

Zertifikate für Nebraska

ACHTUNG:

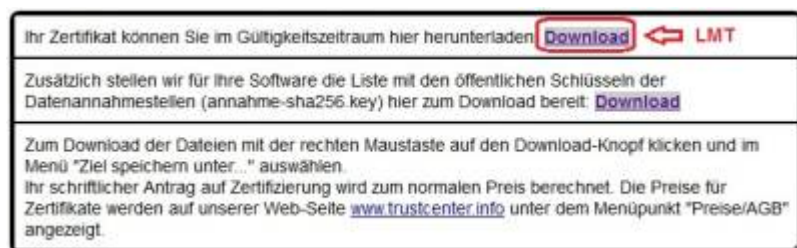


Solange der Zertifikatsantrag unterwegs ist, keinen neuen Schlüssel erzeugen - erst nach Ablauf des Zertifikates nach ca. 3 Jahren wieder erforderlich. Wenn sie trotzdem einen neuen Schlüssel erzeugen, stimmt er nicht mehr mit den Daten überein, die im Antrag mitgeschickt worden sind und sie dürfen den Antrag nochmals stellen (und nochmals 70 Euro berappen).

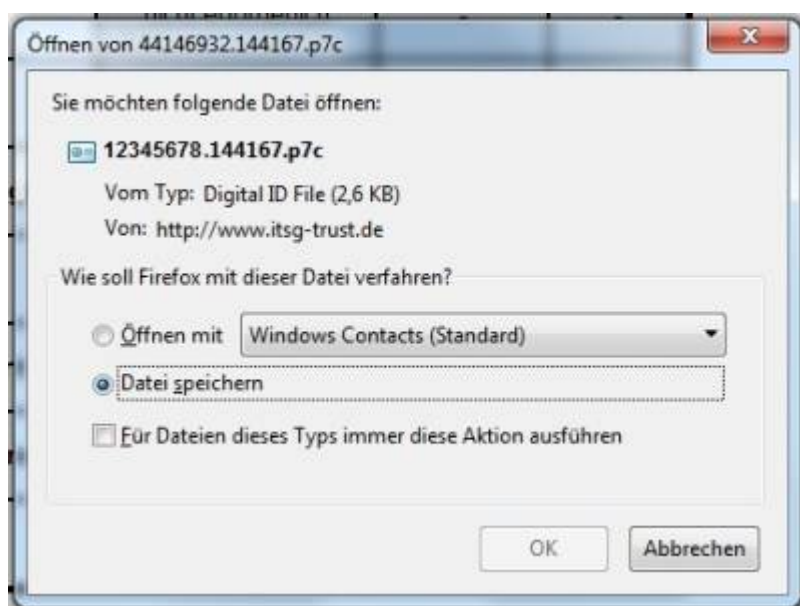
Nach etwa 3-5 Tagen bekommen Sie eine Antwortmail von der ITSG. In dieser Mail ist ein Link zu einer Seite, auf der Sie Ihren „Auftragstatus“ nachvollziehen können. Ist alles in Ordnung können Sie von dieser Seite auch ihr Zertifikat, sowie die Liste mit den öffentlichen Schlüsseln der Datenannahmestellen (annahme-sha256.key) herunterladen. **Diesen Link bitte nicht verlieren.**

4. Einlesen des Zertifikats-Reply

Nachdem die [Bearbeitung des Zertifikat-Antrages](#) durch die ITSG abgeschlossen ist, kann dieses in Nebraska eingelesen werden.



Zunächst laden Sie das Zertifikat herunter (**LMT**-Klick auf Download-Link) und speichern es im Ordner <Thera-Pi-Verzeichnis>/keystore/<Ihr-IK>.



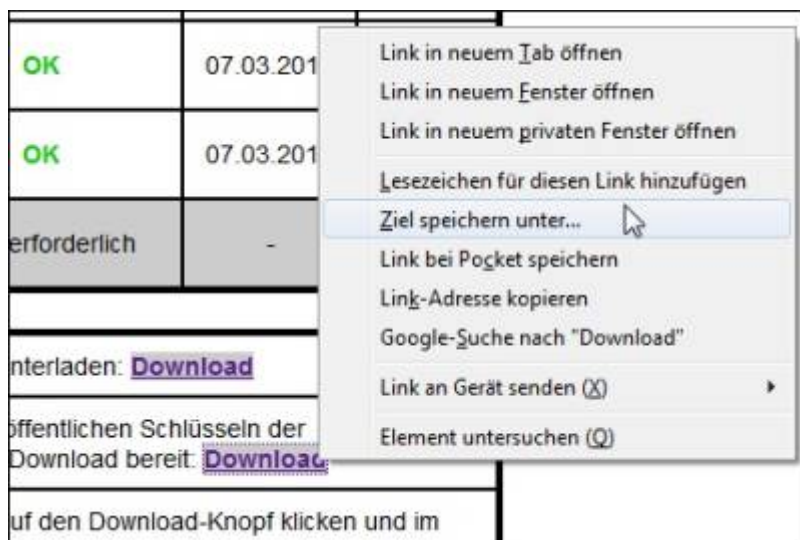
In der Zeit von Anfang 2018 bis Jahresende 2019 lieferte die ITSG eine Datei mit dem Namensschema **<erste 8 Stellen Ihres IK>.<6-stell. Nummer>.p7c.** wenn der Zertifikatsantrag einen Schlüssel mit 2048 bit Länge enthielt.

Sollte dies noch der Fall sein, so kürzen Sie den Dateinamen auf die ersten 8 Stellen Ihrer IK.

Seit Anfang 2019 kommt (wieder) das Namensschema **<erste 8 Stellen Ihres IK>.p7c.**

zum Einsatz wenn der Zertifikatsantrag mit einem 4096 bit Schlüssel gestellt wurde.

Nebraska erkennt selbständig anhand der Länge des eigenen Schlüssels, wie die Datei mit der Zertifikatsantwort heißen muss und fordert diese ein, falls nicht im keystore-Ordner vorhanden.



Ebenfalls in Abhängigkeit von der Schlüssellänge des eigenen Zertifikates muss die Datei mit den Zertifikaten der Datenannahmestellen passend im keystore-Verzeichnis bereitgestellt werden:

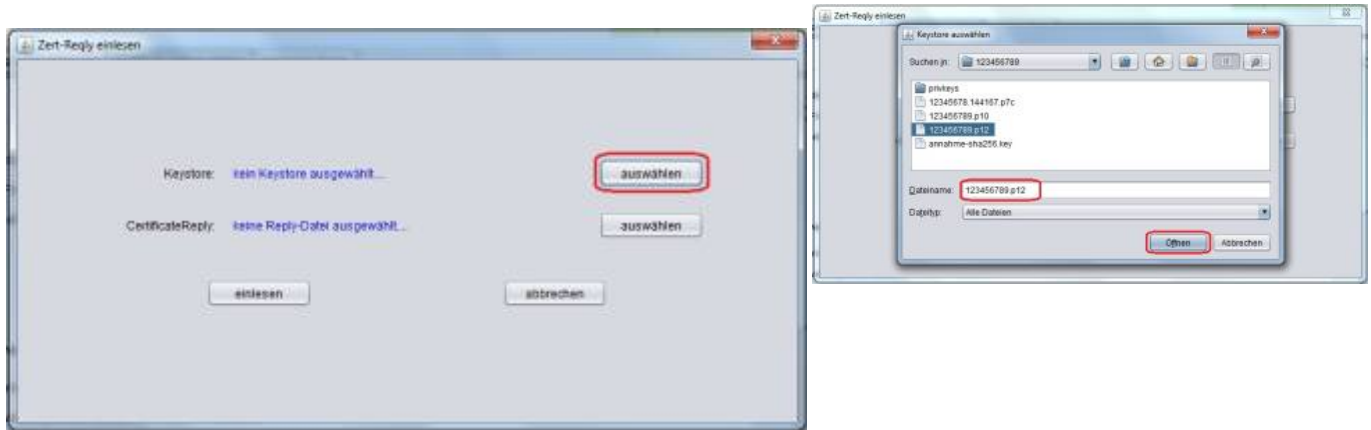
- annahme-sha256.key, falls noch ein 2048 bit Zertifikat vorhanden ist (diese bleiben bis zum Ablauf weiterhin gültig) oder
- annahme-rsa4096.key wenn es sich um ein Zertifikat mit 4096 bit Schlüssel handelt.

Zum Download der Datei führen Sie einen **RMT-Klick** auf Download-Link aus und wählen **Ziel speichern unter ...**. Speichern Sie die Datei ebenfalls im Ordner <Thera-Pi-Verzeichnis>/keystore/<Ihr-IK>.

The screenshot shows the 'Nebraska' software interface. The title bar says 'Nebraska'. The main window has a header with the text 'Antrag auf Zertifizierung bei der ITSG stellen' and instructions. Below this, there are tabs: 'Zertifikate auswerten / manuell Verschlüsseln', 'Zertifikats-Antrag stellen', and 'Nebraska Tools'. The 'Zertifikats-Antrag stellen' tab is active. The form is divided into two main sections: 'Stammdaten' (Personal Data) and 'Freiwillige Angaben zur Software, sowie wichtige Angaben zur Datenübermittlung' (Optional information about the software and important information about data transfer). The 'Stammdaten' section includes fields for 'Institutionskennzeichen (IK)', 'Name/Firma des Antragstellers', 'verantwortlicher Ansprechpartner', 'Straße', 'PLZ', 'Ort', 'Betriebsnummer', 'Telefon-Nr.', 'Telefax-Nr.', 'E-Mail-Adresse', and a checkbox for 'Zertifizierungsantwort an diese E-Mail-Adresse'. The 'Freiwillige Angaben...' section includes fields for 'Mit welchem Softwarehaus arbeiten Sie zusammen?', 'Welche Fachanwendung setzen sie ein?', 'Wie wird der Request der ITSG übermittelt?', and 'optional, max. 12 Zeichen) Das Kundenkennwort ist?'. At the bottom, there are buttons: 'Datenimport aus Thera-Pi', 'Zert-Antrag drucken', 'Zert-Request erzeugen', 'Zert-Reply einlesen' (highlighted with a red rectangle), and 'zusätzl. IK einlesen f. §301'.

Sind alle Dateien bereitgestellt, Nebraska aus Thera-Pi heraus starten und, wie unter [Papierantrag ausfüllen und drucken](#) beschrieben, den Mandanten auswählen, für den das Zertifikat beantragt wurde.

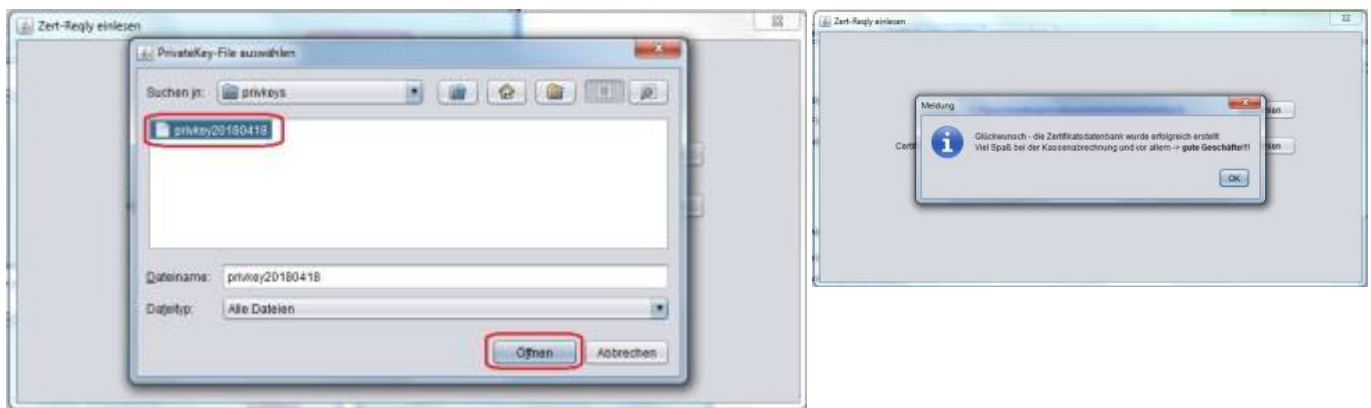
Dann mit dem Button **Zert-Reply einlesen** die Verarbeitung der Zertifikatsdateien starten.



Keystore auswählen (falls nicht nach drücken von **Auswählen** automatisch erkannt) ...



... Zertifikatsdatei wählen (dito) und **Einlesen** starten ...



... auf Nachfrage den privaten Schlüssel, **der zusammen mit dem Zertifikatsrequest erzeugt wurde**, auswählen. Die **Zertifikats-Datei kann nur mit diesem entschlüsselt werden!**

passiert im Hintergrund: Handelt es sich um ein erstmals erteiltes Zertifikat, so müssen zudem noch die **aktuellen Zertifikate der Datenannahmestellen** eingelesen werden.

Kurz darauf ist der keystore mit dem neuen Zertifikat komplett und steht für die Abrechnung zur Verfügung. Sie sehen dann unter dem Reiter **Zertifikate auswerten / manuell verschlüsseln** die Liste gefüllt mit allen offiziellen Kostenträgern aus der Datei annahme-*.key und auch Ihr eigenes Zertifikat ist enthalten.



Tipp:

Wer's gerne ganz sicher hat, verschlüsselt anschließend noch eine beliebige Datei **manuell** (auch) auf das eigene IK. Das manuellen Entschlüsseln der Ergebnisdatei muss wiederum eine Datei liefern, die mit



der Ursprungsdatei identisch ist.

From:

<https://www.thera-pi-software.de/dokuwiki/> - Thera- π Wiki

Permanent link:

https://www.thera-pi-software.de/dokuwiki/doku.php?id=systeminit:nebraska:cert_reply

Last update: **2023/01/21 20:59**

