Configuring Cryptographically Generated Addresses (CGA) using DHCPv6

draft-jiang-dhc-cga-config
IETF 79, DHC WG
November 11, 2010

Sheng Jiang (Speaker)
Sam Zhongqi Xia

Requirements & Motivation

- **CGAs may be used in DHCPv6-managed networks**
  - Designed for SeND, also used in Shim6, Mobile IPv6, etc.
- **Network administrators may want to configure parameters used to generate CGAs and manage the use of CGAs**
  - CGAs are normally generated by hosts
  - Network management configures/enforces CGA relevant parameters to hosts
  - DHCPv6 server approves or rejects the usage of CGAs
- **New DHCPv6 options are needed to to fulfill the functions**

CGA Configure Process Using DHCPv6

- **Configuration of the parameters required for the generation of CGA**
  - Parameters may be configured by network management
    - ✓ Prefix   (RA or DHCP prefix assignment)
    - ✓ **Sec value   (new DHCPv6 option in this draft)**
    - ✓ Public Key   (not suitable for network transmission for security reasons)
    - ✓ Extension Fields   (no use yet)
  - Interaction procedure is described in details

CGA Configure Process Using DHCPv6 (2)

- **DHCPv6 server approves or rejects the usage of CGAs**
  - Hosts send Option Request option, which requests Address Grant Option (**new DHCPv6 option, defined in this draft**)
  - CGAs are carried in the IA Address Options
  - Servers reply a Address Grant Option
  - Upon reception of the ack, hosts use approved CGA or generate new one

New DHCPv6 Options

- **DHCPv6 CGA Sec Option is used to carry a Sec value**

```
 0                   1                   2                   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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          OPTION CGA SEC           |         option-len         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    CGA SEC     |
+-+-+-+-+-+-+-+-+-+
```

   - On receiving the CGA Sec Option, the client SHOULD generate a CGA using a Sec value that is not lower than the option indicated; the client MAY choose to generate a CGA using a lower sec value

- **DHCPv6 Address Grant Option to indicate the DHCPv6 client whether the requested address is granted or not**

```
 0                   1                   2                   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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          OPTION ADDR GRANT        |         option-len         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Addr Grant  |
+-+-+-+-+-+-+-+-+-+
```

Change Log

Removed CGA generation delegation

Comments are welcomed!

Should the WG work on this?

Thank You!