Mobility sensitive master key derivation and fast re-authentication for 802.16m [slides]

IEEE 802.16 Presentation Submission Template (Rev. 8.3)

Document Number:

S802.16m-07/029

Date Submitted:

2007-02-23

Source:

Ronald Mao, Madjid Nakhjiri
Huawei Technologies Co.,Ltd.
10180 Telesis Ct, Suite 365
San Diego, CA 92121

Voice: 858-882-0335
Fax: 858-882-0350
E-Mail: rmao@huawei.com
mnakhjiri@huawei.com

Xiaolu Dong
RITT

Voice: +86-10-62302438
Fax: +86-10-68034801
E-mail: dongxiaolu@mail.ritt.com.cn

Venue:

IEEE 802.16 Session #48 Orlando, FL, USA

Base Document:

IEEE C802.16m-07/029, <http://wirelessman.org/tgm/C80216m-07_029.pdf>

Purpose:

The purpose of this slide set is to support contribution C802.16m-07_029. This document puts forward a requirement to use the HOKEY key hierarchy instead of the EAP key hierarchy for 802.16m.

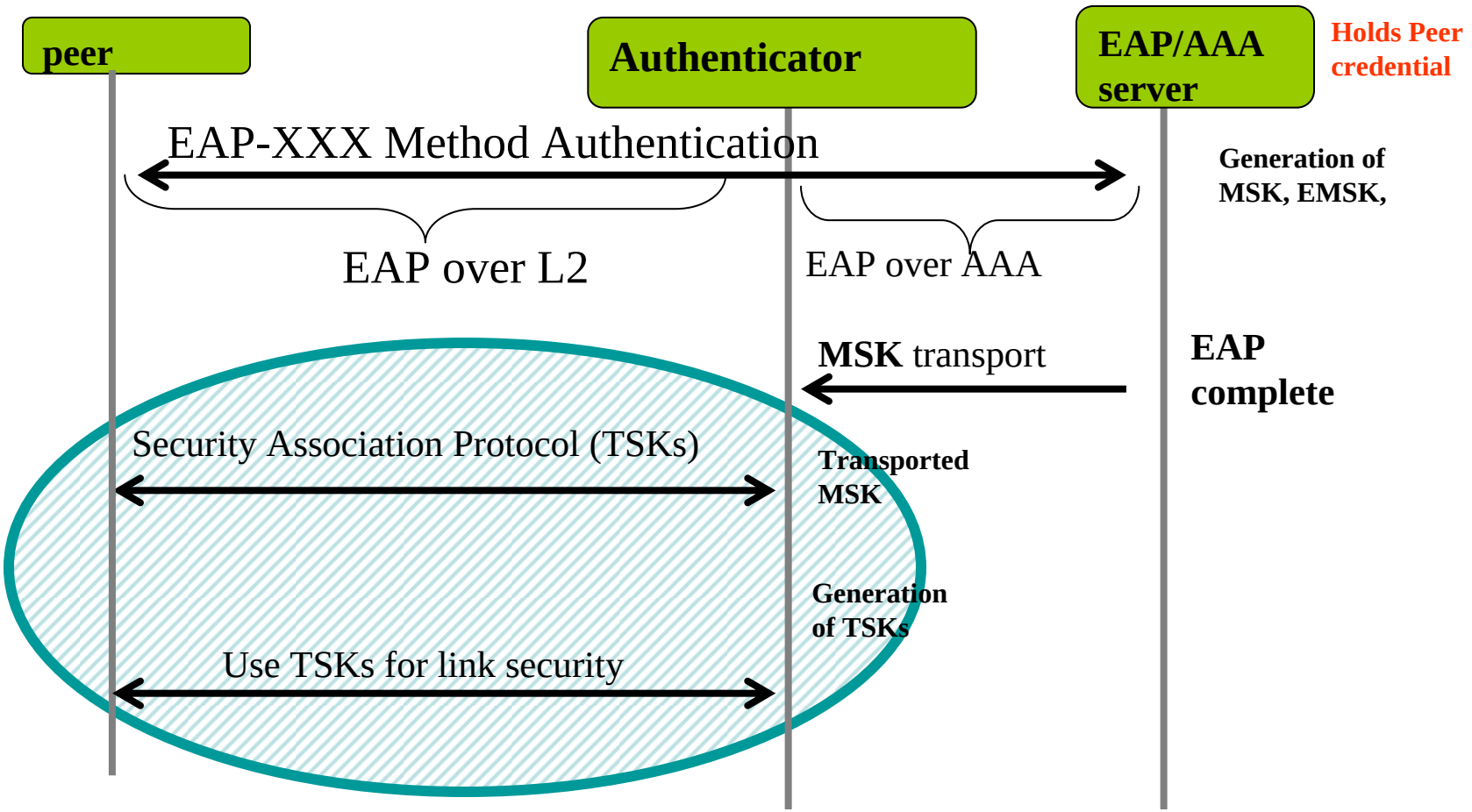
Mobility sensitive master key derivation and fast re-authentication for 802.16m

Reference: draft-nakhjiri-hokey-hierarchy-03

Is EAP enough?

- EAP is an IETF protocol, link layer out of scope
  - EAP key management only down to authenticators
  - Needed: key management between authenticator and end client
- EAP was not designed with mobility performance in mind
  - Issues with wireless deployments architectures
  - Issues with latency performance
  - Needed: overhaul from integrated mobility-security perspective

EAP Key management framework



Outside IETF scope

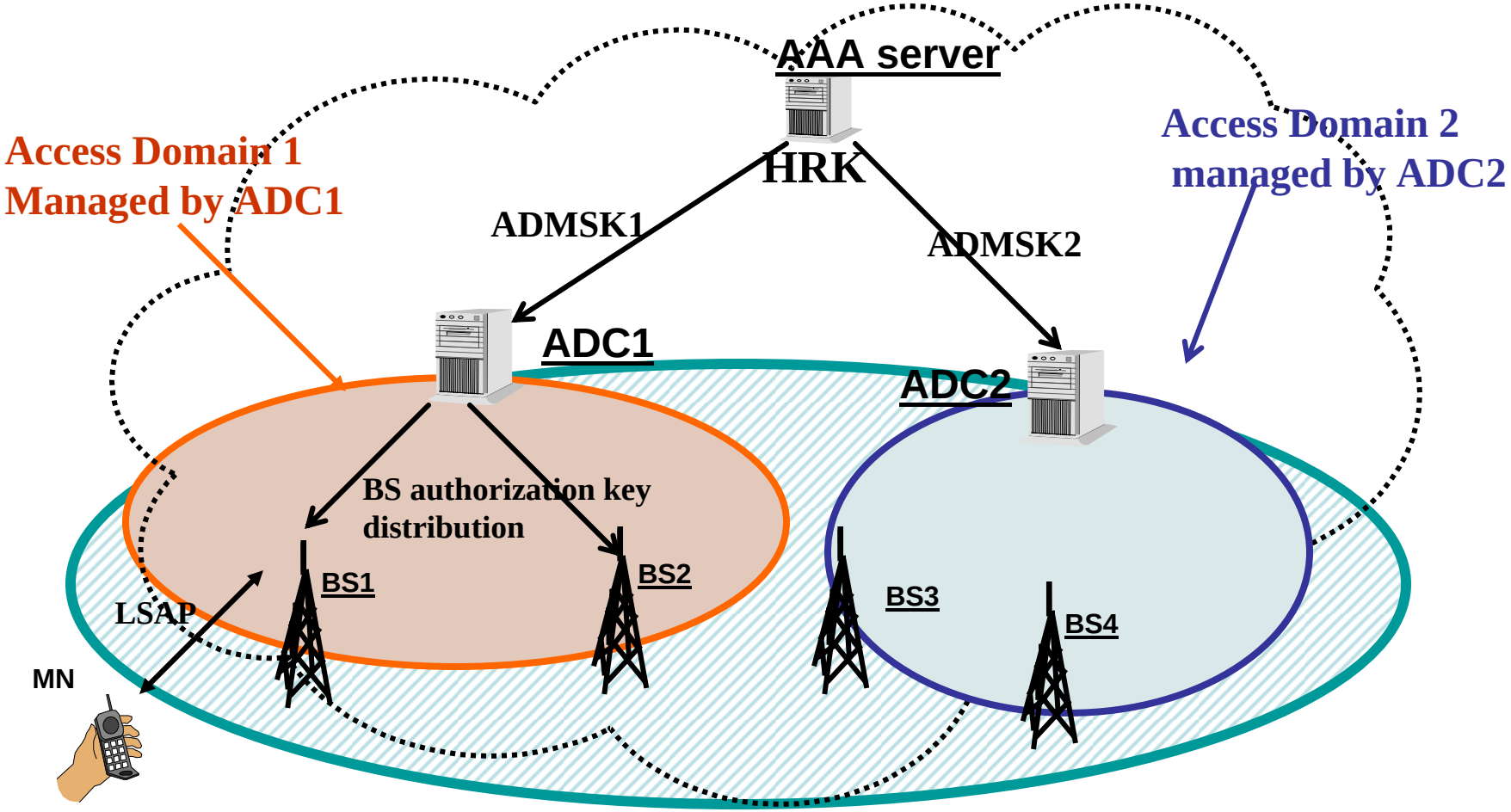
Key generation considerations
Work under progress in HOKEY

- A handover root key, HRK, is derived from EMSK
- AAA server is HRK Key Holder, HRK used for
  - AAA_RK: fast re-authentication/ADC handover authorization/ADMSK channel binding
  - Per-Authenticator/ADC keys (ADMSK)
  - PRF chosen for handover
- ADC is ADMSK Key holder, ADMSK used for
  - Generation of AK, and KEK

Hokey: new WG to deal with EAP deficiencies

- Goal 1: Optimize performance: minimum or no round trips to AAA server
  - Handovers (change of point of attachment to network) without new EAP authentications
  - Roaming (attaching to a new operator network) and using services in a visited network
  - Session extension (when extending the life time of existing session/ keys)
- Goal 2: Security: No domino effects, Principle of least privilage
- How: Expand EAP key management framework by
  - Define a key hierarchy allowing for generation of keys for various contexts
    - keys for contexts outside Hokey scope (Mobile IP, etc)
    - key hierarchy to allow the use of the initial EAP keys for a new authenticator and to re-authenticate

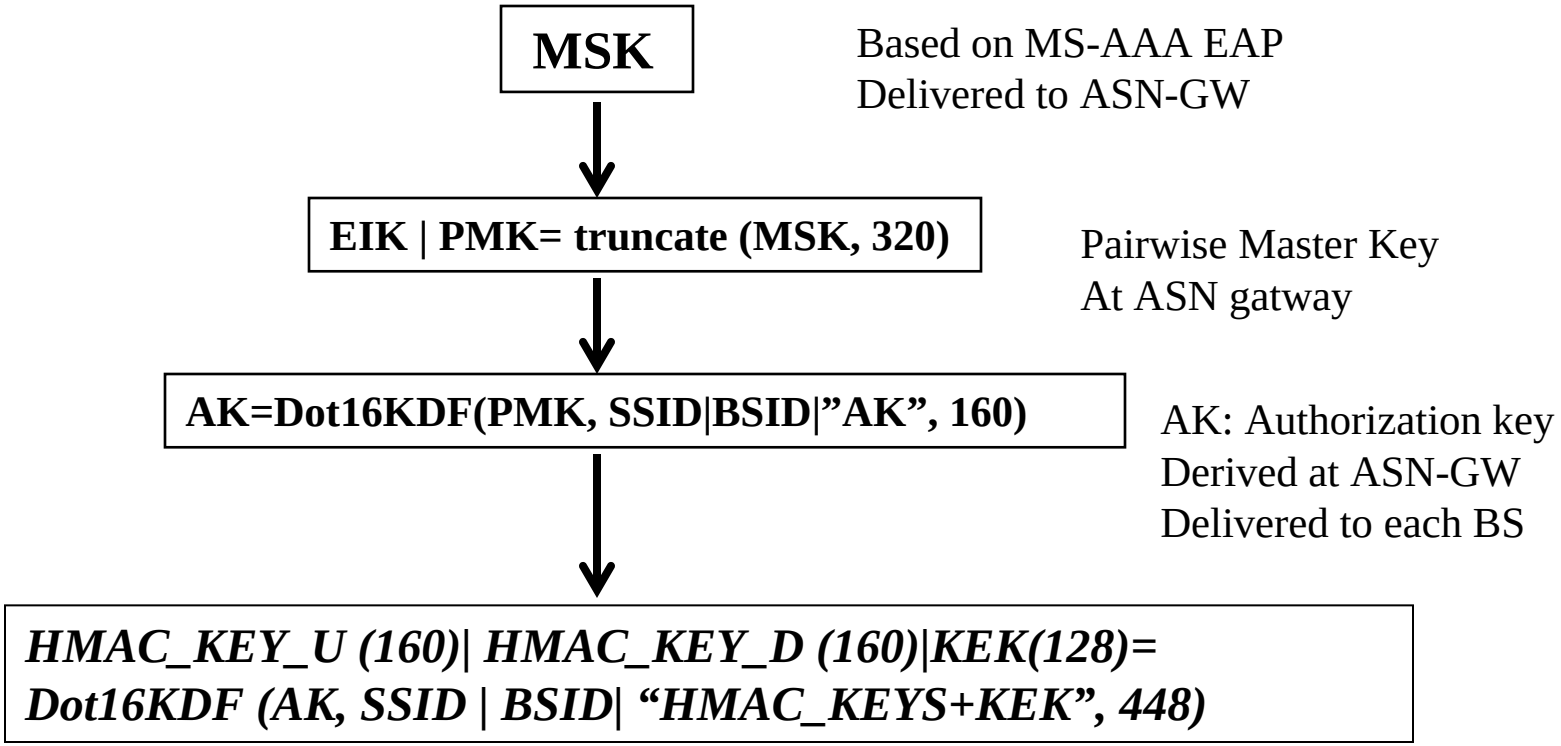
Hierarchical 2 level Deployments: (WiMAX ASN_GW and BS)



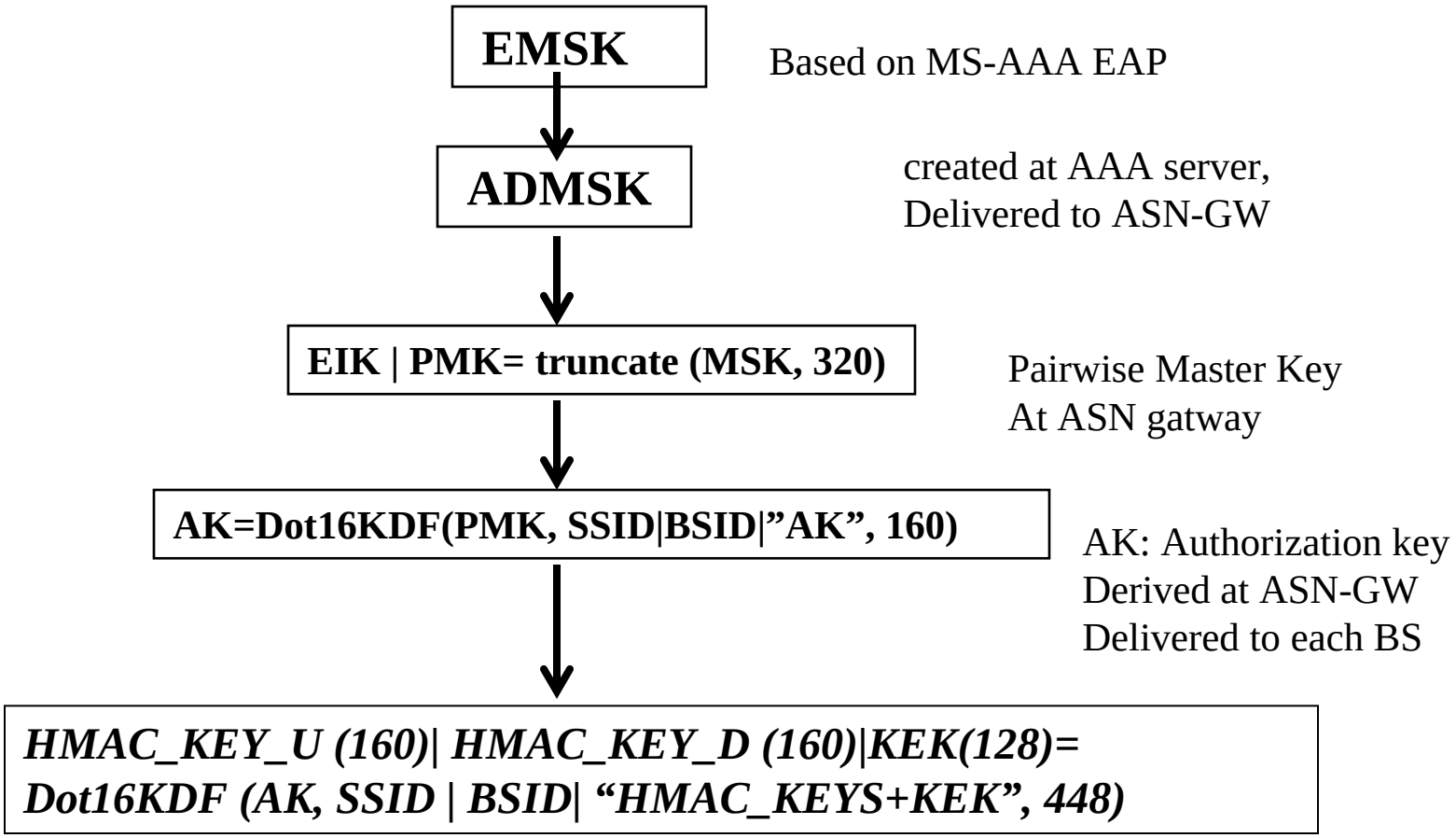
Outside IETF scope

ADC=Authenticator=Access domain controller
ADMSK=Access domain Master key
LSAP=Link Security association protocol

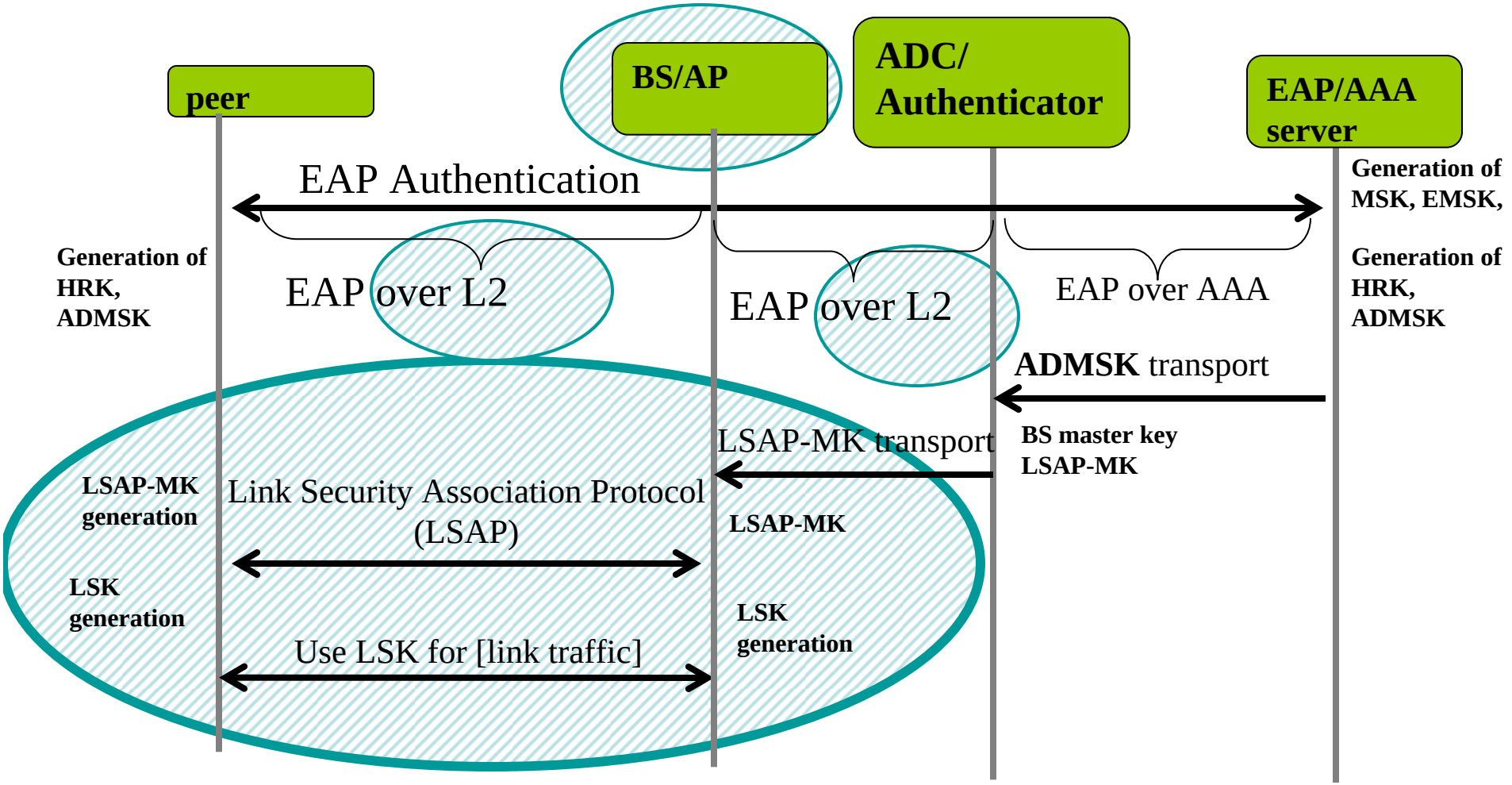
802.16e key hierarchy based on EAP



802.16e/m key hierarchy IF based on HOKEY

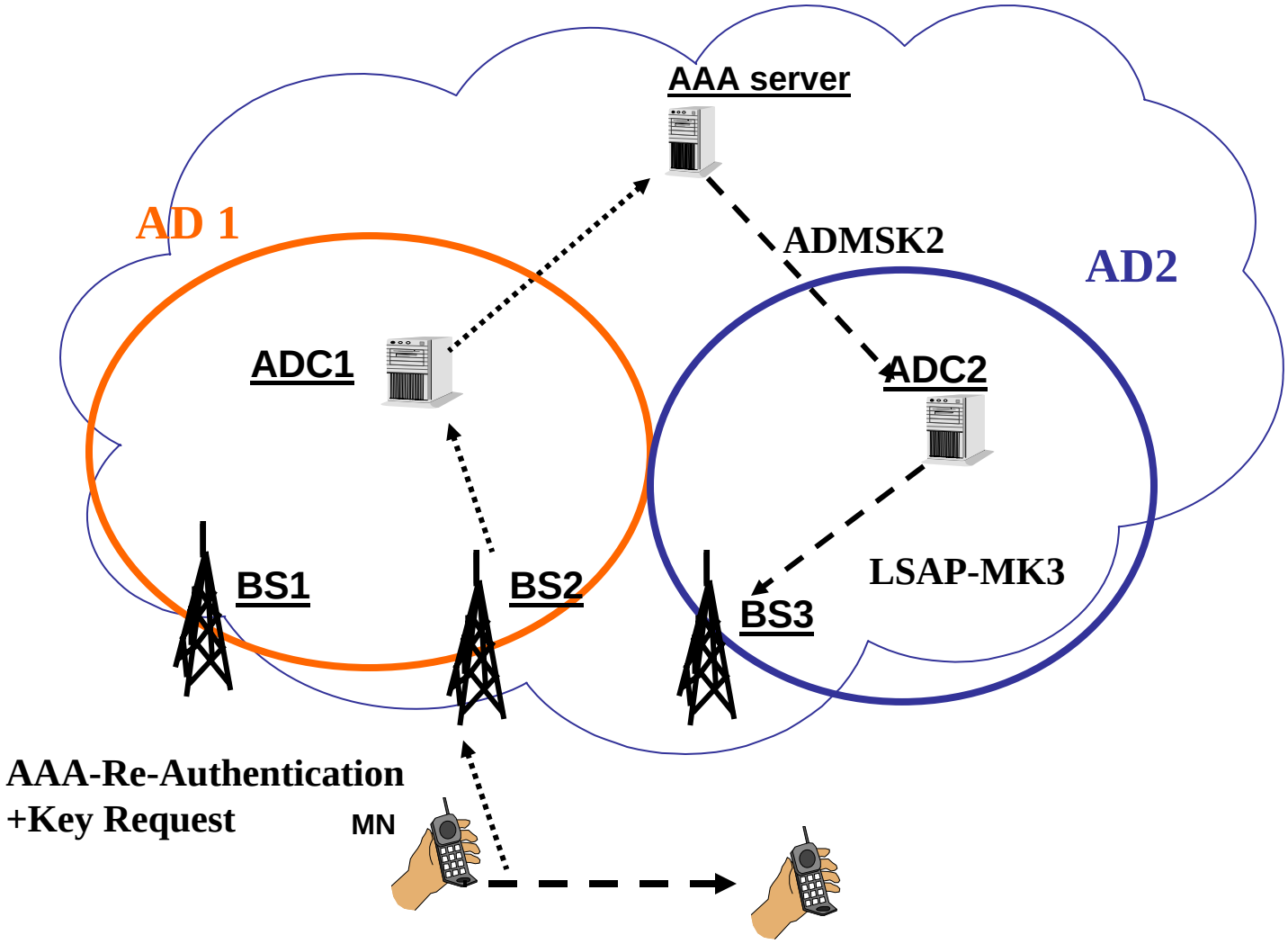


HOKEY framework for common deployments??
Terminology work under progress☺

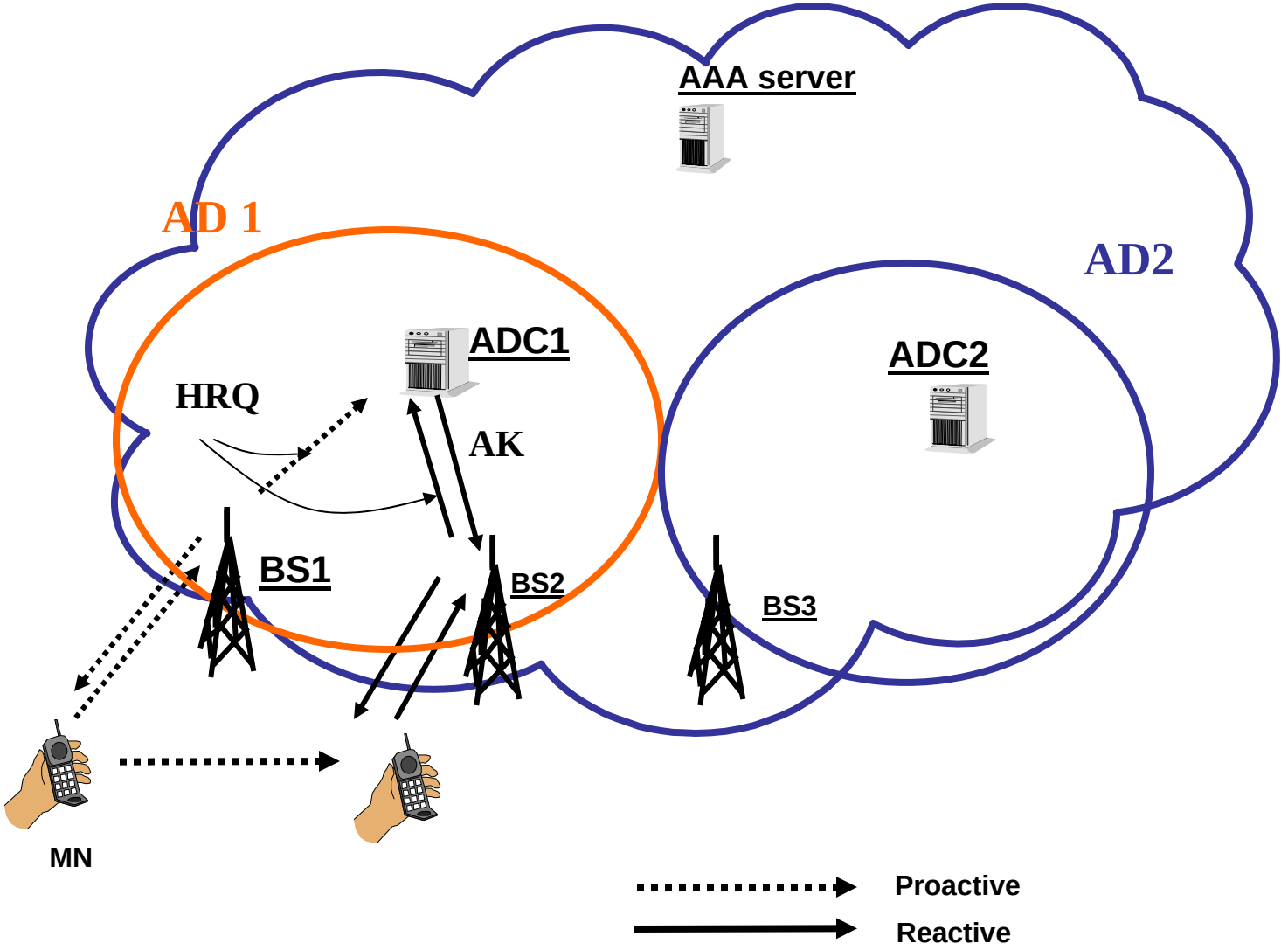


Outside IETF scope

Inter-Authenticator (ADC) handover no longer requires Authenticator anchoring as in current WiMAX



Intra-Authenticator handover scenario (covered in WiMAX)



Hokey scope: Domain level down to authenticator