Network Time Security

draft-ietf-ntp-network-time-security-05
draft-ietf-ntp-cms-for-nts-message-00

Dr. Dieter Sibold[1] Kristof Teichel[1] Stephen Röttger[2]

[1]PTB

[2]Google Inc

IETF 91 (Honolulu), Nov 9 – 14, 2014

Outline

History

- **IETF 83:** Presented security issues of RFC 5906 (autokey)
- **IETF 84:** Presented plan for a new autokey standard
- **IETF 85–86:** Presented I-D “draft-sibold-autokey-nn”
- **IETF 87–90:** Renamed I-D and presented as “draft-ietf-ntp-network-time-security-*nn*”

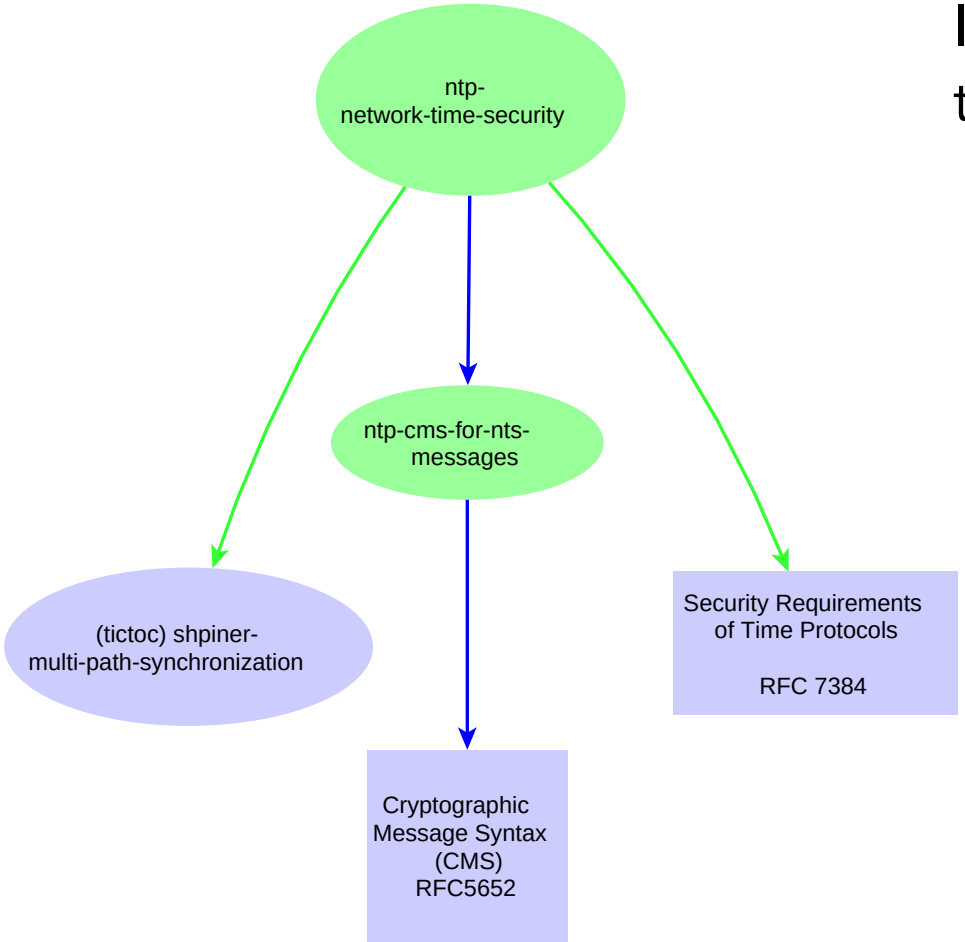
Scope

Network Time Security shall provide:

- Authenticity of time servers
- Integrity of synchronization data packets
- Conformity with the TICTOC Security Requirements
- Support of NTP (unicast and broadcast mode)
- Support of PTP as far as possible

Major Changes

Accompanying document to describe CMS structures for NTS Messages (draft-ietf-ntp-cms-for-nts-messages-00)

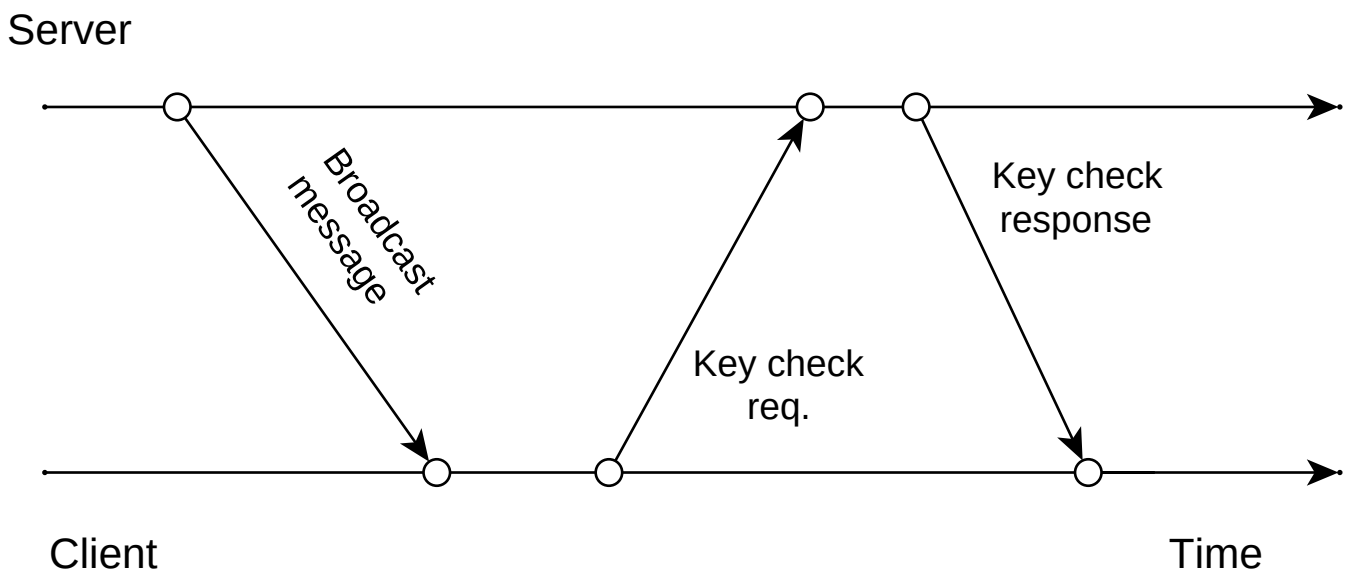


It describes CMS structures for the following NTS message types

- NTS-Plain: Used for the time exchange messages, client and server keyckeck; without CMS
- NTS-Certified: Used during cookie request message
- NTS-Signed-and-Encrypted: Used for secure cookie exchange
- NTS-Signed: Used during authentication process

Major Changes cont.

- Merging of the association and certification steps
  $\rightarrow$ cleaned up appendices
- Added discussion on delay attacks, especially for broadcast
  $\rightarrow$ Customized applied TESLA scheme with an additional key check exchange



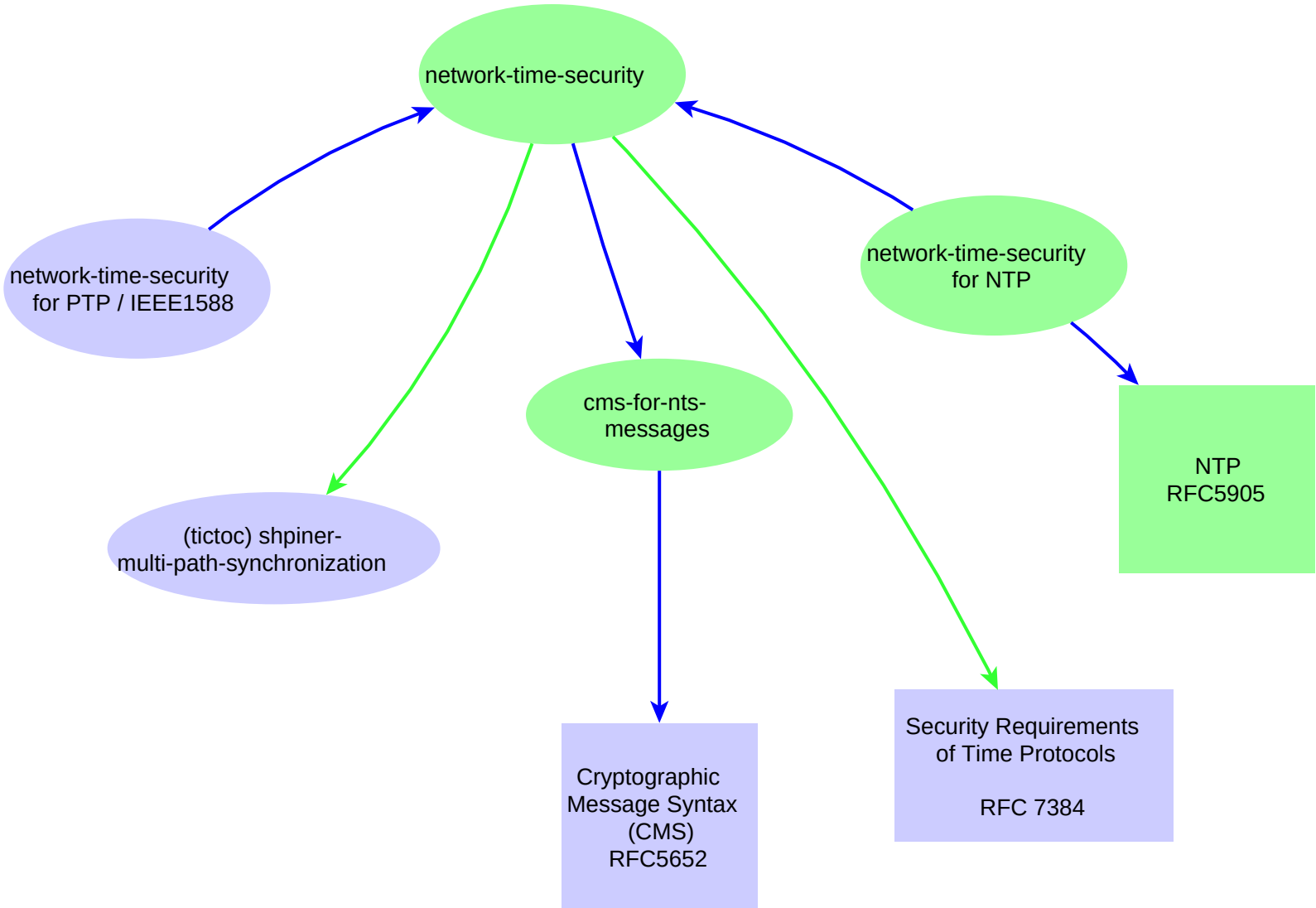
Next steps

Disentanglement of NTP and PTP

- **Motivation**
  - Current NTS documents attempts to be applicable for NTP and PTP (as far as possible)
  - However the current message type description are specific to NTP and are not always appropriate for PTP
- **Suggestion (Comments?)**
  - Formulation of a more generic NTS document, with generic descriptions of manycast und unicast message types
  - Specific documents for NTP and PTP
    - *NTS for NTP*: that would essentially be the current document
    - *NTS for PTP*: existence of this document depends mainly on IEEE P1588 WG

Next steps (continued . . .)

Draft dependency graph



Next steps (continued . . .)

- Consideration of DANE
- IANA Considerations
- **Review and comments are requested from:**
  - TICTOC Working Group
  - NTP Working Group
  - NTP development team