UE
gNB
1. Signed MIB/SIB1
Idle mode
2. Verify SI signature
3. Generate K
Go on with standard communication flow only if UE selects gNB
4. E(PK, K)
5. Hash(K)
6a. Start timer Ta
6b. Start timer Tb
MitM/replay detection part
7a. Activate C-CRC method with K
7b. Activate C-CRC method with K
8. Protocol flow C-CRC protected
9a. Timeout if Ta > Tmax and message 10 not sent
9b. Timeout if Tb > Tmax and message 10 not received
10. Final message
11a. Deactivate C-CRC method with K
11b. Deactivate C-CRC method with K
12. Standard communication