Physikalisch-Technische Bundesanstalt
Braunschweig and Berlin
National Metrology Institute

# Setup of NTS

**Version: 1.6**

## 1 Index


2 NTS-Service and Authenticated Time Synchronization ..... 2

3 Functionality of NTS ..... 2

4 NTS Servers ..... 2

5 Setup of the NTS Client ..... 3

6 Annex ..... 5

6.1 Terms and Abbreviations ..... 5

# 2 NTS-Service and Authenticated Time Synchronization

PTB runs an authenticated time synchronization service. Users have the opportunity to receive secure time information and thus protect themselves against illegal behavior of third parties. To achieve this every customer has to apply for new cryptographic keys annually at PTB and manually add them to his server.

In it's efforts to improve processes PTB has established a time service which implements RFC 8915 of IETF called "Network Time Security" (NTS). Feel free to use this service. This document describes how to set up an NTS client.

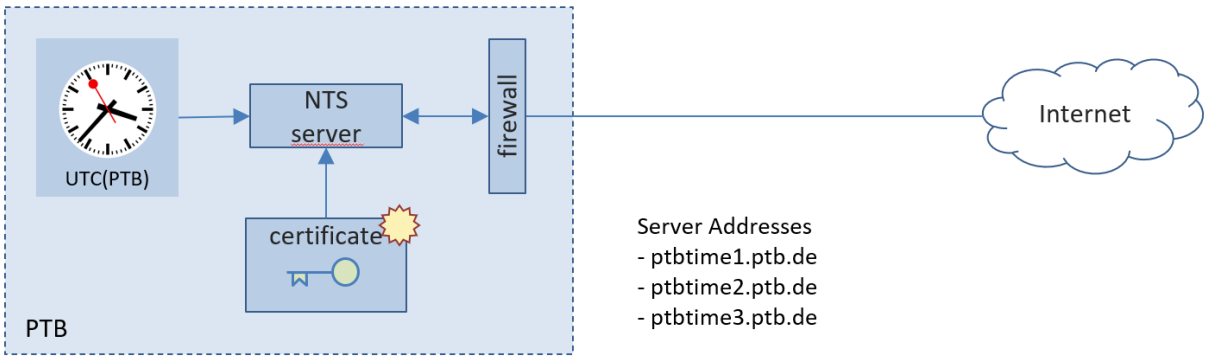
# 3 Functionality of NTS

The NTS standard has been developed to improve security of NTP. NTS is based on NTP and extends this standard by an automatic key exchange. Additionally, several provisions have been taken to protect the service against cyber-attacks.

Communication starts with the establishment of a TLS connection by which the service authenticates itself to the client by means of an X.509 certificate. Then cryptographic keys and several cookies will be exchanged and the connection closes. Using the keys and cookies the client starts enhanced NTP version 4 requests. In it's course new cookies will be exchanged continually which are not necessary for time synchronization but for the connection's security.

# 4 NTS Servers

For the test PTB provides a number of stratum 1 NTS servers. They are accessible on port 4460 via TCP (TLS connection for key exchange) and on port 123 via UDP (NTP requests).




Using the above-mentioned port for key exchange, you can connect to the servers without manual key exchange.

All NTS-Servers use Let's Encrypt certificates.

# 5 Setup of the NTS Client

At first you need an NTS client to connect to the server. Your traditional NTP server is not suitable for this purpose. There are several implementations of the new NTS standard you can use. In this document the NTP server of ntpsec.org will be used as an example. The code is open source and available on GitHub. It is based on NTP and has been enhanced with the NTS functionality. There is a description of compilation and installation available, also.

Your NTS client needs the certificate chain of Let's Encrypt if not available in your operating system. Please download it from https://letsencrypt.org/certificates/

As an example, the installation of NTPSec and configuration as an NTS client on a Ubuntu system is described consecutively. The command line on the client will be used as user root (sudo su).

Installation of necessary software. The number of needed software may vary dependent on the distribution. Here a list as an example.

```
apt-get install gcc
apt-get install python
apt-get install python-dev
apt-get install python-docutils
apt-get install m4
apt-get install xsltproc
apt-get install pkg-config
apt-get install libssl-dev
apt-get install mercurial
apt-get install asciidoc
apt-get install bison
apt-get install ntpdate
```

Download the latest ntpsec-package. On https://ntpsec.org you will find hints and links for download. In this example ntpsec-1.1.6.tar.gz has been downloaded from github. After checking the checksum proceed as follows:

```
cp ./ntpsec-1.1.6.tar.gz /usr/src
cd /usr/src
gunzip ./ntpsec-1.1.6.tar.gz
tar xfv ./ntpsec-1.1.6.tar
cd ntpsec-1.1.6/
./waf configure
./waf build
./waf install
```

The last three commands should show the message „<...> finished successfully". On the test client ntpd didn't start so adjustment of the service was necessary.

```
vi /lib/systemd/system/ntpd.service
```

Change program start as follows:

```
ExecStart=/usr/local/sbin/ntpd -N
```

Adjust the /etc/ntp.conf prior to starting the service. If it doesn't exist create a new one. The following configuration should do for the start.

```
server ptbtime1.ptb.de
statsdir /var/log/ntp/
statistics loopstats
filegen loopstats file loopstats type day link enable

driftfile /var/lib/ntp/drift/ntp.drift # path for drift file

logfile   /var/log/ntp/ntp.log
logconfig =allsync +allclock +allpeer +sysevents
```

Create the following folders.

```
mkdir /var/log/ntp
mkdir /var/lib/ntp
mkdir /var/lib/ntp/drift
```

Now start the service, check whether it is running...

```
systemctl start ntpd
systemctl status ntpd
```

... and query via ntpq -p whether the client connects to ptbtime1.ptb.de. Nevertheless the goal is a connection via NTS. But at first you need to configure the certificate chains of the NTS servers.

```
mkdir /var/lib/ntp/ssl/
cd /var/lib/ntp/ssl/
wget https://letsencrypt.org/certs/isrgrootx1.pem
```

Now configure the server in /etc/ntp.conf ...

```
server ptbtime1.ptb.de nts ca /var/lib/ntp/ssl/isrgrootx1.pem
server ptbtime2.ptb.de nts ca /var/lib/ntp/ssl/isrgrootx1.pem
server ptbtime3.ptb.de nts ca /var/lib/ntp/ssl/isrgrootx1.pem
```

... and restart ntpd.

```
systemctl restart ntpd
```

Now check the connection status.

```
ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
+ptbtime1.ptb.de .PTB.           1 8    37   64  377    0.2366  -0.7400   0.017
*ptbtime2.ptb.de .PTB.           1 8    30   64  377    0.4271  -0.8197   0.031
+ptbtime3.ptb.de .PTB.           1 8    26   64  377    0.7129   0.4231   0.048
```

In column “t” the status shows a number. It corresponds with the number of available cookies. If you see a number instead of a „u“ the connection is an NTS connection.

# 6 Annex

## 6.1 Terms and Abbreviations

| | |
|---|---|
| DFN | Deutsches Forschungsnetz (German National Research and Education Network) |
| NTP | Network Time Protocol |
| NTS | Network Time Security |
| PTB | Physikalisch-Technische Bundesanstalt<br>(The National Metrology Institute of Germany) |
| | |