B-TrunC TR 00x-2015 V0.00

基于LTE技术的宽带集群通信(B-TrunC)系统（第一阶段）安全技术要求

Technical Requirements for LTE based Broadband Trunking Communication(B-TrunC) System (Phase 1)



2015年6月

声明：本文件由宽带集群（B-TrunC）产业联盟制定，未来联盟可继续编制完善。本文件版权完全属于宽带集群（B-TrunC）产业联盟。未经许可，不能复制本文件中的任何部分。版权限制适用于所有媒体的复制方式。.

版本修订记录

|  |  |  |
| --- | --- | --- |
| **版本** | **主要修订内容** | **日期** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

前 言

本标准是由宽带集群产业（B-TrunC）联盟制定的《基于LTE技术的宽带集群通信(B-TrunC)系统总体技术要求（第一阶段）》系列标准之一，该系列标准的结构和名称预计如下：

1. TR 001-2013 基于LTE技术的宽带集群通信(B-TrunC)系统（第一阶段）总体技术要求
2. TR 002-2014 基于LTE技术的宽带集群通信(B-TrunC)系统（第一阶段）端到端流程
3. TR 003-2014 基于LTE技术的宽带集群通信(B-TrunC)系统接口技术要求（第一阶段）空中接口
4. TM 001-2014 基于LTE技术的宽带集群通信(B-TrunC)系统接口测试方法（第一阶段） 空中接口
5. TR 004-2014 基于LTE技术的宽带集群通信(B-TrunC)系统接口技术要求（第一阶段）终端到集群核心网接口
6. TM 002-2014 基于LTE技术的宽带集群通信(B-TrunC)系统接口测试方法（第一阶段）终端到集群核心网接口
7. TR 005-2014 基于LTE技术的宽带集群通信(B-TrunC)系统接口技术要求（第一阶段）集群核心网到调度台接口
8. TM 003-2014 基于LTE技术的宽带集群通信(B-TrunC)系统接口测试方法（第一阶段）集群核心网到调度台接口
9. TR 006-2014 基于LTE技术的宽带集群通信(B-TrunC)系统（第一阶段）网络设备技术要求
10. TM 004-2014 基于LTE技术的宽带集群通信(B-TrunC)系统（第一阶段）网络设备测试方法
11. TR 007-2014 基于LTE技术的宽带集群通信(B-TrunC)系统（第一阶段）终端设备技术要求
12. TM 005-2014 基于LTE技术的宽带集群通信(B-TrunC)系统（第一阶段）终端设备测试方法
13. TM 006-2014 基于LTE技术的宽带集群通信(B-TrunC)系统（第一阶段）终端与网络互操作测试方法
14. TR 008-2014 基于LTE技术的宽带集群通信(B-TrunC)系统（第一阶段）调度台设备技术要求
15. TM 007-2014 基于LTE技术的宽带集群通信(B-TrunC)系统（第一阶段）调度台设备测试方法
16. SC 001-2015 基于LTE技术的宽带集群通信(B-TrunC)系统（第一阶段）标准澄清文件

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（B-TrunC）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、国家无线电监测中心、北京市政务网络管理中心、公安部第一研究所、鼎桥通信技术有限公司、普天信息技术有限公司、深圳市中兴高达技术有限公司、中兴通讯股份有限公司、华为技术有限公司、大唐电信科技产业集团、北京信威通信技术股份有限公司、重庆重邮信科通信技术有限公司

本标准主要起草人：龚达宁、黄标、方箭、朱颖、李延春、徐贵森、陈迎、杨小倩、蔡杰、毛磊、褚丽、徐晖、郑伟、唐春莺、杨美荟、宋得龙、李明春、郄卫军、李晓华、许玲、尹桂杰、林庆、艾明、王浩、段红光、李侠宇、徐霞艳、宋得龙、赵洪坤、王璐、王小平、杨宝国

目  次

[版本修订记录 I](#_Toc433622137)

[前 言 II](#_Toc433622138)

[1 范围 1](#_Toc433622139)

[2 规范性引用文件 1](#_Toc433622140)

[3 术语、定义和缩略语 1](#_Toc433622141)

[3.1 术语和定义 1](#_Toc433622142)

[3.2 缩略语 1](#_Toc433622143)

[4 指导原则和应用场景 2](#_Toc433622144)

[4.1 指导原则 2](#_Toc433622145)

[4.2 应用场景 2](#_Toc433622146)

[5 安全需求 2](#_Toc433622147)

[6 系统架构 2](#_Toc433622148)

[6.1 系统架构 2](#_Toc433622149)

[6.2 网络实体 2](#_Toc433622150)

[6.3 接口 3](#_Toc433622151)

[7 密钥管理要求 3](#_Toc433622152)

[7.1 密钥的分级和生成 3](#_Toc433622153)

[7.2 密钥的分发和更新 4](#_Toc433622154)

[8 加密算法 4](#_Toc433622155)

[9 故障弱化下的安全 5](#_Toc433622156)

基于LTE技术的宽带集群通信(B-TrunC)系统（第一阶段） 安全技术要求

1. 范围

本标准规定了基于LTE技术的宽带集群通信(B-TrunC)系统总体技术要求（第一阶段），包括指导原则、业务和应用场景、详细功能和性能需求、系统架构、接口要求、编号和寻址和编解码器要求等。

本标准适用于基于LTE技术的宽带集群通信(B-TrunC)系统（第一阶段）的终端、基站、集群核心网和调度台设备。

1. 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。

YD/T 2560-2013 TD-LTE数字蜂窝移动通信网Uu接口物理层技术要求（第一阶段）

YD/T 2571-2013 TD-LTE数字蜂窝移动通信网基站设备技术要求（第一阶段）

YD/T 2575-2013 TD-LTE数字蜂窝移动通信网 终端技术要求（第一阶段）

YD/T 2620.1-2013 演进的移动分组核心网络（EPC）总体技术要求第1部分：支持E-UTRAN接入

3GPP TS 36.113 演进的陆地无线接入基站和直放站电磁兼容性(Evolved Universal Terrestrial Radio Access (E-UTRA); Base Station (BS) and repeater ElectroMagnetic Compatibility (EMC)

1. 术语、定义和缩略语
   1. 术语和定义

下列术语和定义适用于本文件。

宽带集群 broadband trunking

基于宽带无线移动通信技术，支持宽带数据传输业务、语音和多媒体形式的集群指挥调度业务的宽带无线通信系统。

* 1. 缩略语

|  |  |  |
| --- | --- | --- |
| 下列缩略语适用于本文件。 |  |  |
| |  |  |  | | --- | --- | --- | | AMR | 自适应多速率编码 | Adaptive Multi-Rate | | APN | 接入点名 | Access Point Name | | BBU | 室内基带单元 | Building Base-band Unit | | B-TrunC | 宽带集群通信 | Broadband Trunking Communication | |

1. 指导原则和应用场景
   1. 指导原则
      1. xx

系统应具备高等级的安全性，保证宽带数据和集群业务的安全。

* 1. 应用场景
     1. xx

xx。

1. 安全需求

用户面和控制面均应支持一话一密。

【待定】是否需要业务鉴权？

1. 系统架构
   1. 系统架构

基于LTE技术的专网宽带集群系统由LTE宽带集群终端、LTE数据终端、LTE宽带集群基站、LTE宽带集群核心网和调度台组成，如所示。

图 1. 基于LTE的宽带集群系统架构

* 1. 网络实体
     1. LTE宽带集群终端

LTE宽带集群终端的安全功能应符合YD/T xxxx-2013的要求，并且还应支持以下集群安全功能

* Xxxx
* xxxxxx

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx。

* + 1. LTE宽带集群基站

LTE宽带集群基站的安全功能应符合YD/T xxxx-2013的要求，并且还应支持以下集群安全功能

xxxx：

* Xxxx
* xxxxxx

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx。

* + 1. LTE宽带集群核心网

LTE宽带集群基站的安全功能应符合YD/T xxxx-2013的要求，并且还应支持以下集群安全功能

xxxx：

* Xxxx
* xxxxxx

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx。

* + 1. 调度台

调度台应支持以下集群安全功能

xxxx：

* Xxxx
* xxxxxx

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx。

* 1. 接口

xx接口：xxx与xxx之间的接口。xxxxxx。

1. 密钥管理要求
   1. 密钥的分级和生成
      1. 集群密钥架构

|  |  |  |
| --- | --- | --- |
| 密钥 | 长度 | 功能 |
| 组根密钥 |  |  |
| …… |  |  |
|  |  |  |

在一次组呼通话中，组呼控制面和用户面的密钥，所有基站都相同。

组根密钥：在组产生时由网络生成。网络侧存储在eHSS，终端侧放在RAM中

随机数：在寻呼消息中携带，每次呼叫保持不变。

【待定】随机数的生成机制和长度：

生成网元： eHSS？ eNB？

生成方法：由集群key衍生？ 由其他参数衍生？

长度：需综合平衡寻呼信道容量和安全性

* 1. 密钥的分发和更新
     1. 概述

用户面和控制面均应支持一话一密。

* + 1. 组根密钥的分发

eHSS应能够将组根密钥安全传输到终端侧。

【待定】分发方案待定，目前的2种方案

* + - 1）密文传输：从HSS直接到终端，采用LTE原有的key（如Kasme）或者集群新定义的key（如UE的集群根密钥）对GK进行加密后传输给终端；
    - 2）明文传输：采用分段机制，即HSS-eMME，eMME-MS，明文传输，安全性由各接口的安全性负责。
    1. 组根密钥更新

组根密钥更新的机制与分发机制保持一致。 触发更新的场景包括：

* + - 事件触发：组信息（包括组成员增删和动态重组）变化时，使用组信息更新流程更新
    - 周期更新

组根密钥更新需要一段时间，密钥更新不应该影响已经进行中的呼叫。在密钥更新期间，存在着新旧两个密钥，所以需要采用秘钥版本号的机制。

* + - 在组信息更新中，版本号和密钥同时下发
    - 在寻呼消息中将版本号下发给终端，指示启用哪个版本的密钥
    - 版本号长度4比特
    - 需要补充两个异常流程（UE主动申请秘钥同步、UE没有旧秘钥）

1. 加密算法

网络和终端都应支持以下算法：

|  |  |
| --- | --- |
| 完整性保护 | 加密 |
| EIA0 | EEA0 |
| 128-EIA1 | 128-EEA1 |
| 128-EIA2 | 128-EEA2 |
| 128-EIA3 | 128-EEA3 |

【待定】：本次呼叫使用的算法，如何通知UE？

1. 故障弱化下的安全