draft-ietf-lisp-sec-18

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

June 2nd Updates

1. a mechanism that allows an ITR to secure downgrade to non LISP-SEC Map-Requests, if it wishes to do so. This is done as discussed in the list and in Prague with Ben
2. the use of a per-message key (derived from the pre-shared secret) to protect transport of One-Time-Key from ITR->Map-Resolver and from Map-Server->ETR. This is consistent with the changes that are being introduced in 6833bis for Map-Register, and with what discussed with Ben in Prague
3. Comments posted by Med on 1/28 are addressed

Changes in ECM Authentication Data

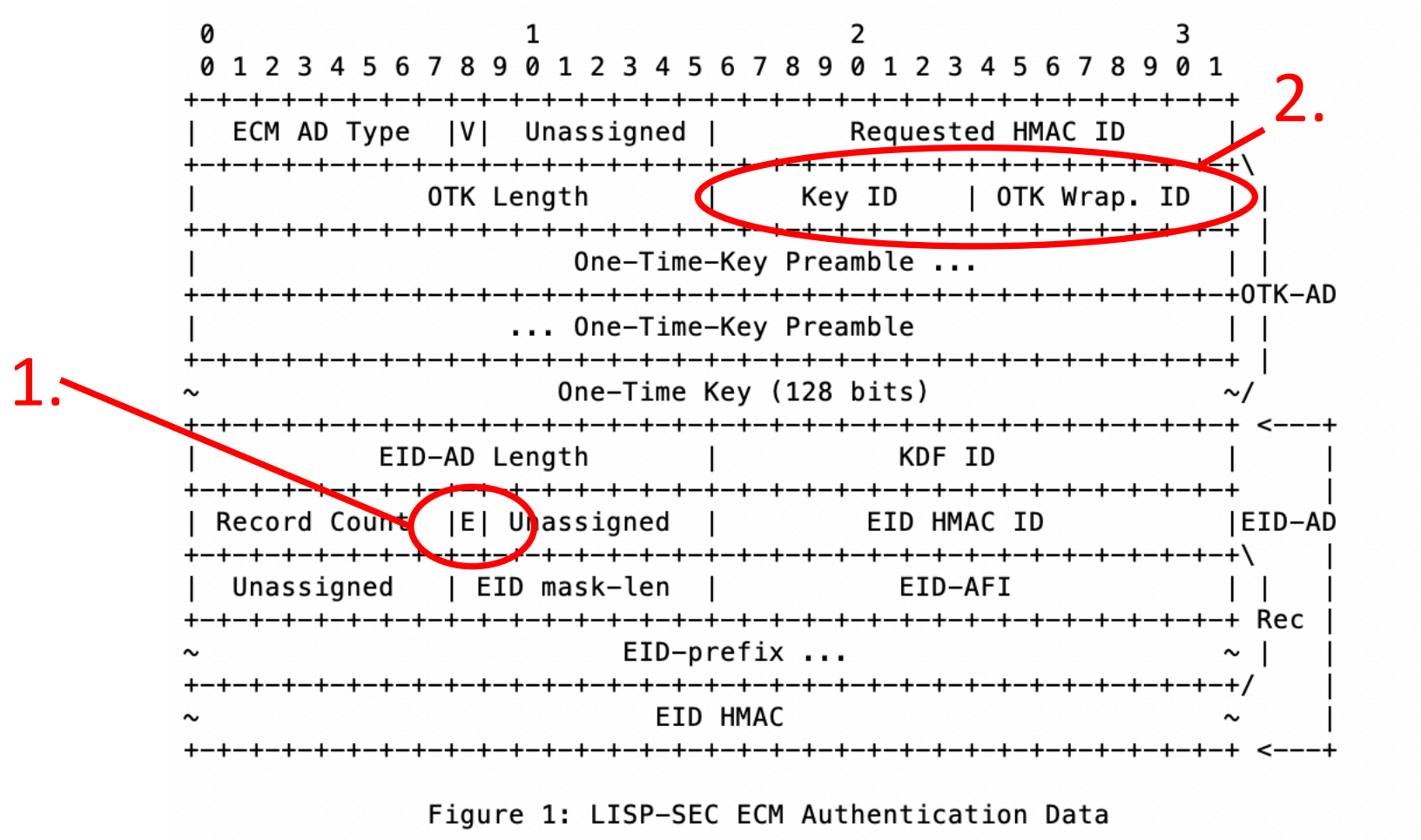

Figure 1: LISP-SEC ECM Authentication Data

ITR Secure Downgrade to non LISP-SEC

- allows secure downgrade to non LISP-SEC (if the ITR chooses to do so)
- Uses the ETR-Cant-Sign bit ‘E’
- Described in section 5.7

Matching Condition	Processing
1. At least one of the ETRs authoritative for the EID prefix included in the Map-Request registered with the P-bit set to 1	The Map-Server MUST generate a LISP-SEC protected Map-Reply as specified in Section 5.7.2. The ETR-Cant-Sign E-bit in the EID Authentication Data (EID-AD) MUST be set to 0.
2. At least one of the ETRs authoritative for the EID prefix included in the Map-Request registered with the S-bit set to 1	The Map-Server MUST generate a LISP-SEC protected Encapsulated Map-Request (as specified in Section 5.7.1), to be sent to one of the authoritative ETRs that registered with the S-bit set to 1 (and the P-bit set to 0). If there is at least one ETR that registered with the S-bit set to 0, the ETR-Cant-Sign E-bit of the EID-AD MUST be set to 1 to signal the ITR that a non LISP-SEC Map-Request might reach additional ETRs that have LISP-SEC disabled.
3. All the ETRs authoritative for the EID prefix included in the Map-Request registered with the S-bit set to 0	The Map-Server MUST send a Negative Map-Reply protected with LISP-SEC, as described in Section 5.7.2. The ETR-Cant-Sign E-bit MUST be set to 1 to signal the ITR that a non LISP-SEC Map-Request might reach additional ETRs that have LISP-SEC disabled.

Per-message Key to Protect OTK transport

- “OTK Encryption ID” 16-bit field in the ECM Authentication Data is split into two 8-bit fields:
  - **Key ID** identifies the pre-shared secret
  - **OTK Wrapping ID** identifies the KDF used to derive the per-message OTK encryption key AND the OTK Wrapping algorithm
- per-message OTK encryption key is derived from pre-shared secret
  - described in Section 5.5
  - OTK Wrap. ID identifies both the *Key Wrap Algorithm* as well as the *Key Derivation Function* (AES-KEY-WRAP-128+HKDF-SHA256)
  - consistent with how last rev of 6833bis derives per-message Map-register authentication key

Comments Posted by Med on June 3rd

- Will be addressed in rev -19 (thanks for the detailed review Med!)

Next Steps

- Review by SECDIR