A keying Hierarchy for Managing Wireless Handover Security

draft-nakhjiri-hokey-hierarchy-02
IETF 67, Nov 2006

Madjid Nakhjiri

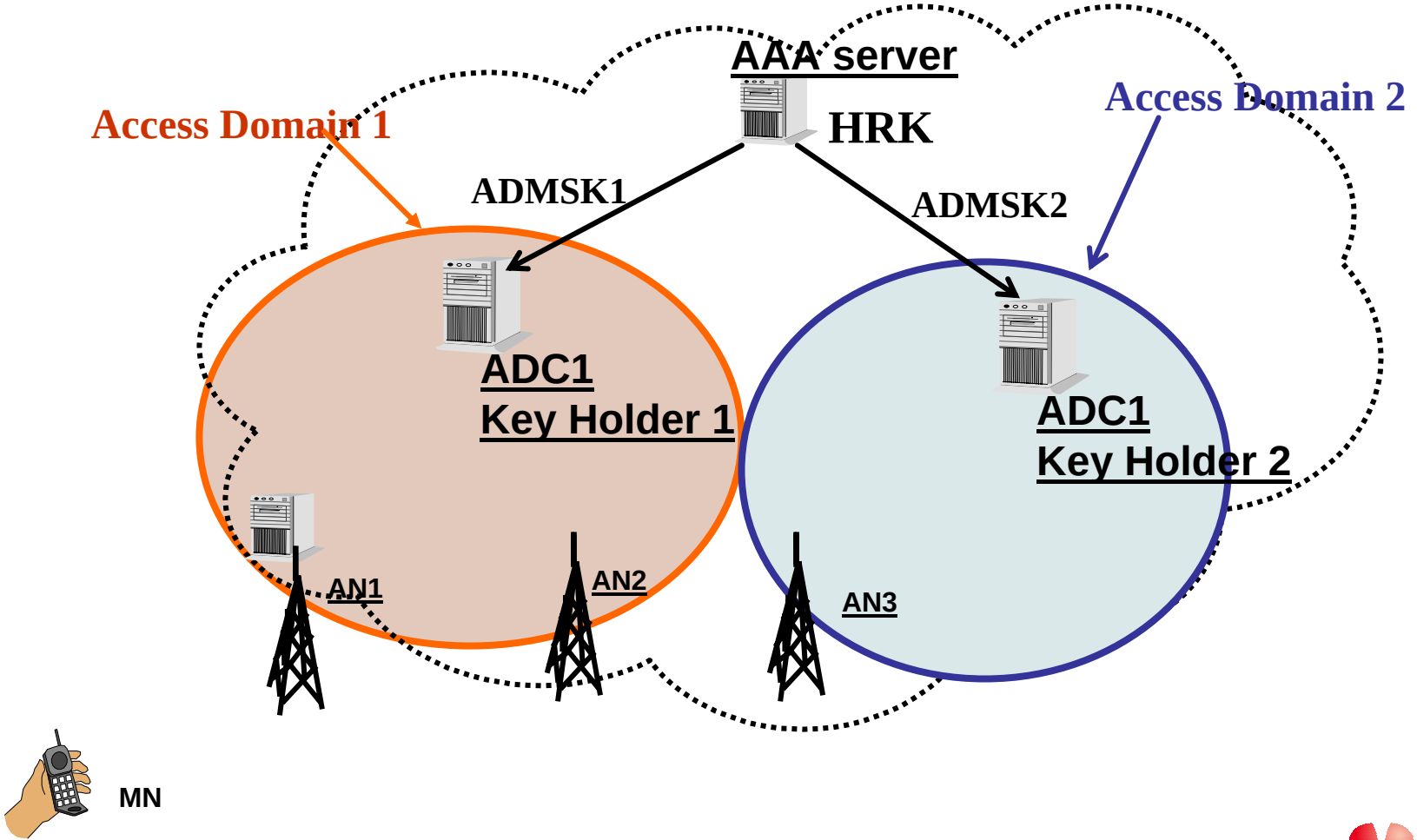
HUAWEI

Main Ideas
Key names in draft need to be updated

- HRK is derived from either MSK or EMSK (EMSK)
  - MSK is not used directly
  - PRF/KDF choice at EAP/AAA server (crypto-separation)
- AAA server is HRK Key Holder
  - HRK to create the Key hierarchy
    - Derive per-ADC keys (ADMSK)
    - Derive MN (AAA_REAUTH_KEY)
- ADC is ADMSK Key holder
  - Key hierarchy below ADC can use different KDF
- Allow physically separate ADC and ANs
  - ADC handles AN-handovers within Access Domain
  - Deeper key hierarchy/ Channel binding/ signaling

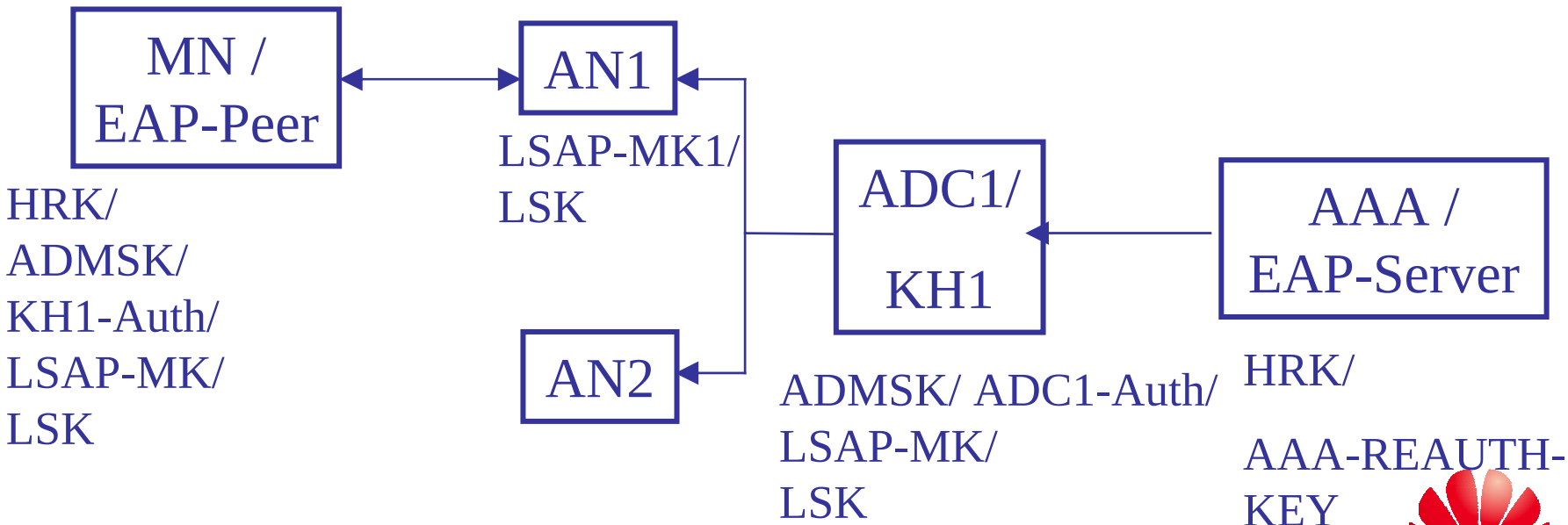
HUAWEI

Assumed architecture and Keying hierarchy

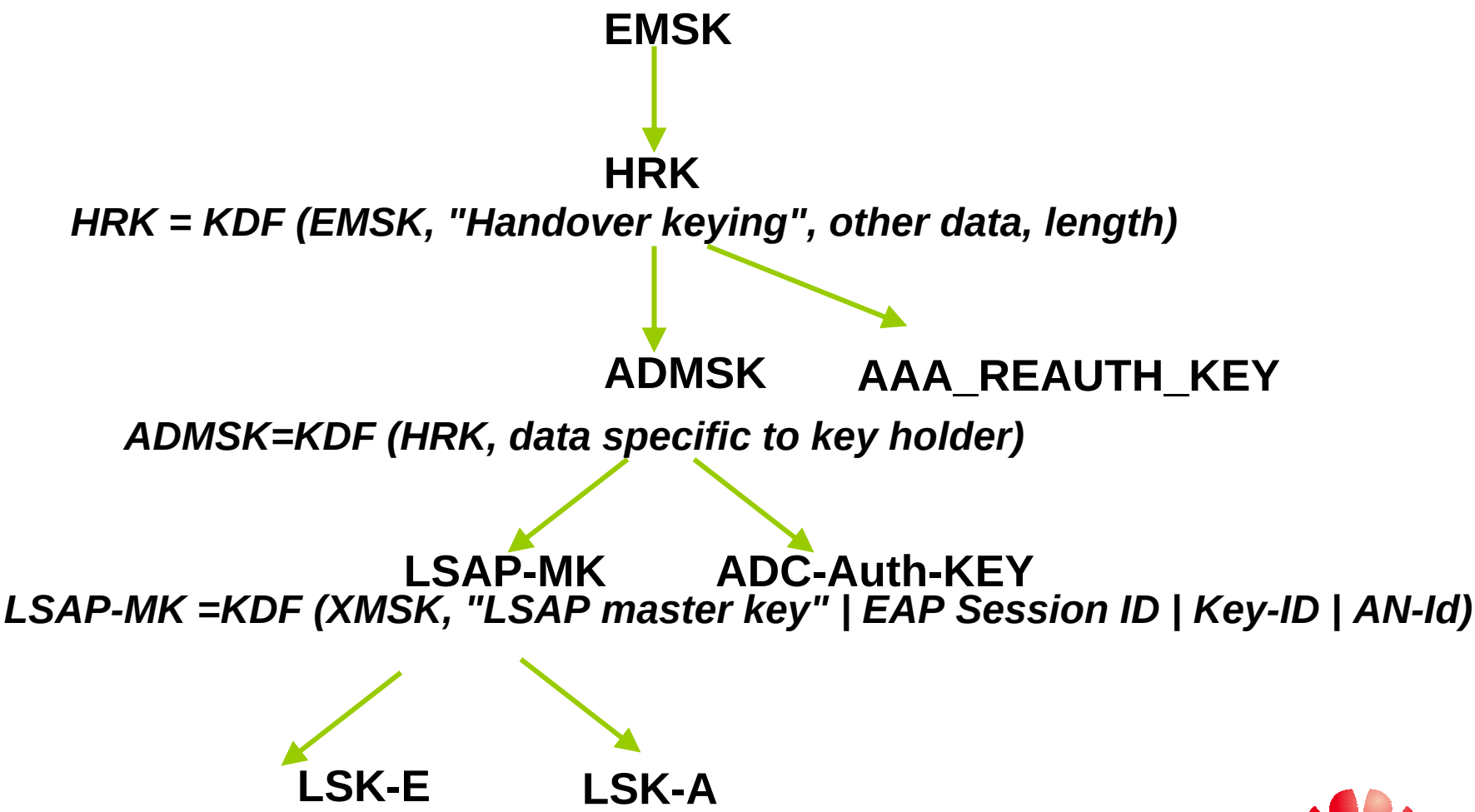


Proposed Key hierarchy/ caches

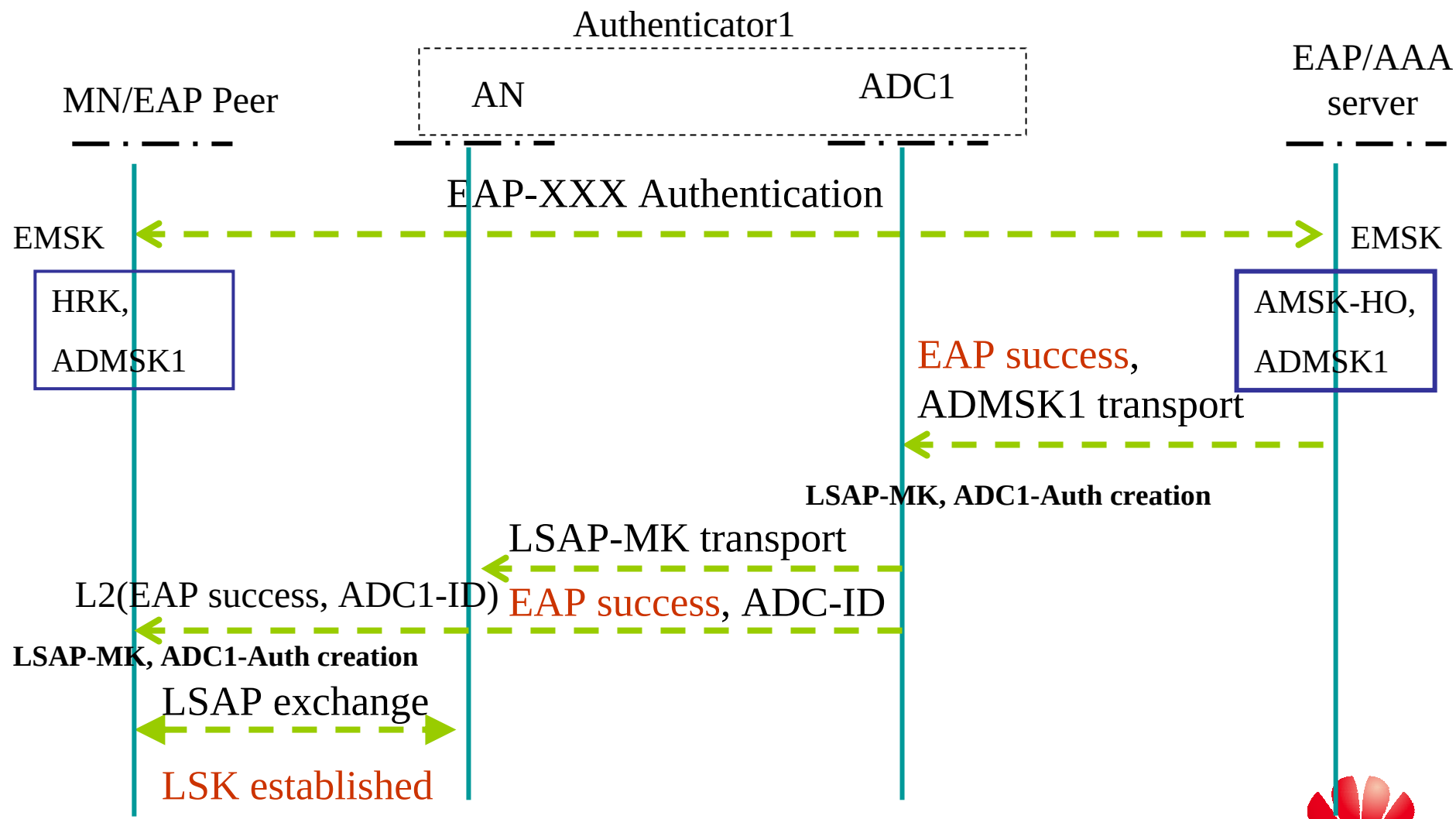
- AAA-REAUTH
  - Fast Re-authentication, ADC Handovers
- Intra-ADC AN handovers handled at ADC
  - No AAA interaction



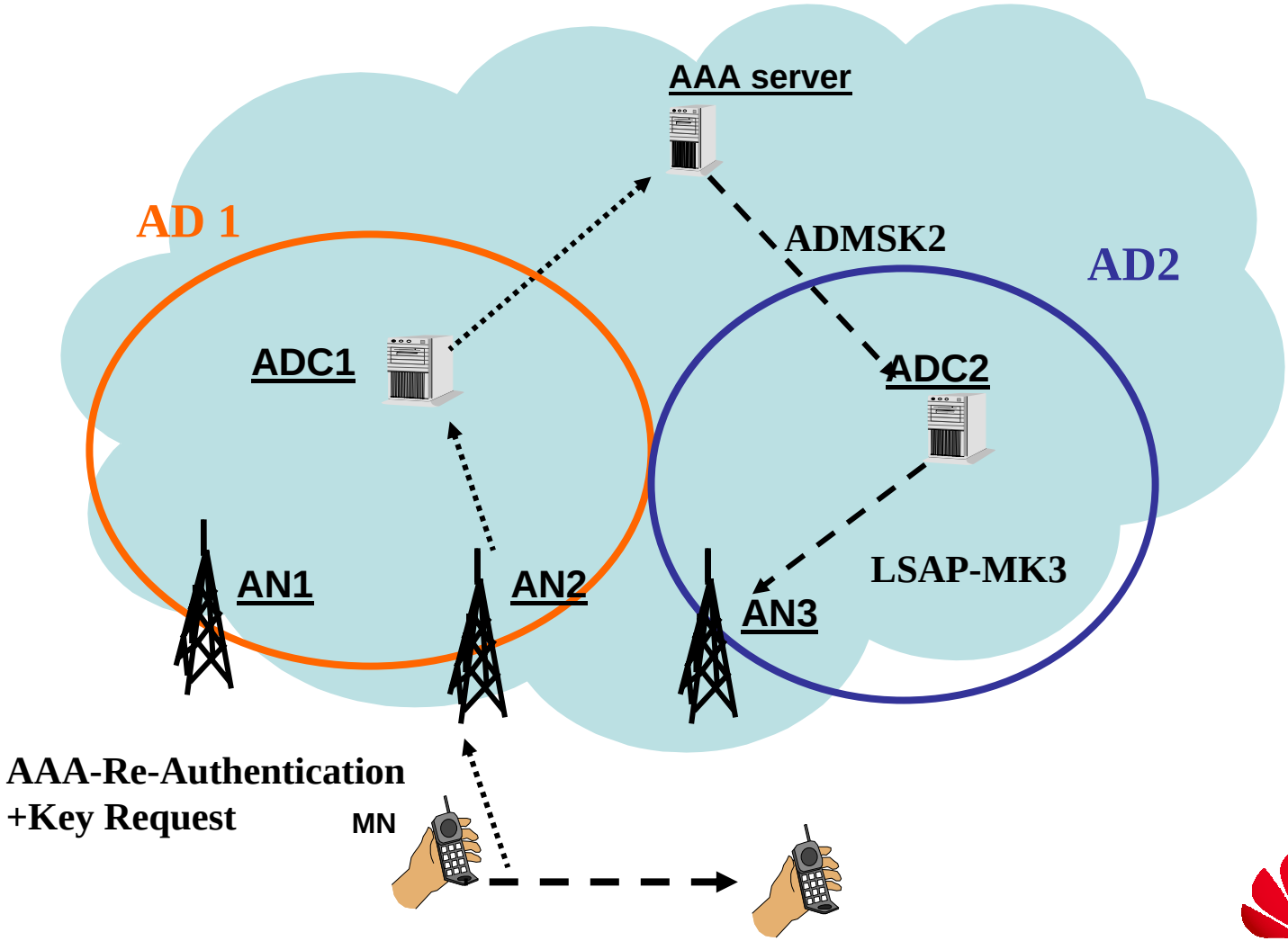
Key generation



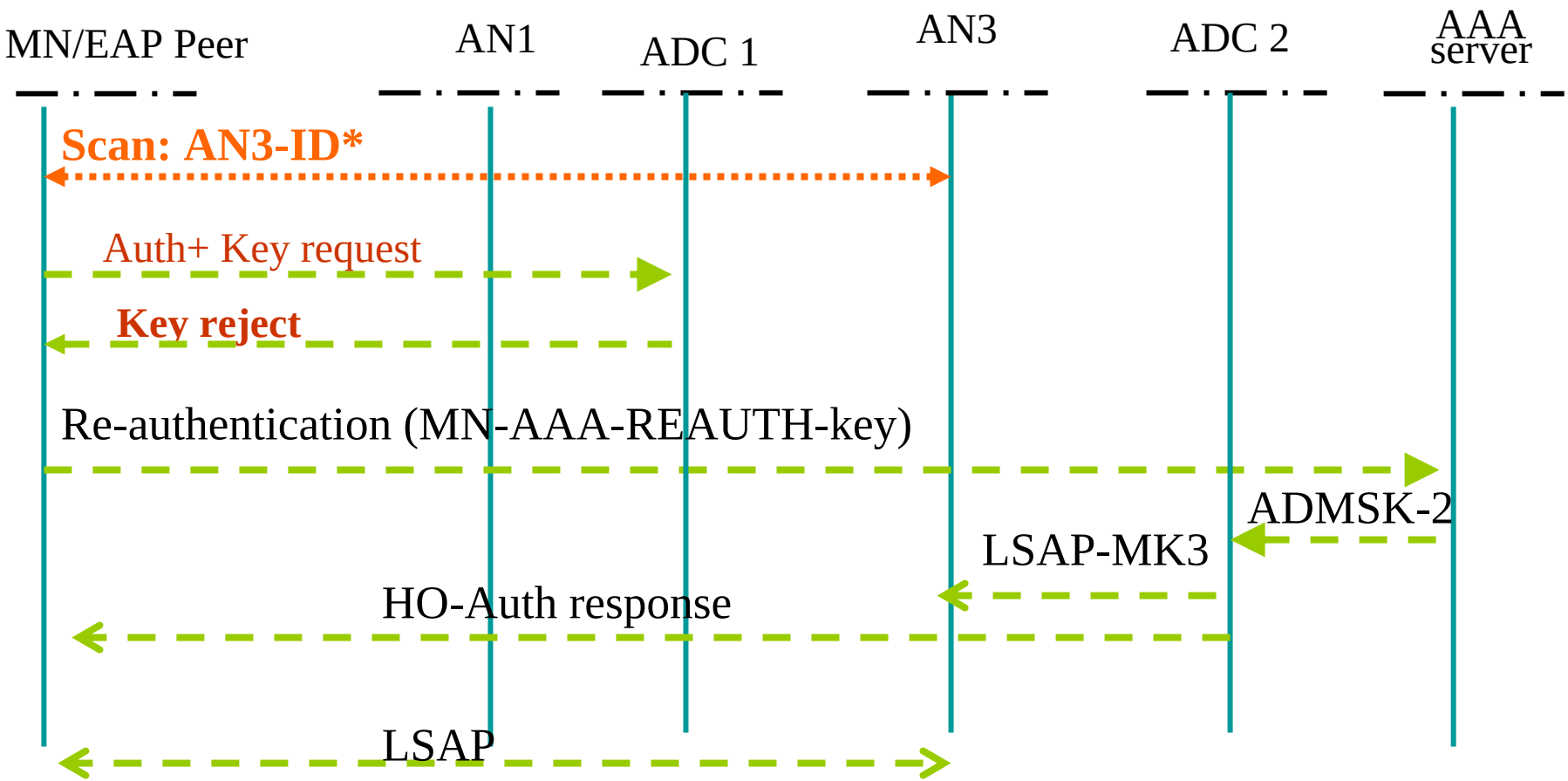
Keying during Initial entry



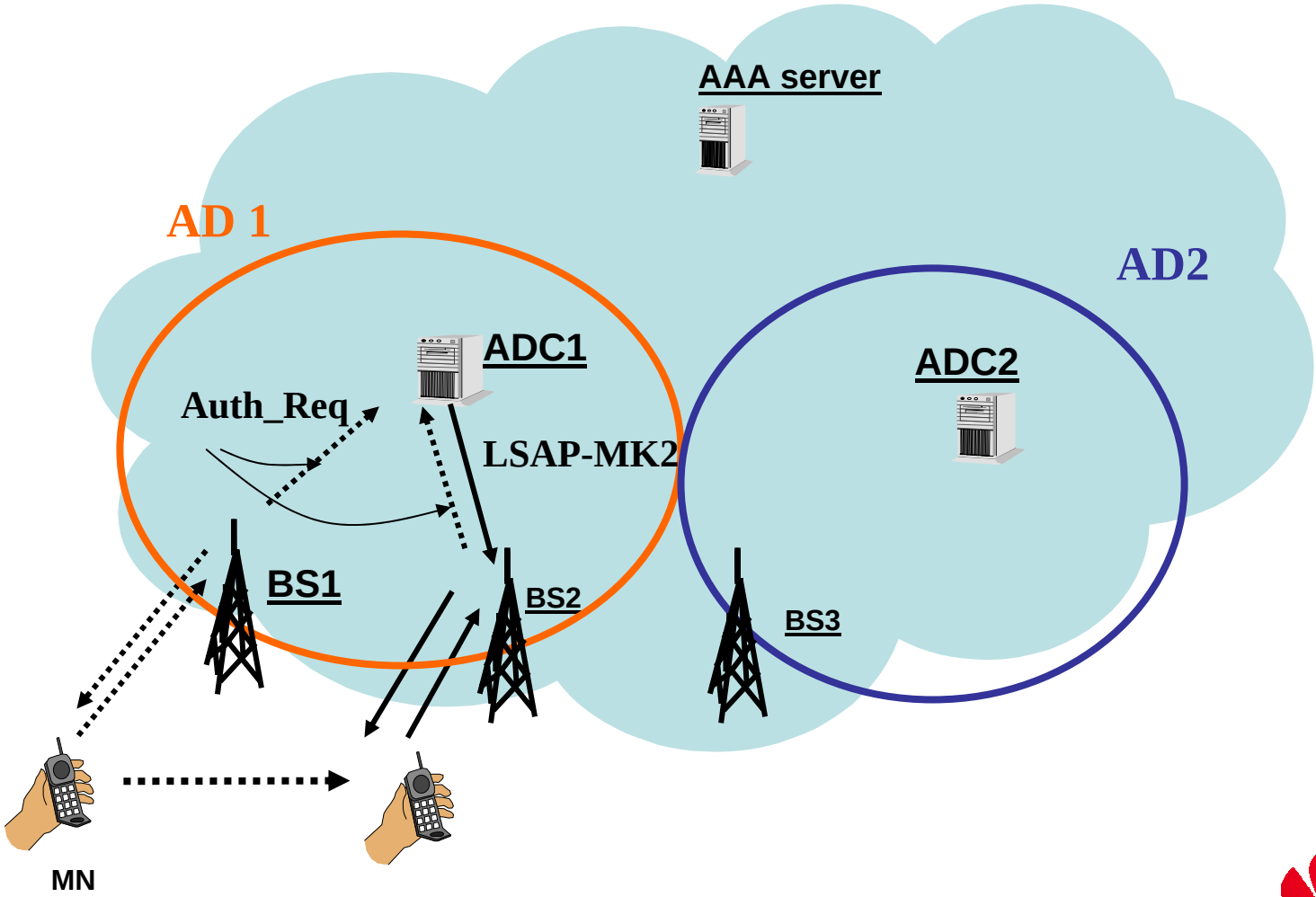
Inter-ADC handover scenario



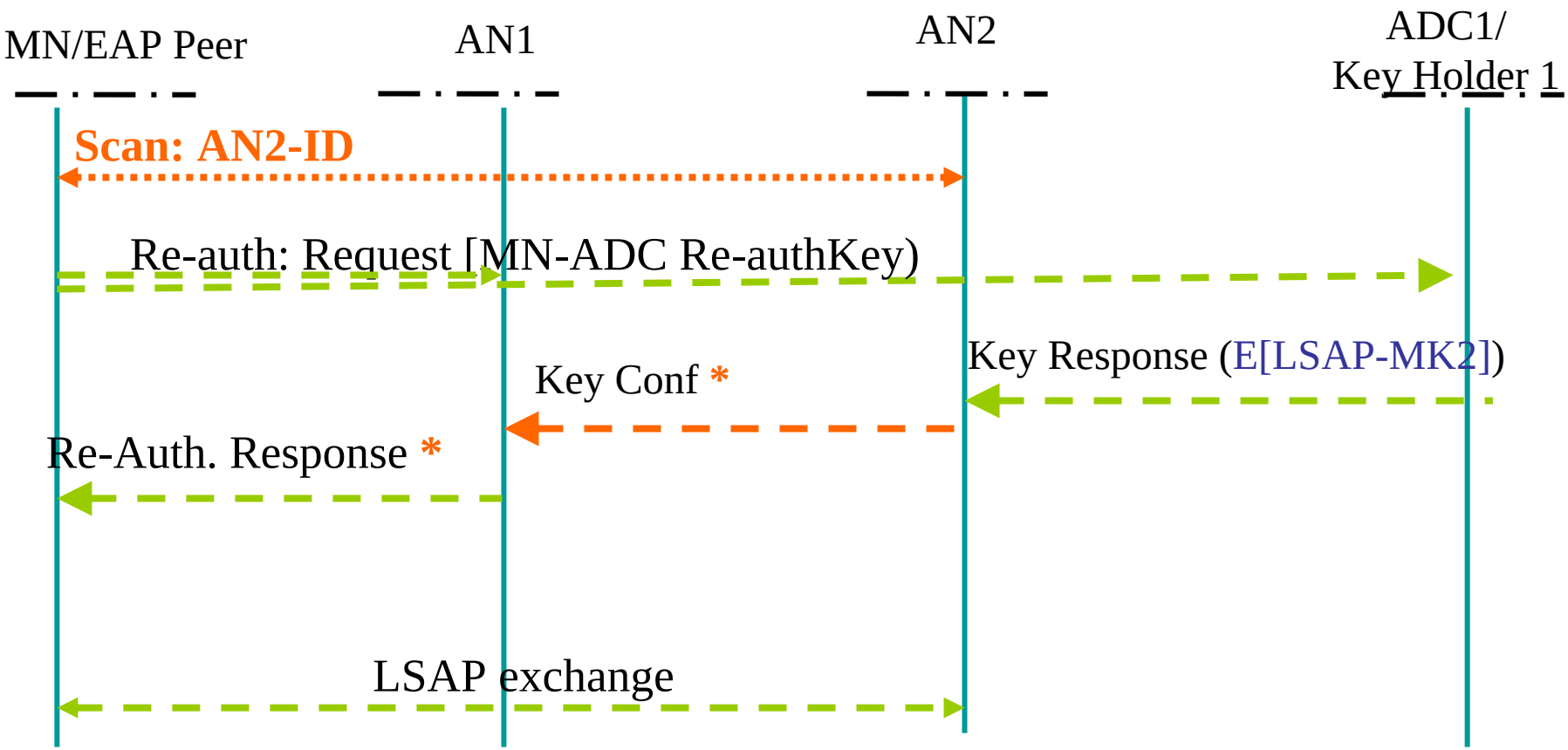
Inter-ADC Handover Keying/ AAA re-auth



Intra-ADC handover scenario



No interaction with AAA server during handover



E[X]=Encryption of X with (KH1, AN2) key.

Messaging with ADC through AN1 or AN2 depending on link availability.

HUAWEI

Bells and whistles

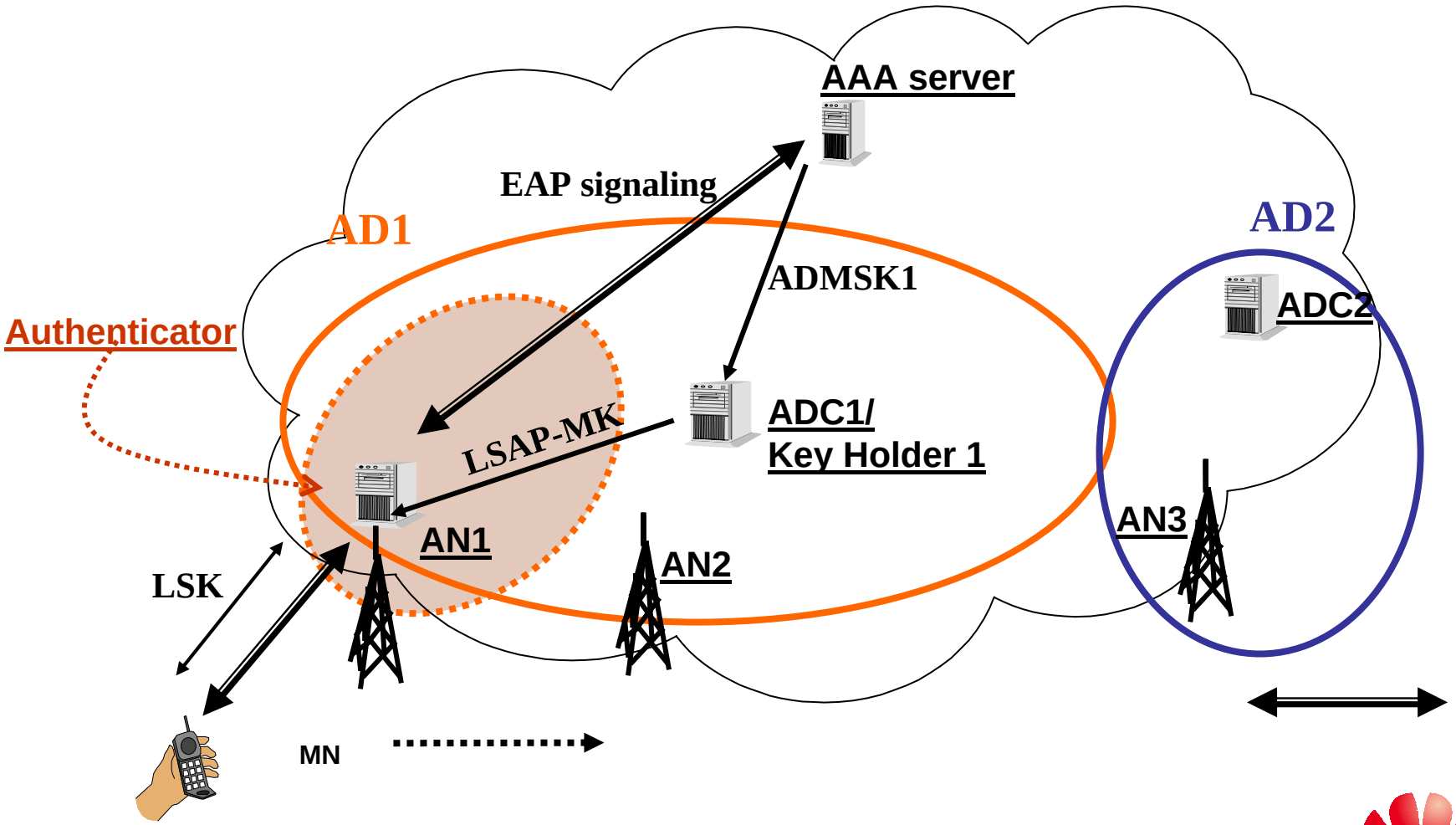
- Use different KDFs at different levels if needed
- Separation of ADC and ANs
  - Re-auths both at AAA level and local level
  - Inter-ADC handovers Intra-ADC handovers
  - Possibility of keying for multiple ANs (neighbor-lists)
- Key distribution messaging options
  - Proactive requests (through old AN)
  - Reactive requests (through new AN)
- Generic Channel binding solution
- Positioning of ADC outside authenticator
  - Getting ADC-ID to the AAA server

HUAWEI

To do

- Terminology
- Position of authenticator versus ADC
- Messaging definitions

Positioning of EAP authenticator wrt ADC (alternative 2)



HUAWEI

Positioning of EAP authenticator wrt ADC