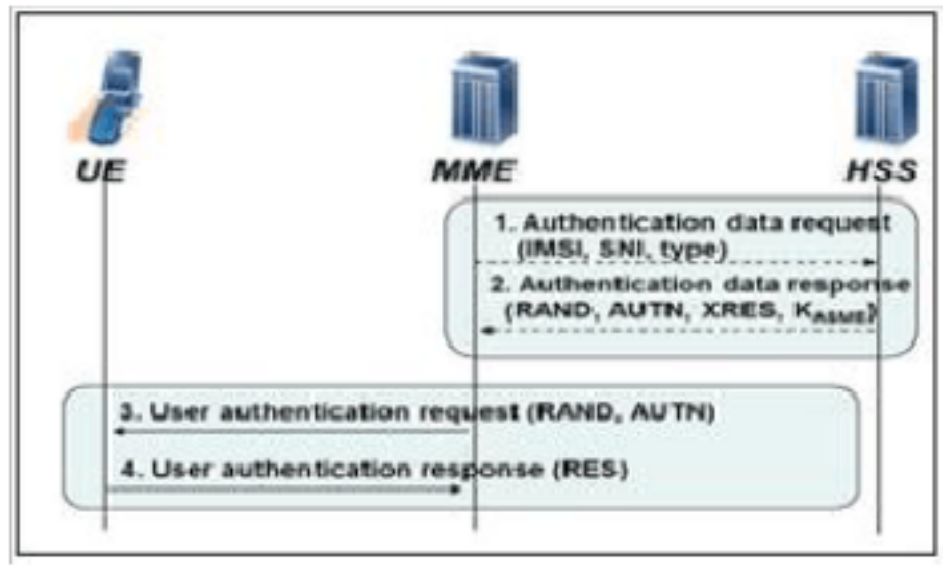
MME 的鉴权和加密过程

鉴权流程的目的是由 HSS 向 MME 提供 EPS 鉴权向量 (RAND, AUTN, XRES, KASME)，并用来对用户进行鉴权。



1) MME 发送 Authentication Data Request 消息给 HSS，消息中需要包含 IMSI，网络 ID，如 MCC + MNC 和网络类型，如 E-UTRAN

2) HSS 收到 MME 的请求后，使用 authentication response 消息将鉴权向量发送给 MME

3) MME 向 UE 发送 User Authentication Request 消息，对用户进行鉴权，消息中包含 RAND 和 AUTN 这两个参数

4) UE 收到 MME 发来的请求后，先验证 AUTN 是否可接受， UE 首先通过对比自己计算出来的 XMAC 和来自网络的 MAC （包含在 AUTN 内）以对网络进行认证，如果不一致，则 UE 认为这是一个非法的网络。如果一致，然后计算 RES值，并通过 User Authentication Response 消息发送给 MME 。MME 检查 RES 和 XRES 的是否一致，如果一致，则鉴权通过。

EPS鉴权向量由 RAND 、AUTN 、XRES和 KASME 四元组组成。 EPS鉴权向量由 MME 向 HSS 请求获取。 EPS鉴权四元组：

l RAND （Random Challenge ）：RAND 是网络提供给 UE 的不可预知的随机数，长度为 16 octets 。

l AUTN （Authentication Token ）：AUTN 的作用是提供信息给 UE，使 UE 可以用它来对网络进行鉴权。 AUTN 的长度为 17octets

l XRES（Expected Response ）：XRES 是期望的 UE 鉴权响应参数。用于和 UE 产生的 RES(或 RES+RES_EXT)进行比较，以决定鉴权是否成功。 XRES的长度为 4-16 octets 。

l KASME 是根据 CK/IK 以及 ASME （MME ）的 PLMN ID 推演得到的一个根密钥。 KASME 长度 32octets 。

l ASME 从 HSS 中接收顶层密钥，在 E-UTRAN 接入模式下， MME 扮演 ASME 的角色。

l CK ：为加密密钥， CK 长度为 16 octets 。

l IK ：完整性保护密钥，长度为 16 octets 。

在鉴权过程中， MME 向 USIM 发送 RAND 和 AUTN ， USIM 可以决定返回 RES还是拒绝鉴权。

1. MME 发起 AUTH REQ 消息，携带鉴权相关信息 RAND 和 AUTN ；

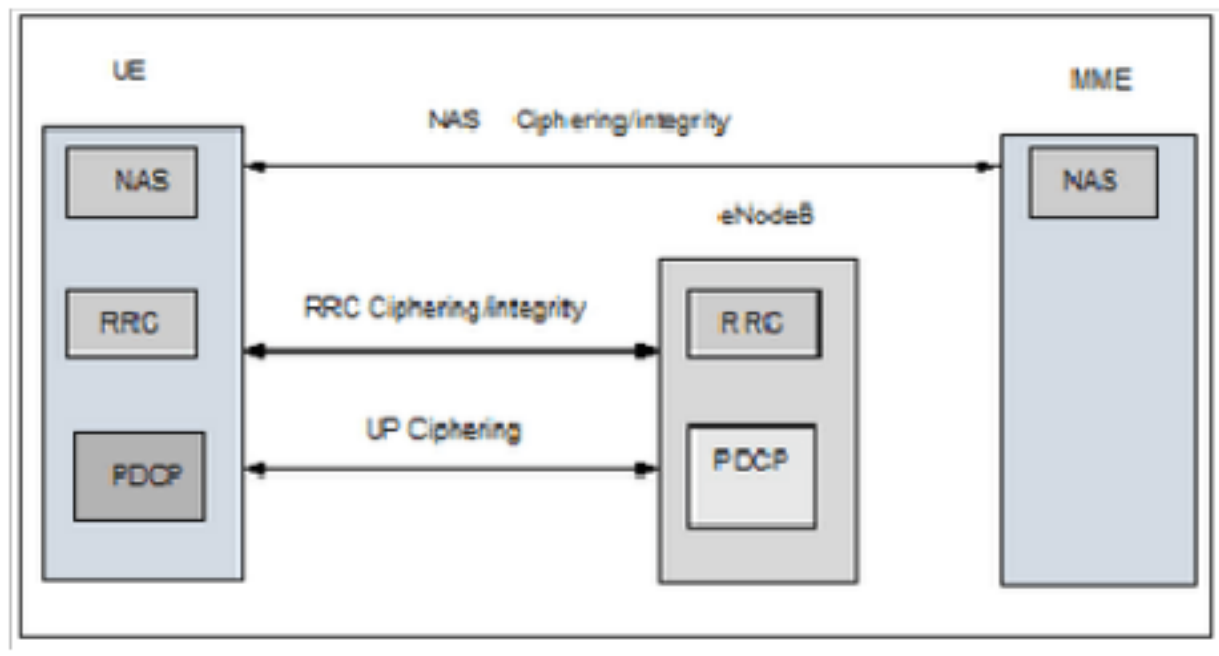
第一条 S1AP_DL_NAS_TRANS

2. UE 收到 AUTH REQ 消息后回复 AUTH RES（携带 RES 参数）。

第一条 S1AP_UL_NAS_TRANS

3. MME 收到 AUTH RES 后，触发安全模式流程，否则返回 AUTH REJ 消息。

EPS的安全架构如下：

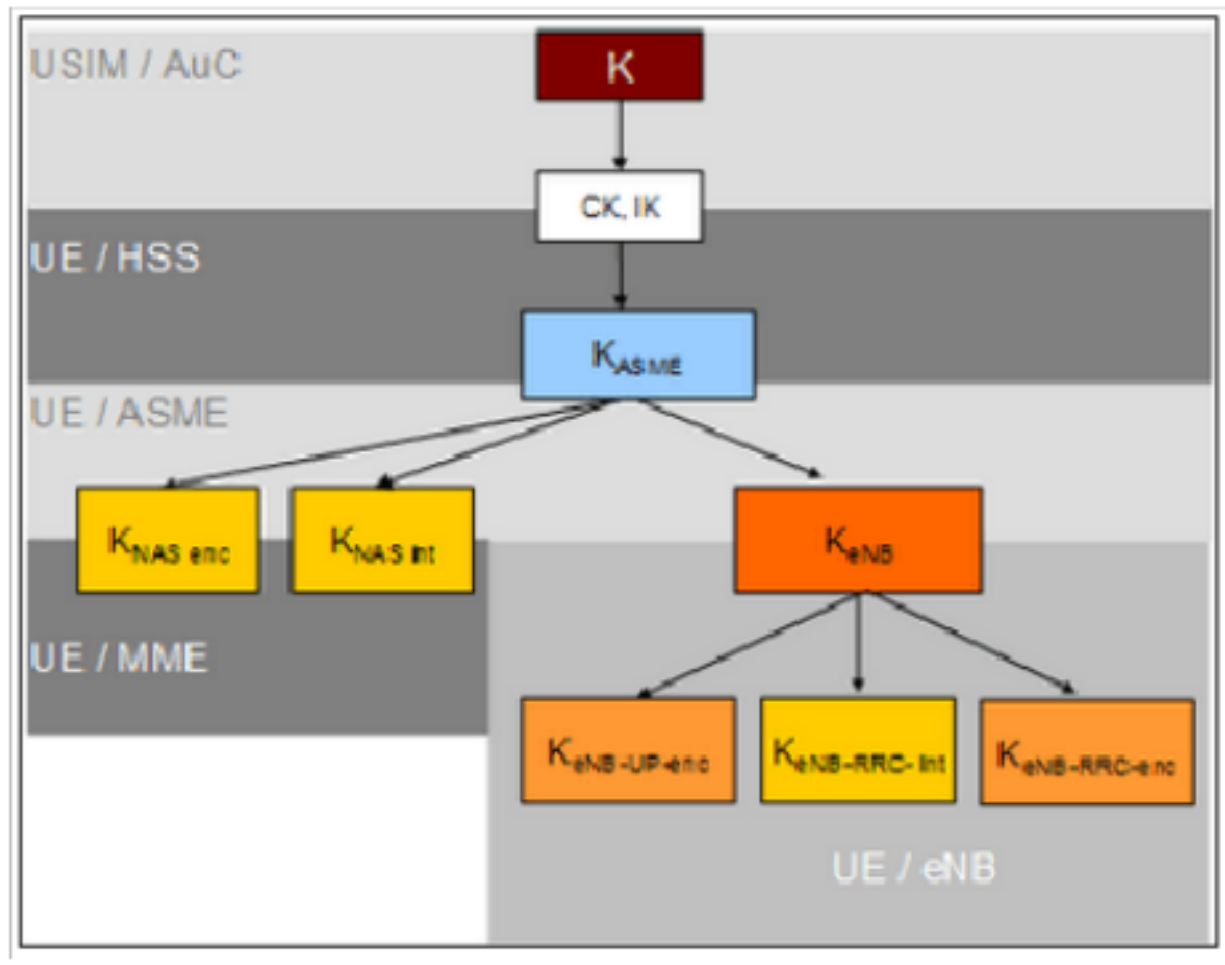


EPS安全架构中有相互独立的分层安全：

MME 和 UE 执行 NAS（ Non-access stratum ，非接入层）信令加密和完整性保护。

eNodeB 和 UE 执行 RRC 信令加密和完整性保护， UP 加密。

E-UTRAN 里的密钥层次架构：



密钥的层次架构里包含以下密钥 ：KeNodeB, KNASint, KNASenc, KUPenc, KRRCint 和 KRRCenc

- KeNodeB 是由 UE 和 MME 各自根据 KASME 计算得到的，可用于派生 KRRCint、KRRCenc 和 KUPenc，发生切换时也可用于派生 KeNodeB* 。在初始连接建立时，由 UE 和 MME 分别从 E-UTRAN 的顶层密钥中派生出来的。

KeNodeB* 是由 UE 和源 eNodeB 根据目的物理小区号、下行频率、 KeNodeB（或新 NH）派生出来，并在切换后被 UE 和目的 eNodeB 用作新的 KeNodeB 。NH （Next Hop ）是用于在 UE 和 eNodeB 中派生 KeNodeB* 。当安全上下文建立时， NH 由 UE 和 MME 从 KeNodeB 派生出来；当发生切换时，从上一个 NH 派生出来。

- NAS 信令的密钥：

- KNASint 是用于 NAS 信令完整性保护的密钥 ,是由 UE 和 MME 各自根据双方协商的完整性算保护算法计算得到的 .

- KNASenc 是用于 NAS 信令加密的密钥 ,是由 UE 和 MME 各自根据双方协商的加密算法计算得到的 .

- 用户数据的密钥：

- KUP enc 是专门用于加密用户面数据的密钥，由 KeNodeB 派生出来，存在于 UE 和 eNodeB 中。

- RRC 信令的密钥：

- KRRC int 是用于保护 RRC 信令完整性的密钥，由 KeNodeB 派生出来，存在于 UE 和 eNodeB 中。

- KRRC enc 是用于加密 RRC 信令的密钥，由 KeNodeB 派生出来，存在于 UE 和 eNodeB 中。

4 UE 收到 SMC 消息后：

- 根据 SMC 消息中的 Selected NAS security algorithms 信元计算出 KnasEnc 和 KnasInt 密钥；

- 校验信元 UE security capabilities 和 KSI 是否合法，如果合法，则回复 MME SECURITY MODE COMPLETE 消息，否则返回 SECURITY MODE REJECT消息。

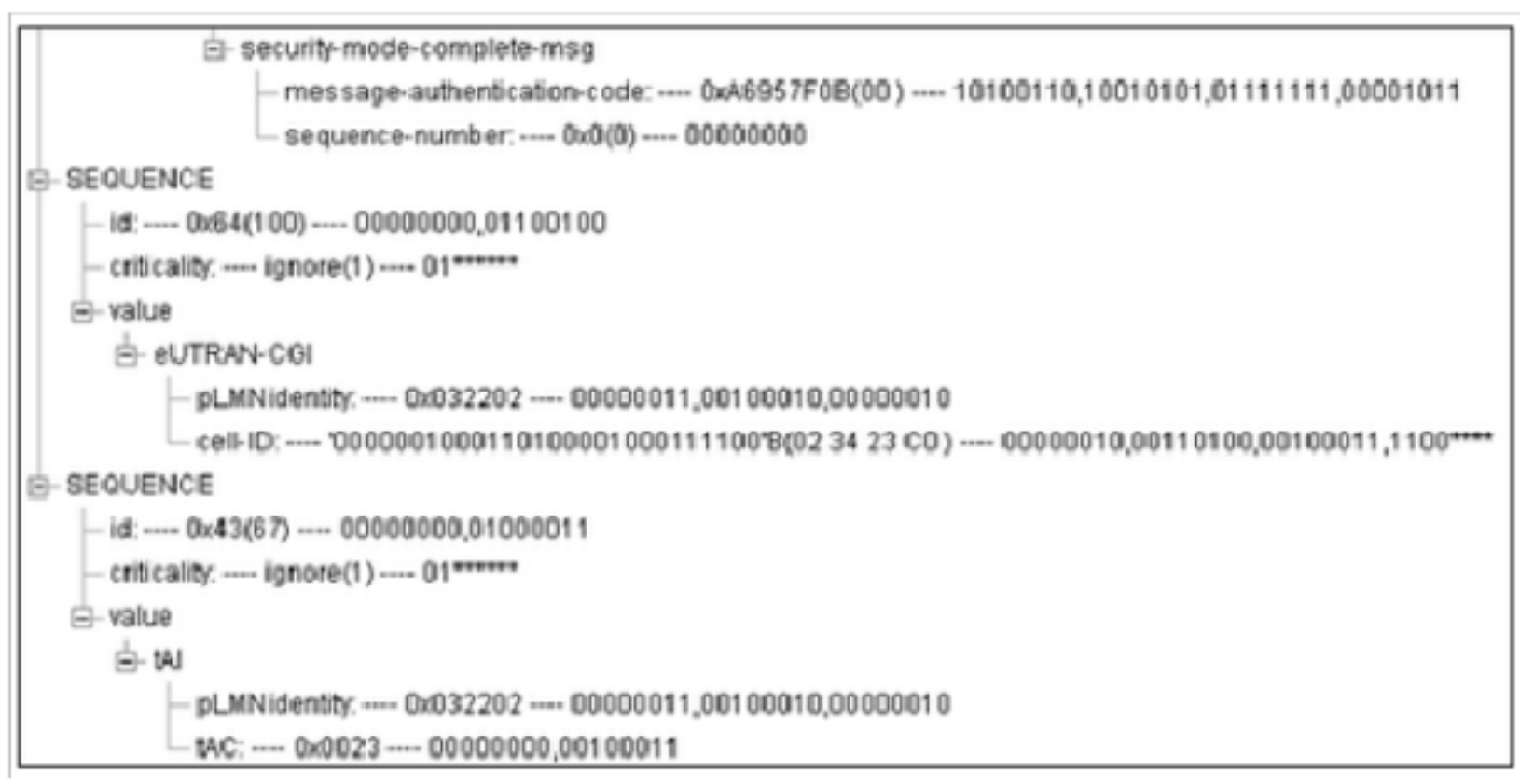
第二条 S1AP_DL_NAS_TRANS

应用完整性保护和加密特性时，要求 UE 和 MME 满足 33.401 的如下要求：

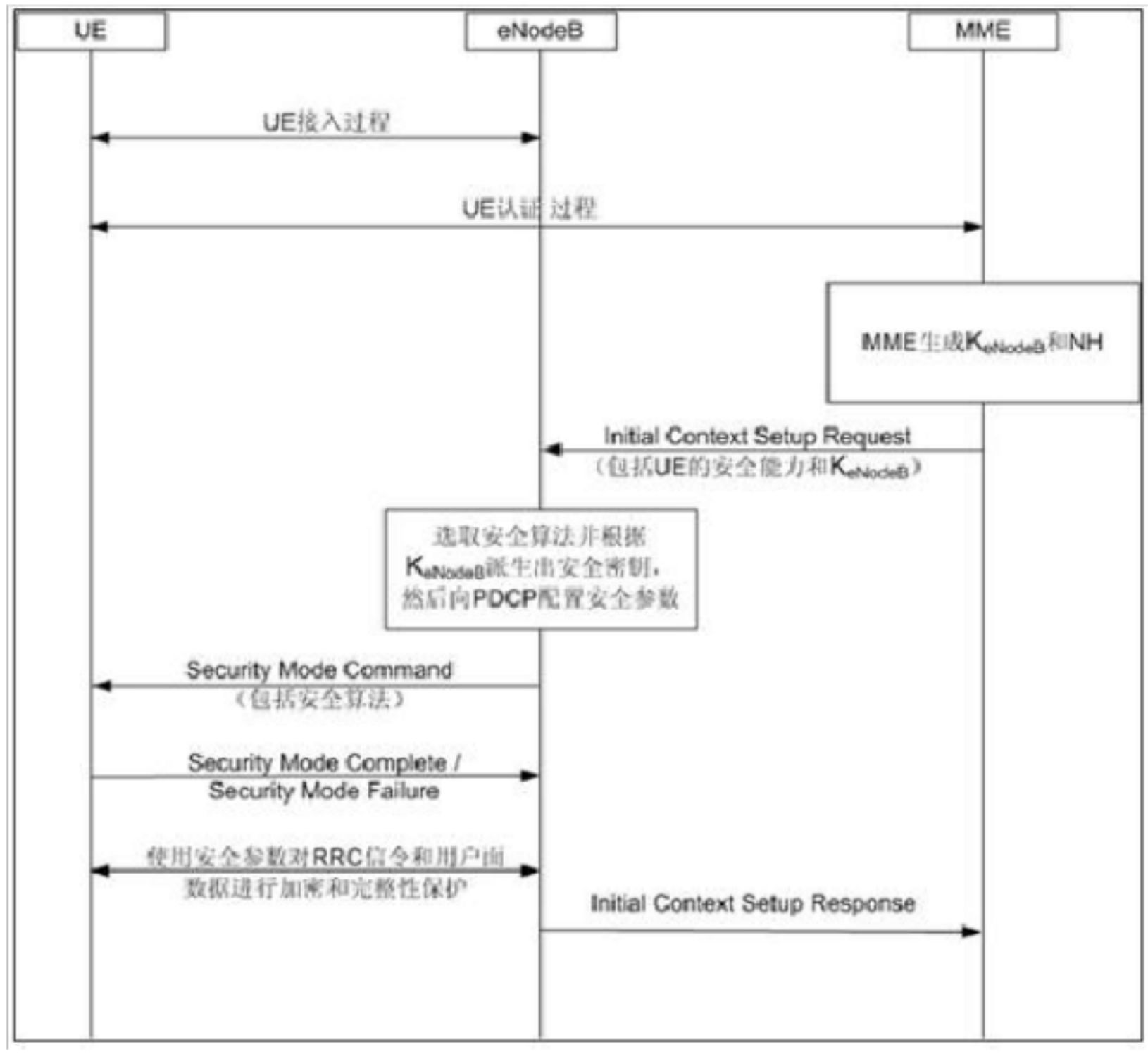
- 对于 NAS 信令加密， UE 和 MME 需支持 128-EEA0 （NULL ）， 128-EEA1 （Snow3G ）和 128-EEA2 （AES）。
- 对于 NAS 信令的完整性保护， UE 和 MME 需支持 128-EIA1 （Snow3G ）和 128-EIA2 （AES）。
- （可选） UE 和 MME 支持 128-EIA0 （NULL）。对于未经认证的紧急呼叫，未要求必须支持，即使 MME 和 eNodeB 部署了 128-EIA0 （NULL ）的配置也将失效。

无线侧的完整性保护和加密保护功能在 eNodeB 配置，对 eNodeB 上所有小区有效。

第二条 S1AP_UL_NAS_TRANS



eNodeB 通过 Security Mode Command 通知 UE 启动完整性保护和加密过程，UE 通过消息中的安全算法计算获取密钥。此时下行加密已开始。



1) RRC 连接建立完成后， MME 生成 KeNodeB 和 NH，并向 eNodeB 发送 UE 的安全能力和 KeNodeB 。安全能力包含 UE 支持的加密算法和完整性算法。

2) eNodeB 将完整性保护算法优先级列表和 UE 安全能力取交集，选取优先级最高的完整性算法。

3) eNodeB 将加密算法优先级列表和 UE 安全能力取交集，选取优先级最高的加密算法。

4) eNodeB 根据 KeNodeB 和选取的安全算法来计算出 KUP enc， KRRC int 和 KRRC enc 密钥，并为 PDCP 配置相应的加密参数和完整性参数。

5) eNodeB 通过 Security Mode Command 消息向 UE 发送安全模式参数配置。 Security Mode Command 消息通过 SRB1 发送，由 eNodeB 进行完整性保护，没有加密保护。

6) eNodeB 接收到 UE 反馈的消息 .