国 际 电 信 联 盟

ITU-T

国际电信联盟
电信标准化部门

Y.2760

(05/2011)

Y系列：全球信息基础设施，互联网的协议问题和下一代网络

下一代网络 – 安全

下一代网络的移动安全框架

ITU-T Y.2760 建议书

国际电信联盟

ITU-T Y系列建议书

全球信息基础设施、互联网的协议问题和下一代网络

全球信息基础设施	
概要	Y.100–Y.199
业务、应用和中间件	Y.200–Y.299
网络方面	Y.300–Y.399
接口和协议	Y.400–Y.499
编号、寻址和命名	Y.500–Y.599
运营、管理和维护	Y.600–Y.699
安全	Y.700–Y.799
性能	Y.800–Y.899
互联网的协议问题	
概要	Y.1000–Y.1099
业务和应用	Y.1100–Y.1199
体系、接入、网络能力和资源管理	Y.1200-Y.1299
传输	Y.1300–Y.1399
互通	Y.1400–Y.1499
服务质量和网络性能	Y.1500–Y.1599
信令	Y.1600–Y.1699
运营、管理和维护	Y.1700–Y.1799
计费	Y.1800–Y.1899
运行于NGN的IPTV	Y.1900–Y.1999
下一代网络	
框架和功能体系模型	Y.2000–Y.2099
服务质量和性能	Y.2100–Y.2199
业务方面：业务能力和业务体系	Y.2200–Y.2249
业务方面：NGN中业务和网络的互操作性	Y.2250–Y.2299
编号、命名和寻址	Y.2300–Y.2399
网络管理	Y.2400–Y.2499
网络控制体系和协议	Y.2500–Y.2599
智能泛在网络	Y.2600–Y.2699
安全	**Y.2700–Y.2799**
通用移动性	Y.2800–Y.2899
电信级开放环境	Y.2900–Y.2999
未来网络	Y.3000–Y.3099

如果需要进一步了解细目，请查阅ITU-T建议书清单。

ITU-T Y.2760 建议书

下一代网络（NGN）的移动安全框架

摘要

ITU-T Y.2760建议书规定下一代网络（NGN）传输层的移动安全框架，具体规定NGN移动管理与控制的安全要求、安全机制和程序。

历史沿革

版本	建议书	批准日期	研究组	
1.0	ITU-T Y.2760	2011-05-20	13	

关键词

移动安全、下一代网络（NGN）。

前言

国际电信联盟（国际电联）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电联的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会(WTSA)确定 ITU-T 各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA 第 1 号决议规定了批准建议书须遵循的程序。

属 ITU-T 研究范围的某些信息技术领域的必要标准，是与国际标准化组织(ISO)和国际电工委员会(IEC)合作制定的。

注

本建议书为简要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款(以确保例如互操作性或适用性等)，只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其他一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其他机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能不是最新信息，因此大力提倡他们通过下列网址查询电信标准化局(TSB)的专利数据库： http://www.itu.int/ITU-T/ipr/.

目录

页码

ITU-T Y.2760 建议书

下一代网络的移动安全框架

1 范围

本建议书描述下一代网络（NGN）传输层的移动安全框架。本建议书考虑了[ITU-T Y. 2018]中的安全要求，并包括认证和密钥管理；安全环境建立；IP移动安全；传输层的移动管理、控制和传送安全。本建议书研究探讨的情形包括技术内和技术间移动性以及域内和域间移动性。

2 参考文献

下列ITU-T建议书和其它参考文献的条款，在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有建议书和其它参考文献均会得到修订，本建议书的使用者应查证是否有可能使用下列建议书或其它参考文献的最新版本。当前有效的ITU-T建议书清单定期出版。本建议书引用的文件自成一体时不具备建议书的地位。

[ITU-T Q.1706] ITU-T Q.1706 /Y.2801建议书（2006年），下一代网络的移动性管理要求。

[ITU-T X.805] ITU-T X.805建议书(2003)，提供端到端通信系统的安全架构。

[ITU-T Y.2011] ITU-T Y. 2011建议书(2004)，下一代网络的一般原则和通用参考模型。

[ITU-T Y.2012] ITU-T Y.2012建议书(2010)，下一代网络的功能要求和架构。

[ITU-T Y.2014] ITU-T Y.2014建议书(2010)，下一代网络的网络连接控制功能。

[ITU-T Y.2018] ITU-T Y.2018建议书(2009)，NGN中的移动管理和控制功能。

[ITU-T Y.2701] ITU-T Y.2701建议书（2007年），第1版下一代网络（NGN）的安全性要求。

[ITU-T Y.2704] ITU-T Y.2704建议书（2010年），下一代网络（NGN）的安全机制和程序。

[ITU-T Y.2000 增补7] ITU-T Y.2000系列建议书（2008），对第2版NGN范围的增补

[ITU-R M.1645] ITU-R M.1645建议书 （2003），IMT-2000未来发展及超IMT-2000系统的框架和总体目标。

3 定义

3.1 其它文件定义的术语

本建议书使用其它文件定义的下列术语：

3.1.1 **切换** [6.2.2/ITU-T Q.1706]：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。

3.1.2 **水平移动性**[6.2.3/ITU-T Q.1706]：在［ITU-R M.1645］中所定义的相同层次上的移动性。它一般被称为在相同接入技术内的移动性。

3.1.3 **移动性**[3.2/ITU-T Q.1706]：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。

3.1.4 **NGN传输层**[3.10/ ITU-T Y.2011]：NGN中负责提供传送数据和功能 – 这些功能旨在控制和管理终接实体间进行此类数据传送的传输资源 – 的用户功能部分。

3.1.5 **信任**[3.2.9/ITU-T Y.2701]：当且仅当实体X依赖实体Y以某种特殊方式来执行相关的活动时，才被认为在一系列活动方面信任实体Y。

3.1.6 **垂直移动性**[6.2.3/ITU-T Q.1706]：在［ITU-R M.1645］中所定义的不同层之间的移动性。它一般被称为不同接入技术之间的移动性。

3.2 本建议书定义的术语

本建议书定义了以下术语：

3.2.1 **技术间移动性**：见垂直移动性，见第3.1节。

3.2.2 **技术内移动性**：见水平移动性，见第3.1节。

3.2.3 **安全环境**：包括识别符、密钥材料和密钥算法等在内的一套安全参数。

4 缩写词和首字母缩略语

本建议书使用以下缩写词和首字母缩略语：

3G 第3代
ABG-FE 接入边界网关功能实体
AE 认证扩展
AKA 认证和密钥协议
AM-FE 接入管理功能实体
AN-FE 接入节点功能实体
ANI 网络接口应用
AR-FE 接入中继功能实体
DDoS 分布式拒绝服务
EAP 可扩展认证协议
EN-FE 边缘节点功能实体
FA 外来代理

HA 归属代理
HDC-FE 切换决定和控制功能实体
IP 互联网协议
L3HEF 第3层切换执行功能
MIP 移动IP
MIPv4 IPv4的移动IP。见[b-IETF RFC 3220]
MIPv6 IPv6的移动IP。见[b-IETF RFC 3775]
MLM-FE 移动定位管理功能
MMCF 移动管理控制功能
MN 移动节点
MOBIKE IKEv2移动和多归属协议。见[b-IETF RFC 4555]
NACF 网络附着控制功能
NGN 下一代网络
NID-FE 网络信息分布功能实体
NNI 网络至网络接口
PKI 公共密钥基础设施
PMIPv6 代理移动IPv6。见[b-IETF RFC 5213]
RAN 无线电接入网络
RRP 注册回复
RRQ 注册请求
TAA-FE 传送认证和授权功能实体
TLM-FE 传送定位管理功能
TLS 传输层安全
TTLS 隧道式传输层安全
TUP-FE 传送用户资料功能实体
UE 用户设备
UNI 用户到网络接口
WiMax 微波接入全球互操作性
WLAN 无线局域网（LAN）

5 下一代网络的移动安全要求

下一代网络（NGN）支持多种接入技术，包括WLAN、WiMax和3G RAN等[ITU-T Y.2012]。支持移动性是NGN的功能特性之一，其中包括游牧性和切换。在第2版本NGN中，切换涵盖接入网络之间和接入网络内情形[ITU-T Y. Sup. 7]。

NGN支持下列功能特性：

1) 信任模型：NGN安全信任模型确定了三个安全区：受信任区、受信任但较脆弱区和不受信任区[ITU-T Y.2701]。这一模型表明，接入网在接入核心网之前必须通过安全网关。

2) NGN支持多种接入技术。

3) NGN支持若干移动性协议，如MIPv4、MIPv6、DSMIPv6、PMIPv6和MOBIKE。

4) NGN支持多种无线电用户设备（UE），如WLAN、WiMax、3G RAN等。

5) 在异质接入系统之间进行切换时NGN支持业务连续性。

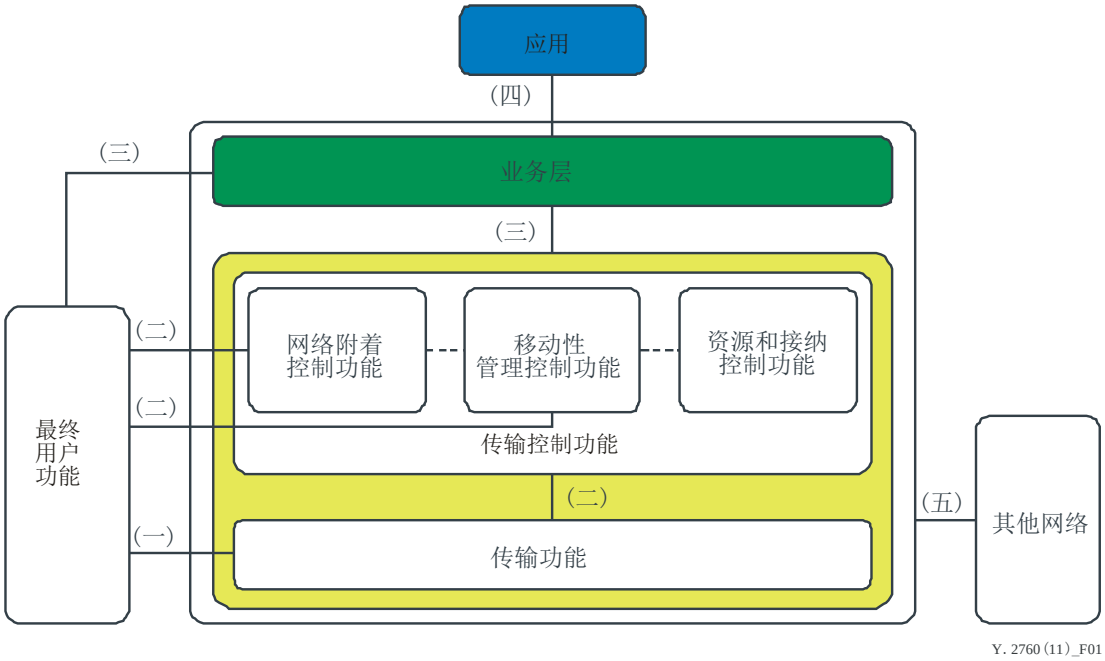


图1 – NGN的移动安全架构

本建议书定义五类安全功能特性：

（一） 重点为最终用户功能和传输功能之间传输层的安全，如传送功能中最终用户功能与接入网络实体之间可能得到实际或物理保护的接入安全。（一）亦涉及到最终用户功能与传输功能之间的UNI安全。

（二） 重点关注最终用户功能与传输控制功能实体之间控制层的安全。（二）亦专注于传输功能实体与传输控制功能实体之间控制信息接口的安全。（二）涉及最终用户功能与传输控制功能之间的UNI安全。

（三） 重点关注最终用户功能与业务层之间的接口安全。（三）的另一个重点是传输控制功能实体与业务层之间控制信息接口的安全。（三）涉及最终用户功能与业务层之间的UNI安全。

（四） 重点为业务层与应用实体之间的接口安全。（四）涉及最终用户功能与传输功能之间的ANI安全。

（五） 重点关注NGN与其他网络之间的接口安全，其中既包括传输层也包括控制层。（五）涉及NGN网络与其他网络之间的NNI安全。

[ITU-T X.805]确定的原则适用于本建议书明确的各种安全威胁和安全要求。

5.1 安全威胁

[ITU-T Y. 2018]明确了下列安全威胁。

T1 UE可在未经授权情况下启动与MLM-FE的移动信令。

T2 入侵者可能破坏移动信令。

T3 MLM-FE可能被假冒，从而向UE提供虚假信息。

T4 UE定位可能被入侵者偷听。

T5 可能发生改变流量方向的攻击。

T6 攻击者可利用中间人攻击方式将自己加入到路径上。

T7 DdoS攻击可能消耗大量的网络资源。

T8 UE可在未经授权情况下从HDC-FE或NID-FE处得到信息。

T9 HDC-FE或NID-FE可能被假冒，从而向UE推出虚假信息。

T10 UE与DC-FE或NID-FE之间的信令可能被修改或偷听。

T11 用户面数据可能被偷听或修改。

5.2 安全要求

[ITU-T Y. 2018]确定了下列安全要求。

R1 要求UE与NID-FE进行相互认证。

R2 要求UE与MLM-FE之间的信令得到完整性和保密性保护。

R3 要求UE与MLM-FE之间的信令免受中继攻击的影响。

R4 要求提供UE的定位隐私。

R5 要求UE和HDC-FE之间进行相互认证。

R6 要求UE与HDC-FE之间的信令得到完整性和保密性保护。

R7 要求UE和HDC-FE之间的信令免受中继攻击影响。

R8 要求提供低时延认证和信令保护。

R9 要求优化安全环境转让。

R10 要求移动安全解决方案独立于媒介。

R11 当用户资料给出指示时，要求提供保护UE与EN-FE之间用户面流量的机制。

除[ITU-T Y. 2018]确定的上述安全要求外，还涉及到了下列安全要求。

R12 – 要求支持多连接安全。

6 相关功能实体支持的安全能力

NGN网络中与移动安全有关的功能实体如下：

- 传输用户资料功能实体（TUP-FE）
- 传输认证和授权功能实体（TAA-FE）
- 移动定位管理功能实体（MLM-FE）
- 切换决定控制功能实体（HDC-FE）

- 网络信息分布功能实体（NID-FE）
- 接入管理功能实体（AM-FE）
- 第3层切换执行功能（L3HEF）
- 接入节点功能实体（AN-FE）

6.1 传输用户资料功能实体（TUP-FE）

TUP-FE存储订购用户认证数据，如密钥材料、认证方法和用户传输资料。有关TUP-FE的详细功能描述请见[ITU-T Y. 2014]。

6.2 传输认证和授权功能实体（TAA-FE）

TAA-FE从TUP-FE处检索认证数据和接入授权信息，TAA-FE还作为代理行事。

其详细功能描述请见[ITU-T Y. 2014]。

6.3 移动定位管理功能实体（MLM-FE）

MLM-FE从NACF处获得认证、授权和结算信息，与UE进行相互认证，并建立UE与MLM-FE之间的安全关联性。其详细功能描述请见[ITU-T Y. 2018]。

6.4 切换决定控制功能实体（HDC-FE）

要求HDC-FE建立与UE的安全关联性，并通过TLM-FE从TAA-FE处获得用于安全关联性的安全密钥。其详细功能描述请见[ITU-T Y. 2018]。

6.5 网络信息分布功能实体（NID-FE）

要求NID-FE建立与UE之间的安全关联性，以保护诸如网络选择等信息。NID-FE可通过TLM-FE从TAA-FE处获得安全信息。其详细功能描述请见[ITU-T Y. 2018]。

6.6 接入管理控制功能实体（AM-FE）

AM-FE向TAA-FE前转网络接入请求，以对用户进行认证和授权，或拒绝其接入网络，同时检索用户的具体接入配置参数。AM-FE可无需重复完整的网络注册/认证/配置程序而重复使用网络注册/认证数据，以实现快速恢复。其详细功能描述请见[ITU-T Y. 2014]。

6.7 第3层切换执行功能（L3HEF）

要求L3HEF建立与UE之间的安全关联性，以保护二者之间的流量。其详细功能描述请见[ITU-T Y. 2018]。

注 — L3HEF的安全研究解决UE与EN-FE之间用户面流量保护的安全要求。

6.8 接入节点功能实体（AN-FE）

要求AN-FE建立与UE之间的安全关联性，同时它通过AM-FE从TAA-FE获得密钥材料。其详细功能描述请见[ITU-T Y. 2018]。

7 密钥管理和认证

7.1 密钥管理框架

NGN移动安全使用分层的密钥衍生机制，NGN中存在若干种不同密钥材料，如根密钥和会话密钥等。根密钥是一种得到安全存储的长期证书（如共用秘密密钥或密码）。会话密钥是一种在根密钥基础上生成的短期密钥材料。NGN的UE和认证实体（如TAA-FE/TUP-FE）均存储共享根密钥。

通常而言，会话密钥材料在根密钥和其它密钥生成参数基础上产生（如认证程序过程中的谈判信息）。会话密钥材料用于保护信令流量和用户流量，会话密钥可得到进一步衍生，该密钥衍生机制取决于具体的加密算法或协议。

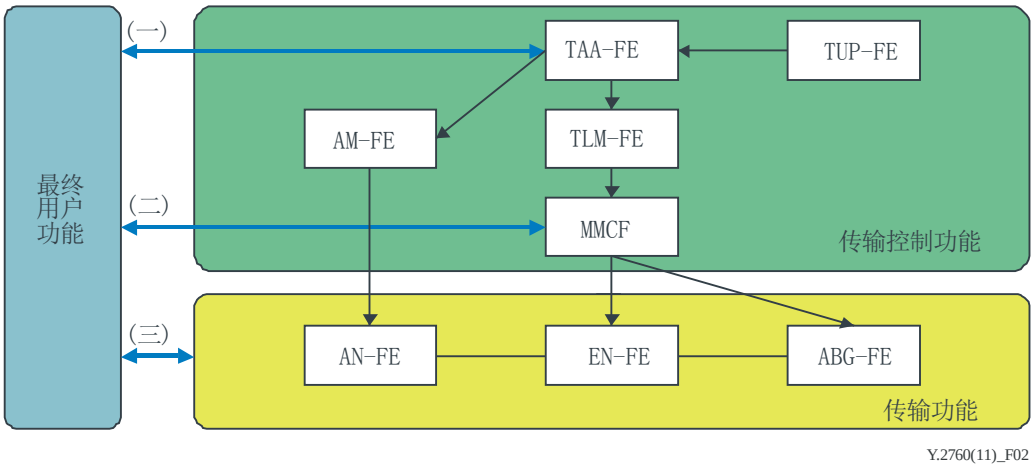


图2 - NGN移动安全的一般性密钥生成框架

以下阐述NGN移动安全的一般性密钥生成（keying）框架。

（一） UE与NGN的功能实体之间进行相互认证，在认证过程中，TUP-FE根据根密钥材料生成认证矢量，并将这些认证矢量发至TAA-FE。成功完成相互认证程序之后，TAA-FE和UE均生成会话密钥材料，会话密钥材料可用于生成子会话密钥材料。会话密钥材料被传至AM-FE和MMCF等功能实体。AM-FE和MMCF均可根据收到的会话密钥材料生成子会话密钥材料。

（二） UE与MMCF之间参考点的安全关联性以通过TLM-FE处获得的会话密钥材料为基础，（二）使用的会话密钥材料根据TAA-FE中的会话密钥材料生成或衍生。

（三） UE与传输功能层之间的安全关联性根据共享密钥材料（通过TAA-FE、AM-FE或MMCF中此前的会话密钥材料生成）建立。AN-FE通过AM-FE从TAA-FE处接收会话密钥材料。如果AM-FE具有衍生会话密钥材料的能力，则AN-FE可直接从AM-FE处获得会话密钥材料。EN-FE和ABG-FE均通过TLM-FE和MMCF接收由TAA-FE生成的密钥材料。如果MMCF具有生成会话密钥材料的能力，则EN-FE和ABG-FE可从MMCF处获得密钥材料。

认证程序以质疑 – 答复协议（如AKA [b-3GPP TS 33.102]）为基础。

7.2 认证

7.2.1 一般性认证程序

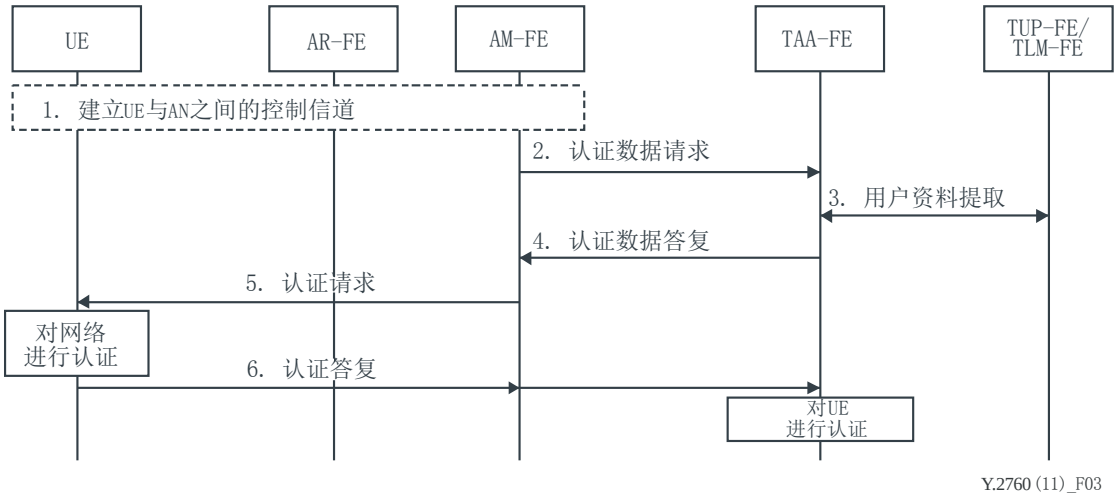


图 3 – 一般性认证程序

1) 建立UE与接入网功能之间的控制信道（该程序不属于本建议书的范围）。

2) AM-FE将UE信息发至TAA-FE，请求得到认证数据。

3) TAA-FE从认证请求中获得认证信息（其中包括用户和签约用户身份（ID）和接入网信息），与TUP-FE/TLM-FE互动，从而获得用户资料和认证矢量，包括认证令牌和会话密钥材料。

4) TAA-FE向AM-FE发送认证数据答复，其中包括认证令牌。

5) AM-FE将认证请求发至UE，UE从认证请求中提取认证令牌，生成本地认证矢量，其中包括以认证令牌和根密钥为基础的会话密钥材料。UE通过证实所收到的认证令牌对网络进行认证。

6) UE向AM-FE发送认证答复，其中包括由UE生成的认证令牌。AM-FE将信息前转至TAA-FE，TAA-FE提取认证令牌，检查所收到的认证令牌的有效性，从而对UE进行认证。

7.2.2. 一般性快速再认证程序

一般性快速再认证程序旨在减少切换时延。TUP-FE/TLM-FE不参与快速再认证程序，从而加快了认证程序，并减轻了TUP-FE/TLM-FE的负载。建议NGN的UE和认证实体均支持一般性快速再认证程序。

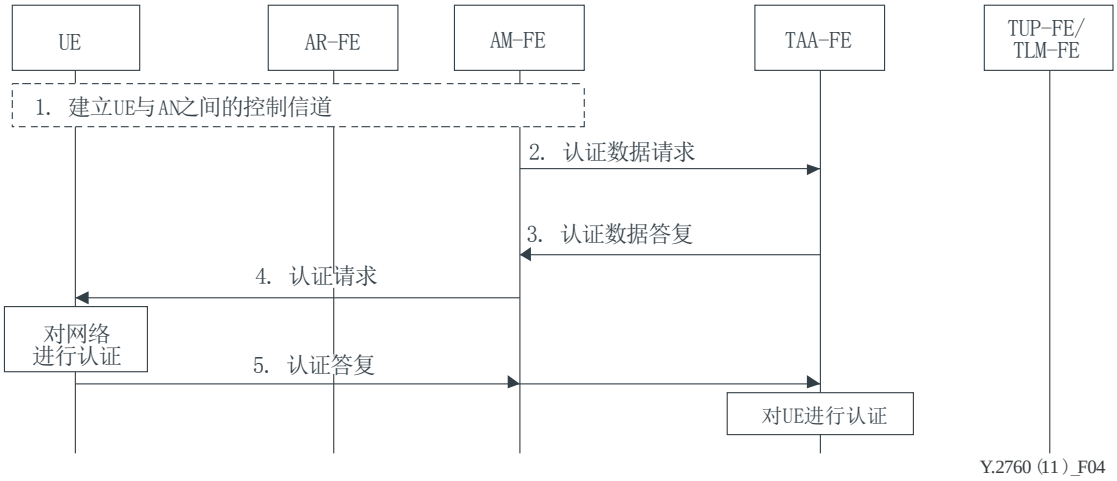


图 4 – 一般性快速再认证程序

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。

1) 建立UE与接入网功能之间的控制信道（该程序不属于本建议书的范围）。

2) AM-FE将UE信息发至TAA-FE，请求得到认证数据。

3) TAA-FE向AM-FE发送认证数据答复，其中包括认证令牌。

4) AM-FE将认证请求发至UE，UE从认证请求中提取认证令牌，生成本地认证矢量，其中包括以认证令牌和根密钥为基础的会话密钥材料。UE通过证实所收到的认证令牌对网络进行认证。

5) UE向AM-FE发送认证答复，其中包括由UE生成的认证令牌。AM-FE将信息前转至TAA-FE，TAA-FE提取认证令牌，检查所收到的认证令牌的有效性，从而对UE进行认证。

当UE重复使用会话密钥材料时，快速再认证信息仅用于相互认证。如果UE不重复使用会话密钥，则UE和认证实体（TAA-FE /TUP-FE）均在会话密钥材料和快速再认证信息基础上生成新的会话密钥。

7.2.2.1 优化快速再认证程序

为使快速再认证程序得到优化，由NGN网络首先对UE进行认证，UE生成认证信息。该程序与普通程序中的一般性再认证不同，在普通程序中， UE首先对NGN网络进行认证，NGN网络生成认证令牌。

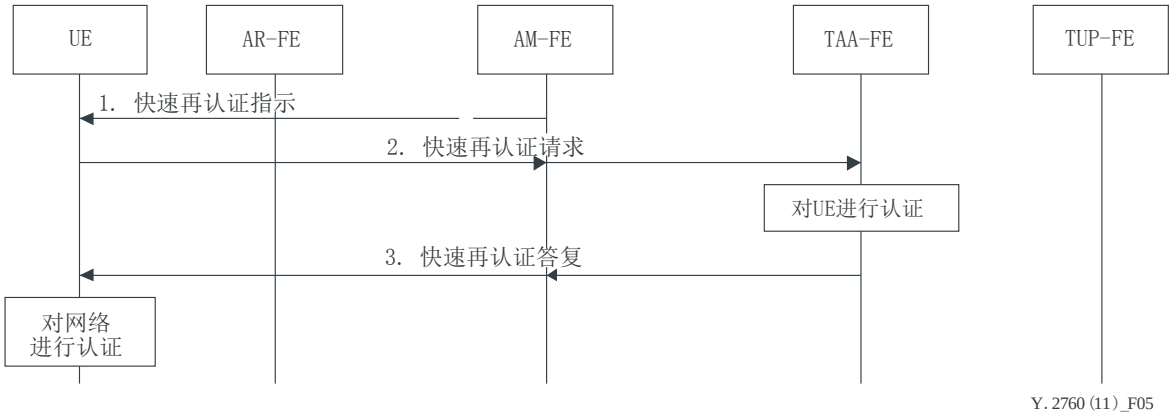


图 5 – 经优化的快速再认证程序

1) 建立UE与接入网络功能之间的控制信道（该程序不属于本建议书的范围）。AM-FE向UE发送优化再认证指示，其中表明TAA-FE支持经优化的快速再认证。

2) UE生成认证矢量并通过AM-FE向TAA-FE发送优化再认证的请求，优化再认证请求包含认证令牌和再认证信息。TAA-FE根据再认证信息和会话密钥材料生成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对UE进行认证。

3) TAA-FE通过AM-FE向UE发送包括认证令牌在内的再认证答复。UE通过自身的认证矢量对网络进行认证，认证成功完成之后，UE可生成子会话密钥材料。

7.2.3 域内认证

7.2.3.1 单一网络连接中的认证

单一网络连接意味着UE可检测到不同网络，但一次仅接入一个网络。预认证意味着UE在切换到目标网络之前通过主服务（serving）网络与目标网络进行相互认证。如UE是单一网络连接基础上的UE，则UE通过使用预认证保持业务连续性和低时延。预认证程序与一般性认证程序类似。必要时预认证程序可有主服务AM-FE、主服务AM-FE、目标AM-FE和目标AM-FE的参与。

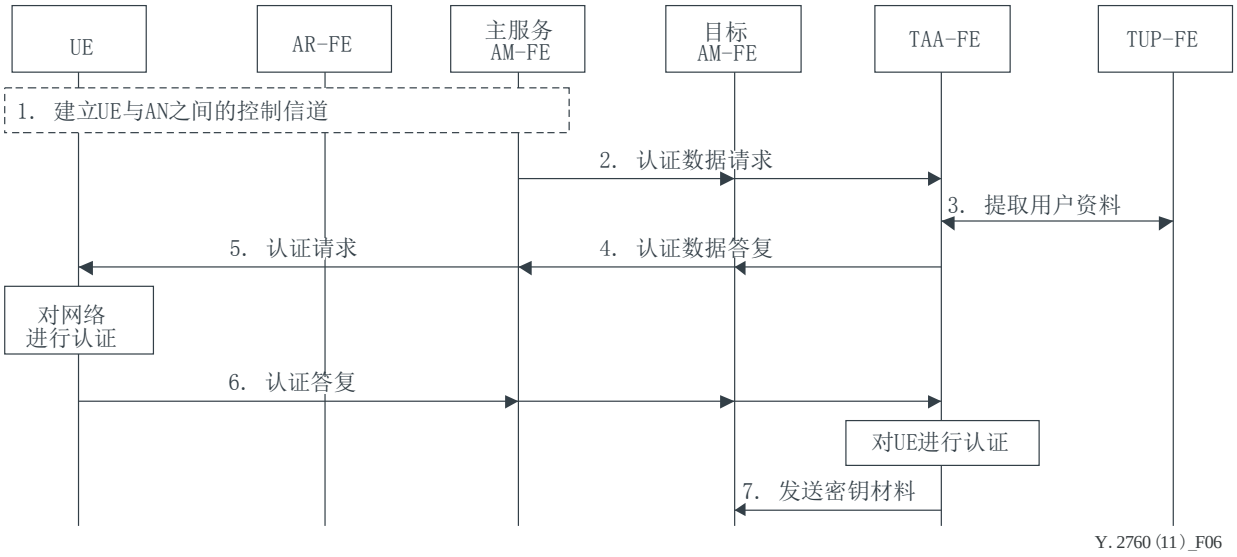


图 6 – 基于预认证程序的单一网络连接

1) 建立UE与接入网功能之间的控制信道（该程序不属于本建议书的范围）。

2) AM-FE向TAA-FE发出认证数据请求，其中包括签约用户信息。认证数据请求由主服务AM-FE向目标AM-FE前转。

3) TAA-FE通过与TUP-FE互动提取用户资料。

4) TAA-FE向目标AM-FE和主服务AM-FE发送认证数据答复，其中包括认证令牌。

5) 主服务AM-FE向UE发送认证请求，UE提取认证令牌，并通过其自身认证信息对网络进行认证。认证成功完成之后，UE生成会话密钥材料。

6) UE向主服务AM-FE发送认证答复，主服务AM-FE向目标AM-FE和TAA-FE前转信息（其中包括认证令牌）。TAA-FE检索认证令牌并对UE进行认证。成功完成认证之后，TAA-FE生成会话密钥材料，必要时可通过该材料衍生子会话材料。

7) TAA-FE向目标AM-FE发送密钥材料，该材料将在UE执行向目标网络的切换后得到使用，以保护UE与目标网络之间的通信。

7.2.4 域间认证

不同的管理域意味着不同的NGN提供商的存在。以下阐述不同管理域之间UE切换的认证程序。

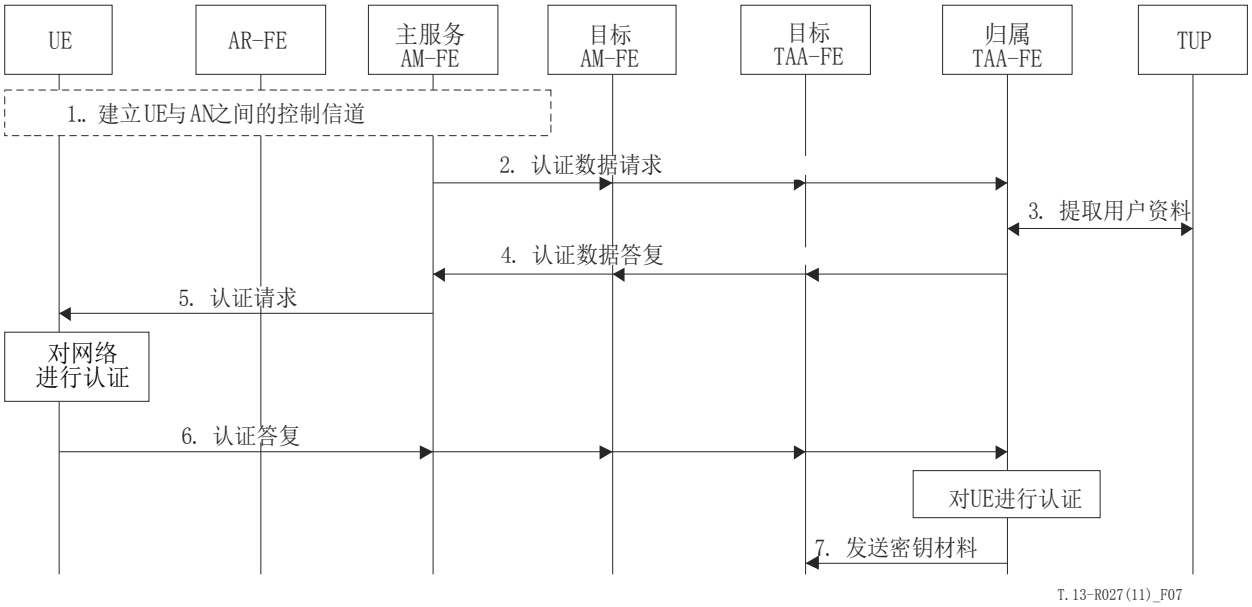


图 7 – 不同域之间的认证程序

1) 建立UE与接入网络功能之间的控制信道（该程序不属于本建议书的范围）。

2) 主服务AM-FE向归属TAA-FE发送认证数据请求，包括签约用户信息。认证数据请求由目标AM-FE和目标TAA-FE前转。归属TAA-FE通过与TUP-FE互动提取用户资料。

3) TAA-FE通过与TUP-FE互动提取用户资料。

4) 归属TAA-FE向主服务AM-FE发送认证数据答复，其中包括认证令牌。认证数据响应由目标TAA-FE和目标AM-FE前转。

5) 主服务AM-FE向UE发送认证请求，UE提取认证令牌，并通过自身的认证信息对网络进行认证。认证成功完成之后，UE生成会话密钥材料。

6) UE向归属TAA-FE发送认证答复，其中包括认证令牌。归属TAA-FE检索认证令牌，并对UE进行认证。认证成功完成之后，归属TAA-FE生成会话密钥材料，必要时该密钥材料可用于衍生子会话密钥材料。

7) 成功完成认证之后，归属TAA-FE向目标TAA-FE发送密钥材料，该材料在UE由主服务网络向目标网络切换之后加以使用，以保护UE与目标网络之间的通信。

7.2.5 认证中密钥材料的映射机制

当UE从主服务网络移动到目标网络时，需进行相互认证，并生成会话密钥材料。NGN支持不同的密钥衍生机制，并利用密钥材料映射协调用于不同密钥衍生机制的密钥材料。

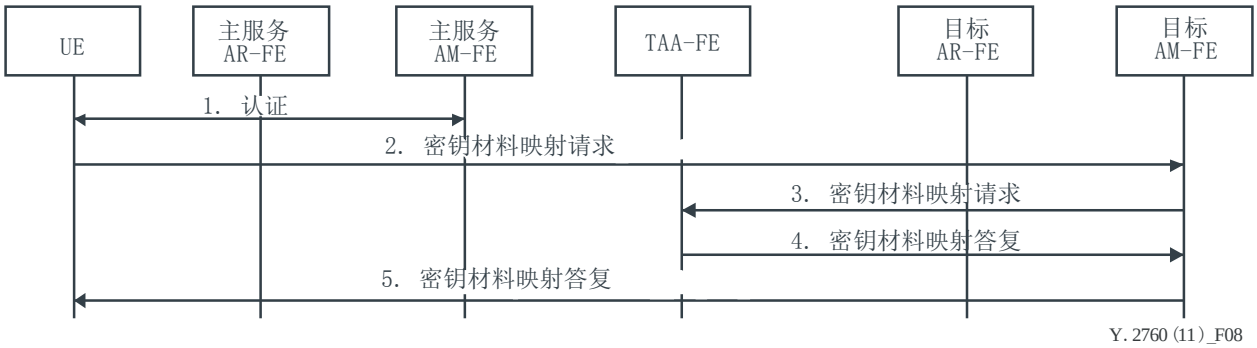


图 8 – 密钥材料映射程序

1) UE与TAA-FE之间建立连接，完成认证程序并生成会话密钥材料。

2) UE检测到目标网络，并准备向目标网络进行切换。UE向目标AM-FE发送密钥材料映射请求。密钥材料映射请求包括映射信息，如当前密钥衍生机制和所支持的密钥衍生机制。

3) 目标AM-FE向TAA-FE发送密钥材料映射请求。

4) TAA-FE接收密钥材料映射请求并将主服务网络中的密钥材料映射到目标网络中的密钥材料上，同时向目标AM-FE发送密钥材料映射答复。

5) 目标AM-FE向UE发送映射答复。UE将主服务网络中的密钥材料映射到目标网络中的目标密钥材料上。目标网络中的UE和TAA-FE均拥有共享的目标密钥材料，用以保护UE和目标网络之间的流量。

7.2.6 基于多网络接入的认证

基于多网络接入的认证意味着UE有能力同时与多个接入网通信。当UE具有多网络接入能力时，UE在断开与服务网络的连接之前与目标网络进行连接并完成相互认证程序。该相互认证为图3所示的一般性认证。成功完成相互认证之后，UE和TAA-FE均生成共享的会话密钥材料，且TAA-FE向目标AM-FE发送会话密钥材料。当UE移动到目标网络时，通过会话密钥材料或其子密钥材料保护UE与目标网络之间的流量。

7.2.7 基于多连接的认证

多连接意味着UE同时保持一个以上的网络连接。不同类型的网络连接可能为用户提供不同的客户体验，如很高的带宽、很低的时延和很高的安全性。不同管理域的多连接情况不属于本建议书的范围。

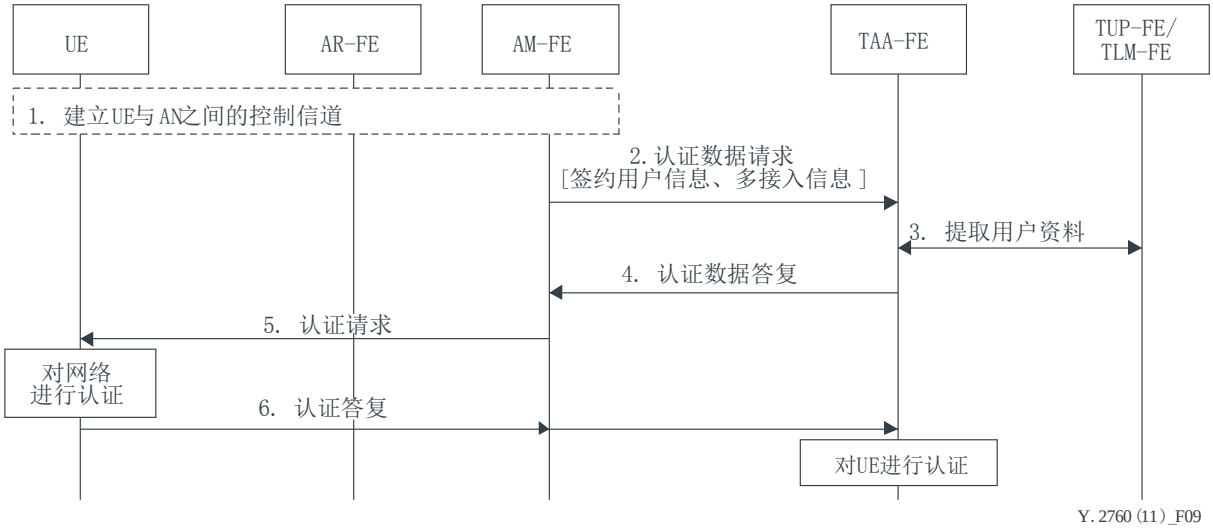


图 9 – 基于多连接的认证

1) 建立UE与接入网功能之间的控制信道（该程序不属于本建议书的范围）。UE从接入网处获得信息以及有关支持多接入认证的指示。

2) AM-FE向TAA-FE发送认证数据请求，认证数据请求包括UE信息，如签约用户信息（如用户签约用户身份）；多接入信息（如多接入指示和多接入接口身份）。

3) TAA-FE获得认证信息并与TUP-FE/TLM-FE进行互动，获得用户资料和认证矢量。认证矢量在TUP-FE/TLM-FE中生成，认证矢量中包含认证令牌。

4) TAA-FE向AM-FE发送认证数据答复，其中包括认证令牌。

5) AM-FE向UE发送认证请求。UE根据认证请求信息中的认证信息生成本地认证令牌，UE根据本地认证令牌检查所收到的认证令牌的有效性，从而对网络进行认证。成功完成认证之后，UE根据认证信息，生成会话密钥材料。如果设定多接入指示，则UE根据多接入信息生成多会话密钥材料。

6) UE向AM-FE发送认证答复信息，AM-FE将信息前转至TAA-FE，其中包括由UE生成的认证令牌。TAA-FE从认证答复信息中提取认证令牌，并根据TAA-FE中的认证矢量对UE进行认证。成功完成认证之后，TAA-FE根据认证令牌生成会话密钥材料。如果设定多接入指示，则TAA-FE根据多接入信息生成多会话密钥材料。

8 建立安全环境

8.1 主服务AM-FE与目标AM-FE之间安全环境的转移

应保护主服务AM-FE与目标AM-FE之间安全环境转移的流量。主服务AM-FE与目标AM-FE之间的安全可通过建立安全关联性实现。如果两个AM-FE处于相同区域，则不需要建立安全关联性。如果两个AM-FE处于不同区域，如在不同的运营商域，则通过安全机制和运营商的政策或协议建立安全关联性。

8.2 主服务AR-FE与目标AR-FE之间安全环境的转移

当UE在主服务AR-FE与目标AR-FE之间进行切换时，须保护目标AR-FE与主服务AR-FE之间安全环境的转移流量。主服务AR-FE与目标AR-FE之间的安全环境转移的安全通过建立安全关联性实现。

8.3 UE与HDC-FE之间的安全环境转移

8.3.1 主机启动的安全环境转移

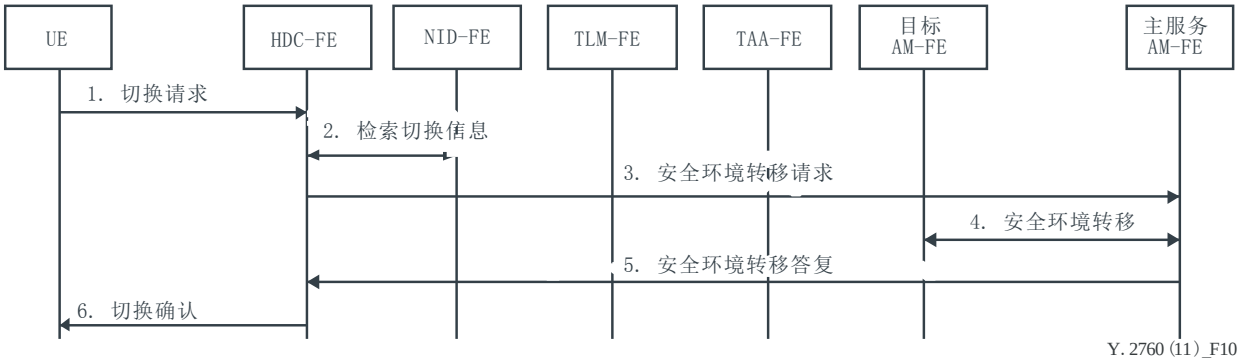


图 10 – 主机启动的安全环境转移程序

当UE决定从主服务网络到目标网络进行切换时，UE向HDC-FE发送切换请求，该请求将触发安全环境转移。完成安全环境转移后，目标AM-FE利用安全环境保护UE与目标网络之间的流量，具体步骤如下：

1) UE向HDC-FE发送切换请求。

2) HDC-FE接收切换请求，与NID-FE进行互动，以获得与切换相关的信息。

3) HDC-FE向主服务AM-FE前转切换请求，其中包括与切换相关的信息。

4) 主服务AM-FE与目标AM-FE互动，转移安全环境。

5) 完成安全环境转移后，主服务AM-FE向HDC-FE发送安全环境转移答复。

6) HDC-FE接收安全环境转移答复。如成功完成安全环境转移，则HDC-FE向UE发送切换确认信息。

8.3.2 网络启动的安全环境转移

当HDC-FE决定触发UE从主服务网络向目标网络进行切换时，则HDC-FE发送切换自举（bootstrapping）信息，以触发安全环境转移。安全环境转移完成后，目标AM-FE利用安全环境保护UE与目标网络之间的流量。

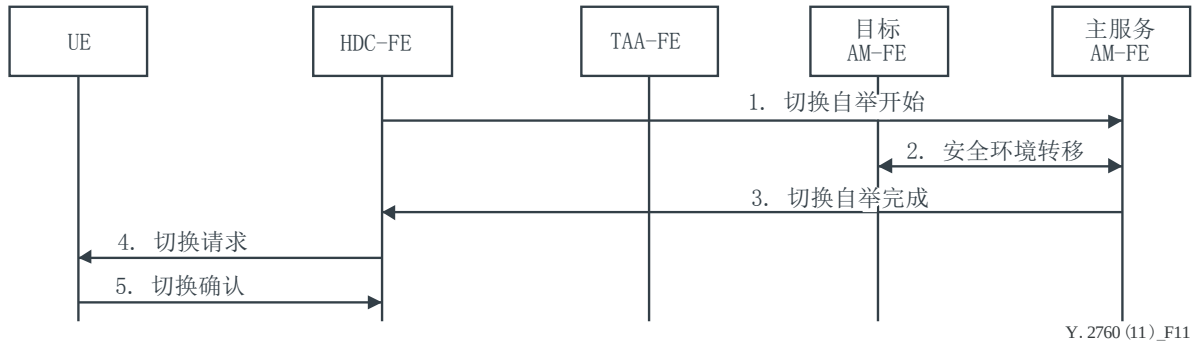


图 11 – 网络启动的安全环境转移程序

1) HDC-FE做出有关切换程序方面的准备，并向主服务AM-FE发送切换自举开始信息，以触发安全环境转移。

2) 主服务AM-FE与目标AM-FE进行互动，实施安全环境转移。

3) 安全环境转移完成后，主服务AM-FE向HDC-FE发送切换自举完成信息。

4) HDC-FE收到切换自举完成信息后，向UE发送切换请求，从而开始切换程序。

5) 切换完成后，UE发送切换确认信息。

9 IP移动安全

9.1 基于主机的移动安全

要求保护基于主机的、UE与MLM-FE (C)之间的移动控制流量，同时要求建立UE与MLM-FE (C)之间的安全关联性(SA)。UE与MLM-FE (P)之间的SA为可选功能。

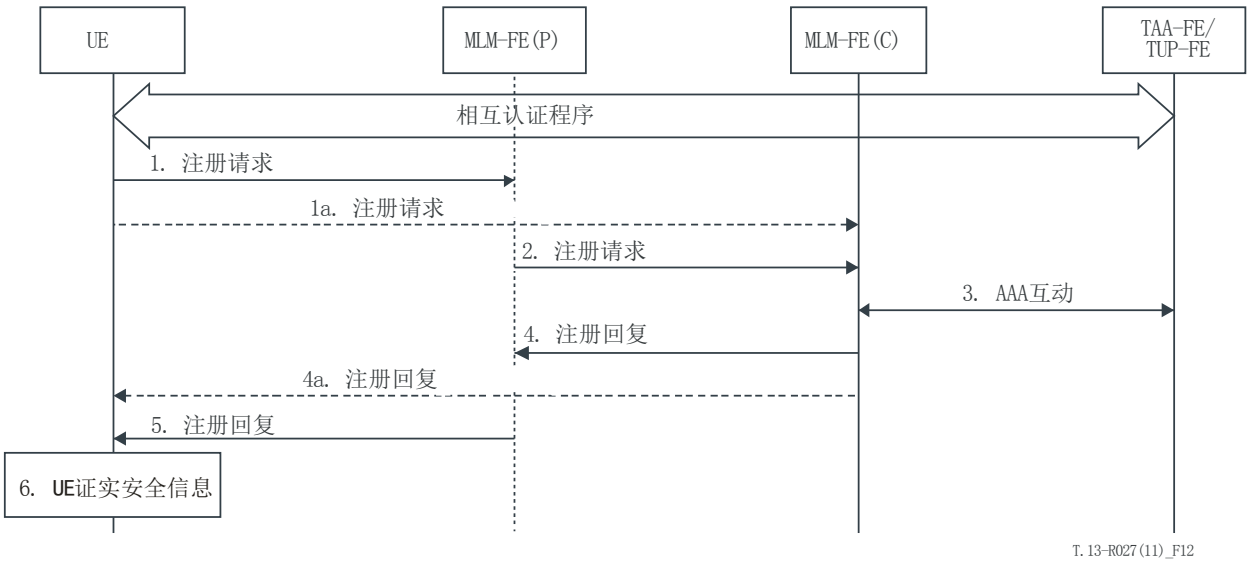


图 12 – 基于主机的移动程序

在假设UE与TAA-FE之间已完成一般性认证程序的情况下，需执行下列步骤。

1) UE向MLM-FE(P)发送注册请求，该注册请求包括UE与MLM-FE(C)之间的安全信息以及UE与MLM-FE(P)之间的安全信息。

   - 1a. 如不存在MLM-FE(P)，则UE直接向MLM-FE(C)发送注册请求。

2) MLM-FE(P)证实UE与MLM-FE(P)之间的安全信息，并将注册请求前转至MLM-FE(C)。MLM-FE(P)在前转注册请求之前可在该请求信息中增加MLM-FE(P)与MLM-FE(C)之间的安全信息。

3) MLM-FE(C)与TAA-FE/TUP-FE进行互动，以获得认证信息和授权信息。

4) MLM-FE(C)证实注册请求中UE与MLM-FE(C)之间的安全信息。MLM-FE(C)向MLM-FE(P)发送注册回复和安全信息。注册回复可包括UE与MLM-FE(C)之间的安全信息以及MLM-FE(P)与MLM-FE(C)之间的安全信息。

   - 4a. 如不存在MLM-FE (P)，则MLM-FE(C)向UE直接发送注册回复。注册回复可包括UE与MLM-FE(C)之间的安全信息。

5) MLM-FE(P)证实MLM-FE(P)与MLM-FE(C)之间的安全信息，并向UE发送注册回复。MLM-FE(P)在将注册回复信息前转之前可在其中增加UE与MLM-FE(P)之间的安全信息。

6) MLM-FE(C)证实UE与MLM-FE(C)之间的安全信息，并建立UE与MLM-FE(C)之间的SA。如果存在MLM-FE(P)，则UE证实UE与MLM-FE(P)之间的安全信息，并建立UE与MLM-FE(P)之间的SA。

9.2 基于网络的移动安全

对处于可信任区或可信任但脆弱区的两个网络实体之间基于网络的保护是可选功能，且以运营商的政策为基础。基于网络的移动控制流量的安全机制以[ITU-T Y.2704]中的安全机制为基础。

10 UE与HDC-FE之间的安全

UE与HDC-FE之间的信息流旨在承载有关作出切换决定的信息。UE与HDC-FE之间应建立安全关联性，以保护UE与HDC-FE之间的信息流。

10.1 主机启动的UE与HDC-FE之间安全关联性的建立

主机启动的安全关联性的建立程序意味着UE触发有关建立UE与HDC-FE之间安全关联性的程序（见图13）。建立由主机启动的UE与HDC-FE之间的安全关联性有两个先决条件。首先，UE与TAA-FE之间拥有预共享密钥材料，在相互认证之间，可获得预共享密钥材料。其次，UE了解有关HDC-FE的信息，如有关UE向HDC-FE发送安全关联性请求的地址。关于UE如何获得HDC-FE信息的方法不属于本建议书的范围。TLM的目的是以接力方式传送发往/来自TAA-FE的密钥材料信息，因此在下图中略去。

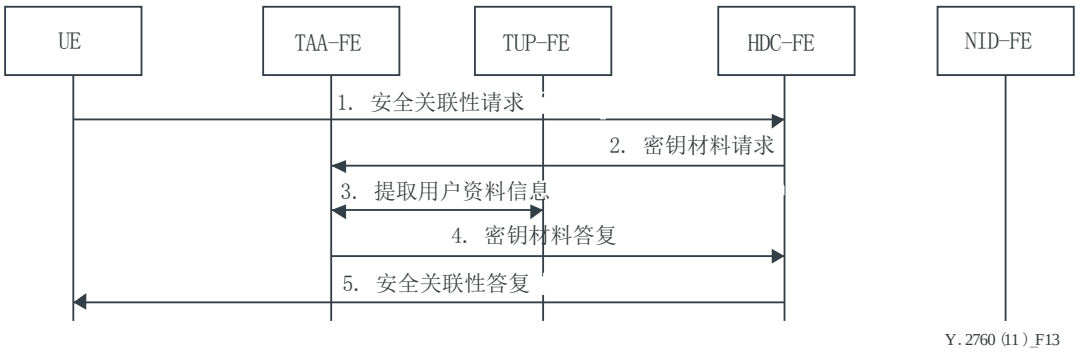


图 13 – 主机启动的安全关联性的建立程序

1) UE按照认证信息生成与HDC-FE建立关联性的共享密钥材料，UE向HDC-FE发送安全关联性请求，其中包括认证信息和UE信息。

2) HDC-FE向TAA-FE发送密钥材料请求，其中包括HDC-FE信息、认证信息和UE信息。

3) TAA-FE通过与TUP-FE进行互动提取用户资料信息，并检查确认HDC-FE已得到授权来建立与UE之间的安全关联性。

4) 当HDC-FE拥有建立与UE之间安全关联性的授权时，TAA-FE根据认证信息、HDC-FE信息和UE信息为HDC-FE生成密钥材料。TAA-FE向HDC-FE发送密钥材料答复，其中包括HDC-FE的密钥材料以及密钥寿命期等信息。

5) HDC-FE发送安全关联性答复，以做出有关已建立UE与HDC-FE之间安全关联性的通知。

10.2 网络启动的UE与HDC-FE之间安全关联性的建立

网络启动的安全关联性的建立程序意味着由网络端触发建立UE与HDC-FE之间安全关联性的程序（见图14）。建立UE与HDC-FE之间网络启动的安全关联性具有两个先决条件。首先，UE与TAA-FE之间拥有共享密钥材料，共享会话密钥材料可在相互认证之后生成。其次，HDC-FE了解UE的相关信息，如签约用户信息或HDC-FE向UE发送安全关联性信息的位置信息。HDC-FE如何获得UE信息的方法不属于本建议书的范围。

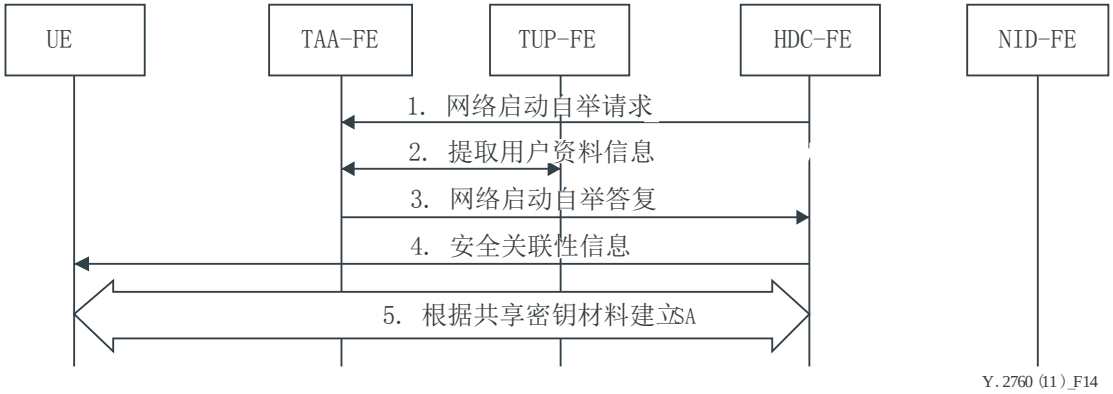


图 14 – 网络启动的安全关联性的建立程序

1) HDC-FE向TAA-FE发送网络启动的自举请求，其中包括HDC-FE信息和UE信息。

2) TAA-FE通过与TUP-FE互动提取用户资料信息，并检查确认HDC-FE已得到授权来启动与UE之间建立安全关联性的工作。

3) 当HDC-FE具有启动与UE建立安全关联性的授权时，TAA-FE根据HDC-FE信息和UE信息为HDC-FE生成密钥材料。TAA-FE向HDC-FE发送网络启动的自举答复，其中包括HDC-FE密钥材料及其寿命期的认证信息。

4) HDC-FE向UE发送包括认证信息在内的安全关联性信息，以建立安全关联性。

5) UE根据安全关联性信息中的认证信息为HDC-FE生成密钥材料，并证实安全关联性信息。由此HDC-FE与UE之间的安全关联性得到建立。

10.3 根据PKI预先建立UE与HDC-FE之间的安全关联性

图15所示为根据PKI建立UE与HDC-FE之间安全关联性的程序。UE与HDC-FE之间关联性建立程序的先决条件是UE了解有关HDC-FE的相关信息，如UE向HDC-FE发送安全关联性请求的地址。有关UE如何获得HDC-FE信息的方法不属于本建议书的范围。

图 15 – 根据PKI建立安全关联性的程序

1) UE向HDC-FE发送安全关联性请求，其中包括UE证书和UE信息。

2) HDC-FE证实UE证书，并向TAA-FE发送授权请求，其中包括UE信息和HDC-FE信息。

3) TAA-FE根据UE信息和HDC-FE检查授权情况。如UE已被授权使用HDC-FE，则TAA-FE向HDC-FE发送授权答复，其中包括授权信息和服务器证书。

4) HDC-FE接受授权信息，并向UE发送包括服务器证书在内的安全关联性答复。

5) 如UE与TAA-FE之间需要共享密钥材料，则TAA-FE向UE发送步骤4中的密钥生成信息。UE根据收到的密钥生成信息和本地密钥生成信息生成共享的密钥材料。UE向HDC-FE发送本地密钥生成信息。

6) HDC-FE根据收到的密钥生成信息和本地密钥生成信息生成密钥材料。HDC-FE向UE发送安全关联性答复。由此UE与HDC-FE之间建立了安全关联性。

11 UE与NID-FE之间的安全关联性

11.1 主机启动的UE与NID-FE之间的安全关联性的建立

图16所示为主机启动的UE与NID-FE之间的安全关联性的建立程序。UE与NID-FE之间安全关联性建立程序的先决条件如下： 1) UE与TAA-FE之间拥有共享密钥材料，可在完成相互认证程序之后生成共享的会话密钥材料。2) UE了解有关NID-FE的信息，如UE向NID-FE发送安全关联性请求的地址。UE如何获得NID-FE信息的方法不属于本建议书的范围。

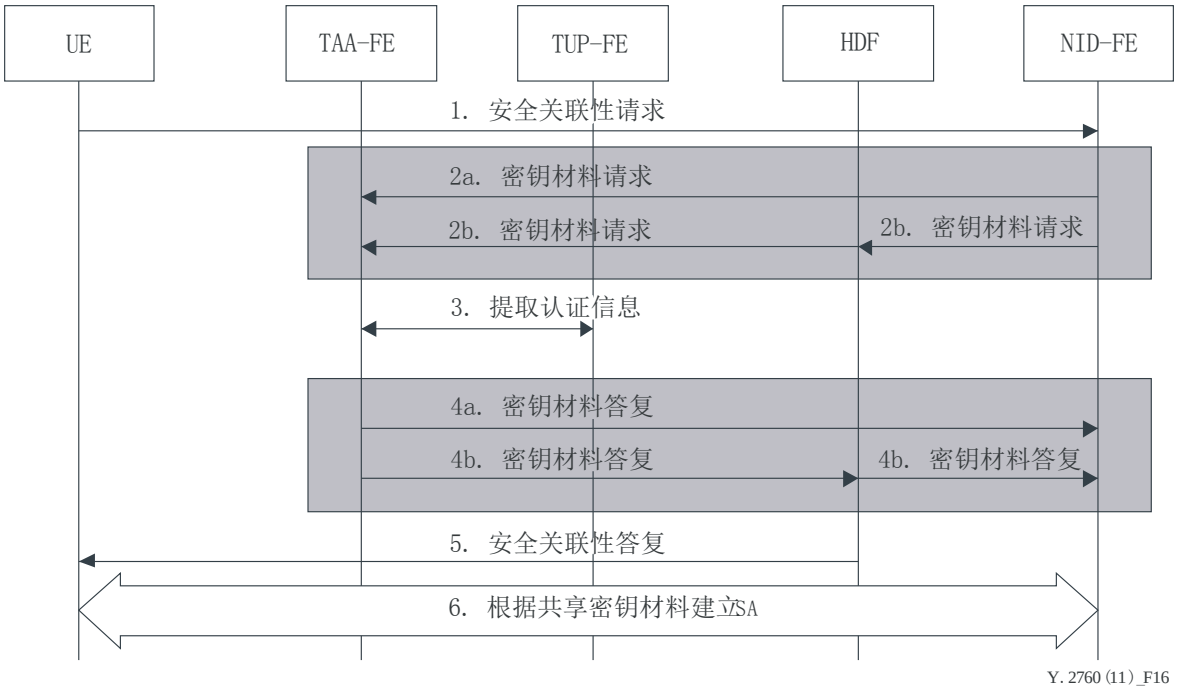


图 16 – 主机启动的安全关联性的建立

1) UE向NID-FE发送安全关联性请求

2) NID-FE向TAA-FE发送密钥材料请求，其中包括NID-FE信息和UE信息。当NID-FE不支持直接向TAA-FE发送认证请求时，则NID-FE通过HDC-FE向TAA-FE发送认证请求。

3) TAA-FE与TUP-FE进行互动，并为NID-FE生成密钥材料。

4) TAA-FE向HDC-FE发送包括认证信息在内的密钥材料答复。认证信息包括共享密钥材料及其寿命期信息。当TAA-FE不支持直接向NID-FE发送认证请求时，则TAA-FE通过HDC-FE向NID-FE发送认证请求。

5) NID-FE向UE发送包括认证信息在内的安全关联性答复（得到共享密钥材料保护）。

6) UE生成共享密钥材料并证实安全关联性答复。由此在共享密钥材料基础上建立了NID-FE与UE之间的安全关联性。

11.2 网络启动的UE与NID-FE之间的安全关联性的建立

图17所示为网络启动的UE与NID-FE之间的安全关联性的建立程序。UE与NID-FE之间安全关联性建立程序的先决条件如下： 1) UE与TAA-FE之间拥有共享密钥材料。在完成相互认证程序之后，可生成共享会话密钥材料。2) UE了解有关NID-FE的信息，如UE向NID-FE发送安全关联性请求的地址。有关UE如何获得NID-FE信息的方法不属于本建议书的范围。

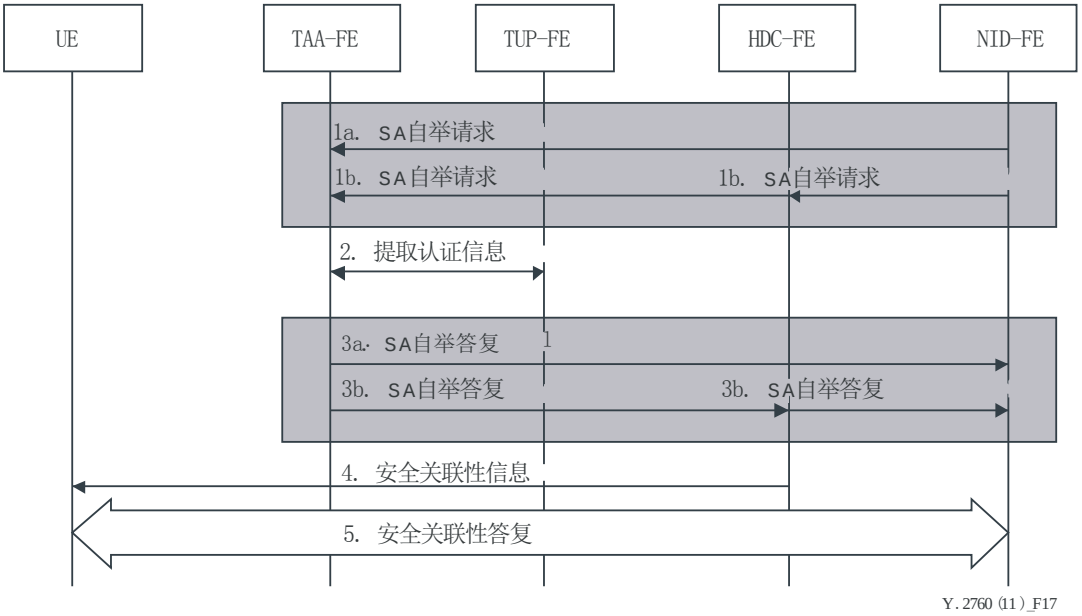


图 17 – 网络启动的安全关联性的建立

1) NID-FE向TAA-FE发送包括NID-FE信息在内的SA自举请求。当NID-FE不支持向TAA-FE直接发送SA自举请求时，NID-FE通过HDC-FE向TAA-FE发送SA自举请求。

2) TAA-FE与TUP-FE进行互动，并为NID-FE生成密钥材料。

3) TAA-FE向NID-FE发送包括认证信息在内的SA自举答复。认证信息包括密钥材料及其寿命期信息。当TAA-FE不支持直接向NID-FE发送SA自举答复时，TAA-FE通过HDC-FE向NID-FE发送SA自举答复。

4) NID-FE向UE发送包括认证信息在内的安全关联性信息（由共享密钥材料保护）。

5) UE生成共享密钥材料并证实安全关联性信息。由此根据共享密钥材料建立了NID-FE与UE之间的安全关联性。

11.3 根据PKI建立UE与NID-FE之间的安全关联性

图18所示为根据PKI建立UE与NID-FE之间安全关联性的程序。UE与NID-FE之间安全关联性建立程序的先决条件是UE了解有关NID-FE的信息，如UE向NID-FE发送安全关联性请求的地址。有关UE如何获得NID-FE信息的方法不属于本建议书的范围。

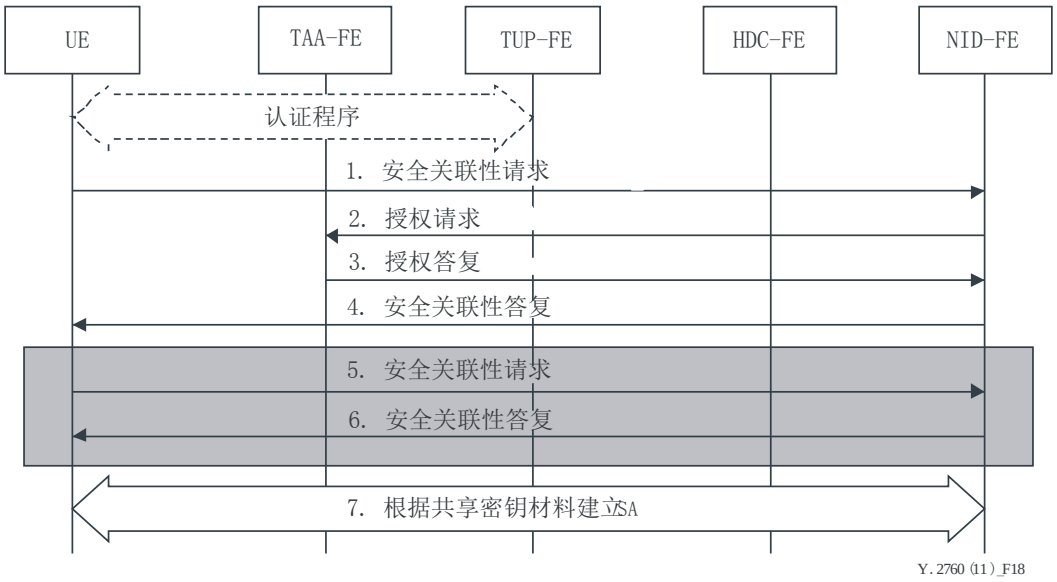


图18 – 根据PKI建立安全关联性的程序

在完成TUP-FE与TAA-FE之间的认证程序之后，应执行下列步骤。

1) UE向NID-FE发送包括UE证书和UE信息在内的安全关联性请求。

2) NID-FE证实UE证书并向TAA-FE发送包括UE信息和NID-FE在内的授权请求。

3) TAA-FE根据UE信息和NID-FE检查授权情况。如UE已被授权使用NID-FE，则TAA-FE向NID-FE发送授权答复，其中包括授权信息和服务器证书。

4) NID-FE接收授权信息并向UE发送包括服务器证书在内的安全关联性答复。

5) 如在UE与TAA-FE之间需要共享密钥材料，则TAA-FE向UE发送步骤4中的密钥生成信息。UE根据收到的密钥生成信息和本地密钥生成信息生成共享密钥材料。UE将本地密钥生成信息作为安全关联性请求的一部分发送至NID-FE。

6) NID-FE根据收到的密钥生成信息和本地密钥生成信息生成密钥材料。NID-FE向UE发送安全关联性答复。

7) 由此建立了UE与NID-FE之间的安全关联性。

12 传输功能安全

12.1 UE与接入节点功能实体之间的安全

应保护UE与AN-FE之间的流量，UE与AN-FE之间的安全关联性以共享密钥材料为基础。在成功完成UE与TAA-FE之间的认证程序之后，UE和TAA-FE都生成诸如会话密钥等的密钥材料，以保护UE与AN-FE之间的流量。TAA-FE通过AM-FE和AR-FE向AN-FE发送密钥材料。

12.2 UE与L3HEF（第3层切换执行功能）之间的安全

应保护UE与L3HEF之间的流量。UE与L3HEF之间的安全关联性是在预共享密钥材料基础上建立的。在成功完成相互认证之后，UE和TAA-FE均生成诸如会话密钥等密钥材料，以保护UE与L3HEF之间的流量。L3HEF从TAA-FE处直接获得密钥材料，同时L3HEF亦通过AM-FE或HDC-FE从TAA-FE处获得密钥材料。

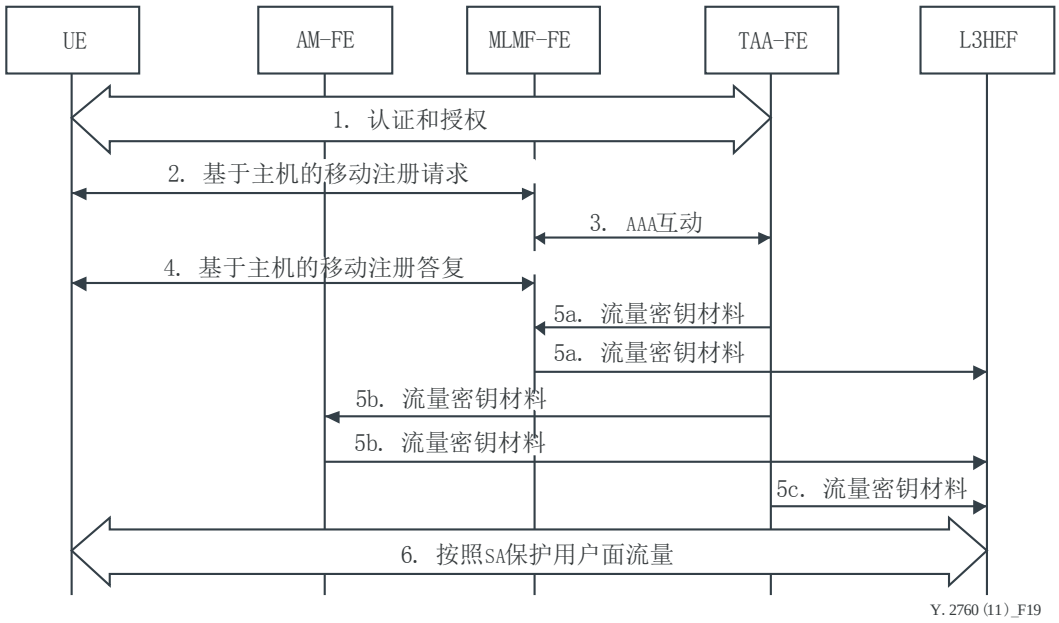


图 19 – UE与L3HEF之间的用户面流量安全程序

1) UE与TAA-FE之间建立连接，完成相互认证之后，UE和TAA-FE均生成共享密钥材料，如瞬间密钥材料和会话密钥材料。

2) UE向MLM-FE发送基于主机的移动注册请求，以建立主机移动安全关联性。

3) MLM-FE通过与TAA-FE互动获得密钥材料。MLM-FE根据密钥材料对UE进行认证。成功完成认证之后，MLM-FE根据密钥材料建立与UE之间的安全关联性。

4) MLM-FE向UE发送基于主机的移动注册答复，UE证实基于主机的移动注册答复信息并与MLM-FE建立安全关联性。

5) 建立UE与MLM-FE之间的安全关联性之后，将出现三种情况。

   5a. TAA生成流量密钥材料并通过MLM-FE向L3HEF发送流量密钥材料。

   5b. TAA生成流量密钥材料并通过MLM-FE和AM-FE向L3HEF发送流量密钥材料。

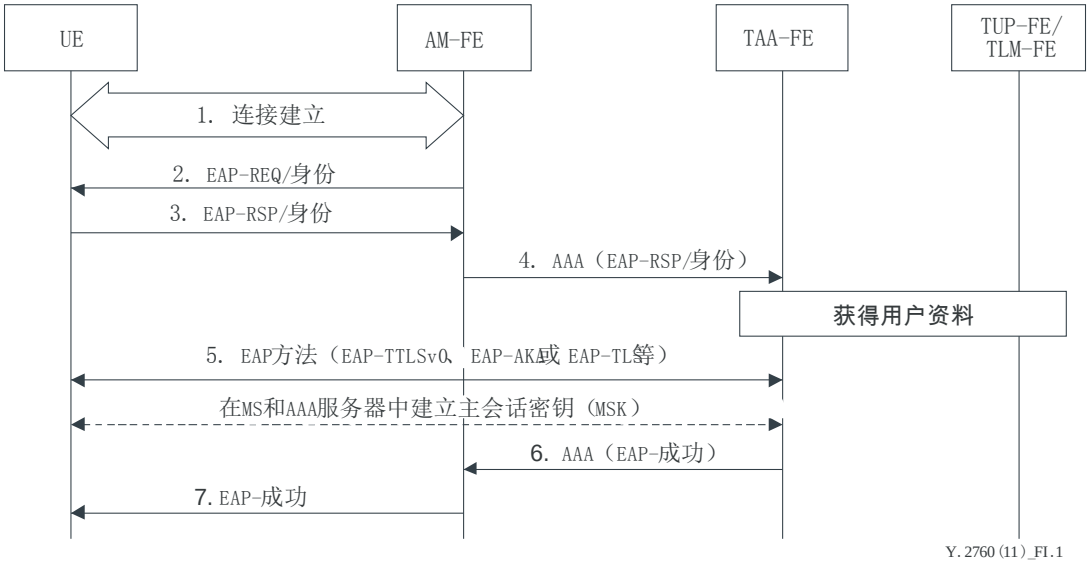
   5c. TAA-FE直接向L3HEF发送流量密钥材料。

6) L3HEF利用流量密钥材料保护UE与L3HEF之间的用户面流量。

附录 I

（本附录是本建议书的组成部分）

I.1 完整认证程序示例



图I.1 – 总体认证程序

注 — 步骤2-4中的身份系指UE身份。

所示为认证自举。

1) UE与AM-FE之间建立连接。

2) AM-FE向UE发送EAP请求（EAP-REQ）/身份[b-IETF RFC 3748]。

3) UE发送EAP答复(EAP-RSP)/身份信息。

4) AM-FE向TAA-FE前转EAP-RSP/身份，之后TAA-FE与TUP-FE/TLM-FE进行交换，并由TUP-FE/TLM-FE向TAA-FE发送用户信息（包括资料）。

5) 密钥衍生和分布程序在TAA-FE和UE中执行，其中可考虑若干方法，如EAP-TTLS、EAP-AKA、EAP-TLS等。

6) TAA-FE向AM-FE发送EAP成功信息。

7) AM-FE利用EAP成功信息通知UE已成功进行认证，由此已成功完成基于EAP的密钥交换程序，且UE与AM-FE之间共享在该交换程序中衍生的密钥材料。

I.2 快速再认证程序示例

在出现切换时，快速再认证可在时延很低的情况下保持业务连续性。快速再认证需要使用快速再认证身份，并无需与TAA-FE和TUP-FE/TLM-FE进行认证信息的交换。

以下所示为快速再认证的总体程序。

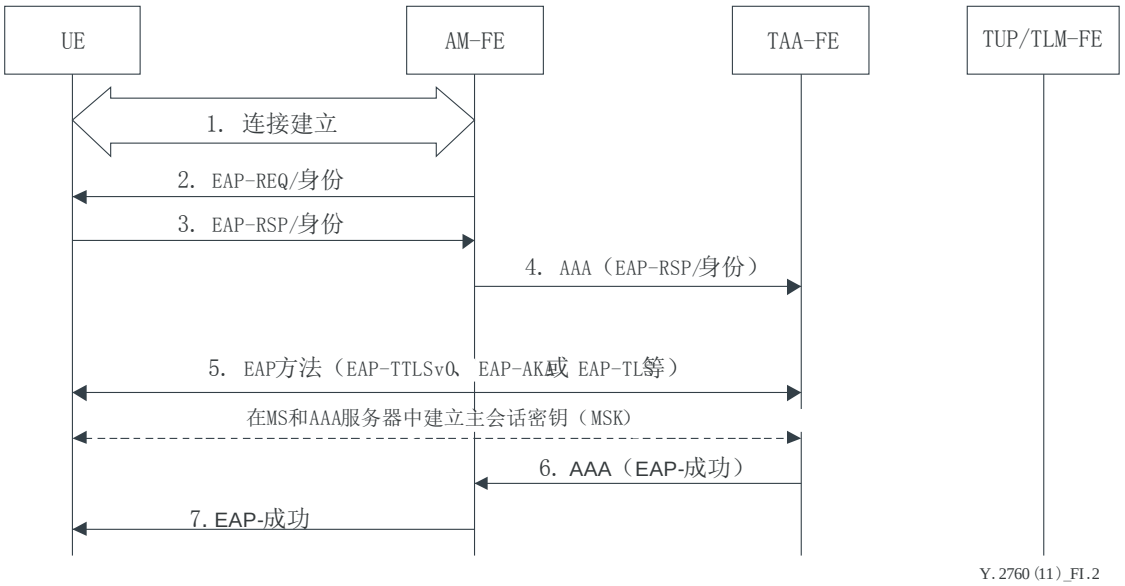


图 I.2 – 快速再认证程序

1) UE与AM-FE之间建立连接
2) AM-FE向UE发送EAP-REQ/身份，其中载有再认证身份。
3) UE发送EAP答复/身份信息。
4) AM-FE向TAA-FE前转EAP-RSP/身份信息。
5) 执行密钥衍生和分布程序，可考虑若干种方法，如EAP-AKA、EAP-TLS等。
6) TAA-FE向AM-FE发送EAP成功信息。
7) AM-FE通过EAP成功信息通知UE已成功完成认证，由此已成功完成基于EAP的密钥交换程序，且UE和AM-FE I共享在该交换中衍生的密钥材料。

I.3 主机启动的移动示例

对MIPv4而言，IP移动安全是以[b-IETF RFC 3344]确定的MIP认证扩展为基础的。必须使用 MIP扩展保护UE与作为HA（即MLM-FE）行事的节点之间的IP移动信令信息，UE与作为FA （即MLM-FE）行事的节点之间的信令信息保护为可选功能。

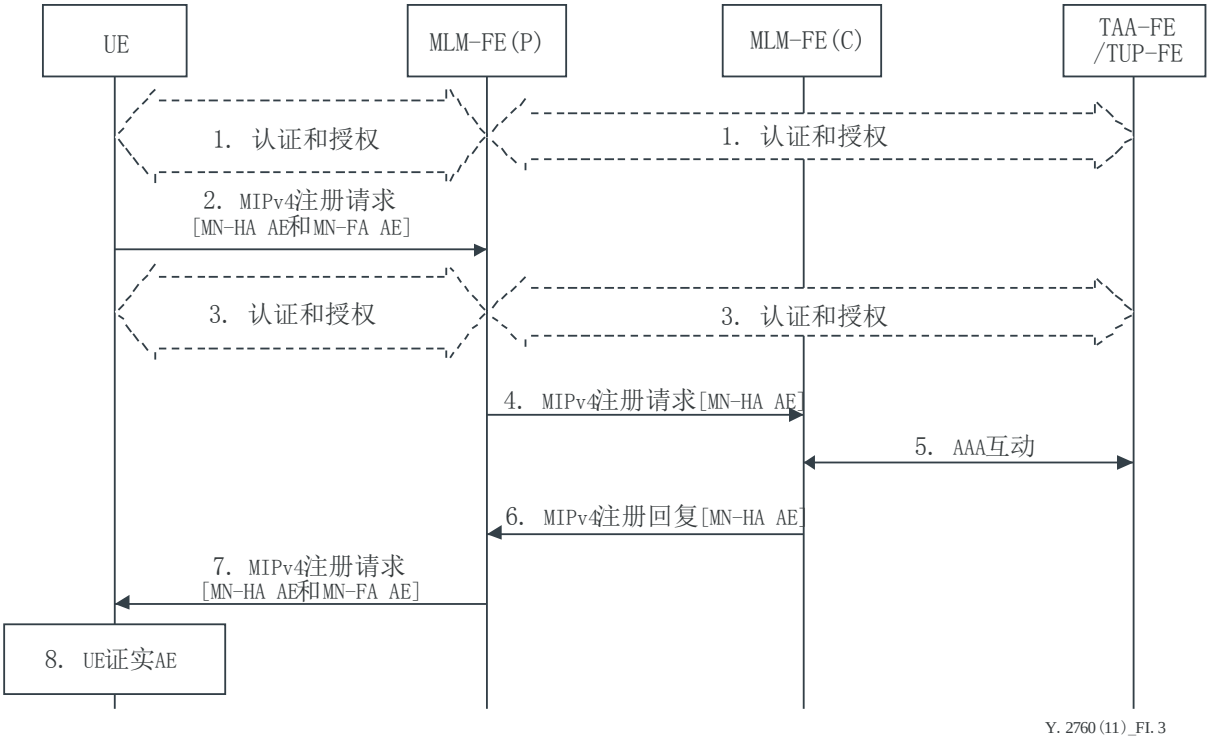


图 I.3 – MIPv4自举程序

图I. 3所示的MIPv4自举程序如下。

1) 通过TAA-FE /TUP-FE的帮助进行UE与MLM-FE之间的认证和授权。

2) UE向与FA (MLM-FE)发送注册请求（RRQ）信息。如[b-IETF RFC 3344]所述，UE包含MN-HA认证扩展（AE）并作为可选功能，包含MN-FA认证扩展（AE）。

3) RRQ触发接入认证程序。

4) FA根据[b-IETF RFC 3344]处理信息，并在存在MN-FA认证扩展时对其进行证实，之后FA将RRQ信息前转至HA(MLM-FE)。

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

6) MLM-FE证实MN-HA认证扩展，成功证实认证扩展后，MLM-FE通过FA向UE发送注册回复（RRP）。

7) FA根据[b-IETF RFC 3344]处理RRP，之后FA向UE前转RRP信息。如果FA在RRQ信息中收到MN-FA认证扩展，则FA将MN-FA认证扩展包括进来。

8) UE证实MN-HA认证扩展，并在MN-FA认证扩展存在时对其予以证实。

参考资料

[b-IETF RFC 3220] IETF RFC 3220 (2002), *IP Mobility Support for IPv4.*

[b-IETF RFC 3344] IETF RFC 3344 (2002), *IP Mobility Support for IPv4.*

[b-IETF RFC 3775] IETF RFC 3775 (2004), *Mobility Support in IPv6*

[b-IETF RFC 5213] IETF RFC 5213 (2008), *Proxy Mobile IPv6.*

[b-IETF RFC 3748] IETF RFC 3748 (2004), *Extensible Authentication Protocol (EAP).*

[b-IETF RFC 4555] IETF RFC 4555 (2006), IKEv2 Mobility and Multihoming Protocol.

[b-3GPP TS 33.102] 3GPP TS 33.102 V7.1.0 (2007), *3G Security: Security Architecture.*

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其他多媒体信号的传输
K系列	干扰的防护
L系列	电缆和外部设备其他组件的结构、安装和保护
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备的技术规范
P系列	终端和主观与客观评估方法
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	数据网、开放系统通信和安全性
Y系列	**全球信息基础设施、互联网的协议问题和下一代网络**
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2012年，日内瓦