

6.4.2 Ciphering and integrity mode negotiation

When an MS wishes to establish a connection with the network, the MS shall indicate to the network in the MS/USIM Classmark which cipher and integrity algorithms the MS supports. The ciphering algorithms respective the integrity algorithms that the MS supports shall be indicated in the order of algorithm preferences, given by the USIM. This information itself must be integrity protected. As it is the case that the RNC does not have the integrity key IK when receiving the MS/USIM Classmark this information must be stored in the RNC. The data integrity of the classmark is performed, during the security mode set-up procedure by use of the most recently generated IK (see section 6.4.5).

The network shall compare its integrity protection capabilities and preferences, and any special requirements of the subscription of the MS, with ~~these~~ integrity protection capabilities and preferences indicated by the MS and act according to the following rules:

- 1) If the MS and the SN have no versions of the UIA algorithm in common, then the connection shall be released.
- 2) If the MS and the SN have at least one version of the UIA algorithm in common, then the network shall select one of the mutually acceptable versions of the UIA algorithm for use on that connection. The network shall then take into account the UIA preferences of the MS and select among the common UIAs the most preferred UIA of the MS.

The network shall compare its ciphering capabilities and preferences, and any special requirements of the subscription of the MS, with ~~these~~ ciphering capabilities and preferences indicated by the MS and act according to the following rules:

- 1) If the MS and the network have no versions of the UEA algorithm in common and the network is not prepared to use an unciphered connection, then the connection shall be released.
- 2) If the MS and the network have at least one version of the UEA algorithm in common, then the network shall select one of the mutually acceptable versions of the UEA algorithm for use on that connection. The network shall then take into account the UEA preferences of the MS and select among the common UEAs the most preferred UEA of the MS.
- 3) If the MS and the network have no versions of the UEA algorithm in common and the user (respectively the user's HE) and the SN are willing to use an unciphered connection, then an unciphered connection shall be used.

Because of the separate mobility management for CS and PS services, one CN domain may, independent of the other CN, establish a connection to one and the same MS. Change of ciphering and integrity mode (algorithms) at establishment of a second MS to CN connection shall not be permitted. The preferences and special requirements for the ciphering and integrity mode setting shall be common for both domains. (e.g. the order of preference of the algorithms).