Physikalisch-Technische Bundesanstalt
Braunschweig und Berlin
Nationales Metrologieinstitut

Einrichtung NTS

Version: 1.3

1 Inhaltsverzeichnis

2 Der NTS-Dienst und die Authentifizierte Zeitsynchronisation

Die PTB betreibt einen Dienst zur Authentifizierten Zeitsynchronisation. Damit haben Nutzer die Möglichkeit, eine gesicherte Zeitinformation zu empfangen und sich auf die Weise gegen rechtswidriges Verhalten Dritter zu schützen. Um dies zu erreichen, muss jeder Kunde jährlich neue kryptografische Schlüssel bei der PTB beantragen und nach Erhalt manuell installieren.

In ihrem Bestreben, die Abläufe zu vereinfachen, hat die PTB zum Test einen Zeitdienst aufgebaut, der den neuen RFC 8915 der IETF, „Network Time Security“ (NTS), umsetzt. Sie sind eingeladen, an diesem Test teilzunehmen. Das vorliegende Dokument erläutert, wie Sie einen NTS-Client aufsetzen können.

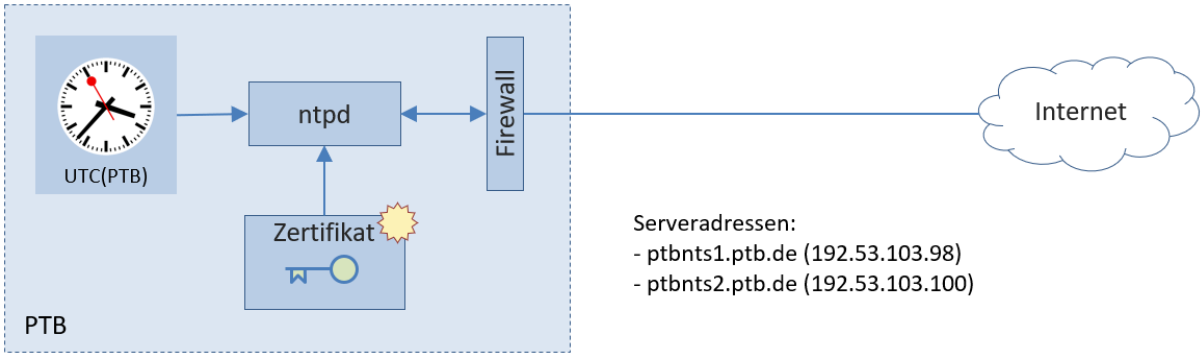
3 Funktionsweise von NTS

Der NTS-Standard wird entwickelt, um NTP sicherer zu machen. NTS basiert auf NTP, erweitert diesen Standard jedoch um einen automatischen Schlüsselaustausch. Zudem wurden eine Reihe Vorkehrungen getroffen, die den Dienst möglichst schwer angreifbar machen.

Die Kommunikation beginnt mit dem Aufbau einer TLS-Verbindung, über die sich der Dienst mit Hilfe eines X.509 Zertifikates gegenüber dem Client authentifiziert. Anschließend werden kryptografische Schlüssel sowie eine Anzahl Cookies ausgetauscht und die Verbindung wieder geschlossen. Mit Hilfe der Schlüssel und Cookies kann der Client nun NTP-Abfragen starten, die erweiterten NTP-Abfragen der Version 4 entsprechen. Dabei werden fortwährend neue Cookies ausgetauscht, die keine Relevanz für die Zeitsynchronisation haben, aber der Sicherheit der Verbindung dienen.

4 Testaufbau

Die PTB stellt zum Test zwei Stratum 1 NTS-Server zur Verfügung. Sie sind auf Port 4460 über TCP (TLS-Verbindung) und auf Port 123 über UDP (NTP-Abfragen) erreichbar.



Unter Verwendung der o.g. Ports können Sie sich ohne weiteren Schlüsselaustausch auf die Server verbinden.

Die NTS-Server verwenden folgende Zertifikate:

- ptbnts1.ptb.de : Zertifikat des DFN
- ptbnts2.ptb.de : Let’s Encrypt Zertifikat

5 Einrichtung des NTS-Clients

Wie bereits dargelegt, benötigen Sie einen NTS-Client, um sich mit dem Server zu verbinden. Ihr normaler NTP-Client ist dazu nicht geeignet. Es gibt bereits mehrere Implementierungen des neuen NTS-Standards, die Sie nutzen können. Als Beispiel sei hier die Verwendung des NTP-Servers von ntpsec.org angeführt, mid dem eine Verbindung zu ptbnts1.ptb.de aufgebaut werden soll. Der Code ist Open Source und auf GitHub verfügbar. Er basiert auf NTP und wurde unter Anderem um die NTS-Funktionen erweitert. Die Übersetzung und Installation sind dort beschrieben.

Ihr NTS-Client benötigt die Zertifikatkette des DFN-Vereins, um das X.509-Zertifikat unseres Servers prüfen zu können. Die Zertifikatkette erhalten Sie auf https://pki.pca.dfn.de/dfn-ca-global-g2/cgi-bin/pub/pki?cmd=getStaticPage;name=index;id=2&RA_ID=5110 unter „Zertifikatkette anzeigen“.

Nachfolgend wird beispielhaft die Installation des NTPsec und Einrichtung als NTS-Client auf einem Ubuntu-System beschrieben. Eingaben auf dem Client werden als User root durchgeführt (sudo su).

Erforderliche Pakete installieren. Die Zahl der erforderlichen Pakete kann abhängig von der Distribution variieren. Hier eine Beispielliste.

```
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
```

Neustes ntpsec-Paket herunterladen. Unter https://ntpsec.org finden sich Hinweise und Links zum Download. In diesem Beispiel wurde bei github die ntpsec-1.1.6.tar.gz heruntergeladen. Nach der Prüfung der Checksumme ist wie folgt weiter zu verfahren:

```
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
```

Die letzten drei Befehle müssen mit der Meldung „<...> finished successfully“ abgeschlossen werden. Auf dem Testclient startete der ntpd nicht, so dass der Dienst etwas angepasst werden musste.

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

Programmstart wie folgt verändert:

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

Vor dem Start des Dienstes muss die /etc/ntp.conf angepasst werden. Wenn sie nicht existiert muss sie neu erzeugt werden. Für den Anfang dürfte folgende Konfiguration ausreichen:

```
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
```

Dazu werden die entsprechenden Verzeichnisse erzeugt.

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

Nun können Sie den Dienst starten und schauen, ob er läuft...

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

... und mit ntpq -p abfragen, ob sich der Client mit ptbtime1.ptb.de verbindet. Das Ziel ist jedoch die Verbindung mit dem NTS-Server ptbnts1.ptb.de. Dazu muss zunächst die Zertifikatkette des NTS-Servers hinterlegt werden.

```
mkdir /var/lib/ntp/ssl/
cd /var/lib/ntp/ssl/
wget https://pki.pca.dfn.de/dfn-ca-global-g2/pub/cacert/chain.txt
mv ./chain.txt chain.pem
```

Nun tragen Sie den Server in die /etc/ntp.conf ein ...

```
server ptbnts1.ptb.de nts ca /var/lib/ntp/ssl/chain.pem
```

... und starten den ntpd neu.

```
systemctl restart ntpd
```

Nun können Sie den Verbindungsstatus prüfen.

```
ntpq -p
```

```
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
+ptbtime1.ptb.de .PTB.            1 u   37   64  377    0.2366  -0.7400   0.017
*ptbnts1.ptb.de  .PTB.            1 8   35   64  377    0.5211   0.5211   0.021
```

In der Spalte “t” sehen Sie, dass die Verbindung zu ptbnts1.ptb.de eine NTS-Verbindung ist. Hier wird die Anzahl der verfügbaren Session Cookies angezeigt.

6 Anhang

6.1 Begriffe, Abkürzungen

DFN	Deutsches Forschungsnetz
NTP	Network Time Protocol
NTS	Network Time Security
PTB	Physikalisch-Technische Bundesanstalt