Network Time Security

draft-ietf-ntp-network-time-security-09
draft-ietf-ntp-cms-for-nts-message-04
draft-ietf-ntp-using-nts-for-ntp-01

Dr. Dieter Sibold **Kristof Teichel** **Stephen Röttger**

IETF 93 (Prague, Czech Republic), July 19–24, 2015

Outline

History

- Document's Dependency Graph

Scope

Progress/Major Changes

- Implementation
- Implementation Status
- Major Changes

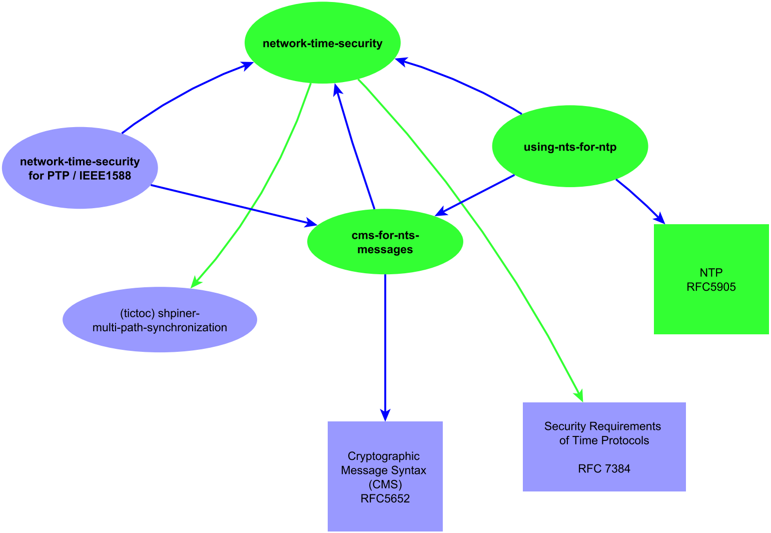
Open Questions

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*"
- **Since IETF 92:**
  - draft-ietf-ntp-network-time-security-*NN*
  - draft-ietf-ntp-cms-for-nts-message-*NN*
  - draft-ietf-ntp-using-nts-for-ntp-*NN*

New Structure: Overview


network-time-security
network-time-security for PTP / IEEE1588
using-nts-for-ntp
cms-for-nts-messages
(tictoc) shpiner-multi-path-synchronization
NTP RFC5905
Cryptographic Message Syntax (CMS) RFC5652
Security Requirements of Time Protocols
RFC 7384

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

Implementation

Two independent implementations from:

- Network Time Foundation
- University of Applied Science Wolfenbüttel, Germany

Currently both implementations focus on the realization of NTS for NTP

- Implementation of the authentication frame work and the secure cookie exchange
- Securing the time request and time response messages of the unicast associations

Implementation Status

Network Time Foundation

- Cryptographic primitives for CMS based authentication complete
- Unit tests for same nearly complete
- Systems with older versions of OpenSSL will be unable to use this implementation unless OpenSSL version is manually updated (such systems include RHEL 5, CentOS 5 and Mac OS X)

University of Applied Science Wolfenbüttel

- This is current work in the context of a Master thesis

Major Changes in the drafts

Network Time Security draft

- Description of Authentication and cookie exchange is replaced by a list of requirements
- CMS-base exchanges are moved to an appendix (Appendix B)

NTS for NTP draft

- Implementation MUST provide authentication and cookie exchange as described in Appendix B of the NTS document
- Implementation MAY optionally provide alternative means for authentication and cookie exchange (e. g. DTLS or DANE)

Open Questions

Stefan Weimers comments

- Clear separation of initial cookie exchange and subsequent time exchange messages
- Photuris cookie for the CMS-based authentication to protect for DoS attacks
- Session state variable definition as *opaque structure* (RFC 5077)

Next Steps

- Implementation
  - Finalization and testing of the unicast associations
  - Considerations regarding Broadcast/Multicast mode
- CMS-based association exchange: Introduction of additional features and partial redrafting. Relevant for:
  - Network Time Security draft, Appendix B
  - NTS for NTP draft