Agenda for IETF 55 - IPSECKEY (BOF)

IPSEC KEYing information resource record BOF

AGENDA:

1. Open meeting and welcome

2. Scribe and blue sheet Olafur Gudmundsson
3. Introduction Michael Richardson
4. Documents
4.1 Why the KEY record was restricted to only DNSSEC keys.
 □Scott Rose
     see draft-ietf-dnsext-restrict-key-for-dnssec-04.txt

4.2 A method for storing IPsec keying material in DNS.
 □draft-richardson-ipsec-rr-00.txt

 □Michael Richardson
5. open mike

6. Next step.   Olafur Gudmundsson

7. Charter discussion Olafur Gudmundsson
8. schedule discussion

Mailing list info

LIST: ipseckey@sandelman.ottawa.on.ca
Archive: http://www.sandelman.ca/lists/html/ipseckey/threads.html

email to: majordomo@sandelman.ottawa.on.ca
body "subscribe ipseckey"

2. Blue Sheet

3. Introduction

What we need for Opportunistic Encryption:

☐ see draft-richardson-ipsec-opportunistic-10.txt

☐ the public key (RSA) of the remote system

☐ the IP address (v4 or v6) of the gateway
  ○ self if in host mode

☐ we need this data indexed by IP address, i.e. we need it in in-addr.arpa.

4.   Documents

- 4.1 Why the KEY record was restricted to only DNSSEC keys.
  - Scott Rose
  - see draft-ietf-dnsext-restrict-key-for-dnssec-04.txt

- 4.2 A method for storing IPsec keying material in DNS.
  - draft-richardson-ipsec-rr-00.txt
  - Michael Richardson

Scott Rose

Why the KEY record was restricted to only DNSSEC keys.

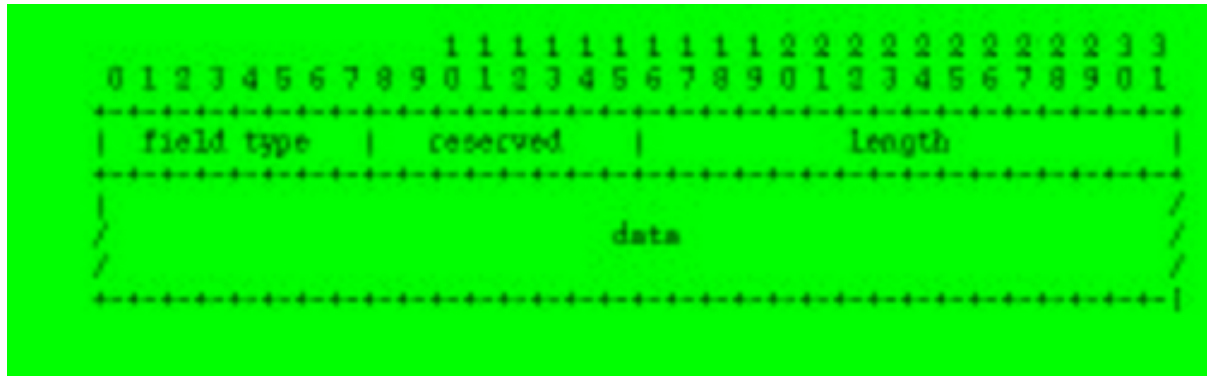draft-ietf-dnsext-restrict-key-for-dnssec-04.txt

initial proposal

- new resource record type
- a series of type-length-value pairs
- currently is extensible (too flexible?)

RR contents

A method for storing IPsec keying material in DNS.

```
                      1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 | field type   |  reserved   |            length               |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                                                               /
 /                          data                                 /
 /                                                               /
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
```

Definitions for field types:

- 0 no more fields
- 1 priority of this entry
- 2 IPv4 address of the gateway for this host
- 3 IPv6 address of the gateway for this host
- 4 FQDN of the gateway for this host
- 5 RSA public key for the gateway

5. open mike

6. Next steps

Olafur Gudmundsson

7. Charter discussion

Olafur Gudmundsson

8. schedule discussion

IPSEC KEYing information resource record

Working group info
ipseckey@sandelman.ottawa.on.ca

email to: majordomo@sandelman.ottawa.on.ca
body "subscribe ipseckey"

Drafts:
- draft-ietf-dnsext-restrict-key-for-dnssec-04.txt
- draft-richardson-ipsec-rr-00.txt