ICS 33.060
M 36

YD

中华人民共和国通信行业标准

YD/T 2558-2013

基于祖冲之算法的 LTE 终端和网络设备安全技术要求

Security technical requirements for LTE terminal and network equipment based on ZUC algorithm

2013-07-22 发布　　2013-10-01 实施

中华人民共和国工业和信息化部　发布

目　　次

前　言

本标准是基于祖冲之算法的LTE终端和网络设备安全系列标准之一，该系列标准的名称如下：

a）YD/T 2558-2013《基于祖冲之算法的LTE终端和网络设备安全技术要求》；

b）YD/T 2559-2013《基于祖冲之算法的LTE终端和网络设备安全测试方法》。

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由中国通信标准化协会归口。

本标准起草单位：工业和信息化部电信研究院、中国科学院数据与通信保护研究教育中心、中国移动通信集团公司、中国联合网络通信集团有限公司、华为技术有限公司、中兴通讯股份有限公司、大唐电信科技产业集团、诺基亚通信有限公司、诺基亚西门子通信（上海）有限公司、上海贝尔股份有限公司。

本标准主要起草人：袁　琦、刘东明、荆继武、查达仁、刘　斐、张　尼、杜志敏、许怡娴、李　阳、徐　晖、张大江、陆　伟、胡志远、崔媛媛、蒋晓琳。

引　言

本文件的发布机构提请注意，声明符合本文件时，可能涉及到祖冲之（ZUC）算法相关的专利的使用。

本文件的发布机构对于该专利的真实性、有效性和范围无任何立场。

该专利持有人已向本文件的发布机构保证，他愿意在公平、合理、无歧视的基础上，为申请实施者在实施本文件时提供专利的免费许可，前提是：申请实施者若持有实施本文件密码算法的技术上的必要专利，也愿意在公平、合理和无歧视的基础上，对该专利（祖冲之算法相关专利）持有人在实施本文件时提供专利的免费许可。

该专利持有人的声明已在本文件的发布机构备案。相关信息可以通过以下联系方式获得：

专利持有人姓名：中国科学院数据与通信保护研究教育中心

地址：北京市海淀区闵庄路甲89号

请注意除上述专利外，本文件的某些内容仍可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

基于祖冲之算法的 LTE 终端和网络设备安全技术要求

1 范围

本标准规定了基于祖冲之算法的 LTE 终端和网络设备安全技术要求，包括 HSS 设备、MME 设备、eNB 设备和 UE 等安全技术要求。

本标准适用于 LTE 终端和网络设备。

2 缩略语

下列缩略语适用于本文件。

3GPP	3rd Generation Mobile System	第三代移动通信系统
AS	Access Stratum	接入层
AES	Advanced Encryption Standard	高级加密标准
AKA	Authentication and Key Agreement	认证与密钥协商
AMF	Authentication Management Field	认证管理字段
AuC	Authentication centre	鉴权中心
CG	Charging Gateway	计费网关
eNB	Evolved Node B	演进型节点B
EPC	Evolved Packet Core	演进的分组核心（网）
EPS	Evolved Packet System	演进的分组系统
E-UTRAN	Evolved Universal Terrestrial Radio Access Network	演进的通用陆地接入网
GPRS	General Packet Radio Service	通用分组无线业务
GERAN	GSM EDGE Radio Access Network	增强型数据速率GSM演进无线接入网络
GUTI	Globally Unique Temporary Identity	全局唯一临时标识
HLR	Home Location Register	归属位置寄存器
HSS	Home Subscriber Server	归属签约用户服务器
IMSI	International Mobile Subscriber Identity	国际移动用户识别码
IP	Internet Protocol	互联网协议
LTE	Long Term Evolution	长期演进
MME	Mobility Management Entity	移动管理实体
MS	Mobile Station	移动台
NAS	Non-Access Stratum	非接入层
NCC	Next hop Chaining Counter	下一跳链计数器
NH	Next Hop	下一跳
PCRF	Policy and Charging Rules Function	策略及计费规则功能

PDCP	Packet Data Convergence Protocol	分组数据集中协议
PDN	Packet Data Network	分组数据网
P-GW	PDN Gateway	分组数据网网关
QoS	Quality of Service	业务质量
RRC	Radio Resource Control	无线资源控制
SGSN	Serving GPRS Support Node	服务GPRS支持节点
S-GW	Serving Gateway	服务网关
UE	User Equipment	用户设备
UTRAN	Universal Terrestrial Radio Access Network	通用陆地无线接入网
ZUC	Zhuchongzhi	祖冲之

3 概述

3.1 EPS 网络架构

EPC网络设备包括移动性管理设备（MME）、服务网关（S-GW）、PDN网关（P-GW）、服务GPRS支持节点（SGSN）、归属签约用户服务器（HSS）以及策略和计费控制单元（PCRF）等组成。网络架构如图1所示，其中S-GW和P-GW可以合设，也可以分设。

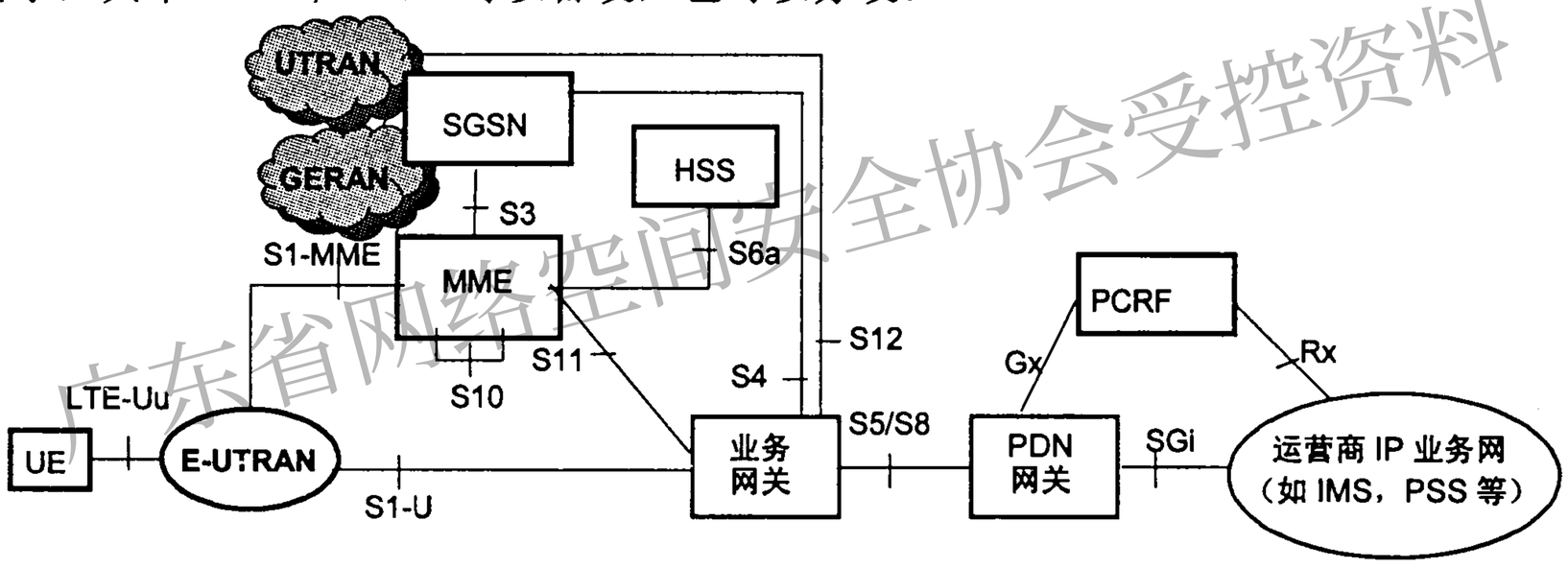

图1 EPS网络架构（S-GW与P-GW分设）

3.2 网络设备

eNB集成了3G中NodeB与RNC的功能，实现了UE附着时的MME选择，寻呼和广播消息的调度传输以及对RRC信令和用户数据的加解密等功能。eNB之间底层采用IP传输，逻辑上通过X2接口互相连接。

MME的主要功能包括：支持NAS信令及其安全、跟踪区域（Tracking Area）列表的管理、P-GW和S-GW的选择、跨MME切换时MME的选择、在向2G/3G接入系统切换过程中SGSN的选择、用户的认证、漫游控制以及承载管理、3GPP不同接入网络的核心网络节点之间的移动性管理，以及UE在ECM-IDLE状态下可达性管理等。

S-GW是终止于E-UTRAN接口的网关，该设备的主要功能包括：eNodeB间切换时的本地锚定点、3GPP不同接入系统间切换时的移动性锚点、执行合法侦听功能、数据包的路由和前转、上下行传输层的分组标记、ECM-IDLE状态下分组缓存及寻呼触发、计费等。

P-GW是面向PDN终结于SGi接口的网关，该设备的主要功能包括：基于用户的包过滤功能、合法侦听功能、UE的IP地址分配功能、上下行传输层的分组标记、计费、门控、QoS控制和承载控制等。

与EPC系统互通的SGSN在现有SGSN功能之上还需支持：2G/3G/LTE接入网间的移动信令交互、P-GW和S-GW的选择、MME的选择。

HSS是用于存储用户签约信息的数据库。该设备的主要功能包括：存储用户签约信息、用户认证参数生成和位置信息管理等。

PCRF终结于Rx接口和Gx接口，该设备主要功能包括：提供基于业务数据流的QoS控制、门控和计费控制等。

EPC网络各实体之间接口均基于IP传输。

S1接口是无线接入网与核心网的接口。基于控制与承载相分离的思想，S1接口分为用户平面和控制平面。其中用户平面接口S1-U将eNB和SGW连接，用于传送用户数据和相应的用户平面控制帧。而控制平面接口S1-MME则将eNB和MME相连，主要完成S1接口的无线接入承载控制、接口专用的操作维护等功能。

4 HSS 设备鉴权功能要求

4.1 用户认证支持

HSS合一了认证中心的功能，HSS应能根据MME请求向MME提供一组或者多组认证参数，支持认证业务相关处理。对支持HLR功能的HSS设备，HSS和HLR设备应共享认证中心。

HSS/AuC负责生成用户认证相关的密钥材料与认证向量，除认证向量相关的参数，即RAND、AUTN、XRES、K_{ASME}（用于EPS AKA）或CK/IK（用于UMTS AKA）这些参数外，HSS中所有生成和存储的参数不允许离开HSS。HSS中涉及到的安全参数有：K、r1-r5、c1-c5、AMF、SQN、RAND、OPc，CK、IK、K_{ASME}、AK、SN ID、AUTN、X_{RES}。

4.2 认证逻辑功能

HSS应能支持 UMTS AKA与EPS AKA。

HSS应能支持以下认证算法：应能同时支持3G系统的多种算法与LTE的算法，包括MILENAGE算法（包括f0、f1、f1*、f2、f3、f4、f5、f5*）、HMAC-SHA-256算法及其他移动可能所要求的算法；能够根据服务网络请求生成并传输认证向量；存储用户对应的认证算法标识与服务网络的网络标识，能够根据用户认证算法标识与服务网络的网络标识获得该用户对应的认证算法，并进行相应运算；不保存OP值并且不存在导入OP值的接口。

4.3 认证流程

当HSS接收到来自服务网络的认证数据请求（这将包括用户标识、服务网络标识和网络类型）时，应当保证请求认证数据的服务网络有资格使用认证请求中的服务网络标识。如果HSS已经预先计算好认证向量，则直接从数据库中提取，否则按要求计算得到认证向量。

HSS向服务网络返回认证响应，提供被请求信息。若服务网络请求多个认证向量，则认证响应按向量序列号依次返回。

4.4 认证机制输入/输出参数设置

HSS应负责存储用户的根密钥K，K应安全存储在HSS中，不应以任何方式被泄漏。

HSS应负责存储与计算AKA认证中所需要的各种输入参数，包括RAND、SQN、AMF、Opc、r1-r5、c1-c5。

HSS应负责生成与发送AKA认证所需要的各种输出参数，包括同时作为输入参数的RAND，计算得到的AUTN、XRES与K_{ASME}。

5 MME 设备安全功能要求

5.1 接入安全

1）认证鉴权功能：MME通过认证功能实现网络和用户之间的相互认证以及密钥协商，确保用户请求的业务在当前网络是可以授权使用的，通常这个功能连同移动性管理过程一起使用。认证包括对IMSI、GUTI等的校验，可以通过人机命令开启或关闭可选认证功能。

应认证鉴权的场合包括：

— UE初次附着；

— UE附着，且网络中不存在UE的安全上下文；

— 进行跟踪区更新等NAS流程时，带上来的GUTI与网络侧不符合的情况；

— 进行跟踪区更新时完整性检查失败；

— NAS计数器值达到一定数值后。

MME应支持按运营商要求，根据信令类别进行配置，在如下可选场合进行认证鉴权：

— 业务请求过程；

— 其他附着过程；

— 其他跟踪区更新。

MME应支持在GUTI认证失败后发起二次认证。

2）GUTI分配功能：GUTI作为临时用户标识，在空口上保护IMSI的安全性，在用户首次附着后，MME应为其分配GUTI值。可发起GUTI重分配过程的场合如下：

— 附着过程；

— 跟踪区更新过程；

— 连接状态下用户的GUTI标识重分配过程。

3）AS安全上下文下发功能：MME会在发给eNB的Initial Context Setup Request消息中包含AS安全上下文和UE的安全能力，eNodeB会参照UE的能力选择AS算法实现RRC信令的机密性和完整性保护。

4）NAS信令机密性和完整性保护功能：MME会在发给UE的NAS安全模式命令（Security Mode Command）消息中加入支持NAS安全算法列表和KSI， MME选择安全算法并利用生成的密钥实现对NAS信令的机密性和完整性保护。

5.2 支持认证鉴权功能

EPC网络能够为UE提供双向认证功能。作为认证与密钥协商的结果，由HSS生成中间密钥K_{ASME}，发给MME。

5.3 用户身份保护功能

MME应能向UE分配一GUTI，以保护用户身份的机密性。当MME不能根据GUTI识别用户身份时，应当由MME发起用户识别身份标识流程，向用户请求永久身份标识（IMSI）。

5.4 用户永久身份与认证向量传递功能

在同一服务网络域内，MME之间应当能够在收到用户的跟踪区更新后传递用户永久身份与认证向量。

在不同的服务域内，MME之间不能传递未使用的EPC和UMTS认证向量。MME允许接收来自SGSN的未使用过的UMTS认证向量并允许将它返送回原SGSN，但不允许转发给其他SGSN或者使用UMTS认证向量。EPC认证向量不能从MME转发给SGSN。

5.5 支持 NAS 层消息安全功能

UE和MME之间的NAS层消息需要经过加密和完整性保护，提供NAS层消息安全。加密算法支持EEA3:ZUC，EEA2：AES, EEA1: SNOW 3G，EEA0: Null algorithm，标识符分别为0011、0010、0001和0000，完整性保护算法支持EIA3: ZUC, EIA2: AES, EIA1: SNOW 3G，EIA0: Null algorithm，标识符分别为：0011、0010、0001和0000。MME在接收到一个有错误或者缺失NAS-MAC的NAS消息时，应可丢弃相关的NAS消息。

5.6 支持 AS 安全功能

MME能够支持AS密码生成，能够触发AS层安全流程，从而激活AS层安全功能。

5.7 加密和完整性保护算法要求

MME应实现基于ZUC、AES、SNOW 3G的密码算法。

MME应实现应实现ZUC、AES、SNOW 3G的加密功能和不加密功能。算法标识符分配如下：

— EEA3: ZUC, 算法标识符为0011；

— EEA2: AES，算法标识符为0010；

— EEA1: SNOW 3G，算法标识符为0001；

— EEA0：NULL，不进行加密，算法标识符为0000。

MME应实现ZUC、AES、SNOW 3G的完整性保护功能和不进行完整性保护功能。算法标识符分配如下：

— EIA3: ZUC，算法标识符为0011；

— EIA2: AES，算法标识符为0010；

— EIA1: SNOW 3G，算法标识符为0001；

— EIA0:NULL，不进行完整性保护（仅用于受限业务模式下紧急呼叫），算法标识符为0000。

5.8 密钥层次结构及分发推衍要求

MME应能从K_{ASME}推衍产生K_{NASint}、K_{NASenc}、中间密钥K_{eNB}。

5.9 密钥标识符与使用要求

MME应能分配密钥组标识KSI_{ASME}，经认证请求消息发送至移动终端。在E-UTRAN空闲模式下或从GERAN/UTRAN切换至E-UTRAN过程中，MME还应能在推衍映射K_{ASME}时产生KSI_{SGSN}。密钥标识符使得UE与MME不用通过认证也能确定本地K_{ASME}。

5.10 安全上下文的建立要求

当接入层安全上下文在eNB上建立时，MME应向eNB发送UE的EPC安全能力。在MME分别接收到X2切换消息和S1切换消息后，MME应能校验来自eNB的UE安全能力是否与本地存储的UE安全能力相一致。

在非接入层安全上下文建立时，MME应能与UE通过NAS安全模式命令协商NAS的完整性与加密算法。

5.11 用户附着/非附着状态切换时的密钥处理要求

当附着请求被拒绝时，MME应删除其中的所有认证数据。

如果UE关机，MME应删除剩余的鉴权数据，但本地EPS NAS安全上下文应该保存，没有使用过的鉴权向量也可以保存。

如果UE去附着原因是重新附着，MME应删除inter-RAT切换时或空闲模式下移动时产生的映射安全上下文，保留其他所有认证数据。

如果HSS发送“用户撤销登记”消息，MME应删除其所有认证数据。

UE附着时如果存在EPC NAS安全上文且NAS算法变更，MME应重新推衍NAS密钥并告知UE。

UE附着时如果不存在EPC NAS安全上下文，则需要运行EPC AKA认证过程并生成密钥。

5.12 空闲状态/连接状态切换时的密钥处理要求

从ECM-IDLE状态向ECM-CONNECTED状态转变时，MME应能根据判断是否需要进行新一轮认证，MME应产生接入层密钥K_{eNB}与相关参数NH。

从ECM-CONNECTED状态向ECM-IDLE状态转变时，MME应保留存储的EPC NAS安全上下文，删除NH和NCC。

5.13 移动性密钥管理要求

在空闲状态下，如果源MME 和目标MME分别使用不同的NAS算法，目标MME重新推衍NAS密钥。

当进行eNB内切换时，eNB应当负责生成K_{eNB}*，并将K_{eNB}*和用于生成K_{eNB}*的NCC放在HO Command消息中传给UE。当进行X2切换时，源eNB应当负责生成K_{eNB}*，并将{K_{eNB}*, NCC}传给目标eNB；当进行S1切换时，源MME应该生成新的{NH，NCC}参数对，然后和K_{ASME}一起通过S10 FORWARD RELOCATION REQUEST消息传给目标MME，目标MME通过S1 HANDOVER REQUEST消息将{NH，NCC}传给目标eNB。

5.14 密钥更新要求

MME需要在以下情况时重新生成eNB密钥；

— MME和UE运行AKA认证后激活新的EPC安全上下文时。

MME需要在以下情况时重新生成NAS密钥：

— MME重新进行EPC AKA认证时；

— 当前安全上下文的NAS上行或下行计数器即将回卷时。

6 eNB 设备安全功能要求

6.1 支持 AS 层消息安全功能

UE和eNB之间的RRC消息需要经过加密和完整性保护，提供AS层消息安全。加密算法支持EEA3:ZUC，EEA2: AES, EEA1: SNOW 3G，EEA0: Null algorithm，标识符分别为0011、0010、0001和0000，完整性保护算法支持EIA3: ZUC, EIA2: AES, EIA1: SNOW 3G，EIA0: Null algorithm，标识符分别为0011、0010、0001和0000。

6.2 支持用户面数据安全功能

UE和eNB之间的用户面数据需要经过加密性保护，提供用户面数据安全。加密算法支持EEA3:ZUC，EEA2: AES, EEA1: SNOW 3G，EEA0: Null algorithm，标识符分别为0011、0010、0001和0000。

6.3 加密和完整性保护算法要求

eNB应实现基于ZUC、AES、SNOW 3G的密码算法。

eNB应实现ZUC、AES、SNOW 3G的加密功能和不加密功能。算法标识符分配如下：

— EEA3: ZUC，算法标识符为0011；

— EEA2: AES，算法标识符为0010；

— EEA1: SNOW 3G，算法标识符为0001；

— EEA0：NULL，不进行加密，算法标识符为0000。

eNB应实现ZUC、AES、SNOW 3G的完整性保护功能和不进行完整性保护功能。算法标识符分配如下：

— EIA3: ZUC，算法标识符为0011；

— EIA2: AES，算法标识符为0010；

— EIA1: SNOW 3G，算法标识符为0001；

— EIA0:NULL，不进行完整性保护（仅用于受限业务模式下紧急呼叫），算法标识符为0000。

6.4 密钥层次结构及分发推衍要求

eNB应能从K_{eNB}推衍产生K_{UPenc}、K_{RRCint}、K_{RRCenc}、和K_{eNB}*。

6.5 安全上下文的建立要求

当接入层安全上下文在eNB上建立时，MME应向eNB发送UE的EPC安全能力。

6.6 X2 切换时 AS 层协商过程

源eNB经X2接口向目标eNB切换时，源eNB应在切换请求消息中附带UE安全能力。目标eNB应从本地配置的按优先级排序的算法列表（包括完整性算法和加密算法）中选取UE安全能力能满足的最高优先级算法。指定算法应通过切换命令告知UE。在通道切换消息中，目标eNB应把来自源eNB的UE安全能力发送至MME。MME应能校验来自eNB的UE安全能力是否与本地存储的UE安全能力相一致。

6.7 S1 切换时 AS 层协商过程

源eNB经S1接口向目标eNB切换时，源eNB应把UE安全能力以透明集合的形式通过切换请求消息经S1-AP发送至目标eNB。目标eNB应从本地配置的按优先级排序的算法列表（包括完整性算法和加密算法）中选取UE安全能力能满足的最高优先级算法。目标eNB选择了不同的算法时，指定算法应通过切换命令告知UE。在切换通知消息中，目标eNB应把来自源eNB的UE安全能力发送至MME。目标MME通过S1 Handover Request消息通知目标enode B UE的安全能力。

6.8 移动性密钥管理要求

当进行 eNB 内切换时，eNB 应当负责生成 K_{eNB}*，并将 K_{eNB}*和用于生成 K_{eNB}*的 NCC 放在 HO Command 消息中传给 UE。当进行 X2 切换时，源 eNB 应当负责生成 K_{eNB}*，并将{K_{eNB}*, NCC}传给目标 eNB；当进行 S1 切换时，源 MME 应该生成新的{NH，NCC}参数对，然后和 K_{ASME} 一起通过 S10 FORWARD RELOCATION REQUEST 消息传给目标 MME，目标 MME 通过 S1 HANDOVER REQUEST 消息将{NH，NCC}传给目标 eNB。

6.9 密钥更新要求

eNB需要在以下情况时重新生成AS密钥：$K_{RRC\text{-}enc}$、$K_{RRC\text{-}int}$和$K_{UP\text{-}enc}$：

— 由MME和UE在激活不同于当前有效EPS AS安全上下文的另一个安全上下文时发起；

— 由eNB在PDCP计数器即将回卷时发起；

— K_{eNB}、$K_{RRC-enc}$、$K_{RRC-int}$和K_{UP-enc}都允许重新生成，由MME在激活不同于当前有效EPS AS安全上下文的另一个安全上下文时发起。$K_{NAS-enc}$和$K_{NAS-int}$也允许被重新生成，且应由MME在需激活不同于当前有效EPS NAS安全上下文的另一个安全上下文时发起。

6.10 性能要求

在20MHz带宽，2:2子帧配比的配置条件下，采用CAT3终端，在不使用加密算法时应达到下行58Mbit/s、上行19Mbit/s以上。在实现ZUC算法后，eNB应能够保持上述指标。

在20MHz带宽的配置条件下，采用CAT3终端，在不使用加密算法时应达到下行100Mbit/s、上行50Mbit/s以上。在实现ZUC算法后，eNB应能够保持上述指标。

7 UE 安全功能要求

7.1 业务能力

UE开启加密算法，应不影响用户业务使用。

7.2 用户身份保护功能

MME应能向UE分配一GUTI，UE获得GUTI，以保护用户身份的机密性。

7.3 支持认证和密钥协商

UE应支持EPS AKA双向身份认证及密钥协议流程。UE应正确响应MME发出的用户认证请求，并能根据MME发送的User authentication request启动EPS AKA过程，执行正确的EPS AKA过程，生成UE与MME间的共享密钥K_{ASME}。

7.4 NAS 层安全要求

UE应能正确响应MME发出的NAS安全模式命令消息(NAS Security Mode Command)，执行消息完整性验证，开始加/解密，并正确返回NAS安全模式完成消息(NAS Security Mode Complete)。

UE应支持与MME之间的NAS层信令加密和完整性保护。

UE与MME之间NAS层信令的加密应支持如下加密算法：

— EEA3: ZUC，算法标识符为0011；

— EEA2: AES，算法标识符为0010；

— EEA1: SNOW 3G，算法标识符为0001；

— EEA0：NULL，不进行加密，算法标识符为0000。

UE与MME之间NAS层信令应支持如下完整性算法：

— EIA3: ZUC，算法标识符为0011；

— EIA2: AES，算法标识符为0010；

— EIA1: SNOW 3G，算法标识符为0001；

— EIA0:NULL，不进行完整性保护（仅用于受限业务模式下紧急呼叫），算法标识符为0000。

7.5 AS 层安全要求

UE应能正确响应eNB发出的AS安全模式命令消息(AS Security Mode Command)，执行消息完整性验证，开始加/解密，并正确返回AS安全模式完成消息(AS Security Mode Complete)。

UE应支持与eNB之间的RRC信令的加密和完整性保护，UP数据的加密保护。

UE与eNB之间的RRC信令与UP数据加密应支持如下加密算法：EEA3、EEA2、EEA1与EEA0。

UE与eNB之间的RRC信令完整性保护应支持的完整性保护算法：EIA3、EIA2、EIA1和EIA0。

7.6 加密和完整性保护算法要求

UE应实现基于ZUC、AES、SNOW 3G的加密算法。

UE应实现ZUC、AES、SNOW 3G的加密功能和不加密功能。算法标识符分配如下：

— EEA3: ZUC，算法标识符为0011；

— EEA2: AES，算法标识符为0010；

— EEA1: SNOW 3G，算法标识符为0001；

— EEA0：NULL，不进行加密，算法标识符为0000。

UE应实现ZUC、AES、SNOW 3G的完整性保护功能和不进行完整性保护功能。算法标识符分配如下：

— EIA3: ZUC，算法标识符为0011；

— EIA2: AES，算法标识符为0010；

— EIA1: SNOW 3G，算法标识符为0001；

— EIA0:NULL，不进行完整性保护（仅用于受限业务模式下紧急呼叫），算法标识符为0000。

7.7 密钥层次结构及分发推衍要求

UE应能从CK/IK推衍产生K_{ASME}。

UE应能从K_{ASME}推衍产生K_{eNB}、K_{NASint}、K_{NASenc}、中间密钥K_{eNB}。

UE应能从K_{eNB}推衍产生K_{UPenc}、K_{RRCint}、K_{RRCenc}、中间密钥K_{eNB}*。

7.8 安全上下文的建立要求

当接入层安全上下文在eNB上建立时，MME应向eNB发送UE的EPC安全能力。

在非接入层安全上下文建立时，MME应能与UE通过NAS安全模式命令协商NAS的完整性与加密算法。

7.9 X2 切换时 AS 层协商过程

源eNB经X2接口向目标eNB切换时，源eNB应在切换请求消息中附带UE安全能力。目标eNB应从本地配置的按优先级排序的算法列表（包括完整性算法和加密算法）中选取UE安全能力能满足的最高优先级算法。指定算法应通过切换命令告知UE。在通道切换消息中，目标eNB应把来自源eNB的UE安全能力发送至MME。

7.10 S1 切换时 AS 层协商过程

源eNB经S1接口向目标eNB切换时，源eNB应把UE安全能力以透明集合的形式通过切换请求消息经S1-AP发送至目标eNB。目标eNB应从本地配置的按优先级排序的算法列表（包括完整性算法和加密算法）中选取UE安全能力能满足的最高优先级算法。指定算法应通过切换命令告知UE。在切换通知消息中，目标eNB应把来自源eNB的UE安全能力发送至MME。

7.11 密钥更新要求

UE需要在以下情况时重新生成eNB密钥；

— MME和UE运行AKA认证后激活新的EPC安全上下文时。

UE需要在以下情况时重新生成NAS密钥：

— MME和UE重新进行EPC AKA认证时；

— 当前安全上下文的NAS上行或下行计数器即将回卷时。

UE需要在以下情况时重新生成AS密钥：$K_{RRC-enc}$、$K_{RRC-int}$和K_{UP-enc}；

— 由MME和UE在激活不同于当前有效EPS AS安全上下文的另一个安全上下文时发起；

— 由eNB在PDCP计数器即将回卷时发起；

— K_{eNB}、$K_{RRC-enc}$、$K_{RRC-int}$和K_{UP-enc}都允许重新生成，由MME在激活不同于当前有效EPS AS安全上下文的另一个安全上下文时发起；

— $K_{NAS-enc}$和$K_{NAS-int}$也允许被重新生成，且应由MME在需激活不同于当前有效EPS NAS安全上下文的另一个安全上下文时发起。

7.12 性能要求

TD-LTE或LTE FDD终端在不使用加密算法的情况下，上、下行峰值速率应能达到其传输能力等级对应的理论速率的85%。在开启ZUC算法的情况下，上、下行峰值速率应能够保持上述指标。

中华人民共和国
通信行业标准

基于祖冲之算法的 LTE 终端和网络设备安全技术要求

YD/T 2558–2013

*

人民邮电出版社出版发行
北京市崇文区夕照寺街 14 号 A 座
邮政编码：100061
宝隆元（北京）印刷技术有限公司印刷

*

开本：880 × 1230　1/16　　2013 年 9 月第 1 版
印张：1.25　　2013 年 9 月北京第 1 次印刷
字数：29 千字

15115 • 265
定价：20 元