STAATSMINISTERIUM
DES INNERN

Freistaat
SACHSEN

Handlungsanleitung zur Beantragung von Serverzertifikaten für HTTPS-Seiten und -dienste der Landesverwaltung Sachsen unter **Microsoft IIS**

Handlungsanleitung zur Beantragung von Serverzertifikaten
für HTTPS-Seiten und -dienste der Landesverwaltung Sachsen
unter Microsoft IIS

Dokumentenkontrolle:

Versionskontrolle:

Version	Datum	Kommentar
V1.0	17.07.2014	Erarbeitung durch Kernteam Verschlüsselung der AG IS
V2.0	12.12.2014	Aktualisierte und überarbeitete Fassung zur Veröffentlichung

Inhaltsverzeichnis

1. Grundlagen

Der Freistaat Sachsen betreibt seit 2009 in Kooperation mit dem Verein zur Förderung eines Deutschen Forschungsnetzes (DFN-Verein) eine Ausgabestelle für Serverzertifikate. Mit Hilfe dieser sogenannten »Sachsen Global CA« können alle Behörden des Freistaats Sachsen ihre Internetangebote ohne zusätzliche Kosten so absichern, dass die Daten während der Übertragung zum Nutzer nicht von Dritten gelesen oder verändert werden können. Zusätzlich können die Nutzer auf diesem Weg jederzeit prüfen, ob die Internetangebote tatsächlich vom Freistaat Sachsen bereitgestellt wurden.

In einem ressortübergreifenden Sicherheitstest Anfang des Jahres 2014 wurde festgestellt, dass auf vielen mit HTTPS abgesicherten Internetseiten der Landesverwaltung Zertifikatsfehler vorliegen, die sich durch eine korrekte Zertifikatsbeantragung und -konfiguration einfach beseitigen lassen würden. Einen Eindruck des aktuellen Standes für Ihre Webseite können Sie über den kostenlosen SSL-Servertest der Firma Qualys unter *https://www.ssllabs.com/ssltest* (Häkchen bei Option »Do not show the results on the boards« nicht vergessen) gewinnen.

Zeigt darüber hinaus ein HTTPS-Aufruf Ihrer Webseite unter verschiedenen Browsern Zertifikatsfehler an, sollten Sie Ihr Serverzertifikat wie in dieser Handlungsanleitung dargestellt neu beantragen und neu konfigurieren. Die kostenfreie Beantragung der Serverzertifikate über die Sachsen Global CA erfolgt über den Staatsbetrieb Sächsische Informatikdienste (SID) auf dem im Folgenden beschriebenen Weg.

Wichtig: es können nur für solche Domains (Seitennamen) Zertifikate über die Sachsen Global CA beantragt werden, die einer Behörde des Freistaats Sachsen gehören. Der Domaininhaber (Admin-C, z. B. über DENIC.de feststellbar) muss diese Zugehörigkeit deutlich erkennen lassen. Das gilt auch für bei externen Dritten betriebene Domains.

Für Fragen zum Prozess können Sie sich per E-Mail an das Zertifikatsmanagement-Team unter der Adresse *SachsenGlobalCaZm@sid.sachsen.de* wenden. Allgemeine Fragen zu Zertifikaten und Zertifikatsanträgen beantwortet die ausführliche FAQ-Seite der DFN-PKI unter *https://www.pki.dfn.de/index.php?id=faqpki-allgemein*.

2. Technische und organisatorische Umsetzung in Sachsen

2.1. Vorbereitung eines Zertifikatsantrags

Vor Beantragung eines HTTPS-Serverzertifikats über die Sachsen Global CA müssen Sie lokal eine Zertifikatsantragsdatei (Format PKCS#10) erstellen, die die notwendigen Angaben zu Ihrem Webserver enthält.

Folgende Richtlinien müssen Sie bei der Erstellung einhalten (die Einhaltung wird geprüft):

- der Name im PKCS#10-Zertifikatsantrag muss enden auf:
  O=Freistaat Sachsen, L=Dresden, ST=Sachsen, C=DE
- der Schlüssel muss 2048 Bit lang sein
- der Zertifikatname darf keine Umlaute und andere Sonderzeichen enthalten.
  Erlaubt sind a-z, A-Z, 0-9, (,), :, ., -, Komma und Leerzeichen.
  Insbesondere bei dem Wort »Sächsisch« ist dies zu beachten
  (»Saechsisch« verwenden).

Zur Erstellung einer Zertifikatsantragsdatei direkt aus Microsoft IIS (Version 2008) heraus öffnen Sie den IIS-Manager. Auf der Startseitenansicht der Webseite können Sie unter dem Punkt »Serverzertifikate« den Prozess zur Erzeugung eines Zertifikatsantrags starten.

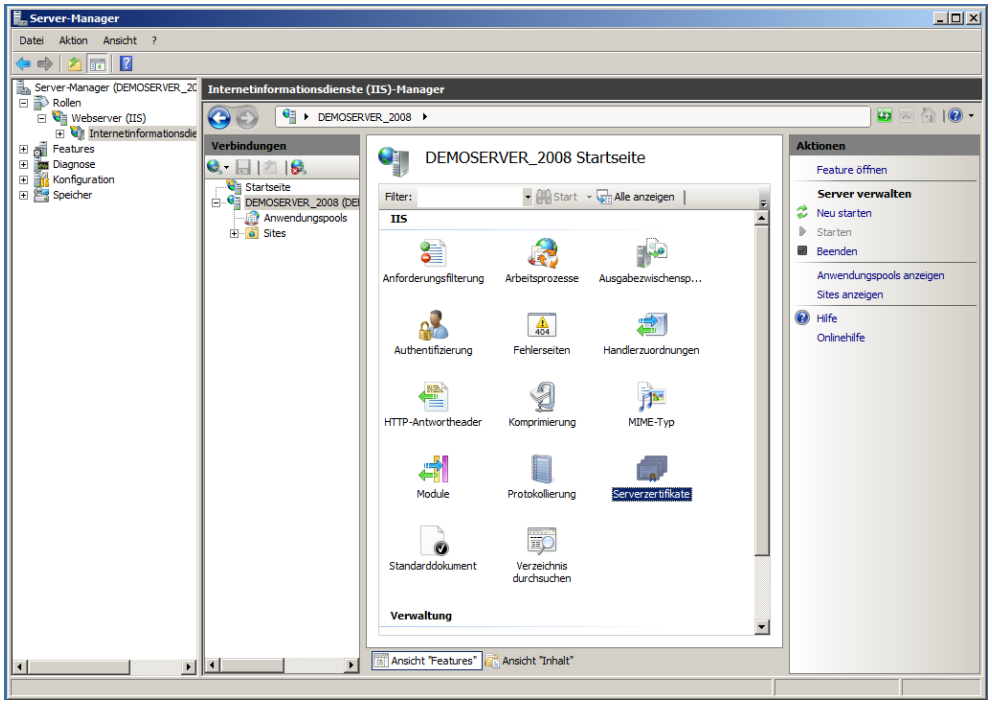


Abbildung 1: Startseitenansicht einer Webseite im Microsoft IIS-Manager

Wählen Sie in der Ansicht »Serverzertifikate« oben rechts die Aktion »Zertifikatanforderung erstellen« aus.

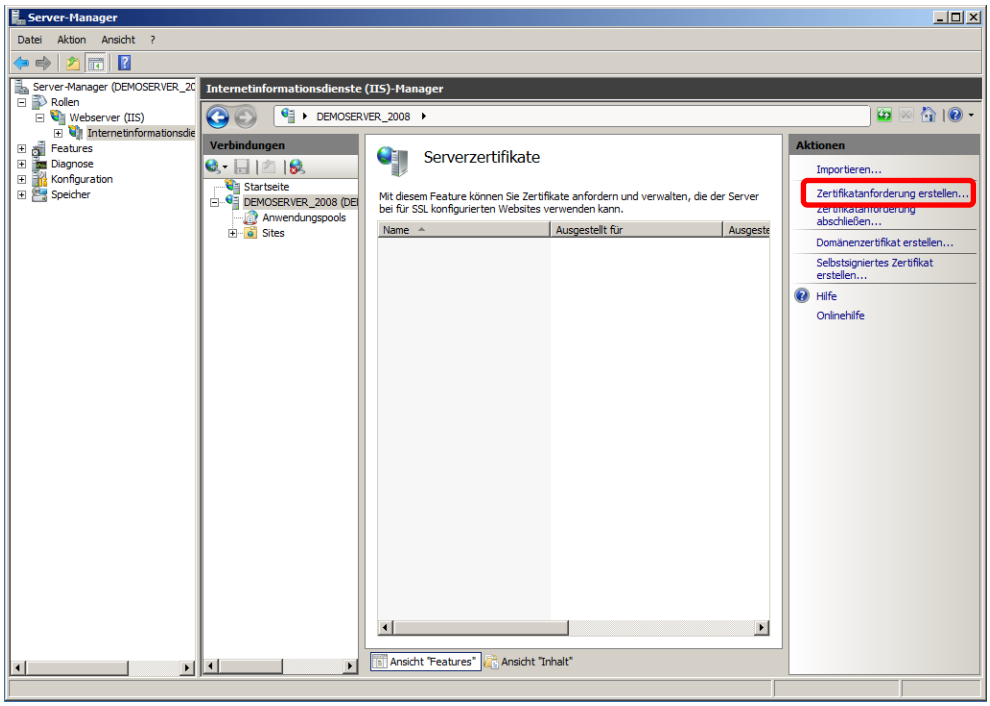


Abbildung 2: Zertifikatanforderung erstellen

Im nächsten Schritt muss der vollqualifizierte DNS-Hostname des Rechners, von dem das Zertifikat später verwendet werden soll, eingegeben werden (Gemeinsamer Name, Common Name, CN, z. B. »beispiel.sachsen.de«). **Anträge für Domänen außerhalb von sachsen.de sind möglich, erfordern aber eine vorherige Klärung mit dem Zertifikatsmanagement.**

Dazu ist folgender Prozess einzuhalten: Die DFN PKI benötigt zur Freischaltung neuer Domains (z. B. beispiel-sachsen.de) ein Autorisierungsschreiben des Domaininhabers (Admin-C). Der Domaininhaber ist z. B. über DENIC.de abfragbar. Die folgende Vorlage kann hierzu verwendet werden:

> Sehr geehrte Damen und Herren,
>
> hiermit gewähren wir dem Freistaat Sachsen das Recht, im Rahmen der DFN-PKI beliebige Zertifikate für die folgende Domain zu erhalten: <beispiel-sachsen.de>
>
> <Unterschrift: zeichnungsberechtigter Domaininhaber/Admin-C>

Senden Sie dieses Schreiben per Brief an:

> DFN-CERT Services GmbH
>
> DFN-PCA
>
> Sachsenstrasse 5
>
> 20097 Hamburg

und in Kopie an die SachsenGlobalCA:

Staatsbetrieb Sächsische Informatik Dienste
Fachbereich 3.1 | E-Government- und Querschnittverfahren
Zertifizierungsstelle SachsenGlobalCA
Riesaer Str. 7 | 01129 Dresden

Die Freischaltung erfolgt nach erfolgreicher Prüfung durch die DFN-PKI in der Regel innerhalb einer Woche. Ob die Freischaltung erfolgt ist, können Sie über die Beantragungsseite für Serverzertifikate unter dem Link: *»Die folgenden Domainnamen können Sie in Servernamen nutzen:>>«* abfragen.

Als Organisationsname (Organization, O) muss »Freistaat Sachsen« eingegeben werden. Der Behördenname (Organizational Unit, OU) ist im Prinzip frei wählbar, muss aber die beantragende Behörde klar erkennen lassen. Beachten Sie bitte, dass keine Sonderzeichen wie z. B. der Umlaut »ä« zulässig sind (hier z. B. »Saechsisch« verwenden). Wie schon der Organisationsname »Freistaat Sachsen« sind auch die geografischen Angaben zum Standort der CA, d. h. Land (Country, C, »DE«), Bundesland (State, ST, »Sachsen«) und Ort (Locality, L, »Dresden«) fest vorgegeben. Andere Angaben oder das Weglassen von Einträgen sind bei allen diesen Feldern nicht zulässig.

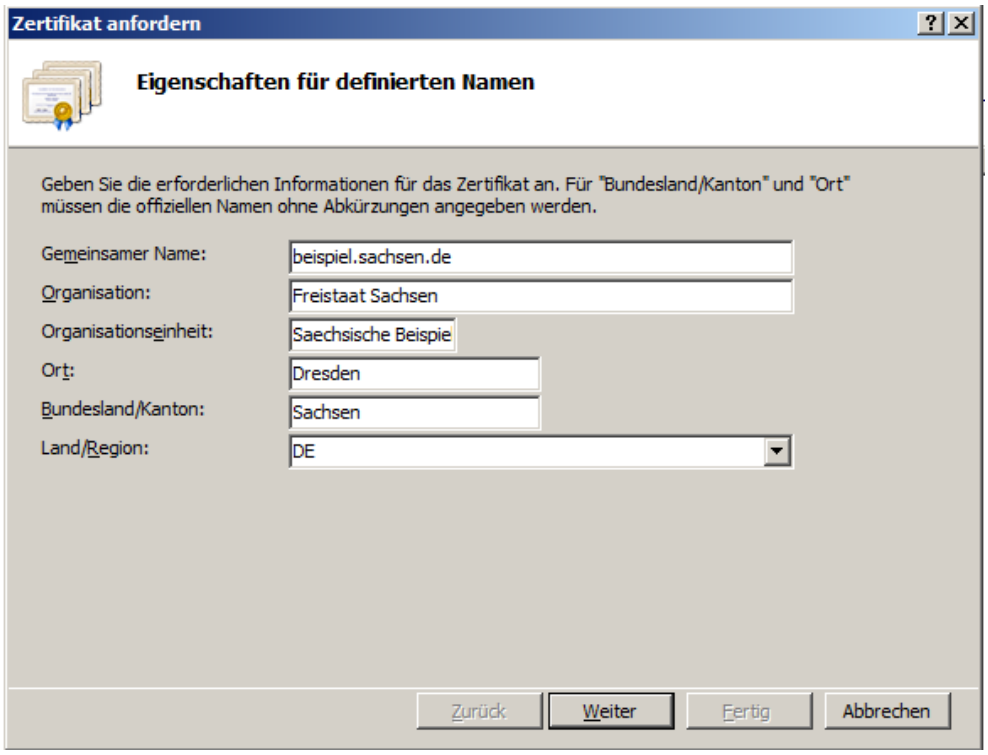


Abbildung 3: Eingabe der Zertifikatsinformationen

Im nächsten Fenster **wählen Sie bitte eine Schlüssellänge von 2048 Bit.** Der angegebene Kryptografiedienstanbieter sollte unverändert gelassen werden.

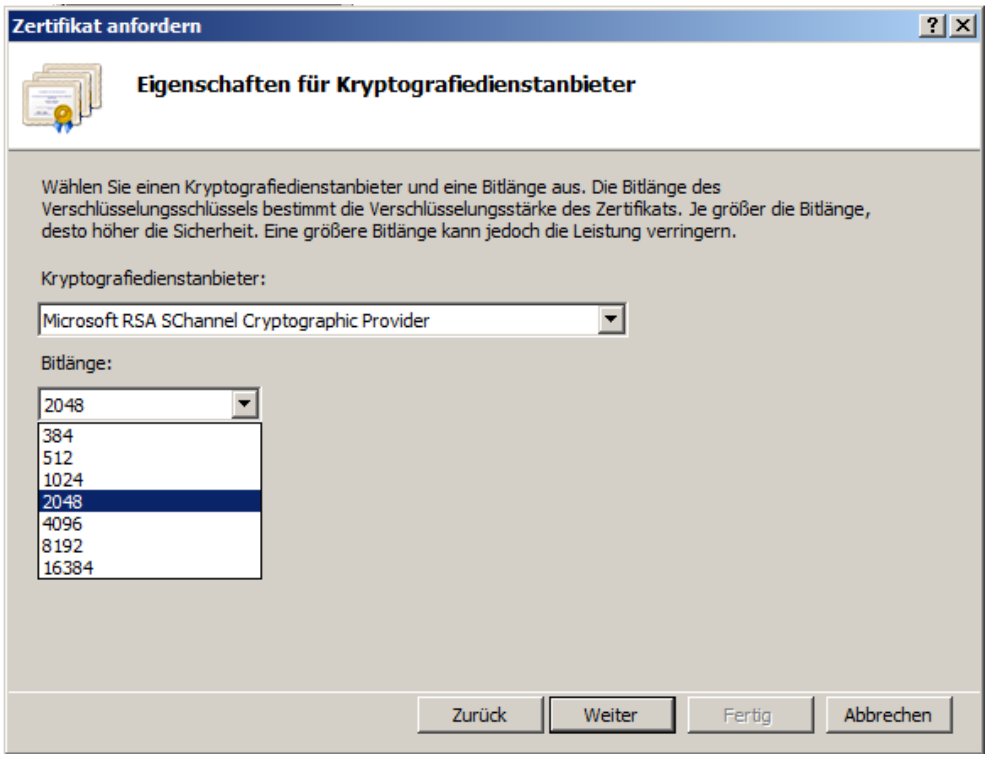


Abbildung 4: Schlüssellänge

Im nächsten Schritt wird der Name der Datei abgefragt, in der der Zertifikatantrag gespeichert werden soll. Geben Sie einen geeigneten Namen ein und klicken Sie auf Fertig.

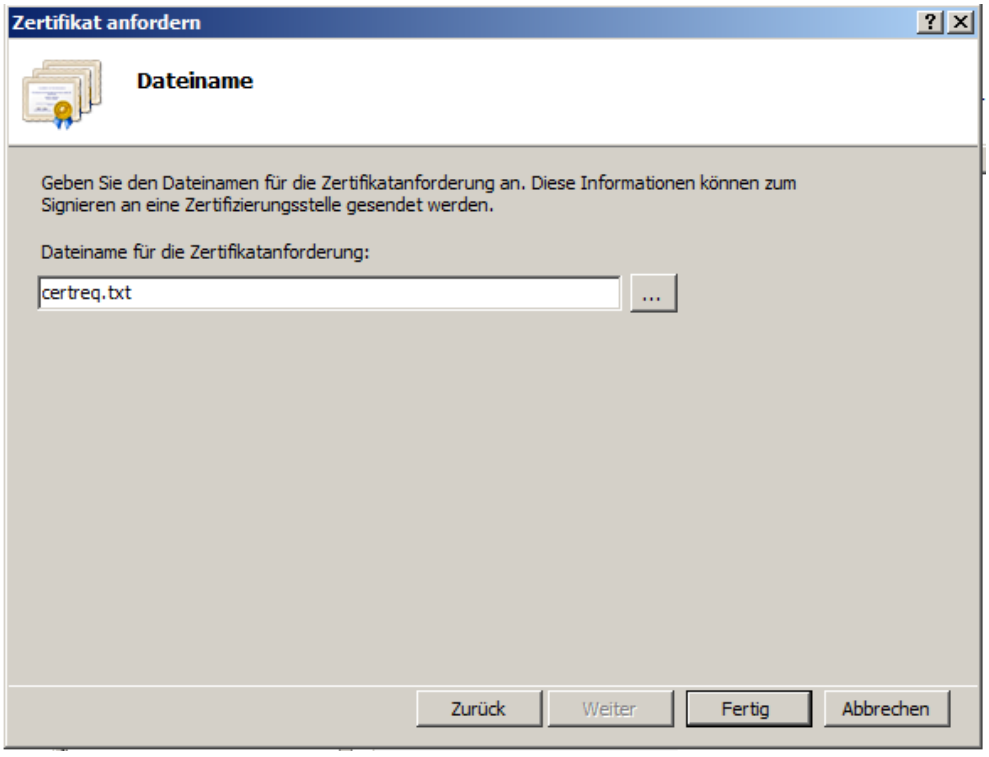


Abbildung 5: Dateiname zur Speicherung des Zertifikatantrags

Die Zertifikatsantragsdatei im PKCS#10-Format liegt nun vor.

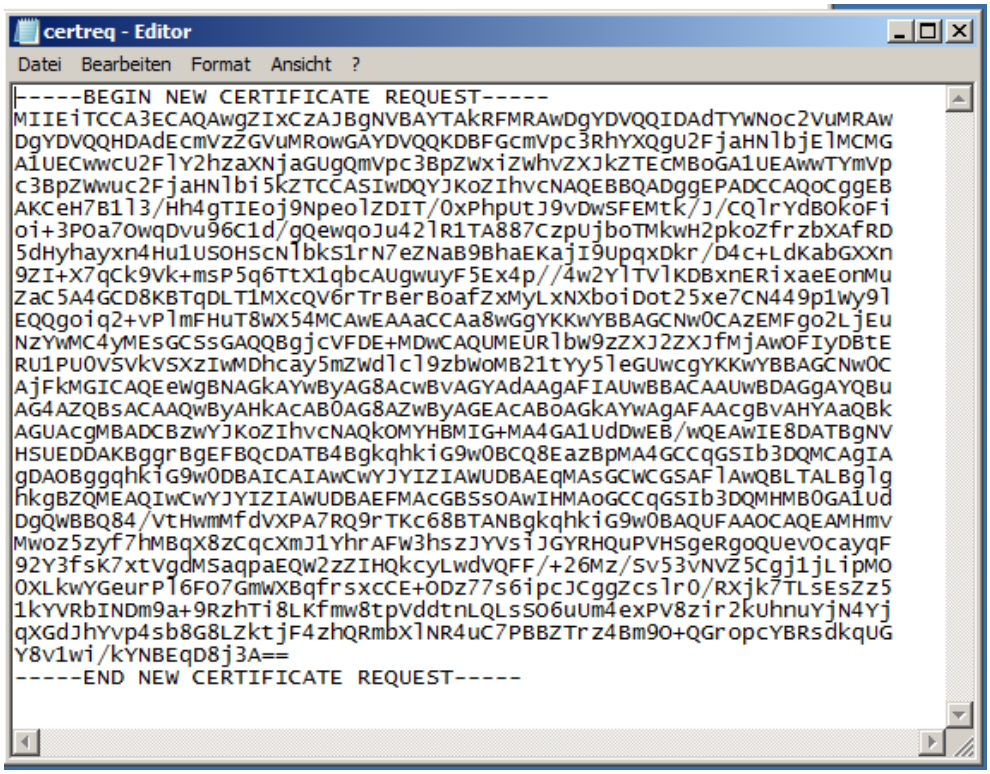


Abbildung 6: Zertifikatsantrag im PKCS#10-Format

Alternativ können Sie den Zertifikatsrequest auch über die Kommandozeile erstellen. Hierfür muss zunächst eine Textdatei mit folgendem Inhalt erstellt werden:

```
[NewRequest]
Exportable      = TRUE
KeyLength       = 2048
MachineKeySet   = TRUE
Subject         = "CN=<FQDN>,OU=<Behoerdenname>,O=Freistaat Sachsen,
L=Dresden,ST=Sachsen,C=DE"
RequestType     = PKCS10
UserProtected   = FALSE
```

Angaben in spitzen Klammern sind entsprechend zu ersetzen (z. B. CN=beispiel.sachsen.de, OU=Saechsische Beispielbehoerde etc.). Eine Aufnahme zusätzlicher Zertifikatserweiterungen in die Konfigurationsdatei wird seitens der Sachsen Global CA ignoriert bzw. mit den folgenden vorgegebenen Standardwerten überschrieben: *https://www.pki.dfn.de/fileadmin/PKI/anleitungen/DFN-PKI-Zertifikatprofile_Global.pdf*

Die eigentliche Zertifikatsantragsdatei kann danach mit dem folgenden Aufruf des in Windows enthaltenen Kommandozeilen-Werkzeugs certreq.exe erstellt werden (Ausführung als Administrator erforderlich):

```
certreq -new <oben erstellte Textdatei> <Zertifikatsantragsdatei>
```

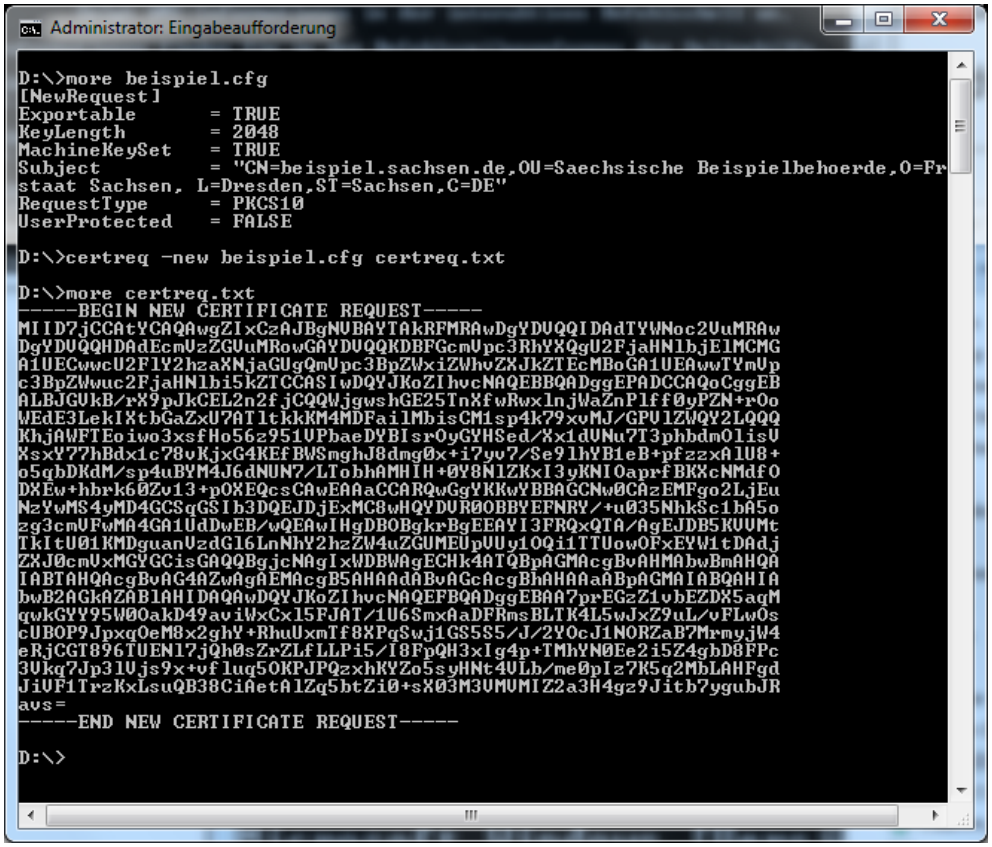


Abbildung 7: Zertifikatsantrag über Kommandozeile

2.2. Einsatz eines Zertifikates auf mehreren Webservern

Wichtig: wenn ein gemeinsames Serverzertifikat auf mehreren zusammengehörigen Webservern (z. B. mehrere Webserver auf einem physischen Server bzw. auf einer IP oder mehrere Weiterleitungsseiten mit einem gemeinsamen Weiterleitungsziel) zum Einsatz kommen soll, dann müssen diese Servernamen (z. B. sachsen.de und www.sachsen.de) bereits im Rahmen des Zertifikatsantrags als Synonyme in das Zertifikat eingetragen werden. Anderenfalls werden in allen gängigen Browsern massive Sicherheitswarnungen beim Aufruf der Seite angezeigt, da Zertifikat und Name der Webseite nicht zusammenpassen und ein Betrugsversuch angenommen werden muss.

Die Einbindung praktisch beliebig vieler solche Synonyme (Subject Alternative Names oder kurz: SANs) ist im Rahmen des Antragsprozesses über die Sachsen Global CA einfach möglich. Dazu müssen in der Textdatei als Basis für das Kommandozeilentool certreq.exe die in das Zertifikat aufzunehmenden SANs in einem neuen Abschnitt [Extensions] in folgendem Format aufgeführt werden:

```
[NewRequest]
Exportable      = TRUE
KeyLength       = 2048
MachineKeySet   = TRUE
Subject         = CN=beispiel.sachsen.de,OU=Saechsische
Beispielbehoerde,O=Freistaat Sachsen, L=Dresden,ST=Sachsen,C=DE“
RequestType     = PKCS10
UserProtected   = FALSE
```

```
[Extensions]
2.5.29.17 = "{text}"
_continue_      = "dns=beispiel.sachsen.de&"
_continue_      = "dns=www.beispiel.sachsen.de&"
_continue_      = "dns=sample.sachsen.de&"
```

Abbildung 8: Anpassung der Konfigurationsdatei bei SAN-Einträgen

Diese Einbindung von SANs ist ggf. nicht kompatibel mit älteren Versionen von Windows bzw. des darin enthaltenen Tools certreq.exe. Wenn Einbindung der SAN-Einträge in die Zertifikatsantragsdatei erfolgreich war, werden die SAN auch im Antragsformular angezeigt (nach dem späteren Hochladen des Requests auf der Antragsseite der Sachsen Global CA).

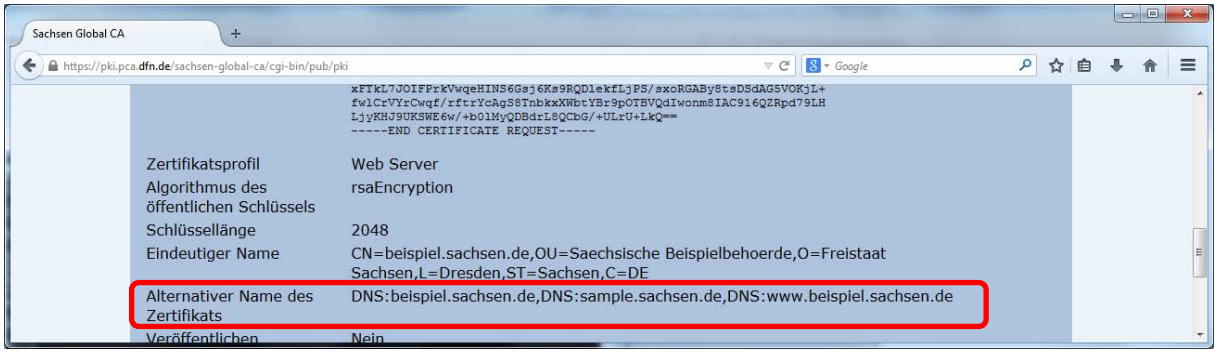


Abbildung 9: Anzeige der SAN-Einträge auf der Antragsseite der Sachsen Global CA

Eine zusätzliche Kontrolle / Prüfmöglichkeit besteht im Base64-Decodieren und Prüfen der Antragsdatei. Weitere Informationen zur Erzeugung eines SAN-Requests finden Sie auf der FAQ-Seite der DFN-PKI unter *https://www.pki.dfn.de/faqpki/faqpki-allgemein/#c15085*.

Sollte es Ihnen aus technischen Gründen nicht möglich sein, die SAN korrekt im Request zu erzeugen, können die SAN auch nachträglich durch die Zertifikatsmanager der Sachsen Global CA eingetragen werden. Dafür legen Sie bitte dem Antrag eine formlose Aufstellung der gewünschten SAN bei (mit einem Hinweis auf die später zugeteilte Antragsnummer des zugehörigen Zertifikatsantrags).

2.3. Antrag bei der Sachsen Global CA

Nachdem die Zertifikatsantragsdatei lokal erstellt wurde, können Sie nun ein Zertifikat der Sachsen Global CA über die entsprechende Webschnittstelle beantragen.

Zur kostenfreien Erstellung des weltweit gültigen HTTPS-Serverzertifikats nutzen Sie bitte folgende Webadresse *https://pki.pca.dfn.de/sachsen-global-ca/pub* (nur für Behörden des Freistaats Sachsen).

Es erfolgt eine Weiterleitung auf die zentrale Zertifikatsantragsseite der Sachsen Global CA. Im Reiter »Zertifikate« wählen Sie bitte den Menüpunkt »Serverzertifikat« und anschließend das Zertifikatsprofil »Web Server«.

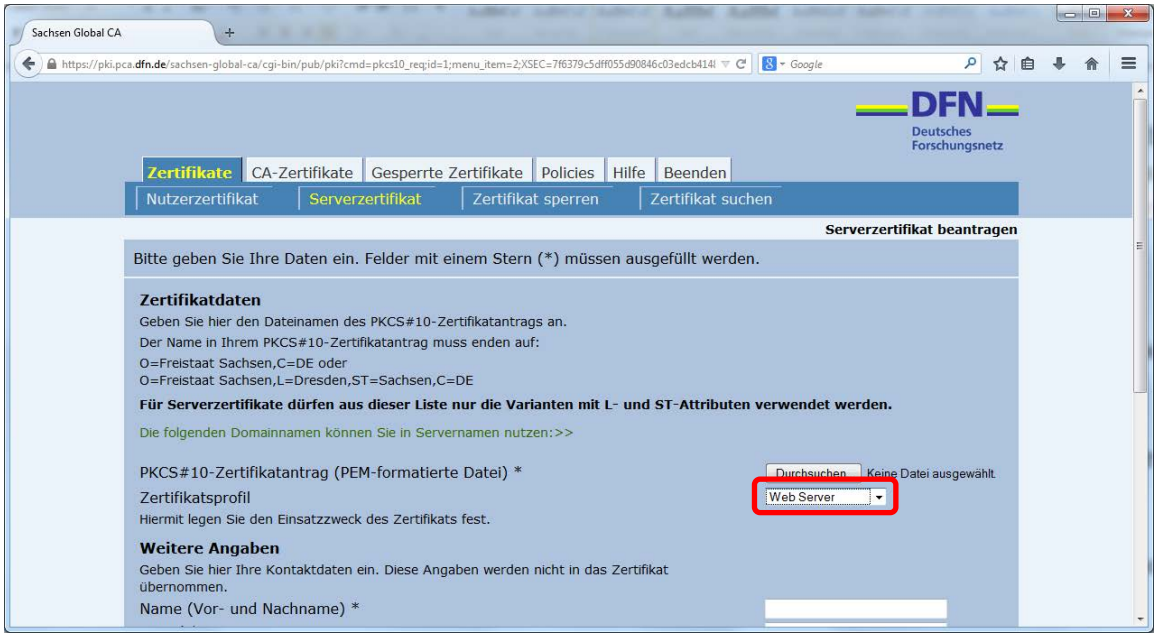


Abbildung 10: Serverzertifikat und Zertifikatsprofil

Anschließend ist die vorab erstellte Zertifikatsantragsdatei (PKCS#10-Format) hochzuladen und die Kontaktdaten des Antragstellers sind auszufüllen. Die Kontaktdaten dienen vor allem zur Auslieferung des Zertifikats und für Rückfragen zum Antrag. Die eingegebenen Daten werden nicht ins Zertifikat übernommen (das Zertifikat wird automatisch mit den Angaben aus der Zertifikatsantragsdatei ausgefüllt).

Alle Felder des Formulars sind auszufüllen. Im Feld Abteilung sind die Behörde bzw. der Bereich des Antragstellers anzugeben. Der Veröffentlichung des Zertifikats sollte zugestimmt werden. Bestätigen Sie Ihre Angaben mit der Schaltfläche »Weiter«.

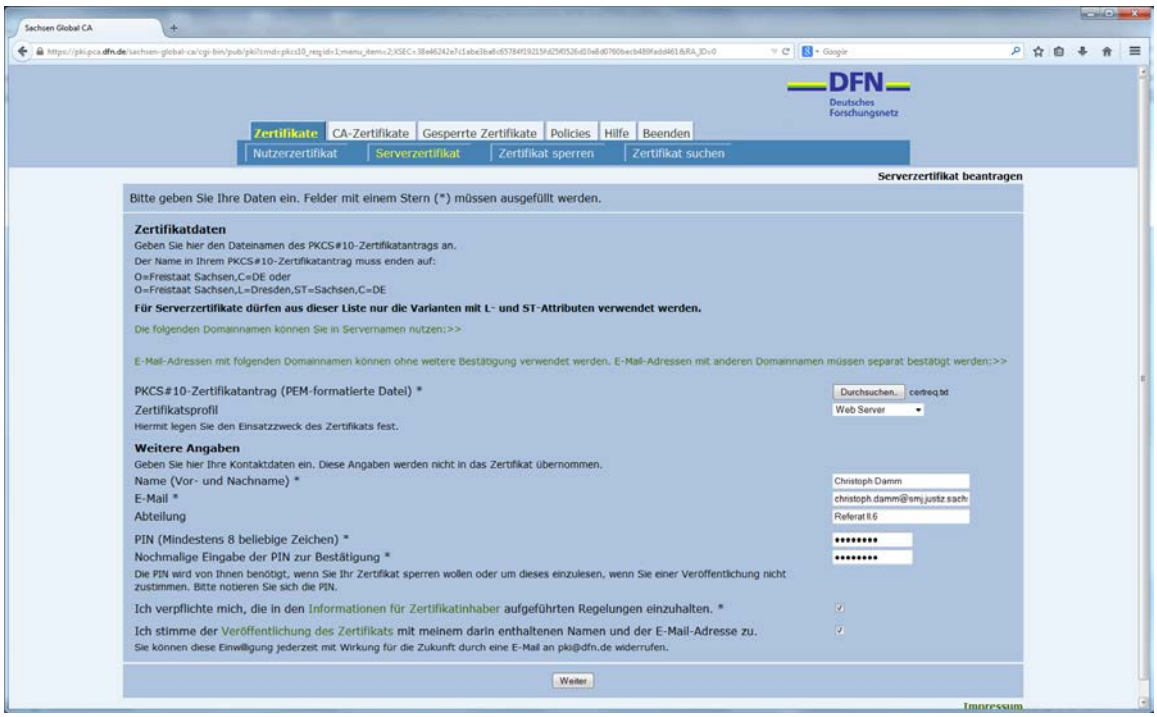


Abbildung 11: Eingabe der Zertifikatsdaten und weiterer Angaben

Anschließend werden die aus der Zertifikatsantragsdatei gelesenen und die eingegebenen Daten noch einmal angezeigt. Bitte prüfen und bestätigen Sie, dass alle Angaben korrekt sind und ob z. B. eingetragene SAN-Angaben beim evtl. geplanten Einsatz des Zertifikats auf mehreren Webservern korrekt übernommen wurden.

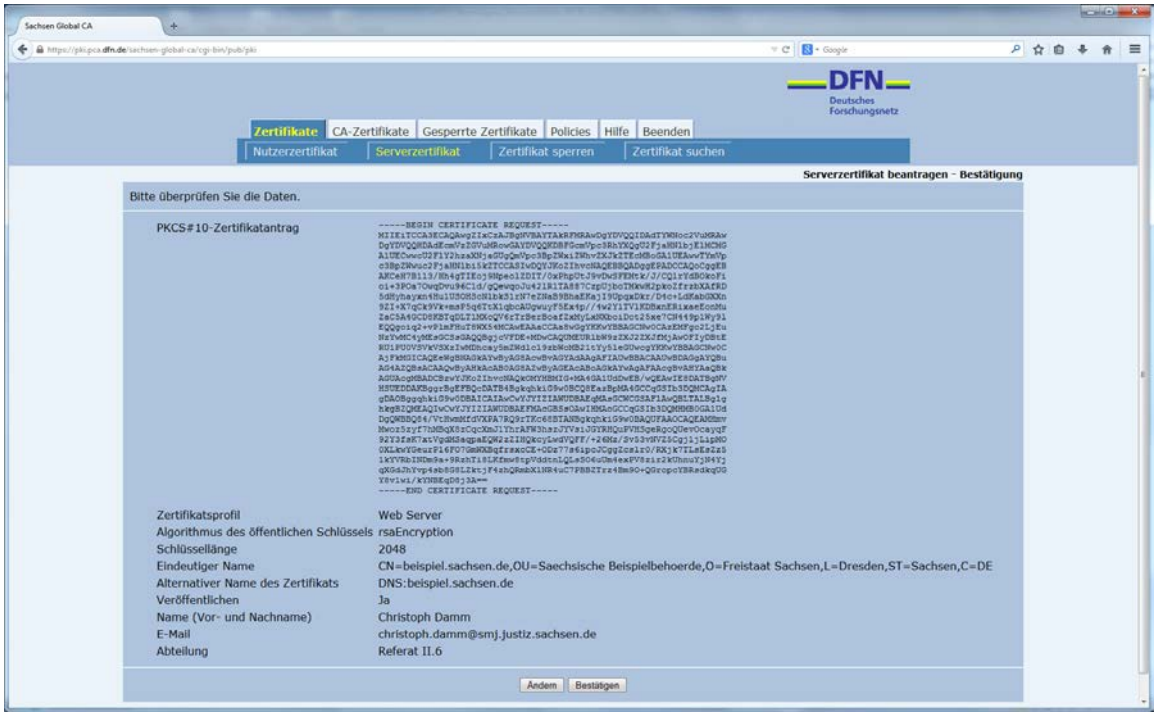


Abbildung 12: Bestätigung der Zertifikatsdaten

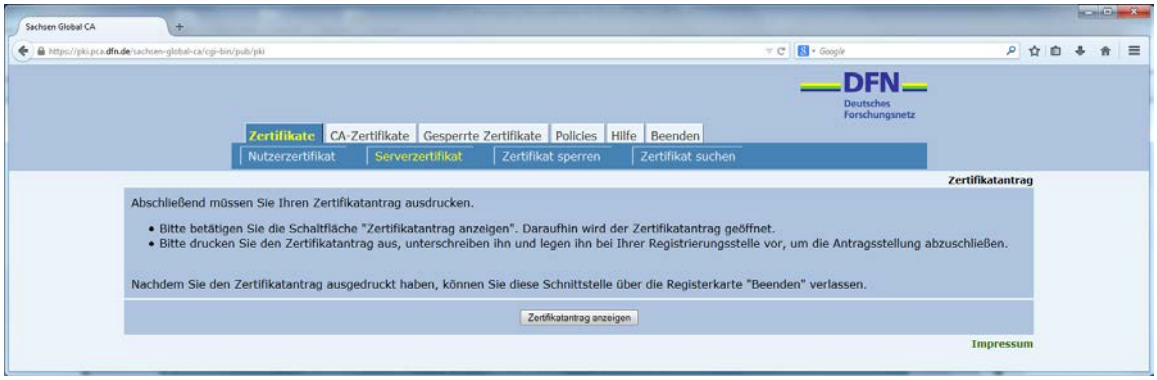


Abbildung 13: Anzeige des Zertifikatantrags

Der Zertifikatantrag wurde damit elektronisch vorab an die Sachsen Global CA übermittelt. Zur Genehmigung ist jedoch noch die Einreichung eines unterschriebenen Originals des Antrags notwendig.

2.4. Absenden und Freigabe des Zertifikatsantrags

Drucken und unterschreiben Sie den Antrag bzw. lassen Sie den Antrag unterschreiben. Eine persönliche Identifizierung des Antragstellers per Ausweiskopie oder Ausweisnummer ist nicht notwendig, jedoch eine klare Kennzeichnung einer Behörde (z. B. durch einen Behördenstempel) und eines verantwortlichen Ansprechpartners (Name und E-Mail, ggf. Telefonnummer).

Der Kasten im unteren Bereich des Antrags ist leer zu lassen, da er nur der internen Verwaltung in der Registrierungsstelle dient.

DFN-PKI

Zertifikatantrag für ein Serverzertifikat

- an: Sächsisches Staatsministerium des Inneren -

Antragsnummer 334368

Antragssteller

Vorname Nachname	Christoph Damm
E-Mail	christoph.damm@smj.justiz.sachsen.de
Abteilung	Referat II.6

Zertifikatdaten

Eindeutiger Name	CN=beispiel.sachsen.de, OU=Saechsische Beispielbehoerde, O=Freistaat Sachsen, L=Dresden, ST=Sachsen, C=DE
Alternativer Name	DNS:beispiel.sachsen.de
Public Key Fingerprint	43:39:B6:2C:D1:48:EB:05:21:65:81:15:69:24:06:F7:00:DA:02:0D
Veröffentlichen	Ja
Zertifikatprofil	Web Server

Erklärung des Antragsstellers

Hiermit beantrage ich ein Serverzertifikat in der DFN-PKI und verpflichte mich, die Regelungen der unter https://info.pca.dfn.de/doc/Info_Zertifikatinhaber.pdf veröffentlichten „Informationen für Zertifikatinhaber" einzuhalten. Das heißt insbesondere:

- Das Zertifikat darf nur auf Servern installiert werden, die unter den im Zertifikat enthaltenen Namen erreichbar sind.
- Der private Schlüssel darf nur Administratoren der im Zertifikat genannten Server zugänglich sein.
- Jeder im Zertifikat genannte Server, der aus dem Internet erreichbar ist, muss angemessen geschützt werden. Das heißt z. B.:
  - Der Server befindet sich in einer gesicherten Infrastruktur, z.B. hinter einer geeignet konfigurierten Firewall.
  - Der Server wird professionell betrieben, u.a. durch regelmäßiges Einspielen von Sicherheits-Patches.
  - Der administrative Zugriff auf den Server und somit auf den privaten Schlüssel ist klar geregelt.

Ich erkläre mich mit der Verarbeitung und Nutzung der erhobenen Daten zum Zweck der Zertifikaterstellung einverstanden. Die Daten dürfen an den DFN-Verein übermittelt und dort beschränkt auf diesen Zweck verarbeitet und genutzt werden.

(Ort, Datum) (Unterschrift)

Wird vom Teilnehmerservice ausgefüllt

Antragsprüfung:

- ☐ Name des Antragsstellers geprüft
- ☐ Berechtigung des Antragsstellers zum Erhalt des beantragten Zertifikats geprüft
- ☐ Berechtigung der Einrichtung zur Verwendung der enthaltenen Domain-Namen geprüft
- ☐ E-Mail-Adresse(n) sind dem Antragssteller zugeordnet

Name des TS-Mitarbeiters: _____

Zugehörige TS-Stelle: _____

(Datum, Unterschrift)

Seite 1/1 (Antragsnummer 334368) sachsen-global-ca

Abbildung 14: Zertifikatsantrag mit Identifizierung

Senden Sie den ausgedruckten, unterschriebenen Zertifikatsantrag an:

> Staatsbetrieb Sächsische Informatik Dienste
> Fachbereich 3.1 | E-Government- und Querschnittverfahren
> Zertifikatsmanager SachsenGlobalCA
> Riesaer Str. 7 | 01129 Dresden

Um die Bearbeitungszeit (Postlaufzeit) zu verkürzen, wird vorab ein Fax des Antrages akzeptiert. Senden Sie dieses an die Faxnummer +49 (0)3578 33 55 47 91.

Sobald der unterschriebene Antrag der Registrierungsstelle vorliegt, wird er kurzfristig geprüft und (in der Regel innerhalb von 2 bis 3 Arbeitstagen) freigegeben. Nach Freigabe durch den Zertifikatsmanager bekommen Sie eine E-Mail von pki@smi.sachsen.de mit Auslieferung des Zertifikats, welches Sie nun in Ihren Webserver importieren müssen.

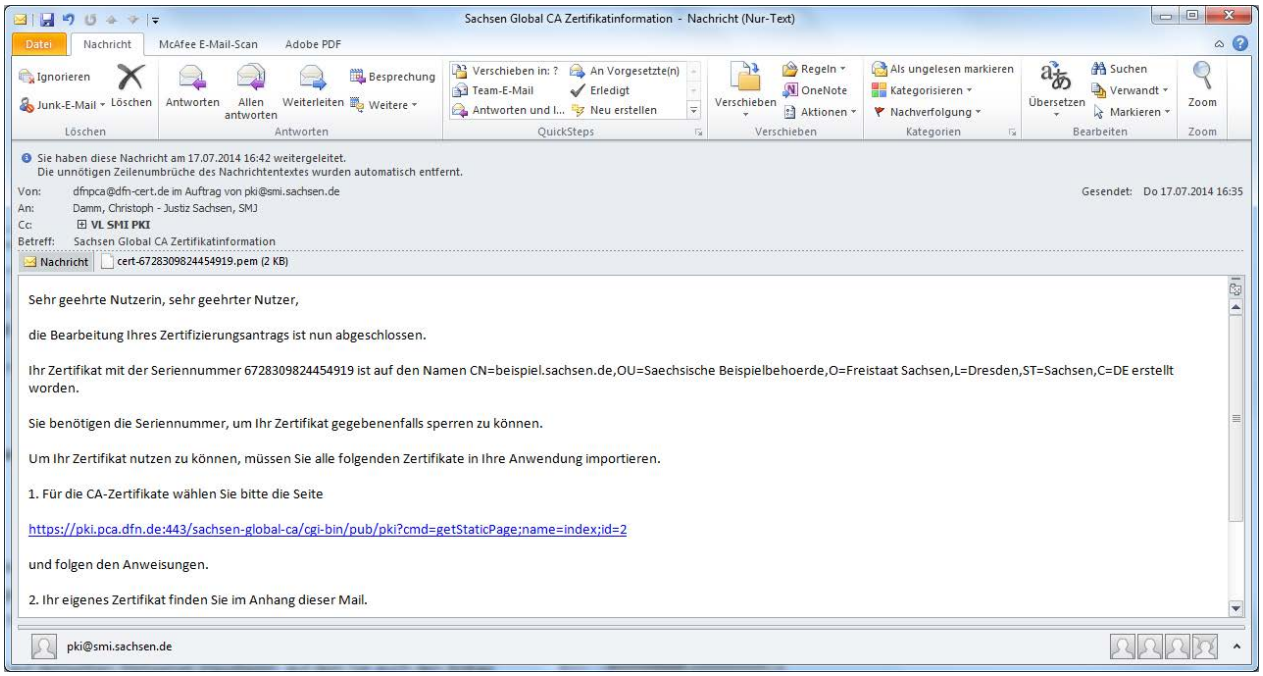


Abbildung 15: E-Mail mit Auslieferung des Zertifikats

2.5. Zertifikatsimport

Das ausgestellte Zertifikat haben Sie als Anhang einer E-Mail in Form einer PEM-Datei erhalten. Dieses Zertifikat müssen Sie mit dem geheimen Schlüssel, den Sie bei der Beantragung erzeugt haben, zusammenführen, um das Zertifikat nutzen zu können.

Achtung: Sie müssen das Zertifikat auf demselben Webserver importieren, auf dem Sie auch den Antrag erstellt haben, da nur auf diesem Webserver der geheime (private) Schlüssel vorliegt. Bei SAN-Anträgen müssen Sie entsprechend das Kommandozeilen-Werkzeug certreq.exe verwenden.

Das Zusammenführen von geheimem Schlüssel und Zertifikat im Microsoft IIS wird analog zum Erstellen eines Zertifikatantrags mit Hilfe des IIS-Managers durchgeführt. Auf der Startseitenansicht der Webseite können Sie unter dem Punkt »Serverzertifikate« den Prozess der Zertifikatanforderung abschließen. Wählen Sie dazu in der Ansicht »Serverzertifikate« oben links die Aktion »Zertifikatanforderung abschließen«.

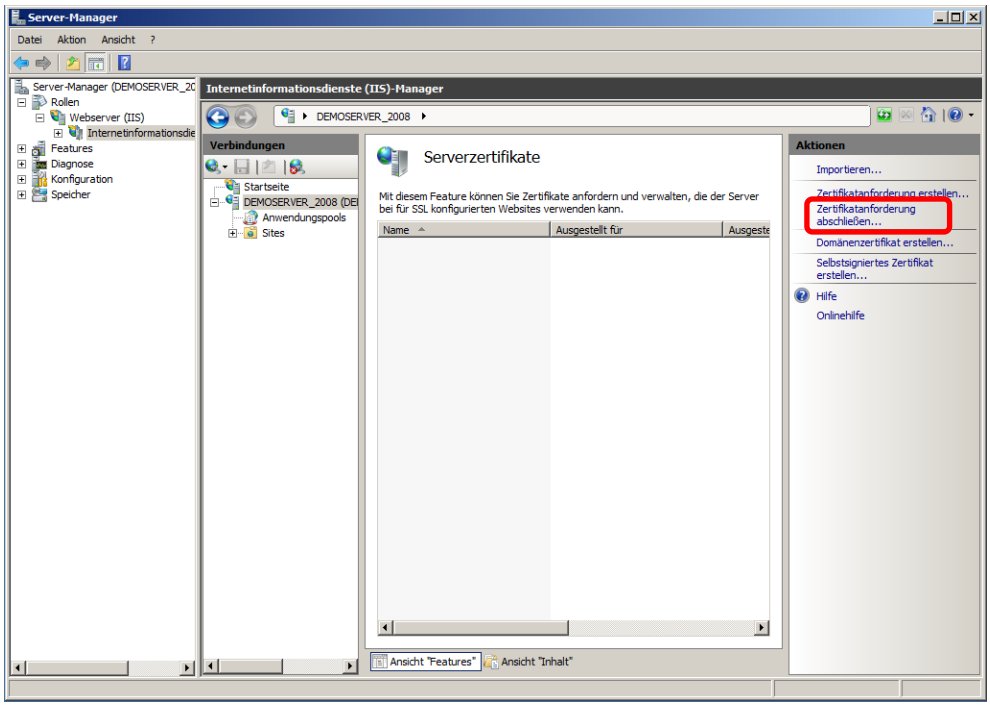


Abbildung 16: Zertifikatanforderung abschließen

Wählen Sie im nächsten Dialogfeld die PEM-Datei mit dem von der Sachsen Global CA ausgestellten Zertifikat aus, dass Sie von der E-Mail-Adresse pki@smi.sachsen.de erhalten haben, und klicken Sie auf Weiter.

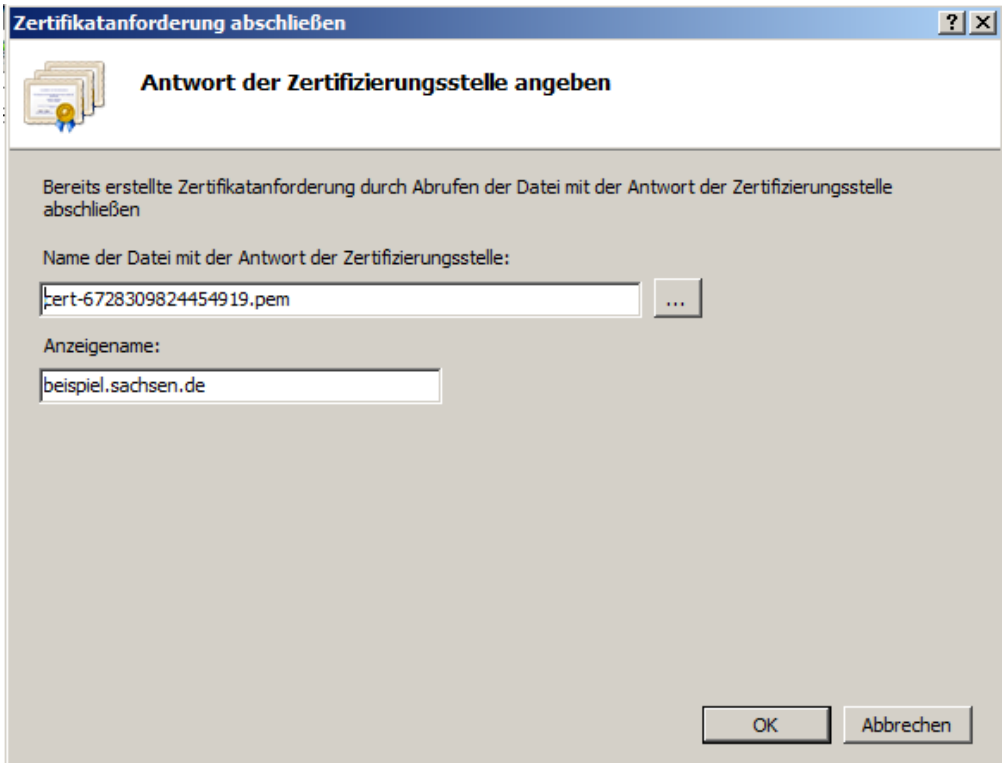


Abbildung 17: Auswahl der PEM-Datei

Das Zertifikat ist nun im Microsoft IIS importiert und kann für die Absicherung der HTTPS-Seite genutzt werden.

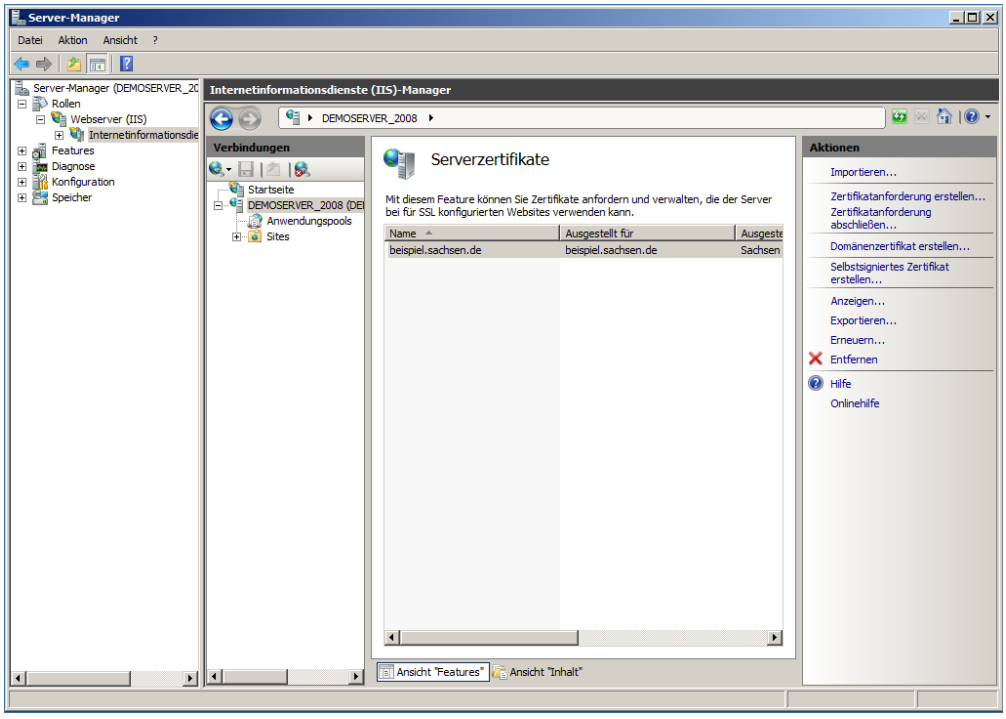


Abbildung 18: Zertifikat ist importiert

Ein Doppelklick auf das Zertifikat zeigt eine Zusammenfassung der im Zertifikat enthaltenen Daten.

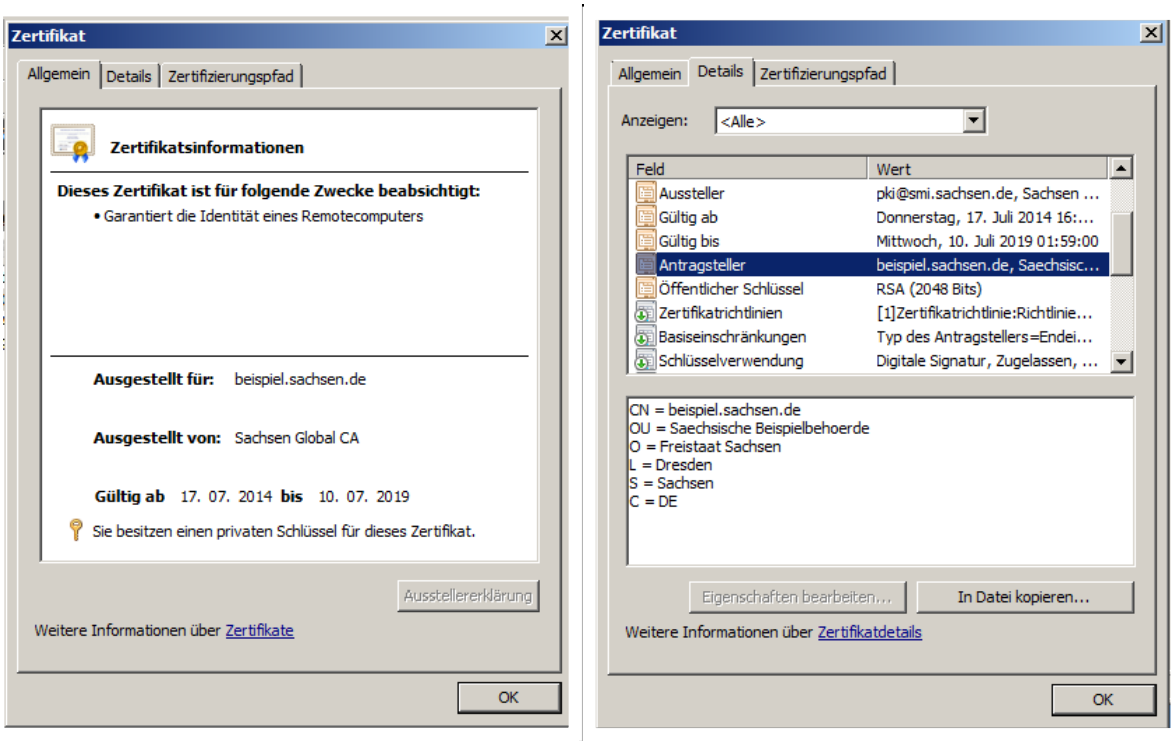


Abbildung 19: Zusammenfassung der im Zertifikat enthaltenen Daten

Das Zertifikat ist nun im Microsoft IIS importiert und kann für die Absicherung der HTTPS-Seite genutzt werden.

Alternativ kann ein Zertifikat auch mit Hilfe der Kommandozeile mit dem entsprechenden geheimen Schlüssel zusammengeführt werden. Hierfür geben Sie auf demselben Rechner, auf dem auch der Zertifikatsantrag erzeugt wurde, die folgende Kommandozeile ein:

```
certreq -accept <Zertifikatdatei>
```

Anschließend kann das Zertifikat (inkl. des privaten Schlüssels) exportiert und auf dem Zielsystem installiert werden.

2.6. Vermeidung von Problemen mit Zwischenzertifizierungsstellen

Trotz Einbindung der übergeordneten Wurzelzertifikate der Sachsen Global CA werden von den Nutzern vereinzelt Browserprobleme mit angeblich unbekannten Zertifikaten gemeldet. Grund hierfür ist in der Regel, dass der betreffende HTTPS-Webserver bei dem Verbindungsaufbau nicht die komplette CA-Kette mit allen Zwischenzertifizierungsstellen (das DFN-Verein PCA Global-G01 Zertifikat und das Zertifikat Ihrer ausgelagerten CA) ausliefert. Dadurch kann der Browser des Nutzers keine Verkettung zu dem vorinstallierten Wurzelzertifikat herstellen.

Um diese Probleme zu vermeiden, muss seitens des Webseitenbetreibers - also durch Sie - für Ihre HTTPS-Seiten im »Internet Information Server« die Zertifikatkette in den Zertifikatspeicher »Zwischenzertifizierungsstellen« importiert werden.

Die dafür benötigte Zertifikatkette der Sachsen Global CA finden Sie unter *https://pki.pca.dfn.de/sachsen-global-ca/pub/cacert/chain.txt*.

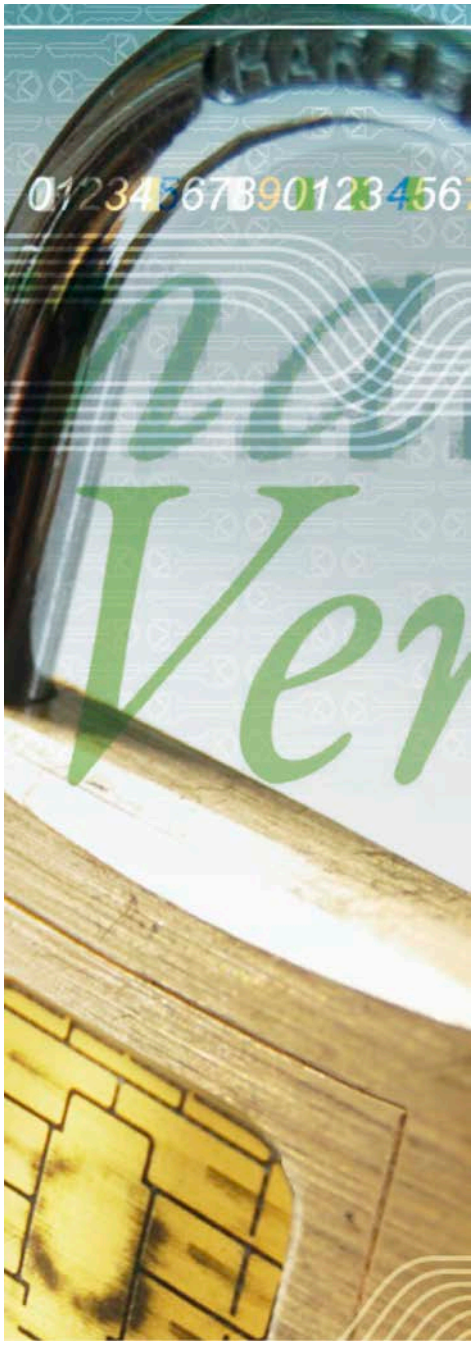
Ggf. ist nun noch ein Neustart von Microsoft IIS notwendig, damit das neue Zertifikat korrekt genutzt wird.

Anschließend sollte das Ergebnis der geänderten Konfiguration mit dem SSL-Servertest unter *https://www.ssllabs.com/ssltest* (Häkchen bei Option »Do not show the results on the boards« nicht vergessen) erneut getestet und mit dem Ergebnis vor dem Zertifikatsaustausch verglichen werden.

Auf die Nutzungsrichtlinien für den Einsatz der beantragten Serverzertifikate wird verwiesen *https://info.pca.dfn.de/doc/Info_Zertifikatinhaber.pdf*.

Die grundsätzlichen Nutzungsbedingungen der Sachsen Global CA sind beschrieben unter *https://www.pki.dfn.de/fileadmin/PKI/DFN-PKI_CP.pdf* und unter *https://www.pki.dfn.de/fileadmin/PKI/DFN-PKI_CPS.pdf*.

Für Rückfragen zu dieser Handlungsanleitung steht Ihnen ein E-Mail-Support unter *SachsenGlobalCaZm@sid.sachsen.de* zur Verfügung.



Herausgeber & Redaktion
Sächsisches Staatsministerium des Innern
Wilhelm-Buck-Straße 4
01097 Dresden

Verteilerhinweis

Diese Informationsschrift wird von der Sächsischen Staatsregierung im Rahmen ihrer verfassungsmäßigen Verpflichtung zur Information der Öffentlichkeit herausgegeben. Sie darf weder von Parteien noch von deren Kandidaten oder Helfern im Zeitraum von sechs Monaten vor einer Wahl zum Zwecke der Wahlwerbung verwendet werden. Dies gilt für alle Wahlen.

Missbräuchlich ist insbesondere die Verteilung auf Wahlveranstaltungen, an Informationsständen der Parteien sowie das Einlegen, Aufdrucken oder Aufkleben parteipolitischer Informationen oder Werbemittel. Untersagt ist auch die Weitergabe an Dritte zur Verwendung bei der Wahlwerbung. Auch ohne zeitlichen Bezug zu einer bevorstehenden Wahl darf die vorliegende Druckschrift nicht so verwendet werden, dass dies als Parteinahme des Herausgebers zu Gunsten einzelner politischer Gruppen verstanden werden könnte.

Diese Beschränkungen gelten unabhängig vom Vertriebsweg, also unabhängig davon, auf welchem Wege und in welcher Anzahl diese Informationsschrift dem Empfänger zugegangen ist. Erlaubt ist jedoch den Parteien, diese Informationsschrift zur Unterrichtung ihrer Mitglieder zu verwenden.