Die Zeitserver der PTB

Der Auftrag

Die Physikalisch-Technische Bundesanstalt hat <...> die gesetzliche Zeit darzustellen und zu verbreiten. (§6, Abs. 2 EinhZeitG)

Die gesetzliche Zeit ist in §4 EinhZeitG definiert. Sie ist bestimmt durch die koordinierte Weltzeit unter Hinzufügung einer Stunde (Winterzeit) bzw. zwei Stunden (Sommerzeit).

Die PTB verteilt die Zeitinformationen auf verschiedenen Wegen. Diese Unterlage beschreibt die Weitergabe der Zeit über das Internet.

Grundsätze der Zeitverteilung

Die Priorität liegt auf der Verteilung der korrekten Zeit. Die Verfügbarkeit eines Zeitservers steht dem in der Priorität nach. Gibt es zu hohe Abweichungen von der korrekten Zeit oder Zweifel an der Korrektheit, wird der Zeitserver abgeschaltet.

Wartungen werden immer nur an einem Server gleichzeitig durchgeführt und nur dann, wenn kein anderer Server ausgefallen ist. Damit stehen zu jedem Zeitpunkt hinreichend viele Server zur Verfügung.

Die Überwachung der Zeitserver erfolgt auf verschiedenen Ebenen. Neben der Korrektheit der Zeit werden für den Betrieb wichtige Funktionen überwacht sowie Zertifikatwechsel und Sicherung der Statistiken überprüft.

Die Zeitserver

Die PTB betreibt vier öffentliche Zeitserver an zwei Standorten. Diese Server nutzten zur Zeitverteilung die folgenden IETF-Standards:

- NTP: „Network Time Protocol“, Version 4 (RFC 5905)
- NTS: „Network Time Security“ (RFC 8915)

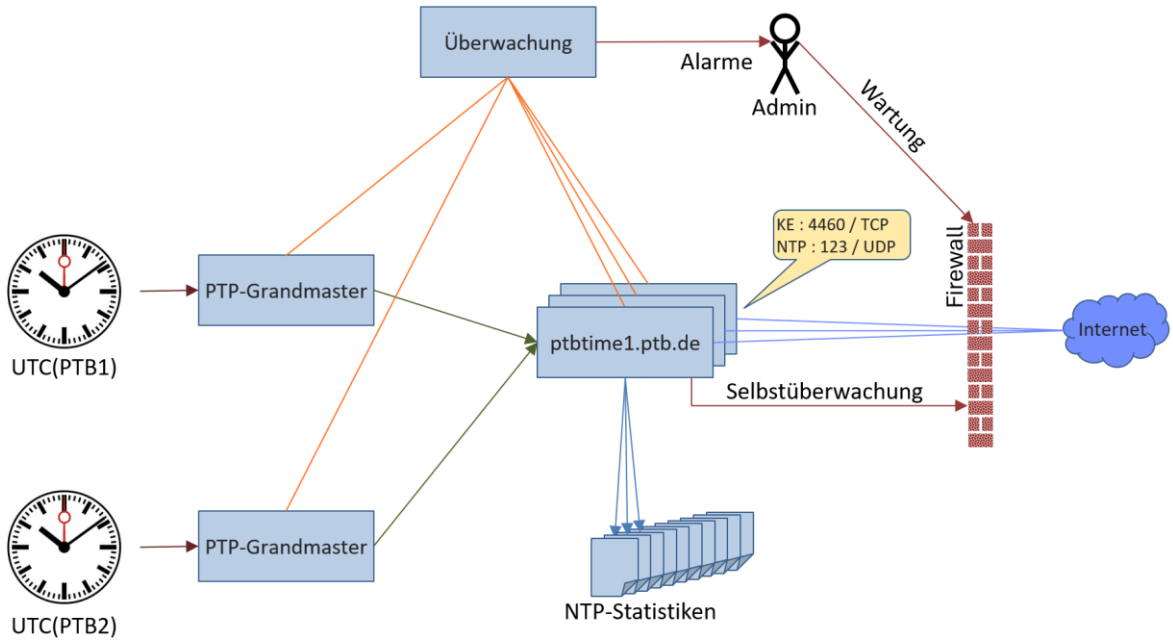
Mit NTP lassen sich die Zeitinformationen über das Internet abrufen. In Verbindung mit NTS wird der ansonsten ungeschützte NTP-Datenverkehr mit einem Message Authentication Code (MAC) authentifiziert. Der Austausch von kryptografischen Schlüsseln und die Authentifizierung des Zeitservers (basierend auf digitalen Zertifikaten) erfolgen automatisch durch den NTP/NTS-Client über eine initiale TLS-Verbindung.

Die PTB unterstützt die Übertragung der NTP-Zeitinformationen in ungesicherter und NTS-gesicherter Form. Dies hängt ausschließlich von der Konfiguration des anfragenden Clients ab.

Zeitserver-Infrastruktur

Die Zeitserver synchronisieren sich auf die in der PTB ansässigen Atomuhren. Die Anbindung erfolgt redundant. Bei Ausfall einer Quelle sind die Zeitserver weiterhin voll arbeitsfähig.

Aktuelle Architektur am Beispiel Braunschweig



Jeder Server verfügt über eine Selbstüberwachung. Steigt die Zeitabweichung von den Primärzeitquellen zu stark an, schaltet sich der Zeitserver automatisch ab.

Technische Informationen

Server	ptbtime[1,2,3,4].ptb.de
Erreichbarkeit	über IPv4 und IPv6
Ports	4460/TCP für den NTS-Key-Establishment-Dienst (der initiale TLS-Kanal) 123/UDP für den NTP-Dienst
ICMP-Ping	nicht möglich
NTP/NTS-Dienst	Chrony
Zeitzone	UTC
Rate Limiting	ausgeschaltet
Diensttrennung	NTS-Key-Establishment-Dienst und NTP laufen auf derselben Maschine
Serverzertifikate	Es werden Serverzertifikate von Let's Encrypt eingesetzt
Selbstabschaltung	Bei Abweichungen > 10 ms
Recovery	Automatisch, wenn der Time Offset mindestens 5 Minuten unter 10 ms bleibt
Netzwerkanbindung	redundant je Server
Primärzeitquellen	redundant
Statistiken	In der Form wie tracking.log bei chrony, jedoch eine Datei pro Tag. Aufbewahrungsfrist: 15 Jahre. Bereitstellung bei Bedarf. Logdaten: Offset, Standardabweichung, Root Delay usw.

Eigenschaften von NTS für NTPv4

Was NTS bietet

NTS sichert den Transport von Zeitinformationen kryptografisch ab

- Es ermöglicht die Integritätsprüfung der übertragenen Zeitinformationen
- Es ermöglicht die Authentizitätsprüfung des Absenders
- Es verhindert Tracking von NTS-Informationen

Was NTS nicht bietet

- NTS verschlüsselt nicht die Zeitinformationen im NTP-Paket
- NTS gibt keine rechtsverbindliche Aussage über die Zeitinformationen
    - Es gibt keine Garantie, dass die übertragene Zeit korrekt ist
    - Es gibt keine Garantie, dass der Empfänger die empfangene Zeit korrekt einsetzt

Weitere Eigenschaften

- NTS-gesicherte NTP Clients benötigen das korrekte Root-Zertifikat und eine grobe Zeit, um den Zeitserver zu authentifizieren.
- Die Synchronisationsgenauigkeit verschlechtert sich durch NTS typischerweise nur sehr gering (<100µs).
- Es besteht die Möglichkeit, dass NTS-gesicherte NTP-Pakete aufgrund von Filtern/Firewalls nicht empfangen werden.