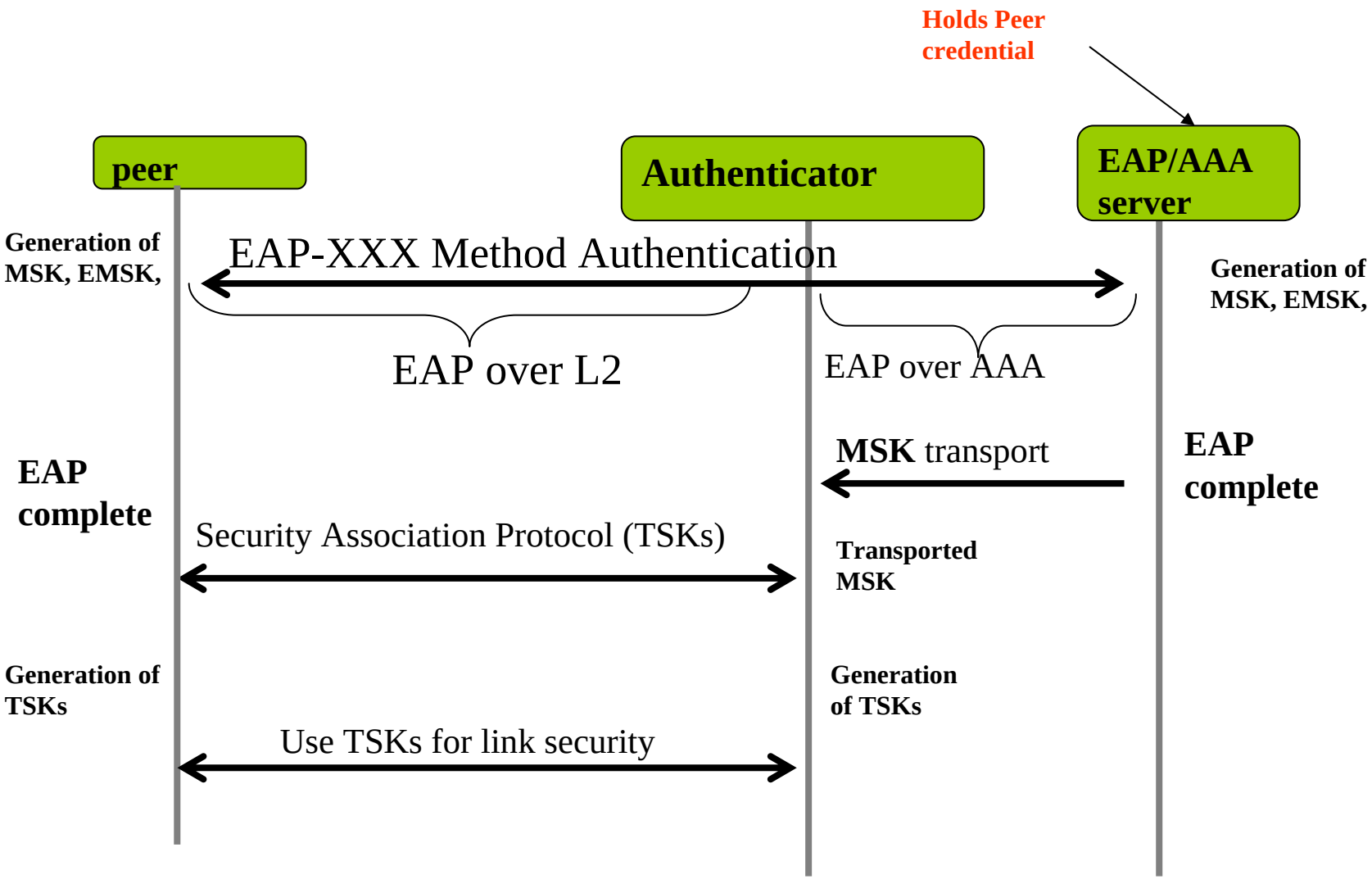
AAA based Keying for Wireless Handovers: Problem Statement

draft-nakhjiri-aaa-hokey-ps-03

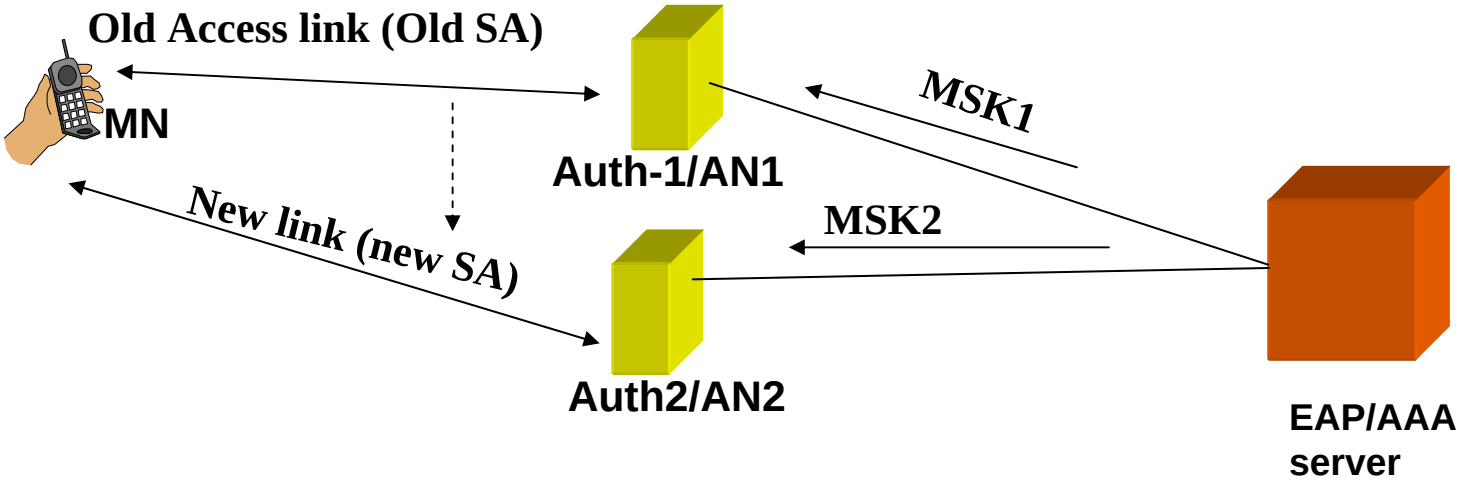
Madjid Nakhjiri (Huawei USA/Motorola Labs)
Mohan Parthasarathy (Nokia)
Julien Bournelle (GET/INT/FT)
Hannes Tschofenig (Siemens)
R. Marin Lopez (TARI)

IETF 67 San Diego

Slide from IETF 65: EAP Keying for fixed peers

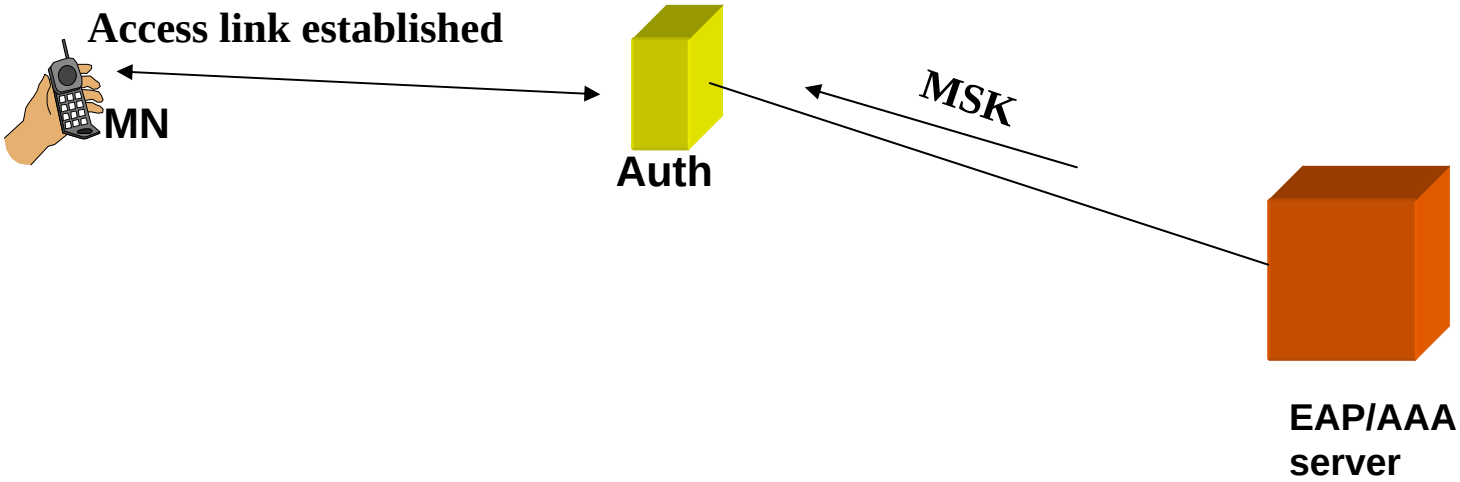


Mobility



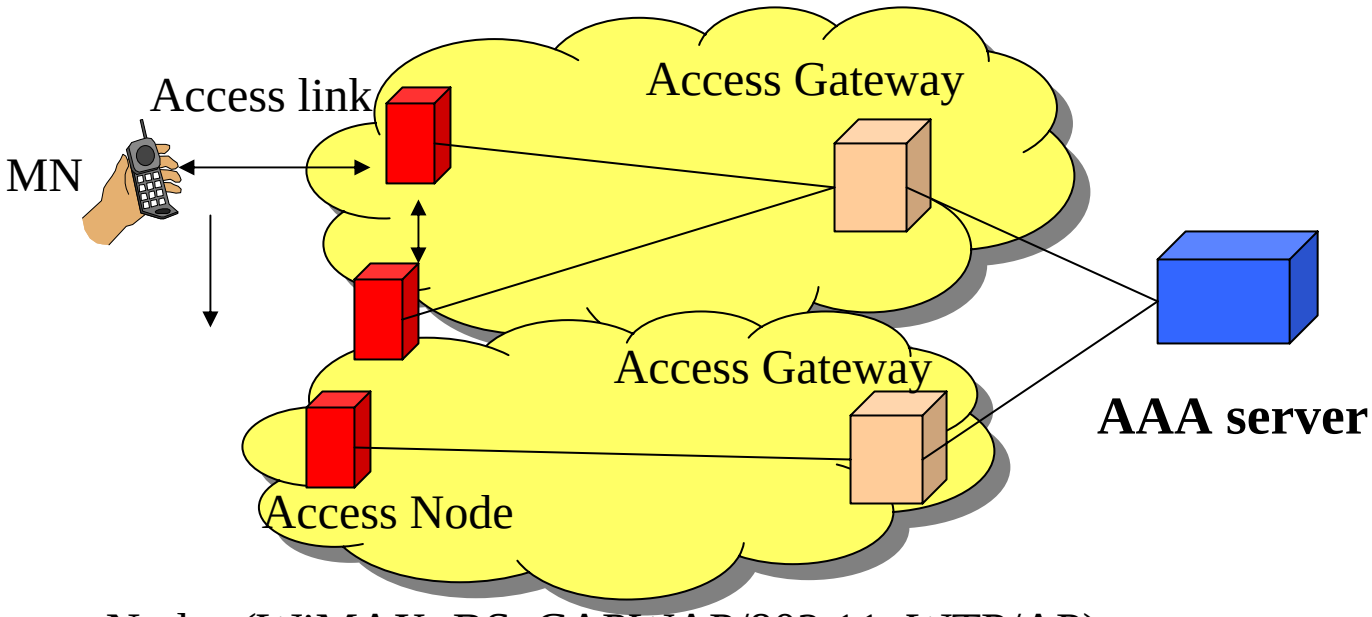
- Secure Access link: MN-AN SA
- Access link Handover: create MN-AN2 SA
- If Authenticator=AN:
  - MSK goes to AN1
  - MN-AN2 SA: requires new MSK at AN2?
- Run EAP again?? Handover performance suffers
- Don't send MSK to Authenticator,
  - Extend key hierarchy, create a per-authenticator key derived from previous EAP

Session Longevity



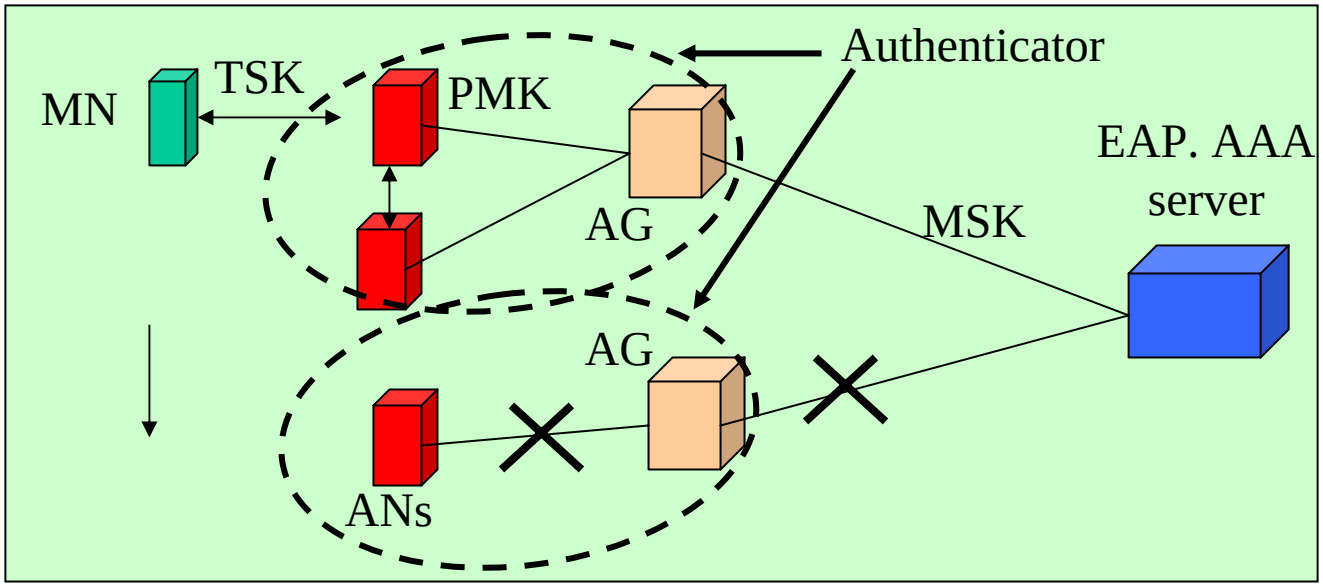
- Secure session established: previous lengthy EAP-XXX
- Session and keys about to expire
- Run EAP-XXX again?
- No, perform a “fast re-authentication”
  - Use state/keys from previous EAP
  - Design specific signaling for re-authentication

Network Management scalability
Wireless Access Network Architecture/CAPWAP



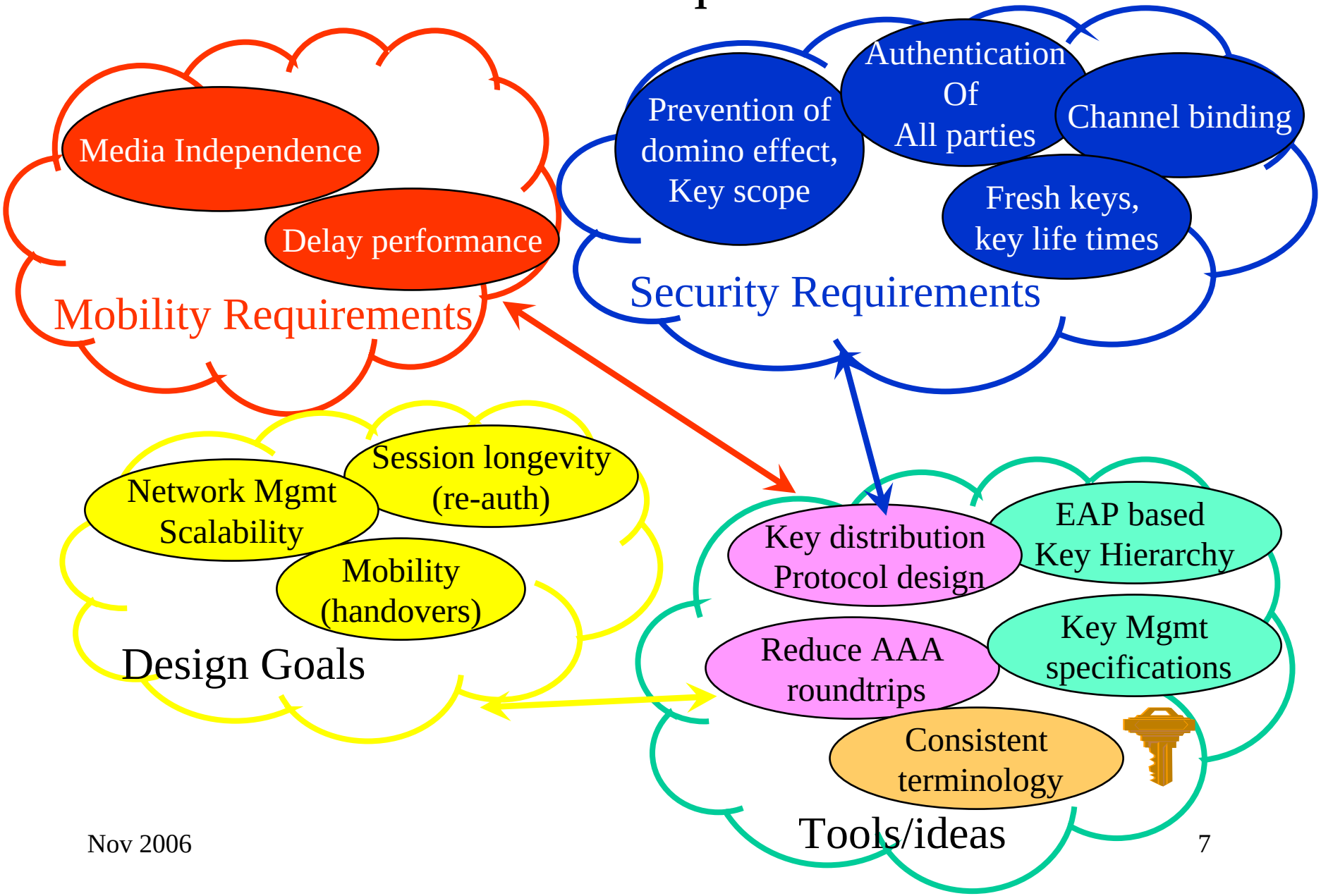
- Access Nodes (WiMAX: BS, CAPWAP/802.11: WTP/AP)
  - providing access links (wireless termination)
  - Lightweight/ less security-AAA functions/ less need for upgrades
- Access Gateways (WiMAX: ASN-GW, CAPWAP AC)
  - Management functions, backend communications
  - More trusted, AAA server interaction
  - Manages mobility across ANs (handovers) without interaction with AAA server
  - Typically manages one access technology.

EAP authenticator split to Manage scalability and AN-handover performance



- Splitting the EAP authenticator into 2 solves the intra-authenticator handover performance problem (SDOs)
  1. ASN_GW, R0KH, AC:
     - holds key from AAA server, creates per AN keys:
  2. AN, WTP, Auth port
     - receives Per AN keys, creates SA with peer (MN)
- It does not solve Inter-authenticator problem
- Authenticator a logical function, AN/AG physical entities (channel binding)
- Solutions varies between SDOs: media-independent handover difficult

Goals and Requirements



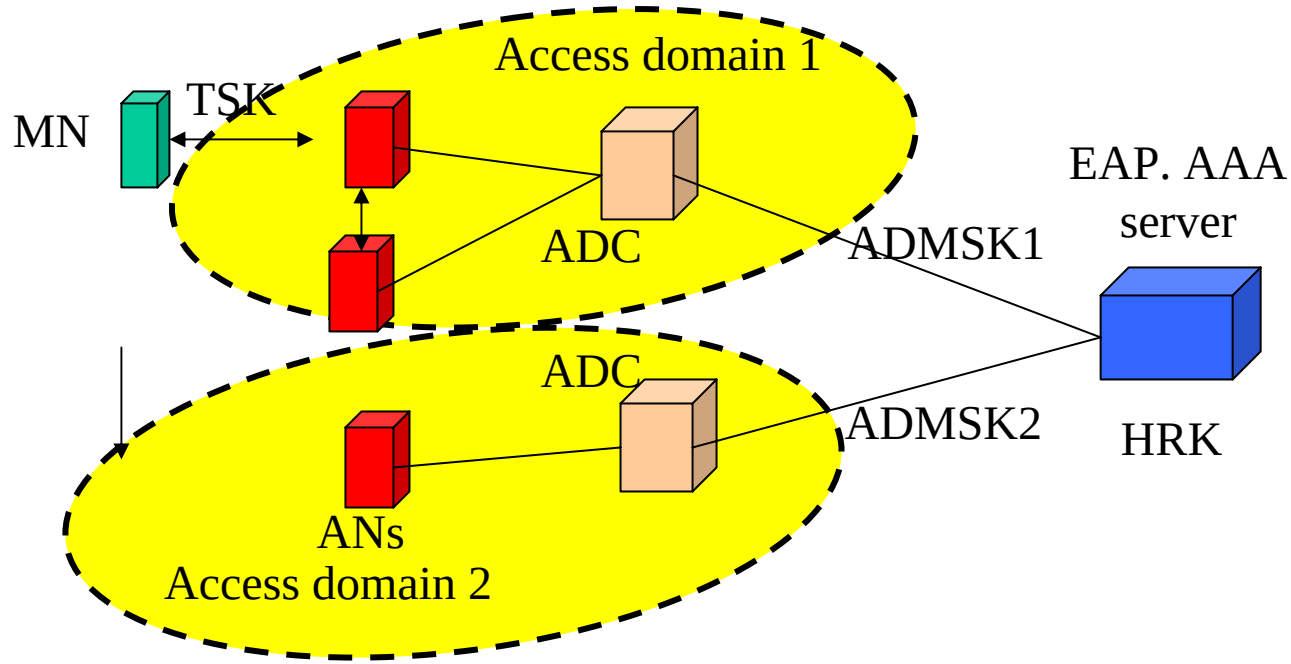
Problem statement/ To Dos

- Create consistent terminology
- Specify security, mobility, management goals
- Decide levels of key hierarchy
  - Map hierarchy levels to key holders
  - Define key derivation function and parameters
  - Define messaging to exchange the parameters
  - Define key management rules
- How far down the key hierarchy can IETF go?
- Do the needed protocols exist?

New Terminology/ Concepts

- Handover Root Key (HRK)
  - Used as the root of key hierarchy for handover (and re-auth)
  - AAA server is HRK holder
  - HRK is used to create per-ADC keys (ADMSKs)
- Access Domain Controller (ADC)
  - Top level key holder in an access domain (holds ADMSK)
  - Responsible for keying needs within an Access Domain (reduce the need to AAA interactions).
  - 802.11r calls this Mobility domain controller (MDC):
    - MDC or ADC?

Access Domain controllers



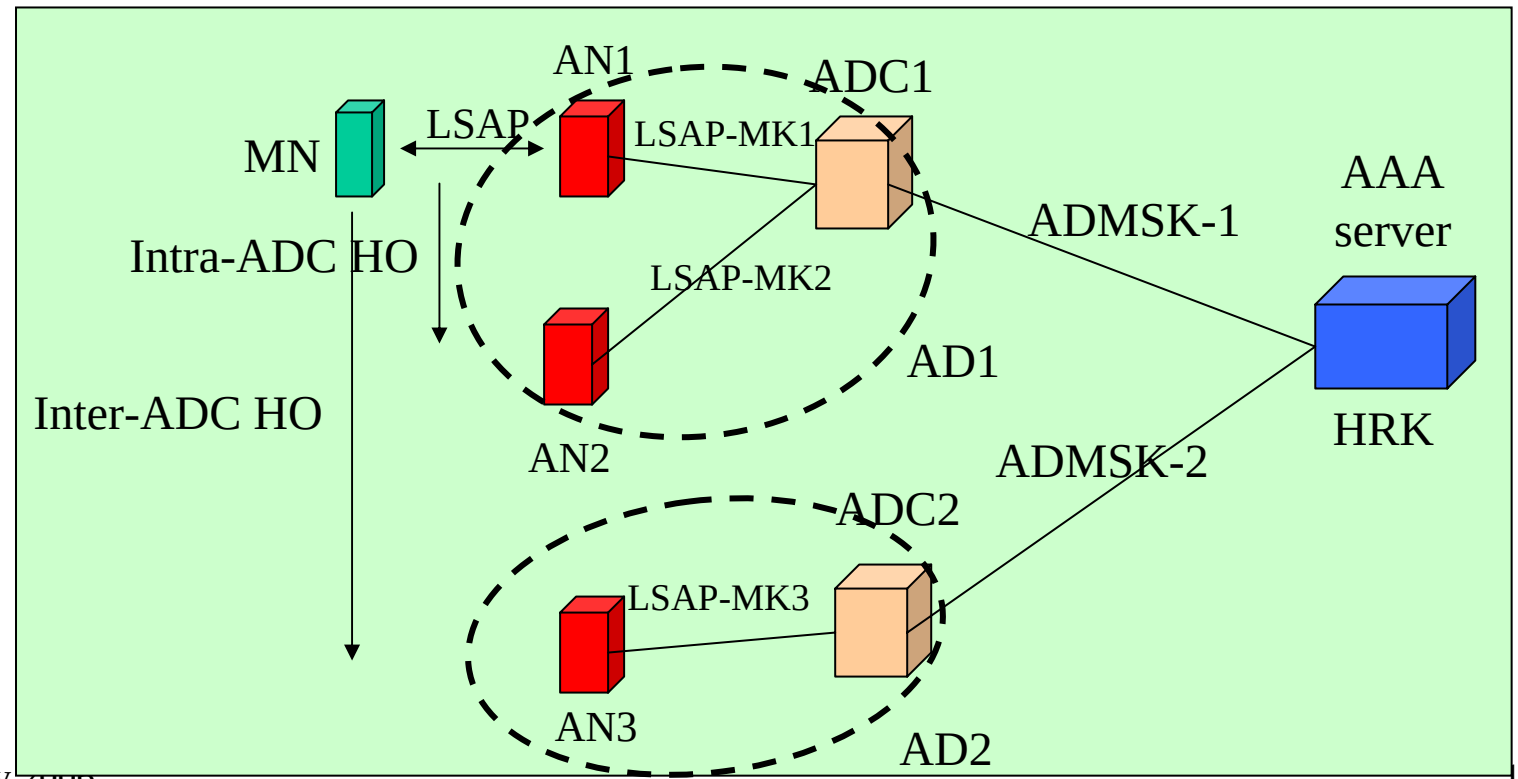
- ADC is a key holder and a AAA client
  - It can be the authenticator, but does not have to be
  - ADC is a AAA client (it receives ADMSK from AAA server)
  - Both authenticator-split and flat architectures can be supported.
  - ADC provisions the access domain ANs with keys
  - Access domain can be mapped to an access technology region, if needed

Tough problems

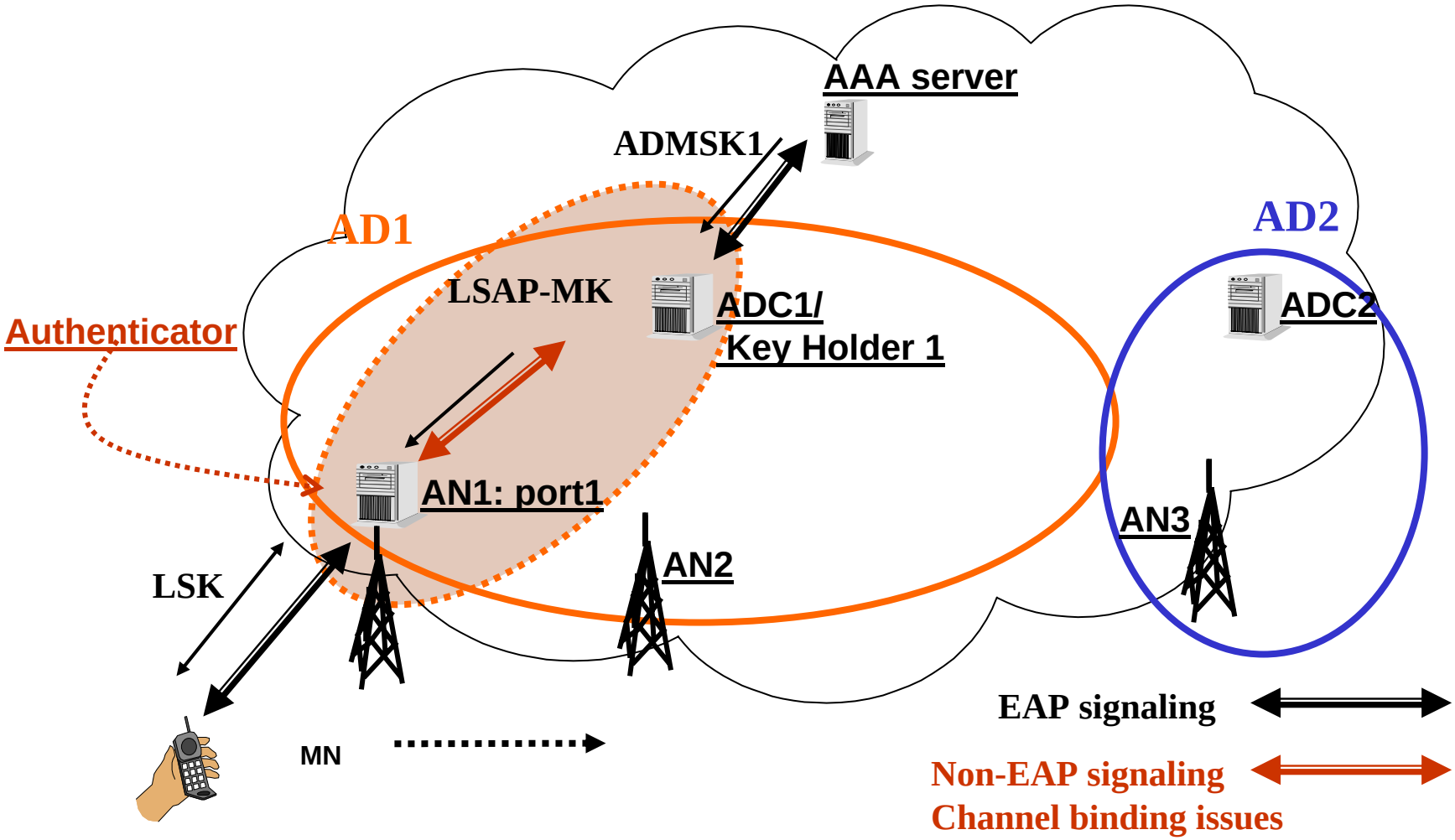
- Terminology, Terminology, terminology
- What key to use to derive handover root key?
  - MSK or as USRK from EMSK? (created at EAP server?)
    - Compatibility with other SDOs? Backward compatibility?
- Architecture:
  - ADC part of the authenticator? Positioning ADC vs Authenticator?
  - Access technology mapping
  - To accomodate physically separate ADC and AN?
    - Channel binding/ key derivation parameters/ Messaging
      - ADC and AN collocated (EAP keying) or not (SDO)
- Messaging
  - Exchange parameters for key derivation (e.g. ADC-ID)
- Channel binding
  - EAP keying item: ADC and AN are both part of Authenticator
  - Handover keying with deeper hierarchy?

Problem: IETF scope?
LSAP-MK should be defined in Info RFCs, IMHO

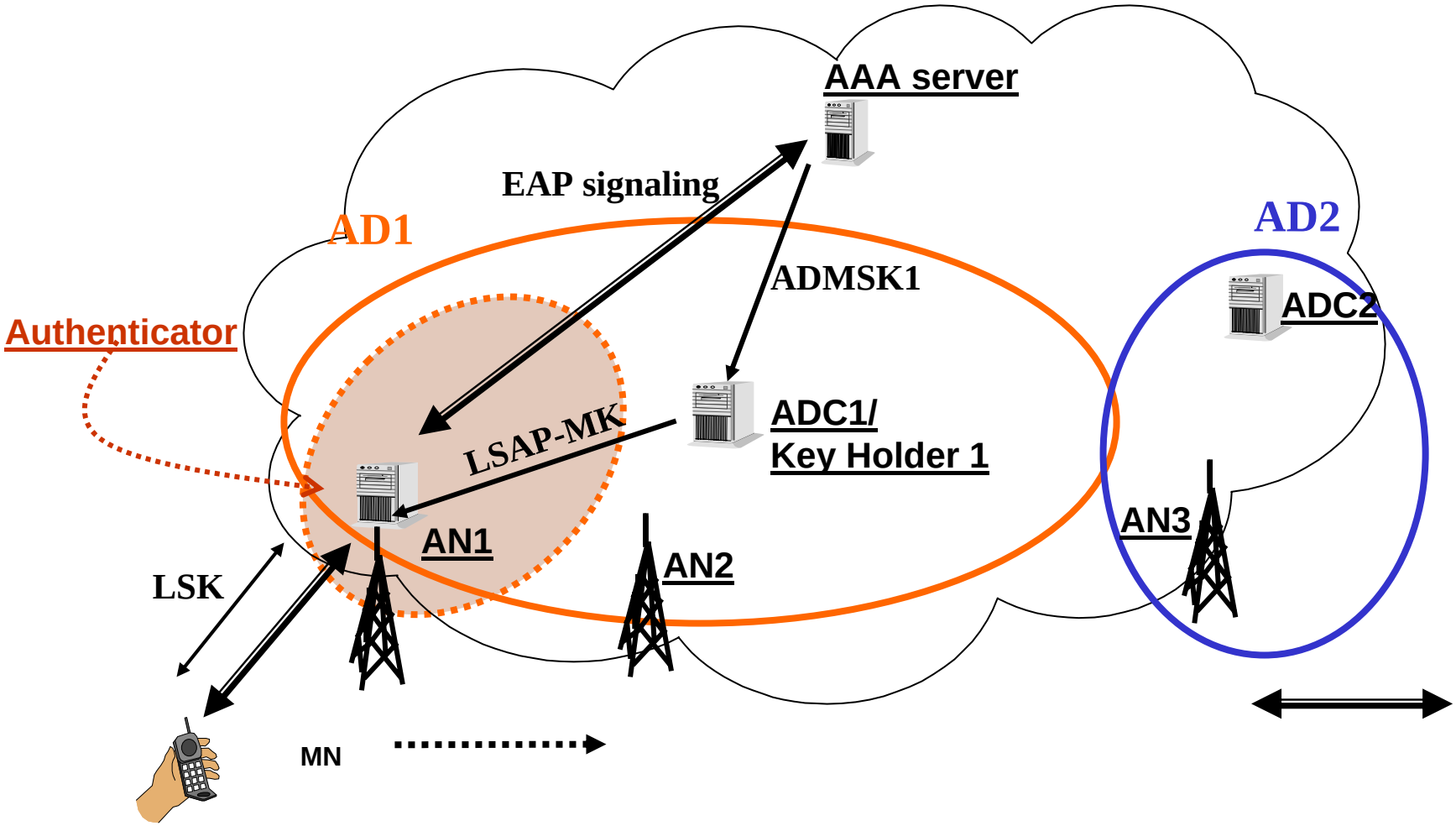
- Intra ADC handover: Key management and key derivation inside same ADC (Is this within IETF scope? Info RFCs?)
- Inter ADC handover: Key Management and key derivation through different ADCs but same AAA, without running EAP again.



Positioning of EAP authenticator wrt ADC (alternative 1)



Positioning of EAP authenticator wrt ADC (alternative 1)



Backup:Related charter deliverables

- Re-authentication (including handover) and key management problem statement
  - Security and performance goals.
- Choice of MSK or EMSK in HRK (not a deliverable, but important)
- Handover Root Key (HRK) and key hierarchy derivation and management specification
- Handover/re-authentication protocol specification
- Key distribution protocol specifications

Backup: Why ADC instead of Authenticator

- Allows for easier management of heterogeneous roaming/ handovers (e.g. per-domain technology)
  - Combine key mgmt with mobility mgmt
- Handover root key transport/caching behavior
  - HRK (e.g. MSK) is kept at AAA server, not sent to authenticator
  - A per ADC master keys (ADMSK) are sent to ADC
- Separation of EAP auth. and handover keying signaling
  - Key mgmt and mobility mgmt can be inside an ADC, independent of entity that acts as pass-thru Auth,
  - Pass-thru auth either in AN or ADC
- More crisp key usage guidelines
  - Authenticator master key<->Authenticator port master key?
  - Use ADC master key (ADMSK) and AN master key (LSAP_MK) instead