LISP Digital Signatures

IETF LISP WG Singapore
November 2017

Dino Farinacci & Erik Nordmark
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

Prefix (hash-len is 64):

```
[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-----
MHcCAQEELtLcxh1GjBAgu6HgL0B2Cmz3EQezZeIFu30cjdpqRloAoGCCqGSM49
AwEHoUQOgAEZ7VqsKlGrW+DnpTwaBnSyh8E6a/UbwOtgnzb3bxyLRw4QqZtnb
wOCkwvdsCsbDi/bwdMmjQKkh1gZVTjsUXA==
-----END EC PRIVATE KEY-----
```

Public key for lisp.config file:
```
LS0tLS1CIRUdJTiBQVUJMSUMgS0VZLS0tLS0tKUZrd0V3WUhlb1pJemowQ0FRWUllb1pJemowREFRy0RRZ0FFWjd2UXNLSUdyVytCZG5wVHdhQm5TZHloOEU2YQovVWJ3MHZnbn
piM2J4eUXsvRRCVpUbJK3t0Nr3ZxcD0NzYqXq2J3ze00a1FLaGszR1pWVPzVvH8BT0KLS0tLS1FTkQyUFVCET1DEtFWS0tLS0tCg==
```

EID signature for lisp.config file:
```
+66AYq4Jaf6GgfX4X/R/XOD52JqWlYTvmmUTbknWkVChpeHCRZbYs7We8fVAACJo40y271dtXR4FTsNJkpEXQ==
```
Provisioning Example

Add the following commands to the lisp.config file:

```lisp
lisp json {
    json-name = 'pubkey-54b1'
    json-string = """public-key" : "LS0tLS1CRUdJTiBQVUJMSUMgS0VZLS0tLS0KLURd0V3WUhLb1pJemowQ0FRUJlLb1pJemowREFRY0RRZ0FFWjd2UXNLdSjcyVytcZGswdHdhOmSTZHzl0OEU2YQovVWJ3MHl6bnpiM0Z4eUXzZvRccVmpUbkJ3T0Nrd3ZKc0NzYQxL2J3ZE00a1FLaGsxR1pMVYgpbzVvbBPT0KL50tLS1FTkQ0UFVCTE1DIEtFWS0tLS0tCg=="
}
}
```

```lisp
lisp database-mapping {
    prefix {
        instance-id = 1000
        eid-prefix = 'hash-bbf7:3b1f:3fac:54b1'
    }
    rloc {
        json-name = 'pubkey-54b1'
        priority = 255
    }
}
```

```lisp
lisp json {
    json-name = 'signature-54b1'
    json-string = """signature" : "+nGAY9a4JaF6GqfX4XR/X0DS2JqWYTVmUThkVhpeHCRZbYS7WEe8fVvAACJo40y271dtXRx4FTsNJkpEX=="
}
```

```lisp
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: psItmMf, record-count: 1, nonce: 0xaabbccdddfdf02, key/alg-id: 0/2, auth-len: 32, xtr-id: 0x9514073a4c6aa489, site-id: 0
11/01/17 14:50:57.030: ms: Authentication passed for dynamic EID-prefix [85865]f8d1:abc5:7d7e:bc7d: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:bc7d:40d9:df2c:be4b:600' not found

Map-Request - no public key

11/01/17 14:50:47.167: ms: itr-rloc: afe 2 38.108.181.203, ECDH cipher-suite: 5, local-key: none, remote-key: 0x2b31...d748(32)
11/01/17 14:50:47.167: ms: EID-crypto-hash signature verification failed
11/01/17 14:50:47.167: ms: Map-Reply -> flags: res, record-count: 1, nonce: 0x2495be36218d724
11/01/17 14:50:47.167: ms: Send Map-Reply to 38.108.181.203
Map-Register - signature good

11/01/17 14:51:08.457: ms: Map-Register -> flags: psItrmNf, record-count: 1, nonce: 0xaabbccddf1df02, key/alg-id: 0/2, auth-len: 32, xtr-id: 0xd31b7eda363d3f00, site-id: 0
8
11/01/17 14:51:08.457: ms: RLOC-record with public-key 'LS0tLS1C...LS0tCg==' found
11/01/17 14:51:08.503: ms: RLOC-record -> flags: lpR, 255/0/255/0, afi: 0, rloc: no-address, json: {"signature":"FjPKouIi6PquRo+NZyVqt0x95dWn50CyDK2GToJEAYd/P1fdk1UCbX/mDaNLXnl4N58d0G6496eBPC9ulQdQ=="}

Map-Request - signature good

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 14:52:07.625: ms: EID-crypto-hash signature verification passed
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: 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 14:52:07.625: ms: RLOC-record -> flags: lpR, 2/0/255/0, afi: 2, rloc: fe80::9a7bf3ff:fe1a:409f
11/01/17 14:52:07.625: 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