Network Time Security

draft-ietf-ntp-cms-for-nts-messages-06
draft-ietf-ntp-network-time-security-14
draft-ietf-ntp-using-nts-for-ntp-05

Kristof Teichel, Dieter Sibold

NTS: WGLC Design Team Progress

- WGLC generated large amounts of feedback (too much for the two-man main team to manage)
- Led to creation of Design Team

Key Exchange

- IP fragmentation
  - NTS key exchange (MUST requirement in draft-ietf-ntp-using-nts-for-ntp-05) will cause IP fragmentation
    - → potential problems with NAT devices
    - → Negative implications on protocol security
- Considered alternatives
  - Appling DTLS for the key exchange
  - Time exchange always secured via NTS

Key Exchange (KE)	Port KE	Port TE
~~NTS Custom~~	~~NTP-EF via 123/udp~~	~~123/udp~~
~~NTS Custom~~	~~NNN/tcp~~	~~123/udp~~
DTLS native	NNN/udp	123/udp
DTLS over NTP	123/udp	123/udp

Key Exchange (continued …)

- Issues to deal with for any KE candidate
  - How to avoid fragmentation on IP level?
  - Whether/how to deal with rate limitations and NTP port usage? (Assumed important)

Port for KE	**Adhere to usual NTP rate limitations?**	**Comment**
UDP 123	YES	• Maximum compatibility, • Possibly very (!) slow
UDP 123	NO	• Might not be accepted at certain NTP providers
UDP != 123 or TCP (any)	NO	• Requires additional open port (might slow down rollout)

Key Exchange (continued …)

- Issues to deal with for any KE candidate
  - Under which conditions to allow usage of unauthenticated time stamps?
  - Whether/how to handle peer mode?
  - Whether/how to include authorization?
  - Requirement for two-way authentication?
  - How to ensure cryptographic algorithm agility (BCP 201)?

Questions about NTS Key Exchange

- Fewer overall exchanges?
- Fewer cryptographic operations?
- Seed refresh: to mention or not?

Other Agenda Items

- Improve handling of cipher suites (for MAC generation)
  - (draft-aanchal4-ntp-mac-00)
  - Already done in NTS: generalize from HMAC to MAC
- Discussion about Chicken-and-Egg problem
- Discussion about benefits/disadvantages of different overall security mechanisms
- Symmetry of message sizes in time sync exchange

Next steps

- Clarification of which KE is mandatory in NTS for NTP draft
- Consideration/inclusion of Daniel Franke's proposal
- Specification of KE in NTS for NTP draft
- Related
  - Peer mode
  - Usage of unauthenticated timing information
- Consideration/inclusion of draft-aanchal4-ntp-mac-00

Next steps (continued …)

- New version of draft-ietf-ntp-using-nts-for-ntp
- WGLC right after IETF 97th (Seoul)
  - Also **requires** WGLC for generic NTS (!)
  - May be possible without CMS-4-NTS (depending on choice of key exchange mechanism)