

Integrity and Confidentiality Algorithms for UE

This chapter describes the implementation of Integrity and Confidentiality Algorithms for UEs in Liminted Service Mode (LSM), and UEs that cannot be authenticated by the MME, to establish emergency calls.

- Feature Description, on page 1
- Configuration Information, on page 2

Feature Description

In this feature, UEs that are in limited service mode (LSM) and UEs that cannot be authenticated by the MME are allowed to establish emergency calls.

MME uses EEA0 (Integrity) and EIA0 (Ciphering) algorithms for emergency attach requests even if the UE does not advertise the support of these algorithms in the request message, to successfully process the VoLTE emergency calls. These algorithms successfully process the VoLTE calls irrespective of the validation level configured for a UE.

The MME provides options to authenticate emergency attaches using the following CLI:

```
ue-validation-level { auth-only | full | imsi | none }
```

Using the above command syntax, it is possible to configure the MME to allow or disallow unauthenticated UEs in LSM to establish bearers for emergency calls. To establish bearers for an emergency call for unauthenticated UEs in LSM, the MME allows NAS protocol to use EIA0 and EEA0 as the integrity and ciphering algorithm respectively.

If the MME allows an unauthenticated UE in LSM to establish bearers for emergency calls on receiving an emergency attach request message from the UE, the MME:

- Selects an algorithm based on the UE's announcement only if the MME supports the requested algorithm. If the MME does not support the requested algorithm or if there is no algorithm announced, then the EEA0 and EIA0 algorithms are used.
- Set the UE EPS security capabilities to only contain EIA0 and EEA0 when sending these to the eNB in the following messages:
  - S1 UE INITIAL CONTEXT SETUP
  - S1 UE CONTEXT MODIFICATION REQUEST
  - S1 HANDOVER REQUEST

Note As a result, the MME only sends a UE with EPS security capability containing EIA0 and EEA0 to the eNB when selecting EIA0 for NAS integrity protection because the eNB is only capable of selecting EIA0 for AS integrity protection and EEA0 for AS confidentiality protection. In general, if EIA0 is used for NAS integrity protection, then EIA0 will always be used for AS integrity protection or vice-versa

The rules for when the MME selects the EIA0 for NAS integrity protection, and when the UE accepts a NAS security mode command selecting EIA0 for NAS integrity protection depends on whether the UE and MME can be certain that no EPS NAS security context can be established. For more information on these rules, refer to *3GPP 33.401 specifications* document.

Configuration Information

The MME provides options to authenticate emergency attaches using the following CLI:

`ue-validation-level { auth-only | full | imsi | none }`

- The ***auth-only*** keyword specifies that only authenticated UEs are allowed to use the emergency bearer services.
- The ***full*** keyword specifies that only UEs that have been authenticated, and have successfully passed subscription and location validation, are allowed to use the emergency bearer services.
- The ***imsi*** keyword specifies that UEs with an International Mobile Subscriber Identity are allowed to use the emergency bearer services regardless of authentication. Even if authentication fails, the UE is granted access to use emergency bearer services.
- The ***none*** keyword specifies that all UEs are allowed to use the emergency bearer services. This keyword is used as a default option.