Network Time Security

`draft-ietf-ntp-using-nts-for-ntp-08`

Kristof Teichel, Dieter Sibold, Daniel Franke

Changes from version 07 to 08

- Replaced DTLS with TLS as the key exchange mechanism for client-server mode
- Re-worked language about (non-)traceability in “Objectives” and “Privacy Considerations” sections
- Removed option to piggy-back key exchange for client-server mode over NTP packets

Key Exchange

Mode	Key Exchange	Port / Key Exchange	NTP Packet Transport	Port / Transport
Mode 1 & 2	DTLS	UDP / ???	as DTLS payload	UDP / ???
Mode 3 & 4	TLS	TCP / ???	NTP Packet with NTS extensions	UDP / 123
Mode 6	DTLS*)	UDP/ ???	as DTLS payload	UDP/???*)

- Piggy backing DTLS KE over NTP (within extension fields) is postponed
- Optional key exchange mechanism are not allowed for NTS for NTP
- *) Support for TCP may be added

Open Issues and Next Steps

- Key management for load-balanced servers (informative)
- Security considerations:
  - Subsection “Usage of NTP Pools”

Generic NTS draft
(draft-ietf-ntp-network-time-security-15)

- What to do with non-NTP-specific NTS document?
  - Is intended to provide protection schemes for unicast and broadcast/multicast time sync messages (NTP and PTP)
  - Until now very limited feedback on the NTS messages for broadcast/multicast time sync messages
- Make it consistent with draft-ietf-ntp-using-nts-for-ntp-08
- Change RFC intended status to “Informational”