UE
gNB
AMF
DSnF
1. Signing_Request (PCI, MIB[SFN=0], SIB1)
2.a Generate a key chain
seed
h0
h1
h63
h64
Anchor Key
2.b. Compute digital signature S over (PCI, MIB, SIB1, T, h64)
3. Signing_Response (T, seed, S)
4.a Generate the key chain from "seed"
seed
4.b. Compute MACs for SFNs where SFN=0, 16, 32, ..., 1008 using the hash chain in reverse order starting from h63
h0 + SFN=1008 = MAC63
h1 + SFN=992 = MAC62
h63 + SFN=0 = MAC0
Key used in reverse order
h64
Anchor Key
i=0
4.c. Broadcast MIB, SFN=i, may include MACi or a subset of MACi
4.d. Broadcast SIB1+MACi
4.e. Broadcast newSIB = T, h64, S, h(63-i)
i=i+1
i< 64 ?
yes
no
Need to obtain a new key chain, e.g., go back to step 1
5.a Acquire MIB+MACi
5.b Acquire SIB1+MACi
5.c Acquire newSIB
5.d verify signature S
5.e verify h(63-i) against h64
5.f verify MACi using h(63-i)
5.g verify time T+SFNx10ms