Physikalisch-Technische Bundesanstalt
Braunschweig und Berlin
Nationales Metrologieinstitut

Network Time Security

draft-ietf-ntp-network-time-security-08
draft-ietf-ntp-cms-for-nts-message-02
draft-ietf-ntp-using-nts-for-ntp-00

Dr. Dieter Sibold Kristof Teichel Stephen Röttger

IETF 92 (Dallas), March 22-27, 2015

Outline

History

Scope

Progress/Major Changes

New Structure
- NTS Document
- CMS-for-NTS Document
- NTS-for-NTP Document

Non IETF activities
- IEEE P1588 WG
- Authenticated NTP Project (ANTP)

Next steps

History

- **IETF 83:** Presentation of security issues of RFC 5906 (autokey)
- **IETF 84:** Presentation of plan for a new autokey standard
- **IETF 85–86:** I-D "draft-sibold-autokey-*nn*"
- **IETF 87–90:** I-D "draft-ietf-ntp-network-time-security-*nn*"
- **IETF 91:** Continuation as "draft-ietf-ntp-network-time-security-05" and addition of document "draft-ietf-ntp-cms-for-nts-message-00"
- **Submission January 2015:**
  - (January 16) draft-ietf-ntp-network-time-security-06
  - (January 22) draft-ietf-ntp-cms-for-nts-message-01
- **Submission March 2015:**
  - (March 03) draft-ietf-ntp-network-time-security-07
  - (March 05) draft-ietf-ntp-network-time-security-08
  - (March 06) draft-ietf-ntp-cms-for-nts-message-02
  - (March 06) draft-ietf-ntp-using-nts-for-ntp-00

Scope

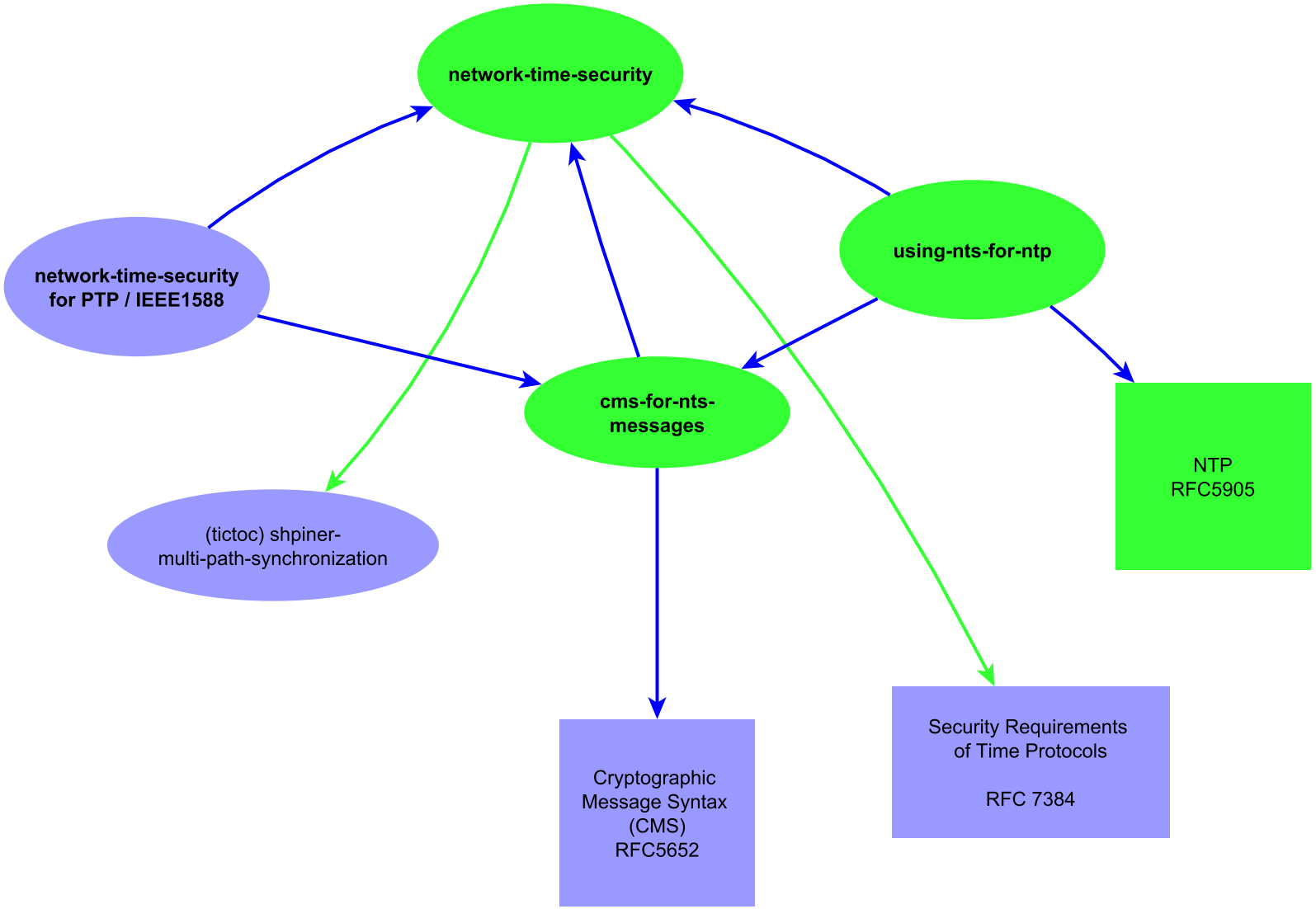
Network Time Security shall provide:

- Authenticity of time servers
- Integrity of synchronization data packets
- Conformity with TICTOC's Security Requirements (RFC 7384)
- Support of NTP and PTP

Progress/Major Changes

- **Contract signed with NTF, implementation underway**
- **Protocol Messages:**
  - Added a nonce to association exchange and extended signature in response message over request data
- **Feedback:**
  - Tal Mizrahi
  - Authors of Authenticated NTP article
- **Document Structure:**
  - Overhaul of main document to be more generic (less NTP specific)
  - Overhaul of "draft-ietf-cms-for-nts-message" to also be more generic
  - Addition of document "draft-ietf-ntp-using-nts-on-ntp" (Holds the NTP specific content lost in the other documents)

New Structure: Overview



New Structure: Main Document

Main document now contains

- Objectives (protocol-independent)
- NTS overview (protocol-independent)
- List of message exchanges, each with:
  - Goals of this specific message exchange (isolated)
  - All necessary message types
  - Exchange procedure overview with diagram
- Considerations on server seed, hash algorithms and MAC generation (all generic; no specific data like bit lengths)
- Protocol-independent security considerations (added privacy discussion)
- Table of requirements (RFC 7384)
- Description of how NTS employs TESLA (generic with respect to bit lengths, choice of one-way function etc.)
- Overview of message dependencies and required pre-shared keys

New Structure: CMS-4-NTS

CMS-4-NTS document now contains:

- CMS conventions
  - Definition of archetypes
  - Use of pre-defined CMS content types
- ASN.1 structures for different message types
  (each has a comment on what additional information is needed for the message type)

New Structure: NTS-4-NTP

NTS-4-NTP document contains:

- Objectives for NTS-secured NTP
- Overview of NTS-secured NTP (unicast and broadcast mode)
- Protocol Sequence
  - Split into client and server behaviour description, each split into unicast and broadcast sequence
  - Sequence and order as appropriate for NTP
  - Behaviour description overlaps with main document
- Implementation notes: extends description from CMS-for-NTS document and gives specifics
- NTP-specific security considerations (e.g. NTP pools)
- Flow diagrams for NTP specific client behaviour

IEEE P1588 working group: NTS-4-PTP

First draft of NTS-4-PTP document contains:

- Protocol sequence as appropriate for PTP in mixed communication mode
- Description of NTS message structures in the context of PTP

Report: ANTP Project (1)

ANTP Contributors:

- Queensland University of Technology:
  Benjamin Dowling,
  Douglas Stebila
- Microsoft Research:
  Greg Zaverucha

Goals for ANTP:

- Authentication of single NTP server to SNTP client
- Integrity protection
- No server-side state for each client
- Low amount of public-key operations on server side

Report: ANTP Project (2)

Main Differences between ANTP and NTS approaches:

Differences in Scope:

- ANTP has no use of client certificates
  $\rightarrow$ no client authorization
- ANTP does not secure NTP broadcast

Differences in Methods:

- ANTP encrypts server state; transmits it to appropriate client
  NTS recalculates server state upon a time request
- ANTP contains additional "zero cryptographic delay" mode
  (sends cryptographic confirmations in a subsequent message)

Next steps

- **Version 09**
- **Future versions**
  - Consideration of DANE
  - IANA Considerations
- **Review and comments are requested from:**
  - TICTOC Working Group
  - NTP Working Group
  - NTP development team

APPENDIX: Detailed Diff (1)

- **Overhaul of main document to be more generic (less NTP specific)**
  - Removed differentiation of unicast and broadcast "mode"
  - Removed NTP inspired protocol sequence
  - Replaced protocol sequence by message dependency diagram
  - Removed specific data like bit length of nonces and keys
  - Removed protocol specific discussion like usage of NTP pools
- **Overhaul of "draft-ietf-cms-for-nts-message" to also be more generic**
  - Removed description of building messages via NTP packets

APPENDIX: Detailed Diff (2)

- **Clean-up of generic main document:**
  - Reworked Introduction
  - Reworked Objectives section
  - Generalized formulation of method for achieving initial time synchronization for TESLA
  - Reworked message dependecy diagram
  - Refreshed requirements table (RFC 7384)
  - For each message exchange, added:
    - description of purpose
    - procedure overview
  - Security Considerations:
    - Added paragraph on privacy
    - Shortened paragraph on certificate validation
    - Moved paragraph on random number generation here (from appendix)

APPENDIX: Detailed Diff (3)

- **Feedback:**
  - Feedback from Tal
    - Overhaul of terminology section (common terminology NTP/PTP)
    - Clarified the use of client certificates and public keys
    - Added message exchange flow diagrams
    - Added table for required pre-shared keys during communication
    - Appropriately marked appendices as normative/informative
  - Feedback from ANTP group
    - Clarified authorization
    - Association exchange: added nonce, also included request data in the signature
- **Corresponding changes in CMS document:**
  - Edited structure of association message objects

APPENDIX: Detailed Diff (4)

- **Last-minute corrections in main document:**
  - Minor syntax corrections
  - Inserted paragraph on different key pairs for encrypting and signing
  - Inserted missing objective as well as necessary client checks for association exchange