LISP Digital Signatures

draft-farinacci-lisp-ecdsa-auth-02

IETF LISP WG Montreal
July 2018

Dino Farinacci & Erik Nordmark

Document Status

Initial
Jul 2017

Update
Oct 2017

Latest
Apr 2018

Plan -03
Summer 2018

Brief Overview

- Authenticate & authorize xTRs using the mapping system
- How to sign Map-Registers
- How to sign Map-Requests
- How to store public-keys in mapping system
- Introduces of Crypto-EIDs
- Introduces of Signature-EIDs

Benefits

- Strong Elliptic Curve Cryptography using DSA
- Can verify and invalidate a single xTR
- Can use the signature-EID for registering any EID type
- Can use public-key for encrypting results sent back to xTR
- Provides identity privacy - multiple key-pairs can be used

Diff -00 to -01

B.1. Changes to draft-farinacci-lisp-ecdsa-auth-01.txt

- Draft posted October 2017.
- Make it more clear what values and format the EID hash is run over.
- Update references to newer RFCs and Internet Drafts.

Diff -01 to -02

B.1. Changes to draft-farinacci-lisp-ecdsa-auth-02.txt

- Draft posted April 2018.
- Generalize text to allow Map-Reqeusting and Map-Registering for any EID type with a proper signature-EID and signature encoded together.

Contents of -03

- Spec how RLOC-probe Map-Requests signatures can be verified by decapsulating xTRs
- Spec how RLOC-probe Map-Replies signatures can be verified by encapsulating xTRs
- Consider Map-Notify signatures so Map-Servers can be authenticated (import for pubsub)
- Consider Multi-Sig

WG Request

- Make -03 WG *draft-ietf-lisp-ecdsa-auth-00*
- Request will be made end of summer

Questions?