (2) AM-FE 向 TAA-FE 发送 UE 的信息来请求认证数据。
- (3) TAA-FE 发送包含认证令牌的认证数据响应到 AM-FE。
- (4) AM-FE 发送认证请求至 UE。UE 从认证请求中获取认证令牌，产生本地认证矢量，该认证矢量包括基于认证令牌和根密钥的会话密钥材料。UE 通过验证收到的认证令牌来认证网络。
- (5) UE 发送认证响应至 AM-FE，该响应包含 UE 产生的认证令牌。AM-FE 转发该信息到 TAA-FE。TAA-FE 获取认证令牌，TAA-FE 检查收到的认证令牌的有效性来认证 UE。

7.2.2.1 优化的快速重认证

对于优化的快速重认证，UE 产生认证信息并由 NGN 网络首先认证 UE。该流程与通用重认证流程区别在于后者 NGN 网络产生认证令牌并首先由 UE 认证 NGN 网络。

优化的快速重认证流程执行如下步骤，如图 5 所示。

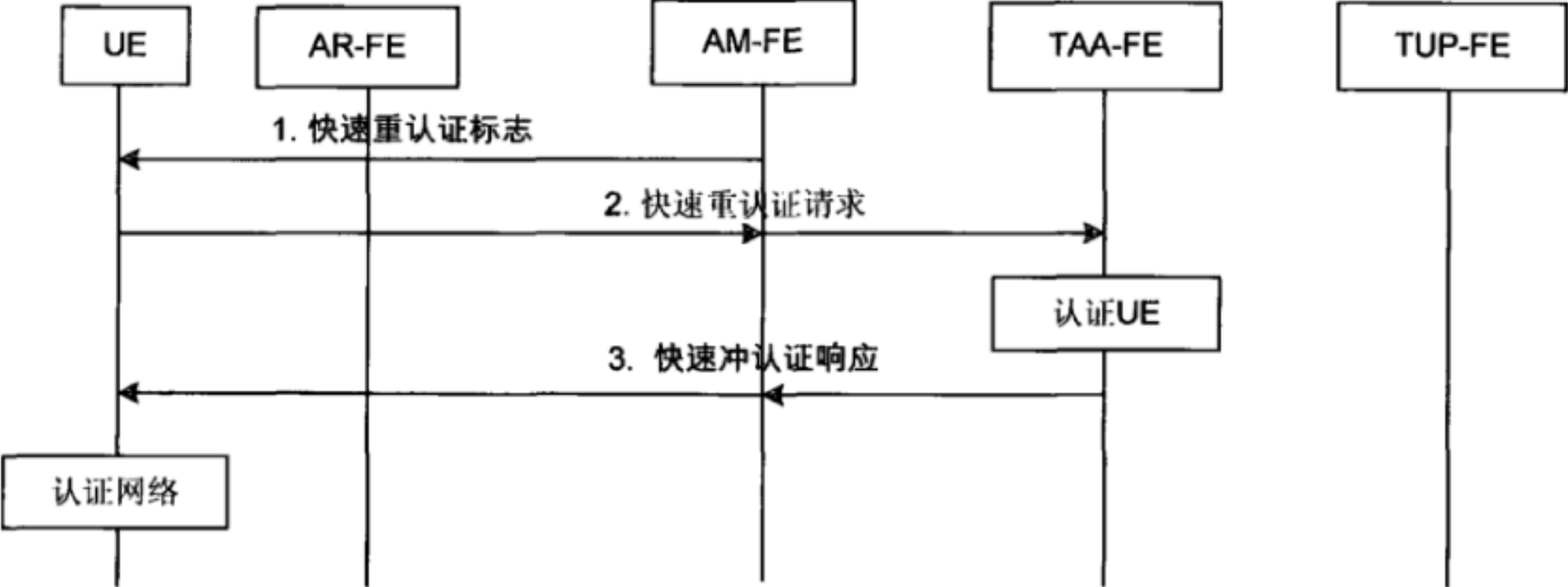


图 5 优化的快速重认证流程

- (1) UE 与接入网功能建立控制通道（该过程不在本标准的范围内）。AM-FE 发送优化的重认证标志到 UE，表示 TAA-FE 支持优化的快速重认证。
- (2) UE 产生认证矢量并通过 AM-FE 发送优化的重认证请求至 TAA-FE。优化的重认证请求包括认证令牌和重认证信息。TAA-FE 基于重认证信息和会话密钥材料产生本地认证矢量和新的会话密钥材料。TAA-FE 通过验证收到的认证令牌认证 UE。
- (3) TAA-FE 通过 AM-FE 发送包含认证令牌的重认证响应到 UE。UE 根据自己的认证矢量认证网络。当认证成功结束后，UE 产生子会话密钥。

7.2.3 域内认证

7.2.3.1 在单个网络连接中的认证

单个网络连接是指 UE 能够检测不同的网络，但是一次只能接入一个网络。预认证指 UE 切换到目标网络前通过服务网络与目标网络相互认证。预认证过程与通用认证过程类似。服务 AM-FE 和目标 AM-FE 涉及到预认证过程。

基于单网络连接的预认证执行如下步骤，如图 6 所示。

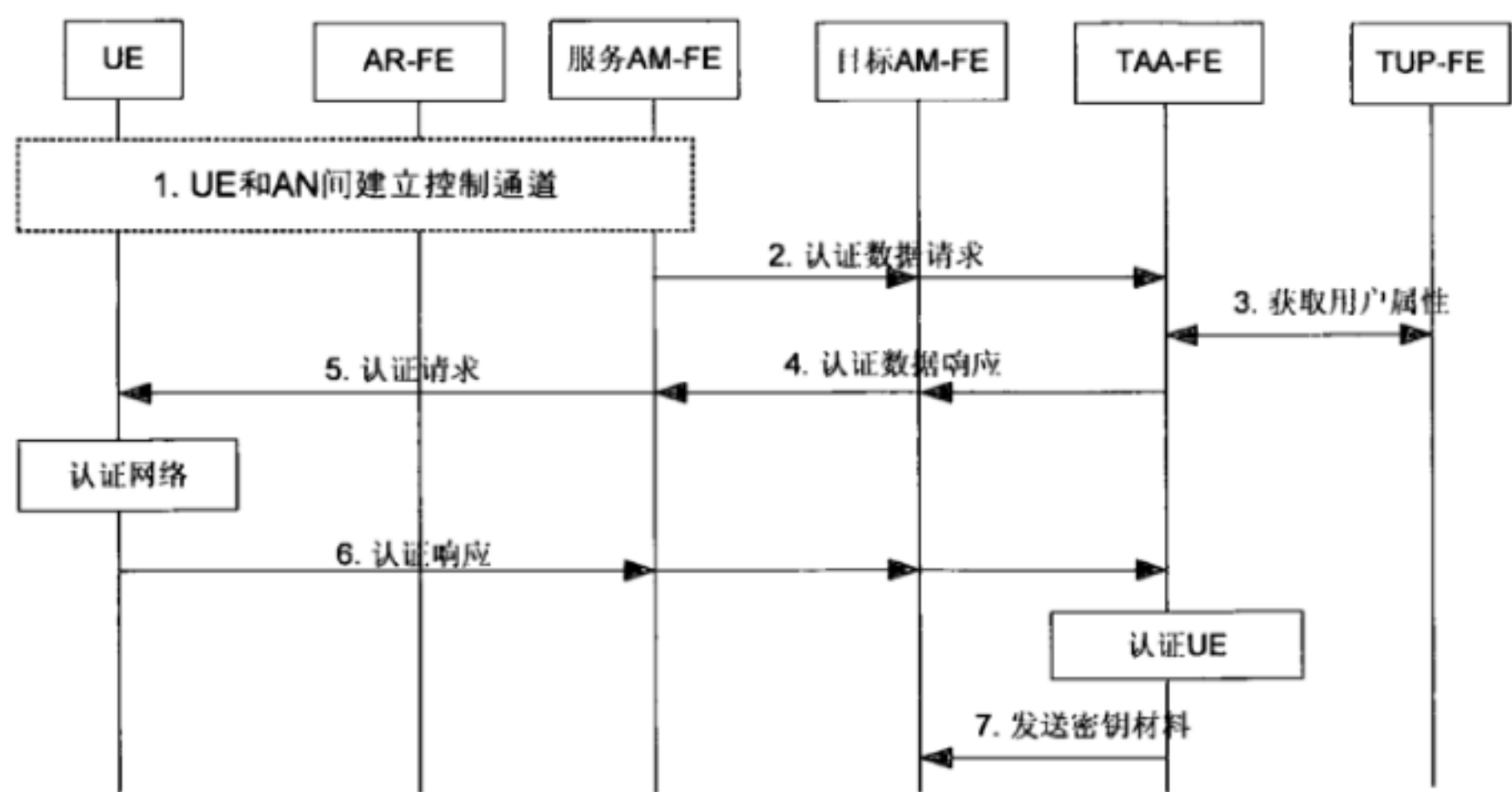


图6 基于单网络连接的预认证流程

- (1) UE 与接入网功能建立控制通道（该过程不在本标准的范围内）。
- (2) AM-FE 发送认证数据请求至 TAA-FE，该请求中包含用户签约信息。认证数据请求通过服务 AM-FE 和目标 AM-FE 进行转发。
- (3) TAA-FE 与 TUP-FE 交互获取用户属性。
- (4) TAA-FE 发送认证数据响应至目标 AM-FE 和服务 AM-FE，该响应中包括认证令牌。
- (5) 服务 AM-FE 发送认证请求至 UE。UE 获取认证令牌并根据认证信息认证网络。认证成功结束后，UE 产生会话密钥材料。
- (6) UE 发送认证响应至服务 AM-FE。服务 AM-FE 转发信息至目标 AM-FE 和 TAA-FE，该信息包含认证令牌。TAA-FE 提取认证令牌并认证 UE。当认证成功结束后，TAA-FE 产生会话密钥材料，在需要时可以导出子会话密钥。
- (7) TAA-FE 发送密钥材料至目标 AM-FE，在 UE 切换到目标网络后用于保护 UE 和目标网络间的通信。

7.2.4 域间认证

不同的管理域是指不同的 NGN 提供商。UE 在不同管理域之间的切换描述如下。  
不同管理域间认证执行如下步骤，如图 7 所示。

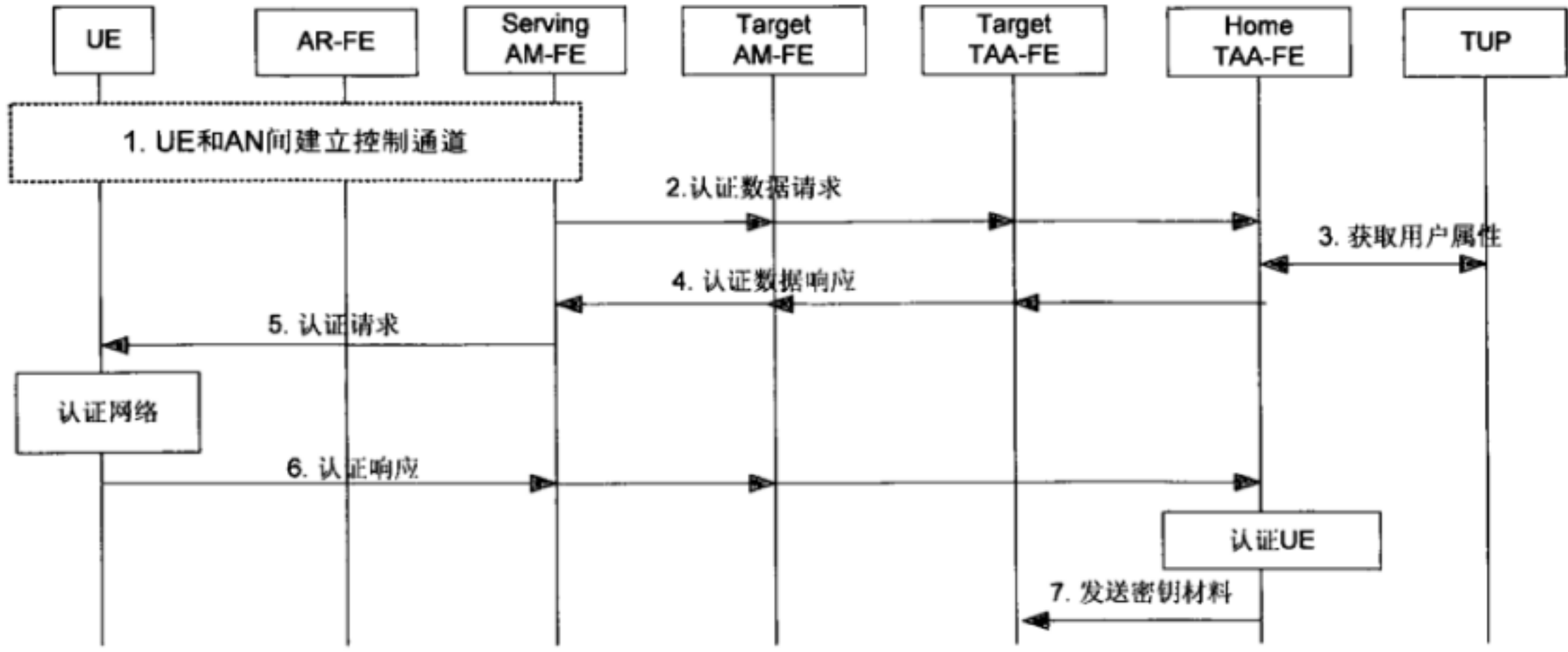


图7 不同管理域间认证流程

- (1) UE 与接入网功能建立控制通道（该过程不在本标准的范围内）。
- (2) 服务 AM-FE 发送认证数据请求至家乡 TAA-FE，该请求中包含用户签约信息。认证数据请求通过目标 AM-FE 和目标 TAA-FE 转发。
- (3) 家乡 TAA-FE 与 TUP-FE 交互获取用户属性。
- (4) 家乡 TAA-FE 包含认证令牌的认证数据请求至业务 AM-FE。认证数据请求通过 TAA-FE、目标 AM-FE 进行转发。
- (5) 业务 AM-FE 发送请求至 UE。UE 获取认证令牌。家乡 TAA-FE 提取认证令牌并认证 UE。认证成功结束后，家乡 TAA-FE 产生会话密钥材料，在需要时可以导出子会话密钥。
- (6) UE 发送包含认证令牌的认证响应至家乡 TAA-FE。家乡 TAA-FE 提取认证令牌并认证 UE。当认证成功结束后，家乡 TAA-FE 产生会话密钥材料，在需要时可以导出子会话密钥。
- (7) 当认证成功结束后，家乡 TAA-FE 发送密钥材料至目标 TAA-FE，在 UE 从服务网络切换到目标网络后用于保护 UE 和目标网络间的通信。

7.2.5 认证中的密钥映射机制

UE 从服务网络切换到目标网络，执行相互认证并产生会话密钥材料。NGN 支持不同的密钥推导机制，密钥材料映射用来协调用于不同密钥推导机制的密钥材料。

密钥材料映射执行如下步骤，如图 8 所示。

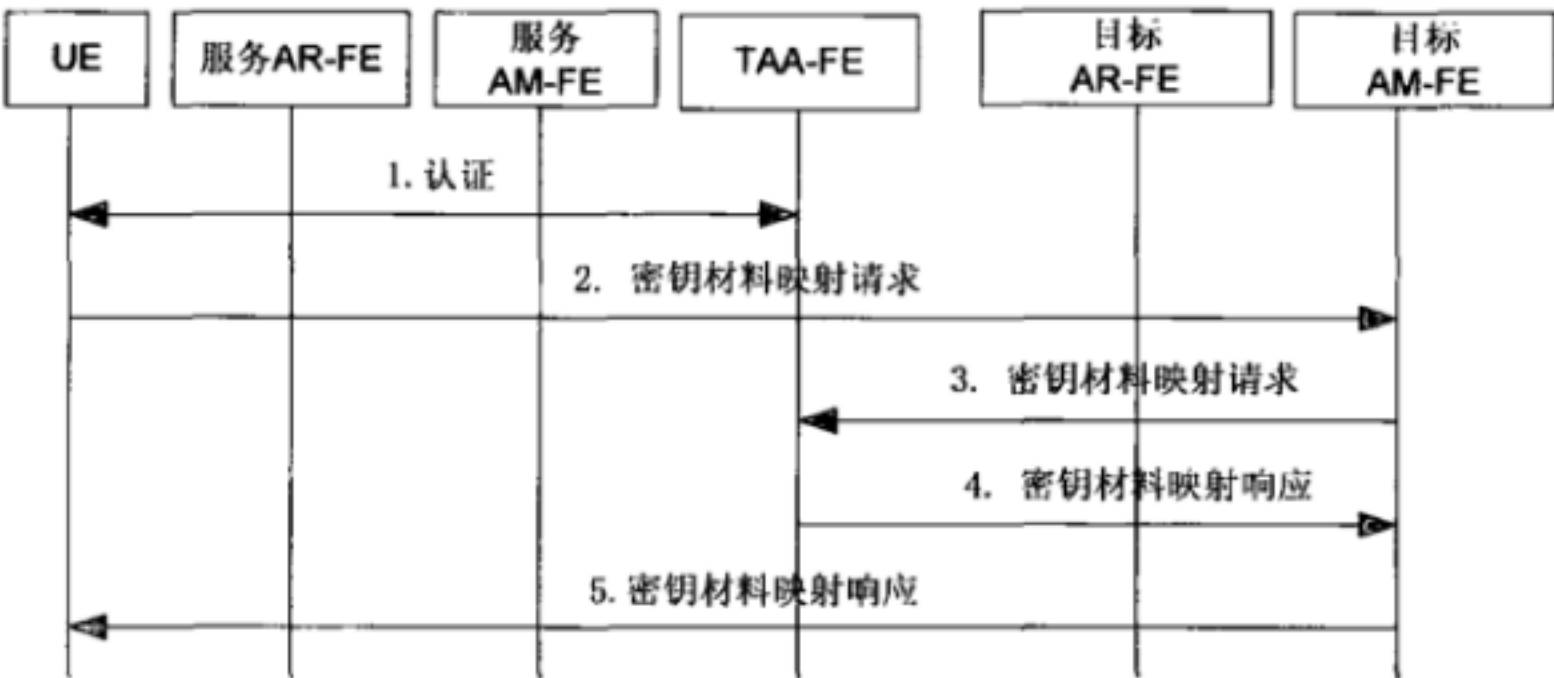


图 8 密钥材料映射流程

- (1) UE和TAA-FE间建立连接，认证过程结束后，产生会话密钥材料。
- (2) UE检测目标网络并准备切换到目标网络。UE发送密钥映射请求至目标AM-FE。密钥材料映射请求包括映射信息，例如当前密钥推导机制和支持的密钥推导机制。
- (3) 目标AM-FE发送密钥材料映射请求至TAA-FE。
- (4) TAA-FE接收密钥材料映射请求并把服务网络中密钥材料映射到目标网络中目标密钥材料，发送密钥材料映射响应至目标AM-FE。
- (5) 目标AM-FE发送映射响应至UE。UE在服务网络中把密钥材料映射到目标网络中目标密钥材料。UE和TAA-FE目标网络中目标密钥材料，用于保护UE和目标网络间的流量。

7.2.6 多网络接入认证

多网络接入指 UE 具有同时与多个接入网通讯的能力。当 UE 有多个网络接入能力时，UE 在断开业务网络前连接到目标网络并执行相互认证流程。相互认证见图 3 的通用认证流程。相互认证流程成功结束后，UE 和 TAA-FE 产生共享会话密钥材料，TAA-FE 发送共享密钥材料至目标 AM-FE。当 UE 移动到

目标网络时，UE 和目标网络间的流量有会话密钥材料或子会话密钥材料保护。

### 7.2.7 多连接认证

多连接是指 UE 同时与多个网络保持连接。不同类型网络连接可以为用户提供不同的用户体验，如高带宽、低时延和高安全。与不同管理域的多连接在本标准的范围外。

基于多连接的认证执行如下步骤，如图 9 所示。

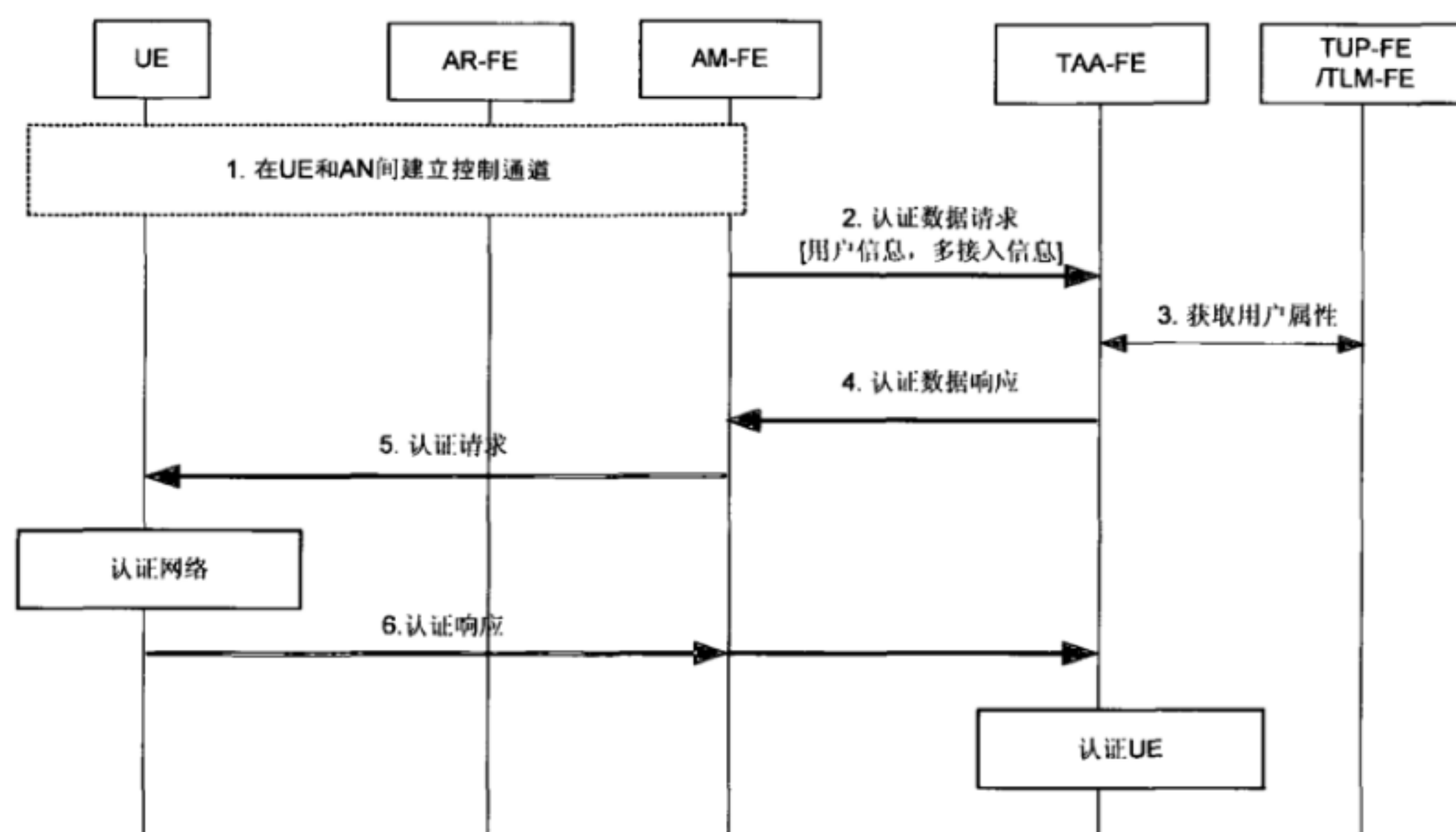


图 9 基于多连接的认证

(1) UE 与接入网功能间建立控制通道（该过程不在本标准的范围内）。UE 从接入网获取信息以及支持多接入认证的标志。

(2) AM-FE 发送认证数据请求至 TAA-FE。认证数据请求包括 UE 信息如签约信息（如用户签约 ID）、多接入信息（如多接入标志和多接入接口 ID）。

(3) TAA-FE 获取认证信息并与 TUP-FE/TLM-FE 交互来获取用户属性和认证矢量。认证矢量在 TUP-FE/TLM-FE 中产生，其中认证矢量包括认证令牌。

(4) TAA-FE 发送包括认证令牌的认证数据响应至 AM-FE。

(5) AM-FE 发送认证请求至 UE。UE 根据认证请求消息中的认证信息产生本地认证令牌。UE 根据本地认证令牌验证接收到的认证令牌来认证网络。认证成功结束后，UE 根据认证信息产生会话密钥材料。若设置多接入标志，UE 根据多接入信息产生多个会话密钥材料。

(6) UE 发送认证响应消息至 AM-FE。AM-FE 把包括由 UE 产生的认证令牌转发至 TAA-FE。TAA-FE 从认证响应消息中获取认证令牌并基于 TAA-FE 中认证矢量来认证 UE。认证成功结束后，TAA-FE 根据认证令牌产生会话密钥材料。若设置多接入标志，TAA-FE 根据多接入信息产生多个会话密钥材料。

## 8 安全上下文建立

### 8.1 服务 AM-FE 与目标 AM-FE 间安全上下文传输

服务 AM-FE 与目标 AM-FE 间安全上下文传输的流量应该被保护。服务 AM-FE 与目标 AM-FE 间的安全通过建立安全关联来实现。若两个 AM-FE 在相同的安全域，则不需要安全关联。若两个 AM-FE 在

不同的安全域，如不同的运营商域，则安全关联根据安全机制和运营商策略来创建。

## 8.2 服务 AR-FE 与目标 AR-FE 间安全上下文传输

当 UE 在服务 AR-FE 与目标 AR-FE 间进行上下文切换时，在服务 AR-FE 和目标 AR-FE 间安全上下文传输的流量应被保护。在服务 AR-FE 与目标 AR-FE 间的安全上下文传输安全通过建立安全关联来实现。

## 8.3 UE 和 HDC-FE 间安全上下文传输

### 8.3.1 主机发起的安全上下文传输

当 UE 决定从服务网络向目标网络切换时，UE 发送切换请求至 HDC-FE，触发安全上下文切换。当安全上下文传输结束后，目标 AM-FE 使用安全上下文保护 UE 和目标网络间的流量。主机发起的安全上下文传输执行如下步骤，如图 10 所示。

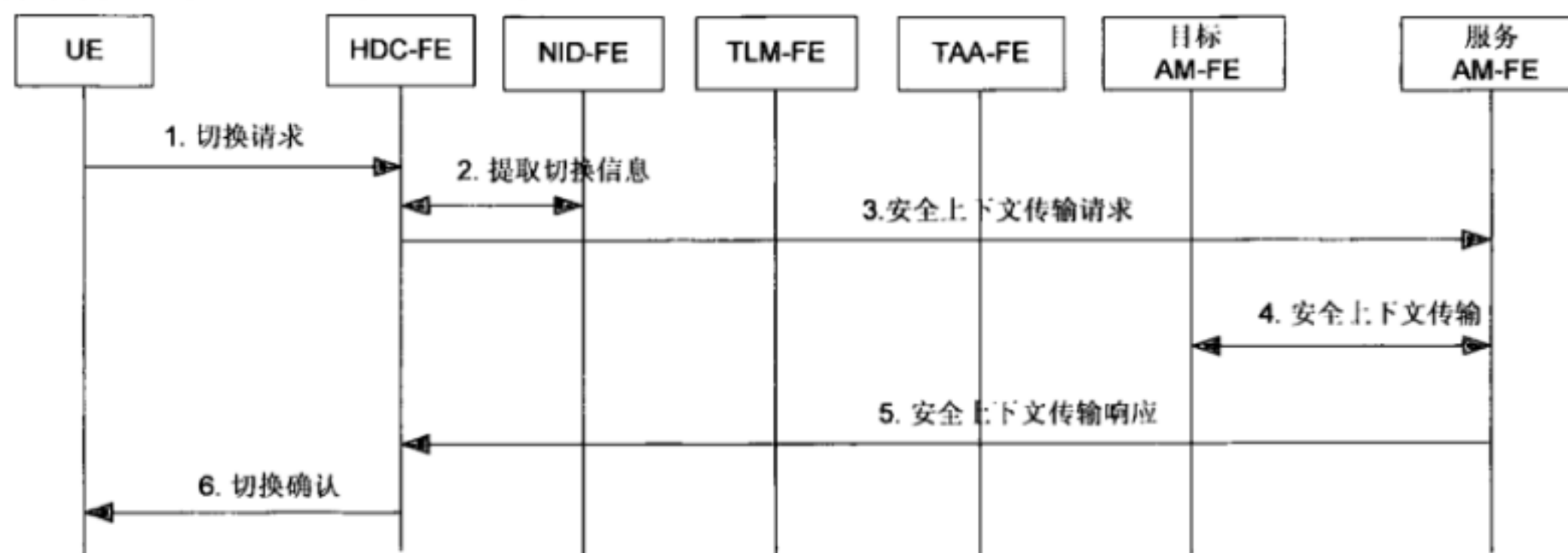


图 10 主机发起的安全上下文传输流程

- (1) UE发送切换请求至HDC-FE。
- (2) HDC-FE接收切换请求，与NID-FE交互获取切换相关的信息。
- (3) HDC-FE转发包含切换相关信息的切换请求至AM-FE。
- (4) 服务AM-FE与目标AM-FE交互来传输安全上下文。
- (5) 当安全上下文传输结束后，服务AM-FE发送安全上下文传输响应至HDC-FE。
- (6) HDC-FE接收安全上下文传输响应。若安全上下文传输成功结束，则HDC-FE发送切换请求确认至UE。

### 8.3.2 网络发起的安全上下文传输

当 HDC-FE 决定从服务网络到目标网络触发 UE 进行切换时，HDC-FE 发送切换引导消息来触发安全上下文传输。当安全上下文传输结束后，目标 AM-FE 使用安全上下文来保护 UE 和目标网络间的流量。网络发起的安全上下文传输执行如下步骤，如图 11 所示。

- (1) HDC-FE准备切换过程，发送切换引导开始消息至服务AM-FE来触发安全上下文传输。
- (2) 服务AM-FE与目标AM-FE交互来传输安全上下文。
- (3) 当安全上下文传输结束后，服务AM-FE发送切换引导结束消息至HDC-FE。
- (4) 当HDC-FE收到切换引导结束消息后，发送切换请求至UE开始切换过程。
- (5) 当切换结束后，UE发送切换确认消息指HDC-FE。

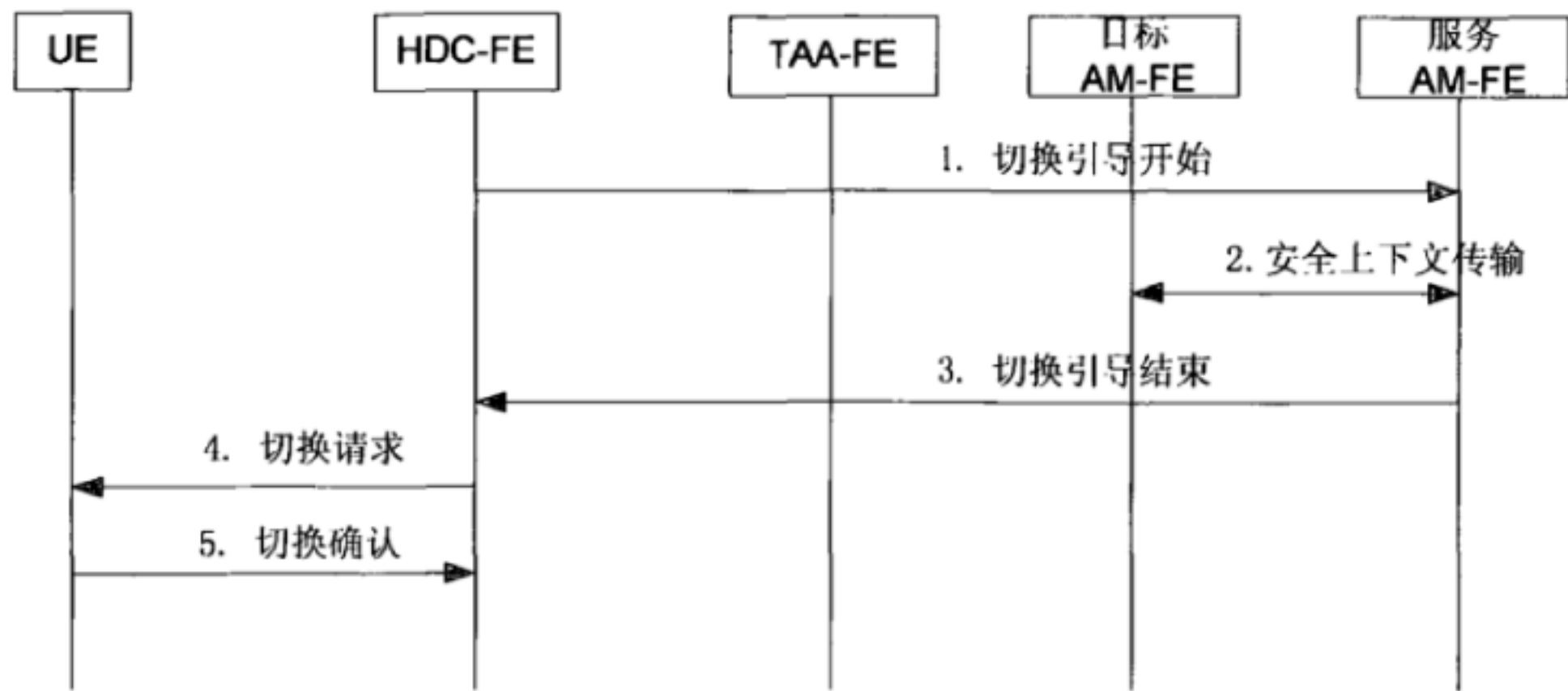


图 11 网络发起的安全上下文传输流程

9 IP 移动性安全

9.1 主机移动性安全

UE 和 MLM-FE (C) 间多基于主机多移动性控制流量需要保护。UE 和 MLM-FE (C) 间需要创建安全关联 (SA)。UE 和 MLM-FE (P) 间的 SA 是可选的。

假设UE和TAA-FE已完成通用认证过程，主机移动性安全的执行步骤如下，如图12所示。

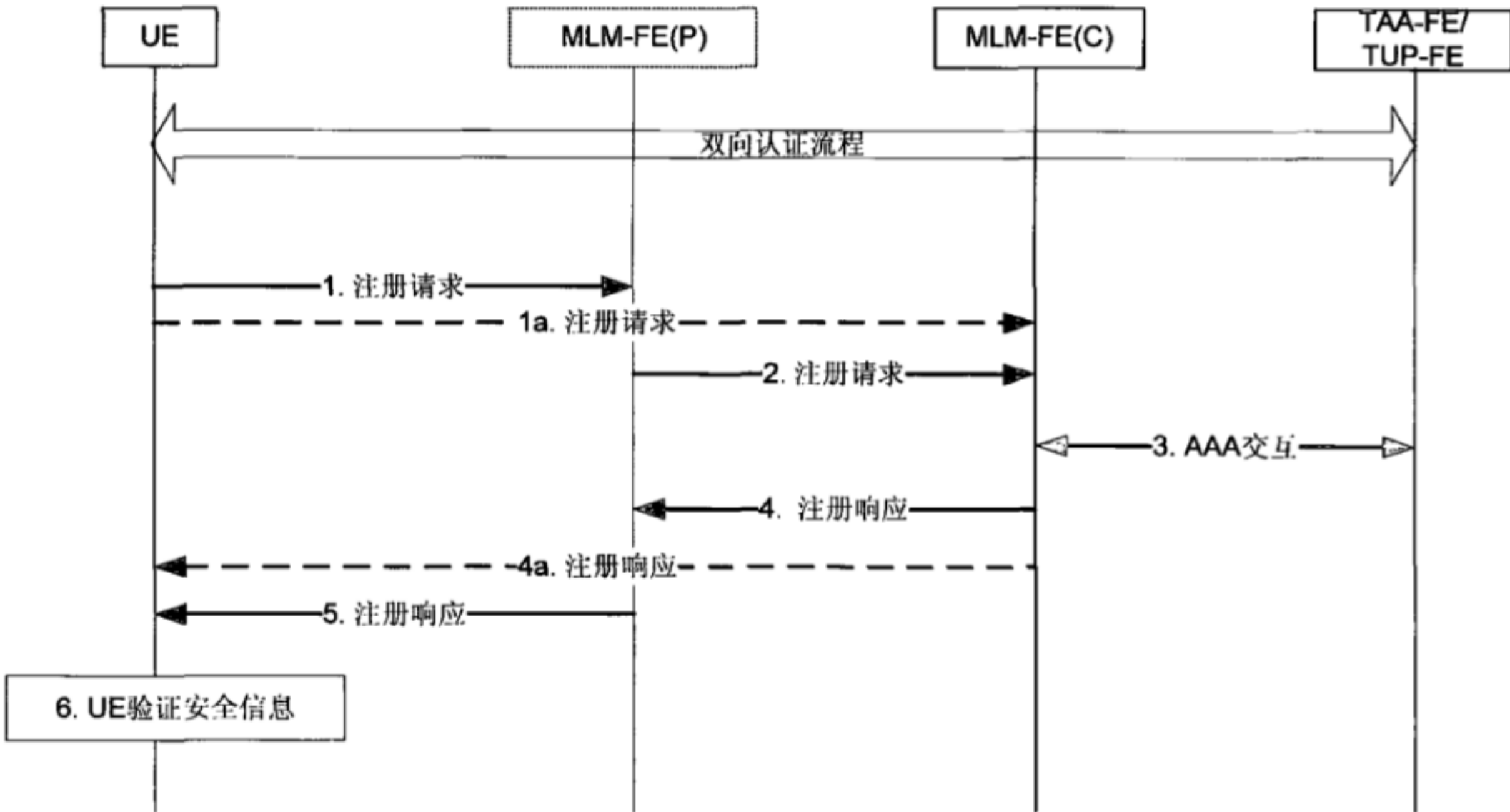


图 12 基于主机的移动性流程

- (1) UE发送注册请求至MLM-FE (P)。注册请求包括UE和MLM-FE (C) 间的安全信息，UE和MLM-FE (P) 间的安全信息。
- 1a. 若MLM-FE (P) 不存在，UE直接发送注册请求至MLM-FE (C) 。
- (2) MLM-FE (P) 验证UE和MLM-FE (P) 间的安全信息并转发注册请求至MLM-FE (C)。MLM-FE (P) 在转发前可能把MM-FE (P) 和MLM-FE (C) 间的安全信息添加到注册请求消息中。
- (3) MLM-FE (C) 与TAA-FE/TUP-FE交互获取认证与授权信息。

(4) MLM-FE (C) 验证注册请求中UE与MLM-FE (C) 间的安全信息。MLM-FE (C) 发送注册响应和安全信息至MLM-FE (P)。注册响应可以包括UE与MLM-FE (C) 间的安全信息, 以及MLM-FE (P) 与MLM-FE (C) 间的安全信息。

4a. 若MLM-FE (P) 不存在, MLM-FE (C) 直接发送注册响应至UE。注册响应可以包括UE和MLM-FE (C) 间的安全信息。

(5) MLM-FE (P) 验证MLM-FE (P) 与MLM-FE (C) 之间的安全信息并发送注册响应至UE。MLM-FE (P) 在转发前可能把UE和MLM-FE (P) 间的安全信息添加到注册响应消息中。

(6) UE验证UE与MLM-FE (C) 间的安全信息并创建UE与MLM-FE (C) 间的安全关联。若MLM-FE (P) 存在, UE验证UE与MLM-FE (P) 之间的安全信息并创建UE与MLM-FE (P) 间的安全关联。

9.2 网络移动性安全

在信任区或信任但脆弱的区域, 两个网络实体间基于网络的移动性控制流量的保护是可选的, 并与运营商的策略相关。基于网络的移动性控制流量的安全机制基于 ITU-T Y.2704 中的安全机制。

10 UE 和 HDC-FE 间的安全

UE 和 HDC-FE 间的信息流用于携带用于切换决策的信息。UE 和 HDC-FE 建立安全关联来保护二者之间的信息流。

10.1 主机发起的 UE 与 HDC-FE 间安全联盟的建立

主机发起的安全联盟建立过程指 UE 触发创建 UE 与 HDC-FE 间安全联盟的过程, 见图 13。该安全联盟的建立过程有两个先决条件。首先, UE 与 TAA-FE 有预共享密钥, 预共享密钥可以在互认证过程结束后获得。其次, UE 知道 HDC-FE 的信息, 如地址, UE 通过该地址发送安全关联请求至 HDC-FE。UE 如何获取 HDC-FE 信息超出本标准的范围。TLM 用于中继到达/来自 TAA-FE 的密钥材料信息, 图 13 中省略。

主机发起的安全关联建立执行如下步骤, 如图 13 所示。

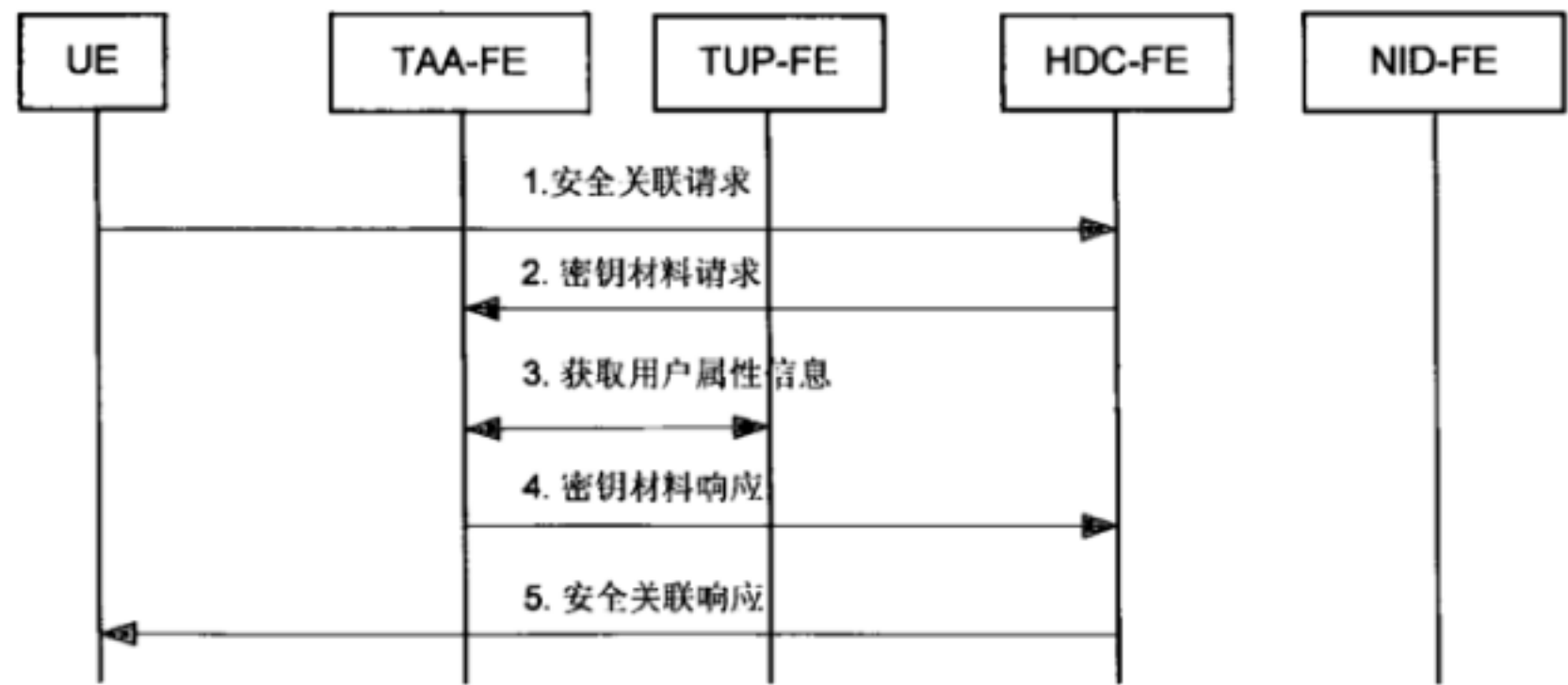


图 13 主机发起的安全关联建立流程

(1) 根据认证信息UE产生共享密钥材料来创建和HDC-FE的安全关联, UE发送安全关联请求至HDC-FE, 该请求中包括认证信息和UE信息。

(2) HDC-FE发送密钥请求至TAA-FE, 密钥请求包括HDC-FE信息、认证信息和UE信息。

(3) TAA-FE与TUP-FE交互获取用户属性信息, 并检查HDC-FE是否授权创建与UE的安全关联。

(4) 当HDC-FE授权创建与UE的安全关联时, 根据认证信息、HDC-FE信息和UE信息, TAA-FE为HDC-FE产生密钥材料。TAA-FE发送密钥材料响应至HDC-FE, 该信息包括HDC-FE的密钥材料、密钥生命周期。

(5) HDC-FE发送安全关联响应来通知UE和HDC-FE间的安全关联已建立。

## 10.2 网络发起的 UE 与 HDC-FE 间的安全关联建立

网络发起的安全关联过程指网络侧触发创建 UE 和 HDC-FE 间安全关联的过程, 见图 14。该安全联盟的建立过程有两个先决条件。首先, UE 与 TAA-FE 有预共享密钥, 预共享密钥可以在互认证过程结束后获得。其次, HDC-FE 知道 UE 信息如签约信息或位置信息, HDC-FE 通过该信息发送安全关联信息至 UE。HDC-FE 如何获得 UE 信息的方法超出本标准的范围。

网络发起的安全关联建立执行如下步骤, 如图 14 所示。

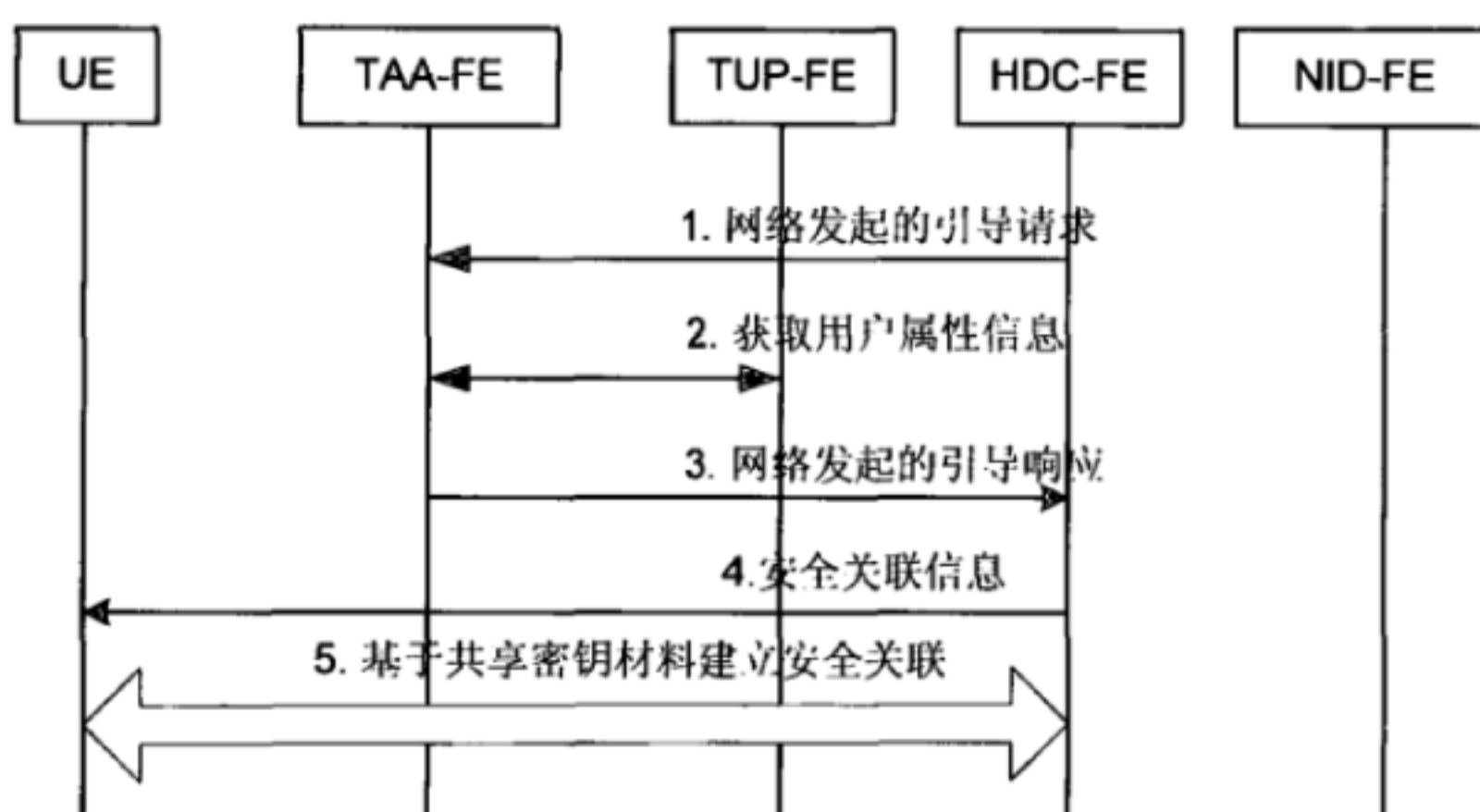


图 14 网络发起的安全关联建立流程

(1) HDC-FE发送网络发起的引导请求至TAA-FE, 该请求包括HDC-FE信息和UE信息。

(2) TAA-FE与TUP-FE交互获取用户属性信息, 并检查HDC-FE是否授权创建与UE的安全关联。

(3) 当HDC-FE授权创建与UE的安全关联是, 根据HDC-FE信息和UE信息, TAA-FE为HDC-FE产生密钥材料。TAA-FE发送网络发起的引导响应至HDC-FE, 该信息包括HDC-FE的密钥材料、密钥生命周期。

(4) HDC-FE发送安全关联信息至UE来创建安全关联。

(5) UE根据安全关联信息为HDC-FE创建密钥材料, 并验证安全关联信息。HDC-FE与UE建立安全关联。

## 11 传输功能层的安全

### 11.1 UE 与接入节点功能模块的安全

UE 与 AN-FE 之间的流量需要被保护。UE 与 AN-FE 间的安全关联基于共享密钥材料。当 UE 与 TAA-FE 间认证过程成功结束后, UE 与 TAA-FE 产生密钥材料如会话密钥来保护 UE 与 AN-FE 间的流量。TAA-FE 经 AM-FE、AR-FE 发送密钥材料至 AN-FE。

### 11.2 UE 与 L3HEF (层 3 切换执行功能)

UE 与 L3HEF 间的流量应该被保护。UE 与 L3HEF 间的安全关联基于预共享密钥材料。当 UE 与 TAA-FE 间认证过程成功结束后, UE 与 TAA-FE 产生密钥材料如会话密钥来保护 UE 与 L3HEF 间的流量。L3HEF 可以直接从 TAA-FE 获取密钥材料。L3HEF 也可以从 TAA-FE 经 AM-FE 或 HDC-FE 获取密

钥材料。

UE 与 L3HEF 间用户面流量安全执行如下步骤，如图 15 所示。

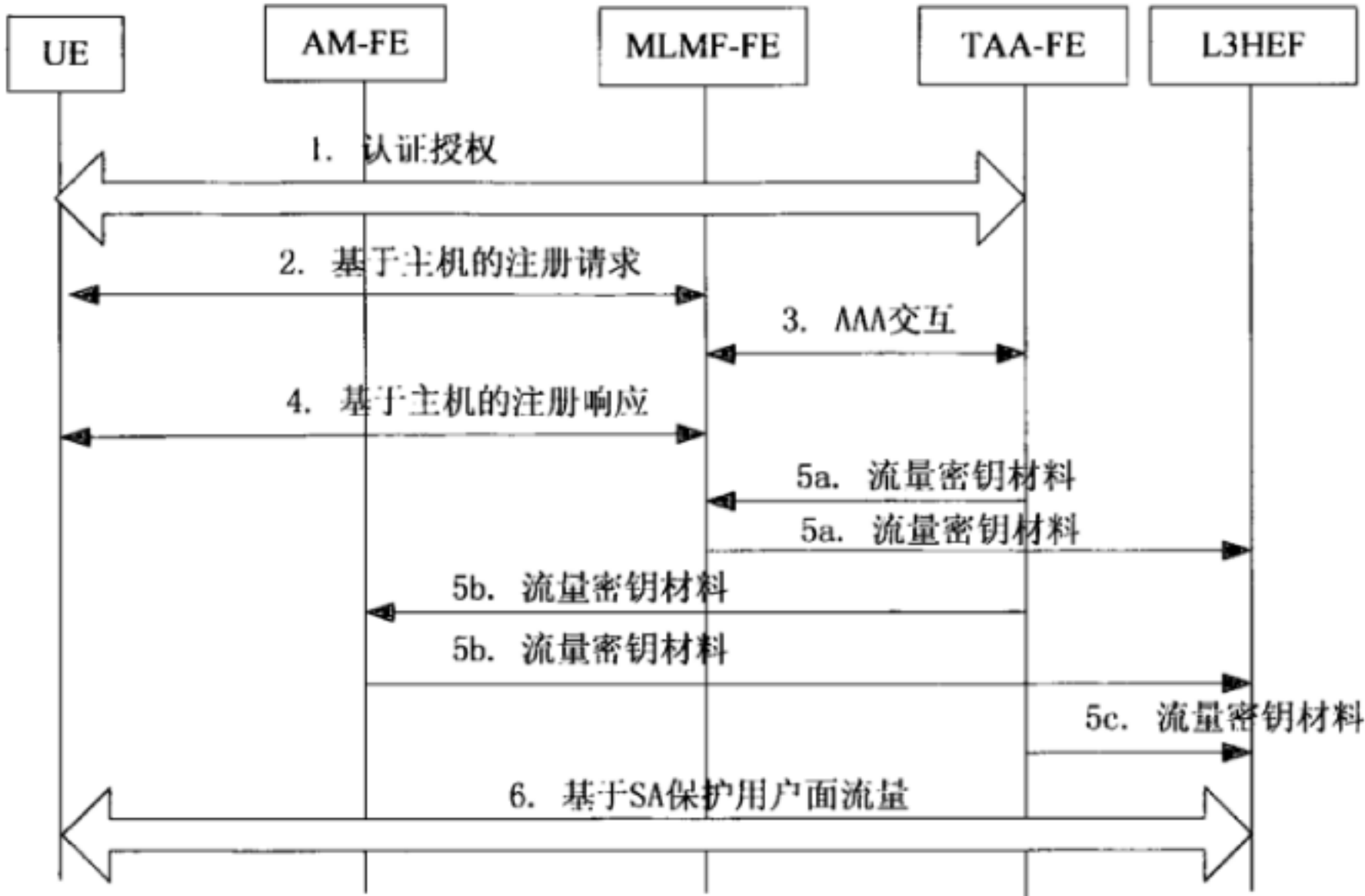


图 15 UE 与 L3HEF 间用户面流量安全

- (1) UE 与 TAA-FE 完成互认证后，UE 与 TAA-FE 均有共享密钥材料。
- (2) UE 发送基于主机的移动性注册请求至 MLMF-FE 以创建主机移动性安全关联。
- (3) MLMF-FE 与 TAA-FE 交互获取密钥材料。MLMF-FE 基于密钥材料认证 UE。当认证成功结束后，MLMF-FE 基于密钥材料与 UE 建立安全关联。
- (4) MLMF-FE 发送基于主机的移动性注册响应至 UE。UE 验证基于主机的移动性注册响应消息并与 MLMF-FE 创建安全关联。
- (5) 当 UE 与 MLMF-FE 间的安全关联创建后，出现三种情况：
  - 5a. TAA-FE 产生流量密钥材料并通过 MLMF-FE 把该密钥材料发送到 L3HEF。
  - 5b. TAA-FE 产生流量密钥材料并通过 MLMF-FE 经 AM-FE 把该密钥材料发送到 L3HEF。
  - 5c. TAA-FE 直接把密钥材料发送到 L3HEF。
- (6) L3HEF 使用流量密钥材料保护 UE 与 L3HEF 间的用户面流量。

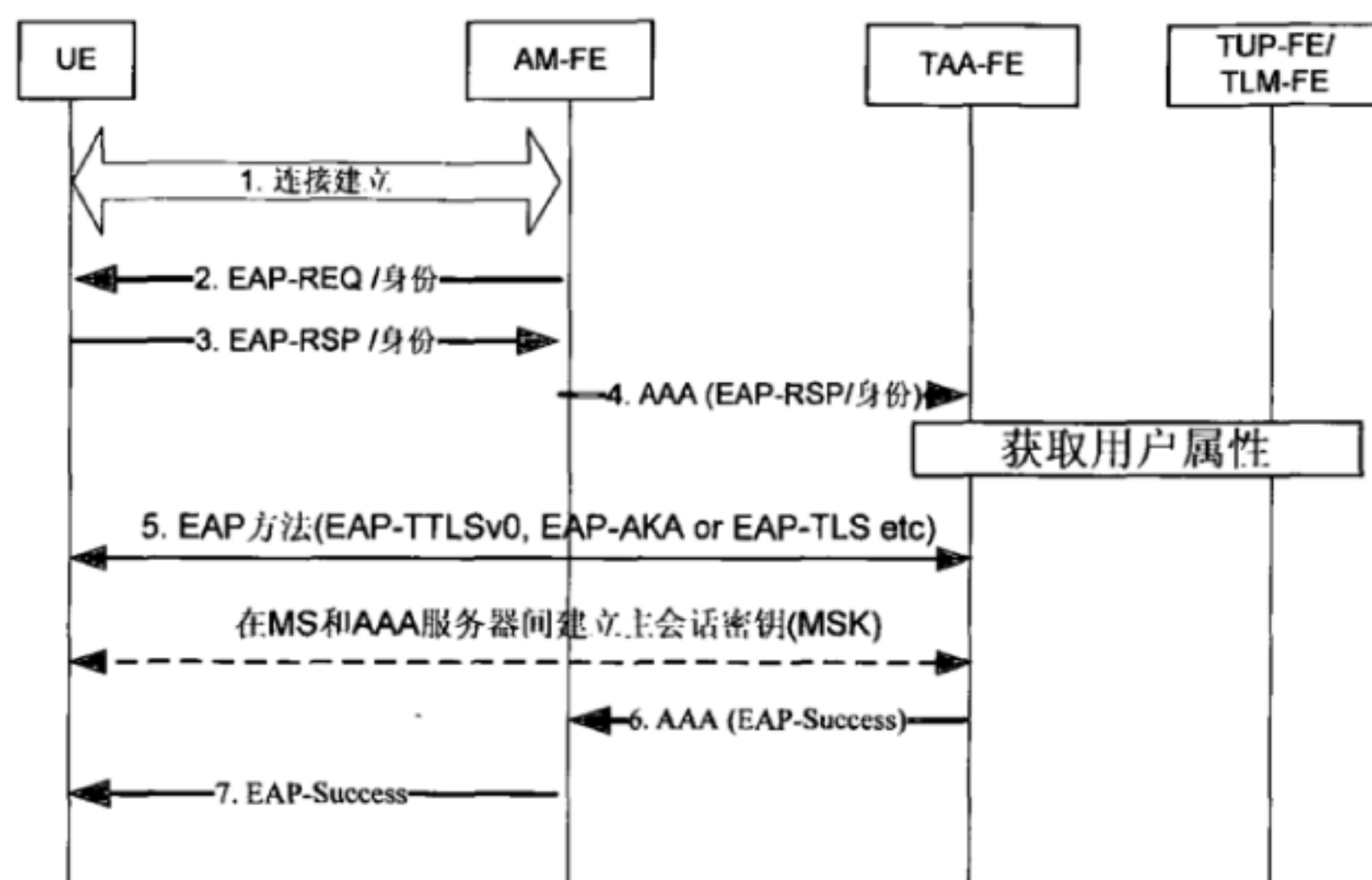
## 附录 A

### (资料性附录)

#### 若干实例

#### A.1 通用认证过程实例

认证过程如图 A.1 所示。



注：在步骤 2~4 中的身份指 UE 身份。

图 A. 1 通用认证过程

- (1) 在 UE 和 AM-FE 之间建立连接。
- (2) AM-FE 发送 EAP 请求 (EAP-REQ) /身份至 UE。
- (3) UE 发送 EAP 响应(EAP-RSP)/身份消息。
- (4) AM-FE 转发 EAP-RSP/身份至 TAA-FE，TAA-FE 和 TUP-FE/TLM-FE 交换信息后，TUP-FE/TLM-FE 发送用户信息至 TAA-FE。
- (5) 在 TAA-FE 和 UE 执行密钥推导和分发过程，可采用 EAP-TTLS，EAP-AKA，EAP-TLS 等。
- (6) TAA-FE 发送 EAP 成功消息至 AM-FE
- (7) AM-FE 向 UE 通知 EAP 成功消息。

现在成功完成了基于 EAP 的密钥交换过程，UE 和 AM-FE 共享交换中导出的密钥材料。

#### A.2 快速重认证过程实例

当切换发生时，快速重认证可以在低延迟情况下保持业务连续性。快速重新认证需要使用快速重新认证的标识，不需要在 TAA-FE 和 TUP-FE/TLM-FE 交换信息。

快速重认证过程如图 A.2 所示。

- (1) UE 和 AM - FE 之间建立连接。
- (2) AM - FE 发送 EAP-REQ/身份发送给 UE，携带重认证标识。
- (3) UE 发送 EAP-RSP/身份消息。
- (4) AM - FE 转发 EAP-RSP/身份至 TAA - FE。
- (5) 执行密钥推导和分发过程。有几种方法可以考虑，例如，EAP-TLS、EAP-AKA 等。

(6) TAA-FE 发送 EAP 成功信息至 AM-FE。

(7) AM-FE 向 UE 通知 EAP 成功消息。基于 EAP 密钥交换过程已经顺利完成，并在交换派生 UE 和 AM - FE 的共享密钥材料。

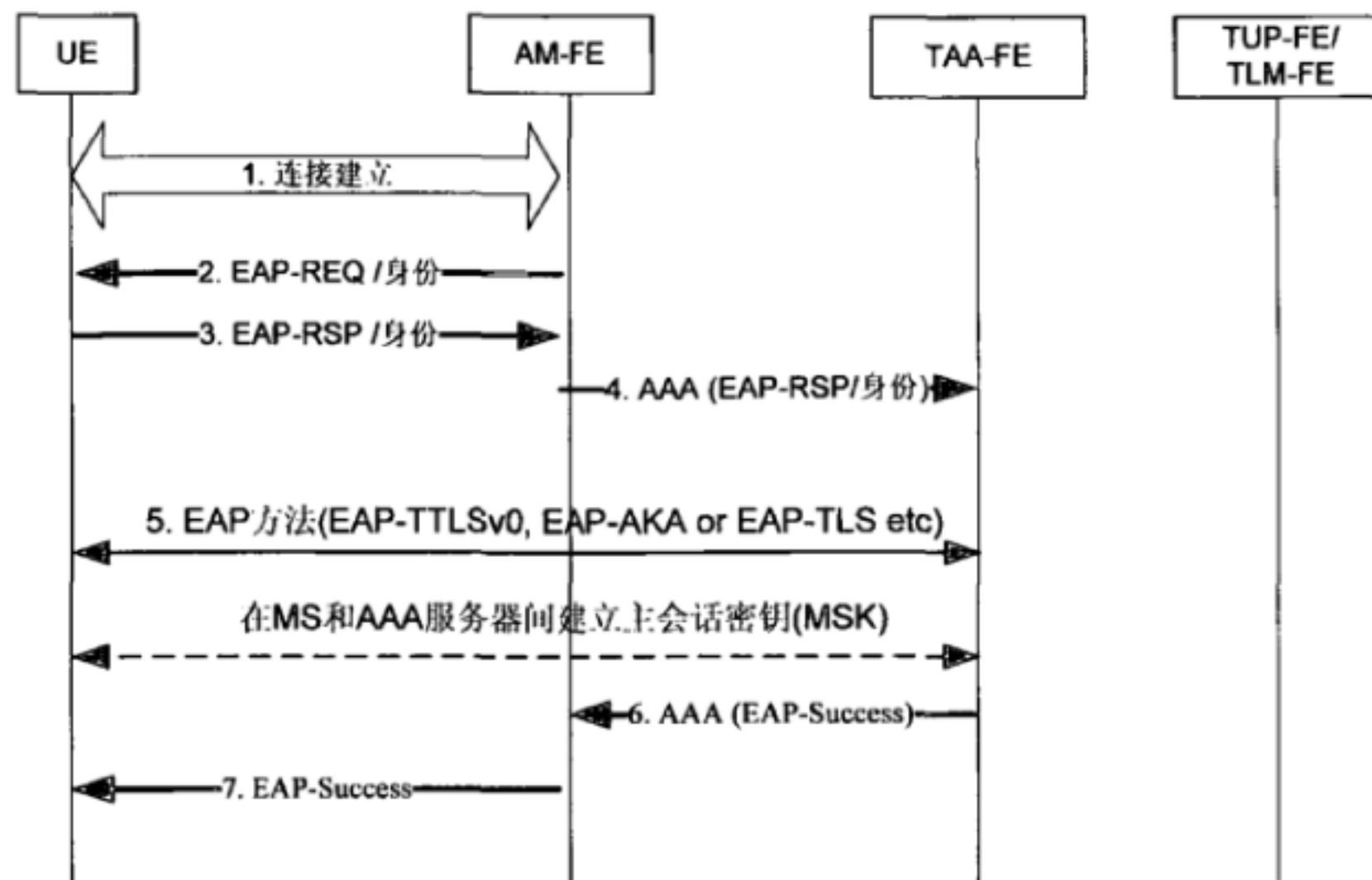


图 A. 2 快速重认证过程

### A.3 基于主机的移动性实例

对于 MIPv4, IP 移动性安全是基于 MIP 的认证扩展。在 UE 和 HA (如 MLM-FE) 节点间的 IP 移动性信令消息使用 MIP 认证扩展来保护, 可选的 UE 和 FA (如 MLM-FE) 的信令消息也需要保护。

MIPv4 认证过程如图 A.3 所示。

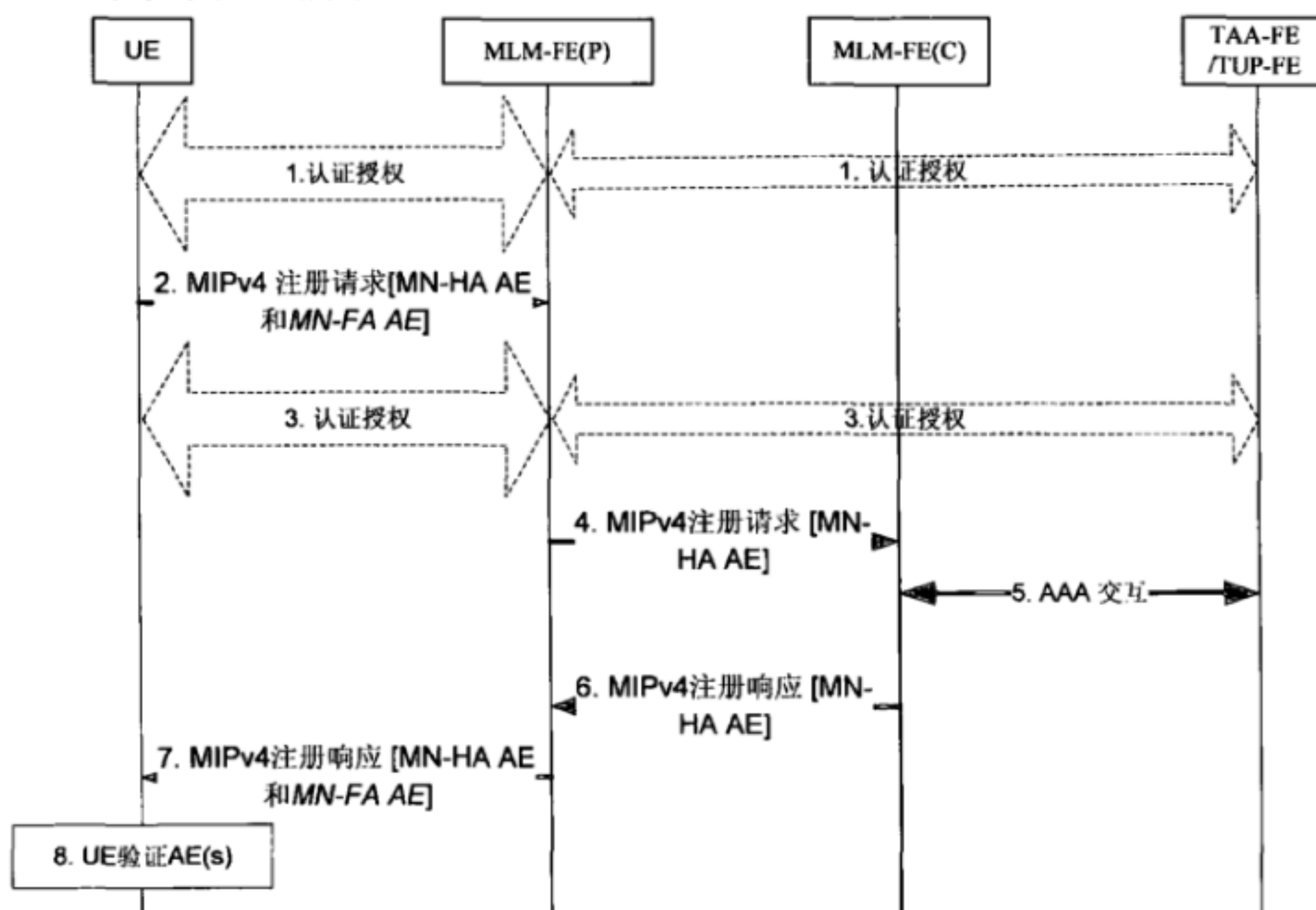


图 A. 3 MIPv4 认证过程

(1) 通过 TAA-FE/TUP-FE, 在 UE 和 MLM-FE 之间进行认证和授权。

(2) UE 发送一个注册请求 (RRQ) 消息至 FA (MLM-FE)。UE 包括 MN - HA 认证扩展 (AE) 和可选的 MN-FA 验证扩展 (AE)。

(3) RRQ 触发接入认证过程。

(4) FA 处理消息并验证 MN - FA 认证扩展。然后 FA 转发 RRQ 消息至 HA (MLM-FE)。

(5) 选定的 MLM - FE 从 TAA-FE / TUP- FE 获得认证和授权信息。

(6) MLM- FE 验证 MN-HA 认证扩展。当成功地验证认证扩展后, MLM- FE 通过 FA 向 UE 发送一个注册应答 (RRP)。

(7) FA 处理 RRP 消息, 然后 FA 转发 RRP 消息至 UE。若 FA 在 RRQ 消息中收到 MN-FA 认证扩展, 则 FA 包括 MN-FA 认证扩展。

(8) UE 验证 MN-HA 认证扩展和可选的 MN-FA 认证扩展。

## 参 考 文 献

- [1] IETF RFC 3344 IP, Mobility Support for IPv4.
  - [2] IETF RFC 3775, Mobility Support in IPv6.
  - [3] IETF RFC 5213, Proxy Mobile IPv6.
  - [4] IETF RFC 3748, Extensible Authentication Protocol (EAP).
  - [5] IETF RFC 4555, IKEv2 Mobility and Multihoming Protocol.
  - [6] 3GPP TS 33.102 V7.1.0, 3G Security: Security Architecture.
-

中华人民共和国  
通信行业标准  
下一代网络移动性安全框架  
YD/T 2911-2015

\*

人民邮电出版社出版发行  
北京市丰台区成寿寺路 11 号邮电出版大厦  
邮政编码：100164  
北京康利胶印厂  
版权所有 不得翻印

\*

开本：880×1230 1/16 2015 年 12 月第 1 版  
印张：1.75 2015 年 12 月北京第 1 次印刷  
字数：45 千字

15115·830

定价：20 元

本书如有印装质量问题，请与本社联系 电话：(010)81055492