STAATSMINISTERIUM
DES INNERN

Freistaat
SACHSEN

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

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

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 Freistaates 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 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 für einen Apache-Webserver können Sie z. B. die in Apache enthaltene Software **OpenSSL** verwenden. Im Folgenden finden Sie eine kurze Anleitung hierzu.

Bitte erstellen Sie zuerst eine leere Textdatei mit dem Namen »SachsenGlobalCA-req.cfg« und kopieren folgende Zeilen hinein:

```
#####################################################################
#
# SachsenGlobalCA-req.cfg
#
# Verwenden Sie diese Datei als Konfigurationsdatei fuer
Zertifikatsantraege der SachsenGlobalCA.
# Das typische Kommando zur Erstellung eines solchen Server-
Zertifikatantrags lautet:
# openssl req -config "SachsenGlobalCA-req.cfg" -newkey rsa:2048 -keyout
"privatekey.pem" -out "certrequest.pem"
#
#####################################################################

[ req ]
default_bits            = 2048
distinguished_name      = req_distinguished_name
req_extensions          = v3_req
string_mask             = nombstr

[ req_distinguished_name ]
countryName             = Land (bitte nicht aendern)
countryName_default     = DE
countryName_min         = 2
countryName_max         = 2

stateOrProvinceName     = Bundesland (bitte nicht aendern)
stateOrProvinceName_default= Sachsen

localityName            = Ort (bitte nicht aendern)
localityName_default    = Dresden

0.organizationName      = Organisation (bitte nicht aendern)
0.organizationName_default = Freistaat Sachsen

0.organizationalUnitName    = Behoerde (Name Ihrer Behoerde eingeben)

commonName              = Domainname der Webseite
commonName_max          = 256

[ v3_req ]

# Kommentarzeichen vor naechster Zeile entfernen, wenn ein oder mehr
zusaetzliche DNS-Namen benoetigt werden
# subjectAltName = DNS:beispiel.sachsen.de, DNS:www.beispiel.sachsen.de,
DNS:sample.sachsen.de
```

Diese Konfigurationsdatei enthält die wichtigsten Einstellungen für einen Zertifikatsantrag mittels OpenSSL.

Die Datei kann auch ohne Änderungen für weitere Anträge verwendet werden. Anpassungen sind nur nötig, wenn mehrere Servernamen in ein Zertifikat geschrieben werden sollen (sog. SAN-Einträge).

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*

Nach Erstellung der Konfigurationsdatei bitte OpenSSL über die Kommandozeile wie folgt ausführen:

```
openssl req -config "SachsenGlobalCA-req.cfg" -newkey rsa:2048 -keyout
"privatekey.pem" -out "certrequest.pem"
```

Eine Beschreibung der wichtigsten Optionen von OpenSSL findet sich z. B. unter
https://www.pki.dfn.de/fileadmin/PKI/anleitungen/Anleitung_Nutzung_OpenSSL.pdf

Die Option »-config« lädt die im ersten Schritt beschriebene Datei. Die Option »-keyout« legt den Dateinamen des erstellten privaten Schlüssels zur Zertifikatsantragsdatei fest, die Option »-out« erstellt die dazu passende Zertifikatsantragsdatei im PKCS#10-Format zum Hochladen auf die Zertifikatsantragsseite der Sachsen Global CA. Beide Dateien haben das Dateiformat PEM.

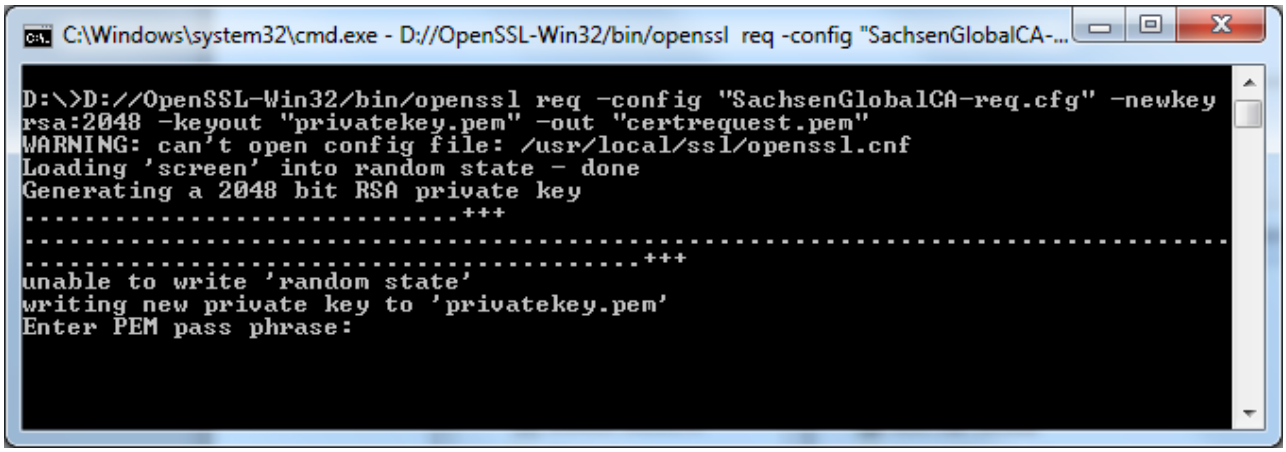


Abbildung 1: Ausführung OpenSSL über Kommandozeile

Für die Erstellung des privaten Schlüssels zur Zertifikatsantragsdatei muss ein Passwort (PEM pass phrase) vergeben werden, welches später für die Einrichtung des Zertifikats auf dem Webserver und auch bei jedem Neustart benötigt wird. Die Erstellung einer ungeschützten Schlüsseldatei ist zwar möglich, aber aus Sicherheitsgründen abzulehnen. Wenn eine solche ungeschützte Datei z. B. vom laufenden Apache gelesen werden kann, besteht die Gefahr dass der private Schlüssel über unsichere CGI-Scripte ausgelesen und die Sicherheit des gesamten Internetauftritts damit untergraben wird.

Anschließend sind die eigentlichen Zertifikatsantragsdaten einzugeben. Durch die Verwendung der Konfigurationsdatei sind die meisten Angaben bereits vorbelegt und müssen nicht mehr ausgefüllt werden. Das betrifft alle Vorgaben wie die Schlüssellänge von 2048 bit und die geografischen Angaben zum Standort der CA, d. h. Land (Country, C, »DE«), Bundesland (State, ST, »Sachsen«), Stadt (Locality, L, »Dresden«) und der Betreiber (Organization, O, »Freistaat Sachsen«). **Andere Angaben oder das Weglassen von Einträgen ist bei allen diesen Feldern nicht zulässig** (bitte alle Angaben jeweils mit Return bestätigen).

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« (»Sächsisch«) zulässig sind**. Der Domainname (vollqualifizierter DNS-Hostname, FQDN) des Webservers, von dem das Zertifikat später verwendet werden soll (z. B. beispiel.sachsen.de) ist im Feld CN (Common Name) anzugeben. IP-Adressen dürfen im CN nicht angegeben werden. **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. 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.

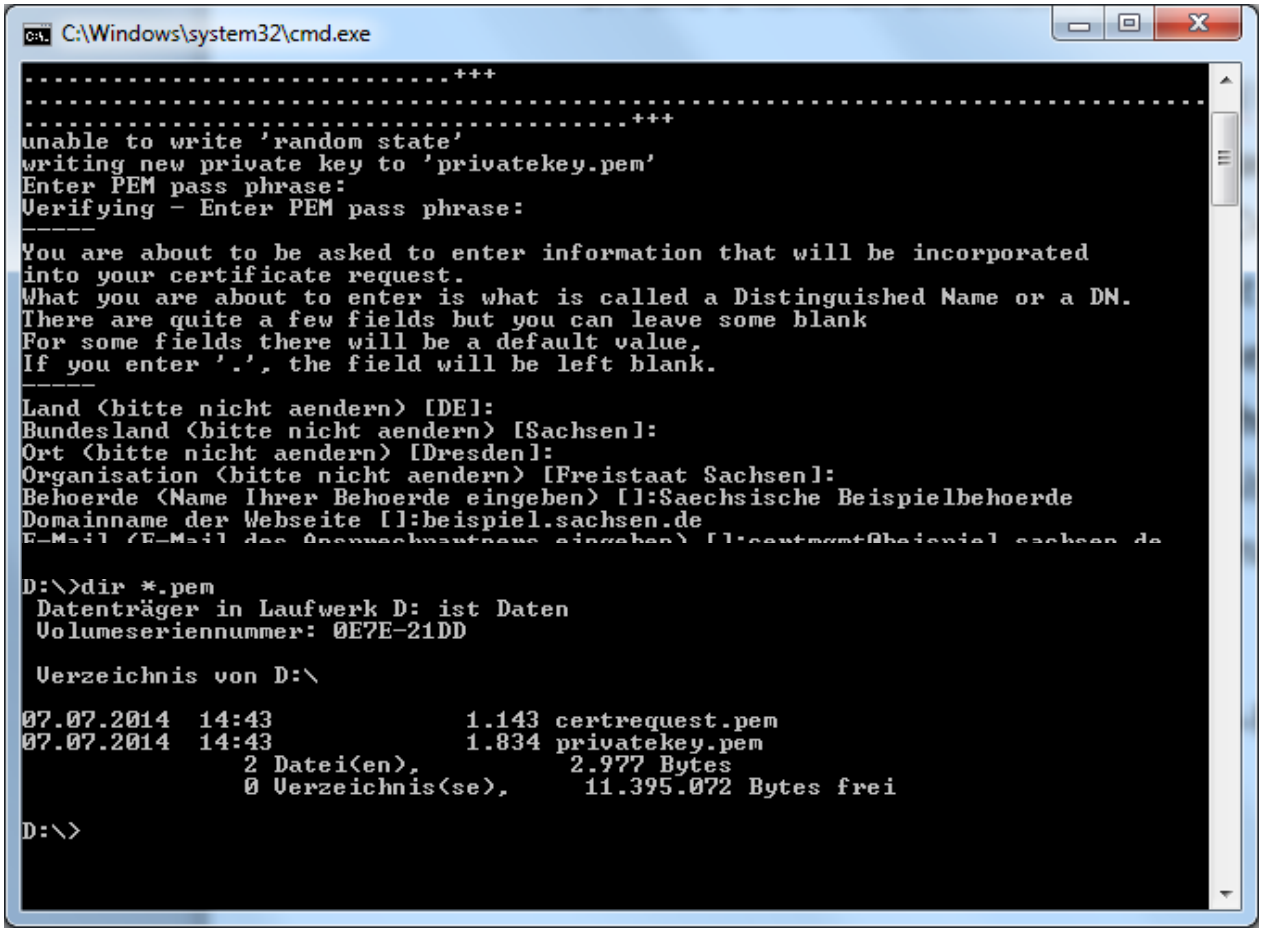


Abbildung 2: Eingabe der Zertifikatsantragsdaten in Kommandozeile

Der private Schlüssel in Form einer passwortgeschützten Datei sowie die Zertifikatsantragsdatei im PKCS#10-Format liegen damit vor.

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 zusammen passen 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 muss in der Konfigurationsdatei SachsenGlobalCA-req.cfg das Kommentarzeichen (#) vor der letzten Zeile (vor dem Wort subjectAltName) entfernt und die in das Zertifikat aufzunehmenden SANs jeweils mit vorangestelltem »DNS:« vor dem Domainnamen und jeweils mit Komma getrennt eingetragen werden. Ein Beispiel hierzu ist nachfolgend dargestellt.

```
# Kommentarzeichen vor naechster Zeile entfernen, wenn ein oder mehr
zusaetzliche DNS-Namen benoetigt werden

subjectAltName = DNS: beispiel.sachsen.de, DNS:www.beispiel.sachsen.de,
DNS:sample.sachsen.de
```

Wichtig: der unter CN angegebene Domainname muss zusätzlich noch einmal in der Liste der SAN-Einträge aufgenommen werden.

Wenn die SAN in der Zertifikatsantragsdatei korrekt eingebunden sind, werden die SAN auch im Antragsformular angezeigt (nach Hochladen des Requests auf der Webseite). 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«.

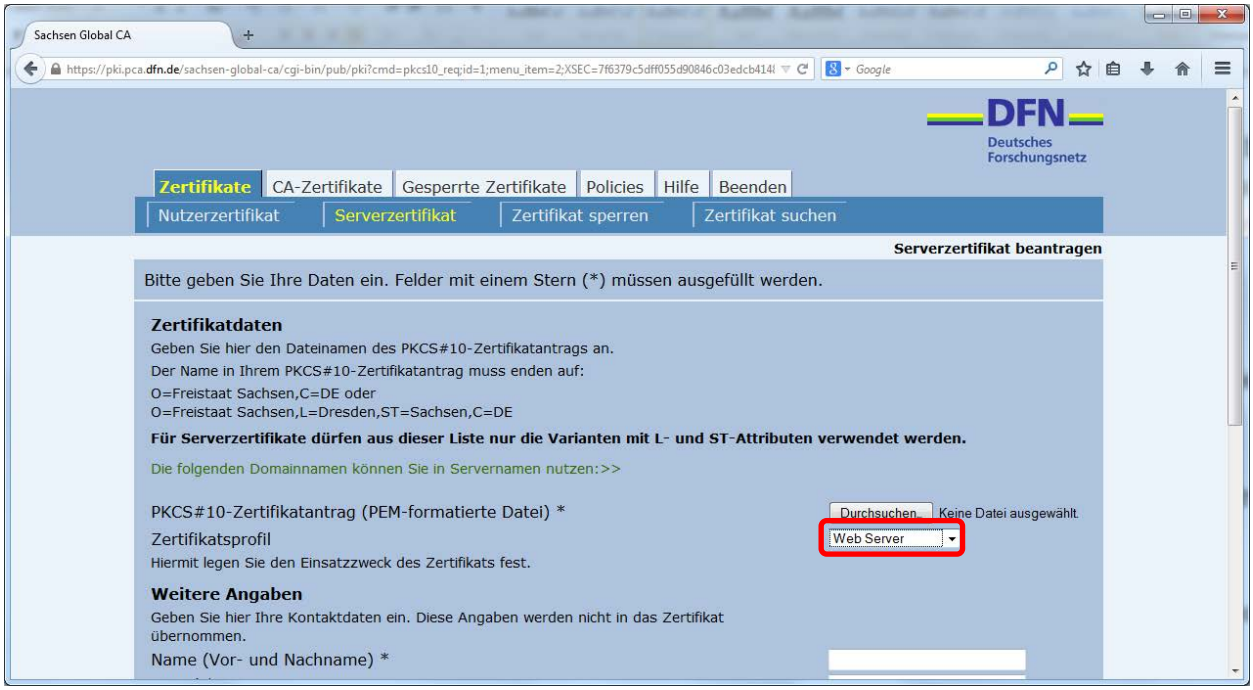


Abbildung 3: Serverzertifikat und Zertifikatsprofil

Anschließend ist die vorab erstellte Zertifikatsantragsdatei (PKCS#10-Format, z. B. certrequest.pem) 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 4: 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, das alle Angaben korrekt sind und ob z. B. eingetragene SAN-Angaben beim evtl. geplanten Einsatz des Zertifikats auf mehreren Webservern korrekt übernommen wurden.

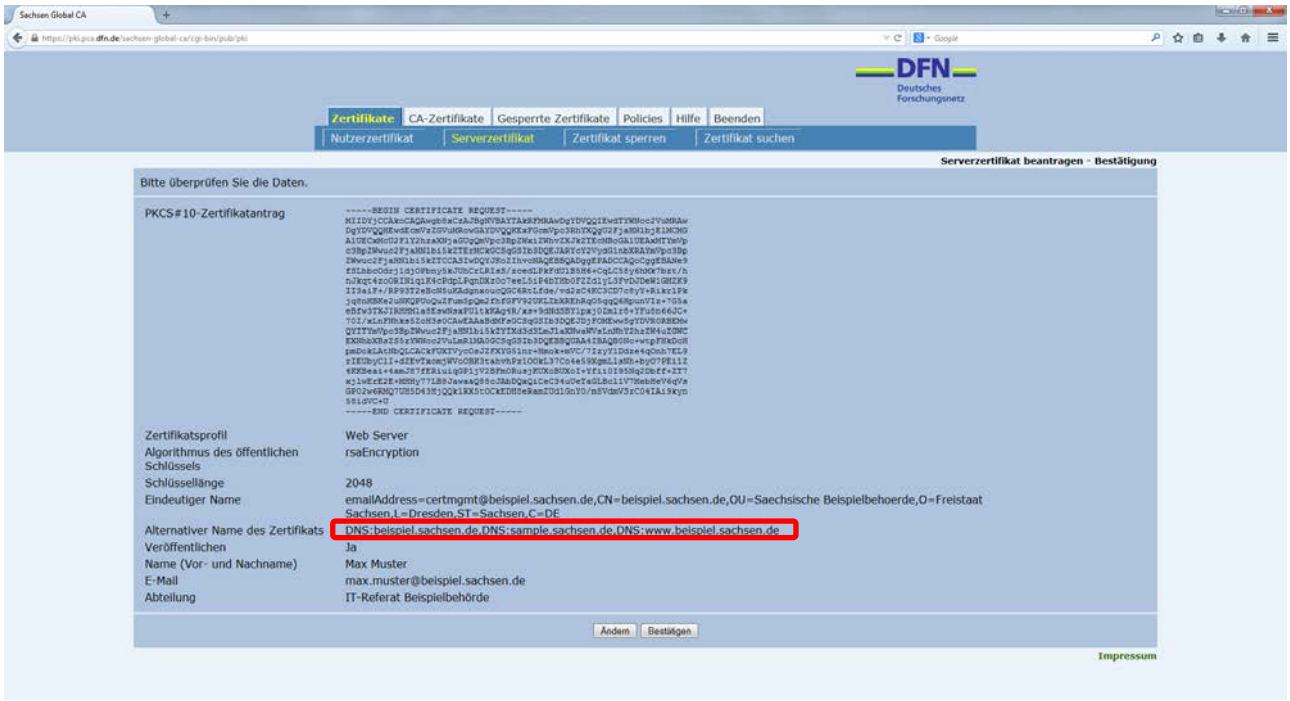


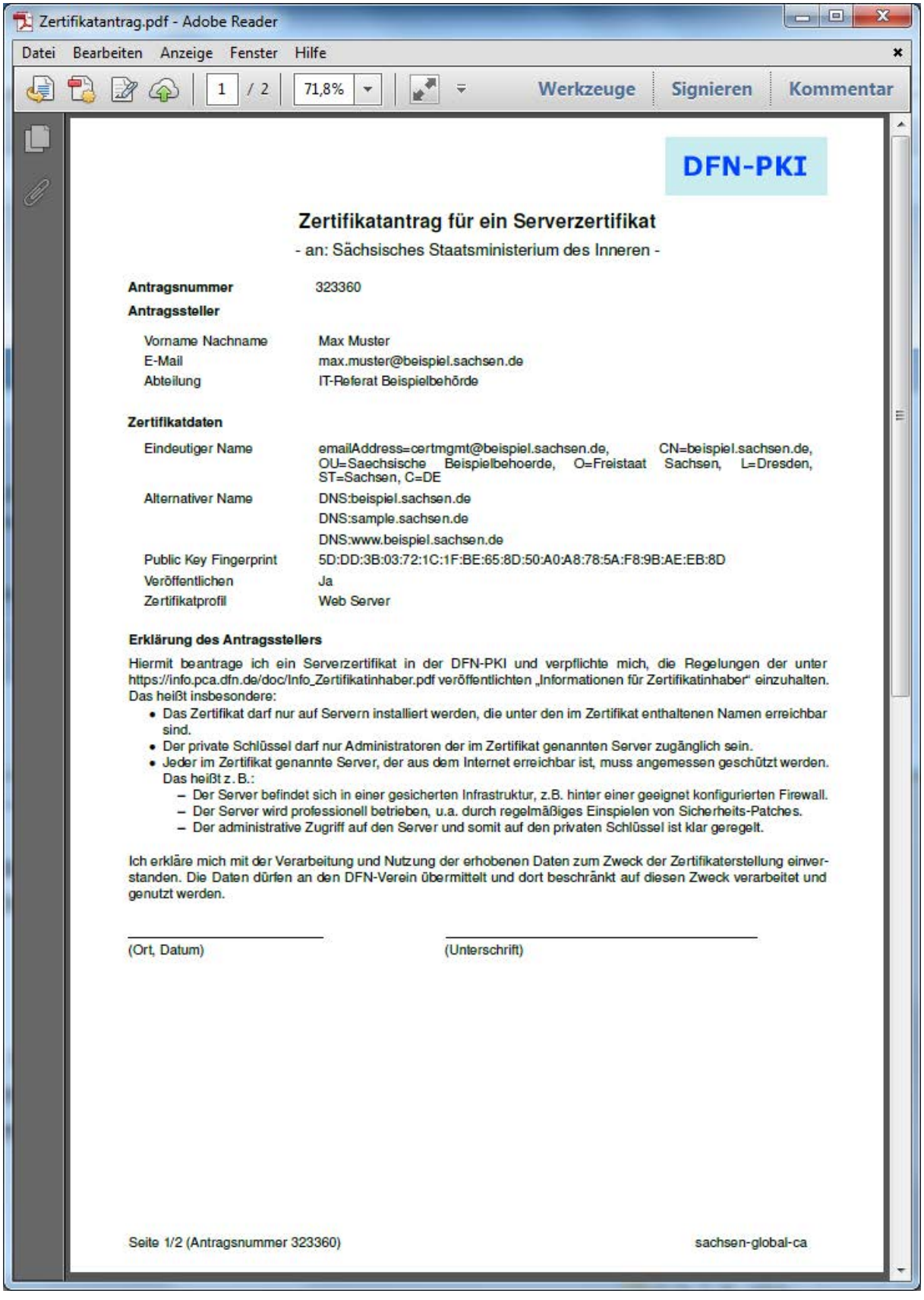
Abbildung 5: Bestätigung der Zertifikatsdaten

In der Zeile »Alternativer Name des Zertifikats« sieht man hier, dass die SAN-Einträge zum Einsatz des Zertifikats auf mehreren Webservern korrekt aus der Zertifikatsantragsdatei übernommen wurden.

Abbildung 6: 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


Zertifikatantrag.pdf - Adobe Reader

Datei Bearbeiten Anzeige Fenster Hilfe

1 / 2 71,8% Werkzeuge Signieren Kommentar

DFN-PKI

Zertifikatantrag für ein Serverzertifikat

- an: Sächsisches Staatsministerium des Inneren -

Antragsnummer 323360

Antragssteller

Vorname Nachname	Max Muster
E-Mail	max.muster@beispiel.sachsen.de
Abteilung	IT-Referat Beispielbehörde

Zertifikatdaten

Eindeutiger Name	emailAddress=certmgmt@beispiel.sachsen.de, CN=beispiel.sachsen.de, OU=Saechsische Beispielbehoerde, O=Freistaat Sachsen, L=Dresden, ST=Sachsen, C=DE
Alternativer Name	DNS:beispiel.sachsen.de DNS:sample.sachsen.de DNS:www.beispiel.sachsen.de
Public Key Fingerprint	5D:DD:3B:03:72:1C:1F:BE:65:8D:50:A0:A8:78:5A:F8:9B:AE:EB:8D
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)

Seite 1/2 (Antragsnummer 323360) sachsen-global-ca

Abbildung 6: Zertifikatantrag für ein Serverzertifikat

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 Antragsformulars ist leer zu lassen, da er nur der internen Verwaltung in der Registrierungsstelle dient. 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.

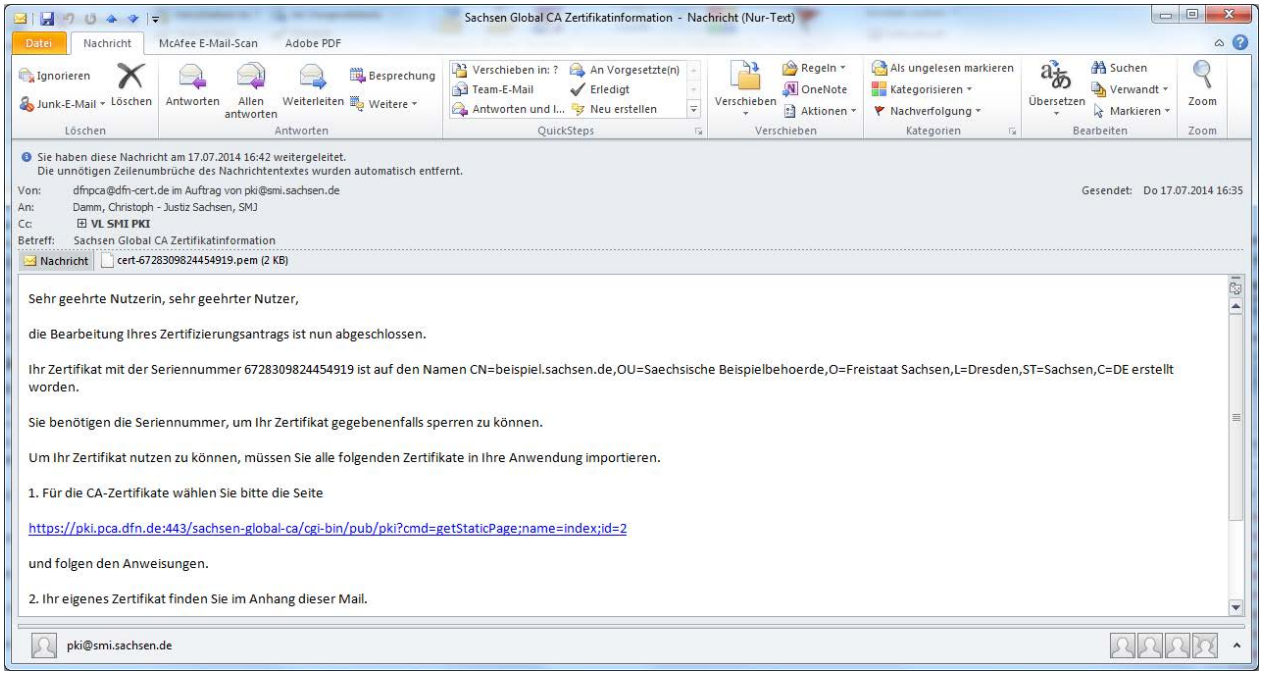


Abbildung 7: E-Mail mit Auslieferung des Zertifikats

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 beim Beantragen erzeugt haben, zusammenführen, um das Zertifikat nutzen zu können.

Unter Linux kann das über eine einfache Verkettung der beiden Dateien über die Kommandozeile erfolgen. Zur Vermeidung eventueller Probleme einzelner Anwendungen bei der Zuordnung des korrekten Wurzelzertifikats sollte an dieser Stelle zusätzlich die Zertifikatkette der Sachsen Global CA mit eingefügt werden. Die Zertifikatkette können Sie unter *https://pki.pca.dfn.de/sachsen-global-ca/pub/cacert/chain.txt* herunterladen.

```
cat <cert-xx.pem> <chain.txt> <privatekey.pem> > <certificate.pem>
```

Unter Windows lautet die Kommandozeile wie folgt:

```
copy <cert-xx.pem> + <chain.txt> + <privatekey.pem> <certificate.pem>
```

Dabei bedeuten die beispielhaften Dateinamen in den spitzen Klammern folgendes:

1. `<cert-xx.pem>` = die per E-Mail über pki@smi.sachsen.de von der Sachsen Global CA erhaltene Zertifikatdatei

2. `<chain.txt>` = die über *https://pki.pca.dfn.de/sachsen-global-ca/pub/cacert/chain.txt* heruntergeladene Zertifikatkettendatei

3. `<privatekey.pem>` = die zu Beginn des Antragsprozesses erstellte passwortgeschützte Datei mit dem privaten Schlüssel

4. `<certificate.pem>` = die zu erstellende Ausgabedatei mit dem Zertifikat

Die nun vorliegende zusammengeführte Zertifikatsdatei muss in den Konfigurationseinstellungen des Apache-Webservers eingetragen werden. Die entsprechende Konfigurationsdatei sollte unter dem Namen »httpd.conf« zu finden sein. Je nach Konfiguration sind die HTTPS-Einstellungen aber auch manchmal in eine gesonderte Datei ausgelagert, meist unter den Namen »ssl.conf« oder »httpd-ssl.conf«.

Der Standardspeicherort der HTTPS-Konfigurationsdatei ist:

```
Windows: C:\Program Files\Apache Software Foundation\Apache2.2\conf.extra
Linux: /usr/local/apache/etc
```

In dieser Datei sind die folgenden Direktiven zu überprüfen und ggf. zu aktualisieren:

`SSLCertificateFile` = Pfad zur Zertifikatdatei (certificate.pem)
`SSLCertificateKeyFile` = Pfad zum privaten Schlüssel (privatekey.pem)
`SSLCertificateChainFile` = Pfad zur Zertifikatskette (chain.txt)

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

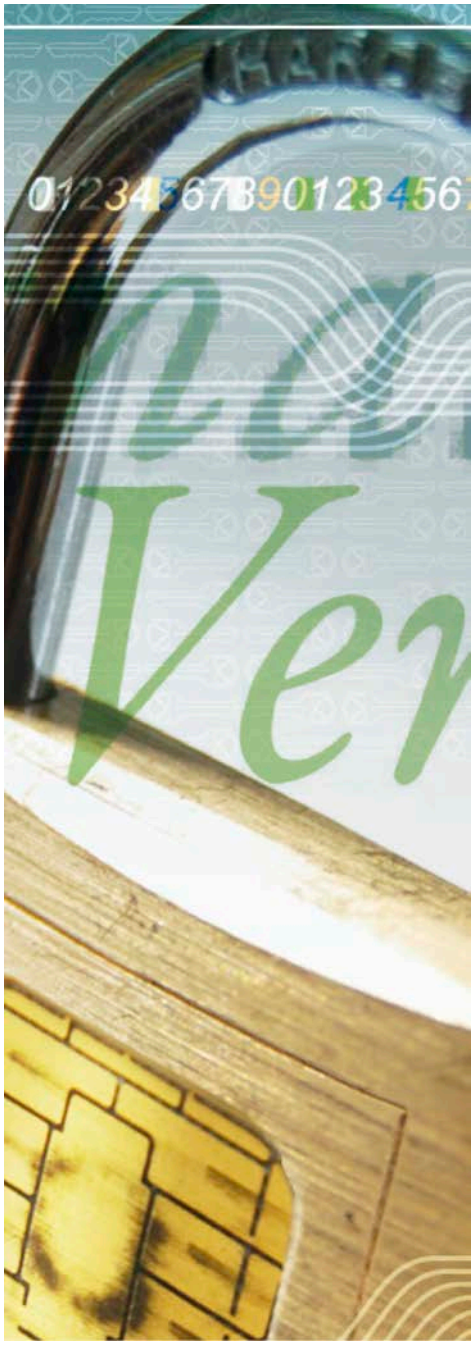
Beim Betrieb mehrerer HTTPS-Domänen auf einem Server können zusätzliche Konfigurationsaufwände entstehen. Im Internet finden sich dazu verschiedene Lösungsvorschläge, z. B. unter *http://www.schirmacher.de/display/INFO/Apache+SSL+Zertifikat+erstellen#ApacheSSLZertifikaterstellen-MehrereSSL-DomainsproServer*

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 *https://www.pki.dfn.de/fileadmin/PKI/DFN-PKI_CPS.pdf*.

Für Rückfragen zu der 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.