



## 6.5 Access link data integrity

### 6.5.1 General

Most control signalling information elements that are sent between the MS and the network are considered sensitive and must be integrity protected. A message authentication function shall be applied on these signalling information elements transmitted between the UE and the RNC.

After the RRC connection establishment and execution of the security mode set-up procedure, all dedicated MS <-> network control signalling messages (e.g. RRC, MM, CC, GMM, and SM messages) shall be integrity protected. The Mobility Management layer in the MS supervises that the integrity protection is started (see section 6.4.5).

All signalling messages except the following ones shall then be integrity protected:

- Paging Type 1
- RRC Connection Request
- RRC Connection Setup
- RRC Connection Setup Complete
- RRC Connection Reject
- System Information (broadcasted information).
- Handover to UTRAN complete

### 6.8.4 Intersystem handover for CS Services – from UTRAN to GSM BSS

If ciphering has been started when an intersystem handover occurs from UTRAN to GSM BSS, the necessary information (e.g. Kc, supported/allowed GSM ciphering algorithms) is transmitted within the system infrastructure before the actual handover is executed to enable the communication to proceed from the old RNC to the new GSM BSS, and to continue the communication in ciphered mode. The intersystem handover will imply a change of ciphering algorithm from a UEA to a GSM A5.

The integrity protection of signalling messages is stopped at handover to GSM BSS.

The highest hyperframe number value reached for all signaling and user data bearers during the RRC connection shall be stored in the UE/USIM at handover to GSM BSS.

### 6.8.5 Intersystem handover for CS Services – from GSM BSS to UTRAN

If ciphering has been started when an intersystem handover occurs from GSM BSS to UTRAN, the necessary information (e.g. CK, IK, initial HFN value information, supported/allowed UMTS algorithms) is transmitted within the system infrastructure before the actual handover is executed to enable the communication to proceed from the old GSM BSS to the new RNC, and to continue the communication in ciphered mode. The intersystem handover will imply a change of ciphering algorithm from a GSM A5 to a UEA.

The integrity protection of signalling messages shall be started immediately after that the intersystem handover from GSM BSS to UTRAN is completed. The Serving RNC will do this by initiating the RRC security mode control procedure when the first RRC message (i.e. the Handover to UTRAN complete message) has been received from the UE. The UE security capability information, that has been sent from UE to RNC via the GSM radio access and the system infrastructure before the actual handover execution, will then be included in the RRC Security mode command message sent to UE and then verified by the UE (i.e. verified that it is equal to the UE security capability information stored in the UE).