Secure DHCPv6 with Public Key

Replacement of draft-ietf-dhc-secure-dhcpv6

IETF 90 DHC WG

July, 2014

Sheng JIANG

Sean SHEN

Dacheng ZHANG (Speaker)

Tatuya Jinmei (New co-author)

Background & Status

- **“Secure DHCPv6 with Public Key” replaced draft-ietf-dhc-secure-dhcpv6, inherited the maturity from old document**

- **Passed WGLC in May 2014, an update version has been submitted**

  - Most of comments are addressed

  - Still one major modification suggested by Francis Dupont, which need WG discussion (later page)

Major Changes

- Added a new section "Deployment Consideration";
- Corrected the format of field in the Public Key Option;
- Added consideration for large DHCPv6 message transmission;
- Added TimestampFail error code;
- Refined the retransmission rules on clients;
- Refined the text and typos.

Planned Updates that Reached Consensus

- Introduce a nonce option which will be processed as an extension of the transaction ID (so there are already 3 octets)
- Put the timestamp in its own option (so it can be omitted)

Discussion

- **Francis: They are useless without the trust anchor, the whole chain, CRLs, etc**
- **Another side: certificate could be very useful for server , which is always online, to authorize the client. It is much less useful on a client, which have to do authorization without network access**

- **Potential choices for WG to pick up:**
  - Keep certificate-based authorization both server/client, and clarify the trust-anchor for validation on client and providing of trust chain is out of scope or future work
  - Keep certificate-based authorization on server, limit certificate on client for Leap of Faith only
  - Keep certificate-based authorization on server, drop certificate on client
  - Drop certificate from this draft totally

Comments are welcomed!

Ready for moving forward

Thank You!