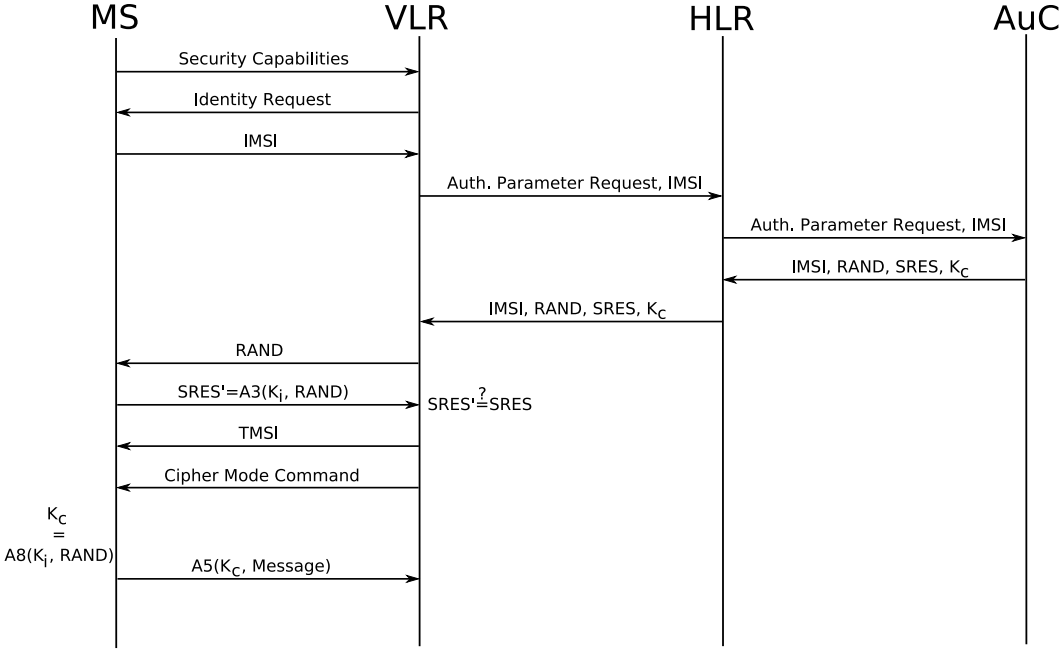
MS
VLR
HLR
AuC
Security Capabilities
Identity Request
IMSI
Auth. Parameter Request, IMSI
Auth. Parameter Request, IMSI
IMSI, RAND, SRES, K_C
IMSI, RAND, SRES, K_C
RAND
SRES'=A3(K_i, RAND)
SRES'$\stackrel{?}{=}$SRES
TMSI
Cipher Mode Command
K_C = A8(K_i, RAND)
A5(K_C, Message)