Network Time Security

draft-ietf-ntp-network-time-security-00

Authors: Dr. D. Sibold – PTB, Stephen Röttger

IETF 87, Berlin, Germany, July 28 – August 2, 2013

Introduction

Scope:

Network Time Security shall provide

- Authenticity of time servers
- Integrity of synchronization data packets
- Conformity with the TICTOC Security Requirements
- It must support NTP
- It can/should support PTP if possible

Introduction

History

IETF 83	Presentation of security issues of RFC 5906 (autokey)
IETF 84	Plan for a new autokey standard was presented
IETF 85	I-D “draft-sibold-autokey-00”
IETF 86	I-D “draft-sibold-autokey-02”

Current Status of the draft

IETF 87	I-D was renamed; it is presented as I-D “draft-ietf-ntp-network-time-security-00”

Changes since IETF 86

- **References to the autokey approach are removed**
- **According to the comments of the last IETF meeting**

  (C) Certificates and timeouts

  Addressed in a new subsection 6.7 (Restart of the Protocol Sequence). It describes the behavior of the client in case of expiration of

  - the server's certificate or seed (unicast and broadcast),
  - and one-way key chain (broadcast).

  Additionally the client may increase security by periodically checking the status of the server's certificate via OSCP.

  (C) Group authentication in broadcast mode (TESLA)

  Addressed in subsection 10.3 (Denial-of-Service in Broadcast Mode) of the section "Security Considerations".

Next steps

Review and comments are requested from

- **TICTOC WG**
- **NTP WG**
- **NTP development team**