draft-maino-lisp-sec-00

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

IETF 80, Prague – March 2011

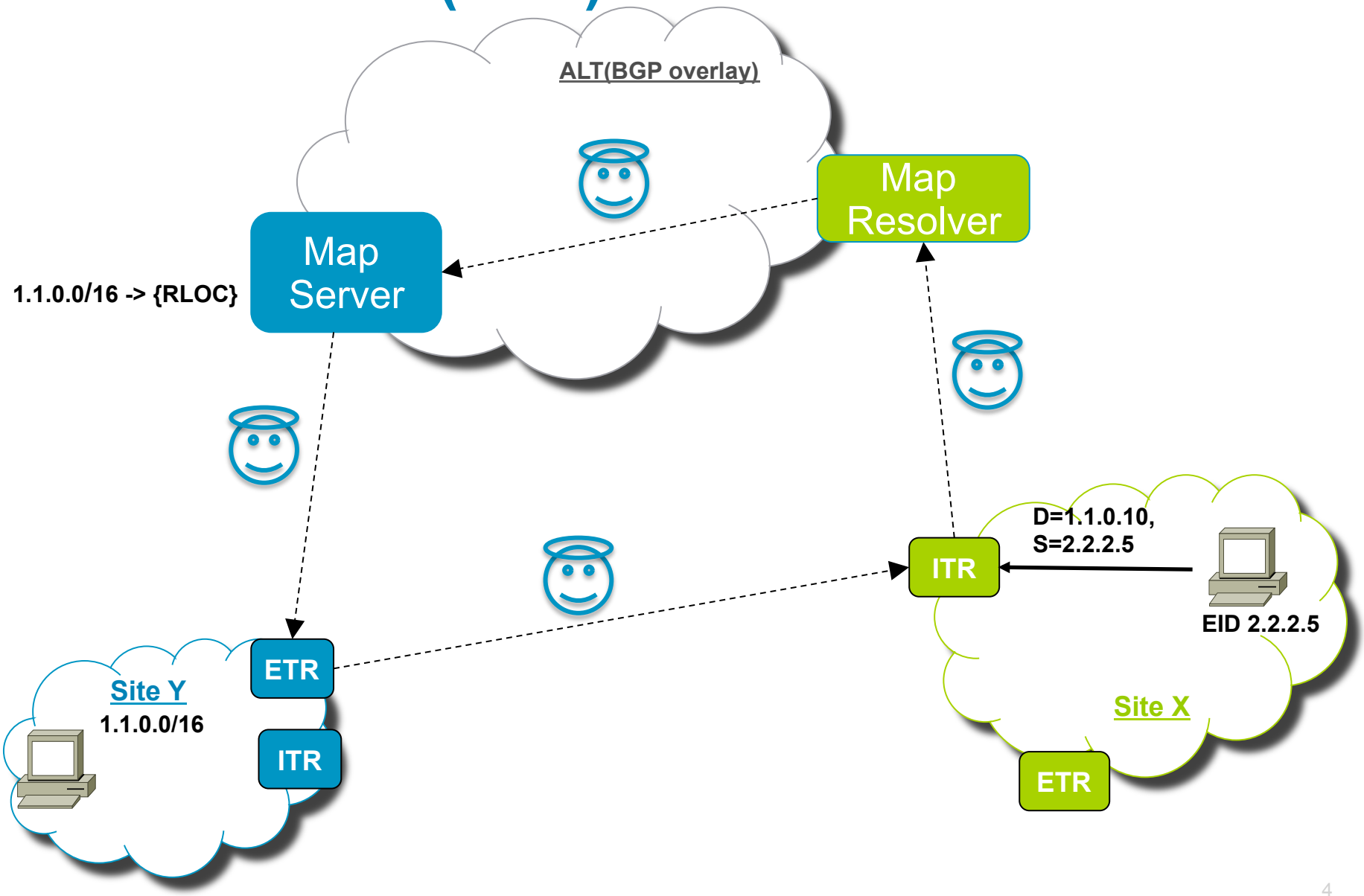
Agenda

- In-Scope
- Out-of-Scope
- One-Time-Key Details
- Threat Model
- LISP-SEC Control Messages
- Q&A

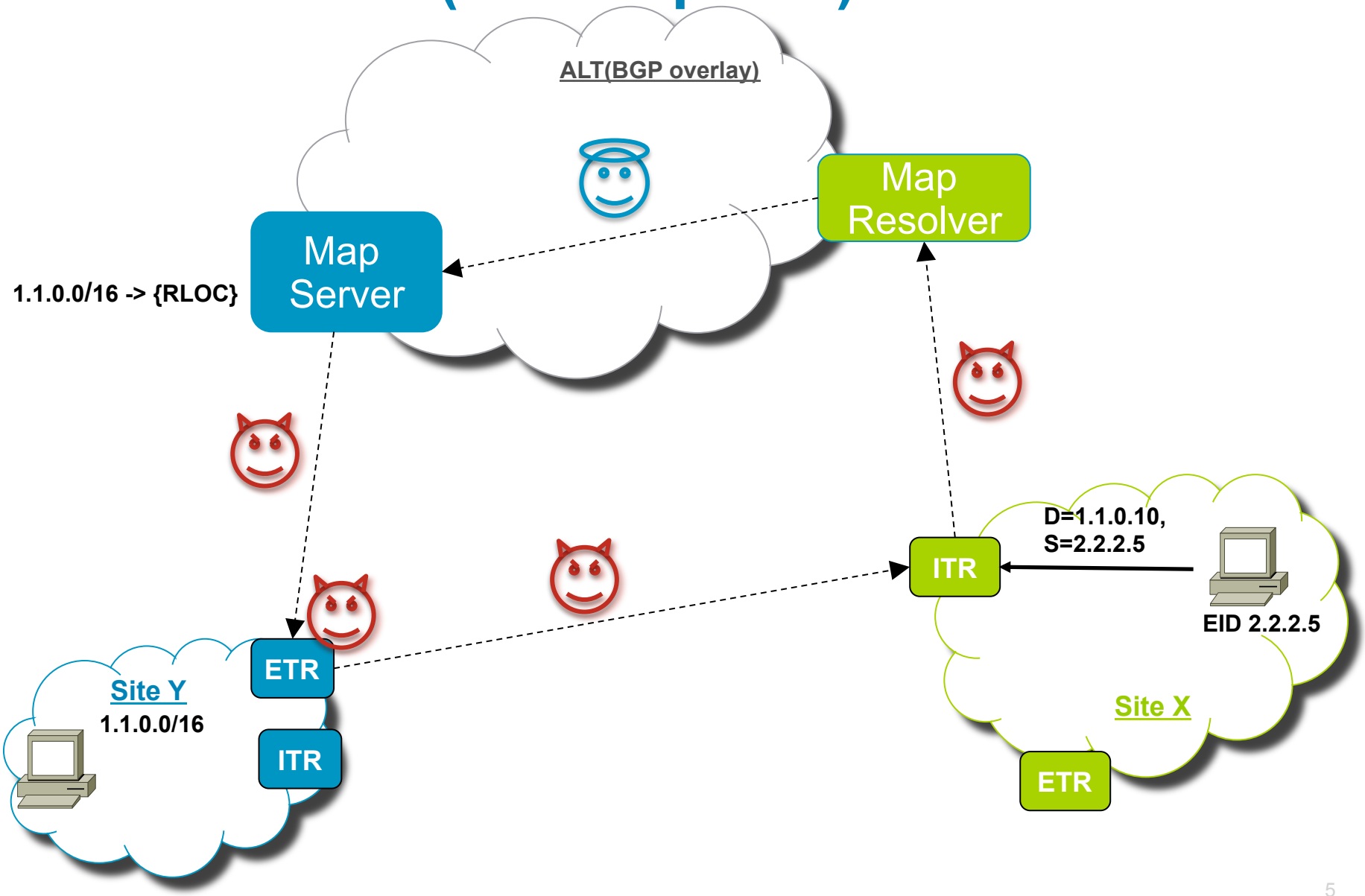
In-Scope

- Protect the Map-Request/Map-Reply exchange
  - –Map-Reply origin authentication, anti-replay and integrity protection
- Protect from over claiming attacks
  - –Prevent the ETR from over claiming EID prefixes

Threat Models (now)



Threat Models (with lisp-sec)



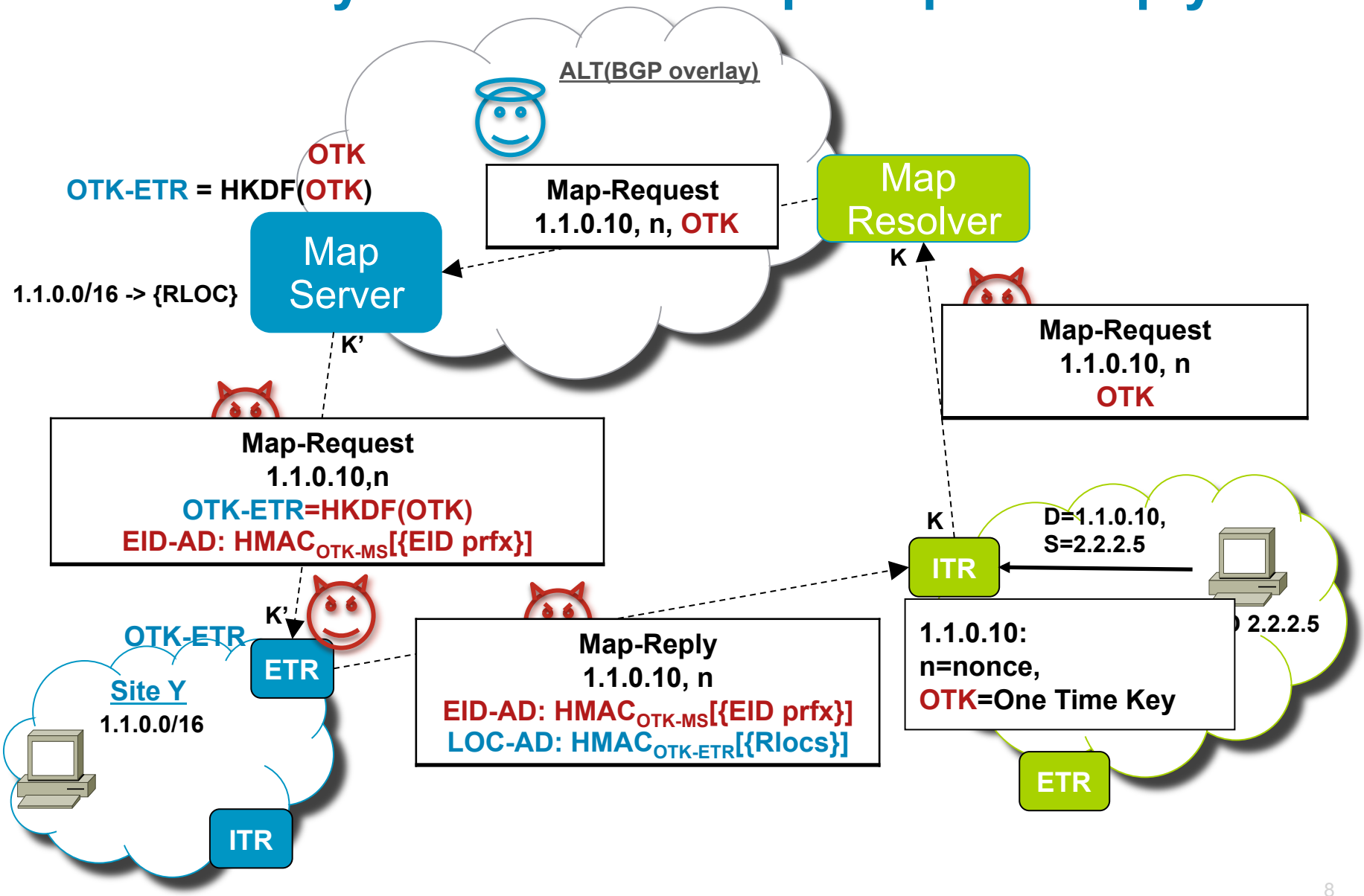
Out-of-Scope

- EID prefix authorization
- ALT/Mapping System security
- Assumptions:
  - –The Mapping System is expected to deliver Map-Request messages to their intended destinations as identified by the EID
  - –No Man-in-the-Middle (MiM) attack can be mounted within the LISP Mapping System
  - –The Mapping System provides confidentiality and integrity protection to LISP control messages (within the Mapping System)

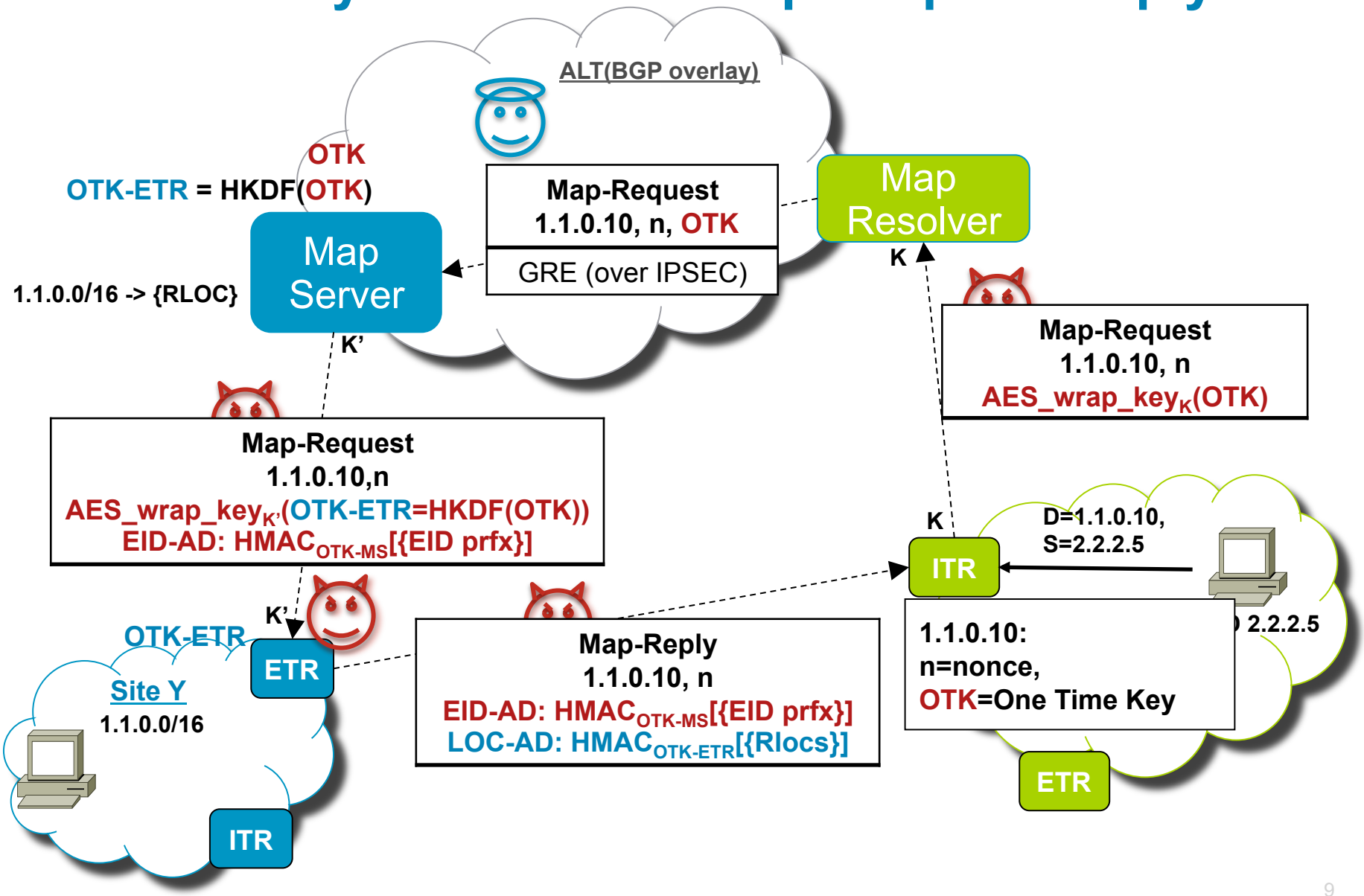
Map-Request/Reply Integrity and EID-prefix Overclaim Protection

ONE-TIME KEY

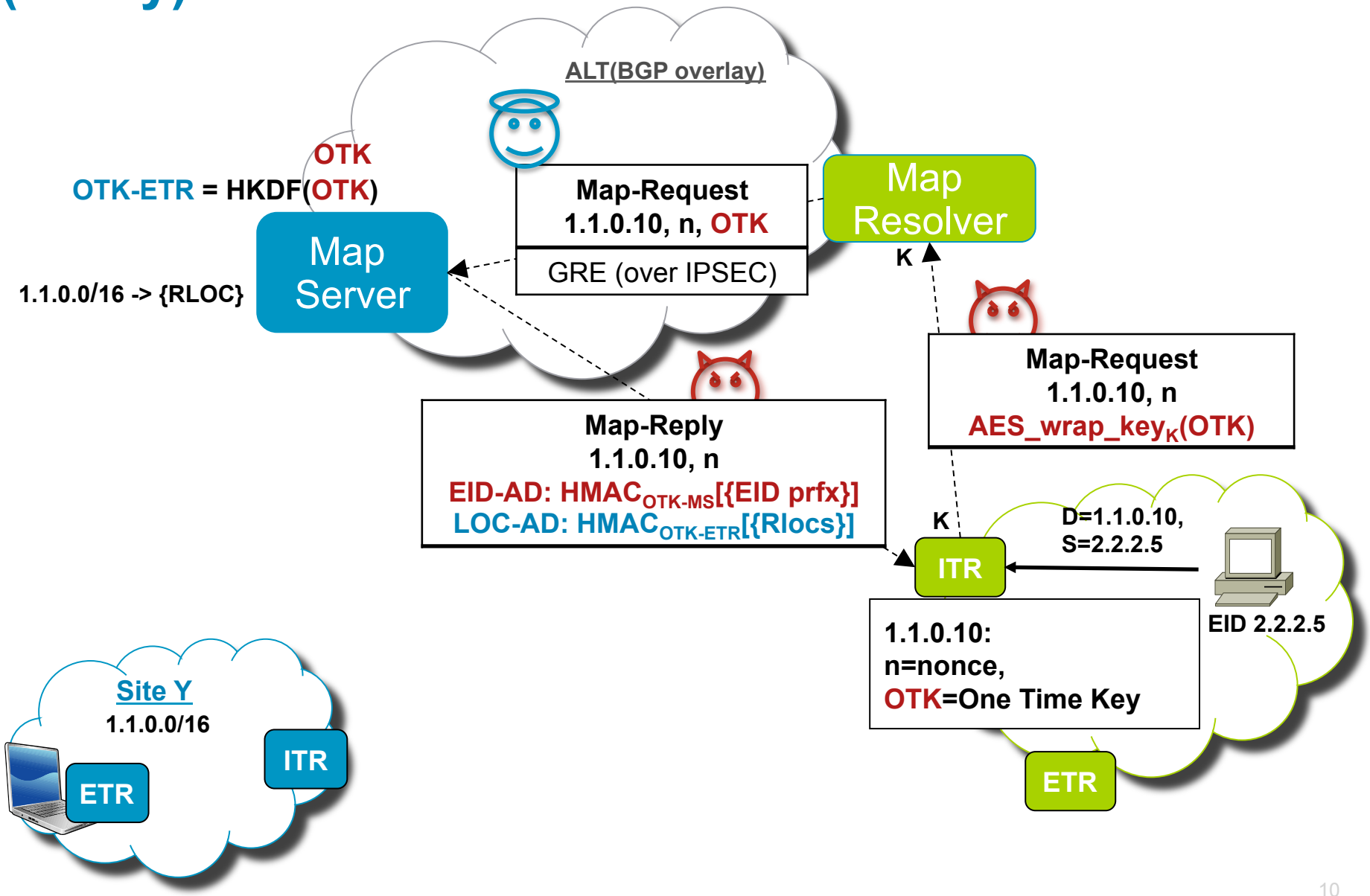
One-Time Keyed HMAC on Map-Request/Reply



One-Time Keyed HMAC on Map-Request/Reply



One Time Keyed HMAC on Map-Request/Reply (Proxy)



OTK Details

- Default OTK is 128-bit
- OTK is encrypted with NIST AES Wrap Key
  - –64-bit of wrap metadata pre-pended to OTK when encrypted
- ITR stores <n, OTK>
  - –May store HKDF(OTK) as a possible optimization

OTK Security

- Map-Reply Integrity is protected using the OTK as a shared secret between the ITR and the MS/ETR
  - –ALT (MS) is trusted for EID prefix authorization, and for OTK transport
- NIST AES Wrap Key is used to
  - –protect OTK confidentiality from ITR to MR
  - –protect OTK confidentiality from MS to ETR (in the non-proxy case)
  - –authenticate ITR to MR, and MS to ETR
- IPsec may be used to protect OTK confidentiality and integrity over the ALT infrastructure

Key Derivation

- OTK-MS is derived from OTK applying a KDF to prevents MS impersonation
  - –including overclaiming attacks mounted at the ETR
- Default KDF is the HMAC-based Key Derivation Function (HKDF)
  - –RFC 5869 (Krawczyk, Eronen)

Threat Model

1. The ALT Mapping System is *secure and well functioning*, and delivers Map-Requests to their intended destinations as identified by the EID
   - EID prefix authorization is delegated to mapping Server Configuration
   - Mapping Server asserts EID prefix authorization
   - Mapping Server is trusted to do proper RLOC mapping (proxy case)
2. ALT GRE tunnels prevent *Man-in-the-Middle (MiM)* attacks and provide *integrity and confidentiality* of the information carried over ALT (i.e. the nonce)
   - Tunnels are in the core of the internet and, optionally, can be secured by GRE over IPsec

Threat Model (II)

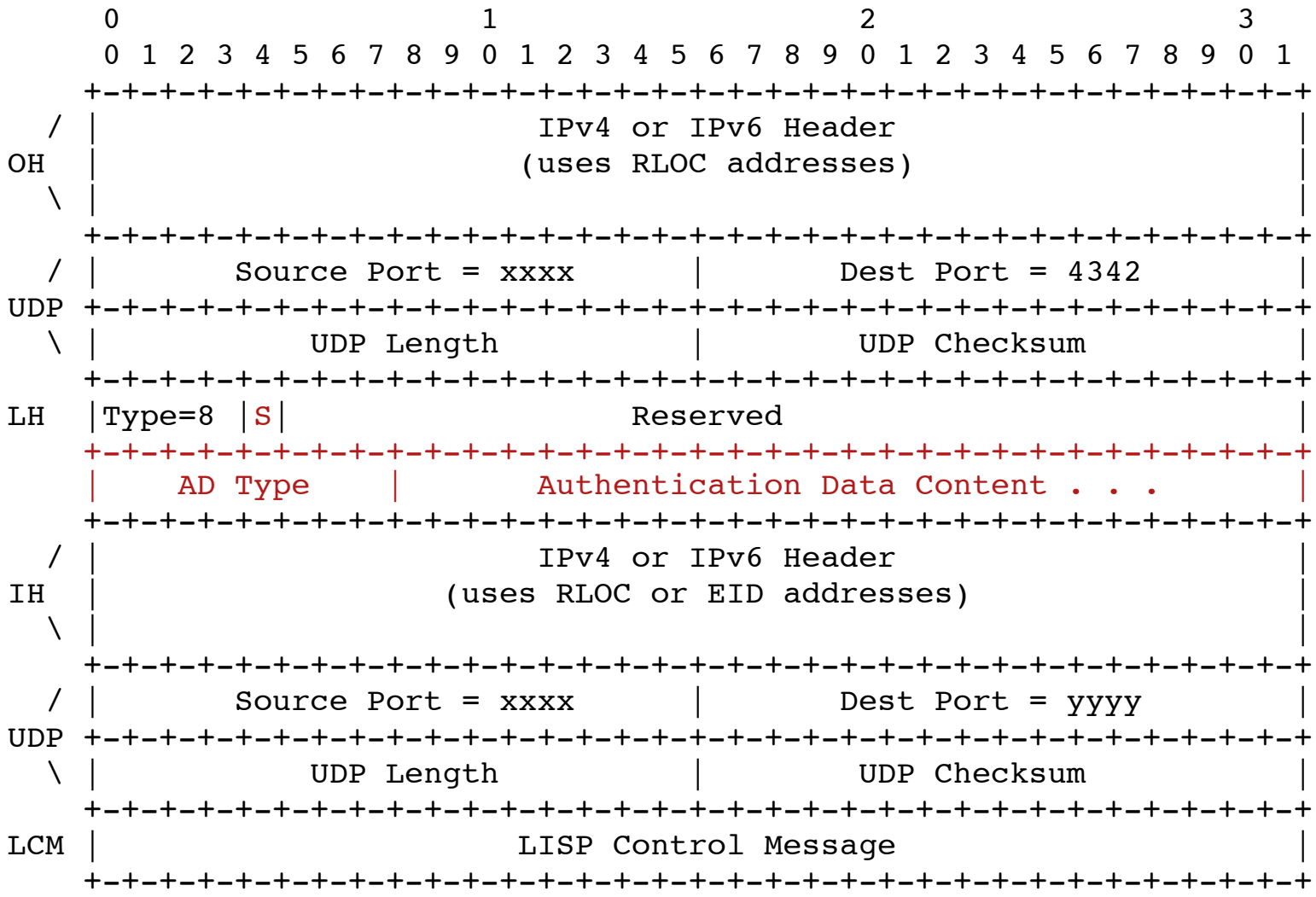
3. MiM attacks can be mounted *outside, and only outside,* of the ALT infrastructure
4. ETR can mount *prefix overclaiming* attacks
   – maliciously or unintentionally (e.g. because the ETR is hacked/compromised)

LISP-SEC CONTROL MESSAGES

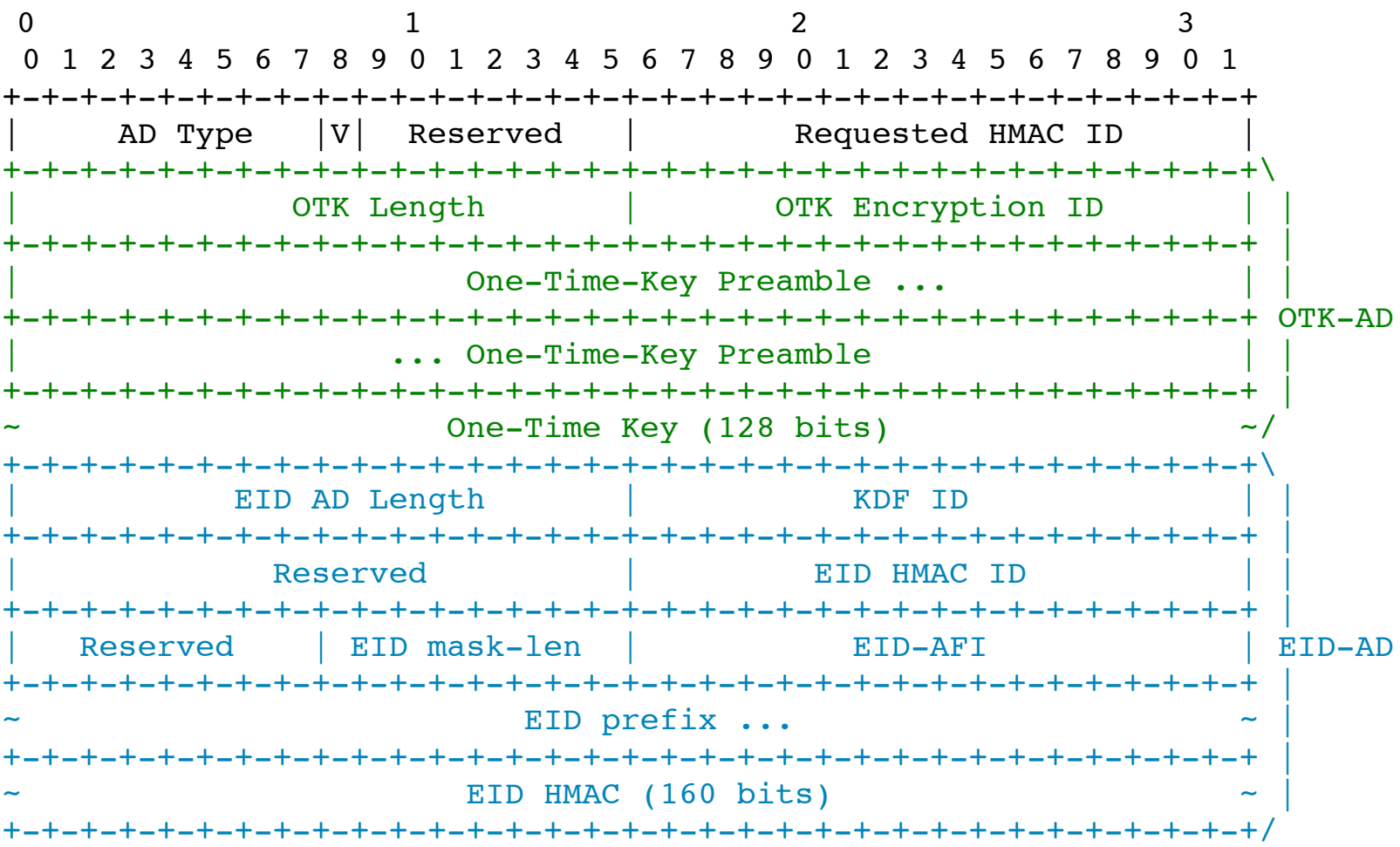
Control Messages Details

- ECM header is extended to include LISP-SEC metadata used to protect Map-Request
  - –LISP-SEC metadata is in an optional Authentication Data field
  - –Map-Requests are ECM encapsulated over ALT (no need to re-originate Map-Requests)
- Map-Reply is extended to include LISP-SEC metadata in an optional Authentication Data field

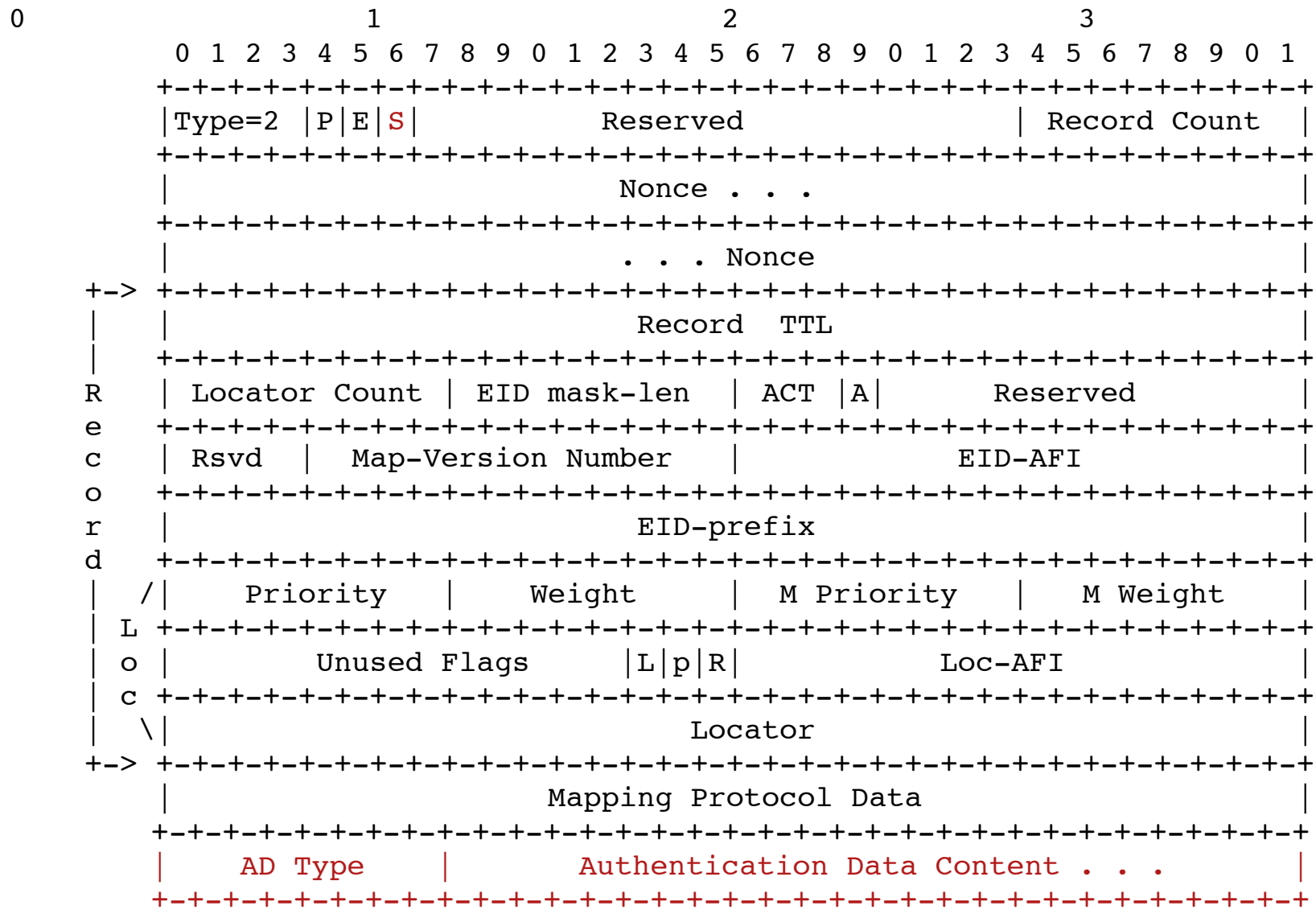
ECM Message LISP-SEC Extensions



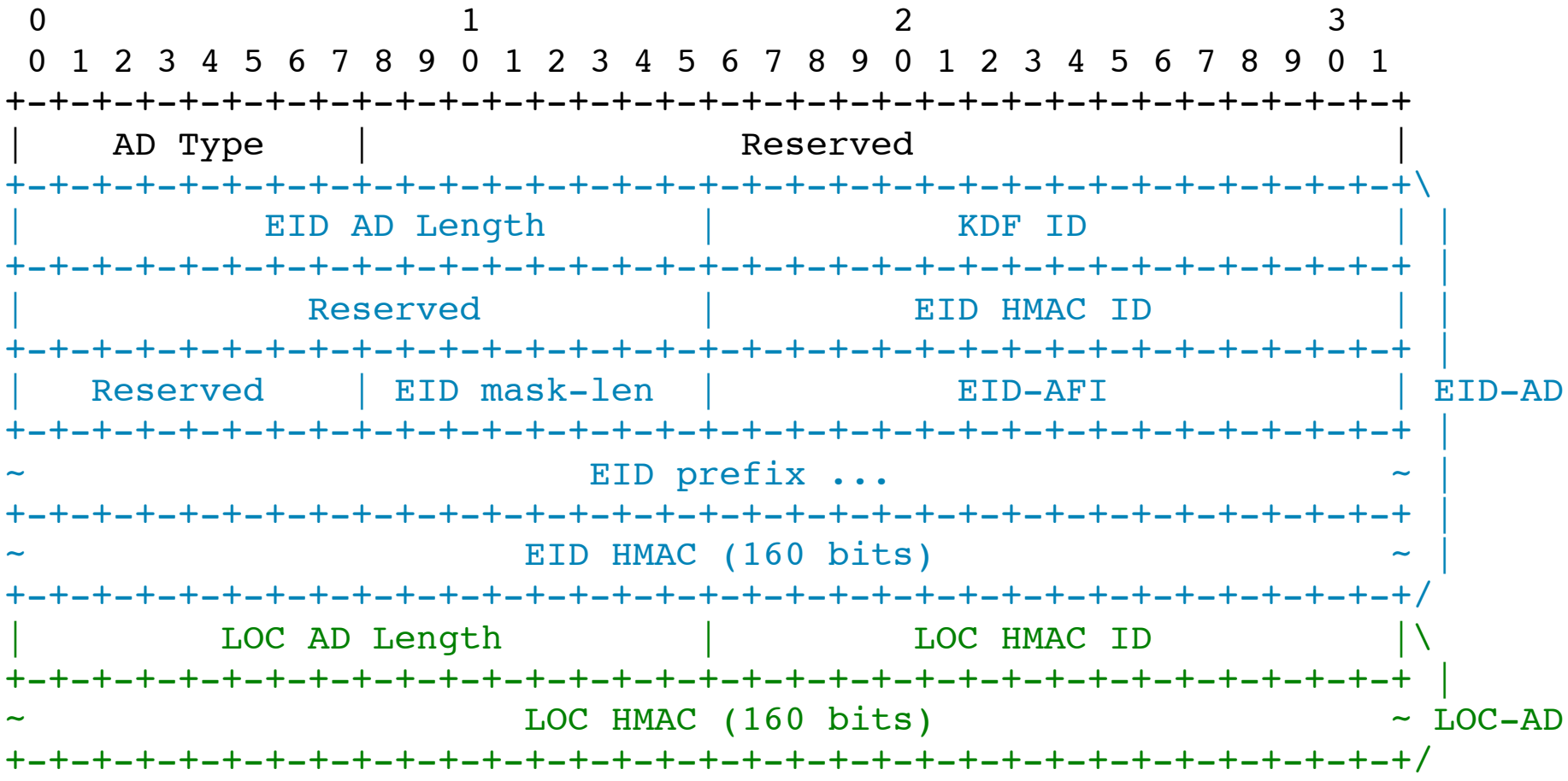
ECM Authentication Data



Map-Reply LISP-SEC Extensions



Map-Reply Authentication Data



THANKS!