16-124-836
Marcel Matti ZAUDER

9.2 Question 2

9.2.A How do GSM and UMTS devices authenticate their network (*i.e. ensure a connection to a legit network*).

GSM
Both the device and the AUC contain the authentication key K_i. In order to be authenticated the subscriber is challenged by given a random number. With this random number and the authentication key as input for the one-way function A3 a signature response (SRES) is returned. Both results from the subscriber as well from the AUC are compared on the network side and on matching the subscriber is authenticated.
UMTS
UMTS is an improved version of GSM in order to provide mutual authentication and a network domain security.
As it is the case for GSM a persisten key is shared between the mobile equipment and the AUC. After a user was identified by the serving network with the use of IMSI or TMSI authentication vectors are created by the AUC based on the IMSI. These are then sent to the VLR or SGSN. The terminal is then requested for an authentication using a randfom number and the AUTN from the authentication vector. By replicating the computation the USIM can verify that AUTN was actually generated by the AUC. If the response of the USIM and the expected response of the authentication vector match the authentication is performed successfully.