Update on 6830bis/6833bis documents

Albert Cabellos (acabello@ac.upc.edu)

IETF 105 – Montreal

July 2019

Since IETF - 104

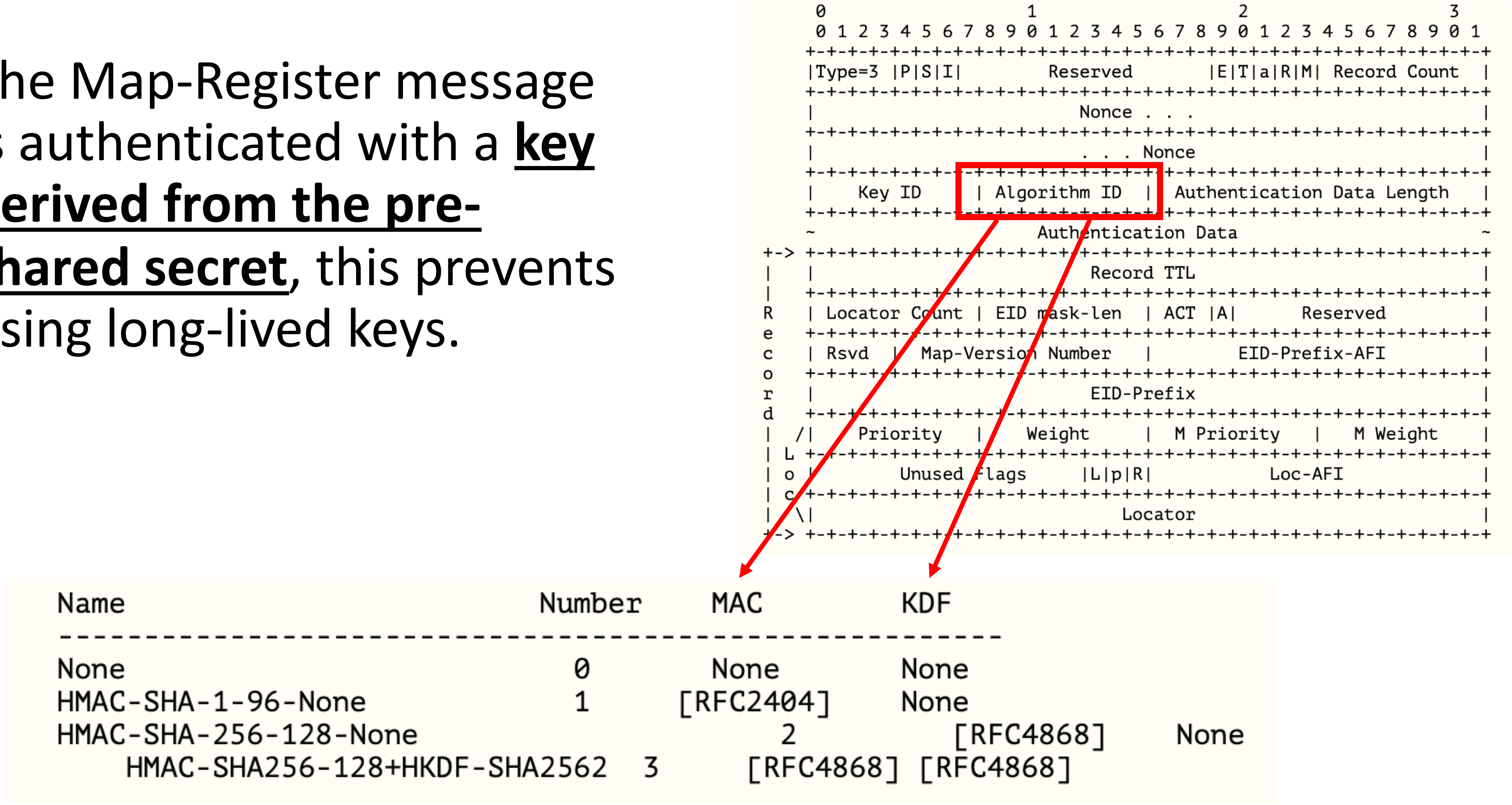
- Posted draft-ietf-lisp-rfc6830bis-27 (June 2019)
- Posted draft-ietf-lisp-rfc6833bis-25 (June 2019)
- **Outline of the changes:**
  1. **Security**
  2. **Rate-Limiting, Loss Detection and Retransmission**
  3. **MTU**
  4. **Other**
  - **Many minor editorial/clarification (not discussed in this presentation)**

Security (6830bis)

- Gleaning, Map-Versioning, LSB and Echo-Nonce **SHOULD NOT be used over the public Internet** and SHOULD only be used in trusted and closed environments. LSB SHOULD be coupled with Map-Versioning.

Security (6833bis)

- The Map-Register message is authenticated with a **key derived from the pre-shared secret**, this prevents using long-lived keys.



```
        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
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |Type=3 |P|S|I|          Reserved         |E|T|a|R|M| Record Count  |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                         Nonce . . .                           |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                         . . . Nonce                           |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |     Key ID    |  Algorithm ID |  Authentication Data Length   |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       ~                     Authentication Data                       ~
   +-> +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |   |                          Record TTL                           |
   |   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   R   | Locator Count | EID mask-len  | ACT |A|       Reserved        |
   e   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   c   | Rsvd  |  Map-Version Number   |       EID-Prefix-AFI          |
   o   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   r   |                          EID-Prefix                           |
   d   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  /|    Priority   |    Weight     |  M Priority   |   M Weight    |
   | L +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | o |        Unused Flags     |L|p|R|           Loc-AFI             |
   | c +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  \|                             Locator                           |
   +-> +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Name	Number	MAC	KDF
None	0	None	None
HMAC-SHA-1-96-None	1	[RFC2404]	None
HMAC-SHA-256-128-None	2	[RFC4868]	None
HMAC-SHA256-128+HKDF-SHA2562	3	[RFC4868]	[RFC4868]

Security (6833bis)

Algorithm used to derive the pre-shared key

1. The KDF algorithm is identified by the field ‘Algorithm ID’
2. The MAC algorithm is identified by the field 'Algorithm ID’
3. The pre-shared secret used to derive the per-message key is represented by PSK[Key ID]
4. The derived per-message key is computed as: per-msg-key=KDF(nonce+s+PSK[Key ID]). 's' is a string equal to "Map-Register Authentication".
5. The MAC output is computed using the MAC algorithm and the per-msg-key over the entire Map-Register

Security (6833bis)

- In Map-Register the nonce is used to prevent anti-replay attacks. The nonce is incremented each successful Map-Register and **indexed by <xTR-ID, key>**
- Specified that they key used to authenticate Map-Register messages is unique per ETR.
- Rewritten Security Considerations according to the changes.

Security (6833bis)

- Following the guidelines of RFC8085 we define these rate-limiters:
  - **Map-Requests MUST be rate-limited to 1 per second per EID-prefix**. After 10 retransmits without receiving the corresponding Map-Reply must wait 30 seconds.
  - **Map-Reply** MUST be rate-limited, it is RECOMMENDED that a Map-Reply **for the same destination RLOC** be sent no more than **one packets per 3 seconds.**
  - [This also applies to the SMR sender and responder]
  - After sending **a Map-Register**, if a Map-Notify is not received after 1 second the transmitter MUST re-transmit the original Map-Register with an **exponential backoff, the maximum backoff is 1 minute.**

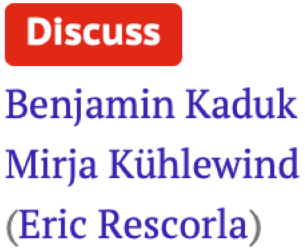
MTU (6830bis)

- Following the guidelines of RFC8085:
  - LISP is expected to be deployed by cooperating entities communicating over underlays. Deployers are expected to set the MTU according to the specific deployment
  - For deployments not aware of the underlay restrictions on path MTU, the message size **MUST be limited to 576 bytes for IPv4** or **1280 bytes for IPv6** as outlined in RFC8085.

Other (6830bis and 6833bis)

- Instance-ID is defined as a 24-bit field in the data-plane.
- Clarified that the nonce (in Map-Request/Map-Reply) is used only to identify the corresponding Map-Request.
- Clarified that 'Explicit Congestion Notification' (ECN) field is processed as specified in [RFC6040].
- Clarified that while the mapping is being retrieved, an ITR/PITR can either drop or buffer the packet, no recommendation provided. This is up to the deployer.

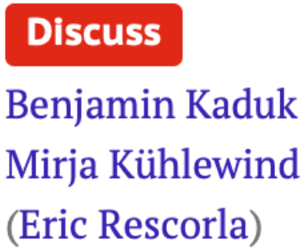
Current IESG Evaluation Record



Discuss

Benjamin Kaduk
Mirja Kühlewind
(Eric Rescorla)

draft-ietf-lisp-rfc6830bis-27



Discuss

Benjamin Kaduk
Mirja Kühlewind
(Eric Rescorla)

draft-ietf-lisp-rfc6833bis-25