ERICSSON

MAP DOI: Modifications and Status

Contributions #27 and #102

Jari Arkko

Ericsson

Jari.Arkko@ericsson.com

ERICSSON

Contents

- MAP DOI
- Modifications in the –01 Internet Draft
- IKE profile
- Status in the IETF
- Process forward

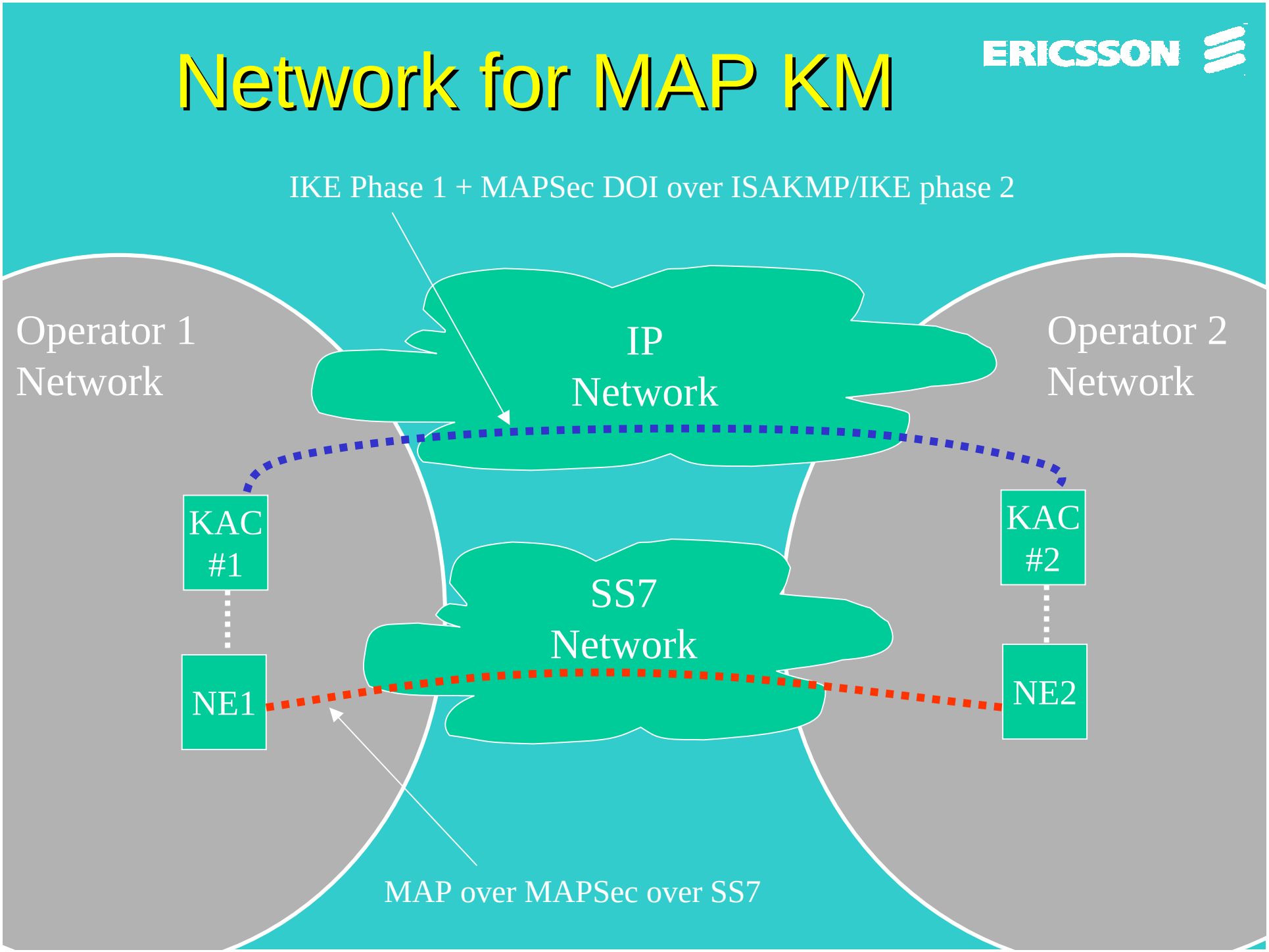
ERICSSON

The Key Management Problem

- How do we set up the security associations between the NEs?
- Lifetimes for security associations
- Capabilities negotiation, algorithms etc
- How to authenticate peers in a scalable manner
- Avoid the NxN configuration problem

=> A key management protocol is also needed

Network for MAP KM



ERICSSON

MAPSec DOI

- Provides key management for MAPsec via IP networks
  - Negotiate algorithms, periodic key refresh, …
  - Reuses IKE technology (code reuse, in the network anyway, avoid tricky protocol design)
- Run phase 1 exactly as in IKE (or KINK)
- Run phase 2 logically equivalently with IKE (or KINK), but with different data and attributes:
  - PROTO_IPSEC_ESP => PROTO_MAPSEC_MAPSEC
  - IPSEC_DES => MAPSEC_AES
  - Identities are not IP addresses, network or node addresses instead
  - ...

ERICSSON

Modifications in draft-arkko-map-doi-01.txt

- IKE has been profiled
- Phase 2 notifications have been removed
- AES-MAC - not HMAC_SHA1 - for MAPSEC
- (Phase 1 to use AES, SHA1)
- Attribute parsing requirements were simplified
- MAP_BLOWFISH has been removed
- MAP_NULL has been removed (pp used instead)
- Rules for assigning new numbers within this DOI have been clarified

ERICSSON

IKE Profile

- Only Phase 1 of IKE is used, the rest is MAP DOI
- Only IPv6 is mandatory
- Perfect Forward Secrecy (PFS) optional: Limits CPU requirements
- Aggressive mode to be mandatory, main mode optional: Limits complexity,loses some security against DoS
- Only FQDN identities to be mandatory: Limits complexity

ERICSSON

IKE Profile Cont'd

- AES, SHA1 used for protection of IKE: No AES-based hash yet in the IETF
- SA lifetime notifications will not be allowed: Limits complexity, ensures simultaneous timeout
- SA deletion will not be allowed: Allows pull-based mode to work
- Also note that IKE mandates preshared secrets, public-key based mechanisms are optional

ERICSSON

Status in the IETF

- Is an Internet-Draft (2nd version)
- Is submitted for Informational category
- Formally, does not require WG handling
- Has been presented to the IPsec WG, however. Main comments:
  - Why select IKE, not e.g. Photuris
  - MAP DOI reuses ISAKMP exactly as intented by the original specification
  - Informational RFC process, magic number allocation from IANA shouldn't be problems
  - Long time ago there was work on TCAP security, but it was abandoned
  - KAC vs node-to-node modes weren't discussed in the presentation

ERICSSON

Process Forward

1. Final agreement on this in SA3.
   - Can we make this happen by Friday (IETF submission)?
2. Put this document to an appendix of 33.200.
   - Acts as a temporary place until RFC status
   - Acts as a backup plan in case there are problems in the IETF
3. In parallel with the above, publish the DOI via IETF.
   - Requires a submission to the RFC Editor
   - This is an editorial process only, no WG
   - At this stage we also get the IANA number for the DOI
   - Technically, the ISAKMP RFC says DOI numbers only for standards track RFCs; in practise we don't believe this is a problem
4. When the DOI RFC comes out, replace appendix with a reference to the RFC.