B-TrunC TM 02.002.02 V2.0

基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）接口测试方法 终端到核心网接口 第2部分：宽带数据

Test method for NAS interface of LTE based broadband trunking communication （B-TrunC） system （Phase 2） part 2: broadband data

宽带集群产业联盟
Broadband Trunking Communication Industry Alliance

2019年8月

版本修订记录

版本	主要修订内容	日期
V1.0	初始发布	
V2.0	统一版本升级	2019/8

前　言

本标准是由宽带集群产业联盟制定的基于 LTE 技术的宽带集群通信（B-TrunC）系统（第二阶段）系列标准之一，该系列标准的结构和名称如下：

1) B-TrunC TS 02.001 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）总体技术要求
2) B-TrunC TS 02.002 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）端到端流程
3) B-TrunC TS 02.003 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）安全技术要求
4) B-TrunC TS 02.004 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）接口技术要求 空中接口
5) B-TrunC TS 02.005 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）接口技术要求 终端到核心网接口
6) B-TrunC TS 02.006 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）接口技术要求 基站与核心网间接口
7) B-TrunC TS 02.007 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）接口技术要求 核心网间接口
8) B-TrunC TS 02.008 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）接口技术要求 核心网到调度台接口
9) B-TrunC TS 02.009 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）终端设备技术要求
10) B-TrunC TS 02.010 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）基站设备技术要求
11) B-TrunC TS 02.011 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）核心网设备技术要求
12) B-TrunC TS 02.012 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）调度台设备技术要求
13) B-TrunC TS 02.013 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）多媒体消息业务技术要求
14) B-TrunC TS 02.014 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）定位业务技术要求
15) B-TrunC TS 02.015 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）B-TrunC与非B-TrunC集群系统间互联互通技术要求
16) B-TrunC TM 02.001.01 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）接口测试方法 空中接口 第1部分：集群
17) B-TrunC TM 02.001.02 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）接口测试方法 空中接口 第2部分：宽带数据
18) B-TrunC TM 02.002.01 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）接口测试方法 终端到核心网接口 第1部分：集群
19) B-TrunC TM 02.002.02 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）接口测试方法 终端到核心网接口 第2部分：宽带数据
20) B-TrunC TM 02.003.01 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）接口测试方法 基站与核心网间接口 第1部分：集群

21) B-TrunC TM 02.003.02 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）接口测试方法 基站与核心网间接口 第2部分：宽带数据
22) B-TrunC TM 02.004.01 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）接口测试方法 核心网间接口 第1部分：集群
23) B-TrunC TM 02.004.02 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）接口测试方法 核心网间接口 第2部分：宽带数据
24) B-TrunC TM 02.005 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）接口测试方法 核心网到调度台接口
25) B-TrunC TM 02.006.01 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）终端设备测试方法 第1部分：集群
26) B-TrunC TM 02.006.02 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）终端设备测试方法 第2部分：宽带数据
27) B-TrunC TM 02.007.01 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）基站设备测试方法 第1部分：集群
28) B-TrunC TM 02.007.02 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）基站设备测试方法 第2部分：宽带数据
29) B-TrunC TM 02.008.01 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）核心网设备测试方法 第1部分：集群
30) B-TrunC TM 02.008.02 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）核心网设备测试方法 第2部分：宽带数据
31) B-TrunC TM 02.009 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）调度台设备测试方法
32) B-TrunC TM 02.010 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）终端与网络互操作测试方法
33) B-TrunC TM 02.011 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）调度台与网络互操作测试方法
34) B-TrunC TM 02.012 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）多媒体消息业务测试方法
35) B-TrunC TM 02.013 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）定位业务测试方法
36) B-TrunC TM 02.014 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）B-TrunC与非B-TrunC集群系统间互联互通测试方法
37) B-TrunC TM 02.015 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）终端设备射频测试方法
38) B-TrunC TM 02.016 基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）基站设备射频测试方法

随着技术的发展，还将制定后续的相关标准。

本标准按照GB/T 1.1-2009给出的规则起草。本标准由宽带集群产业联盟提出并归口。

本标准起草单位：中国信息通信研究院、鼎桥通信技术有限公司、北京中兴高达通信技术有限公司、海能达通信股份有限公司、普天信息技术有限公司、北京信威通信技术股份有限公司、武汉虹信通信技

术有限责任公司、大唐电信科技产业集团、中兴通讯股份有限公司、华为技术有限公司、首都信息发展股份有限公司

本标准主要起草人：杜加懂、宋得龙、陈迎、蔡杰、郑伟、李晓华、袁剑、陈钢、吴迪、叶亚娟、梅晓华、崔媛媛、王威、陈金山、张耀匀、李赛男

目 次

基于 LTE 技术的宽带集群通信（B-TrunC）系统（第二阶段）接口测试方法 终端到核心网接口 第 2 部分：宽带数据

1 范围

本标准规定了基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）终端和核心网接口的宽带数据部分测试方法，包括NAS层接口基本功能及安全功能的测试内容。

本标准适用于基于LTE技术的宽带集群通信（B-TrunC）系统（第二阶段）的终端和网络设备的宽带数据部分。

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。

3 缩略语

下列缩略语适用于本文件。

CP	循环前缀	Cyclic Prefix
eNB	演进的基站	Evolved Node B
ECM	EPS 连接管理	EPS Connection Management
EEA	EPS 加密算法	EPS Encryption Algorithm
EIA	EPS 完整性保护算法	EPS Integrity Algorithm
EMM	EPS 移动性管理	EPS Mobility Management
EPC	演进的分组核心网	Evolved Packet Core
EPS	演进的分组系统	Evolved Packet System
E-UTRAN	演进的接入网	Evolved Universal Terrestrial Radio Access Network
GUTI	全球唯一临时 UE 标识符	Globally Unique Temporary UE Identity
HSS	归属签约服务器	Home Subscriber Server
MME	移动性管理实体	Mobility Management Entity
NAS	非接入层	Non-access stratum
PLMN	公众地面移动网络	Public Land Mobile Network
P-GW	PDN 网关	PDN Gateway
QoS	服务级别	Quality of Service

RRC	无线资源控制	Radio Resource Control
S-GW	服务网关	Serving Gateway
TAU	跟踪区域更新	Tracking Area Update
UE	用户设备	User Equipment

4 概述

4.1 测试配置

终端与核心网接口测试环境连接如图1所示。

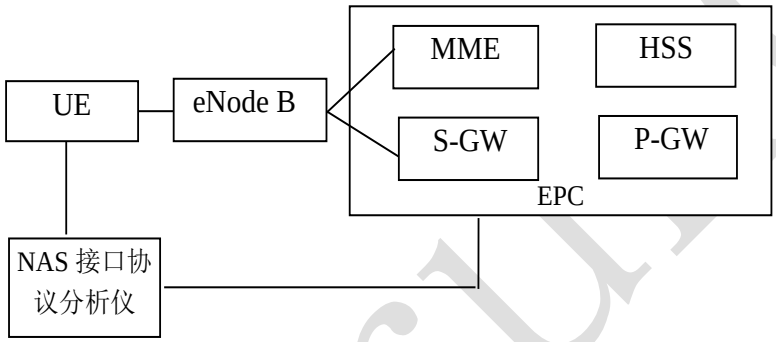


图 1 终端与核心网测试环境示意

4.2 测试的前提条件

测试前，应满足：

——被测设备安装完毕，硬件软件全部工作正常，系统配置数据正确并正常运行；

——辅助测试设备硬件软件全部工作正常，已完成各种逻辑数据的正确设置；

——辅助测试无线环境正常工作。

5 NAS 层接口测试

5.1 PLMN 选择

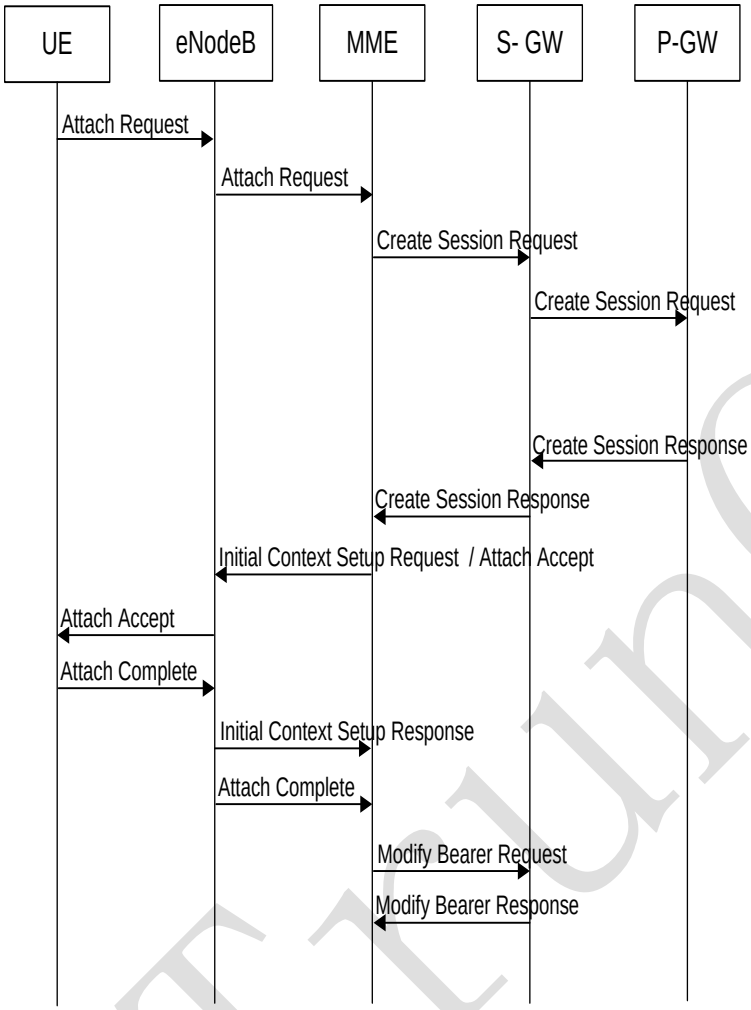
测试项目：PLMN 选择
测试目的： 测试 UE 的 PLMN 选择功能
测试条件： 1） 网络 A 配置为 PLMN1，网络 B 配置为 PLMN2，PLMN1 与 PLMN2 是等效 PLMN； 2） UE 的 HPLMN 为 PLMN1。
测试步骤： 1） UE 在网络 A 开机；

2） 关闭网络 A，启动网络 B。
预期结果： 1） UE 成功在网络 A 驻留，选择 PLMN1； 2） 关闭网络 A 后，UE 成功驻留到网络 B，选择 PLMN2。

5.2 移动性管理

5.2.1 附着

测试项目：移动性管理
测试分项目：附着
测试目的：验证EPS网络能够正确处理用户的IMSI附着。
预置条件： 1） EPS网络中各网元系统及操作维护台运行正常； 2） 用户在HSS中已签约EPS业务； 3） 保证用户使用IMSI附着； 4） 在MME上配置用户附着过程中需要鉴权、加密和完整性保护。
测试步骤： 1） UE开机发起IMSI附着； 2） 在网络侧查询用户的信息。
预期结果： 1） UE成功附着到网络； 2） 缺省承载建立成功； 3） 数据业务正常； 4） 用户EMM状态为EMM-REGISTERED，ECM状态为ECM-CONNECTED； 5） NAS消息流程正确。
测试说明：



1) UE开机发起附着，向MME发送Attach Request（EPS Mobile Identity=IMSI）消息；
2) MME发起鉴权安全流程；
3) MME发送Initial Context Setup Request给eNodeB，里面携带了Attach Accept消息，该消息中包含了Activate Default EPS Bearer Context Request消息，要求建立缺省承载；
4) UE返回Attach Complete，eNodeB返回Initial Context Setup Response消息，建立缺省承载成功。

5.2.2 UE 发起的去附着

测试项目：移动性管理
测试分项：去附着
测试目的：验证MME能够正确处理用户发起的去附着流程。
预置条件： 1) EPS网络中各网元系统及操作维护台运行正常； 2) 用户已经签约EPS业务； 3) UE已经附着到MME，并处于ECM-CONNECTED状态。

测试步骤：

1） UE关机发起去附着；

2） 在网络侧查询用户的信息。

预期结果：

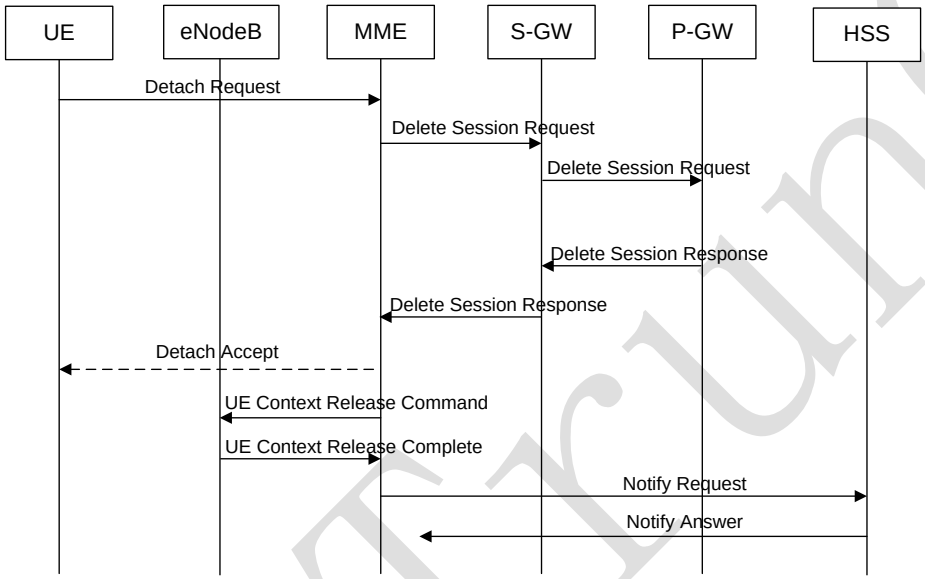
1） UE去附着成功；

2） MME上用户状态为非注册态；

3） 由于是关机去附着，MME不会回Detach Accept消息；

4） NAS消息流程正确。

测试说明：



1） UE发起去附着，向MME发送Detach Request消息；

2） 如果是关机去附着，MME不需要向UE发送Detach Accept消息；

3） 释放成功。

5.2.3 网络发起的去附着

测试项目：去附着

测试分项目：MME发起显式去附着流程

测试目的：验证MME能够显式地去附着用户。

预置条件：

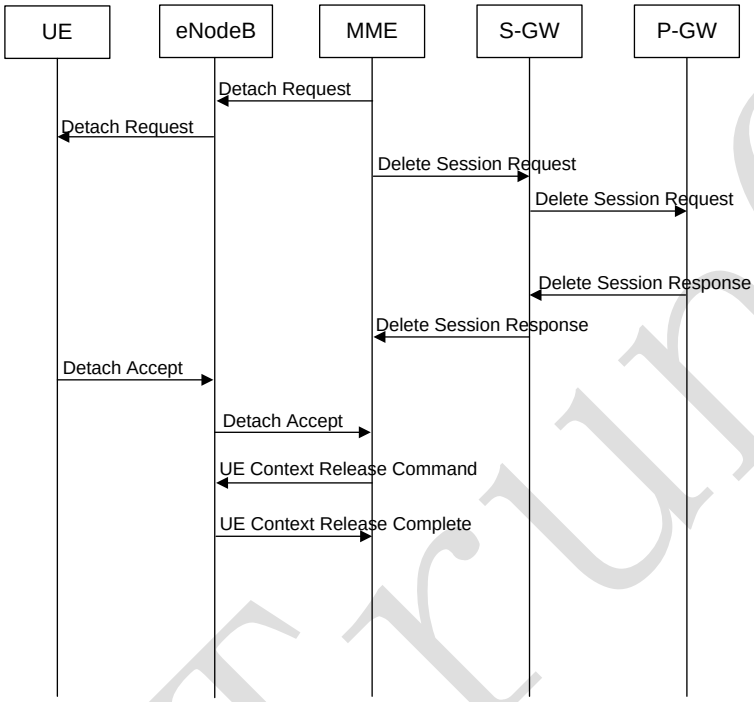
1） EPS网络中各网元系统及操作维护台运行正常；

2） 用户已经签约EPS业务；

3） UE已经附着到MME，并处于ECM-CONNECTED状态。

测试步骤：

1） MME通过操作维护台删除用户，发起Detach流程；

2) 在网络侧查询用户的信息。
预期结果： 1) 去附着成功； 2) MME上用户状态为非注册态； 3) NAS消息流程正确。
测试说明：    1) MME通过操作维护台删除用户，发起去附着流程，向UE发送Detach Request消息； 2) UE收到Detach Request消息后，发送Detach Accept，接受去附着； 3) MME发起S1释放流程，释放成功。

5.2.4 位置改变引起的 TAU

测试项目：移动性管理
测试分项：位置改变引起的TAU
测试目的：验证MME正确处理ECM-IDLE状态下UE发起的TAU，S-GW不变，MME不变。
预置条件： 1) EPS网络中各网元系统及操作维护台运行正常； 2) 用户已经签约EPS业务； 3) UE已经附着，并获取IPv4地址，处于 ECM-IDLE状态。
测试步骤： 1) UE移动到另一个TA中，该TA不属于原来的TA List； 2) 在网络侧查询用户的信息。

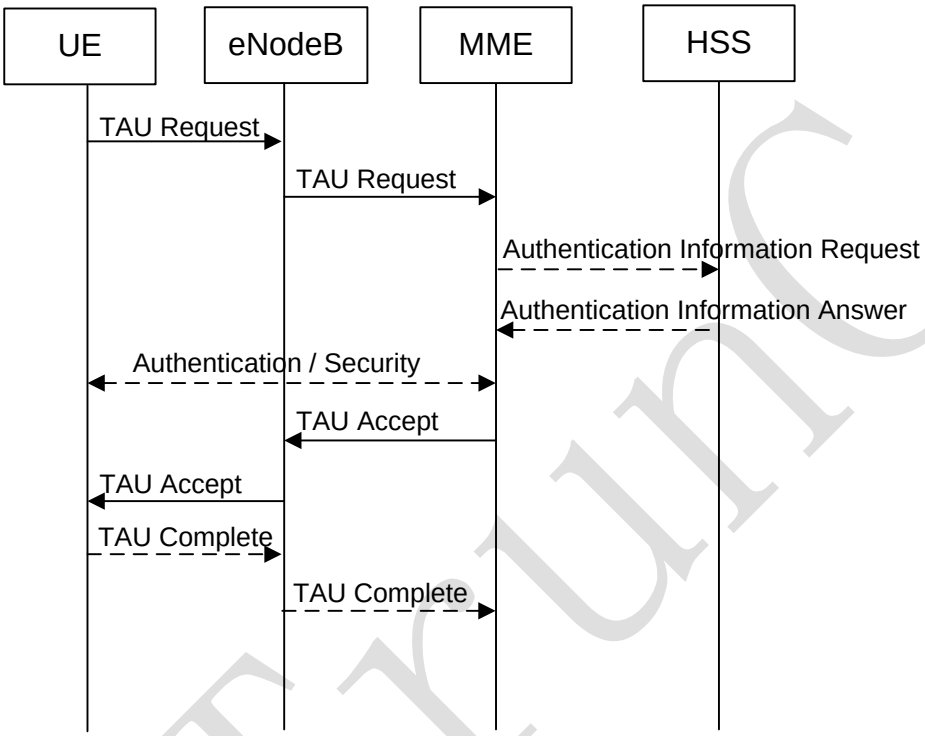
预期结果：

1） TAU成功；

2） MME中用户EMM状态为EMM-REGISTERED，TA是新的TA

3） NAS消息流程正确。

测试说明：



1） UE发送TAU Request消息给MME，发起TAU流程；

2） MME可以发起安全流程；

3） MME发送TAU Accept响应UE；

4） 如果GUTI重新分配了，UE响应TAU Complete消息。

5.3 会话管理

5.3.1 专用 EPS 承载激活

测试项目：会话管理

测试分项：专用 EPS 承载激活

测试目的：

验证终端可以激活专用 EPS 承载。

测试条件：

1） UE驻留在E-UTRA小区CELL1；

2） UE已附着，处于EMM-REGISTERED state和ECM-IDLE mode；

3） 已建立缺省EPS承载，在UE接收到的ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST中已得

到active缺省EPS承载的PDN地址。

测试步骤：

触发建立专用 EPS 承载，如下行灌包。

消息流：

UE - MME	消息
…	…
-->	SERVICE REQUEST（包含在RRC消息RRCConnectionRequest中）
<--	ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST（包含在RRC消息RRCConnectionReconfiguration 消息中）（Linked EPS bearer identity：缺省 EPS 承载上下文的 EPS bearer identity）
-->	ACTIVATE DEDICATE EPS BEARER CONTEXT ACCEPT

预期结果：

1) 专用 EPS 承载建立成功。

5.3.2 专用 EPS 承载修改

测试项目：会话管理

测试分项：专用 EPS 承载修改

测试目的：

验证终端可以修改专用 EPS 承载。

测试条件：

1) UE 驻留在 E-UTRA 小区 CELL1；
2) UE 已附着； UE 处于 BEARER CONTEXT ACTIVE STATE state 和 EMM-CONNECTED mode；
3) UE 已建立 DRB；
4) UE 已建立缺省 EPS 承载和专用 EPS 承载。

测试步骤：

系统触发修改 EPS 承载上下文（比如新的 UL TFT）。

消息流：

UE - MME	消息

…	…
<--	MODIFY EPS BEARER CONTEXT REQUEST
-->	MODIFY EPS BEARER CONTEXT ACCEPT

预期结果：

专用 EPS 承载修改成功。

5.3.3 专用 EPS 承载去激活

测试项目：会话管理

测试分项：专用 EPS 承载去激活

测试目的：

验证终端可以去激活专用 EPS 承载。

测试条件：

1) UE 驻留在 E-UTRA 小区 CELL1；
2) UE 已附着；UE 处于 BEARER CONTEXT ACTIVE STATE state 和 EMM-CONNECTED mode；
3) UE 已建立 DRB；
4) UE 已建立缺省 EPS 承载和专用 EPS 承载。

测试步骤：

系统触发删除一个专用 EPS 承载。

消息流：

UE - MME	消息
…	…
<--	DEACTIVATE EPS BEARER CONTEXT REQUEST（EPS bearer identity:非缺省EPS承载上文的某个EPS承载的ID）
-->	DEACTIVATE EPS BEARER CONTEXT ACCEPT

预期结果：

UE 删除指示的专用 EPS 承载。

5.3.4 Service Request

测试项目：会话管理

测试分项：Service Request

测试目的：验证当UE在ECM-IDLE态下发起Service Request，MME能够恢复承载。

预置条件：

1） EPS网络中各网元系统及操作维护台运行正常；

2） 用户在HSS中已签约EPS业务；

3） 用户已经附着在EPS网络，建立了缺省承载，且处于ECM-IDLE状态。

测试步骤：

1） UE在ECM-IDLE状态下有数据业务发起业务请求；

2） 在网络侧查询用户的信息。

预期结果：

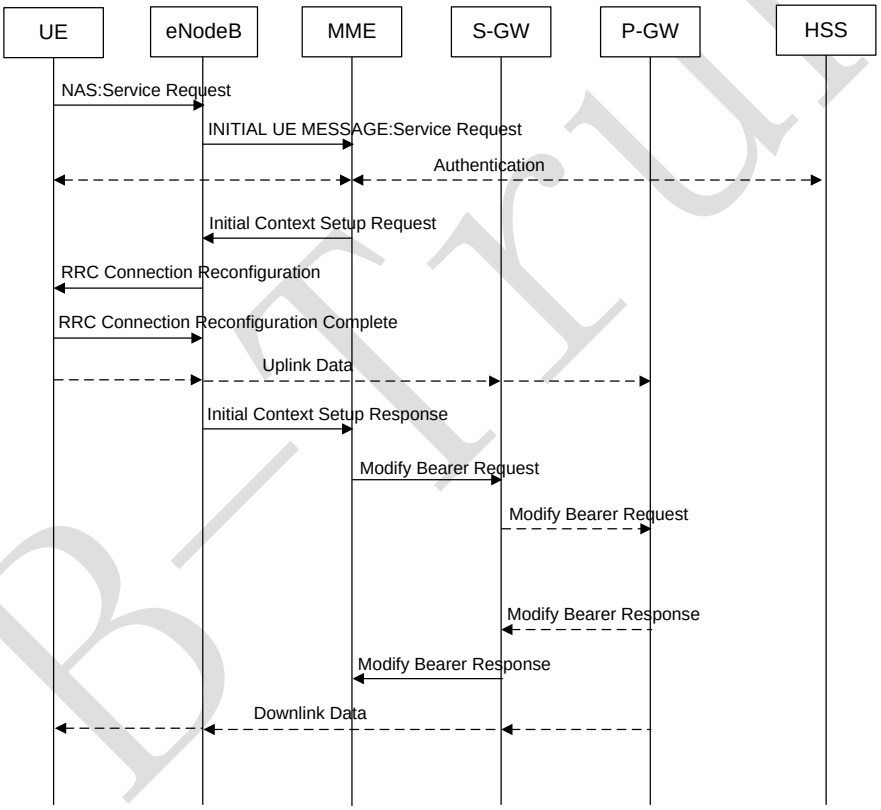
1） Service Request成功；

2） 用户ECM状态为ECM-CONNECTED，存在默认上下文，QoS，用户面IP和TEID等信息正确；

3） 数据业务恢复；

4） NAS消息流程正确。

测试说明：



1） UE由于有上行数据或者信令，则发起Service Request流程。UE通过RRC消息携带Service Request消息给eNodeB，消息中带有用户标识S-TMSI；

2） eNodeB向UE发送RRC Connection Reconfiguration，要求建立无线承载，UE响应RRC Connection Reconfiguration Complete，上行通道恢复。

6 安全功能接口测试

6.1 支持认证和密钥协商

测试项目：支持认证和密钥协商
测试目的：验证UE支持认证和密钥协商功能。
预置条件： 1） EPS网络中各网元系统及操作维护台运行正常； 2） 用户在HSS中已签约EPS业务； 3） MME中没有该用户的信息； 4） 在MME上打开鉴权加密开关，并配置用户附着过程中需要鉴权。
测试步骤： 1） 用户开机发起附着，向MME发送Attach Request（IMSI）消息； 2） MME向UE发起鉴权请求，发送authentication request，包含参数随机数RAND、认证令牌AUTN、KSI_{ASME}； 3） UE根据从MME接收到的参数，以和HSS同样的方式生成相关安全信息，UE根据AUTN认证网络，认证成功后UE向MME返回鉴权响应，携带RES； 4） MME将从UE接收到的RES与从HSS接收到的XRES进行比较，MME鉴权检查通过。 5） 从HSS上可以检查到用户的动态信息已经包含MME地址。
预期结果： 1） MME收到了正确的鉴权请求响应Authentication Information Answer消息，消息中的E-UTRAN鉴权向量正确； 2） MME向UE发起鉴权请求，发送authentication request，包含参数随机数RAND、认证令牌AUTN、KSI_{ASME}； 3） UE向MME返回鉴权响应，携带RES； 4） MME将从UE接收到的RES与从HSS获得的XRES进行比较，MME鉴权检查通过； 5） 从HSS上可以检查到用户的动态信息已经包含MME地址。 6） 消息跟踪能够跟踪到相应的消息，流程正确。

6.2 用户身份保护

测试项目：用户身份保护
测试目的：验证附着时的用户身份识别功能。
预置条件： 1） EPS网络中各网元系统及操作维护台运行正常； 2） 用户在HSS中已签约EPS业务； 3） 用户附着到该MME后关机分离，再删除MME中该用户的信息； 4） 在MME上配置用户附着过程中需要鉴权加密。

测试步骤： 1） UE开机发起GUTI附着，MME识别GUTI失败； 2） 对S1口进行抓包，检查MME是否向UE发起Identity Request消息，该消息的请求类型为IMSI； 3） 对S1口进行抓包，检查UE是否向MME回复Identity Response消息，该消息指示UE的IMSI； 4） 查看UE发送的attach request消息，查看UE身份标识是否为GUTI； 5） UE是否附着成功； 6） MME是否发起认证流程以及是否成功； 7） 默认承载是否建立成功； 8） MME通过工具，检查UE上下文、EMM上下文存在； 9） 消息跟踪是否能够跟踪到相应的消息，流程是否正确； 10）核心网发送attach accept消息后，UE回复attach complete消息，流程是否正常结束； 11）位置更新后，HSS上用户的动态信息是否已经包含MME地址。通过受理台查询用户信息；查看MME地址信息。通过受理台查询用户信息，查看MME地址信息； 12）在网络侧查询用户的信息。
预期结果： 1） UE成功附着到网络； 2） MME发起Identity Request流程，获取IMSI； 3） 默认承载建立成功； 4） 用户EMM状态为EMM-REGISTERED； 5） 消息跟踪能够跟踪到相应的消息，流程正确。

6.3 NAS 层消息安全

测试项目：UE支持NAS消息安全功能
测试目的：验证MME发起NAS Security Mode Command流程，UE完成NAS信令的加密和一致性保护的功能。
预置条件： 1） EPS网络中各网元系统及操作维护台运行正常； 2） 用户在HSS中已签约EPS业务； 3） 在MME上打开鉴权加密开关，并配置用户附着过程中需要鉴权。

测试步骤： 1） UE开机发起IMSI附着； 2） 对S1-MME接口进行抓包，确定NAS Security Mode Command是否携带选择的完整性和加密算法； 3） MME对NAS Security Mode Command进行完整性保护； 4） 对于NAS Security Mode Command消息，在UE查看该消息的安全头和MAC值； UE是否对NAS Security Mode Command消息进行完整性检查通过； 5） UE对NAS Security Mode Complete消息进行完整性保护和加密； 6） 对于NAS Security Mode Complete消息，在MME查看该消息的安全头和MAC值； MME是否对NAS Security Mode Complete消息进行完整性检查通过，解密处理是否正确； 7） 在网络侧查询用户的信息。
预期结果： 1） UE成功附着到网络； 2）MME对NAS Security Mode Command消息进行完整性保护； 3）UE对NAS Security Mode Command消息进行完整性检查通过； 4）UE使用算法对NAS Security Mode Complete消息进行完整性保护和加密处理； 5）MME对NAS Security Mode Complete消息进行解密和完整性检查通过； 6）默认承载建立成功； 7）用户EMM状态为EMM-REGISTERED； 8）消息跟踪能够跟踪到相应的消息，流程正确。

6.4 加密和完整性保护算法

6.4.1 ZUC 算法

测试项目：加密和完整性保护算法
测试分项：ZUC算法
测试目的：验证UE和MME支持ZUC算法。
预置条件： 1） EPS 网络中各网元系统及操作维护台运行正常； 2） UE，eNodeB，MME 支持 ZUC 算法功能； 3） 用户在 HSS 中已签约 EPS 业务； 4） MME 的操作维护台中 ZUC 算法优先级别最高； 5） MME 中没有该用户的信息； 6） 在 MME 上打开认证加密开关，并配置用户附着过程中需要认证。

测试步骤：

1) UE开机发起IMSI附着；
2) 查看UE发送的attach request消息，检查UE携带的UE Security Capabilities信元中是否包括EEA3和EIA3；
3) 查看MME配置算法列表中是否包含有EIA3和EEA3算法，MME是否在NAS Security Mode Command消息中包含EIA3/EEA3算法进行完整性保护。确定NAS Security Mode Command是否携带选择的EIA3/EEA3；
4) UE是否对NAS Security Mode Command消息进行完整性检查通过；
5) UE是否使用EIA3/EEA3算法对NAS Security Mode Complete消息进行完整性保护和加密；
6) MME是否使用EIA3/EEA3算法对NAS Security Mode Complete消息进行完整性检查和解密处理；
7) 默认承载是否建立成功；
8) 查看用户信息。

预期结果：

1) UE成功附着到网络；
2) UE发送的attach request消息，携带的UE网络能力中包含EEA3和EIA3；
3) MME在NAS Security Mode Command消息中选择 EEA3和EIA3；
4) MME对NAS Security Mode Command消息进行完整性保护；
5) UE对NAS Security Mode Command消息进行完整性检查通过；
6) UE使用EIA3/EEA3算法对NAS Security Mode Complete消息进行完整性保护和加密处理；
7) MME对NAS Security Mode Complete消息进行解密和完整性检查通过和解密；
8) 默认承载建立成功；
9) 用户EMM状态为EMM-REGISTERED；
10) 消息跟踪能够跟踪到相应的消息，流程正确。

6.4.2 SNOW 3G 算法

测试项目：加密和完整性保护算法

测试分项：SNOW 3G算法

测试目的：验证UE和MME支持SNOW 3G算法。

预置条件：

1）EPS 网络中各网元系统及操作维护台运行正常；
2）UE，eNodeB，MME 支持 SNOW 3G 算法功能；
3）用户在 HSS 中已签约 EPS 业务；
4）MME 的操作维护台中 SNOW 3G 算法优先级别；
5）MME 中没有该用户的信息；
6）在 MME 上打开认证加密开关，并配置用户附着过程中需要认证。

测试步骤： 1） UE开机发起IMSI附着，是否附着成功； 2） 查看UE发送的attach request消息，检查UE携带的UE Security Capabilities信元中是否包括EEA1和EIA1； 3） 查看MME配置算法列表中是否包含有EIA1和EEA1算法，检查MME是否在NAS Security Mode Command消息中包含EIA1/EEA1算法进行完整性保护。确定NAS Security Mode Command是否携带选择的EIA1/EEA1； 4） UE是否对NAS Security Mode Command消息进行完整性检查通过； 5） UE是否使用EIA1/EEA1算法对NAS Security Mode Complete消息进行完整性保护和加密； 6） MME是否使用EIA1/EEA1算法对NAS Security Mode Complete消息进行完整性检查和解密处理； 7） 默认承载是否建立成功； 8） 查看用户信息。
预期结果： 1） UE成功附着到网络； 2） UE发送的attach request消息，携带的UE网络能力中包含EEA1和EIA1； 3） MME在NAS Security Mode Command消息中选择 EEA1和EIA1； 4） MME对NAS Security Mode Command消息进行完整性； 5） UE对NAS Security Mode Command消息进行完整性检查通过； 6） UE使用EIA1/EEA1算法对NAS Security Mode Complete消息进行完整性保护和加密处理； 7） MME对NAS Security Mode Complete消息进行解密和完整性检查通过； 8） 默认承载建立成功； 9） 用户EMM状态为EMM-REGISTERED； 10） 消息跟踪能够跟踪到相应的消息，流程正确。

6.4.3 AES 算法

测试项目：UE和MME支持AES算法
测试分项：AES算法
测试目的：验证UE和MME支持AES算法。
预置条件： 1）EPS 网络中各网元系统及操作维护台运行正常； 2）UE，eNodeB，MME 支持 AES 算法功能； 3）用户在 HSS 中已签约 EPS 业务； 4）MME 的操作维护台中 AES 算法优先级别最高； 5）MME 中没有该用户的信息；

6）在 MME 上打开认证加密开关，并配置用户附着过程中需要认证。
测试步骤： 1） UE开机发起IMSI附着，是否附着成功； 2） 查看UE发送的attach request消息，检查UE携带的UE Security Capabilities信元中是否包括EEA2和EIA2； 3） 查看MME配置算法列表中是否包含有EIA2和EEA2算法。MME是否在NAS Security Mode Command消息中包含EIA2/EEA2算法进行完整性保护。确定NAS Security Mode Command是否携带选择的EIA2/EEA2; 4） UE是否对NAS Security Mode Command消息进行完整性检查通过； 5） UE使用EIA2/EEA2算法对NAS Security Mode Complete消息进行完整性保护和加密； 6） MME是否使用EIA2/EEA2算法对NAS Security Mode Complete消息进行完整性检查和解密处理； 7） 默认承载是否建立成功； 8） 查看用户信息。
预期结果： 1） UE成功附着到网络； 2） UE发送的attach request消息，携带的UE网络能力中包含EEA2和EIA2； 3） MME在NAS Security Mode Command消息中选择 EEA2和EIA2； 4） MME对NAS Security Mode Command消息进行完整性保护； 5） UE对NAS Security Mode Command消息进行完整性检查通过； 6） UE使用EIA2/EEA2算法对NAS Security Mode Complete消息进行完整性保护和加密处理； 7） MME对NAS Security Mode Complete消息进行解密和完整性检查通过和解密； 8） 默认承载建立成功； 9） 用户EMM状态为EMM-REGISTERED； 10） 消息跟踪能够跟踪到相应的消息，流程正确。