Secure DHCPv6 with Public Key

Replacement of draft-ietf-dhc-secure-dhcpv6

IETF 87 DHC WG

August 1st, 2013

Sheng JIANG (Speaker)
Sean SHEN

Background

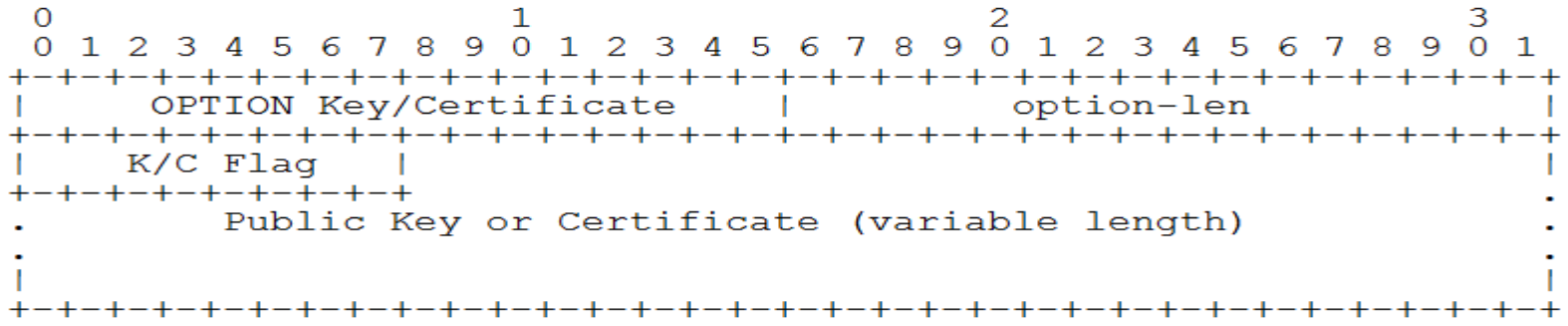
- **It is actually the replacement of draft-ietf-dhc-secure-dhcpv6**
  - draft-ietf-dhc-secure-dhcpv6 “Secure DHCPv6 Using CGA” reached IESG and dead because of consideration regarding to CGA.
  - The use of CGAs in this situation (1) isn't really how they were intended to be used and (2) probably doesn't add any value over a regular public key signature.
- **A suggestion from IESG is to make another public key based security solution, while DHCPv6 needs another security mechanism beyond symmetric key pair**
- **The new draft**
  - dropped CGA relevant mechanism, making it general public key based
  - added PKI as an alternative of pre-config, while keeping "a leap of faith" model possible
  - completed timestamp check mechanism

Secure DHCPv6 Overview

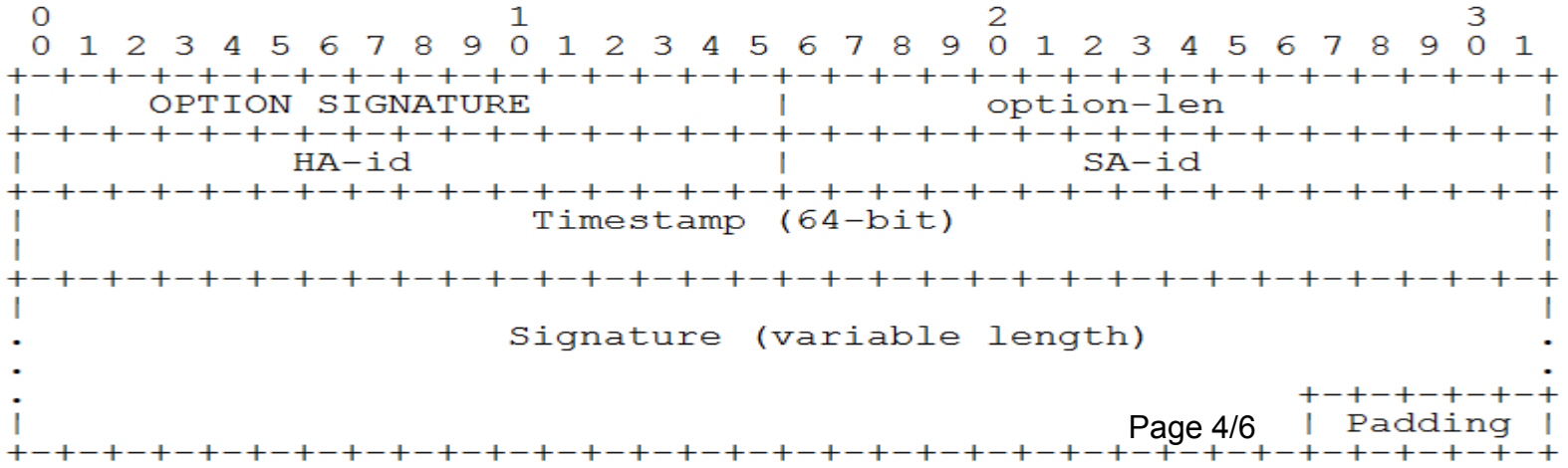
- **The authority of the sender may depend on either pre-configuration mechanism or PKI, or a leap of faith model**
- **By combining with the signatures, sender identity can be verified and messages protected**
- **A Sender MUST have a public/private key pair in order to create Secure DHCPv6 messages**
- **This document introduce a key/certificate option and a signature options with a corresponding verification mechanism**
  - Timestamp is integrated into signature options

New DHCPv6 Options

- **Key/Certificate Option**
  - carries the public key or certificate of the sender



- **Signature Option**
  - Support for algorithm agility
  - Timestamp is integrated into signature options



Process Rules

- **A Secure DHCPv6 message MUST contain both the Key/ Certificate option and the Signature option**
  - except for Relay-forward and Relay-reply Messages
- **Processing Rules of Receiver**
  - SHOULD discard the DHCPv6 message if either the Key/Certificate option or the Signature option is absent
  - SHOULD first check the authority of this sender, by
    - finding a match public key from the local trust public key list, which is pre-configured or recorded from previous communications
    - or validating the sender's certificate following the rules defined in [RFC5280]
    - or the receiver MAY choose to further process the message from an unauthorized sender so that a leap of faith may be built up
  - MUST verify the Signature and check timestamp
    - for authentication, message integrity and anti-replay

Comments are welcomed!

Ready for WGLC!

Thank You!