Suggested improvements to NTS for NTP (draft 12)

draft-dansarie-nts-00

Marcus Dansarie
marcus@dansarie.se

Ragnar “Ragge” Sundblad
ragge@netnod.se

Background

- Swedish IX Netnod operates 8 high-speed stratum-1 NTP servers [1]
  - 4 × 10 Gb/s mode 3 requests per server
  - Implemented in FPGA
  - Free to use for anyone anywhere (www.ntp.se)
- Funding from Swedish Post and Telecom Authority (PTS)
- Would like to offer all its NTP users authenticated time

[1] https://www.netnod.se/sites/default/files/ntp/Network_Time_Protocol_from_a_distributed_timescale_traceable_to_UTC.pdf (https://bit.ly/2utWWSW)

Main changes and additions

- Separation of NTS-KE and NTP servers
  - Addition of “NTS Server Negotiation” NTS record
- Require TLS 1.3 instead of 1.2
- Change of the “NTS Authenticator and Encrypted Extension Fields”
- Require NTS-implementing servers to always include “Unique Identifier” extension field

Main operational improvements

- Allows the use of NTS in pool infrastructures
- Increased resilience of NTP service
- Simplifies implementation in FPGA and hardware
- Increased protection against off-path attacks

Thank you!

- Rfcdiff between draft 12 and our draft:

  https://bit.ly/2NirLB1