HZD
Hessische Zentrale für Datenverarbeitung

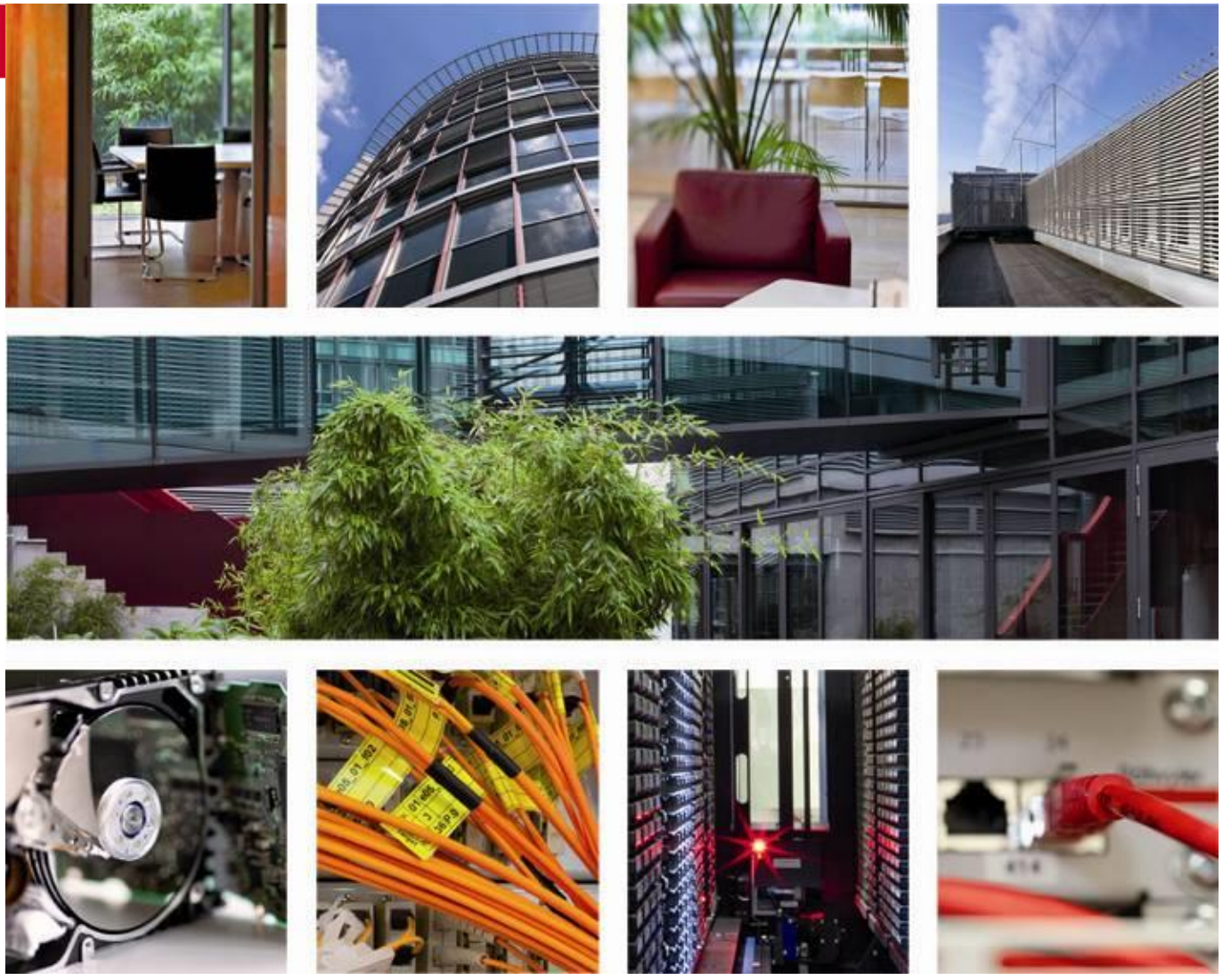
HESSEN

OASIS Zertifikate

Nutzungsbedingungen und Installationsanleitung

ab Release 7.0

veröffentlicht am 04.03.2024



Inhaltsverzeichnis

1 Allgemeines 4

2 Nutzungsbedingungen 4

3 Kurzanleitung 5

4 Installation der Zertifikate auf dem lokalen Computer 5

4.1 Speichern der Zertifikatsdateien auf dem lokalen Computer 6

4.2 Umbenennen der Zertifikatsdateien 7
4.2.1 Dateierweiterungen im (Windows-) Explorer einblenden 9

4.3 Installation der Zertifikate für Microsoft Edge und Google Chrome 10
4.3.1 Installation des personalisierten Zertifikats 10
4.3.2 Installation des OASIS Root-Zertifikats 14
4.3.3 Aufrufen von OASIS WEB in Microsoft Edge und Google Chrome 17

4.4 Installation der Zertifikate für Mozilla Firefox 18
4.4.1 Installation des personalisierten Zertifikats 19
4.4.2 Installation des OASIS Root-Zertifikats 21
4.4.3 Aufrufen von OASIS WEB im Mozilla Firefox 23

5 Prüfen, ob die OASIS Zertifikate korrekt installiert sind 24

5.1 Zertifikate im Microsoft Edge prüfen 24
5.1.1 Zertifikate anzeigen 25

5.2 Zertifikate im Google Chrome prüfen 26

5.3 Zertifikate im Mozilla Firefox prüfen 29

6 FAQ - Häufig gestellte Fragen 31

6.1 Kann ich das Zertifikat mehrmals installieren? 31

6.2 Ich habe mein Passwort für das Zertifikat nicht mehr 31

6.3 Mein Rechner kann keine Verbindung mit OASIS aufbauen 31

6.4 Mein OASIS Zertifikat läuft bald ab. Wie kann ich es verlängern? 32

6.5 Ich habe ein Ersatz-Zertifikat bekommen. Muss ich das mitgelieferte Root-Zertifikat auch installieren? 32

6.6 Mein Rechner wurde gestohlen. Was soll ich tun? 32

7 Anlage Kontaktinformation 32

7.1 OASIS Hotline rund um die Uhr.....32

1 Allgemeines

Ein digitales Zertifikat – im Folgenden kurz Zertifikat genannt – ist eine Datei, die auf einem Computer hinterlegt wird und die Identität von Personen oder Unternehmen bestätigt. Hierzu ist es erforderlich, dass ein Zertifikat durch eine vertrauenswürdige Stelle – der sogenannten Certification Authority (CA) – ausgestellt wird. Beim Einsatz solcher Zertifikate in Computerprogrammen bestätigt die CA die Echtheit des Zertifikats. Insofern verhält sich das digitale Zertifikat wie ein Personalausweis, der durch eine Behörde ausgestellt wird und bei der im Bedarfsfall die Echtheit des Ausweises geprüft werden kann.
Ein personalisiertes Zertifikat erhalten Sie direkt vom OASIS Team. Die Erstellung des Zertifikates erfolgt automatisch nach dem erfolgreichen Vertragsabschluss oder 1 bis 2 Monate vor dem Ablauf eines bestehenden Zertifikats. Die Laufzeit des personalisierten Zertifikats beträgt 2 Jahre.
Sie erhalten den privaten Schlüssel des personalisierten Zertifikates direkt per E-Mail zur Installation auf dem lokalen Computer. Die Auslieferung erfolgt per passwortgeschützter Datei. Das Passwort erhalten Sie entweder direkt vom OASIS Team per Post, oder von der OASIS Hotline nach korrekter Beantwortung der 3 Sicherheitsfragen.
Das Root-Zertifikat des OASIS-CA wird mitgeliefert und muss zusätzlich auf dem lokalen Computer installiert werden. Die Installation dieses Zertifikats erfolgt ohne Passwort.

Das Zertifikat ist grundsätzlich universell auf jedem Betriebssystem einsatzbar. Die hier vorliegende Anleitung bezieht sich jedoch auf den Einsatz des Zertifikates auf einem aktuellen Windows Betriebssystem (Windows 10 oder neuer). Für andere Betriebssysteme kann kein technischer Support geleistet werden. Wenden Sie sich im Zweifelsfall an Ihren technischen Dienstleiter.

Anweisung zu Ihrer Sicherheit:
Um schnellstmöglich auf Probleme mit Ihrem Zertifikat reagieren zu können, sollten Sie dieses Dokument „OASIS Zertifikate“ ausdrucken und verfügbar halten.

2 Nutzungsbedingungen

Es gelten folgende Nutzungsbedingungen:

1. Alle Regelungen der Nutzungsbedingungen sind verpflichtend und von allen OASIS-Vertragspartnern sowie deren Mitarbeiterinnen und Mitarbeitern einzuhalten.
2. Die Zertifikate sowie das Passwort sind vertraulich zu behandeln.
3. Da die Zertifikate an die E-Mailadresse des Veranstalters sowie davon abweichenden Zertifikatsempfängern versendet werden, sind Änderungen per E-Mail an oasis@rpda.hessen.de anzuzeigen.
4. Das Ihnen zur Verfügung gestellte Zertifikat darf nur genutzt werden, solange ein gültiger Nutzungsvertrag besteht. Bei Beendigung des Vertrags sind die Zugangsdaten sowie

das Zertifikat von allen IT-Systemen des Nutzers sowie gegebenenfalls des Dienstleisters zu löschen.

5. Sollte ein Zertifikat kompromittiert werden (z.B. durch Diebstahl eines PCs) ist die OASIS Hotline (Tel.: +49 (0)6652 / 187 22 12) zu unterrichten. Die OASIS Hotline wird das Zertifikat nach korrekter Beantwortung der drei Sicherheitsfragen umgehend sperren und durch ein Neues ersetzen.

3 Kurzanleitung

WICHTIG:
Falls eine externe Softwarelösung für den Anschluss an OASIS eingesetzt wird, sollten Sie mit dem Betreiber der Softwarelösung klären wie die OASIS Zertifikate einzubinden sind. Der IT-Service-Desk kann Sie dabei nicht unterstützen!

Diese Kurzanleitung fasst alle weiter unten ausführlich aufgeführten Schritte zusammen.

1. Speichern Sie die in der E-Mail zugesendeten Zertifikate lokal im Dateisystem ab und löschen Sie im Dateinamen der beiden Zertifikatsdateien die Endung „.123“. (Siehe Anleitung in den Kapiteln 4.1 und 4.2)
2. Installieren Sie beide Zertifikate in Ihren bevorzugten Browser. Der Vorgang ist je nach Browser unterschiedlich. (Siehe Anleitung in Kapitel 4.3.)
3. Rufen Sie die URL https://oasis.hessen.de/oasisweb von OASIS auf. Falls die Anmeldemaske nicht erscheint, prüfen Sie, ob die Zertifikate korrekt installiert sind (Siehe entsprechende Anleitung in Kapitel 5).
4. Loggen Sie sich mit dem erhaltenen OASIS-WEB Account und Passwort ein.
5. Fahren Sie fort wie in der OASIS WEB Anwenderanleitung beschrieben ist. Die aktuelle Version der OASIS WEB Anwenderanleitung kann von einer OASIS Webseite heruntergeladen werden (Siehe Kapitel ‚Anlage Kontaktdaten‘ in diesem Dokument).

4 Installation der Zertifikate auf dem lokalen Computer

Die Zertifikate werden per E-Mail an den Veranstalter und Zertifikatsempfänger geschickt und haben die Endung „.123“. Diese ist erforderlich, damit der Anhang nicht von Sicherheitssystemen ausgefiltert wird und muss vor der Installation entfernt werden. Im ersten Schritt werden die Zertifikatsdateien lokal gespeichert. Dann werden sie umbenannt und anschließend installiert.

4.1 Speichern der Zertifikatsdateien auf dem lokalen Computer

Öffnen Sie in Ihrem Mailclient die Mail mit den von OASIS erstellten Zertifikaten und speichern Sie die Anhänge auf allen Computern die eine Verbindung zu OSIS aufbauen sollen. Bei Windowssystemen eignet sich zum Beispiel der Download Ordner.

Im Folgenden wird beispielhaft dieser Vorgang mit dem Outlook Mailclient vorgeführt.

Die Mail im Outlook Mailclient öffnen.

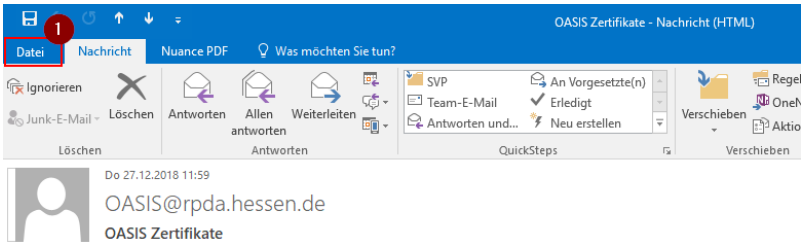


Abbildung 1: Outlook Mailclient

Klick auf „Datei“ um das Untermenü zu öffnen.

Abbildung 2: Speichern der Anlagen über den Outlook Mailclient

„Anlagen speichern“ wählen.

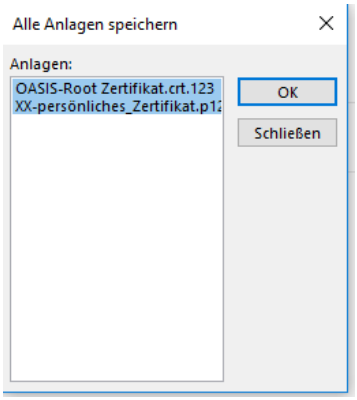


Abbildung 3: "Alle Anlagen speichern" Menü

Weiter mit „OK“ um alle Anlagen zu speichern

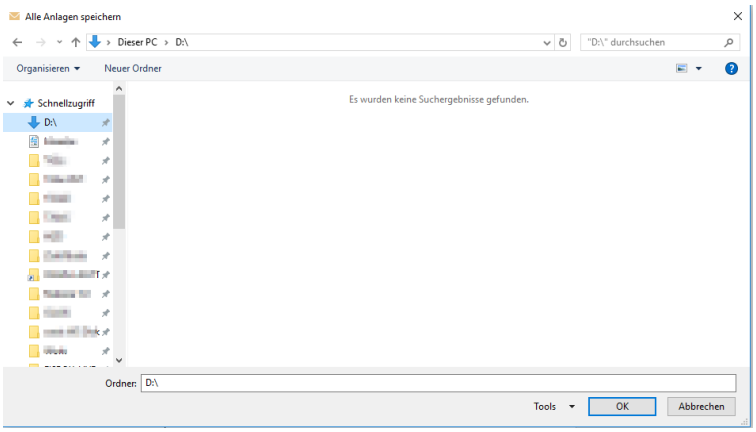


Abbildung 4: Speicherplatz Auswahlmenu

Wählen Sie einen lokalen Ordner, z.B. den Download Ordner, aus und „OK“ um die Anlagen zu speichern.

4.2 Umbenennen der Zertifikatsdateien

Die Endung „.123“ muss entfernt werden, um die Zertifikate zu installieren. Um dies auf einem Windows-Rechner zu tun, öffnen Sie den Ordner im Windows-Explorer, in dem die Zertifikatsdateien gespeichert wurden.

Falls die Endung „.123“ nicht sichtbar ist, führen Sie die Anleitung in dem Unterkapitel ‚Dateierweiterungen im (Windows-) Explorer einblenden‘ aus.

Klicken Sie mit der Rechten-Maustaste auf eine der Zertifikatsdateien und wählen Sie „Umbenennen“.

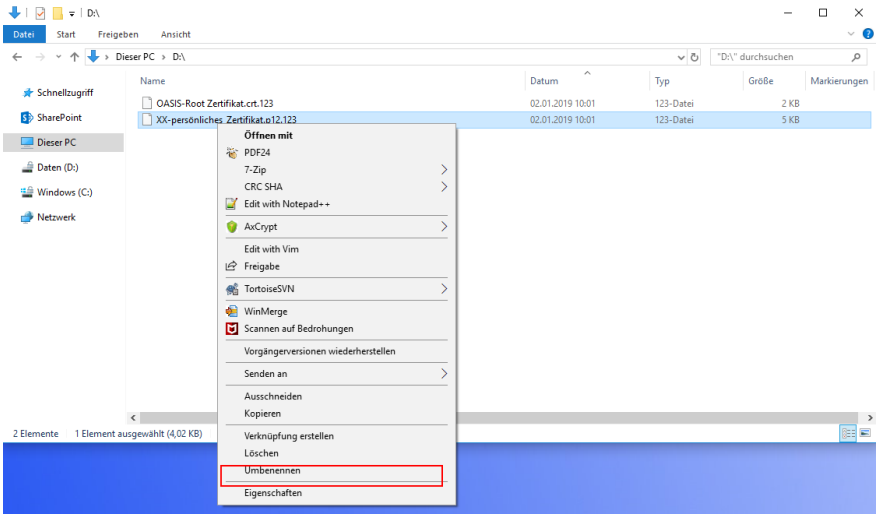


Abbildung 5: Umbenennen der Zertifikatsdatei in Windows Explorer

Klicken Sie in das Kästchen hinten dem „.123“ und entfernen Sie die Endung „.123“.

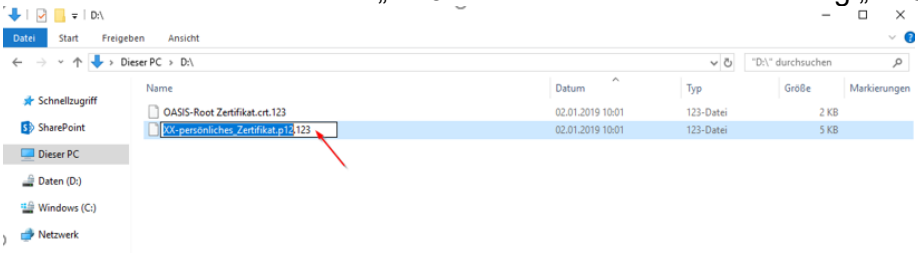


Abbildung 6: Entfernen ".123" in dem Namen der Zertifikatsdatei

Anschließend die Enter-Taste drücken.

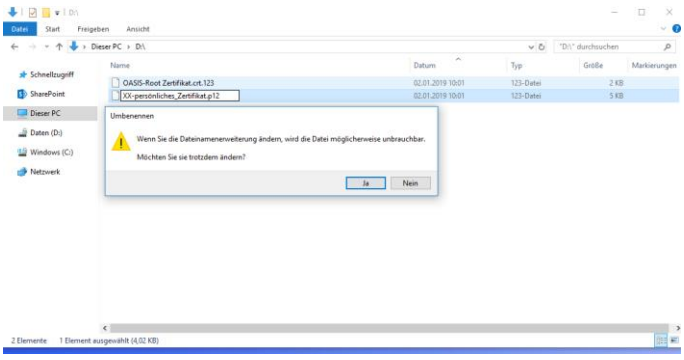


Abbildung 7: Speichern der Dateinamenänderung

Der erscheinende Hinweis ist mit „Ja“ zu beantworten, um die Änderung des Dateinamens zu speichern.

Führen Sie die Schritte für das Umbenennen auch mit der zweiten Zertifikatsdatei aus.

4.2.1 Dateierweiterungen im (Windows-) Explorer einblenden

Im Windows-Explorer-Menü ‚Ansicht' wählen und rechts die Optionen öffnen.

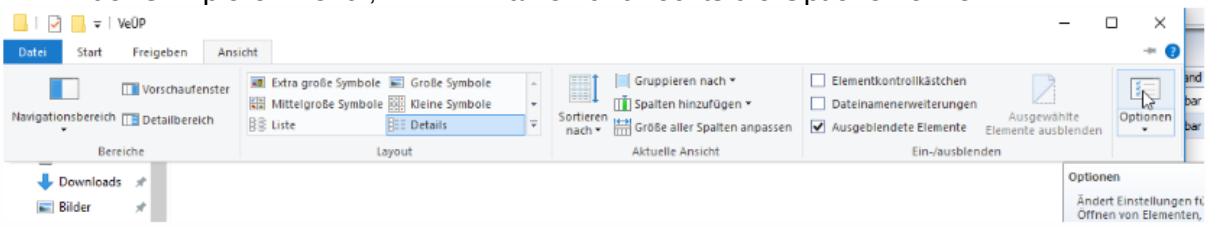


Abbildung 8: Ansicht-Menü in Windows Explorer wählen

In den Ordneroptionen in den Reiter Ansicht wechseln und „Erweiterungen bei bekannten Dateitypen ausblenden" **deaktivieren** und anschließend den Button ‚Übernehmen' tätigen.

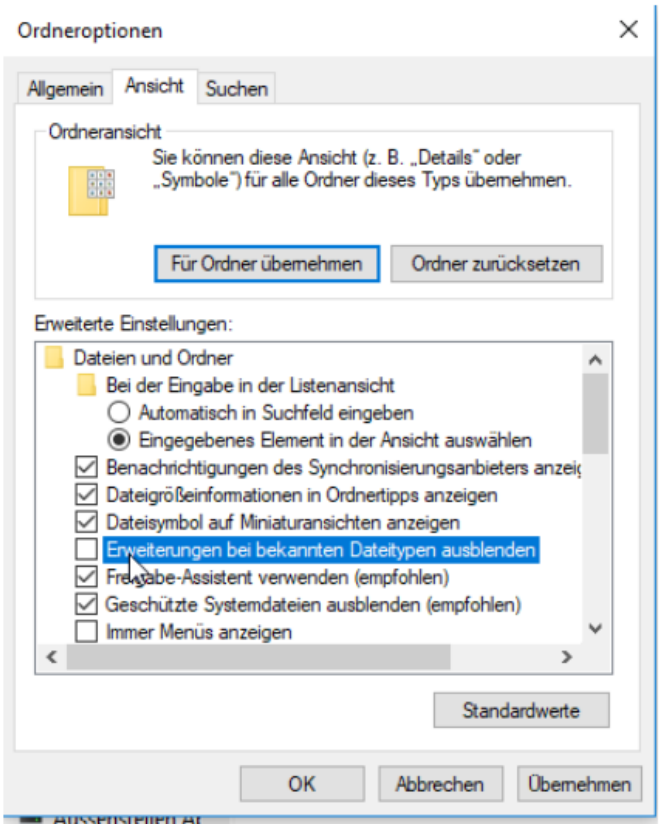


Abbildung 9: Ansicht-Ordneroptionen-Menü

4.3 Installation der Zertifikate für Microsoft Edge und Google Chrome

4.3.1 Installation des personalisierten Zertifikats

Voraussetzungen:

- Die Datei mit dem Zertifikat liegt Ihnen lokal vor,
- Das Zertifikatspasswort, das Sie entweder direkt vom OASIS Team per Post, oder von der OASIS Hotline nach korrekter Beantwortung der 3 Sicherheitsfragen erhalten haben, liegt vor,
- und Sie haben den Ordner mit der Zertifikatsdatei geöffnet.

Führen Sie einen Doppelklick auf die P12-Datei aus. Hierauf startet der Zertifikatimport-Assistent, der Sie durch die weiteren Schritte leitet.

Im ersten Schritt müssen Sie festlegen, welche Nutzer auf Basis des Zertifikats arbeiten sollen. Hat jeder Mitarbeiter am lokalen Computer ein eigenes Benutzerkonto, sollten Sie „Lokaler Computer“ auswählen. Hiermit erhalten alle Nutzer des Computers Zugriff auf das Zertifikat. Wenn Sie hier „Aktueller Benutzer“ auswählen, steht das Zertifikat nur für den angemeldeten Benutzer zur Verfügung.

Achtung: Die Installation mit der Auswahl *Lokaler Computer* funktioniert nur, wenn Sie administrative Rechte auf dem Computer haben!

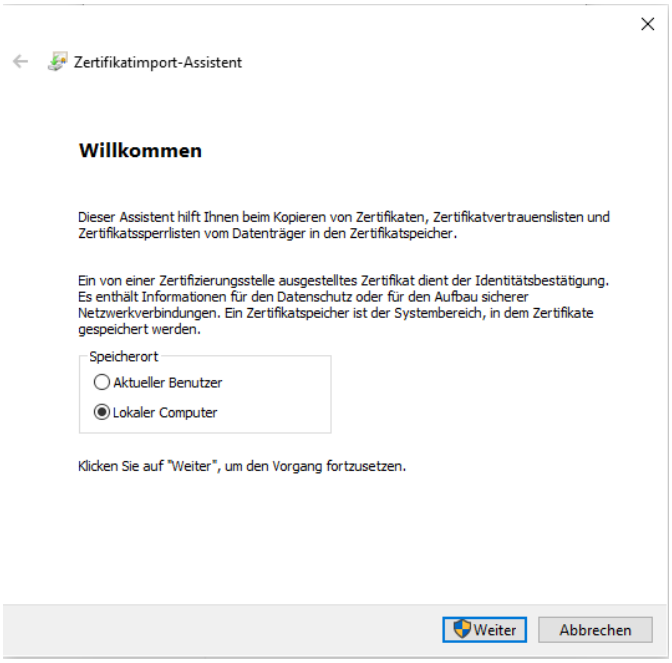


Abbildung 10: Zertifikatsimport-Assistent

Ein Klick auf „Weiter“ führt Sie zum nächsten Schritt. Hier erhalten Sie noch einmal die Möglichkeit, die Zertifikatsdatei auszuwählen. Haben Sie mit einem Doppelklick auf die Datei den Assistenten gestartet, können Sie direkt „Weiter“ wählen.

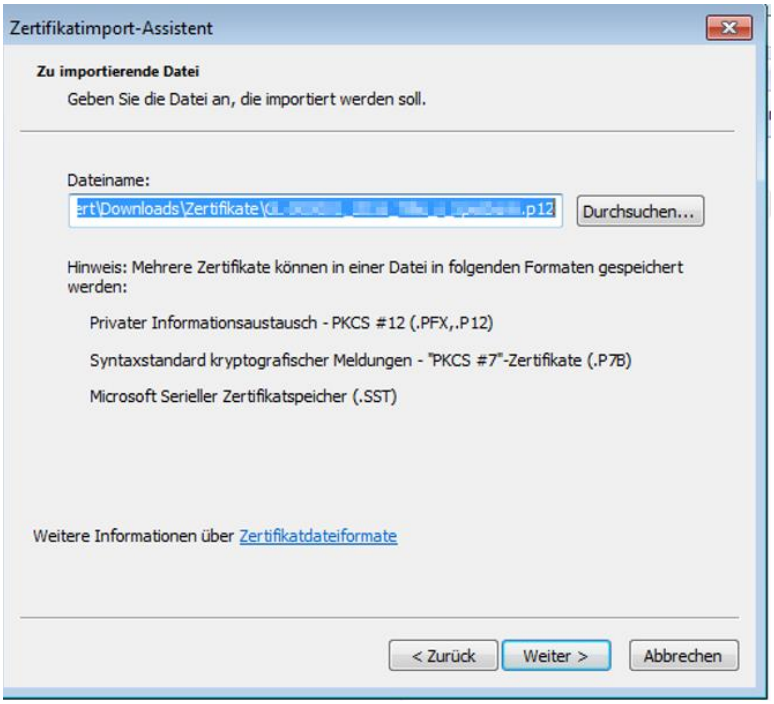


Abbildung 11: Dateiauswahl beim Import

Der folgende Schritt erfordert nun die Eingabe des Passwortes. Aus Sicherheitsgründen soll der Schlüssel nicht exportierbar gesetzt werden und daher soll diese Option nicht gewählt werden. Das Passwort eingeben und „Weiter“ wählen.

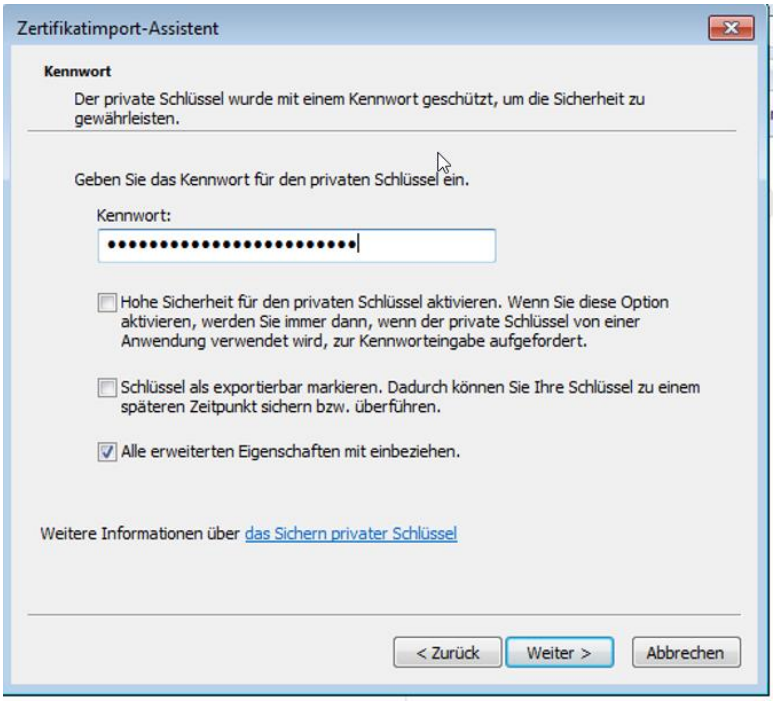


Abbildung 12: Eingabe des Passwortes bei der Zertifikatsinstallation

Im nächsten Fenster können die Voreinstellungen übernommen und direkt „Weiter“ gewählt werden.

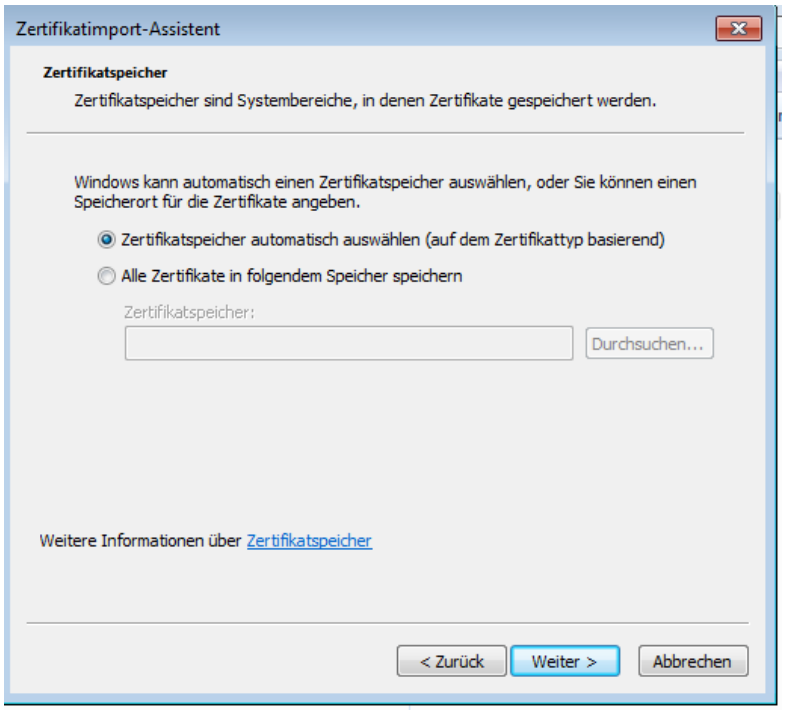


Abbildung 13: Auswahl des Zertifikatspeichers

Das letzte Fenster fasst alle getätigten Einstellungen zusammen und kann mit „Fertig stellen“ abgeschlossen werden.

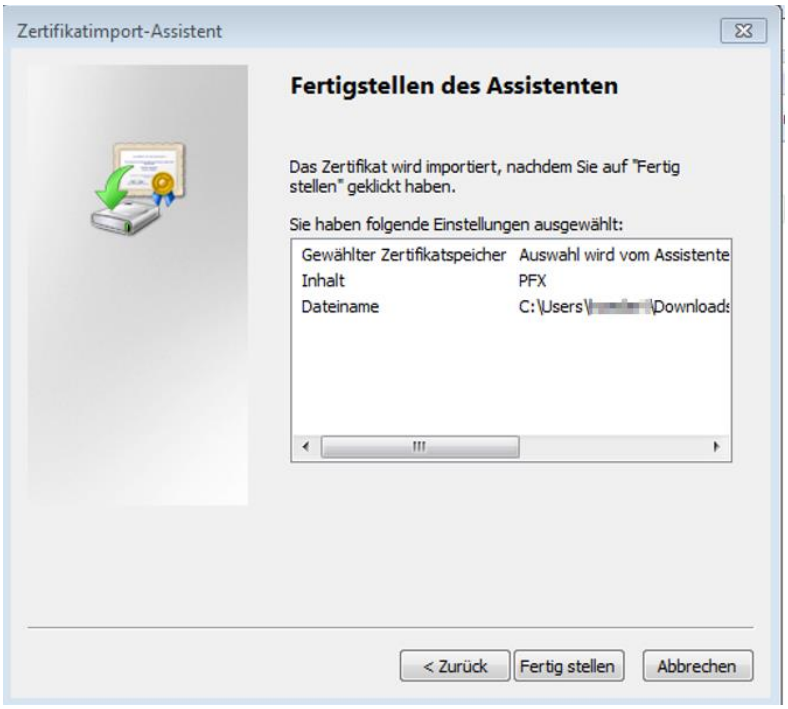


Abbildung 14: Zusammenfassung des Zertifikatimport-Assistenten

Bei der ersten Installation eines OASIS-Zertifikats erscheint die folgende Sicherheitswarnung, die mit „Ja“ beantwortet werden soll. Bitte beachten Sie, dass Ihr „Fingerabdruck“ vom „Fingerabdruck“ des Beispiels abweichen kann.

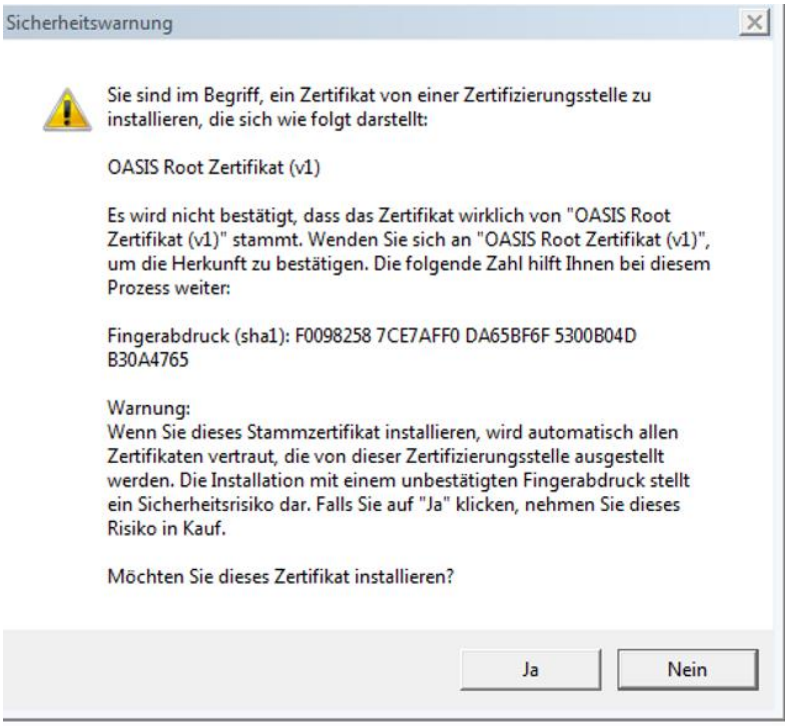


Abbildung 15: Sicherheitswarnung

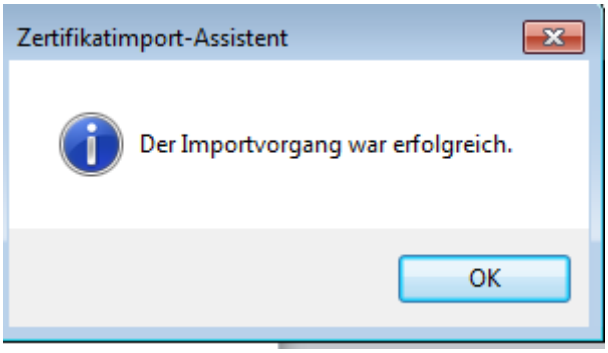


Abbildung 16: Abschluss des Imports

4.3.2 Installation des OASIS Root-Zertifikats

Voraussetzungen: Die Datei mit dem Zertifikat liegt Ihnen lokal vor und Sie haben den Ordner mit der Zertifikatsdatei geöffnet.

Führen Sie einen Doppelklick auf die OASIS-Root-Zertifikat.crt-Datei aus. Die Zertifikatsinformationen werden angezeigt. Bitte beachten Sie, dass der Gültigkeitszeitraum Ihres Root-Zertifikats vom Beispiel abweichen kann.

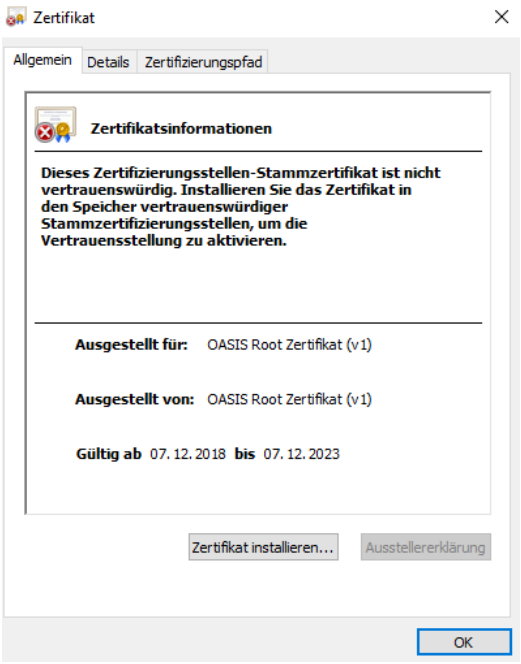


Abbildung 17: Zertifikatsinformationen des OASIS-Root-Zertifikats

Klick auf „Zertifikat installieren“, um den Zertifikatimport-Assistenten zu starten.

Im ersten Schritt müssen Sie festlegen, welche Nutzer auf Basis des Zertifikats arbeiten sollen. Hat jeder Mitarbeiter am lokalen Computer ein eigenes Benutzerkonto sollten Sie „Lokaler Computer“ auswählen. Hiermit erhalten alle Nutzer des Computers Zugriff auf das Zertifikat. Wenn Sie hier „Aktueller Benutzer“ auswählen, steht das Zertifikat nur für den angemeldeten Benutzer zur Verfügung.

Achtung: Die Installation mit der Auswahl *Lokaler Computer* funktioniert nur, wenn Sie administrative Rechte auf dem Computer haben!

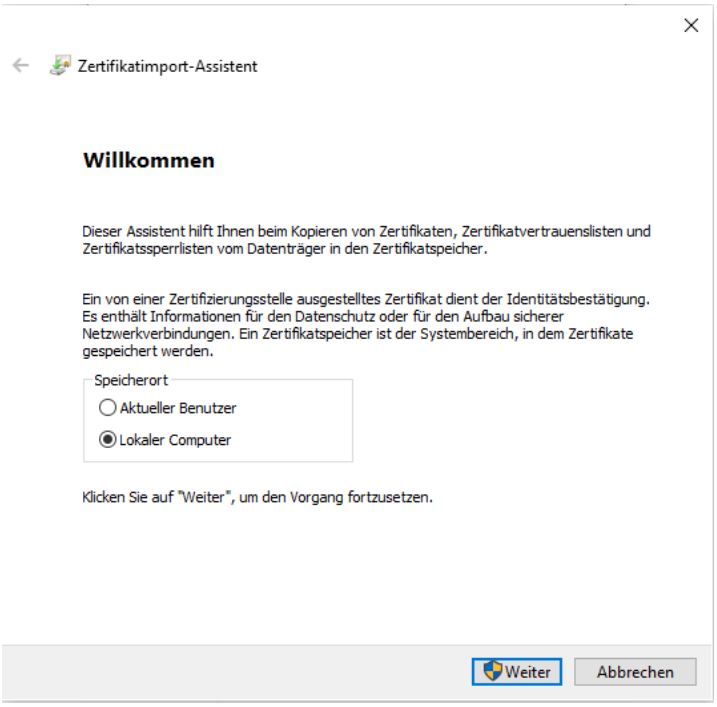


Abbildung 18: Zertifikatsimport-Assistent

Ein Klick auf „Weiter“ führt Sie zum nächsten Schritt.

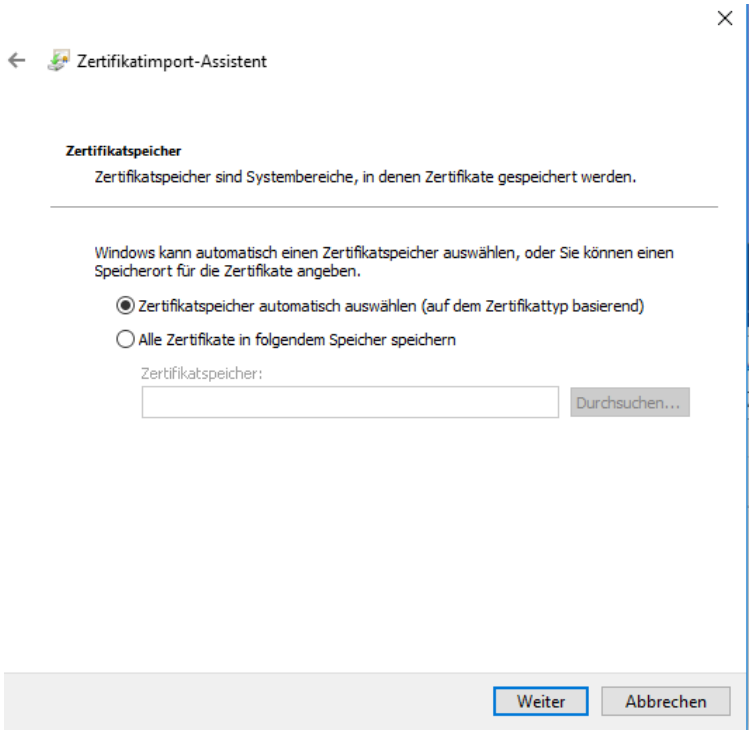


Abbildung 19: Auswahl des Zertifikatsspeichers

Im diesem Fenster können die Voreinstellungen übernommen und direkt „Weiter“ gewählt werden.

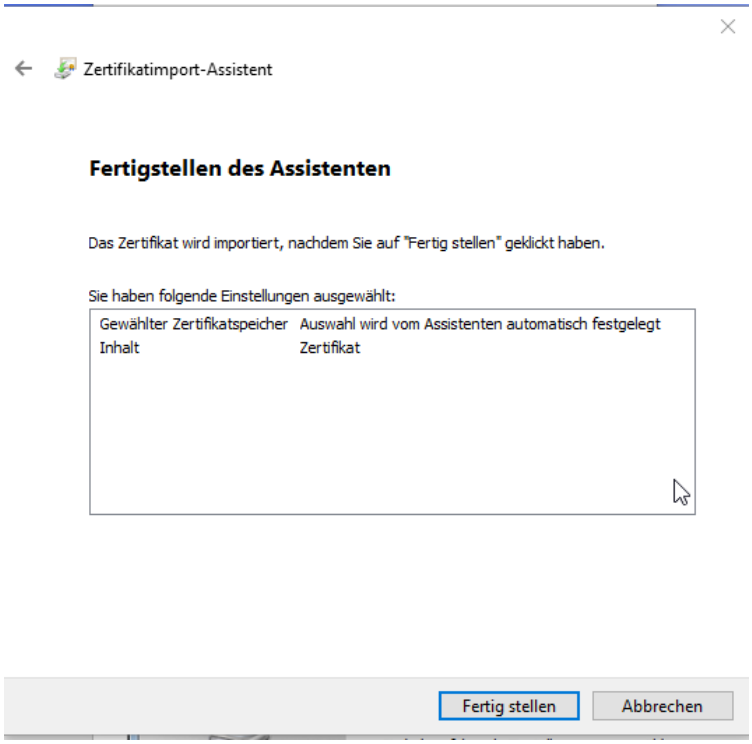


Abbildung 20: Zusammenfassung des Zertifikatimport-Assistenten

Das letzte Fenster fasst alle getätigten Einstellungen zusammen und kann mit „Fertig stellen“ abgeschlossen werden.

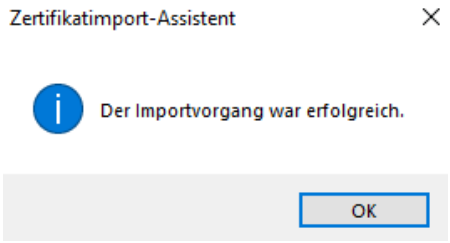


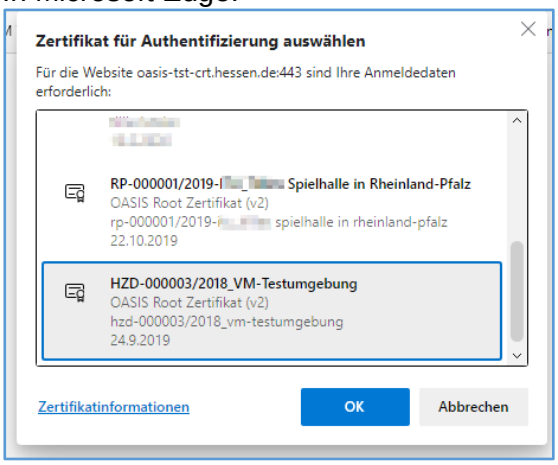
Abbildung 21: Abschluss des Imports

Herzlichen Glückwunsch. Sie haben die Zertifikate erfolgreich installiert.

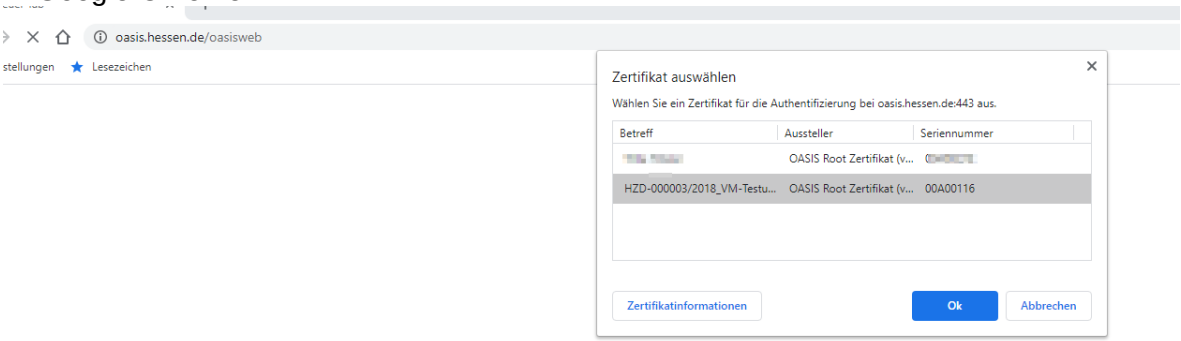
4.3.3 Aufrufen von OASIS WEB in Microsoft Edge und Google Chrome

Rufen Sie über die URL https://oasis.hessen.de/oasisweb OASIS auf und wählen Sie das Client-Zertifikat aus.

In Microsoft Edge:

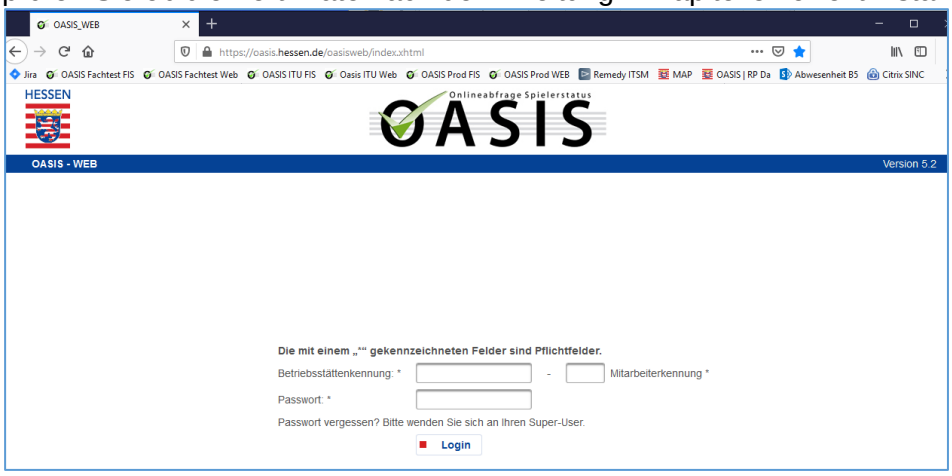


In Google Chrome:



Danach wird eine Passwort-Eingabeanforderungsmaske erscheinen. Hier soll das Passwort für das Zertifikat eingegeben werden.

Nun sollte, wenn alles stimmt, die Anmeldemaske von OASIS-WEB erscheinen. Wenn nicht, prüfen Sie ob die Zertifikate nach der Anleitung in Kapitel 5 korrekt installiert sind.



4.4 Installation der Zertifikate für Mozilla Firefox

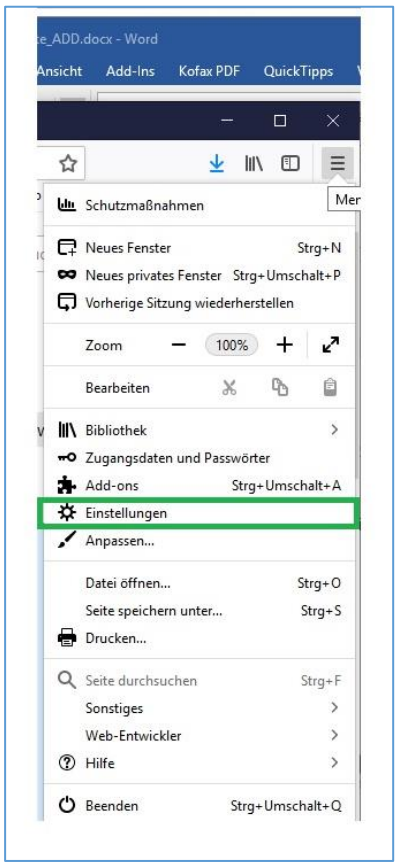
Diese Anleitung ist gültig für Firefox Version 78.10.0esr. Andere Versionen können davon abweichen.
Die Installation der Zertifikate, die in Kapitel 4.3 Installation der Zertifikate für Microsoft Edge und Google Chrome beschrieben ist, gilt nicht für Firefox. Die Zertifikate müssen direkt in Firefox importiert werden.

Voraussetzungen:

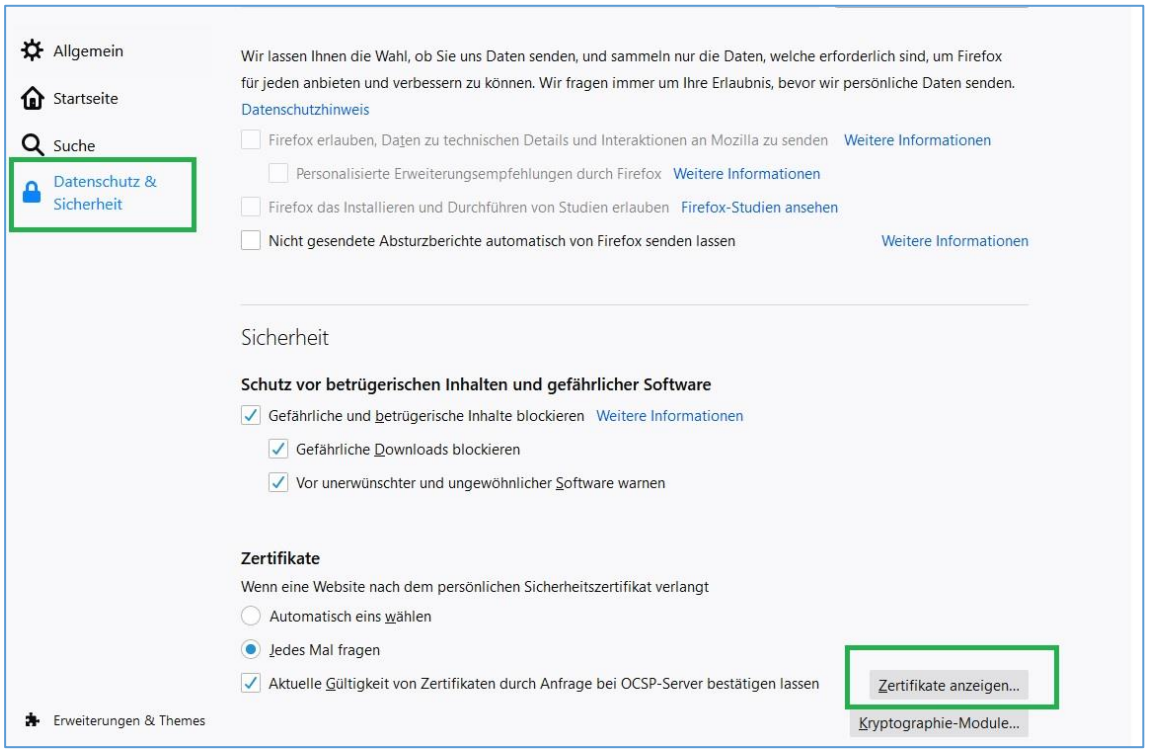
- Die Datei mit dem Zertifikat liegt Ihnen lokal vor.
- Das Zertifikatspasswort, das Sie entweder direkt vom OASIS Team per Post, oder von der OASIS Hotline nach korrekter Beantwortung der 3 Sicherheitsfragen erhalten haben, liegt vor.

Klicken Sie im Firefox oben ganz rechts auf die drei Linien:

Klicken auf *Einstellungen*:

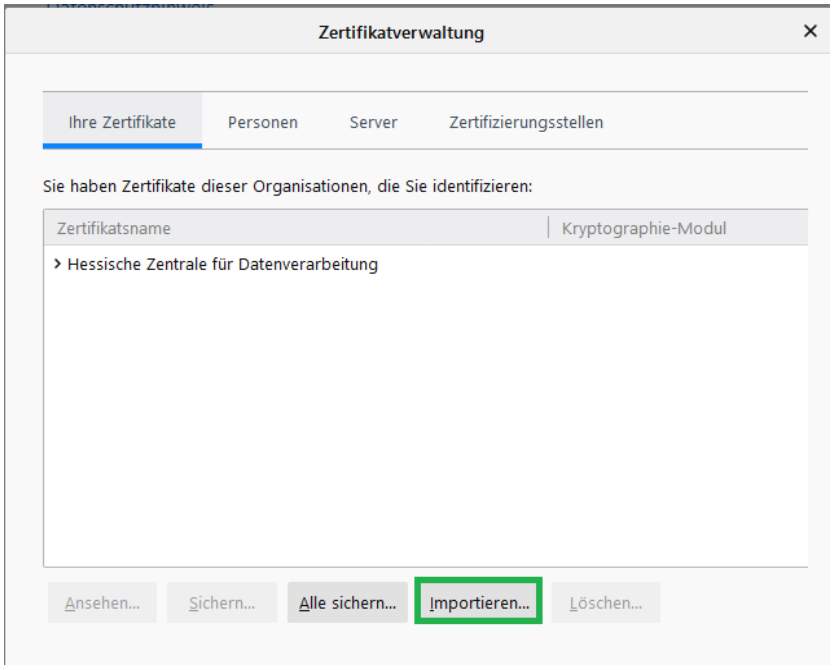


Klicken auf *Datenschutz* und dann auf den Button „Zertifikate anzeigen“:



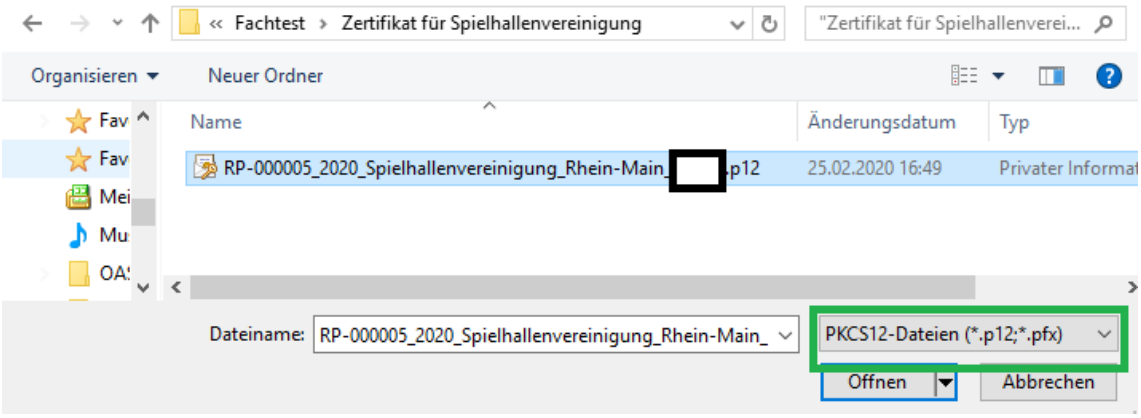
4.4.1 Installation des personalisierten Zertifikats

Unter dem Reiter *Ihre Zertifikate* können Sie die installierten Zertifikate sehen:

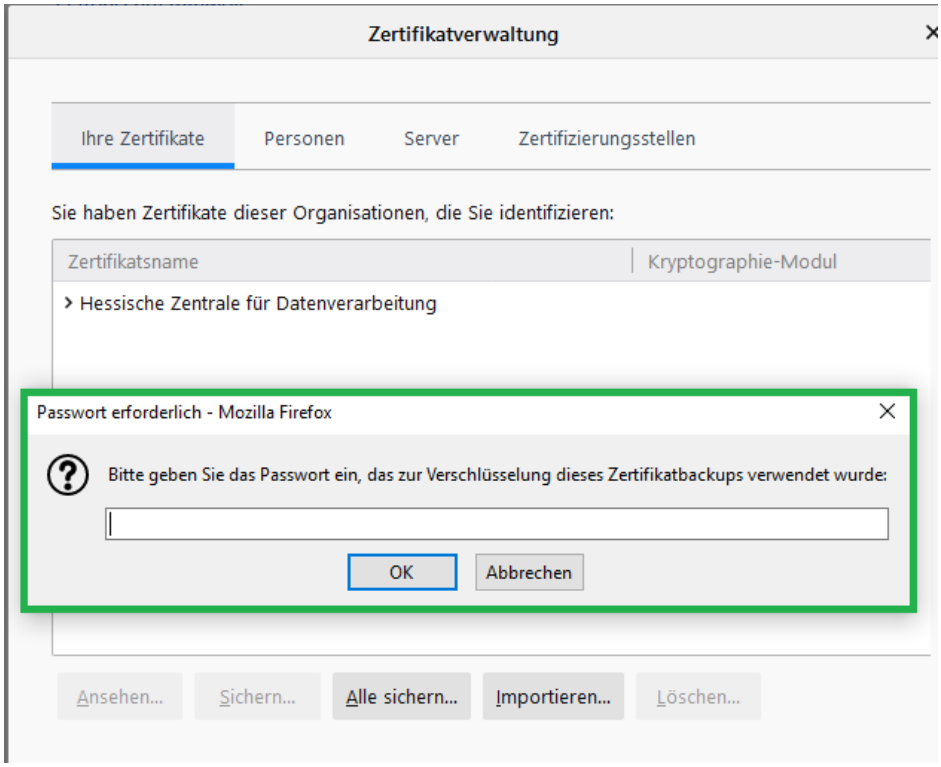


Klicken Sie auf „Importieren“.

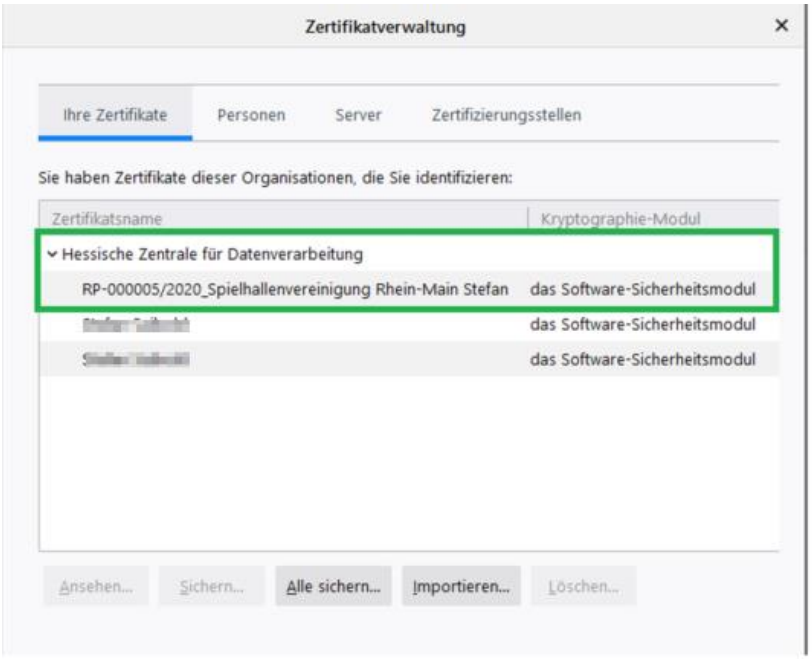
Wählen Sie das Zertifikat mit der Endung .p12 und am Anfang mit der Veranstalternummer aus, und öffnen Sie es.



Das Fenster mit der Abfrage nach dem Passwort geht auf. Bitte geben Sie das Zertifikatpasswort ein.

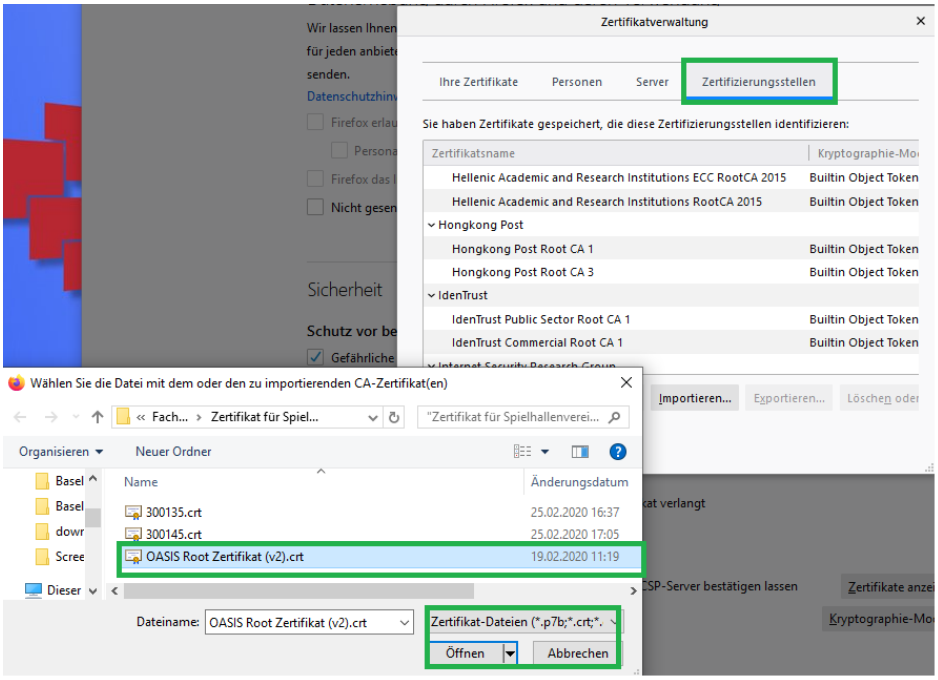


Bei korrekt eingegebenem Passwort wird das Zertifikat importiert und angezeigt:

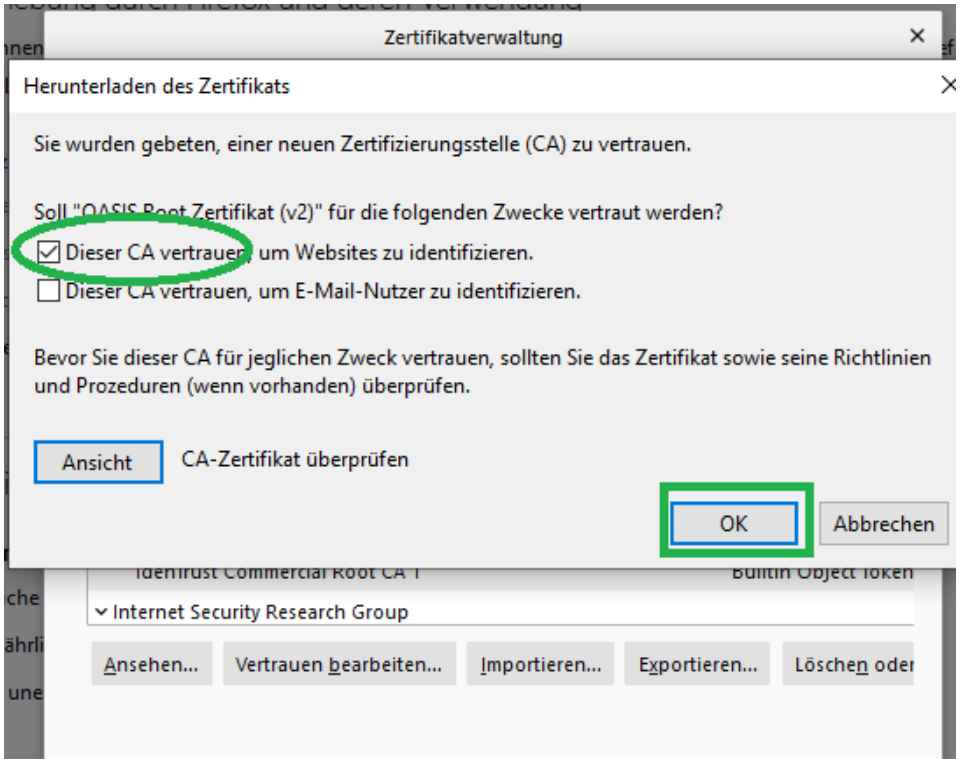


4.4.2 Installation des OASIS Root-Zertifikats

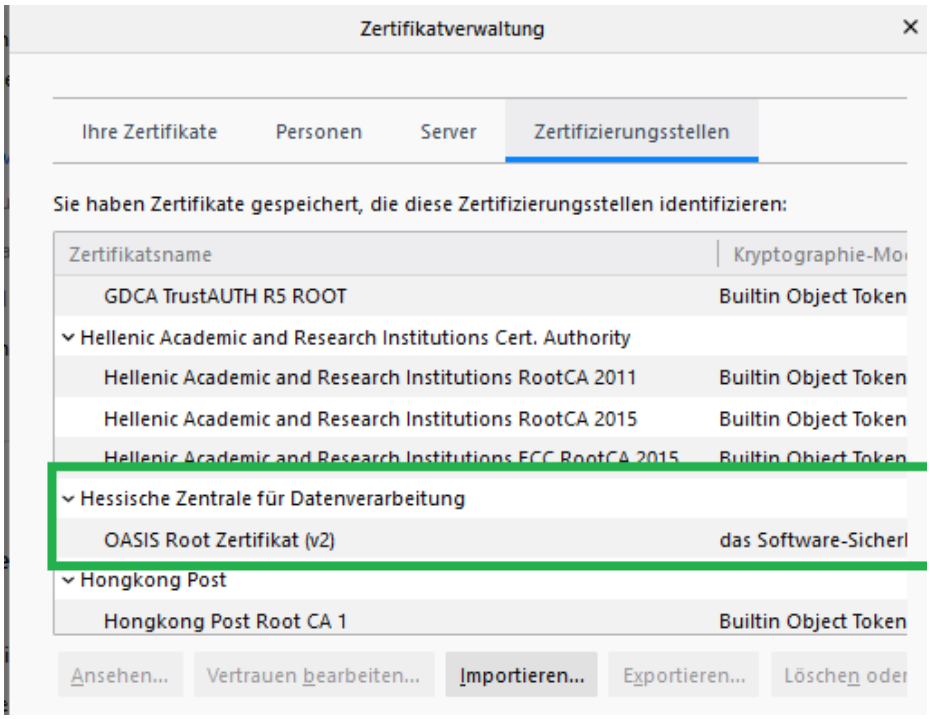
Auf den Reiter *Zertifizierungsstellen* klicken, *Importieren* klicken, das *Oasis Root Zertifikat* im Dateibrowser auswählen und anklicken, öffnen klicken:



Dieser CA vertrauen klicken:



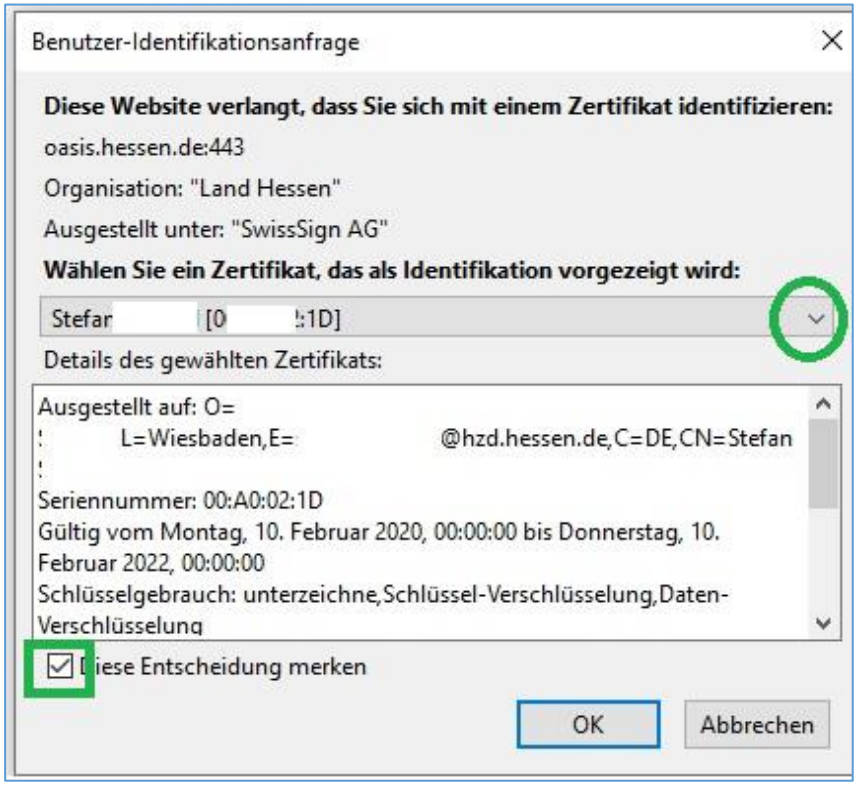
Das Zertifikat sollte nun angezeigt werden:



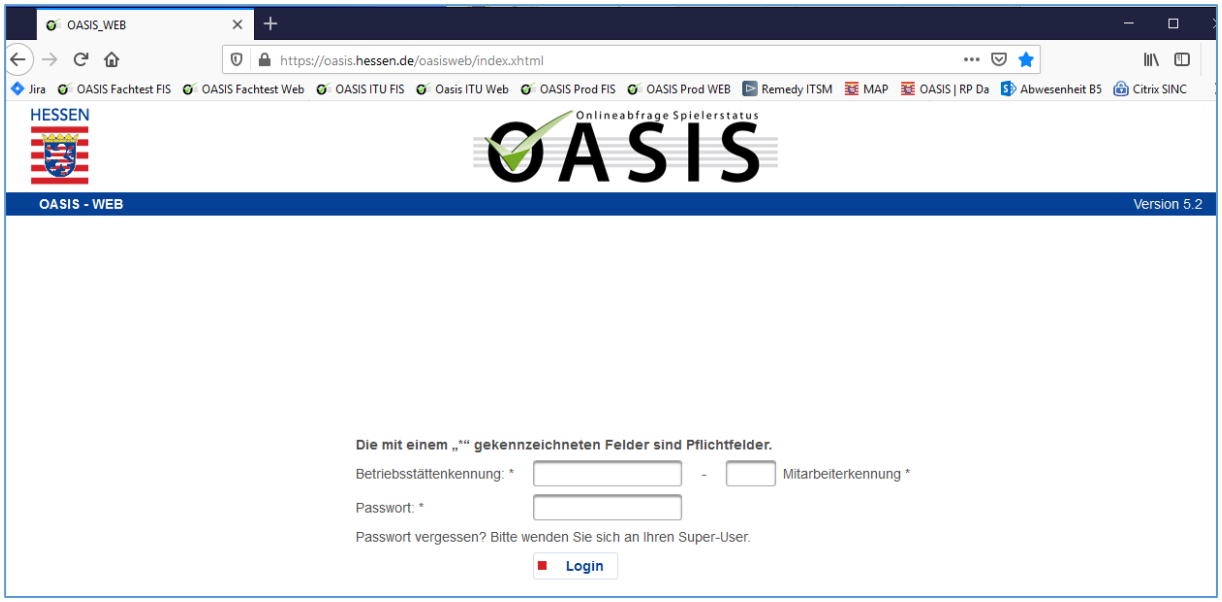
Durch Doppelklick auf das Zertifikat können die Details eingesehen werden.

4.4.3 Aufrufen von OASIS WEB im Mozilla Firefox

Rufen Sie über die URL https://oasis.hessen.de/oasisweb OASIS auf und wählen Sie das Client-Zertifikat aus.
Mit dem Drop Down Menü rechts suchen Sie das Zertifikat, das unter Ihrer Veranstalternummer abgespeichert wurde aus und haken das Kästchen *„Diese Entscheidung merken“* an und bestätigen mit *„OK“*.



Nun sollte, wenn alles stimmt, die Anmeldemaske von OASIS-WEB erscheinen. Wenn nicht, prüfen Sie, ob die Zertifikate nach der Anleitung in Kapitel 5 korrekt installiert sind.



5 Prüfen, ob die OASIS Zertifikate korrekt installiert sind

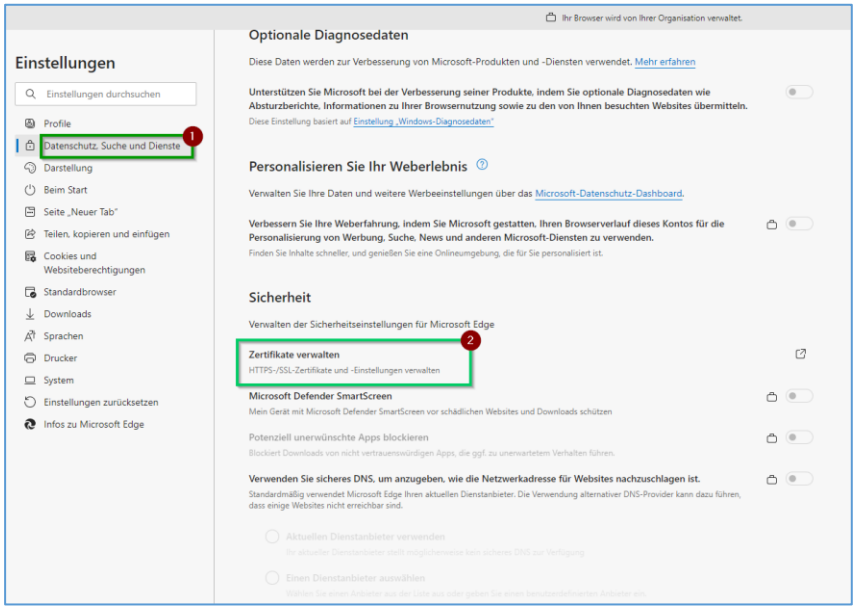
Falls Sie Probleme mit der Verbindung zu OASIS haben, z.B. ‚Die Seite kann nicht angezeigt werden', ‚Diese Webseite kann keine sichere Verbindung bereitstellen', oder ‚Fehler: Gesicherte Verbindung fehlgeschlagen', sollten Sie prüfen, ob die Zertifikate korrekt installiert sind. In den folgenden Unterkapiteln finden Sie die Anleitungen wie Sie prüfen können, ob die Zertifikate korrekt installiert sind. Die Beschreibungen gelten nur für die jeweils angegebene Programmversion. Andere Versionen können abweichen.

5.1 Zertifikate im Microsoft Edge prüfen

Anleitung gültig für Edge Version 90.0.818.56. Andere Versionen können davon abweichen.

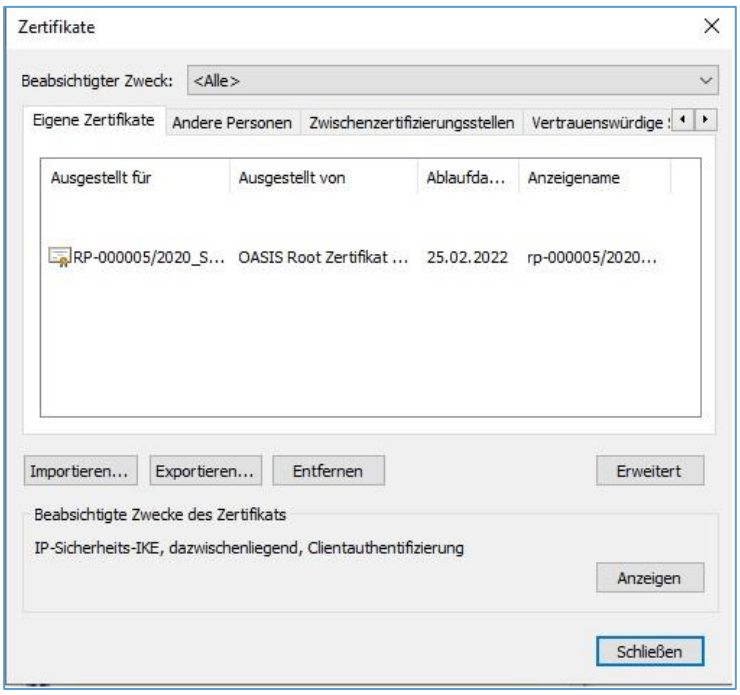
Oben rechts auf den drei Punkten klicken:

„Datenschutz, Suche und Dienste" selektieren, im rechten Menü bis zum ‚Sicherheit' herunterscrollen und ‚Zertifikate verwalten' wählen.



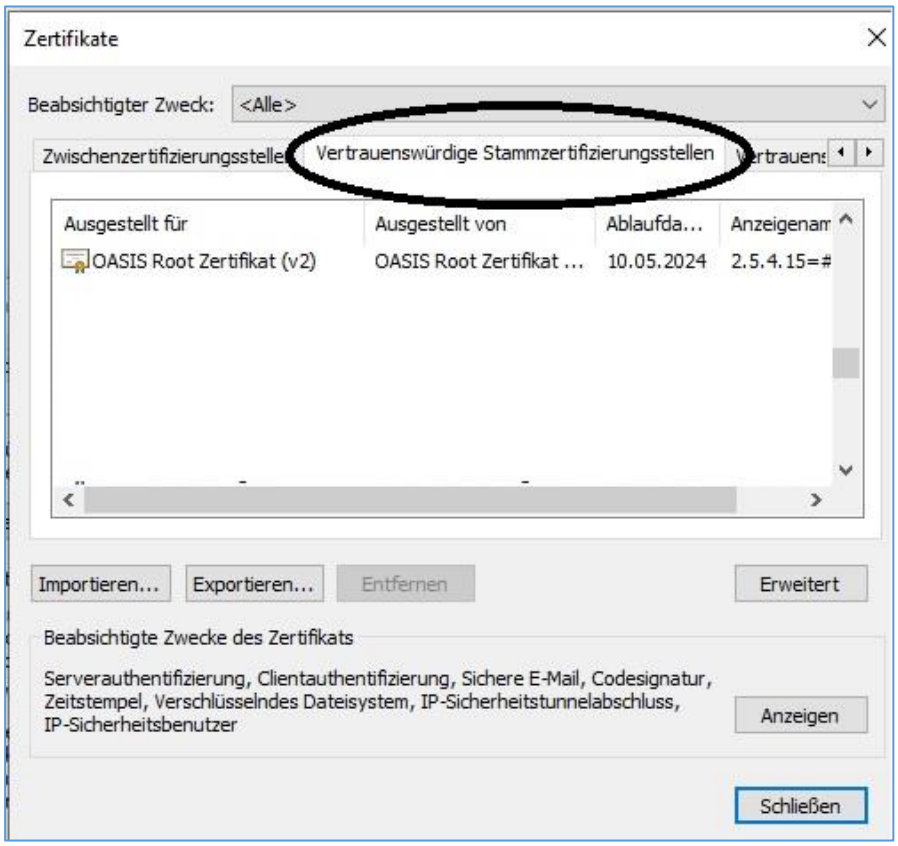
5.1.1 Zertifikate anzeigen

Hier sehen Sie die Angaben zu dem importierten personalisierten Zertifikat mit Angabe des Namens des Zertifikats unter dem Reiter „*Eigene Zertifikate“*.
Die Details zum Zertifikat können Sie über den Button „Anzeigen“ ansehen.



Sollte das personalisierte Zertifikat fehlen können Sie es hier mit Button „Importieren“ installieren.

Unter dem Reiter *Vertrauenswürdige Stammzertifizierungsstellen* ist das importierte Root-Zertifikat von OASIS zu finden.
Die Details zum Zertifikat können Sie über den Button „Anzeigen“ ansehen.



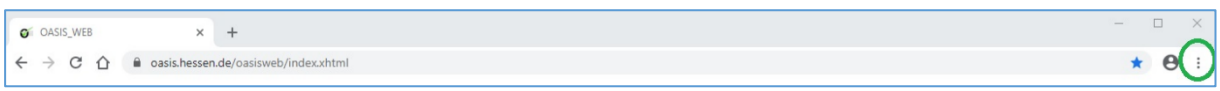
Sollte das Root-Zertifikat fehlen können Sie es hier mit dem Button „Importieren“ installieren.

Wenn diese beiden Zertifikate vorhanden sind und das korrekte Passwort für das Zertifikat beim Aufruf von OASIS eingegeben wurde, sollte der Zugriff auf OASIS funktionieren.

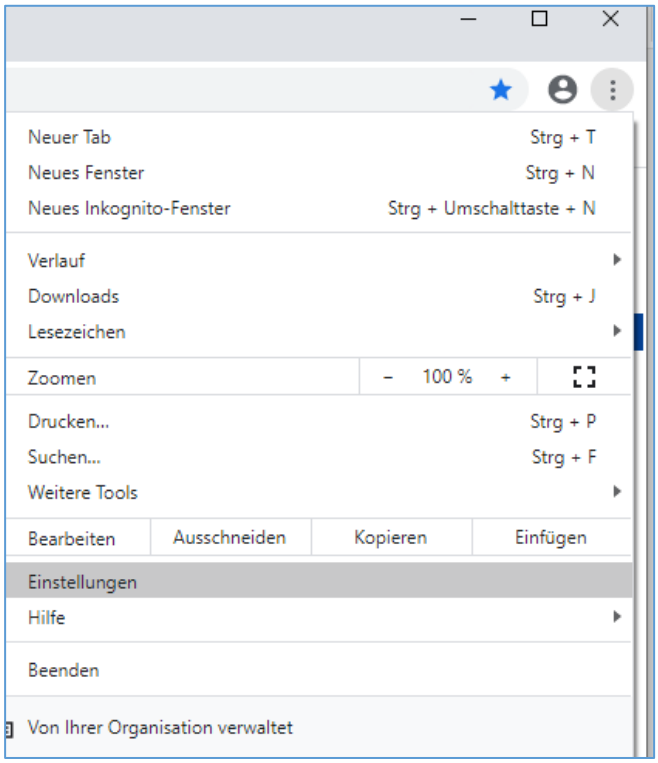
5.2 Zertifikate im Google Chrome prüfen

Diese Anleitung ist gültig für Google Chrome in den aktuellen Versionen. Erstellt wurde die Anleitung mit Version 90.0.4430.85 (Offizieller Build) (32-Bit). Andere Versionen können davon abweichen.

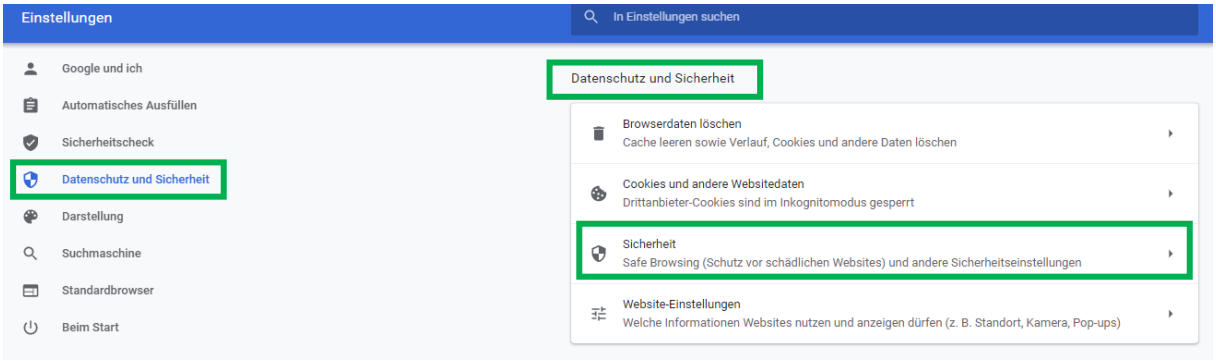
Klicken Sie im Chrome oben ganz rechts auf die drei Punkte:



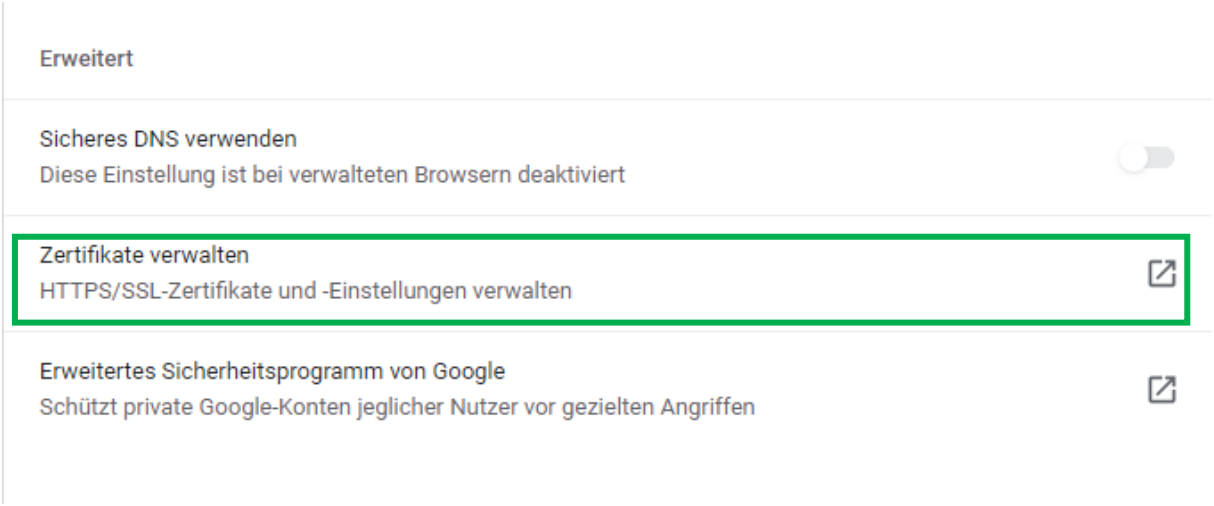
Klicken Sie in dem Menü auf „Einstellungen“:



Klicken Sie auf „Datenschutz und Sicherheit“ links, dann auf der rechten Seite auf „Sicherheit“:



Klicken Sie auf „Zertifikate verwalten“ weiter unten auf der Seite:



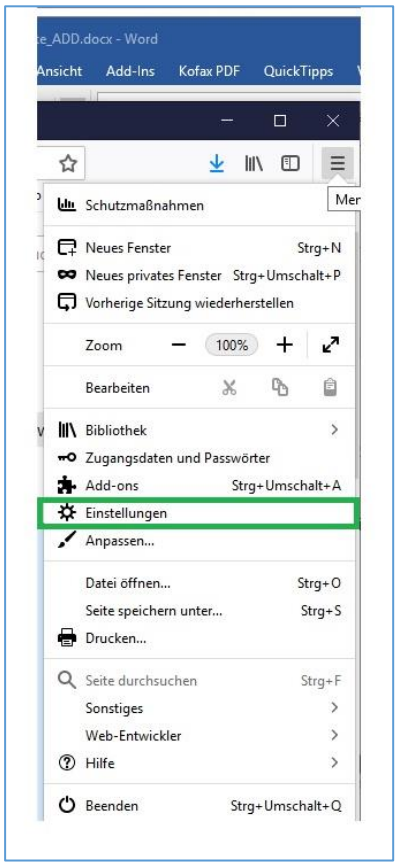
Hier geht es nun genauso weiter wie mit dem Microsoft Edge. Siehe Beschreibung unter 5.1.1 Zertifikate anzeigen.

5.3 Zertifikate im Mozilla Firefox prüfen

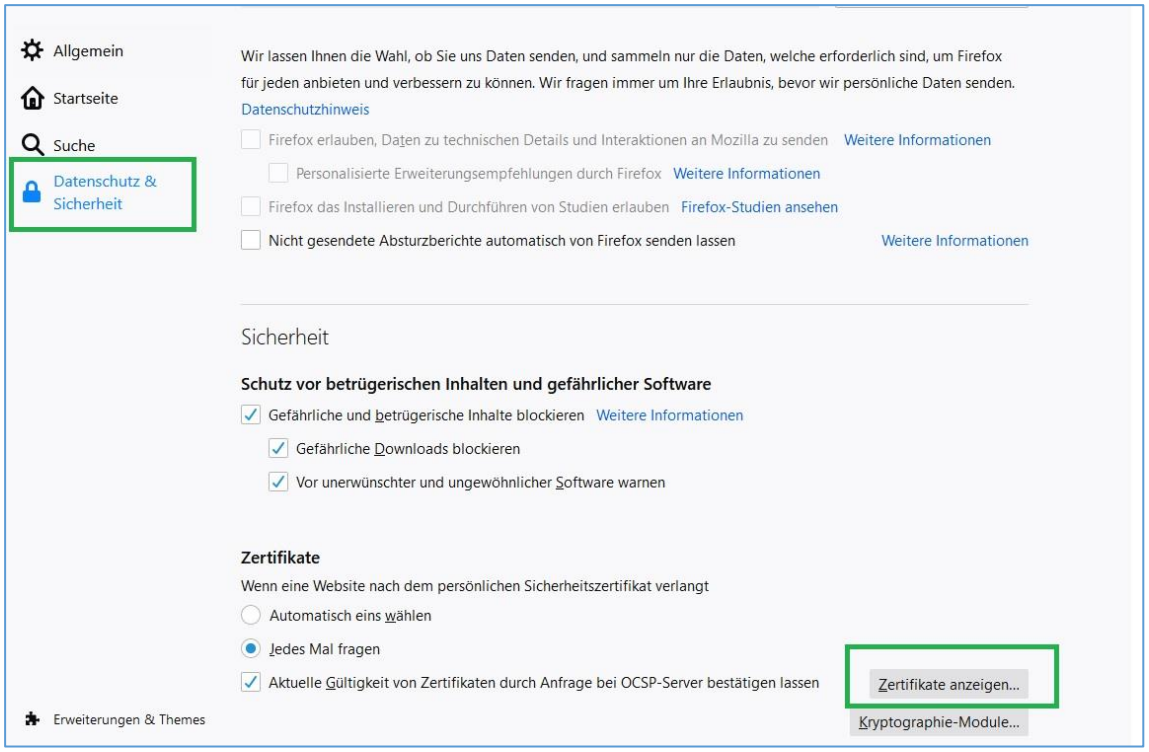
Diese Anleitung ist gültig für Mozilla Firefox in den aktuellen Versionen. Erstellt wurde die Anleitung mit Version 78.10.0esr. Andere Versionen können davon abweichen.

Klicken Sie im Firefox oben ganz rechts auf die drei Linien:

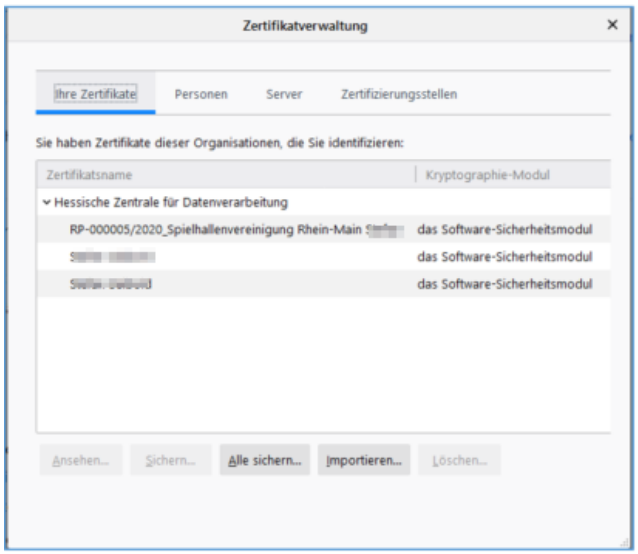
Klicken auf „Einstellungen“:



Klicken auf „Datenschutz & Sicherheit“ und dann auf den Button „Zertifikate anzeigen“ weiter unten auf der Seite:

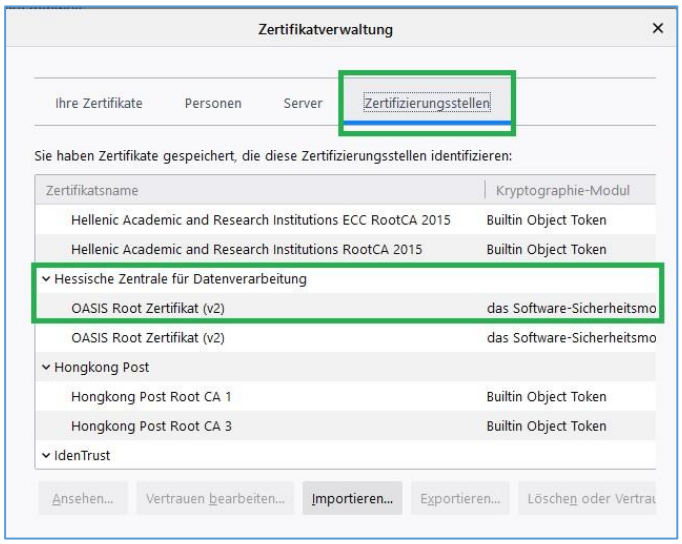


Unter dem Reiter „*Ihre Zertifikate*“ können Sie nun Ihr Zertifikat für OASIS mit Angabe des Namens des Zertifikats sehen:



Durch Doppelklick auf das Zertifikat können die Details eingesehen werden.
Sollte das personalisierten Zertifikat fehlen können Sie es hier mit Button „Importieren“ installieren.

Im demselben Menü wird unter „Zertifizierungsstellen“ das importierte Root-Zertifikat für OASIS angezeigt:



Durch Doppelklick auf das Zertifikat können die Details eingesehen werden.
Sollte das Root-Zertifikat fehlen können Sie es hier mit Button „Importieren“ installieren.

Wenn diese beiden Zertifikate vorhanden sind und das korrekte Passwort für das Zertifikat beim Aufruf von OASIS eingegeben wurde, sollte der Zugriff auf OASIS funktionieren.

6 FAQ - Häufig gestellte Fragen

6.1 Kann ich das Zertifikat mehrmals installieren?

Ja, das ist problemlos möglich.

6.2 Ich habe mein Passwort für das Zertifikat nicht mehr

Das für die Zertifikatsinstallation erforderliche Passwort erfragen Sie bitte telefonisch bei der OASIS-Hotline. Halten Sie hierfür Ihre Vertragsnummer und die Antworten zu den drei Sicherheitsfragen bereit.

6.3 Mein Rechner kann keine Verbindung mit OASIS aufbauen

Falls Sie die Probleme mit der Verbindung zu OASIS haben, z.B. ‚Die Seite kann nicht angezeigt werden‘, ‚Diese Webseite kann keine sichere Verbindung bereitstellen‘, oder ‚Fehler: Gesicherte Verbindung fehlgeschlagen‘, sollten Sie prüfen, ob die Zertifikate korrekt installiert sind. Siehe Anleitung in Kapitel 5.

Falls die Zertifikate korrekt installiert sind und OASIS WEB nicht abgerufen werden kann, löschen Sie die Cookies und den Cache im Browser, und drücken Sie die ‚F5' Taste um die Webseite neu zu laden.

6.4 Mein OASIS Zertifikat läuft bald ab. Wie kann ich es verlängern?

Das personalisierte Zertifikat hat eine Laufzeit von 2 Jahren. Ein neues Zertifikat wird ca. 1 Monat vor dem Ablauf automatisch generiert und an die E-Mailadresse(n) versendet, die Sie in Ihrem Vertrag angegebenen haben.

6.5 Ich habe ein Ersatz-Zertifikat bekommen. Muss ich das mitgelieferte Root-Zertifikat auch installieren?

Ja, Sie sollten vorsichtshalber immer das mitgelieferte Root-Zertifikat installieren, um sicherzustellen, dass das korrekte Root-Zertifikat auf Ihrem Rechner installiert ist. Das Root-Zertifikat wird auch ab und zu aktualisiert und getauscht.

6.6 Mein Rechner wurde gestohlen. Was soll ich tun?

Sie sollten die OASIS Hotline über den Verlust so schnell wie möglich informieren, sodass das Client-Zertifikat gesperrt werden kann. Halten Sie hierfür Ihre Vertragsnummer und die Antworten zu den drei Sicherheitsfragen bereit. Die Hotline kann auch ein neues Zertifikat für Sie ausstellen.

Zu beachten ist, Sie müssen das alte Zertifikat auf allen Rechnern, wo es installiert ist, durch das neue Zertifikat ersetzen.

7 Anlage Kontaktinformation

Die OASIS WEB Anwenderanleitung kann in dem hier angegebenen Link heruntergeladen werden.

Ansprechpartner: Regierungspräsidium Darmstadt
E-Mail: oasis@rpda.hessen.de
Webseite: https://rp-darmstadt.hessen.de/sicherheit/gl%C3%BCcksspiel/spielersperrshysystem-oasis/gl%C3%BCcksspielstaatsvertrag

7.1 OASIS Hotline rund um die Uhr

Telefon: +49 (6652) 187 2212
E-Mail: IT-Service-Desk@hzd.hessen.de