draft-ietf-lisp-sec-00

F. Maino, V. Ermagan, A. Cabellos, D. Saucez, O. Bonaventure
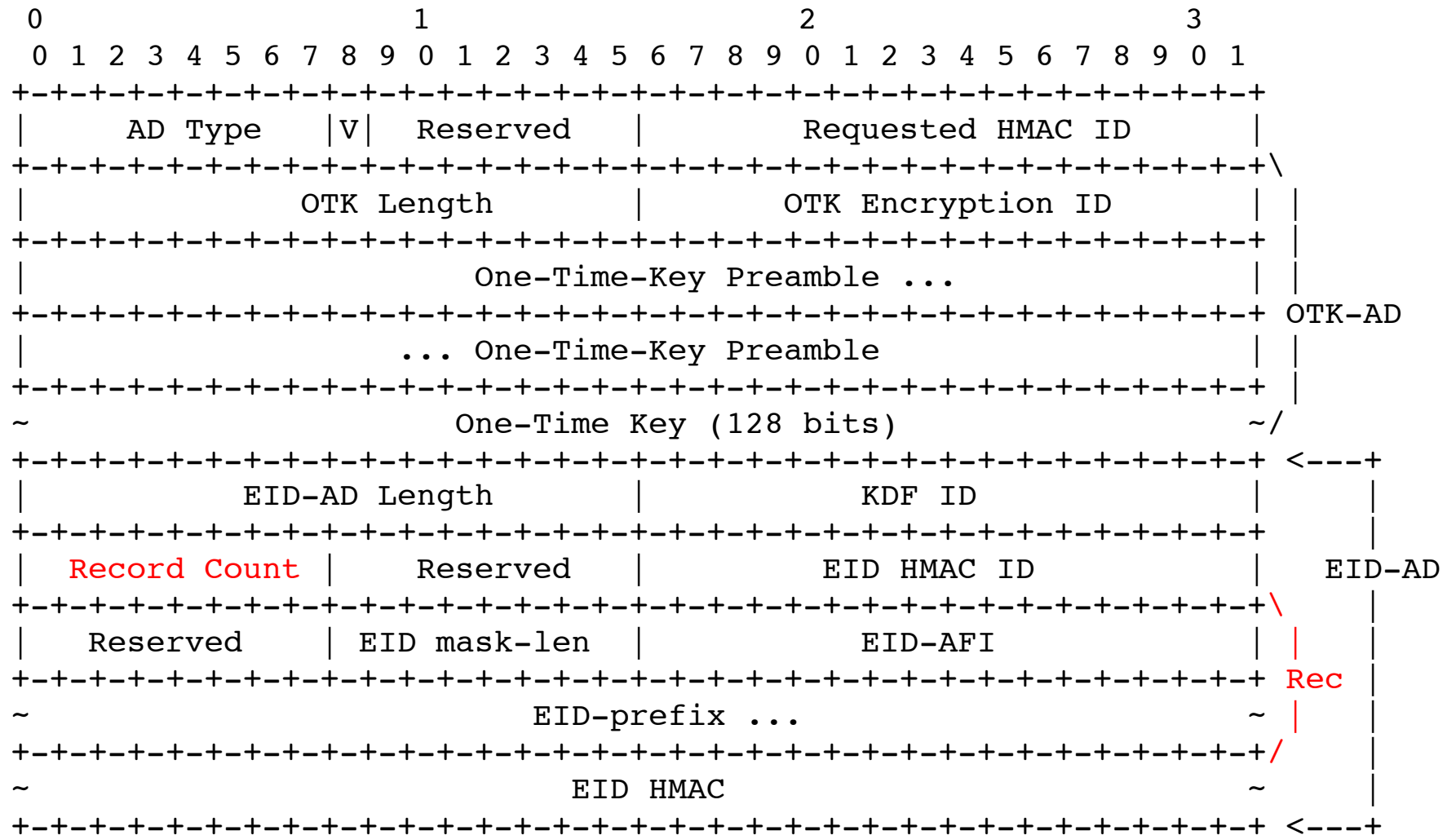
Presenter: Vina Ermagan

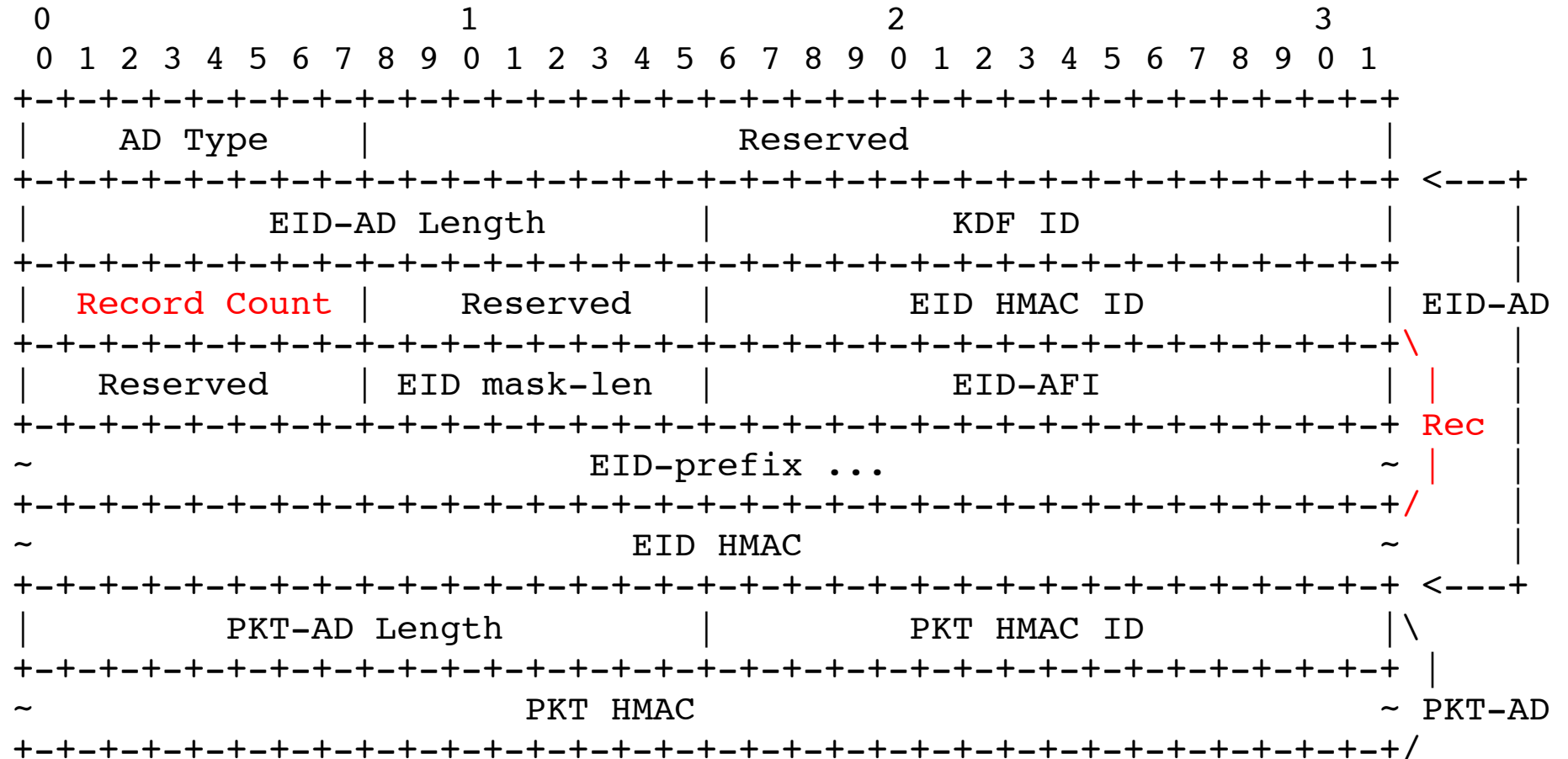IETF 81, Quebec City – July 2011

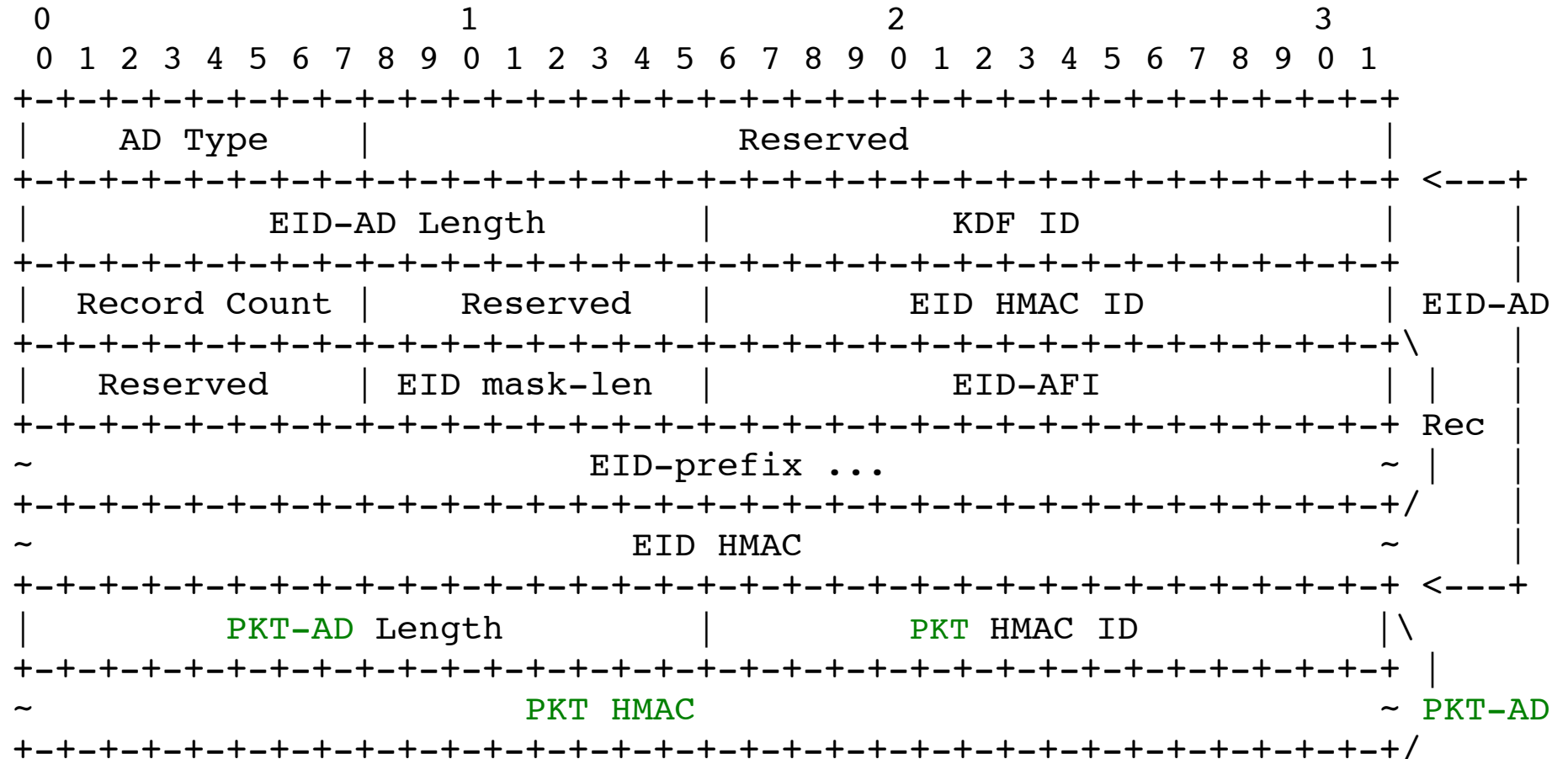# List of changes

- Clarified scope of coverage in abstract and introduction

- Record count for EID prefix in EID-AD

- Scope of PKT-HMAC

- Map-Reply record validation

- PITR processing

- MS and ETR co-location

- Terminology (ITR-OTK, MS-OTK)

ECM Authentication Data

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     AD Type     |V|  Reserved   |        Requested HMAC ID    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+\
|          OTK Length           |        OTK Encryption ID      | |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |
|                     One-Time-Key Preamble ...                 | |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ OTK-AD
|                 ... One-Time-Key Preamble                     | |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |
~                    One-Time Key (128 bits)                    ~/
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ <---+
|          EID-AD Length         |            KDF ID            |    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+    |
| Record Count  |    Reserved   |          EID HMAC ID          | EID-AD
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+\   |
|  Reserved    | EID mask-len   |            EID-AFI            | |  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ Rec |
~                         EID-prefix ...                        ~ |  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+/   |
~                           EID HMAC                            ~    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ <---+
```

Map-Reply Authentication Data

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    AD Type       |                 Reserved                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ <---+
|         EID-AD Length         |              KDF ID           |     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+     |
|  Record Count |    Reserved   |           EID HMAC ID         | EID-AD
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+\    |
|  Reserved     | EID mask-len  |            EID-AFI            | |   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ Rec |
~                          EID-prefix ...                       ~ |   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+/    |
~                            EID HMAC                            ~    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ <---+
|         PKT-AD Length         |            PKT HMAC ID         |\
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |
~                            PKT HMAC                            ~ PKT-AD
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+/
```

List of changes

- Clarified scope of coverage in abstract and introduction

- Record count for EID prefix in EID-AD

- Scope of PKT-HMAC
  - Includes entire Map-Reply packet now

- Map-Reply record validation

- PITR processing

- MS and ETR co-location

- Terminology (ITR-OTK, MS-OTK)

Map-Reply Authentication Data

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     AD Type       |                 Reserved              |    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ <---+
|       EID-AD Length        |               KDF ID          |    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+    |
| Record Count  |   Reserved    |          EID HMAC ID        | EID-AD
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+\   |
|   Reserved    | EID mask-len  |             EID-AFI         | |   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ Rec |
~                        EID-prefix ...                       ~ |   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+/   |
~                           EID HMAC                          ~    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ <---+
|       PKT-AD Length        |           PKT HMAC ID          |\
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |
~                          PKT HMAC                           ~ PKT-AD
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+/
```

List of changes

- Clarified scope of coverage in abstract and introduction

- Record count for EID prefix in EID-AD

- Scope of PKT-HMAC

- ## Map-Reply record validation

  – Both EID-AD and PKT-AD are valid, and

  – The intersection of the EID prefix in the Map-Reply EID-record with one of the EID prefixes contained in the EID-AD is not empty.

- PITR processing

- MS and ETR co-location

- Terminology (ITR-OTK, MS-OTK)

List of changes

- Clarified scope of coverage in abstract and introduction

- Record count for EID prefix in EID-AD

- Scope of PKT-HMAC

- Map-Reply record validation

- PITR processing
  - Similar to ITR if not directly connected to ALT
  - If directly connected to ALT, performs both ITR and Map-Resolver processing

- MS and ETR co-location

- Terminology (ITR-OTK, MS-OTK)

List of changes

- Clarified scope of coverage in abstract and introduction

- Record count for EID prefix in EID-AD

- Scope of PKT-HMAC

- Map-Reply record validation

- PITR processing

- ## MS and ETR co-location

  - ETR falls within trust domain of Map-Servers

  - ETR overclaiming attack in this case is not included in threat model

- Terminology (ITR-OTK, MS-OTK)

List of changes

- Clarified scope of coverage in abstract and introduction

- Record count for EID prefix in EID-AD

- Scope of PKT-HMAC

- Map-Reply record validation

- PITR processing

- MS and ETR co-location

- Terminology
  - OTK => ITR-OTK
  - ETR-OTR => MS-OTK
  - LOC-AD => PKT-AD

THANKS!