

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.

Notice:

This document has been prepared to assist IEEE 802.16. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.

Release:

The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16.

IEEE 802.16 Patent Policy:

The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures <<http://ieee802.org/16/ipr/patents/policy.html>>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, provided the IEEE receives assurance from the patent holder or applicant with respect to patents essential for compliance with both mandatory and optional portions of the standard." Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair <<mailto:chair@wirelessman.org>> as early as possible, in written or electronic form, if patented technology (or technology under patent application) might be incorporated into a draft standard being developed within the IEEE 802.16 Working Group. The Chair will disclose this notification via the IEEE 802.16 web site <<http://ieee802.org/16/ipr/patents/notices>>.

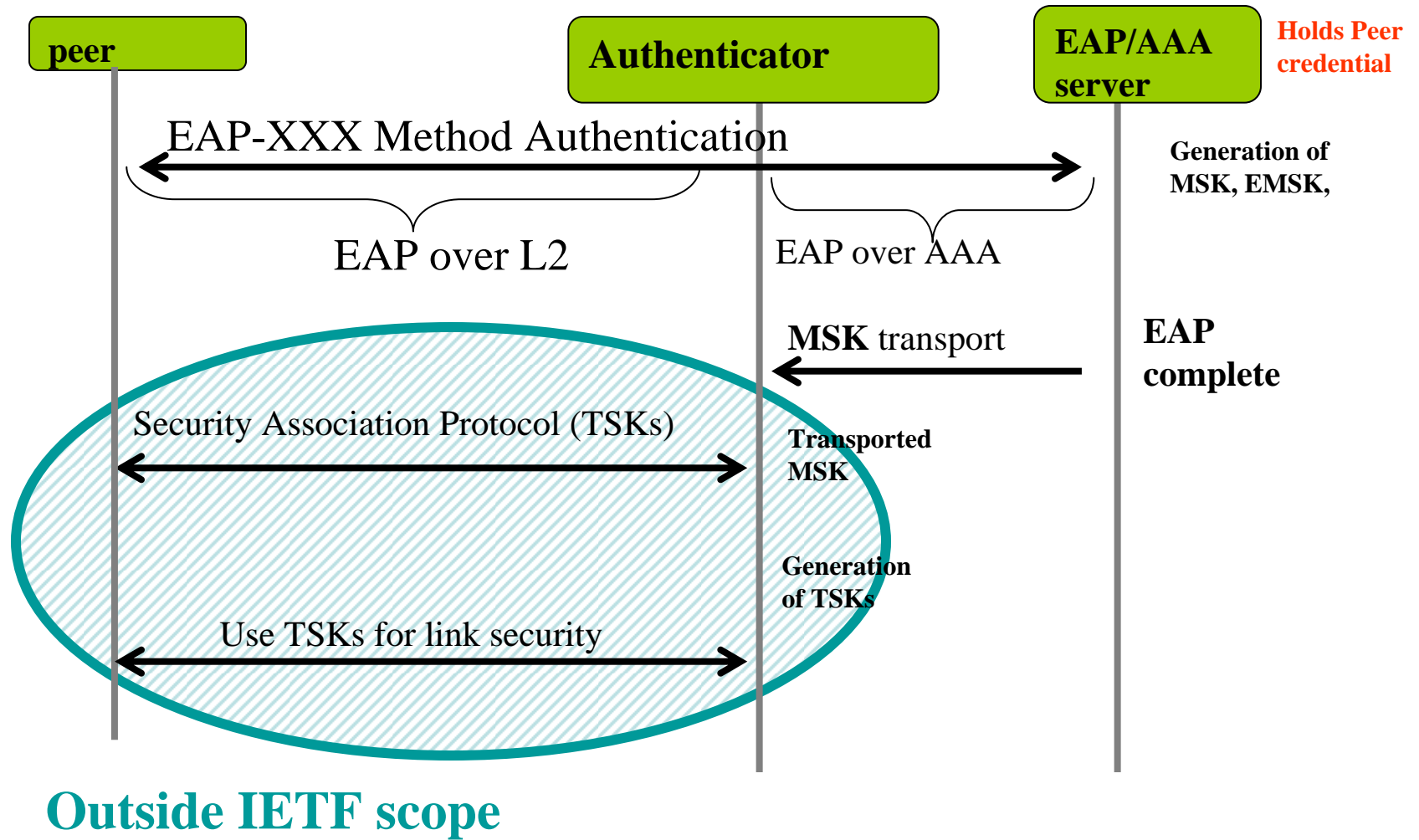
Mobility sensitive master key derivation and fast re-authentication for 802.16m

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



Key generation considerations

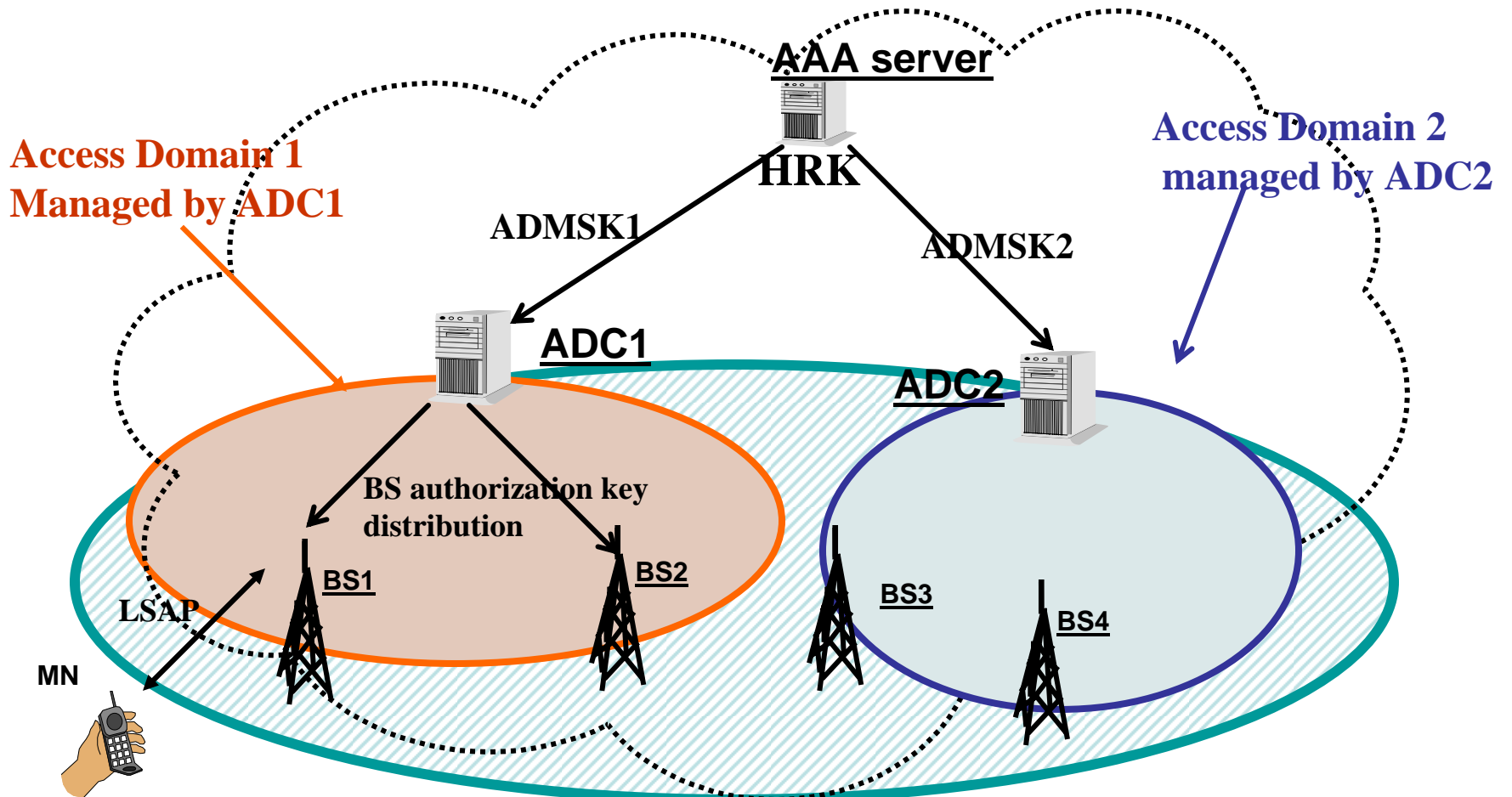
Work under progress in HOKEY

- 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 privilege
- **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)



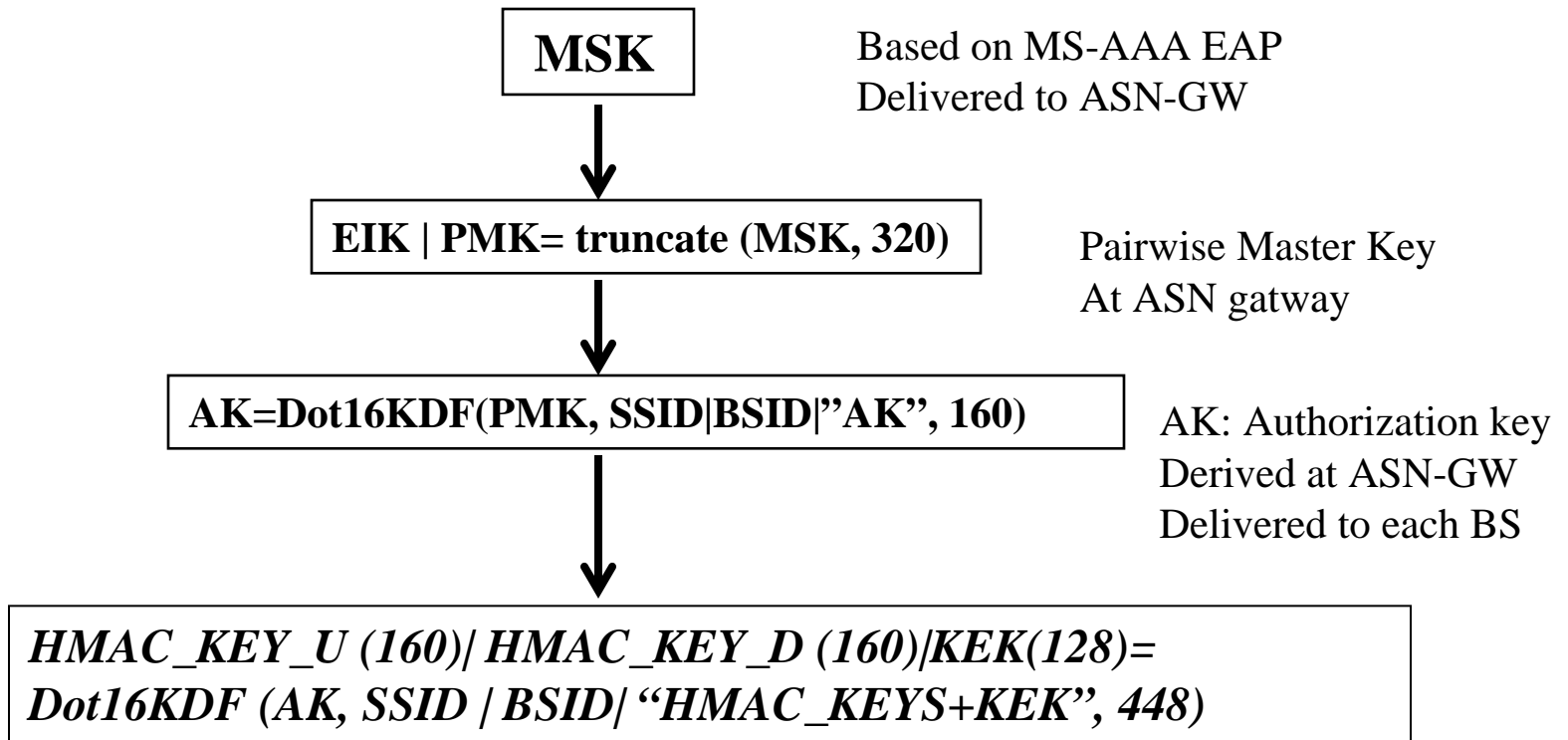
Outside IETF scope

ADC=Authenticator=Access domain controller

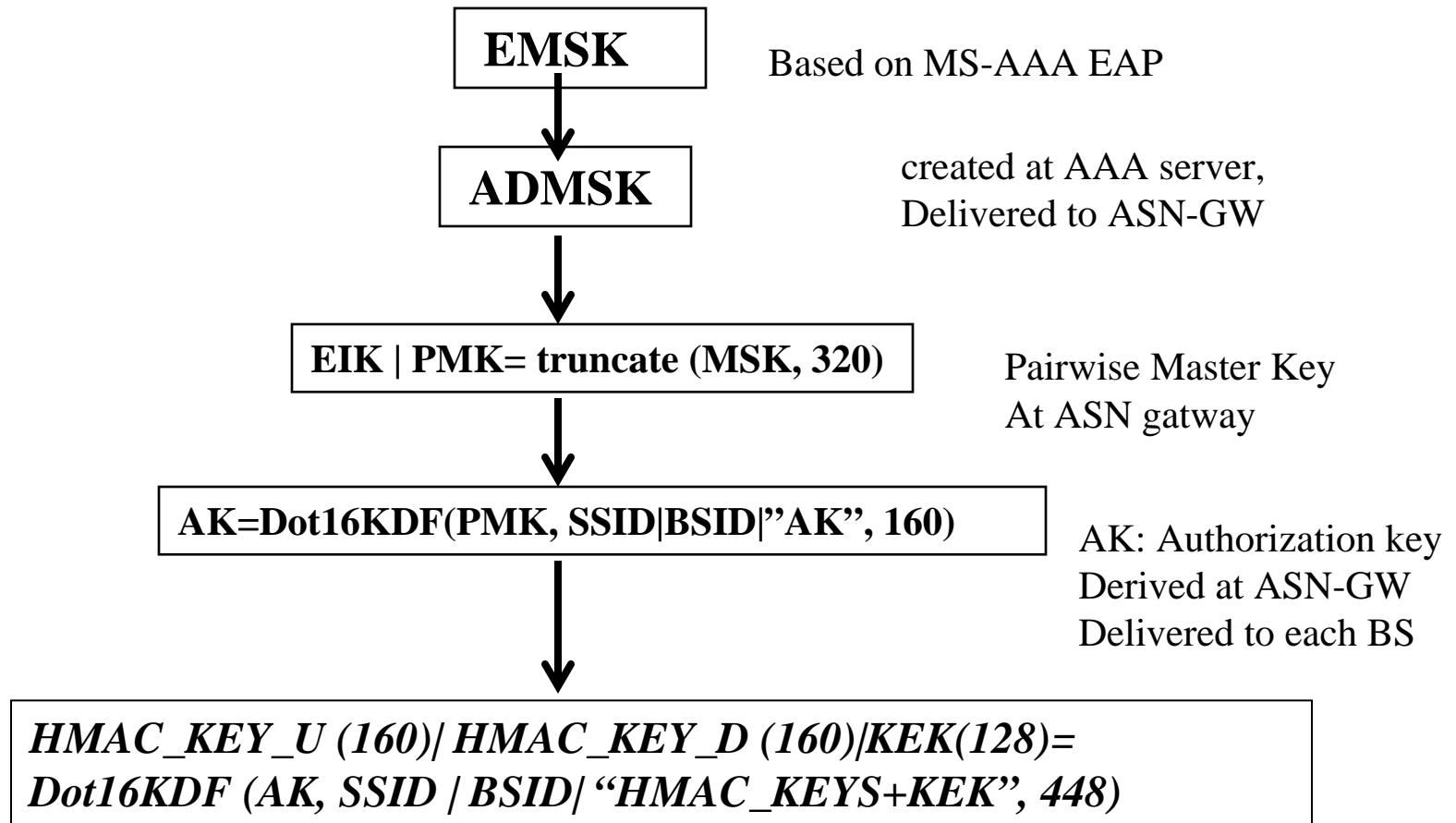
ADMSK=Access domain Master key

LSAP=Link Security association protocol

802.16e key hierarchy based on EAP

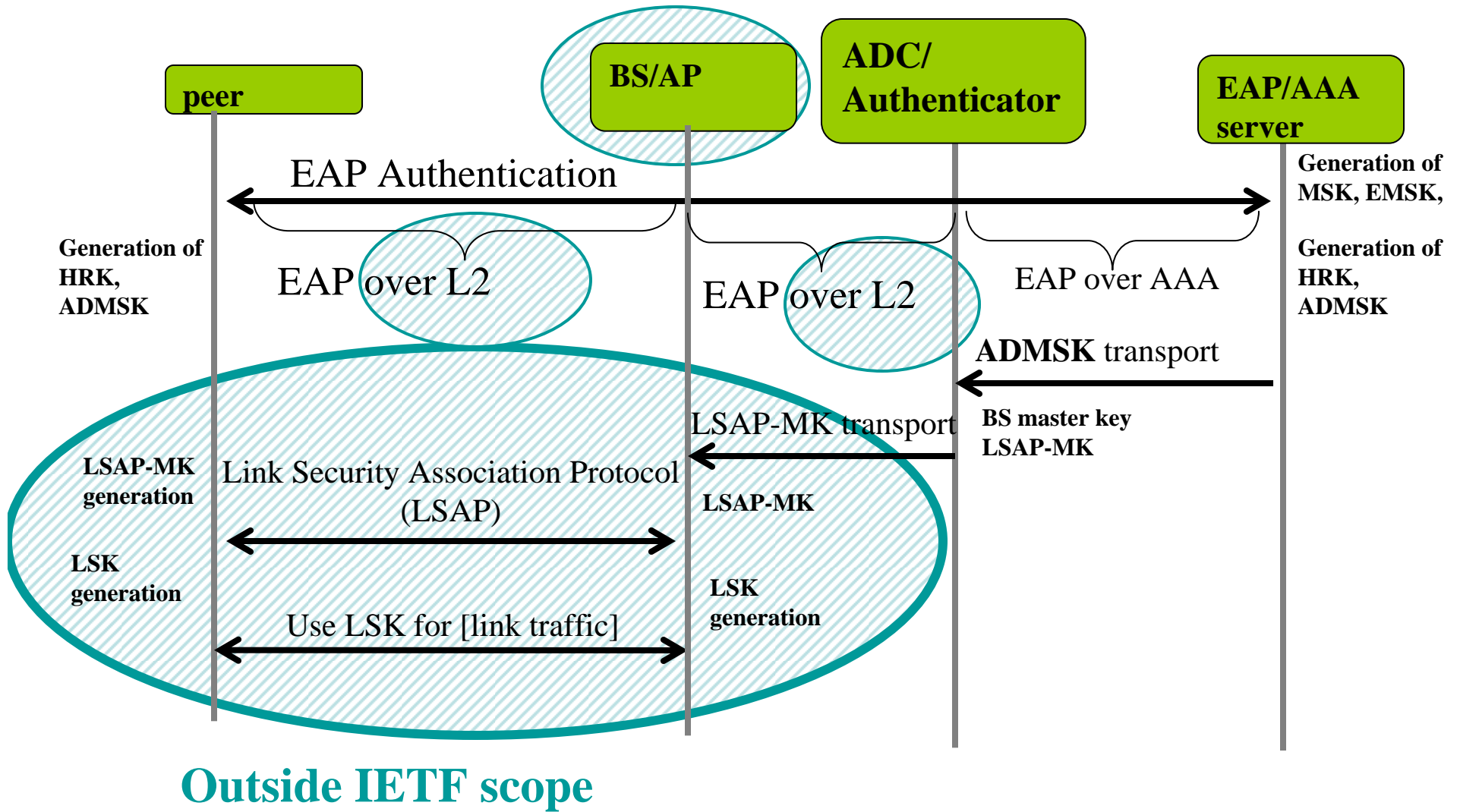


802.16e/m key hierarchy IF based on HOKEY

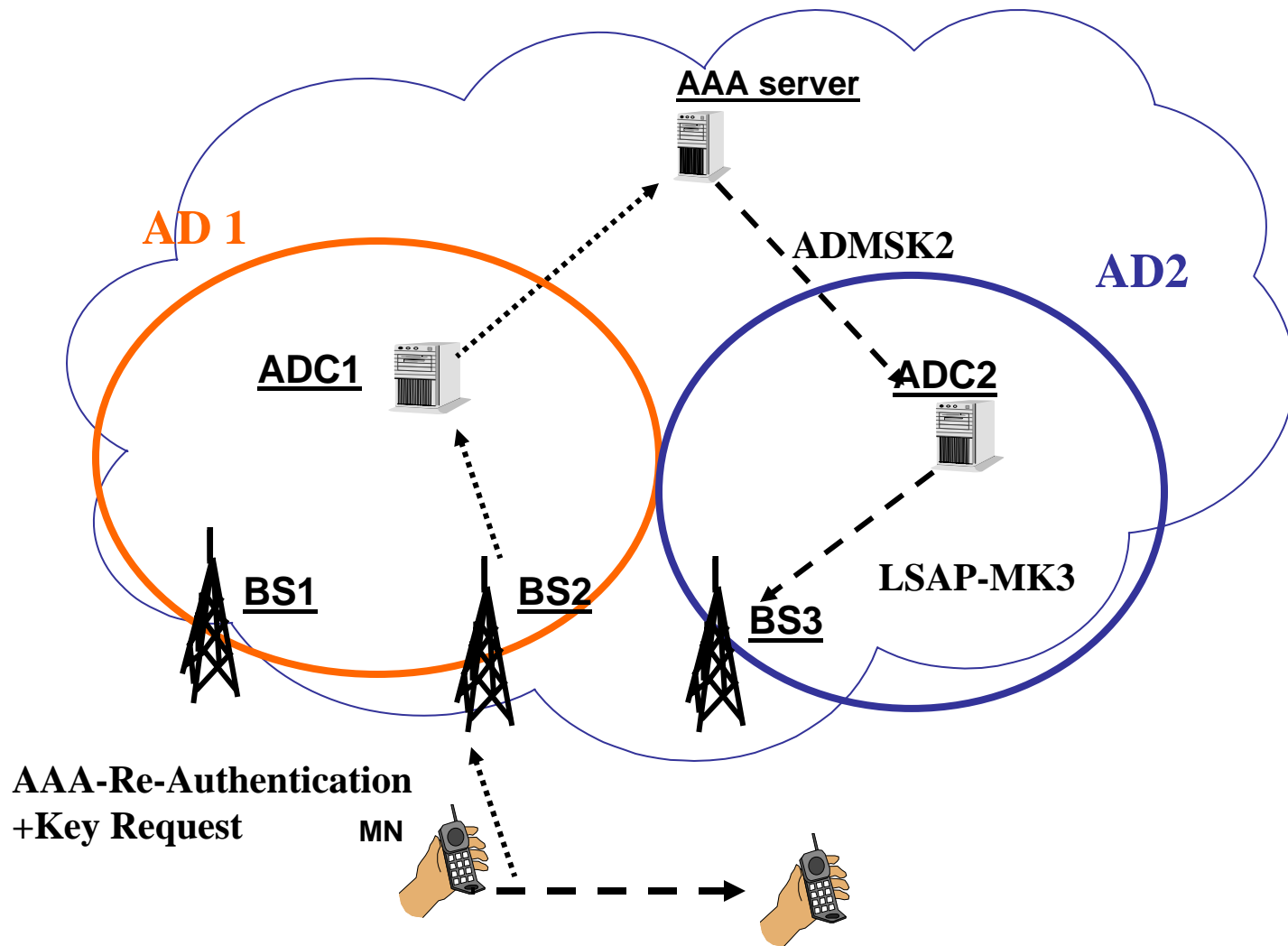


HOKEY framework for common deployments??

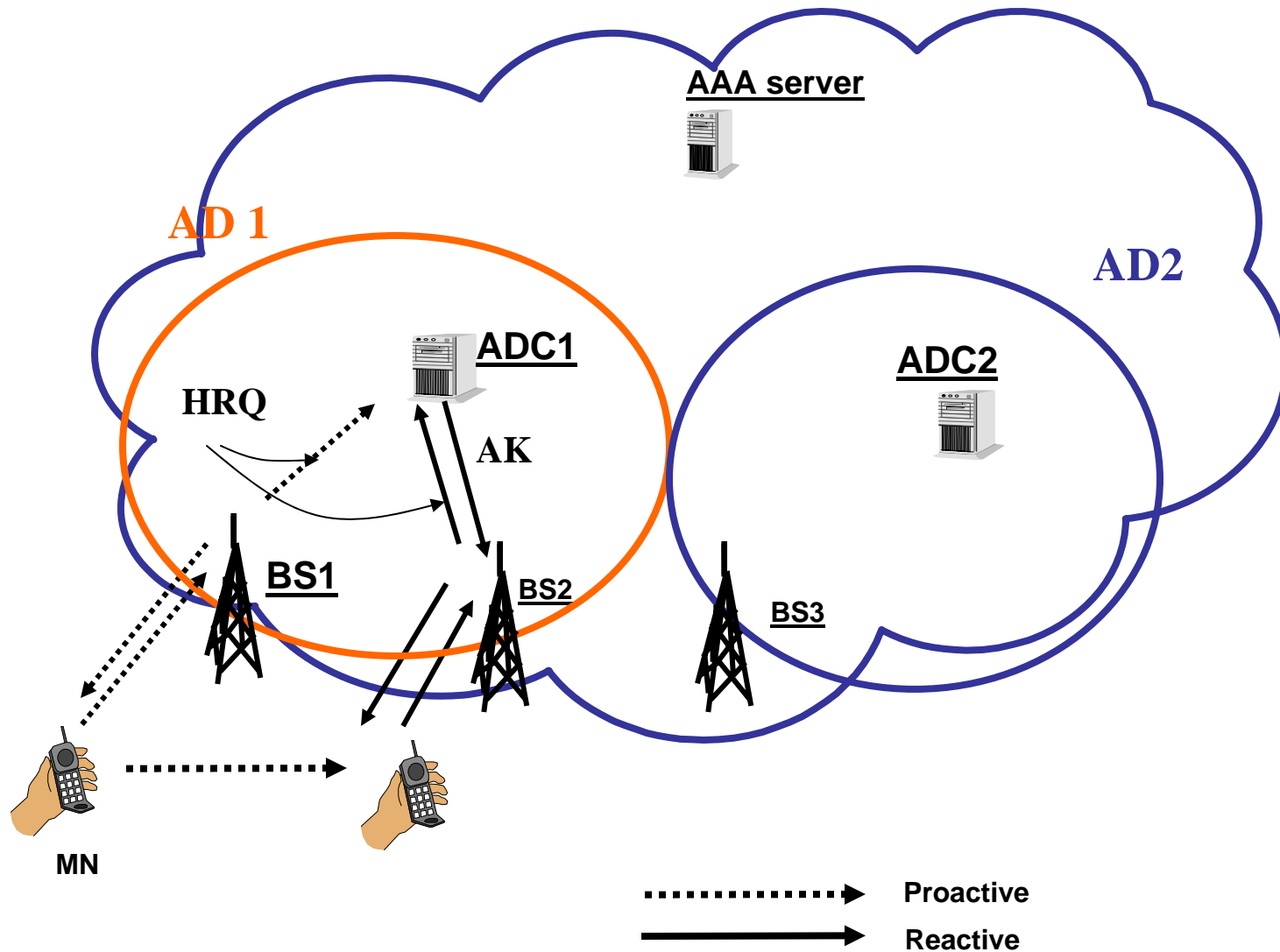
Terminology work under progress☺



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

