PMIPv6 inter-working with WiFi Access Authentication

draft-liebsch-netext-pmip6-authiwk

M. Liebsch, S.Gundavelli, P.Seite

IETF83,
NETEXT WG
March 2012

Outline

- Background & Motivation
- Document Objectives
- WLAN trusted access
- Feedback

Background & Motivation

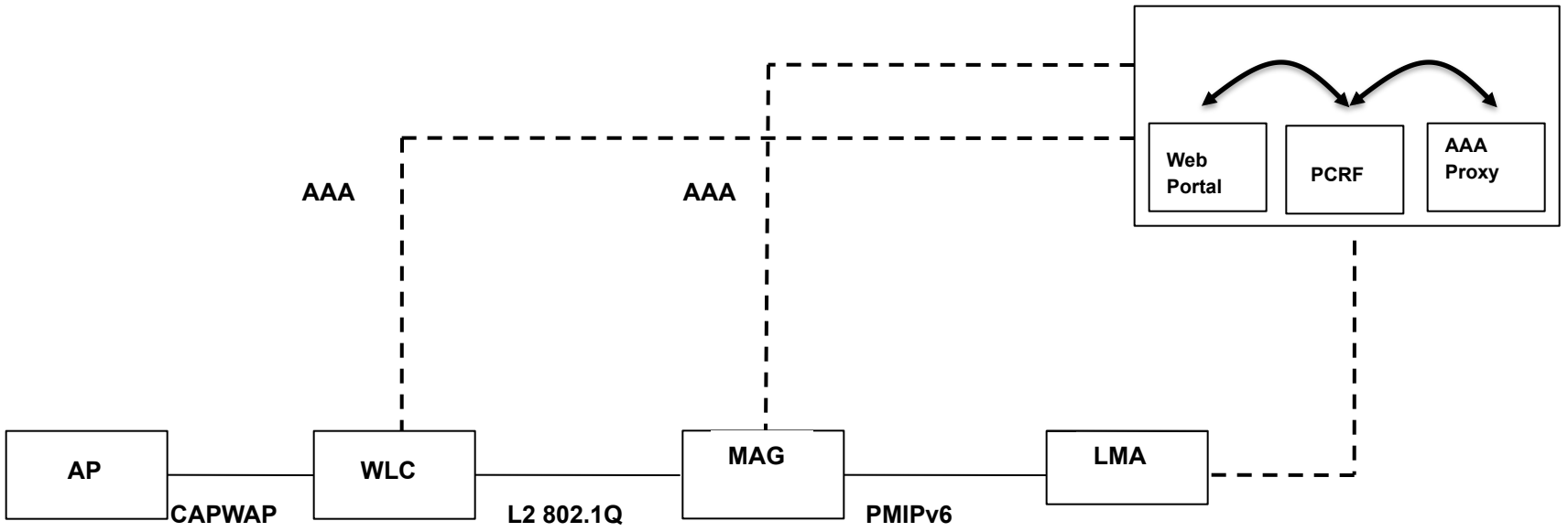
- RFC5213 assumes completed authentication procedure before registration
  - AuthN can provide trigger for PMIPv6 operation after completion
  - Option to derive MN-Identifier from access authentication
    - Contraints: Validity >= duration of mobility session, Scope >= PMIPv6 domain
  - Approach/Solution not documented in the IETF
- WLAN as well accepted access technology
  - Assumed untrusted (HotSpot, ...)
- Enable WLAN trusted access
  - 3GPP recommendations for security and for PMIP operation using non-3GPP radio access
  - WiMAX Forum specification for WiFi inter-working

Document Objectives

- General BCP for AuthN inter-working with PMIPv6
- Advanced documentation
  - Include other SDOs ' deployment and recommendations to use a particular authentication method
  - Include inter-working between WiFi AuthN and operators ' AAA
  - Include considerations related Web-Authentication
- Identification of protocol gaps and need for IETF specification

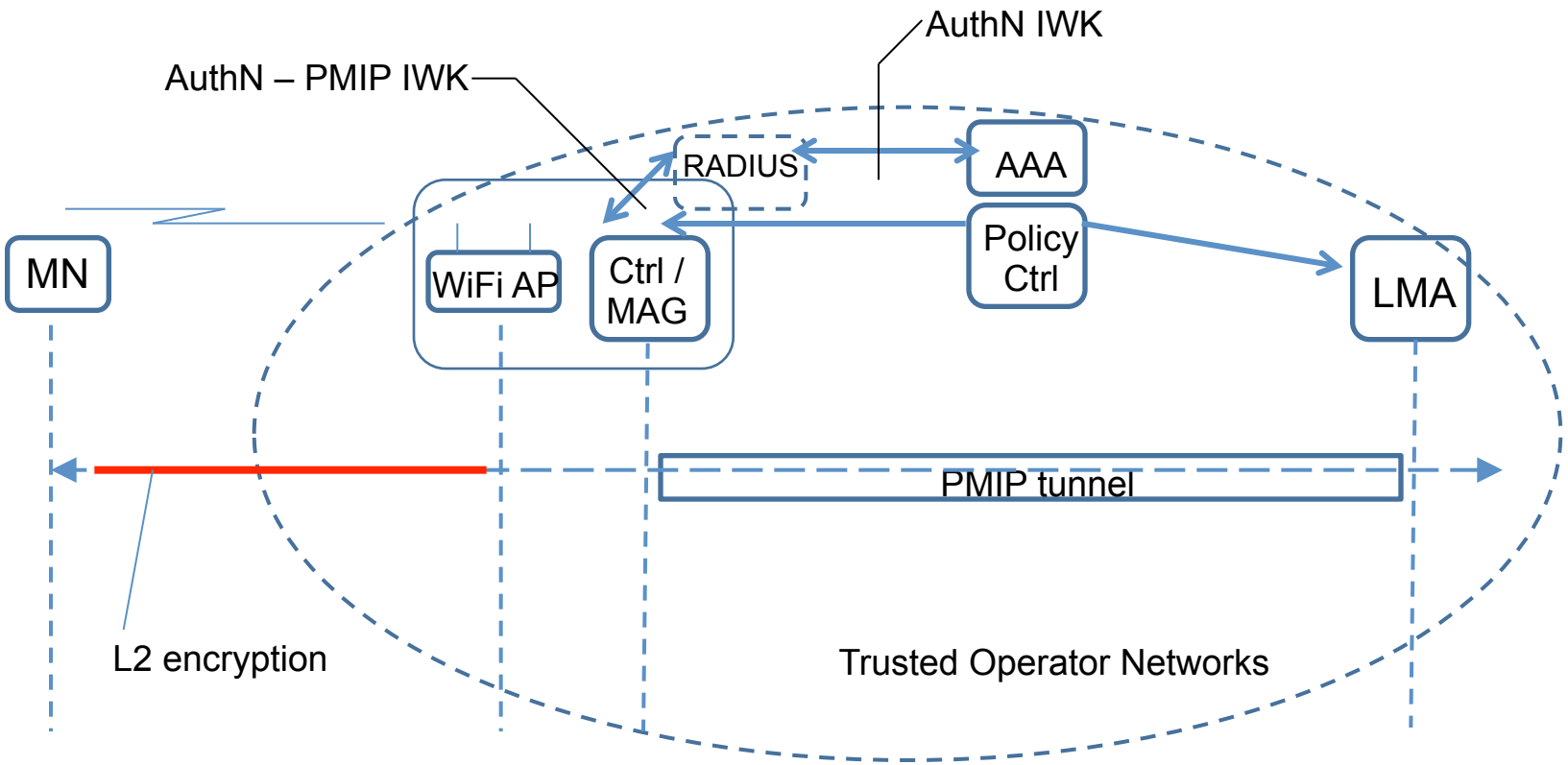
WLAN-EPC Integrated Architecture

- Identifies the primary protocol interfaces in the SP WiFI architecture



Enable WLAN trusted access

- WiFi Access AuthN integral part of the attach sequence
- PMIP tunnel between WLAN access and LMA
- Link-layer security between MN and WiFi AP
- AuthN inter-working with PMIPv6 and mobile operator AAA



Next Steps

- Reasonable scope?
- Adopt as a WG document