

# **draft-ietf-lisp-sec-02 (changes since -00)**

Fabio Maino, Vina Ermagan, Albert Cabellos, Damien Saucez, Olivier Bonaventure

Presenter: Fabio Maino

IETF 83, Paris – March 2012

## Section 5.3 – S-bit in Map-Register

- Used by ETR to indicate LISP-SEC capability to Map-Server

### 5.3. Map-Register LISP-SEC Extentions

The second bit after the Type field in a Map-Register message is allocated as the S bit. The S bit indicates to the Map-Server that the registering ETR is LISP-SEC enabled. An ETR that supports LISP-SEC MUST set the S bit in its Map-Register messages.

# Section 7.1 – HMAC-SHA-1 Length

- aligned with draft-lisp-22 and draft-lisp-ms-16

## 7.1. HMAC functions

The following HMAC ID values are defined by this memo for use as Requested HMAC ID, EID HMAC ID, and PKT HMAC ID in the LISP-SEC Authentication Data:

Name	Number	Defined In
NONE	0	
<del>AUTH-HMAC-SHA-1-160</del>		
AUTH-HMAC-SHA-1-96	1	[RFC2104]
AUTH-HMAC-SHA-256-128	2	[RFC4634]

values 2-65535 are reserved to IANA.

### HMAC Functions

~~AUTH-HMAC-SHA-1-160~~

AUTH-HMAC-SHA-1-96 MUST be supported, AUTH-HMAC-SHA-256-128 should be supported.