# Secure DHCPv6 Using CGA

## draft-ietf-dhc-secure-dhcpv6-06

## IETF 83 DHC WG

March 29, 2011

*Sheng JIANG (Speaker, Huawei)*

*Sean Shen(CNNIC)*

# Update for 05/06 version

- **Receives many comments from saag, the security area, mainly by Stephen Kent**
  - Also comments from Thomas Huth and David Schumacher
- **Reduce the direct quote from CGA and DHCPv6 RFCs**
- **Reorganize the motivation section "Security Overview of DHCPv6"**
  - DHCPv6 server spoof, key management is complex, IPsec is complicated
- **Refine the description of requirement of algorithm agility**
- **Fixed wrong statement for unprotected options leaved behind from early version: all options (including CGA option) are protected except for signature option itself and auth option**

# Update for 05/06 version (2)

- Fixed wrong description regarding to algorithm agility support in the signature option and algorithm-specific examples
- Add Padding for the align of signature option
- Fixed  the bug that the new DUID-SA exceeded 128 bits
- Reorganize processing rules and behaviors in step-by-step manner
- Fixed inconsistencies between different sections of the document
- Fixed several improper references and correspondent texts
- Fixed typo errors in IANA consideration
- Add explanation why randomly generates a CGA Message Type tag value for Secure DHCPv6
- Refine many English

**Comments are welcomed!**

**Ready for WGLC!**

# Thank You!