LISP Digital Signatures

IETF LISP WG Singapore
November 2017

Dino Farinacci & Erik Nordmark

draft-farinacci-lisp-ecdsa-auth-01

- Draft covers:
  - Authentication and authorization of xTRs using the mapping system
  - How to sign Map-Registers
  - How to sign Map-Requests
  - How to store public-keys in mapping system

How it Works

- xTRs are assigned private/public key-pair(s)
- Introduce Crypto-EIDs
  - IPv6 EID divided in two parts, prefix and hash
  - Hash is a crypto hash of the public-key
  - Can be used as a source EID or a signature EID

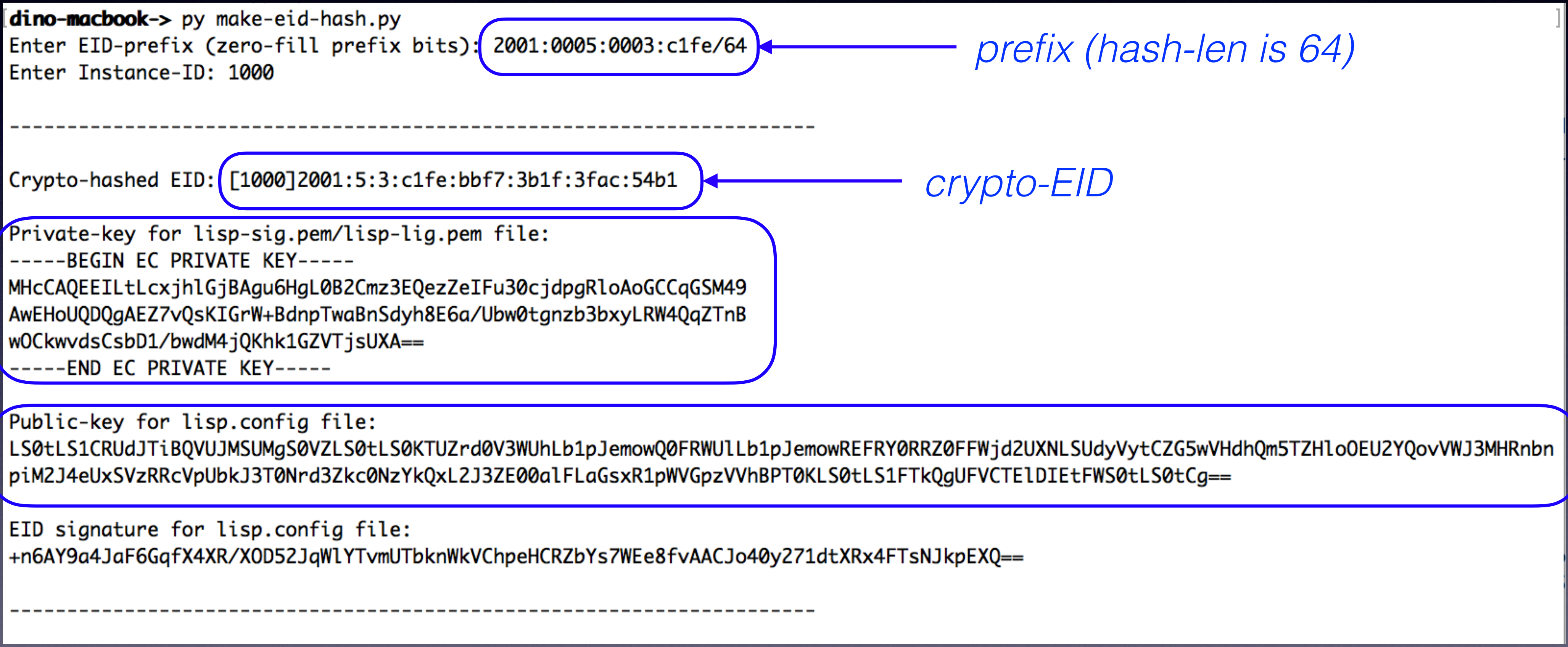
How it Works

- Hash to public-key mappings
  - Go into the mapping system
  - Registered by 3rd-party in same or different Instance-ID
- xTRs sign Map-Register messages with private-key
- Map-Server looks up hash and verifies signature with public-key
  - Registration shared-key still used
  - Both shared-key and signature verification required to accept Map-Register
- xTRs sign Map-Requests with nonce and <iid><eid>
  - Return mapping if signature verification passes
  - Return action="auth-failure" if signature verification fails

Benefits

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

Provisioning Example

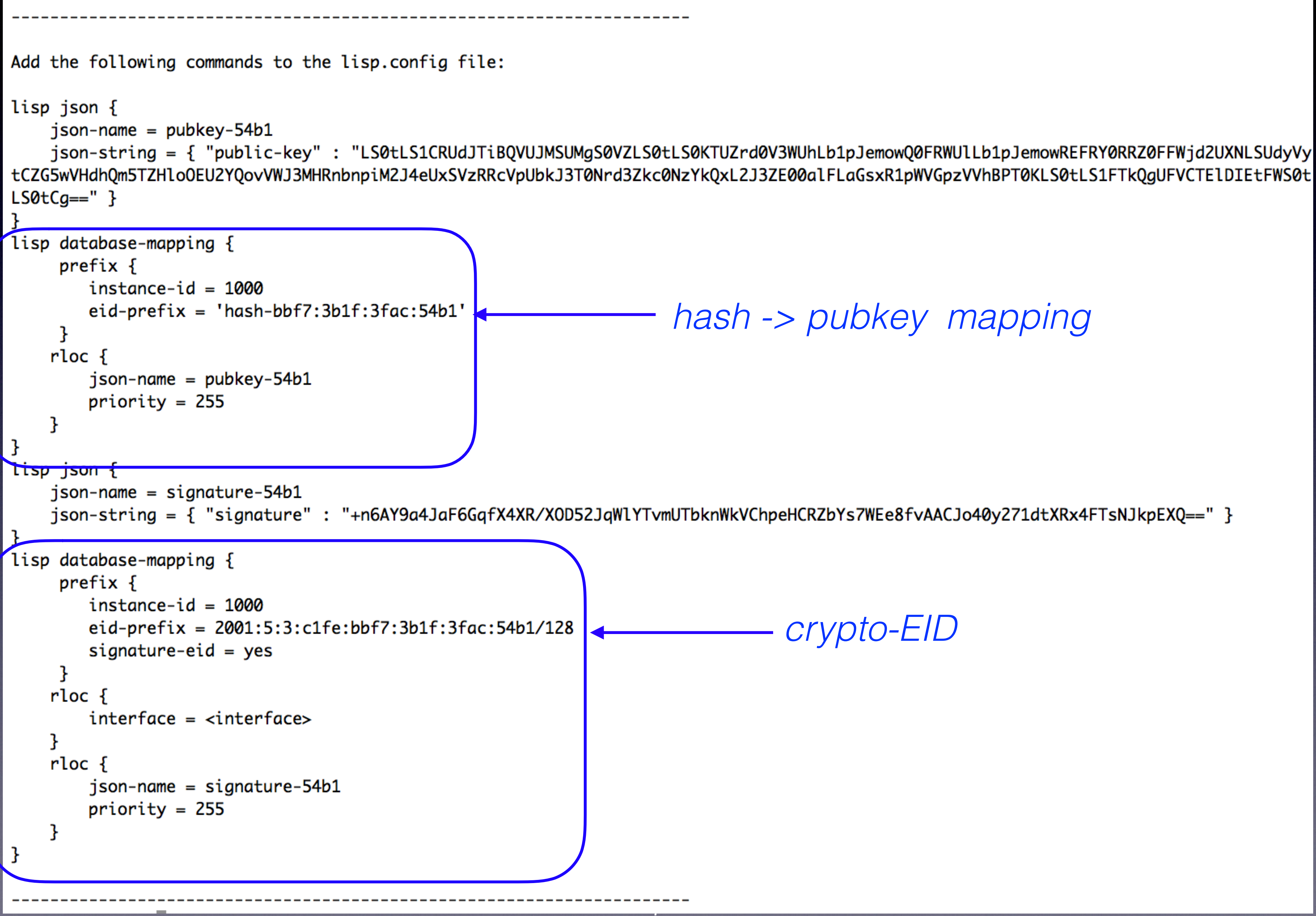


```
dino-macbook-> py make-eid-hash.py
Enter EID-prefix (zero-fill prefix bits): 2001:0005:0003:c1fe/64
Enter Instance-ID: 1000

----------------------------------------------------------------------

Crypto-hashed EID: [1000]2001:5:3:c1fe:bbf7:3b1f:3fac:54b1

Private-key for lisp-sig.pem/lisp-lig.pem file:
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEILtLcxjhlGjBAgu6HgL0B2Cmz3EQezZeIFu30cjdpgRloAoGCCqGSM49
AwEHoUQDQgAEZ7vQsKIGrW+BdnpTwaBnSdyh8E6a/Ubw0tgnzb3bxyLRW4QqZTnB
wOCkwvdsCsbD1/bwdM4jQKhk1GZVTjsUXA==
-----END EC PRIVATE KEY-----

Public-key for lisp.config file:
LS0tLS1CRUdJTiBQVUJMSUMgS0VZLS0tLS0KTUZrd0V3WUhLb1pJemowQ0FRWUlLb1pJemowREFRY0RRZ0FFWjd2UXNLSUdyVytCZG5wVHdhQm5TZHloOEU2YQovVWJ3MHRnbn
piM2J4eUxSVzRRcVpUbkJ3T0Nrd3Zkc0NzYkQxL2J3ZE00alFLaGsxR1pWVGpzVVhBPT0KLS0tLS1FTkQgUFVCTElDIEtFWS0tLS0tCg==

EID signature for lisp.config file:
+n6AY9a4JaF6GqfX4XR/XOD52JqWlYTvmUTbknWkVChpeHCRZbYs7WEe8fvAACJo40y271dtXRx4FTsNJkpEXQ==

----------------------------------------------------------------------
```

prefix (hash-len is 64)

crypto-EID

Provisioning Example

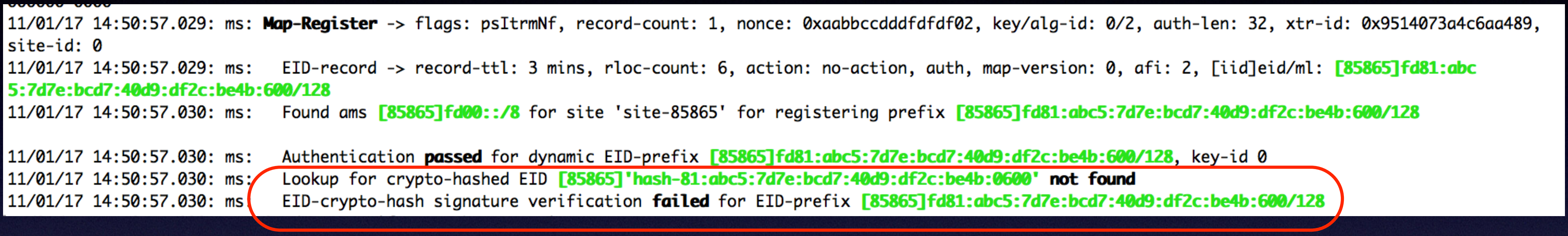


```
---------------------------------------------------------------------

Add the following commands to the lisp.config file:

lisp json {
    json-name = pubkey-54b1
    json-string = { "public-key" : "LS0tLS1CRUdJTiBQVUJMSUMgS0VZLS0tLS0KTUZrd0V3WUhLb1pJemowQ0FRWUlLb1pJemowREFRY0RRZ0FFWjd2UXNLSUdyVy
tCZG5wVHdhQm5TZHloOEU2YQovVWJ3MHRnbnpiM2J4eUxSVzRRcVpUbkJ3T0Nrd3Zkc0NzYkQxL2J3ZE00alFLaGsxR1pWVGpzVVhBPT0KLS0tLS1FTkQgUFVCTElDIEtFWS0t
LS0tCg==" }
}
lisp database-mapping {
     prefix {
        instance-id = 1000
        eid-prefix = 'hash-bbf7:3b1f:3fac:54b1'
     }
    rloc {
        json-name = pubkey-54b1
        priority = 255
    }
}
lisp json {
    json-name = signature-54b1
    json-string = { "signature" : "+n6AY9a4JaF6GqfX4XR/XOD52JqWlYTvmUTbknWkVChpeHCRZbYs7WEe8fvAACJo40y271dtXRx4FTsNJkpEXQ==" }
}
lisp database-mapping {
     prefix {
        instance-id = 1000
        eid-prefix = 2001:5:3:c1fe:bbf7:3b1f:3fac:54b1/128
        signature-eid = yes
     }
    rloc {
        interface = <interface>
    }
    rloc {
        json-name = signature-54b1
        priority = 255
    }
}
---------------------------------------------------------------------
```

hash -> pubkey mapping

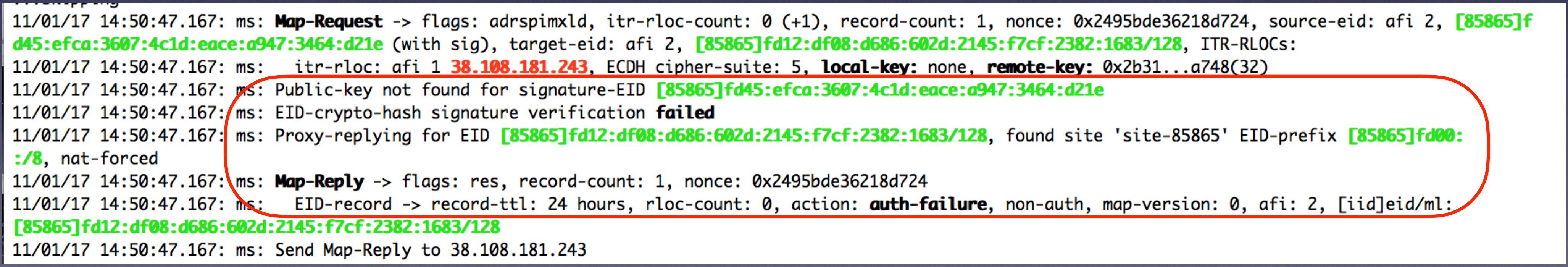
crypto-EID

Map-Register - no public key



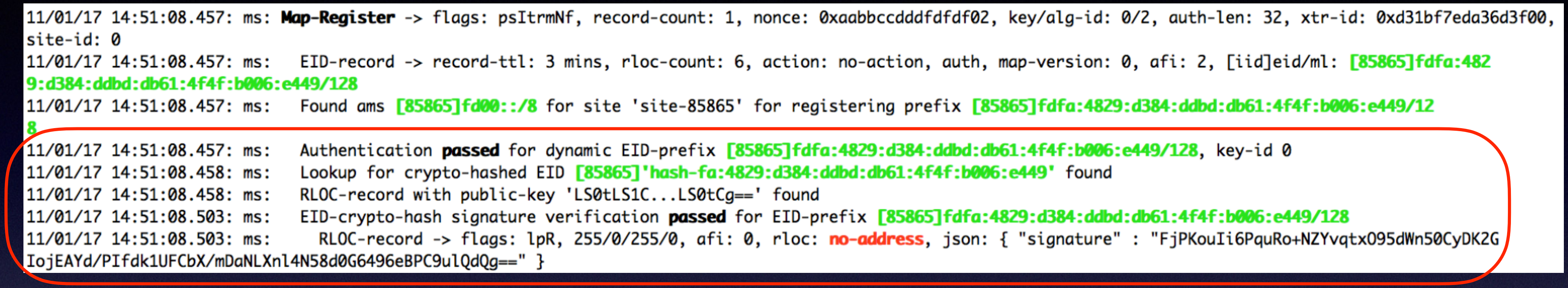
```
11/01/17 14:50:57.029: ms: Map-Register -> flags: psItrmNf, record-count: 1, nonce: 0xaabbccdddfdfdf02, key/alg-id: 0/2, auth-len: 32, xtr-id: 0x9514073a4c6aa489,
site-id: 0
11/01/17 14:50:57.029: ms:   EID-record -> record-ttl: 3 mins, rloc-count: 6, action: no-action, auth, map-version: 0, afi: 2, [iid]eid/ml: [85865]fd81:abc
5:7d7e:bcd7:40d9:df2c:be4b:600/128
11/01/17 14:50:57.030: ms:   Found ams [85865]fd00::/8 for site 'site-85865' for registering prefix [85865]fd81:abc5:7d7e:bcd7:40d9:df2c:be4b:600/128

11/01/17 14:50:57.030: ms:   Authentication passed for dynamic EID-prefix [85865]fd81:abc5:7d7e:bcd7:40d9:df2c:be4b:600/128, key-id 0
11/01/17 14:50:57.030: ms:   Lookup for crypto-hashed EID [85865]'hash-81:abc5:7d7e:bcd7:40d9:df2c:be4b:0600' not found
11/01/17 14:50:57.030: ms:   EID-crypto-hash signature verification failed for EID-prefix [85865]fd81:abc5:7d7e:bcd7:40d9:df2c:be4b:600/128
```

Map-Request - no public key



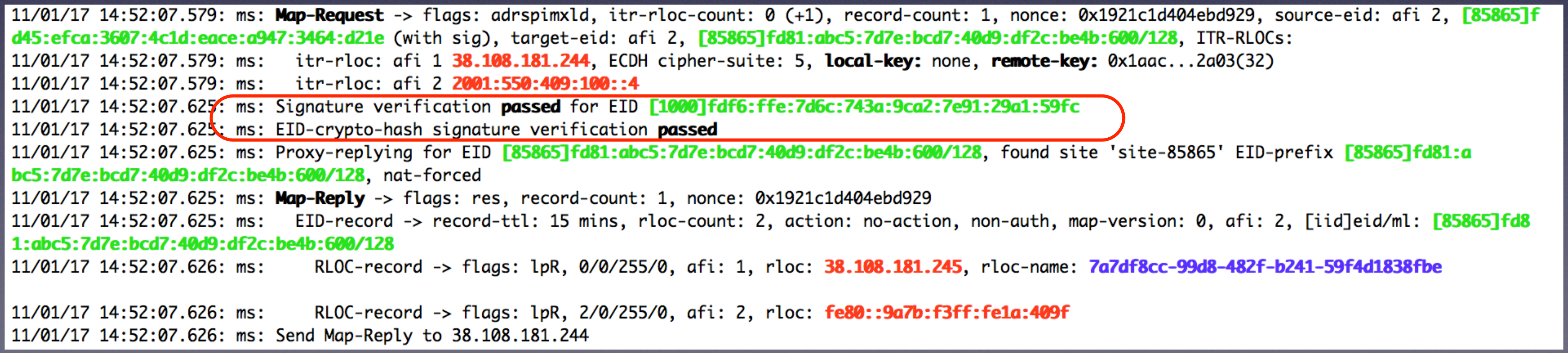
```
11/01/17 14:50:47.167: ms: Map-Request -> flags: adrspimxld, itr-rloc-count: 0 (+1), record-count: 1, nonce: 0x2495bde36218d724, source-eid: afi 2, [85865]f
d45:efca:3607:4c1d:eace:a947:3464:d21e (with sig), target-eid: afi 2, [85865]fd12:df08:d686:602d:2145:f7cf:2382:1683/128, ITR-RLOCs:
11/01/17 14:50:47.167: ms:   itr-rloc: afi 1 38.108.181.243, ECDH cipher-suite: 5, local-key: none, remote-key: 0x2b31...a748(32)
11/01/17 14:50:47.167: ms: Public-key not found for signature-EID [85865]fd45:efca:3607:4c1d:eace:a947:3464:d21e
11/01/17 14:50:47.167: ms: EID-crypto-hash signature verification failed
11/01/17 14:50:47.167: ms: Proxy-replying for EID [85865]fd12:df08:d686:602d:2145:f7cf:2382:1683/128, found site 'site-85865' EID-prefix [85865]fd00:
:/8, nat-forced
11/01/17 14:50:47.167: ms: Map-Reply -> flags: res, record-count: 1, nonce: 0x2495bde36218d724
11/01/17 14:50:47.167: ms:   EID-record -> record-ttl: 24 hours, rloc-count: 0, action: auth-failure, non-auth, map-version: 0, afi: 2, [iid]eid/ml:
[85865]fd12:df08:d686:602d:2145:f7cf:2382:1683/128
11/01/17 14:50:47.167: ms: Send Map-Reply to 38.108.181.243
```

Map-Register - signature good



```
11/01/17 14:51:08.457: ms: Map-Register -> flags: psItrmNf, record-count: 1, nonce: 0xaabbccdddfdfdf02, key/alg-id: 0/2, auth-len: 32, xtr-id: 0xd31bf7eda36d3f00,
site-id: 0
11/01/17 14:51:08.457: ms:   EID-record -> record-ttl: 3 mins, rloc-count: 6, action: no-action, auth, map-version: 0, afi: 2, [iid]eid/ml: [85865]fdfa:482
9:d384:ddbd:db61:4f4f:b006:e449/128
11/01/17 14:51:08.457: ms:   Found ams [85865]fd00::/8 for site 'site-85865' for registering prefix [85865]fdfa:4829:d384:ddbd:db61:4f4f:b006:e449/12
8
11/01/17 14:51:08.457: ms:   Authentication passed for dynamic EID-prefix [85865]fdfa:4829:d384:ddbd:db61:4f4f:b006:e449/128, key-id 0
11/01/17 14:51:08.458: ms:   Lookup for crypto-hashed EID [85865]'hash-fa:4829:d384:ddbd:db61:4f4f:b006:e449' found
11/01/17 14:51:08.458: ms:   RLOC-record with public-key 'LS0tLS1C...LS0tCg==' found
11/01/17 14:51:08.503: ms:   EID-crypto-hash signature verification passed for EID-prefix [85865]fdfa:4829:d384:ddbd:db61:4f4f:b006:e449/128
11/01/17 14:51:08.503: ms:     RLOC-record -> flags: lpR, 255/0/255/0, afi: 0, rloc: no-address, json: { "signature" : "FjPKouIi6PquRo+NZYvqtxO95dWn50CyDK2G
IojEAYd/PIfdk1UFCbX/mDaNLXnl4N58d0G6496eBPC9ulQdQg==" }
```

Map-Request - signature good



```
11/01/17 14:52:07.579: ms: Map-Request -> flags: adrspimxld, itr-rloc-count: 0 (+1), record-count: 1, nonce: 0x1921c1d404ebd929, source-eid: afi 2, [85865]f
d45:efca:3607:4c1d:eace:a947:3464:d21e (with sig), target-eid: afi 2, [85865]fd81:abc5:7d7e:bcd7:40d9:df2c:be4b:600/128, ITR-RLOCs:
11/01/17 14:52:07.579: ms:   itr-rloc: afi 1 38.108.181.244, ECDH cipher-suite: 5, local-key: none, remote-key: 0x1aac...2a03(32)
11/01/17 14:52:07.579: ms:   itr-rloc: afi 2 2001:550:409:100::4
11/01/17 14:52:07.625: ms: Signature verification passed for EID [1000]fdf6:ffe:7d6c:743a:9ca2:7e91:29a1:59fc
11/01/17 14:52:07.625: ms: EID-crypto-hash signature verification passed
11/01/17 14:52:07.625: ms: Proxy-replying for EID [85865]fd81:abc5:7d7e:bcd7:40d9:df2c:be4b:600/128, found site 'site-85865' EID-prefix [85865]fd81:a
bc5:7d7e:bcd7:40d9:df2c:be4b:600/128, nat-forced
11/01/17 14:52:07.625: ms: Map-Reply -> flags: res, record-count: 1, nonce: 0x1921c1d404ebd929
11/01/17 14:52:07.625: ms:   EID-record -> record-ttl: 15 mins, rloc-count: 2, action: no-action, non-auth, map-version: 0, afi: 2, [iid]eid/ml: [85865]fd8
1:abc5:7d7e:bcd7:40d9:df2c:be4b:600/128
11/01/17 14:52:07.626: ms:     RLOC-record -> flags: lpR, 0/0/255/0, afi: 1, rloc: 38.108.181.245, rloc-name: 7a7df8cc-99d8-482f-b241-59f4d1838fbe

11/01/17 14:52:07.626: ms:     RLOC-record -> flags: lpR, 2/0/255/0, afi: 2, rloc: fe80::9a7b:f3ff:fe1a:409f
11/01/17 14:52:07.626: ms: Send Map-Reply to 38.108.181.244
```

Draft Status

- Want to get more implementation experience before requesting WG document
- Request will probably be made next year