B-TrunC TS 02.003 V1.0

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

Technical requirement for security of LTE based broadband trunking communication(B-TrunC) System (Phase 2)

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

2018年6月

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（B-TrunC）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（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、鼎桥通信技术有限公司、北京中兴高达通信技术有限公司、普天信息技术有限公司、北京信威通信技术股份有限公司、海能达通信股份有限公司、武汉虹信通信技术有限责任公司、大唐电信科技产业集团、中国电子科技集团第七研究所、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：陈迎、郑伟、李晓华、陈钢、蔡杰、吴迪、袁剑、李侠宇、叶亚娟、龚达宁、周志宏、郄卫军、赵春平、袁建设、毛磊、曾朝晖.....

目 次

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

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）的安全技术要求，包括安全要求和架构、组呼密钥分层和衍生、安全算法参数、关键流程。

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、基站、集群核心网和调度台设备。

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。

3GPP TS 33.401: "3GPP System Architecture Evolution: Security architecture"

YD/T 2910-2015 LTE/SAE安全技术要求

3 术语、定义和缩略语

3.1 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。

3.2 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
AN	接入网络	Access Network
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
EEA	核心网加密算法	EPS Encryption Algorithm
eHSS	增强的归属用户服务器	Enhanced Home Subscriber Server

GK	组密钥	Group Key
LTE	长期演进	Long Term Evolution
ME	移动设备	Mobile Equipment
eMME	增强的移动管理单元	Enhanced Mobility Management Entity
NAS	非接入层	Non-Access Stratum
RRC	无线资源控制	Radio Resource Control
SAE	系统架构演进	System Architecture Evolution
SN	服务网络	Serving Network
TCF	集群控制功能体	Trunking Control Function
UE	用户设备	User Equipment
USIM	全球用户识别卡	Universal Subscriber Identity Module

4 安全要求和架构

对于各种采用点到点传输的信令和业务，例如：数据业务、集群单呼业务和集群组呼业务中讲话方的上行传输，B-TrunC系统支持以下主要安全功能：

- 用户身份保密；
- 认证和密钥协商；
- RRC和NAS信令机密性保护；
- RRC和NAS信令完整性保护；
- 用户面数据安全；
- 网络域控制面保护；
- Backhaul链路用户面保护；
- S1接口的管理面保护。

上述安全功能的具体要求见YDT 2910-2015。

除了YDT 2910-2015的要求之外，B-TrunC系统增强的安全要求如下：

- 对于集群业务，支持下行点到多点传输的RRC信令空口加密和完整性保护功能，支持下行点到多点传输的用户面的空口加密功能，支持下行点到多点传输的NAS层信令加密和完整性保护功能；并且，下行点到多点传输的RRC信令和用户面支持“一话一密”；
- 对于终端的集群业务，在NAS信令中提供端到端加密信息的传输通道，具体端到端加密方案不在本文规定；
- 对于调度台，支持SIP Digest挑战鉴权机制。

B-TrunC系统的安全架构继承了公网LTE-SAE安全架构，增加了集群业务的安全功能。图1给出了LTE-SAE安全架构的总体情况。

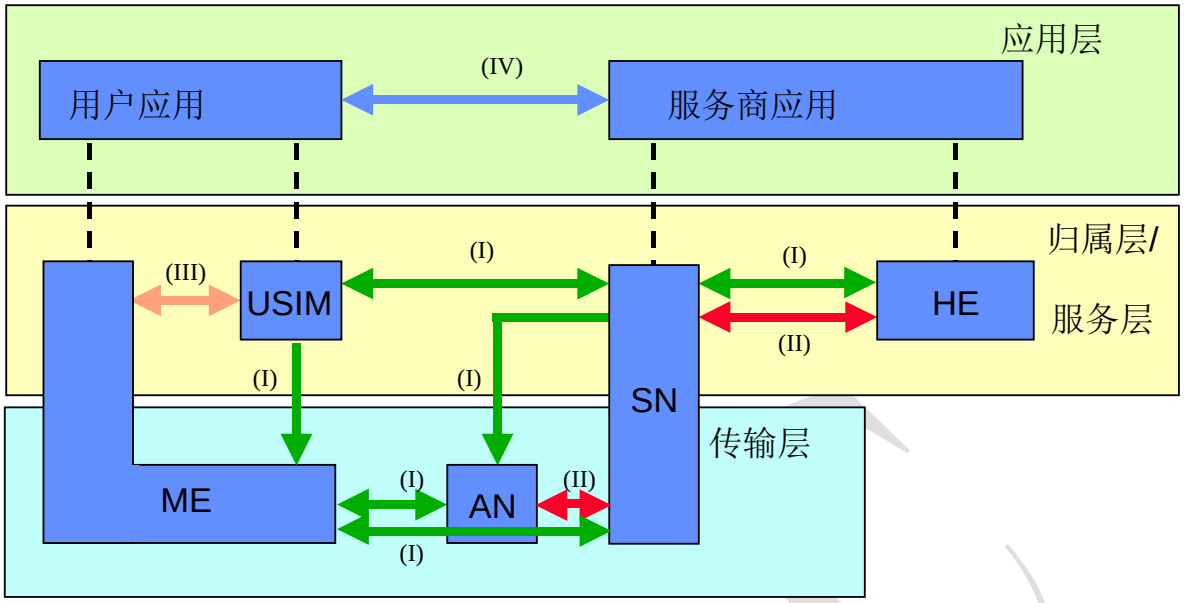


图1 安全架构总体情况

下面定义了五个类型的安全功能，每个类型的安全功能满足一定的威胁，完成一定的安全目标。

a) 网络接入安全(I):此安全功能保证用户安全接入业务,尤其是避免遭受来自无线网络上的攻击。相比 3GPP 协议，B-TrunC 在网络接入安全增加了对于集群业务的支持，包括：下行点到多点传输的信令面的空口加密和完整性保护功能;下行点到多点传输的用户面的空口加密功能。

b) 网络域安全(II):此安全功能保证节点间安全交换信令，避免遭受来自有线网络上的攻击。

c) 用户安全 (III)：此安全功能负责保证机卡接口安全。

d) 应用层安全(IV)：此安全功能保证用户和业务提供者之间能够安全交换信息。

e) 可视可配置安全(V):此安全功能保证无论安全功能是否实施，用户能够知道；业务的使用和配置都应取决于安全功能。

5 组呼下行空口安全密钥分层和衍生

5.1 组呼密钥分层

集群组呼密钥分层如图2所示。

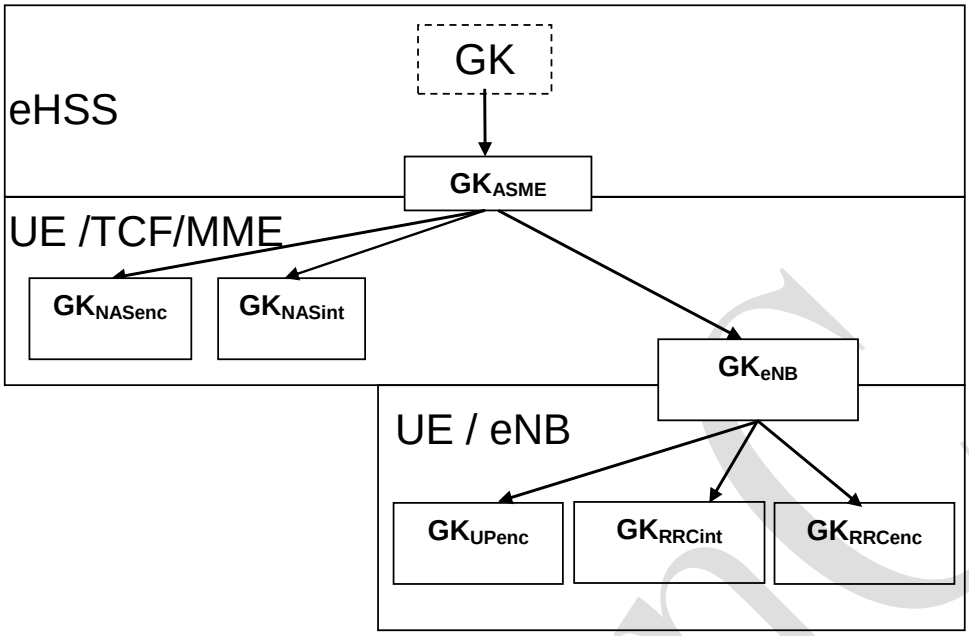


图2 集群密钥分层

注：GK是eHSS内部实现，从协议上不做规定。采用虚框表示。

各个密钥的描述如下：

1) 组根密钥GK_{ASME}：组呼业务安全分层体系中的根密钥。
2) 组NAS机密性保护密钥GK_{NASenc}：对UE和eMME之间的组呼业务相关NAS消息进行机密性保护使用的密钥。
3) 组NAS完整性保护密钥GK_{NASint}：对UE和eMME之间的组呼业务相关NAS消息进行完整性保护使用的密钥。
4) 组基站密钥GK_{eNB}：用于eNodeB派生组呼业务AS层密钥的根密钥。
5) 组RRC机密性保护密钥GK_{RRCenc}：对UE和eNodeB之间的组呼业务相关RRC消息进行机密性保护使用的密钥。
6) 组RRC完整性保护密钥GK_{RRCint}：对UE和eNodeB之间的组呼业务相关RRC消息进行完整性保护使用的密钥。
7) 组UP机密性保护密钥GK_{UPenc}：对UE和eNodeB之间的组呼业务相关用户面数据进行机密性保护使用的密钥。

5.2 组呼密钥衍生方案

组呼密钥衍生网络侧方案如图 3 所示。其中 GK_{NASenc} 和 GK_{NASint} 由核心网和 UE 分别计算生成，GK_{RRCenc}，GK_{RRCint} ，GK_{UPenc} 由 eNB 和 UE 分别计算生成。对于同一个组，所有组呼密钥、安全算法、版本号等安全参数在全网所有网元的取值相同。

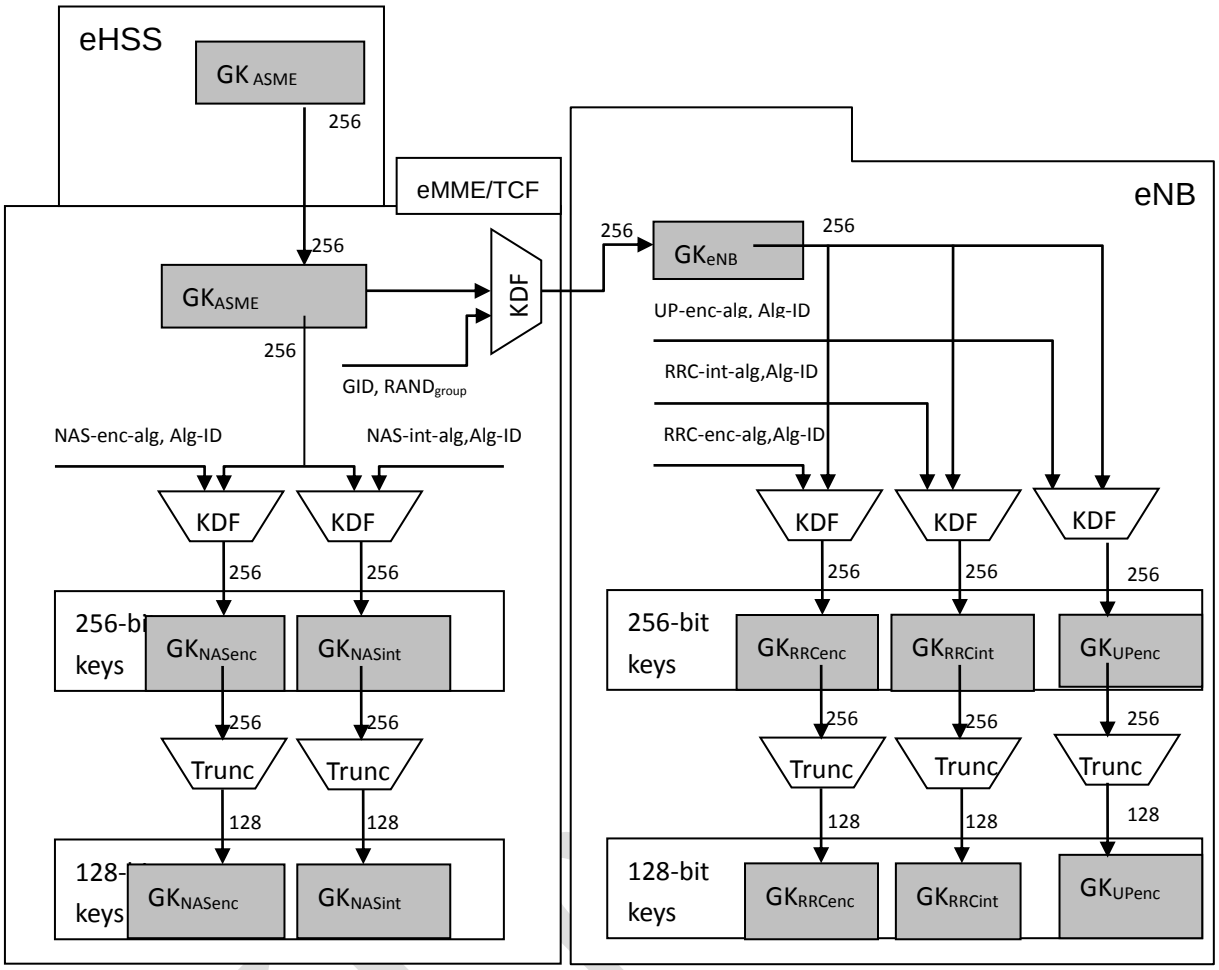


图3 组呼密钥衍生网络侧方案

组呼密钥衍生终端侧方案如图 4 所示。

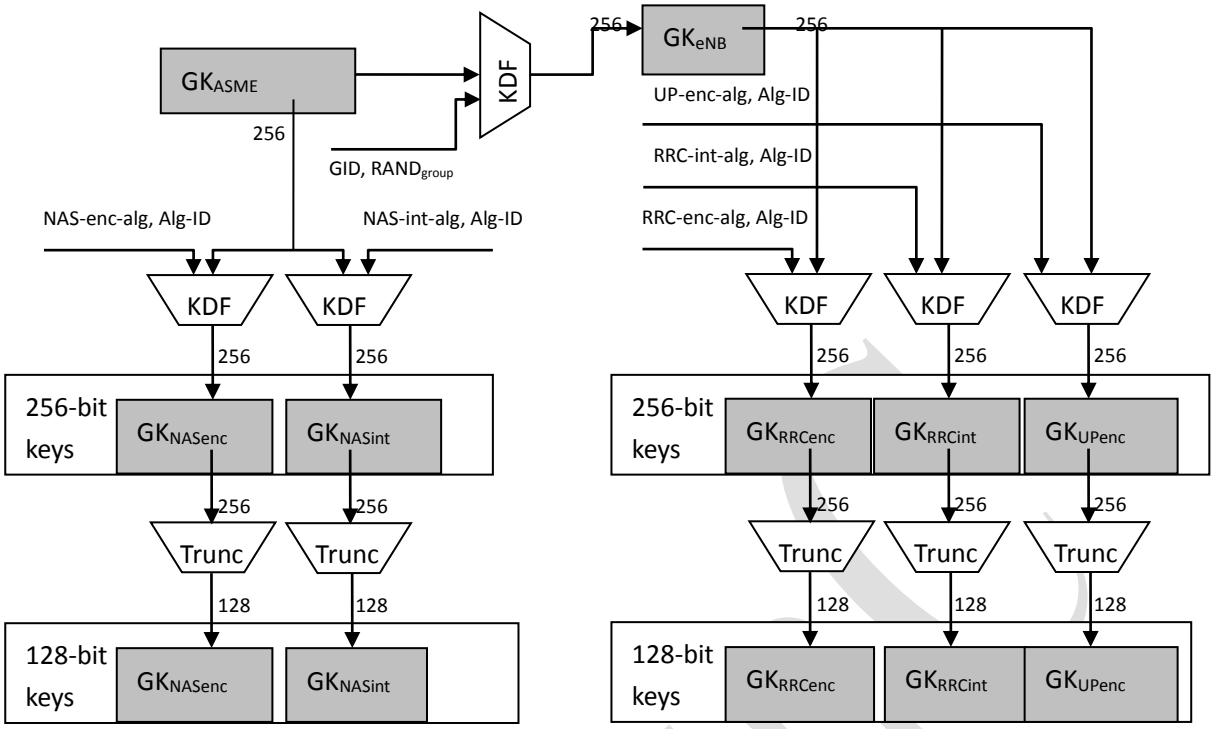


图4 组呼密钥衍生终端侧方案

图2和图3中各个密钥采用KDF（key derivation function）算法生成，参见3GPPTS 33.220，KDF算法中各个参数如表1所示。

表 1 组呼密钥衍生方案中的参数

	Length	FC	P0	L0	P1	L1
GK_{ASME}	256	-	-	-	-	-
GK_{NASenc}	128	0xF0	算法类型	0x00 0x01	算法 ID	0x00 0x01
GK_{NASint}	128	0xF0	算法类型	0x00 0x01	算法 ID	0x00 0x01
GK_{eNB}	256	0xF1	组号	0x00 0x06	随机数	0x00 0x08
GK_{RRCenc}	128	0xF0	算法类型	0x00 0x01	算法 ID	0x00 0x01
GK_{RRCint}	128	0xF0	算法类型	0x00 0x01	算法 ID	0x00 0x01
GK_{UPenc}	128	0xF0	算法类型	0x00 0x01	算法 ID	0x00 0x01

5.3 参数和取值

组呼密钥衍生方案中的算法类型取值如表2所示。

表 2 组呼密钥衍生方案中的算法类型取值

密钥	算法类型取值
NAS-enc-alg	0x01
NAS-int-alg	0x02
RRC-enc-alg	0x03
RRC-int-alg	0x04
UP-enc-alg	0x05
UP-int-alg	0x06

组呼密钥衍生方案中的加密算法ID取值如表3所示。

表 3 组呼密钥衍生方案中的加密算法 ID 取值

加密算法 ID	加密算法	描述
0000_2	EEA0	Null ciphering algorithm
0001_2	128-EEA1	SNOW 3G based algorithm
0010_2	128-EEA2	AES based algorithm
0011_2	128-EEA3	ZUC based algorithm

组呼密钥衍生方案中的完保算法ID取值如表4所示。

表 4 组呼密钥衍生方案中的完保算法 ID 取值

完保算法 ID	完保算法	描述
0000_2	EIA0	Null Integrity Protection algorithm
0001_2	128-EIA1	SNOW 3G based algorithm
0010_2	128-EIA2	AES based algorithm
0011_2	128-EIA3	ZUC based algorithm

组号：以BCD方式编码的Group ID，长度固定11位十进制数。

随机数：由组归属核心网生成的64bit的随机数，用于生成GK_{eNB}。

6 组呼下行空口安全算法参数

6.1 加密算法输入和输出

加密算法的输入参数是128位加密密钥“KEY”，一个32位的计数器“COUNT”，一个5位的承载标识“BEARER”，一个1位的传送方向标识“DIRECTION”，当为上行时方向标识“DIRECTION”为0，下行时为1，密钥流长度“LENGTH”。

图5说明了如何使用EEA加密算法来加密，可以通过异或明文与密钥流加密明文。同时明文可以通过使用相同的输入参数产生相同的密钥流与密文进行异或还原。

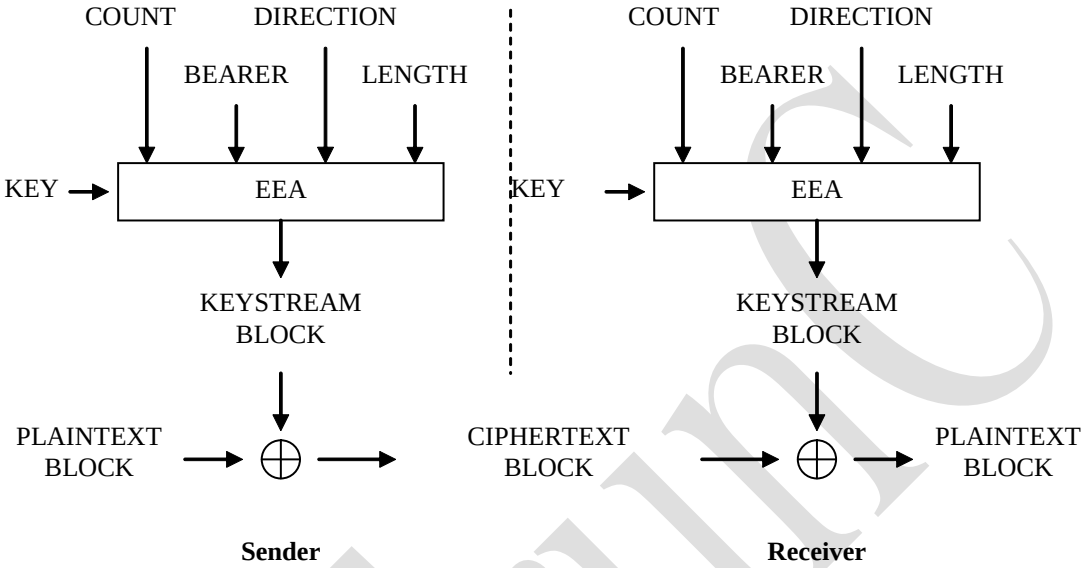


图5 数据的加密

基于输入参数算法可以产生输出密钥流块“KEYSTREAM”,密钥流块可以加密输入明文块“PLAINTEXT”并产生密文块“CIPHERTEXT”。

6.1.1 集群 NAS 信令

集群NAS信令加密算法的输入参数如下：

- KEY：加密密钥，128bit；取值为GK_{NASenc}；
- COUNT ：NAS计数，32bit；取值为0x00||NAS SQN，其中最左面 24bit是0的填充位，NAS SQN是一个8位的序号，携带在每个NAS消息中；
- BEARER：承载标识，5bit， 固定取值0x00；
- DIRECTION：方向，1bit，固定取值0x01；
- LENGTH：密钥流长度。对于EEA1和EEA3，采用流密码加密方式，LENGTH取值为Keystream block的bit数；对于EEA2，采用块密码加密方式，LENGTH取值为Keystream block的字节数。

6.1.2 集群 RRC 信令

集群RRC信令加密算法的输入参数如下：

- KEY：加密密钥，128bit；取值为GK_{RRCenc}；
- COUNT ：PDCP计数，32bit；取值为0x00||PDCP SN，其中最左27bit是0的填充位，PDCP SN是PDCP报文中序号，TSRB的PDCP SN是5bit；

- BEARER：承载标识，5bit， 固定取值0x01；
- DIRECTION：方向，1bit，固定取值0x01；
- LENGTH：密钥流长度。对于EEA1和EEA3，采用流密码加密方式，LENGTH取值为Keystream block的bit数；对于EEA2，采用块密码加密方式，LENGTH取值为Keystream block的字节数。

6.1.3 集群组数据

集群组数据加密算法的输入参数如下：

- KEY：加密密钥，128bit；取值为GK_{UPenc}；
- COUNT ：PDCP计数，32bit；取值为0x00||PDCP SN，其中最左25bit或20bit是0的填充位，PDCP SN是PDCP报文中序号，TDRB的PDCP SN可能是7bit或12bit；
- BEARER：承载标识，5bit， 取值为TDRB ID - 1；
- DIRECTION：方向，1bit，固定取值0x01；
- LENGTH：密钥流长度。对于EEA1和EEA3，采用流密码加密方式，LENGTH取值为Keystream block的bit数；对于EIA2，采用块密码加密方式，LENGTH取值为Keystream block的字节数。

6.2 完整性保护算法输入和输出

完整性算法的输入参数是一个128位的完整性密钥“KEY”，一个32位的计数器“COUNT”，一个5位的承载标识“BEARER”，1个1位的传输方向标识“DIRECTION”，上行时方向位为0，下行时方向位为1。消息体即“MESSAGE”，“MESSAGE”的长度为“LENGTH”。

图6说明了如何用完整性算法EIA来完成消息的完整性认证。

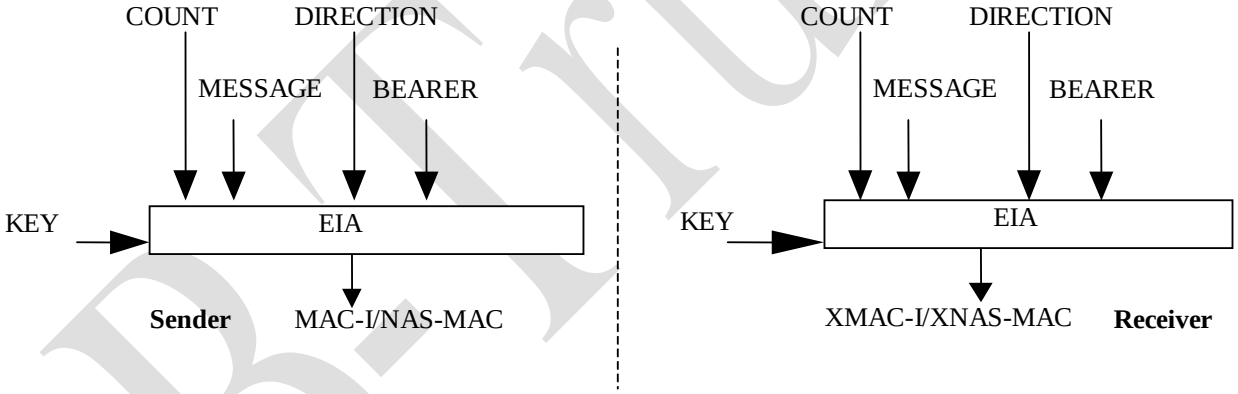


图6 数据的完整性保护

发送方基于输入参数通过完整性算法EIA计算出一个32位消息认证码(MAC-I/NAS-MAC)。发送时消息认证码插入到消息体后发送。对于完整性保护算法不是EIA0的，接收者采用与发送者相同的方法根据收到的消息计算出期望的认证码(XMAC-I/XNAS-MAC)，与收到的消息认证码(MAC-I/NAS-MAC)进行比较校验消息的数据完整性。

6.2.1 集群 NAS 信令

集群NAS信令完整性保护算法的输入参数如下：

- KEY：加密密钥，128bit；取值为GK_{NASint}；
- COUNT ：NAS计数，32bit；取值为0x00||NAS SQN，其中最左面 24bit是0的填充位，NAS SQN是一个8位的序号，携带在每个NAS消息中；

- BEARER：承载标识，5bit，固定取值0x00；
- DIRECTION：方向，1bit，固定取值0x01；
- LENGTH：MESSAGE的长度。对于EIA1和EIA3，采用流密码加密方式，LENGTH取值为MESSAGE的bit数；对于EIA2，采用块密码加密方式，LENGTH取值为MESSAGE的字节数。

6.2.2 集群 RRC 信令

集群RRC信令完整性保护算法的输入参数如下：

- KEY：加密密钥，128bit；取值为GK_{RRCint}；
- COUNT ：PDCP计数，32bit；0x00||PDCP SN，其中最左27bit是0的填充位，PDCP SN是PDCP报文中序号，TSRB的PDCP SN是5bit；
- BEARER：承载标识，5bit， 固定取值0x01；
- DIRECTION：方向，1bit，固定取值0x01；
- LENGTH：MESSAGE的长度。对于EIA1和EIA3，采用流密码加密方式，LENGTH取值为MESSAGE的bit数；对于EIA2，采用块密码加密方式，LENGTH取值为MESSAGE的字节数。

7 组呼下行空口安全关键流程

7.1 终端安全能力上报

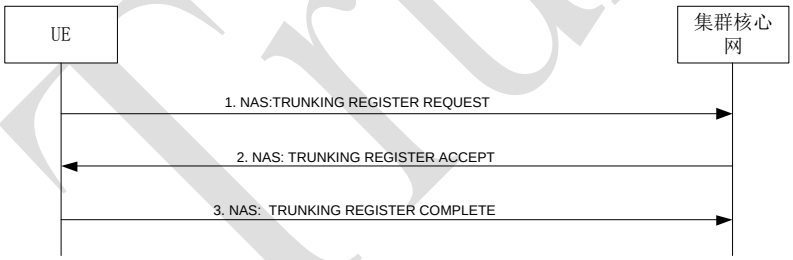


图7 终端上报集群安全能力

流程说明如下：

1） 步骤1：UE向集群核心网发送TRUNKING REGISTER REQUEST消息，消息中携带Trunking Register Type 、UE Trunking Capability、Stun Status、Audio Codec Capability和Video Codec Capability等信息；UE在故障弱化模式下执行集群注册时，还需携带Subscriber BCD Number，可选携带Group ID List。支持点到多点安全的终端必带UE Trunking Security Capability；

2） 步骤2：网络侧收到UE的TRUNKING REGISTER REQUEST消息后查找终端的集群签约信息，如果网络侧处理正常向UE回复TRUNKING REGISTER ACCEPT消息，消息内容包括：如果网络要求UE进行周期性注册，则应携带Trunking update period；对UE初始注册过程，网络应携带Subscriber BCD Number；对UE初始注册过程，如果网络配置了用户的别称时，应携带User name；如果网络配置了用户的紧急呼叫号码时，在UE初始注册过程，以及紧急呼叫号码改变等情况下，应携带Emergency num；在初始注册时，以及网络集群能力改变后，应携带Network trunking capability。网络侧收到UE Trunking Security Capability后存储该用户的安全能力信息；

3） 步骤3：UE接收到TRUNKING REGISTER ACCEPT消息，向网络侧回复TRUNKING REGISTER COMPLETE消息，通知集群注册完成。

7.2 组根密钥更新

组根密钥更新的场景包括：

- 终端开机注册后的组信息更新过程；
- 组信息变化导致的组信息更新过程；
- 组信息周期性更新过程。

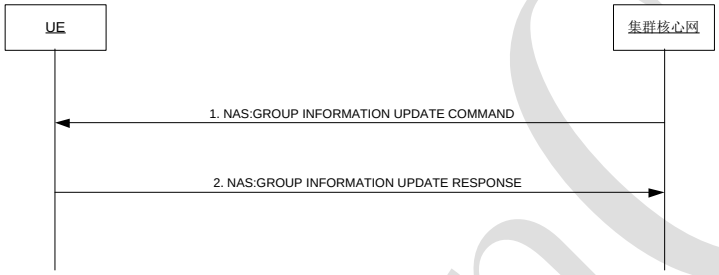


图8 组根密钥更新

流程说明如下：

1） 步骤1：集群核心网通过NAS下行直传消息将组信息更新命令给终端。群组安全参数包括：当前使用的组根密钥GKasme、密钥版本号GKversion、和NAS安全算法TSM Security Algorithm；以及更新后的组根密钥GKasme、密钥版本号GKversion、和NAS安全算法TSM Security Algorithm（算法选择取决于实现）；

2） 步骤2：终端通过NAS上行直传消息将组信息更新响应消息发送给集群核心网。

注：密钥版本号GKversion：在组根密钥更新过程中用到的组根密钥版本号GKversion用于标示组根密钥GK_{ASME}的版本。

7.3 单核心网组呼业务安全

在组呼业务中,需要支持下行点到多点传输的信令面的空口加密和完整性保护功能，以及下行点到多点传输的用户面的空口加密功能。

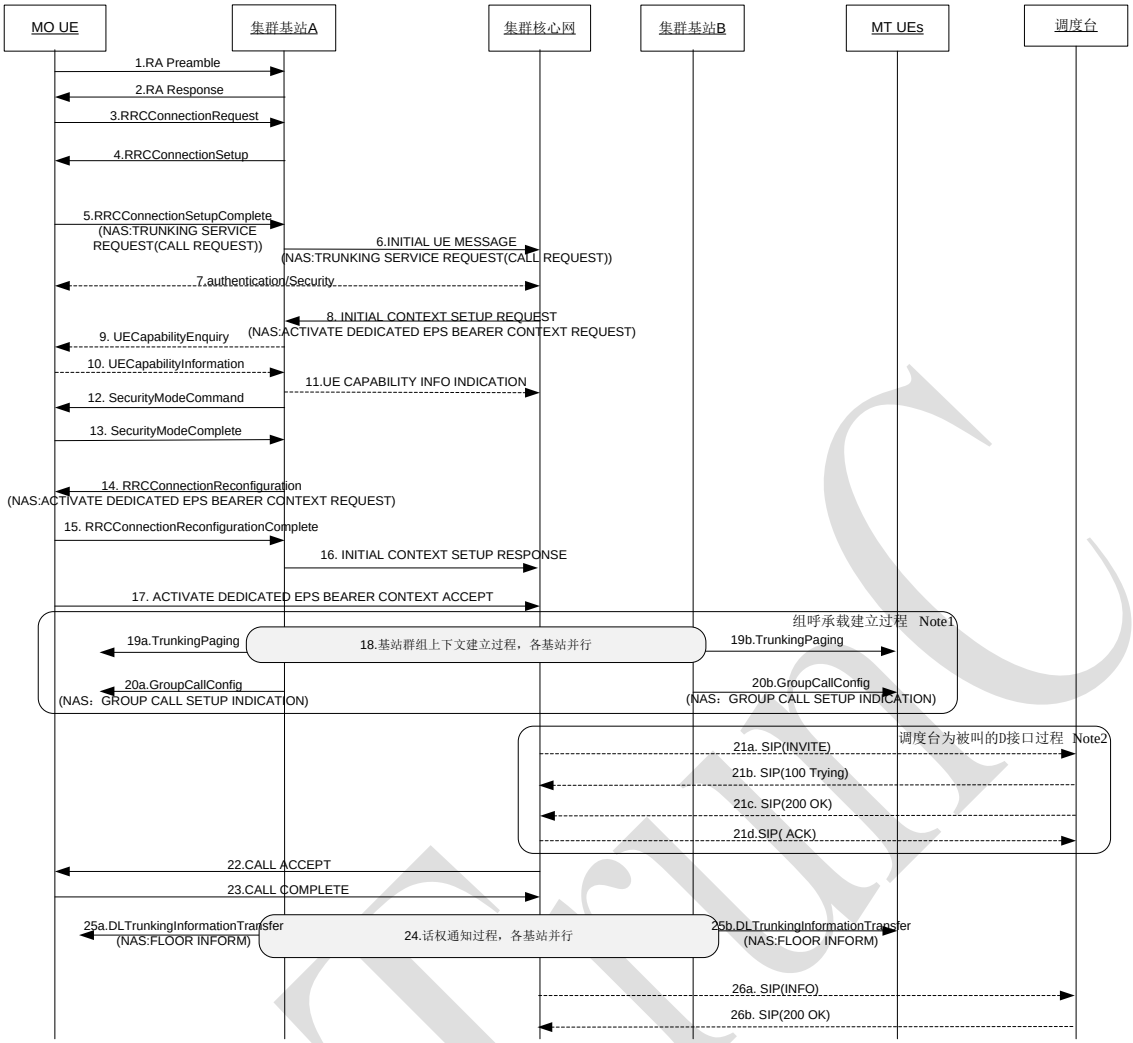


图9 单核心网下用户发起的组呼建立流程

流程说明如下：

1） 步骤1～5：发起组呼的IDLE UE执行RRC连接建立流程。UE在连接建立完成消息中携带NAS消息TRUNKING SERVICE REQUEST，其中除了安全信息外，携带呼叫请求CALL REQUEST（消息中携带呼叫类型、呼叫属性、被叫号码、媒体信息等），用以申请建立一个集群组呼业务；

2） 步骤6：基站通过INITIAL UE MESSAGE向核心网发送初始UE消息，携带TRUNKING SERVICE REQUEST；

3） 步骤7：核心网和UE之间，通过安全鉴权流程来确定用户的合法性；

4） 步骤8：核心网发起触发INITIAL CONTEXT SETUP REQUEST给基站，其中，携带有核心网给UE建立的专用承载(Qos, TFT)，供发起者上行传输使用；

5） 如果消息8中配置了UE Radio Capability IE，则基站不会发送消息9 UECapabilityEnquiry消息给UE，即没有第9-11步过程；否则会触发流程9～11，UE上报无线能力信息后，基站通过UE CAPABILITY INFO INDICATION上报UE的无线能力信息；

6） 步骤12～13：eNB执行空口安全模式操作，激活对应空口的安全机制；

7） 步骤14:eNB通过RRC重配，恢复UE的空口承载。同时，携带专用承载建立请求，建立为发起者初始话权使用的承载；

8） 步骤15～16：UE反馈RRC层的配置结果给基站。基站通过INITIAL CONTEXT SETUP RESPONSE反馈给核心网；

9） 步骤17：UE通过上行直传，向核心网反馈NAS层专用承载建立的结果；

10） 步骤18：核心网向相关基站发起群组下行承载的建立。各基站可以并行此过程，也可以和发起者相关流程并行（步骤8～17），以及与对调度台的通知并行（步骤21）。组上下建立请求消息中可选携带安全参数包括：组基站密钥GKeNB、随机数 RandGroup、AS层安全算法信息 Group As Security Information（算法选择取决于实现）、组根密钥版本号GKversion；

11） 步骤19相关基站发送Trunking Paging消息，其中携带trunkingGroupID,groupPriority，G-RNTI，可选携带随机数 RandGroup、AS层安全算法GroupAsSecurityInformation、组根密钥版本号GKversion；

12） 步骤20，基站在TCCH信道上发送GroupCallConfig，给出群组TTCH的接入层配置参数，其中还包含NAS消息GROUP CALL SETUP INDICATION（携带Call ID、 CallType、MediaType、ServiceType、CallAttribute、CalledNumber和MediaDescription）。各监听UE收到步骤19/20的空口消息后，可以进行群组业务的接收；

Note 1：步骤18-20为组呼承载建立过程，该过程可以在步骤6后开始执行，取决于核心网的实现。

13） 步骤21：如果调度台为被叫，则核心网在收到主叫的Call Request消息之后（，通过D接口发起SIP的Invite 流程，通知调度台接入该组呼。具体包括以下过程：

14） 步骤21a：集群核心网向调度台发送SIP（INVITE）消息，通知调度台进行组呼建立流程，携带业务标识pttcall，呼叫类型calltype，呼叫优先级属性标识PrioAttribute、单双工指示duplex。

15） 步骤21b：被叫调度台向集群核心网回复SIP（100 Trying）消息；

16） 步骤21c：被叫调度台接受当前呼叫，向集群核心网发送SIP（200 OK）消息，确认被叫调度台接听当前呼叫；携带pttcall；

17） 步骤21d：集群核心网向被叫调度台发送SIP（ACK）消息，确认当前组呼建立成功；

Note 2：步骤21为呼叫调度台的过程，该过程可以在步骤6后开始执行，取决于核心网的实现。

18） 步骤22：在至少一个基站下行承载成功建立后，核心网通过CALL ACCEPT通知发起者，相应资源已准备完毕，可以进行上行传输，消息携带呼叫ID、呼叫类型、呼叫属性、呼叫优先级、话权信息、媒体信息等；

19） 步骤23：UE通过CALL COMPLETE通知核心网，CALL ACCEPT已被UE获得；

20） 步骤24，25：核心网通过FLOOR INFORM流程，向监听UE通知群组的当前话权状态；

21） 步骤26a/26b：如果调度台为组呼被叫，核心网向调度台发送SIP（INFO）消息，将话权信息通知到DC，携带话权通知类型标识pttinfo，话权忙闲指示AlertType，如果当前话权占用，携带话权用户的号码；调度台向集群核心网发送SIP（200(OK)）消息，响应集群核心网的话权通知。

说明：上述流程图为IDLE态UE触发的组呼建立过程。如果组呼发起者为连接态UE，则通过NAS直传消息携带CALL REQUEST。

7.4 多核心网组呼业务安全

场景约束：集群核心网A是MO UE的归属核心网和服务核心网，也是组归属核心网；集群核心网B是组内部分成员MT UEs驻留的核心网。

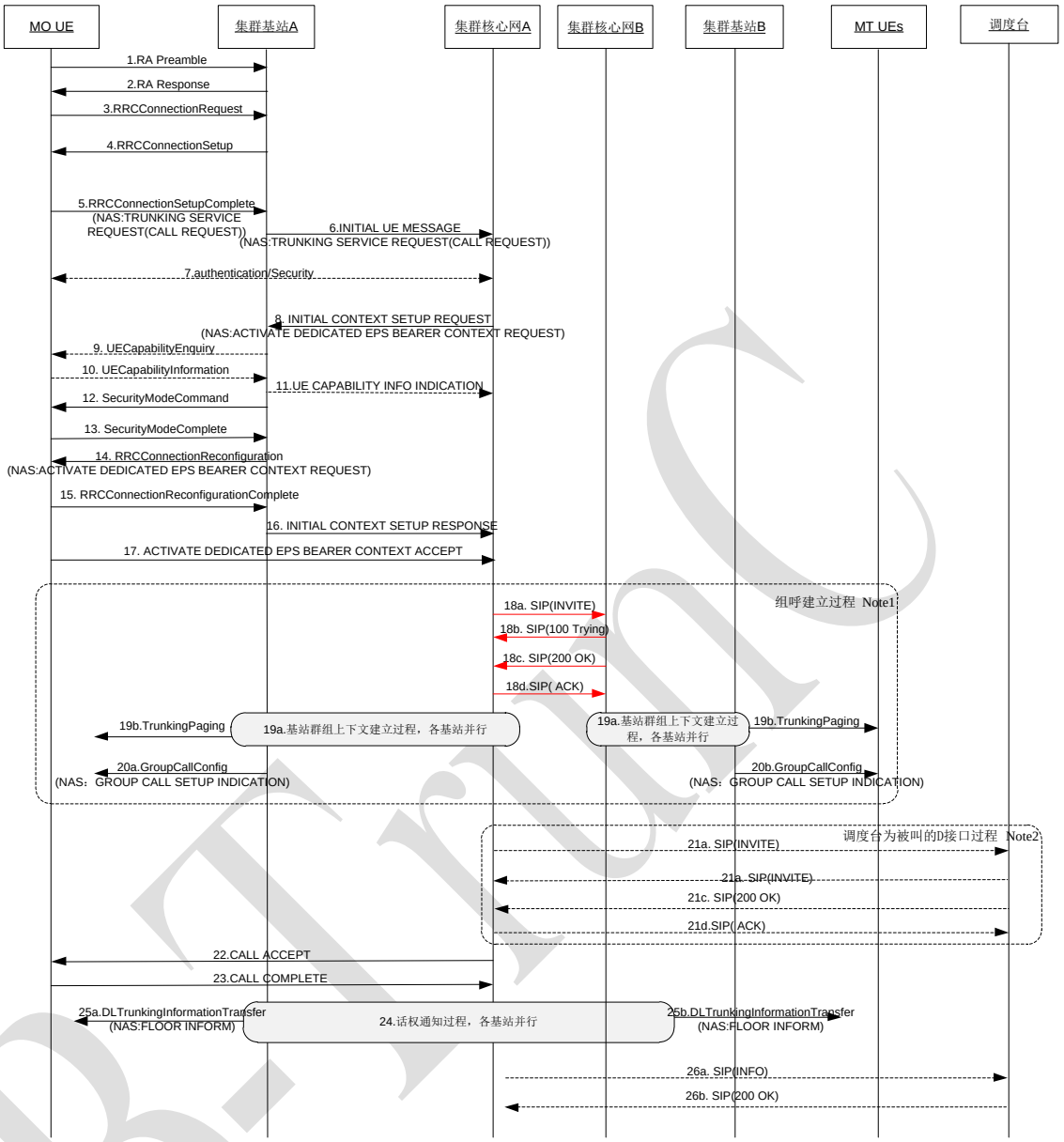


图10　多核心网下用户发起的组呼建立流程

流程说明如下：

1） 步骤1～5：发起组呼的IDLE UE执行RRC连接建立流程。UE在连接建立完成消息中携带NAS消息TRUNKING SERVICE REQUEST，其中除了安全信息外，携带呼叫请求CALL REQUEST（消息中携带呼叫类型、呼叫属性、被叫号码、媒体信息等），用以申请建立一个集群组呼业务；

2） 步骤6：基站通过INITIAL UE MESSAGE向集群核心网A发送初始UE消息，携带TRUNKING SERVICE REQUEST；

3） 步骤7：集群核心网A和UE之间，通过安全鉴权流程来确定用户的合法性；

4） 步骤8：集群核心网A发起触发INITIAL CONTEXT SETUP REQUEST给基站，其中，携带有集群核心网A给UE建立的专用承载(Qos, TFT)，供发起者上行传输使用；

5） 如果消息8中配置了UE Radio Capability IE，则基站不会发送消息9 UECapabilityEnquiry消息给UE，即没有第9-11步过程；否则会触发流程9～11，UE上报无线能力信息后，基站通过UE CAPABILITY INFO INDICATION上报UE的无线能力信息；

6） 步骤12～13：eNB执行空口安全模式操作，激活对应空口的安全机制；

7） 步骤14:eNB通过RRC重配，恢复UE的空口承载。同时，携带专用承载建立请求，建立为发起者初始话权使用的承载；

8） 步骤15～16：UE反馈RRC层的配置结果给基站。基站通过INITIAL CONTEXT SETUP RESPONSE反馈给集群核心网A；

9） 步骤17：UE通过上行直传，向集群核心网A反馈NAS层专用承载建立的结果；

10） 步骤18：集群核心网A通知集群核心网B建立组呼呼叫，发送INVITE消息中的ptt-Extension扩展头携带业务标识pttcall、呼叫类型calltype，呼叫优先级属性标识PrioAttribute、单双工指示duplex、呼叫优先级priority，在线通话识别码OnlinecallID，决策的媒体参数，以及组安全信息：组基站密钥GKeNB、随机数 RandGroup、AS层安全算法信息Group As Security Information、组根密钥版本号GKversion。；

11） 步骤19：集群核心网A与集群核心网B向相关基站发起群组下行承载的建立。各基站可以并行此过程，也可以和发起者相关流程并行（步骤8～17），以及与对调度台的通知并行（步骤21）。组上下建立请求消息中可选携带安全参数包括：组基站密钥GKeNB、随机数 RandGroup、AS层安全算法信息Group As Security Information、组根密钥版本号GKversion。。相关基站建立组上下文之后，发送Trunking Paging消息，其中携带trunkingGroupID, groupPriority，G-RNTI，可选携带随机数RandGroup、AS层安全算法GroupAsSecurityInformation、组根密钥版本号GKversion；

12） 步骤20，基站在TCCH信道上发送GroupCallConfig，给出群组TTCH的接入层配置参数，其中还包含NAS消息GROUP CALL SETUP INDICATION（携带Call ID、 CallType、MediaType、ServiceType、CallAttribute、CalledNumber和MediaDescription）。如果启用组安全机制，该消息需要进行加密与完保。

各监听UE收到步骤19/20的空口消息后，可以进行群组业务的接收。

Note 1：步骤18-20为组呼承载建立过程，该过程可以在步骤6后开始执行，取决于集群核心网A的实现。

13） 步骤21：如果调度台为被叫，则集群核心网A在收到主叫的Call Request消息之后（，通过D接口发起SIP的Invite 流程，通知调度台接入该组呼。具体包括以下过程：

14） 步骤21a：集群集群核心网A向调度台发送SIP（INVITE）消息，通知调度台进行组呼建立流程，携带业务标识pttcall,呼叫类型calltype,呼叫优先级属性标识PrioAttribute、单双工指示duplex；

15） 步骤21b：被叫调度台向集群集群核心网A回复SIP（100 Trying）消息；

16） 步骤21c：被叫调度台接受当前呼叫，向集群集群核心网A发送SIP（200 OK）消息，确认被叫调度台接听当前呼叫；携带pttcall；

17） 步骤21d：集群集群核心网A向被叫调度台发送SIP（ACK）消息，确认当前组呼建立成功；

Note 2：步骤21为呼叫调度台的过程，该过程可以在步骤6后开始执行，取决于集群核心网A的实现。

18） 步骤22：在至少一个基站下行承载成功建立后，集群核心网A通过CALL ACCEPT通知发起者，相应资源已准备完毕，可以进行上行传输，消息携带呼叫ID、呼叫类型、呼叫属性、呼叫优先级、话权信息、媒体信息等；

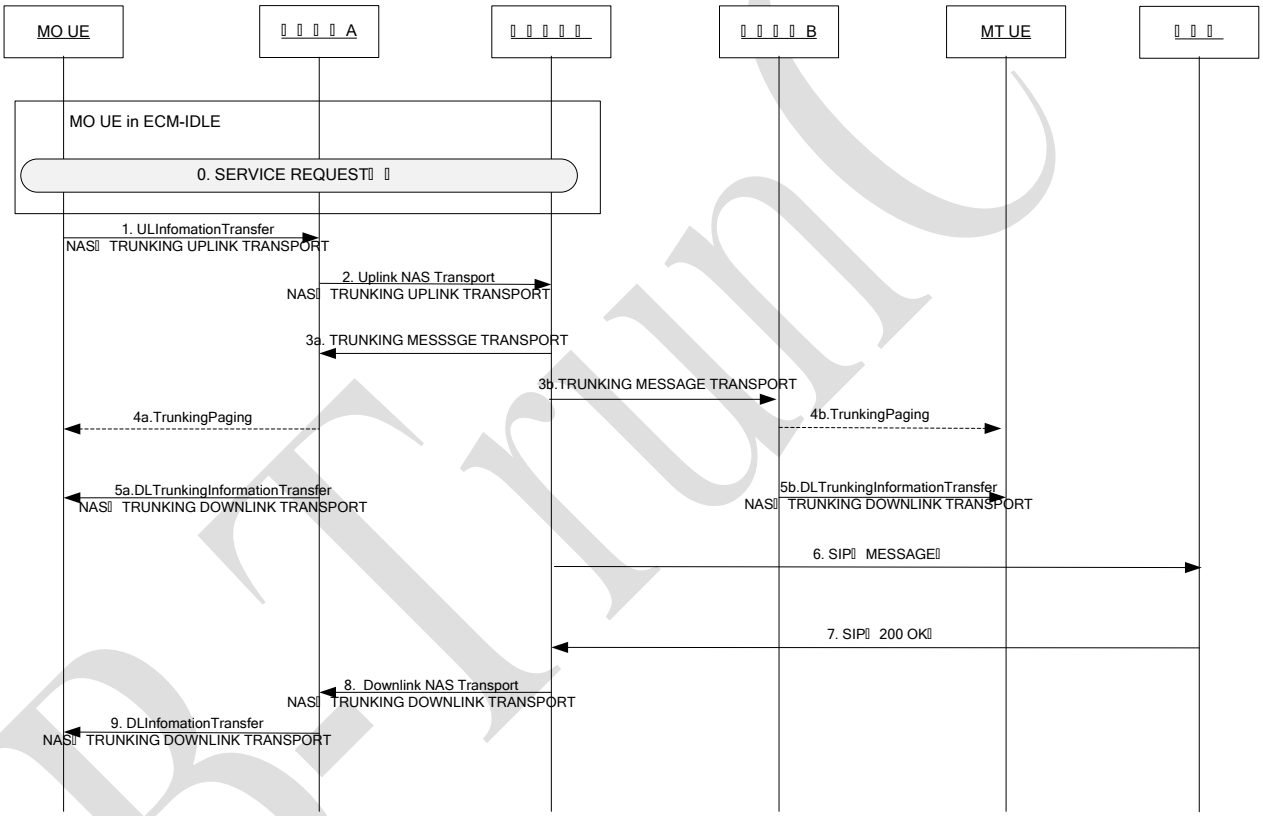
19） 步骤23：UE通过CALL COMPLETE通知集群核心网A，CALL ACCEPT已被UE获得；

20） 步骤24-25：集群核心网A通过FLOOR INFORM流程，向监听UE通知群组的当前话权状态；

21） 步骤26a/26b：如果调度台为组呼被叫，集群核心网A向调度台发送SIP（INFO）消息，将话权信息通知到DC，携带话权通知类型标识pttinfo，话权忙闲指示AlertType，如果当前话权占用，携带话权用户的号码；调度台向集群集群核心网A发送SIP（200(OK)）消息，响应集群集群核心网A的话权通知。

说明：上述流程图为IDLE态UE触发的组呼建立过程。如果组呼发起者为连接态UE，则通过NAS直传消息携带CALL REQUEST。

7.5 单核心网加密组播短数据流程



流程说明如下：

处于ECM-IDLE态的UE，执行步骤0，通过SERVICE REQUEST过程和网络恢复连接。

1） 步骤1-2：UE向集群核心网发送TRUNKING UPLINK TRANSPORT消息，消息的Message Container Type指示为“短数据和状态数据”，Message Container中携带SDS消息 SHORT-MSG，内携带Calling party，Called party，Mode=01H（PTM）；

2） 步骤3：核心网通过TRUNKING MESSAGE TRANSPORT 消息向基站发起组播短数据发送过程，携带NAS消息TRUNKING DOWNLINK TRANSPORT，NAS消息的Message Container Type指示为“短数据和状态数据”，Message Container中携带SDS消息 SHORT-MSG，内携带Calling party，Called party，Mode=01H（PTM）；此过程可以各基站并行，也可以与步骤6对调度台的通知并行；

如果群组已建立，TRUNKING MESSAGE TRANSPORT 消息还携带为该群组分配的MME GROUP S1AP ID和eNB GROUP S1AP ID、并携带PLMN Identity、组号GroupIdentity、业务优先级Call Priority，消息中不携带组安全信息，基站使用已建立的群组安全上下文。

如果群组尚未建立，TRUNKING MESSAGE TRANSPORT 消息还携带PLMN Identity、GroupIdentity、业务优先级Call Priority、业务区域Message Service Area、组安全信息Group Call Security Information，其中Message Service Area指定组播短数据的发送范围，Group Call Security Information包含组基站密钥Group Call Security Key、随机数RAND Group、接入层安全算法Security algorithms、密钥版本号GKversion。

3） 步骤4：基站通过TPCCH向群组UE发送TrunkingPaging消息，其中groupShortMsg-Indication取值为true，并指示该组使用的加密算法cipheringAlgorithm和完保算法integrityProtAlgorithm、随机数randGroup、组密钥版本号groupSecurityVer。如果此时该群组正在进行呼叫，则本步骤可以省略；

注：如果群组未建立，则基站收到TRUNKING MESSAGE TRANSPORT消息后，应根据所携带业务区域Message Service Area临时建立TCCH信道发送DLTrunkingInfomationTransfer消息，当短消息发送完毕后删除TCCH信道，终端执行同样的操作。

4） 步骤5：基站向群组UE发送使用根据组基站密钥衍生的组RRC相关密钥进行加密和完保后的DLTrunkingInfomationTransfer消息，其中携带NAS消息TRUNKING DOWNLINK TRANSPORT，NAS消息的Message Container Type指示为“短数据和状态数据”，Message Container中携带SDS消息SHORT-MSG，内携带Calling party，Called party，Mode=01H（PTM）；

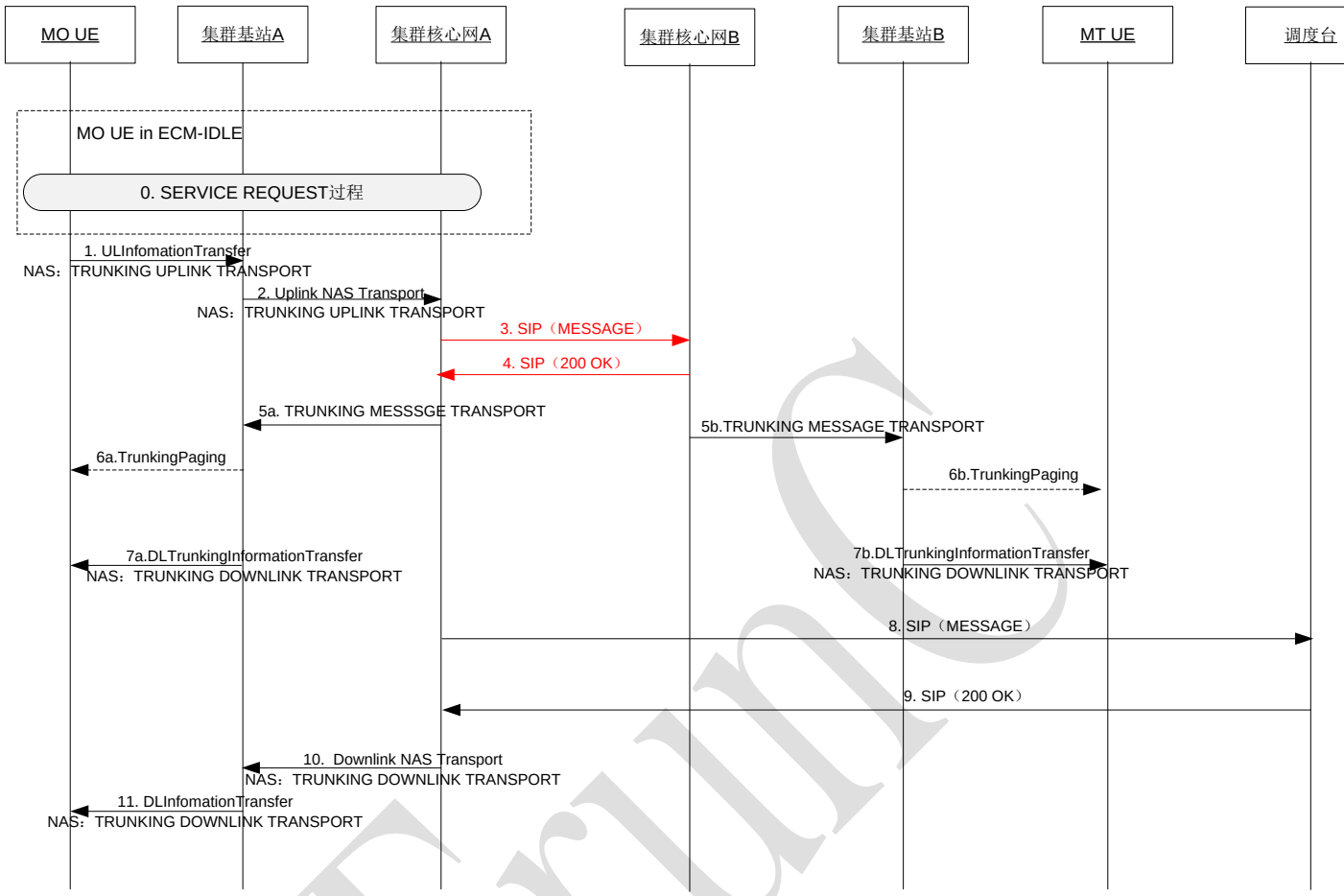
5） 步骤6-7：如果接收方包括调度台，则集群核心网对应调度台发送SIP（MESSAGE）消息，消息包含端到端加密指示e2ee和发送模式msgmode，其中msgmode取值为“2”（组播模式）；

6） 步骤8-9：集群核心网向短数据的发送UE发送TRUNKING DOWNLINK TRANSPORT消息，消息的Message Container Type指示为“短数据和状态数据”，Message Container中携带SDS消息 SHORT-MSG-ACK。

注：步骤 8 可在步骤 3 后执行。

7.6 多核心网加密组播短数据流程

场景描述：集群核心网 A 是短数据发送方 MO UE 的归属核心网和服务核心网，也是组归属核心网；集群核心网 B 是组内部分成员 MT UEs 驻留的核心网



流程说明如下：

处于ECM-IDLE态的UE，执行步骤0，通过SERVICE REQUEST过程和网络恢复连接。

1）步骤1-2：UE向集群核心网A发送TRUNKING UPLINK TRANSPORT消息，消息的Message Container Type指示为“短数据和状态数据”，Message Container中携带SDS消息 SHORT-MSG，内携带Calling party，Called party，Mode=01H（PTM）；

2）步骤3-4：集群核心网A也是组归属集群核心网，根据组内成员注册时位置登记过程上报的当前所在核心网的位置信息，向集群核心网B发送SIP（MESSAGE）消息，携带业务标识pttmsg、PLMN标识、接收组号、端到端加密指示e2ee，短数据类型msgtype，如果群组尚未建立，消息中还携带组安全信息，包括组基站密钥GKeNB、随机数RandGroup、接入层算法GroupASSecurityInfo、密钥版本号GKver，其中，短数据发送模式msgmode设置为“组播模式”，消息内容包含于消息体中，集群核心网B返回SIP(200 OK)响应；

如果群组已经建立，消息中不携带组安全信息，集群核心网B使用已建立的群组安全上下文。

3）步骤5：核心网通过TRUNKING MESSAGE TRANSPORT 消息向基站发起组播短数据发送过程，携带NAS消息TRUNKING DOWNLINK TRANSPORT，NAS消息的Message Container Type指示为“短数据和状态数据”，Message Container中携带SDS消息 SHORT-MSG，内携带Calling party，Called party，Mode=01H（PTM）；此过程可以各基站并行，也可以与步骤6对调度台的通知并行；

如果群组已建立，TRUNKING MESSAGE TRANSPORT 消息还携带为该群组分配的MME GROUP S1AP ID和eNB GROUP S1AP ID、并携带PLMN Identity、组号GroupIdentity、业务优先级Call Priority，消息中不携带组安全信息，基站使用已建立的群组安全上下文。

如果群组尚未建立，TRUNKING MESSAGE TRANSPORT 消息还携带PLMN Identity、GroupIdentity、业务优先级Call Priority、业务区域Message Service Area、组安全信息Group Call Security Information，其中Message Service Area指定组播短数据的发送范围，Group Call Security Information包含组基站密钥Group Call Security Key、随机数RAND Group、接入层安全算法Security algorithms、密钥版本号GKversion。

4） 步骤6：基站通过TPCCH向群组UE发送TrunkingPaging消息，其中groupShortMsg-Indication取值为true，并指示该组使用的加密算法cipheringAlgorithm和完保算法integrityProtAlgorithm、随机数randGroup、组密钥版本号groupSecurityVer。如果此时该群组正在进行呼叫，则本步骤可以省略；

注：如果群组未建立，则基站收到TRUNKING MESSAGE TRANSPORT消息后，应根据所携带业务区域Message Service Area临时建立TCCH信道发送DLTrunkingInfomationTransfer消息，当短消息发送完毕后删除TCCH信道，终端执行同样的操作。

5） 步骤7：基站向群组UE发送使用根据组基站密钥衍生的组RRC相关密钥进行加密和完保后的DLTrunkingInfomationTransfer消息，其中携带NAS消息TRUNKING DOWNLINK TRANSPORT，NAS消息的Message Container Type指示为“短数据和状态数据”，Message Container中携带SDS消息SHORT-MSG，内携带Calling party，Called party，Mode=01H（PTM）；

6） 步骤8-9：如果接收方包括调度台，则集群核心网对应调度台发送SIP（MESSAGE）消息，消息包含端到端加密指示e2ee和发送模式msgmode，其中msgmode取值为“2”（组播模式）；

7） 步骤10-11：集群核心网向短数据的发送UE发送TRUNKING DOWNLINK TRANSPORT消息，消息的Message Container Type指示为“短数据和状态数据”，Message Container中携带SDS消息 SHORT-MSG-ACK。

注：步骤 10 可在步骤 5 后执行。

8 端到端加密关键流程

8.1 终端向核心网发送端到端安全信息

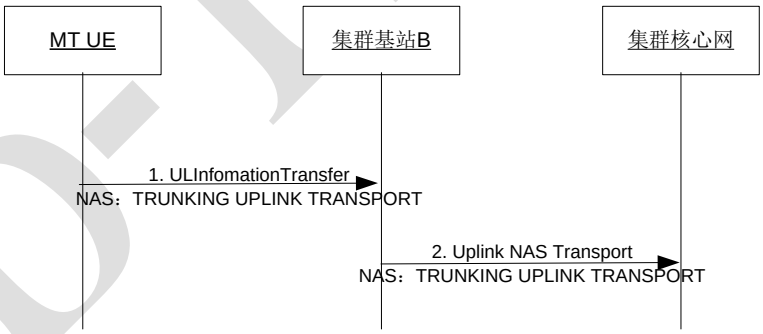


图11 终端向核心网发送端到端安全信息

流程说明如下：

1） 步骤1-2：UE向集群核心网发送TRUNKING UPLINK TRANSPORT消息，message container type 取值为02H（端到端安全信息），消息中包含端到端安全信息。

8.2 核心网向终端发送端到端安全信息

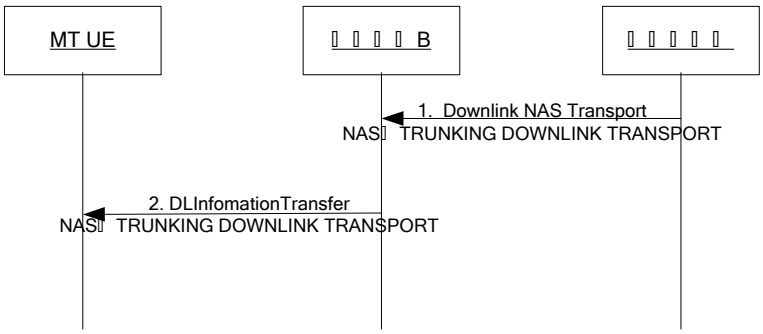


图12 核心网向终端发送端到端安全信息

流程说明如下：

1） 步骤1-2：UE向集群核心网发送TRUNKING UPLINK TRANSPORT消息，message container type 取值为02H（端到端安全信息），消息中包含端到端安全信息。

8.3 调度台向核心网发送端到端安全信息

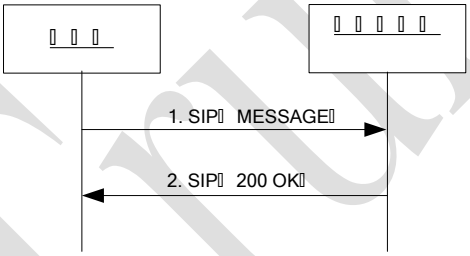


图13 调度台向核心网发送端到端安全信息

流程说明如下：

1） 步骤1：调度台向集群核心网发送SIP（MESSAGE）消息，消息中包含端到端安全信息；

2） 步骤2：集群核心网向调度台返回SIP（200（OK））消息。

8.4 核心网向调度台发送端到端安全信息

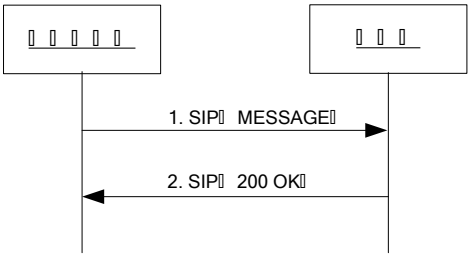


图14 核心网向调度台发送端到端安全信息

流程说明如下：

1） 步骤1：集群核心网向组内的调度台发送SIP（MESSAGE）消息，消息中包含端到端安全信息；

2） 步骤2：调度台向集群核心网返回SIP（200（OK））消息。

8.5 UE 发起的支持端到端加密的组呼建立

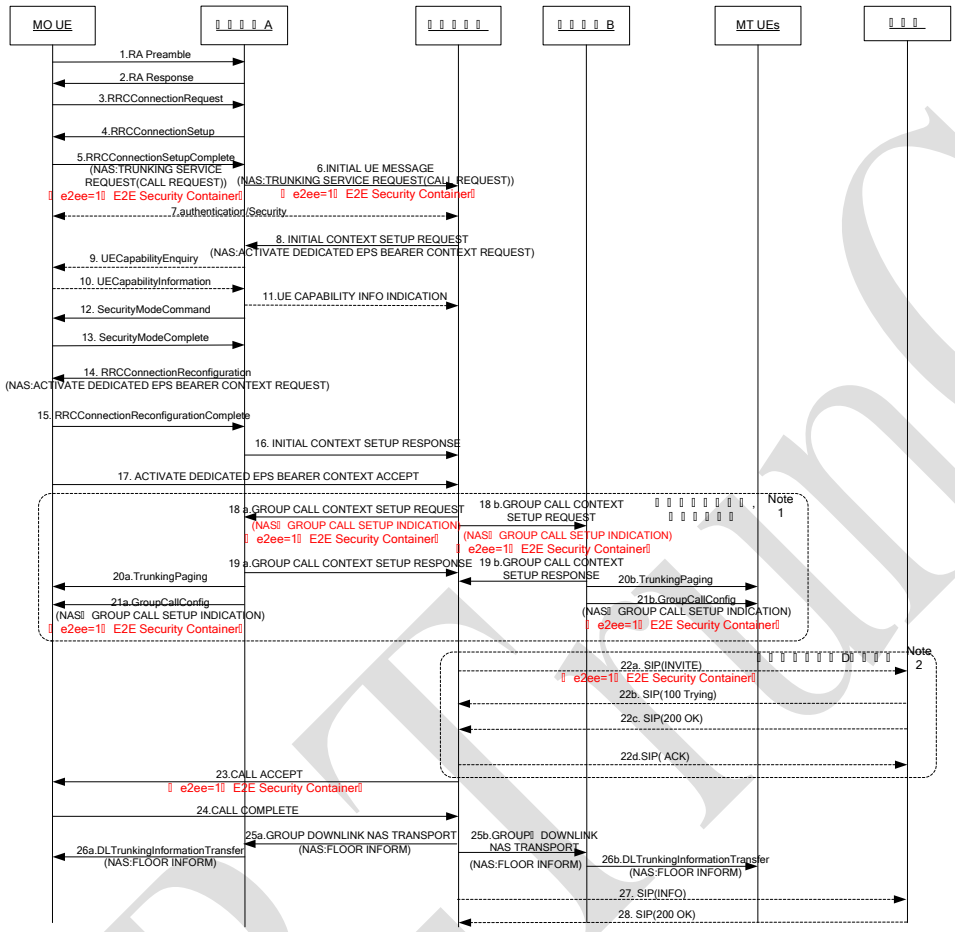


图15 用户发起的组呼建立流程

UE发起的支持端到端加密的组呼建立和普通的UE发起的组呼建立流程是相同的，差别在于：

22） 步骤5：呼叫请求CALL REQUEST申请建立一个集群组呼业务；如果主叫请求对本次呼叫进行端到端加密，则CALL REQUEST 中的Call Attribute IE中的端到端加密指示置为“1”， 可选携带E2E Security Container IE，用于传递端到端安全信息；

23）步骤18:核心网向相关基站发送GROUP CALL CONTEXT SETUP REQUEST消息触发群组上下文建立过程，GROUP CALL CONTEXT SETUP REQUEST消息中携带NAS消息GROUP CALL SETUP INDICATION，如果本次呼叫进行了端到端加密,则Call Attribute IE中的端到端加密指示置为“1”，可选携带E2E Security Container IE，用于传递端到端安全信息；

24）步骤21：基站在TCCH信道上发送GroupCallConfig，给出群组TTCH的接入层配置参数，还包含NAS消息GROUP CALL SETUP INDICATION；

25）步骤22a：集群核心网向调度台发送SIP（INVITE）消息，通知调度台进行组呼建立流程；如果本次呼叫进行了端到端加密，可选携带E2E Security Container IE，用于传递端到端安全信息；

26）步骤23：在至少一个基站下行承载成功建立后，核心网通过CALL ACCEPT通知发起者，相应资源已准备完毕，可以进行上行传输，消息携带呼叫ID、呼叫类型、呼叫属性、呼叫优先级、话权信息、媒体信息等；如果本次呼叫进行了端到端加密，则Call Attribute IE中的端到端加密指示置为“1”，可选携带E2E Security Container IE，用于传递端到端安全信息。

8.6 DC 发起的支持端到端加密的组呼建立

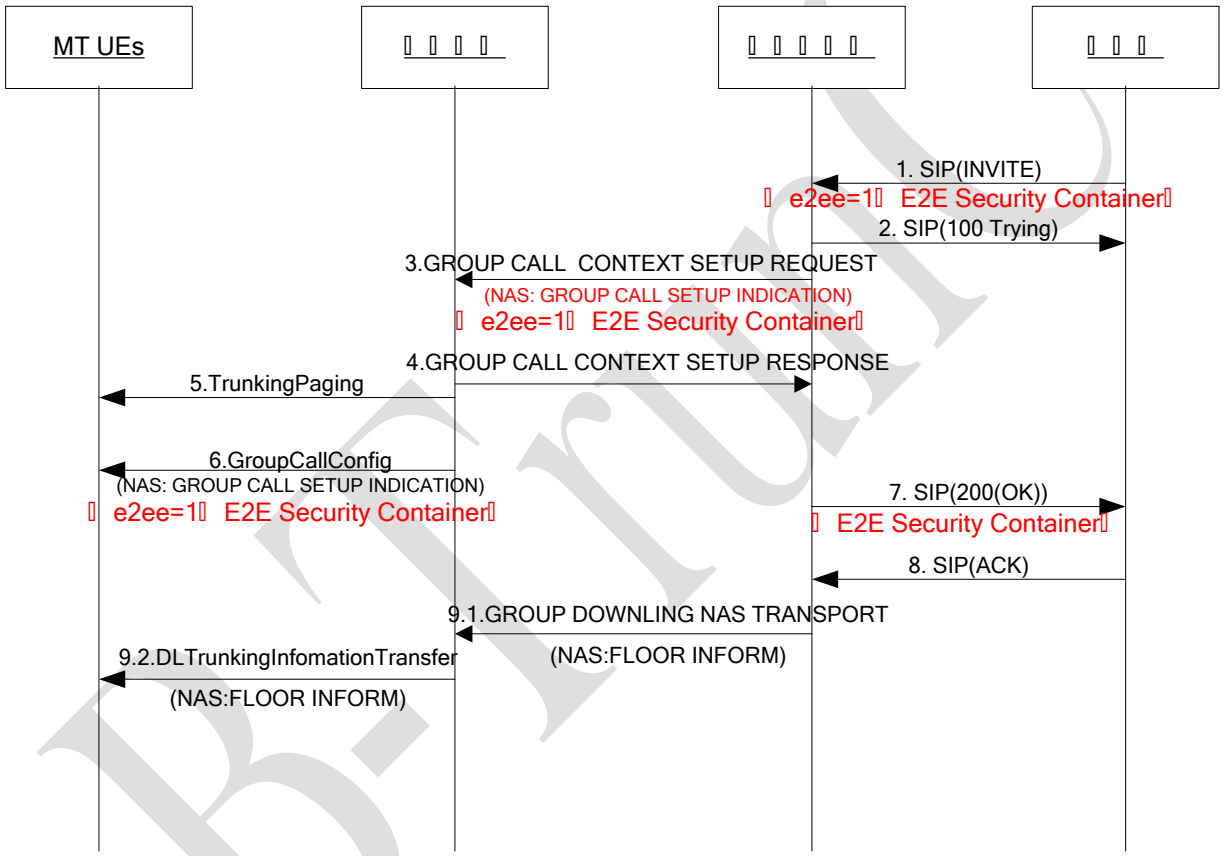


图16 调度台发起的组呼建立流程

DC发起的支持端到端加密的组呼建立和普通的UE发起的组呼建立流程是相同的，差别在于：

1） 步骤1：调度台发送SIP（INVITE）消息到集群核心网，请求建立组呼业务；如果调度台请求对本次呼叫进行端到端加密，则消息中的e2ee IE置为“1”，可选携带E2ESecurityContainer IE，用于传递端到端安全信息；

2） 步骤3：核心网向相关基站发送GROUP CALL CONTEXT SETUP REQUEST消息触发群组上下文建立过程，GROUP CALL CONTEXT SETUP REQUEST消息中携带NAS消息GROUP CALL SETUP INDICATION，如果本次呼叫进行了端到端加密，则Call Attribute IE中的端到端加密指示置为“1”，可选携带E2E Security Container IE，用于传递端到端安全信息；

3） 步骤6：基站在TCCH信道上发送GroupCallConfig，给出群组TTCH的接入层配置参数，还包含NAS消息GROUP CALL SETUP INDICATION；

4） 步骤7：核心网向调度台发送SIP（200 OK）消息，携带本次呼叫的媒体信息；如果本次呼叫进行了端到端加密，则Call Attribute IE中的端到端加密指示置为“1”，可选携带E2ESecurityContainer IE，用于传递端到端安全信息。

8.7 UE 发起的支持端到端加密的全双工单呼建立

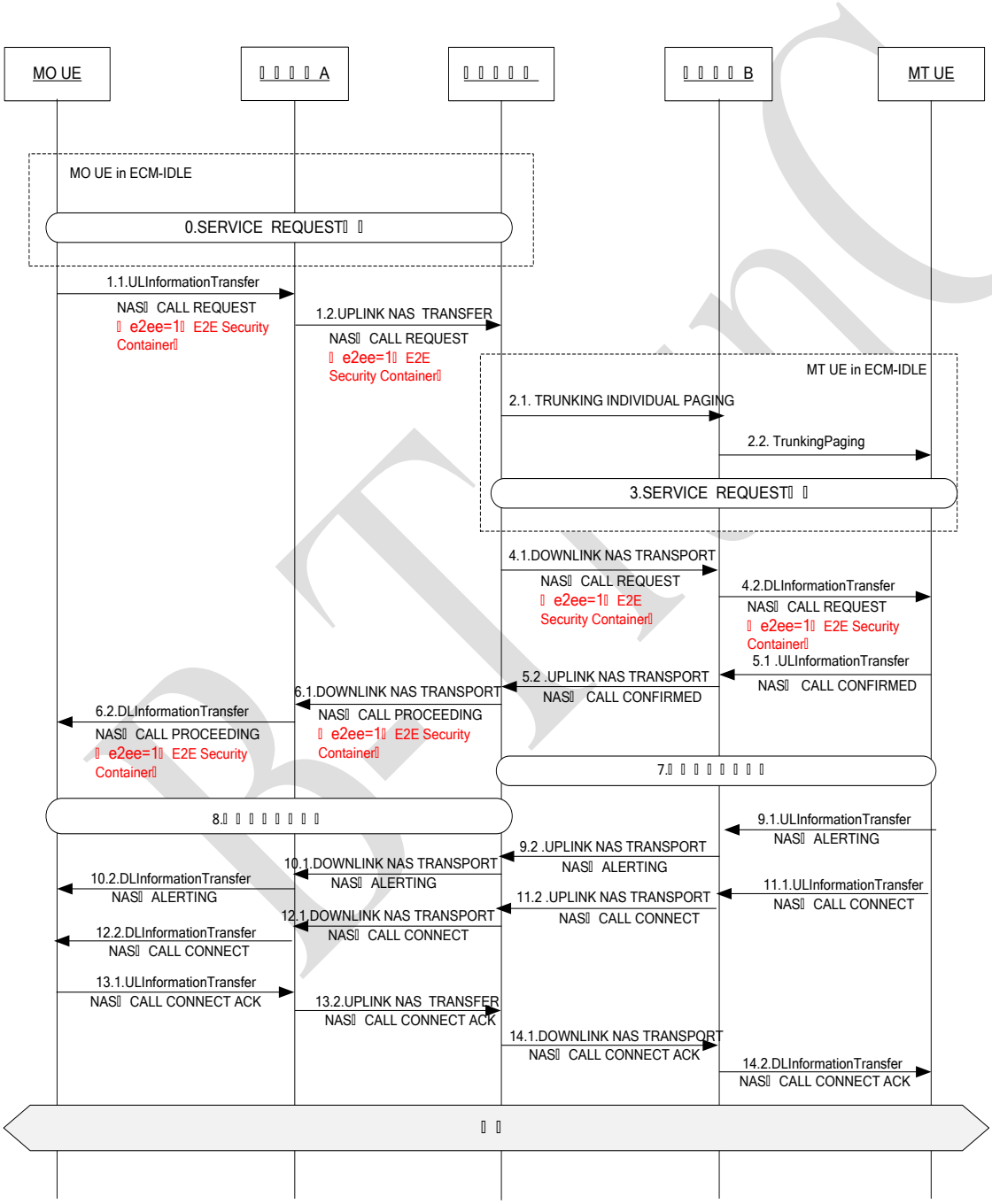


图17 终端发起的单呼建立流程

UE发起的支持端到端加密的单呼建立和普通的UE发起的单呼建立流程是相同的，差别在于：

1） 步骤1：主叫UE通过NAS消息CALL REQUEST，通知网络需要建立全双工单呼。如果主叫请求对本次呼叫进行端到端加密，则CALL REQUEST消息中的Call Attribute IE中的端到端加密指示置为“1”，可选携带E2E Security Container IE，用于传递端到端安全信息；

2） 步骤4：核心网通过CALL REQUEST消息，通知被叫UE此次呼叫的相关信息；如果本次呼叫进行了端到端加密，则Call Attribute IE中的端到端加密指示置为“1”， 可选携带E2E Security Container IE，用于传递端到端安全信息；

3） 步骤6：网络通过CALL PROCEEDING，通知主叫媒体格式；如果本次呼叫进行了端到端加密，则Call Attribute IE中的端到端加密指示置为“1”，可选携带E2E Security Container IE，用于传递端到端安全信息。

8.8 UE 发起的单呼建立拒绝

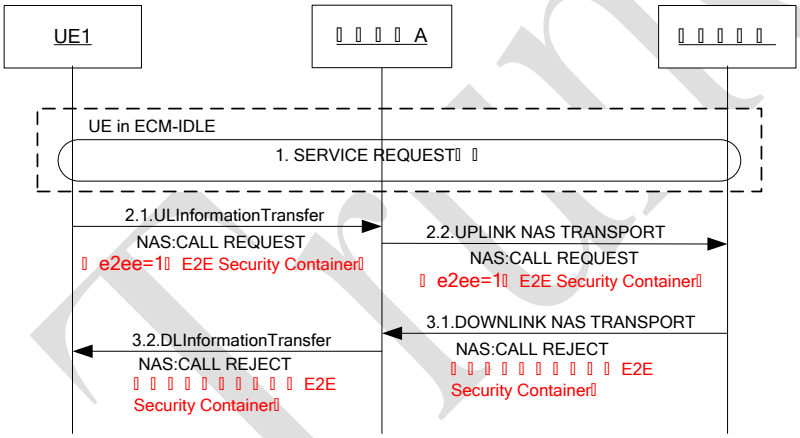


图18 终端发起的单呼建立流程

流程说明如下：

1） 步骤1：如是处于ECM-IDLE态的UE，通过SERVICE REQUEST流程，和网络恢复连接；

2） 步骤2：主叫UE通过NAS消息CALL REQUEST，通知网络需要建立全双工单呼；如果主叫请求对本次呼叫进行端到端加密，则Call Attribute IE中的端到端加密指示置为“1”，可选携带E2E Security Container IE，用于传递端到端安全信息；

3） 步骤3：网络侧收到CALL REQUEST消息之后，如果本次呼叫请求了端到端加密，集群核心网判断无法对本次呼叫进行加密，例如：加密服务器返回失败，或者被叫UE不支持加密等，则核心网向主叫UE发送CALL REJECT消息，其中携带“3d 端到端加密失败”原因值，可选携带E2E Security Container IE，用于传递端到端安全信息。

8.9 DC 发起的支持端到端加密的全双工单呼建立

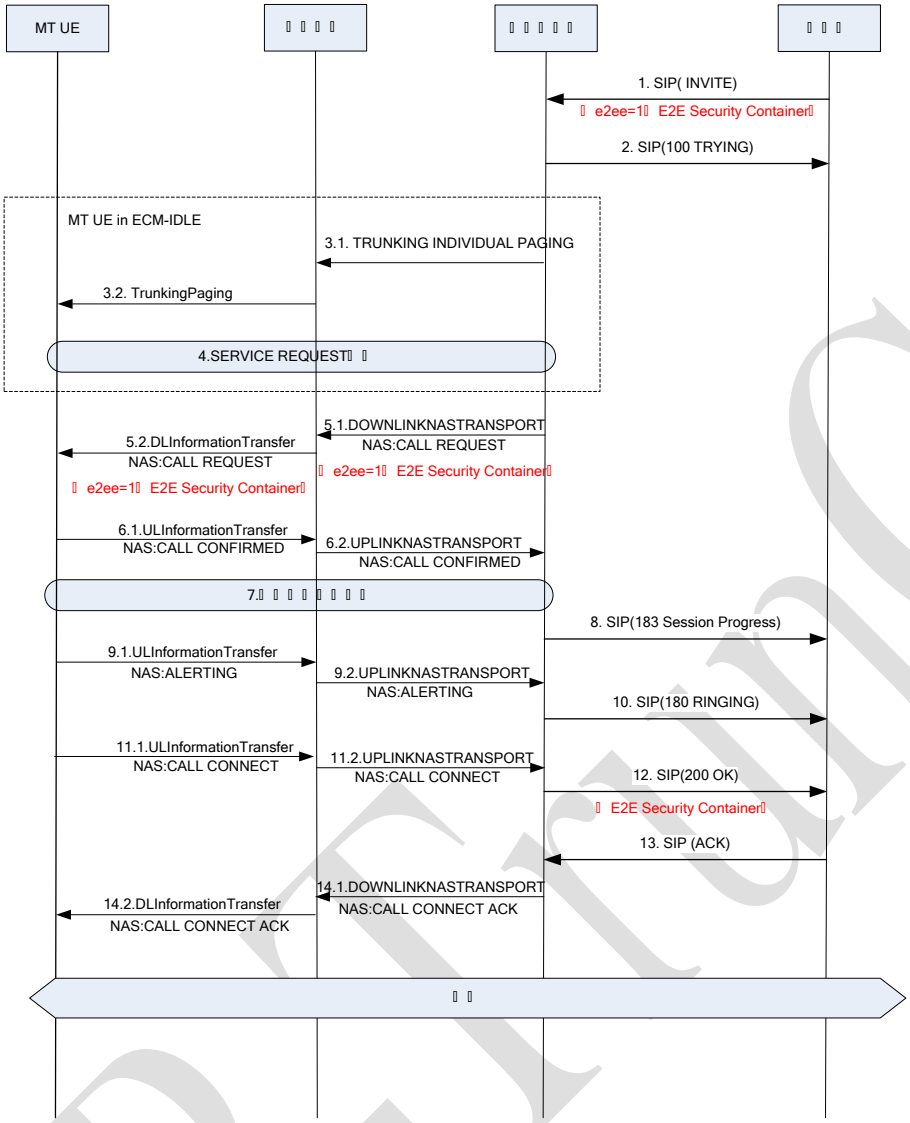


图19 调度台发起的单呼建立流程

DC发起的支持端到端加密的单呼建立和普通的UE发起的单呼建立流程是相同的，差别在于：

1） 步骤1：调度台发送SIP（INVITE）消息；如果调度台请求对本次呼叫进行端到端加密，则消息中的e2ee IE置为“1”， 可选携带E2ESecurityContainer IE，用于传递端到端安全信息；

2） 步骤5：网络向被叫终端发起单呼建立CALL REQUEST消息；如果本次呼叫进行了端到端加密，则Call Attribute IE中的端到端加密指示置为“1”，可选携带E2E Security Container IE，用于传递端到端安全信息；

3） 步骤12：核心网向调度台发送SIP（200 OK）消息，携带本次呼叫的媒体信息；如果本次呼叫进行了端到端加密，则可选携带E2E Security Container IE，用于传递端到端安全信息。