SECDIR Review of 6830bis and 6833bis

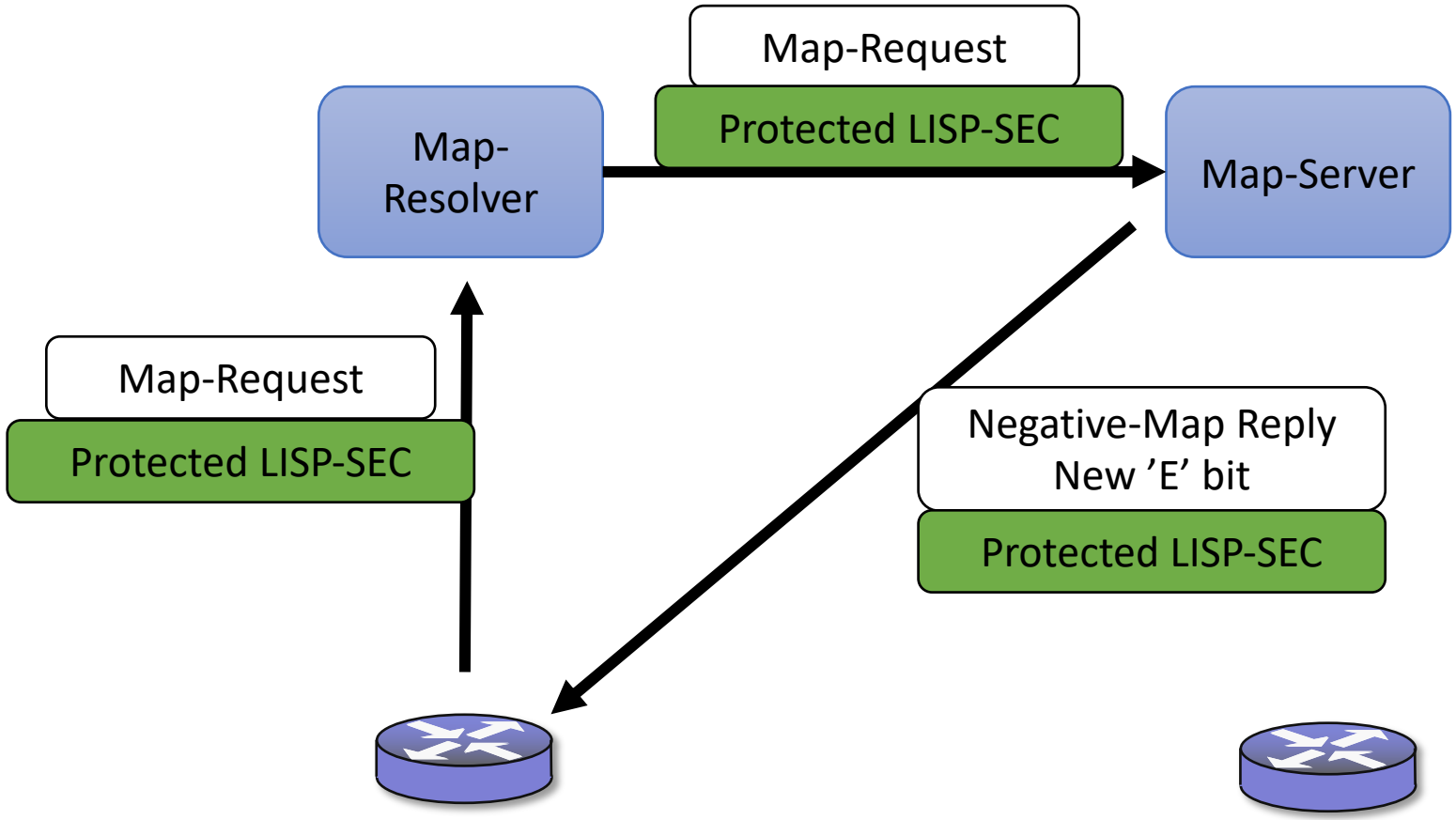
IETF 104 – Prague

March 2019

List of DISCUSS issues

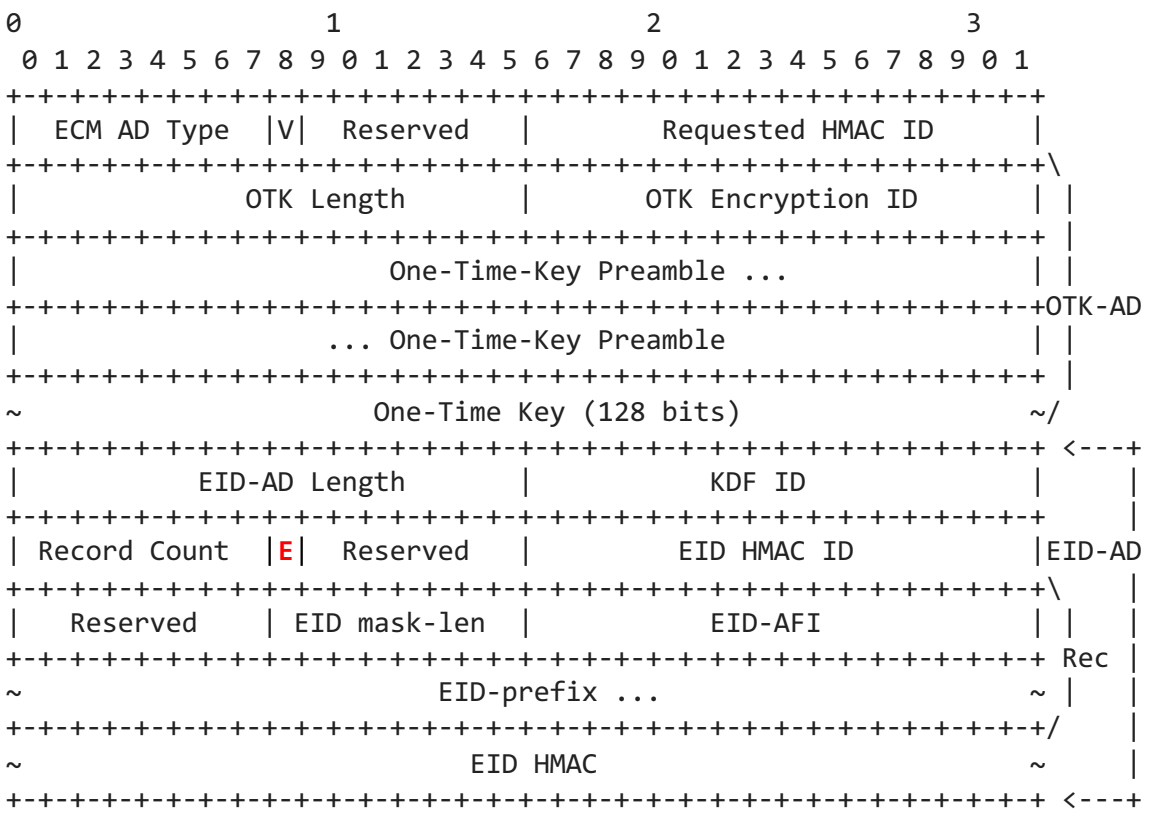
1. Incremental deployment of LISP-SEC and downgrade attacks
2. Security of the gleaning mechanism
   - Traffic redirection of off-path attackers
3. Security of the LSB mechanism
   - Spoofing attacks
4. Security of the Echo-Nonce mechanism
   - Nonce is too short to prevent off-path attackers
5. Security of Map-Versioning
   - Gagging updates
6. Anti-Replay protection of Map-Register
7. Long-lived keys to authenticate Map-Register
8. Map-Request/Reply anti-replay protection

1.- Incremental deployment of LISP-SEC and downgrade attacks



Depending on local policy the ITR
can re-transmit a non-LISP-SEC Map-Request

1.- Incremental deployment of LISP-SEC and downgrade attacks



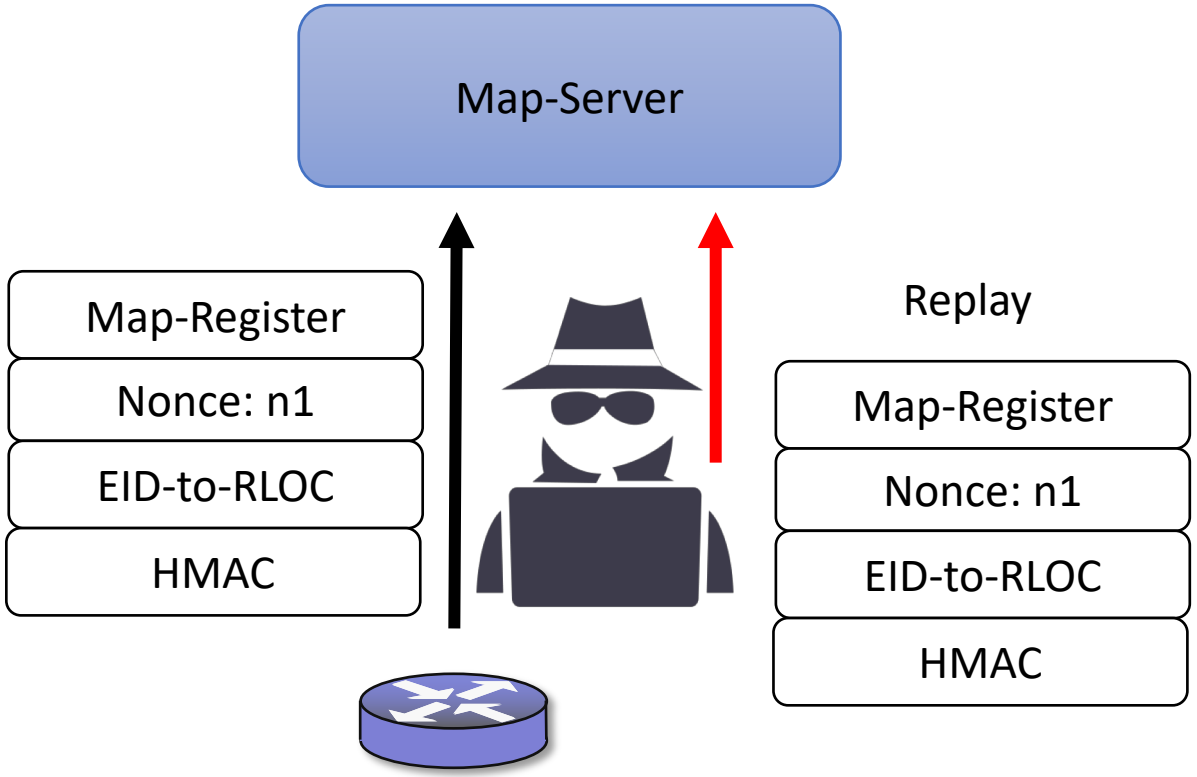
LISP-SEC ECM Authentication Data

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). 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.

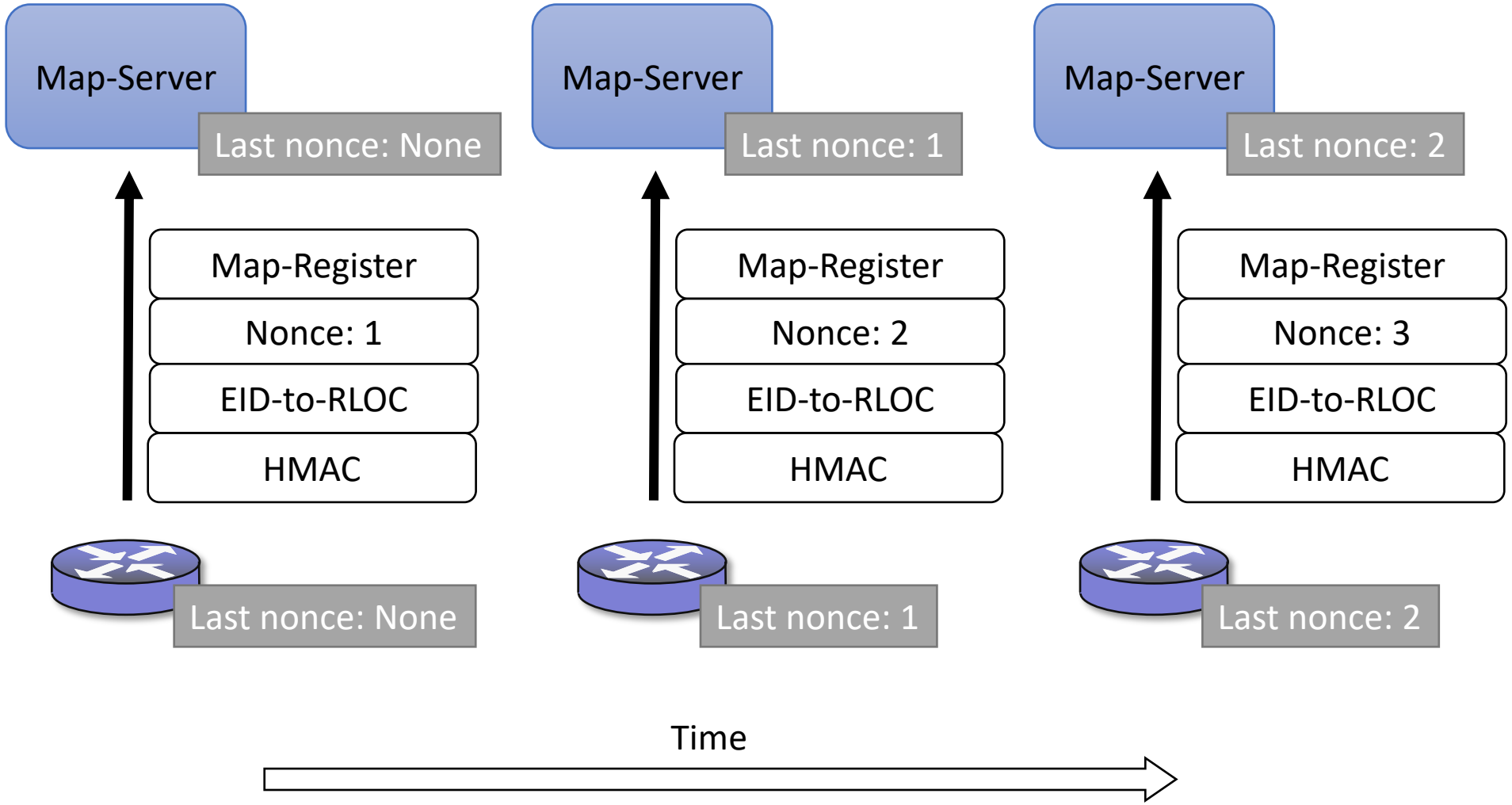
2,3,4,5- Security of Gleaning, LSB, Echo-Nonce and Map-Versioning

- Users communicating over the public Internet SHOULD NOT use Gleaning, LSB, Echo-Nonce and Map-Versioning
- LSB SHOULD work coupled with Map-Versioning

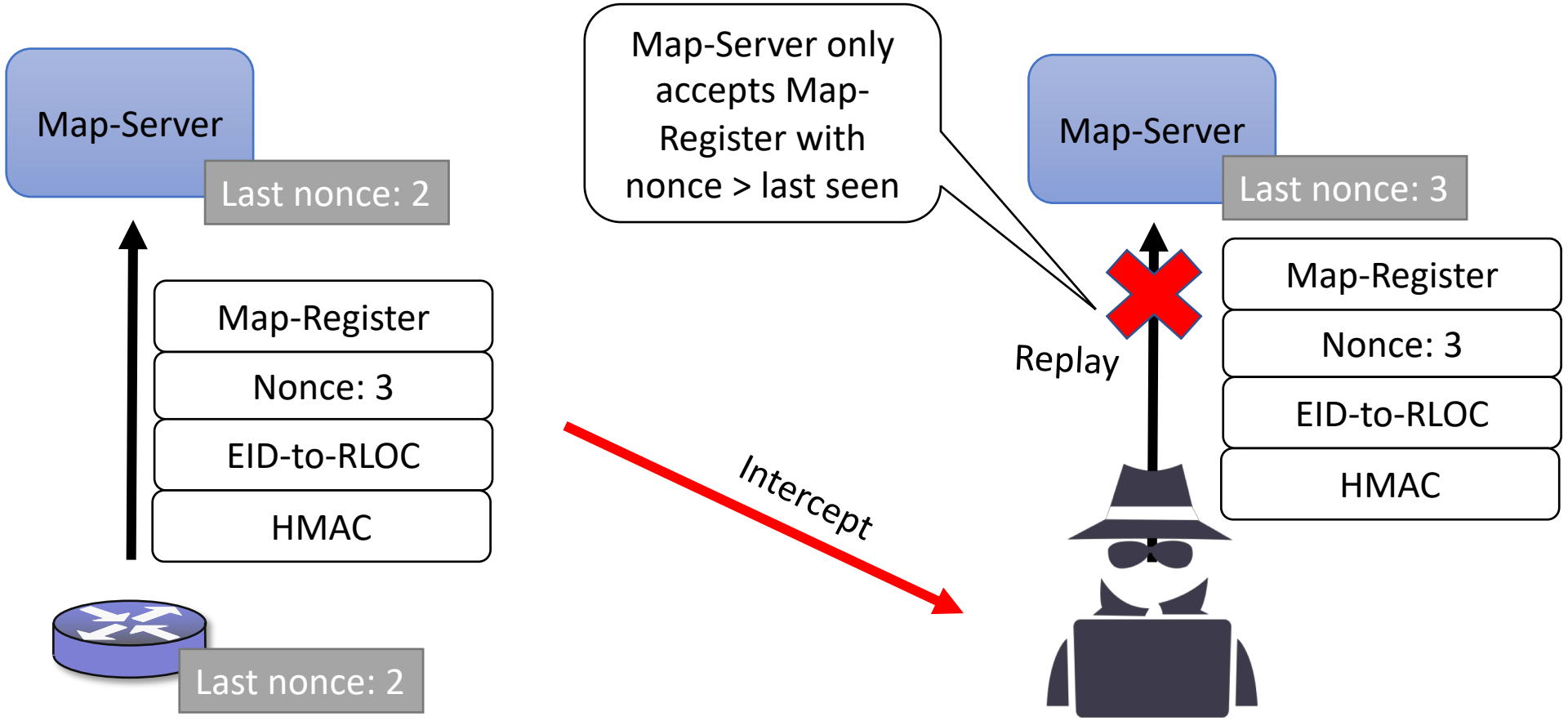
6.- Anti-Replay protection of Map-Register



6.- Anti-Replay protection of Map-Register



6.- Anti-Replay protection of Map-Register



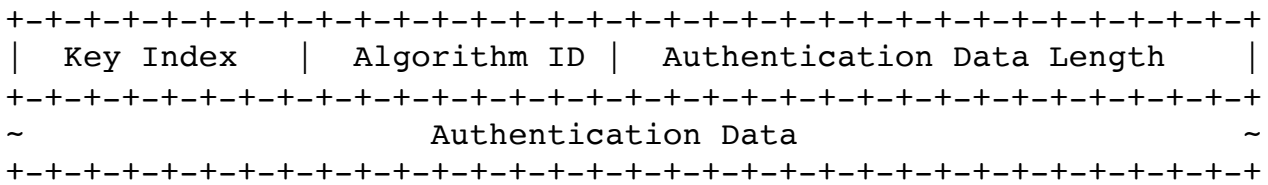
6.- Anti-Replay protection of Map-Register

- Nonce is permanently stored by ETR, and bound to PSK
  - At the typical registration rate of a map-register per minute the nonce will wrap around after 2^32 minutes (~ 8,000 years)
- ETRs that can’t store nonce through reboots MUST change PSK at every reboot

```
An ETR that registers to the mapping system SHOULD store
the last nonce sent in persistent storage so when it restarts it
can continue using an incrementing nonce.  If the the ETR cannot
support saving the nonce, then when it restarts it MUST use a new
authentication key to register to the mapping system.  A Map-
Server MUST track and save in persistent storage the last nonce
received for each ETR xTR-ID that registers to it.
```

7.- Long-lived keys to authenticate Map-Register with nonce

Key-Derivation Function algorithm



1.- The KDF algorithm is identified by the field “Algorithm ID” according to the table in Section 12.5.
2.- The MAC algorithm is identified by the field “Algorithm ID” according to the table in Section 12.5.
3.- The string s is initialized to "Map-Register Authentication"
4.- The shared secret used to derive the key is identified by PSK[KI], that is the shared secret indexed by the key-id.
5.- The derived key is computed as: derived_key=KDF(nonce+s+PSK[KI])
6.- The MAC output is computed using the MAC algorithm and the derived_key over the
entire Map-Register payload (from and including the LISP message type field through the end of the last RLOC record) with the authenticated data field preset to 0.

8.- Map-Request/Reply Anti-Replay Protection (clarification)

- Anti-replay protection of Map-Request/Reply protocol exchange is provided by LISP-SEC's OTK
  - This relaxes requirements on nonce that is just used to match map-reply to map-request

Upon receiving a Map-Reply, the ITR must verify the integrity of both the EID-AD and the PKT-AD, and MUST discard the Map-Reply if one of the integrity checks fails. **After processing the Map-Reply, the ITR MUST discard the <nonce,ITK-OTK> pair associated to the Map-Reply**