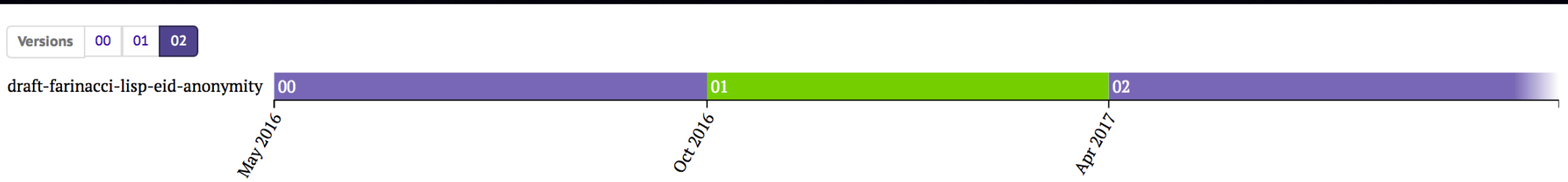
LISP EID Anonymity

draft-farinacci-lisp-eid-anonymity-02

LISP Working Group - Prague IETF
July 2017

Dino Farinacci and Padma Pillay-Esnault

Document Status




```
Appendix B.  Document Change Log

   [RFC Editor: Please delete this section on publication as RFC.]

B.1.  Changes to draft-farinacci-lisp-eid-anonymity-02

   o  Posted April 2017.

   o  Added section describing how ephemeral-EIDs can use a public key
      hash as an alternative to a random number.

   o  Indciate when an EID/RLOC co-located, that the xTR can register
      the EID when it is configured or changed versus waiting for a
      packet to be sent as in the EID/RLOC separated case.

B.2.  Changes to draft-farinacci-lisp-eid-anonymity-01

   o  Posted October 2016.

   o  Update document timer.

B.3.  Changes to draft-farinacci-lisp-eid-anonymity-00

   o  Posted April 2016.

   o  Initial posting.
```

Problem Statement

- How can we make EIDs private?
- Without enforcing payload encryption
- How can we make EIDs untraceable?
- How can we authenticate EIDs?

Solution

- Source creates ephemeral EIDs and starts sending packets from them
- Ephemeral EIDs are IPv6 addresses:
  - Random Number
  - Crypto Hash
- Source is free to create as many as it wants
- Source is free to use them as long as it wants
- Source can stop using them and they are automatically deregistered from mapping system
- Destination doesn't do anything special
- Ephemeral EIDs are typically used on client hosts and not bounded to DNS names

LISP Protocol Changes

- None
- xTRs use mechanisms from `draft-ietf-lisp-eid-mobility-02` to discover and register EIDs
- When source stops sourcing from ephemeral EID, xTRs process event as a move-away event (and deregister)
- All traces of EID are removed from mapping system
- Map-caches in remote ITRs are invalidated

Quick Demo

Ping destination EID **dfdf:4::4**

lispers.net

Scalable Open Overlay Networking

Enter EID for Site-Cache lookup: Submit

LISP-MS Site Information:

Site Name	EID-Prefix or (S,G)	Registered	Last Registerer	Last Registered	First Registered
any	[0]	no (ams)	--	never	never
	[0]4.4.4.4/32	yes (dynamic)	[0]172.17.0.4	0:00:14	1:29:57
	[0]dfdf:4::/32	yes (dynamic)	[0]172.17.0.4	0:00:14	1:29:57
	[0]'d-xtr4'	yes (dynamic)	[0]172.17.0.4	0:00:14	1:29:57
	[0]3.3.3.3/32	yes (dynamic)	[0]172.17.0.3	0:00:14	0:10:14
	[0]dfdf:3::/32	yes (dynamic)	[0]172.17.0.3	0:00:14	0:10:14
	[0]'d-xtr3'	yes (dynamic)	[0]172.17.0.3	0:00:14	0:10:14
	[0]2001:5:ffff::fa4b:8633/128	no (dynamic)	[0]172.17.0.3	0:07:35	0:08:05
	[0]2001:5:ffff::82c8:d66d/128	no (dynamic)	[0]172.17.0.3	0:07:35	0:08:01
	[0]2001:5:ffff::6b78:9b75/128	no (dynamic)	[0]172.17.0.3	0:07:20	0:07:48
	[0]2001:5:ffff::eb93:696d/128	no (dynamic)	[0]172.17.0.3	0:07:05	0:07:33
	[0]2001:5:ffff::7ff0:b852/128	no (dynamic)	[0]172.17.0.3	0:07:05	0:07:29
	[0]2001:5:ffff::67dc:b84a/128	no (dynamic)	[0]172.17.0.3	0:06:50	0:07:16

```
root@xtr3:/dino/code/apps# py ping-from-eeid.py dfdf:4::4 loop 100
Configure 2001:5:ffff::ae7a:5c65 on interface lo ... succeeded
Start ping6 from 2001:5:ffff::ae7a:5c65 to dfdf:4::4 ...
PING dfdf:4::4(dfdf:4::4) from 2001:5:ffff::ae7a:5c65 : 56 data bytes
64 bytes from dfdf:4::4: icmp_seq=2 ttl=62 time=220 ms
64 bytes from dfdf:4::4: icmp_seq=3 ttl=62 time=218 ms
64 bytes from dfdf:4::4: icmp_seq=4 ttl=62 time=217 ms
64 bytes from dfdf:4::4: icmp_seq=5 ttl=62 time=216 ms
64 bytes from dfdf:4::4: icmp_seq=6 ttl=62 time=214 ms
64 bytes from dfdf:4::4: icmp_seq=7 ttl=62 time=212 ms
64 bytes from dfdf:4::4: icmp_seq=8 ttl=62 time=212 ms
64 bytes from dfdf:4::4: icmp_seq=9 ttl=62 time=210 ms
64 bytes from dfdf:4::4: icmp_seq=10 ttl=62 time=209 ms

--- dfdf:4::4 ping statistics ---
10 packets transmitted, 9 received, 10% packet loss, time 9019ms
rtt min/avg/max/mdev = 209.816/214.829/220.720/3.608 ms
Deconfigure 2001:5:ffff::ae7a:5c65 on interface lo ... succeeded
------------------------------------------------------------
Configure 2001:5:ffff::ee0e:1362 on interface lo ... succeeded
Start ping6 from 2001:5:ffff::ee0e:1362 to dfdf:4::4 ...
PING dfdf:4::4(dfdf:4::4) from 2001:5:ffff::ee0e:1362 : 56 data bytes
64 bytes from dfdf:4::4: icmp_seq=2 ttl=62 time=179 ms
64 bytes from dfdf:4::4: icmp_seq=3 ttl=62 time=177 ms
64 bytes from dfdf:4::4: icmp_seq=4 ttl=62 time=177 ms
64 bytes from dfdf:4::4: icmp_seq=5 ttl=62 time=175 ms
64 bytes from dfdf:4::4: icmp_seq=6 ttl=62 time=174 ms
64 bytes from dfdf:4::4: icmp_seq=7 ttl=62 time=174 ms
64 bytes from dfdf:4::4: icmp_seq=8 ttl=62 time=171 ms
64 bytes from dfdf:4::4: icmp_seq=9 ttl=62 time=170 ms
64 bytes from dfdf:4::4: icmp_seq=10 ttl=62 time=168 ms

--- dfdf:4::4 ping statistics ---
10 packets transmitted, 9 received, 10% packet loss, time 9018ms
rtt min/avg/max/mdev = 168.899/174.517/179.824/3.420 ms
Deconfigure 2001:5:ffff::ee0e:1362 on interface lo ... succeeded
------------------------------------------------------------
Configure 2001:5:ffff::18b4:c065 on interface lo ... succeeded
Start ping6 from 2001:5:ffff::18b4:c065 to dfdf:4::4 ...
PING dfdf:4::4(dfdf:4::4) from 2001:5:ffff::18b4:c065 : 56 data bytes
64 bytes from dfdf:4::4: icmp_seq=2 ttl=62 time=239 ms
64 bytes from dfdf:4::4: icmp_seq=3 ttl=62 time=238 ms
64 bytes from dfdf:4::4: icmp_seq=4 ttl=62 time=237 ms
64 bytes from dfdf:4::4: icmp_seq=5 ttl=62 time=236 ms
64 bytes from dfdf:4::4: icmp_seq=6 ttl=62 time=236 ms
64 bytes from dfdf:4::4: icmp_seq=7 ttl=62 time=235 ms
64 bytes from dfdf:4::4: icmp_seq=8 ttl=62 time=234 ms
64 bytes from dfdf:4::4: icmp_seq=9 ttl=62 time=234 ms
64 bytes from dfdf:4::4: icmp_seq=10 ttl=62 time=233 ms

--- dfdf:4::4 ping statistics ---
10 packets transmitted, 9 received, 10% packet loss, time 9013ms
rtt min/avg/max/mdev = 233.697/236.302/239.419/1.830 ms
```

Ephemeral-EIDs timeout
from mapping system when not used

Todo List

- Document ephemeral-EID address collision
  - Tradeoff between address field widths
- Look at Crypto-EIDs in more detail
  - How practical are they as ephemeral-EIDs

Questions/Comments/Tomatoes?