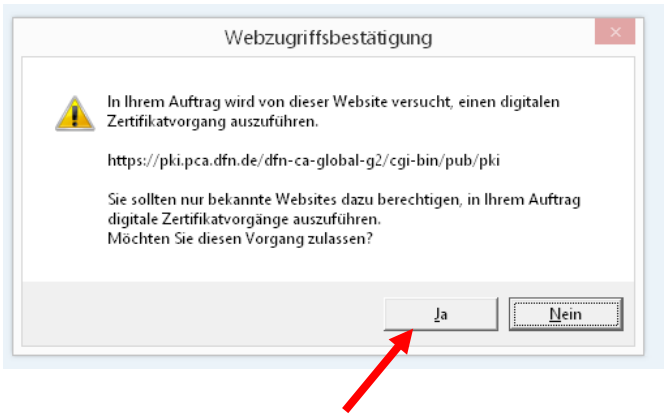
Beantragung eines Nutzerzertifikats mit dem Internet-Explorer:

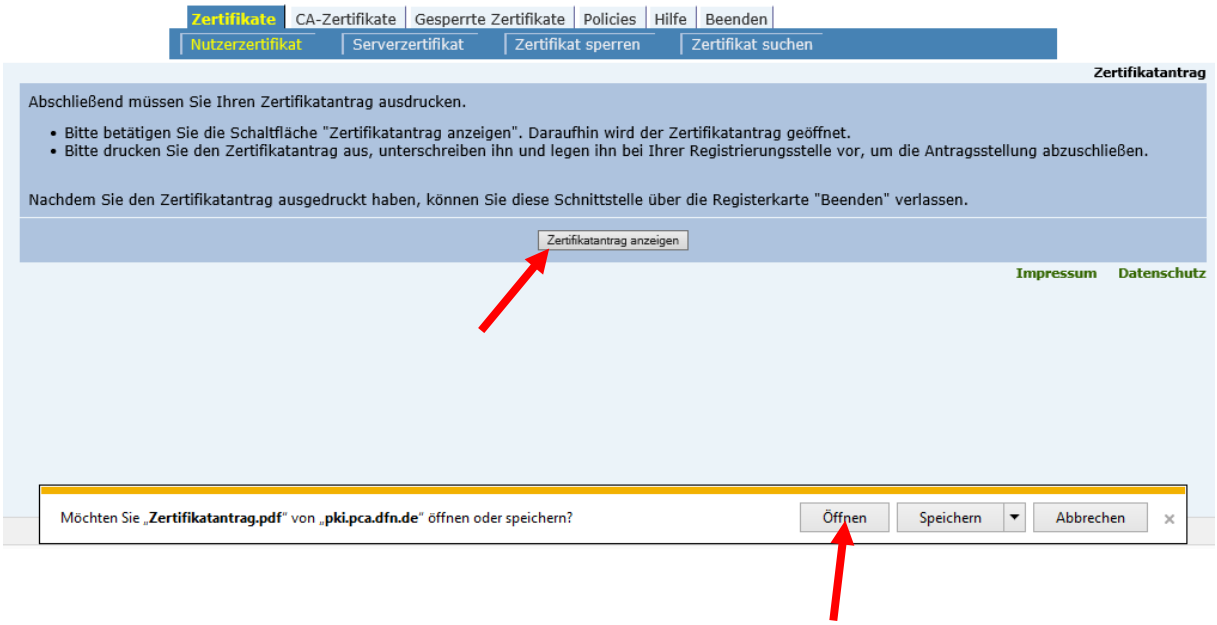
1. Auf der Seite: https://pki.pca.dfn.de/dfn-ca-global-g2/cgi-bin/pub/pki?cmd=getStaticPage&name=index&RA_ID=2100 werden die erforderlichen Angaben gemacht. Weiter.

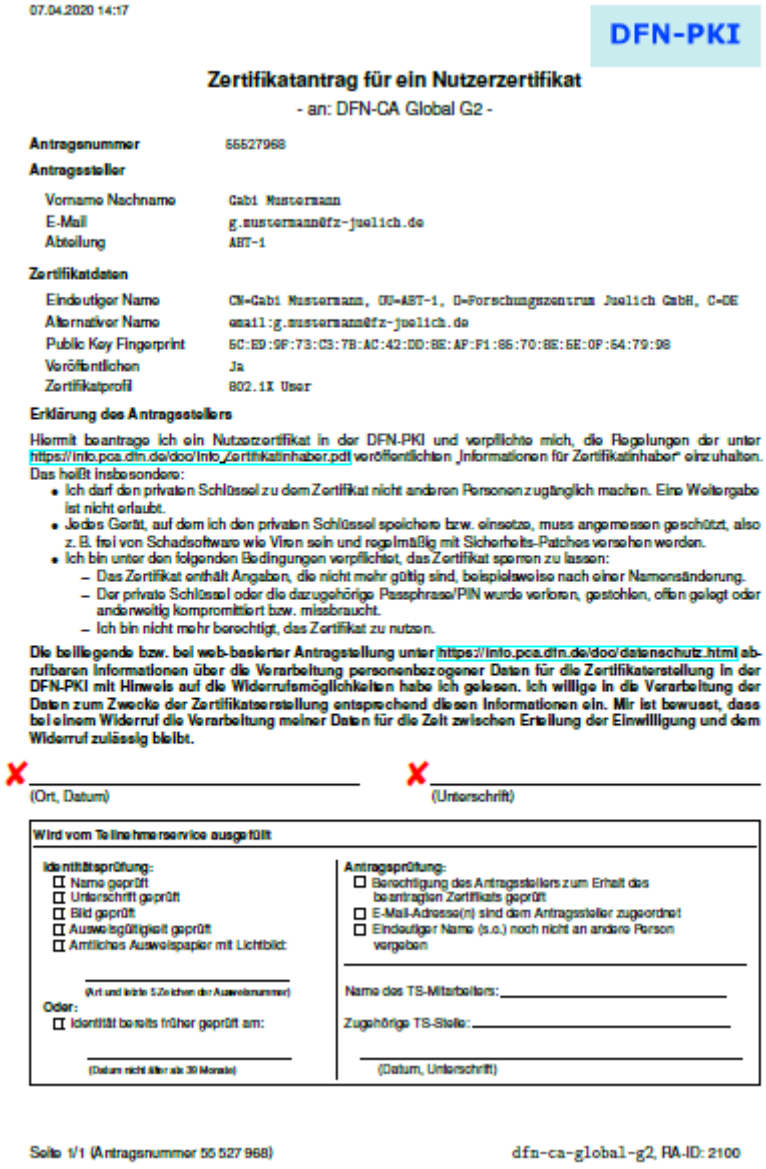
2. Die Frage nach der Webzugriffsbestätigung mit **Ja** beantworten



3. Auf der Folgeseite kann man die Angaben noch einmalprüfen und ggfs. ändern, danach: **Bestätigen**

4. Den **Zertifikatsantrag anzeigen** und **Öffnen,** um ihn auszudrucken.





07.04.2020 14:17

DFN-PKI

Zertifikatantrag für ein Nutzerzertifikat

- an: DFN-CA Global G2 -

Antragsnummer 55527968

Antragsteller

Vorname Nachname	Gabi Mustermann
E-Mail	g.mustermann@fz-juelich.de
Abteilung	ABT-1

Zertifikatdaten

Eindeutiger Name	CN=Gabi Mustermann, OU=ABT-1, O=Forschungszentrum Juelich GmbH, C=DE
Alternativer Name	email:g.mustermann@fz-juelich.de
Public Key Fingerprint	6C:ED:9F:73:C3:7B:AC:42:DD:8E:AF:F1:86:70:8E:6E:0F:54:79:98
Veröffentlichen	Ja
Zertifikatprofil	802.1X User

Erklärung des Antragstellers

Hiermit beantrage ich ein Nutzerzertifikat 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:

- Ich darf den privaten Schlüssel zu dem Zertifikat nicht anderen Personen zugänglich machen. Eine Weitergabe ist nicht erlaubt.
- Jedes Gerät, auf dem ich den privaten Schlüssel speichere bzw. einsetze, muss angemessen geschützt, also z. B. frei von Schadsoftware wie Viren sein und regelmäßig mit Sicherheits-Patches versehen werden.
- Ich bin unter den folgenden Bedingungen verpflichtet, das Zertifikat sperren zu lassen:
  - Das Zertifikat enthält Angaben, die nicht mehr gültig sind, beispielsweise nach einer Namensänderung.
  - Der private Schlüssel oder die dazugehörige Passphrase/PIN wurde verloren, gestohlen, offen gelegt oder anderweitig kompromittiert bzw. missbraucht.
  - Ich bin nicht mehr berechtigt, das Zertifikat zu nutzen.

Die beiliegende bzw. bei web-basierter Antragstellung unter https://info.pca.dfn.de/doc/datenschutz.html abrufbaren Informationen über die Verarbeitung personenbezogener Daten für die Zertifikatserstellung in der DFN-PKI mit Hinweis auf die Widerrufsmöglichkeiten habe ich gelesen. Ich willige in die Verarbeitung der Daten zum Zwecke der Zertifikatserstellung entsprechend diesen Informationen ein. Mir ist bewusst, dass bei einem Widerruf die Verarbeitung meiner Daten für die Zeit zwischen Erteilung der Einwilligung und dem Widerruf zulässig bleibt.

✘ _____ ✘ _____

(Ort, Datum) (Unterschrift)

Wird vom Teilnehmerservice ausgefüllt

Identitätsprüfung:
- ☐ Name geprüft
- ☐ Unterschrift geprüft
- ☐ Bild geprüft
- ☐ Ausweisgültigkeit geprüft
- ☐ Amtliches Ausweispapier mit Lichtbild:

_____
(Art und letzte 5 Zeichen der Ausweisnummer)

Oder:
- ☐ Identität bereits früher geprüft am:

_____
(Datum nicht älter als 39 Monate)

Antragsprüfung:
- ☐ Berechtigung des Antragstellers zum Erhalt des beantragten Zertifikats geprüft
- ☐ E-Mail-Adresse(n) sind dem Antragsteller zugeordnet
- ☐ Eindeutiger Name (s.o.) noch nicht an andere Person vergeben

_____

Name des TS-Mitarbeiters: _____

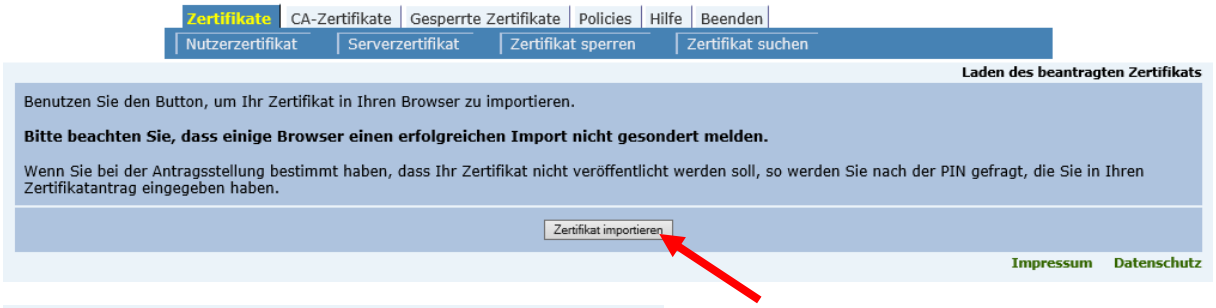
Zugehörige TS-Stelle: _____

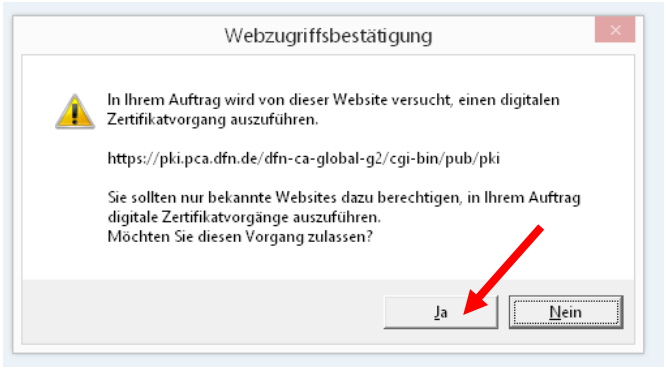
_____
(Datum, Unterschrift)

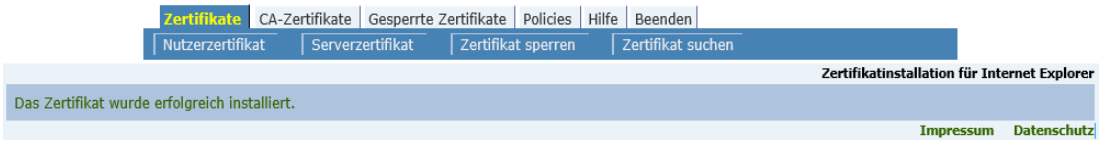
Seite 1/1 (Antragsnummer 55 527 968) dfn-ca-global-g2, RA-ID: 2100

5. Den unterschriebenen Antrag zum JSC-Dispatch (Teilnehmerservice) geben. Bei einem **Erstantrag** ist eine persönliche Authentifizierung mit Personalausweis beim JSC-Dispatch erforderlich. Dasselbe gilt bei einem **Wiederholungsantrag**, falls die letzte persönliche Authentifizierung länger als 39 Monate zurück liegt. Falls nicht, kann der Antrag auch zum Dispatch geschickt werden, dies kann per Post oder in einer vom Antragsteller elektronisch signierten Mail geschehen.
   Öffnungszeiten und Anschrift des Teilnehmerservices finden sich unter: https://www.fz-juelich.de/ias/jsc/DE/Leistungen/Dienstleistungen/Zertifikate/zertifikate_node.html . Die Anträge werden im JSC archiviert.
   Nach erfolgreicher Authentifizierung und Ausstellung des Zertifikats wird der Benutzer **per Mail** informiert. In dieser Mail findet sich auch der Link, mit dem das neue Zertifikat heruntergeladen werden kann.

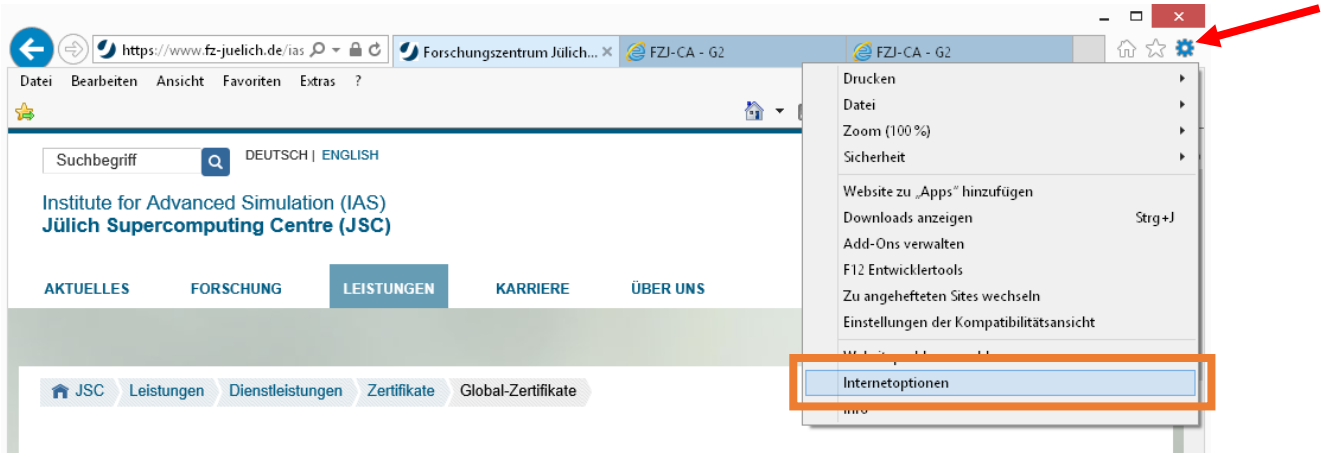
6. Dem Link zum neuen Zertifikat aus der Mail folgen (Internet Explorer!), **Zertifikat importieren** drücken und den **Webzugriff bestätigen.** Anschließend wird die erfolgreiche Installation bestätigt.

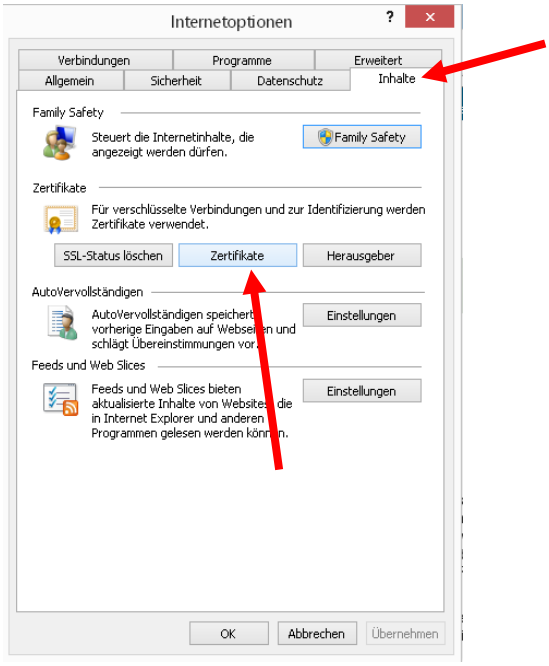


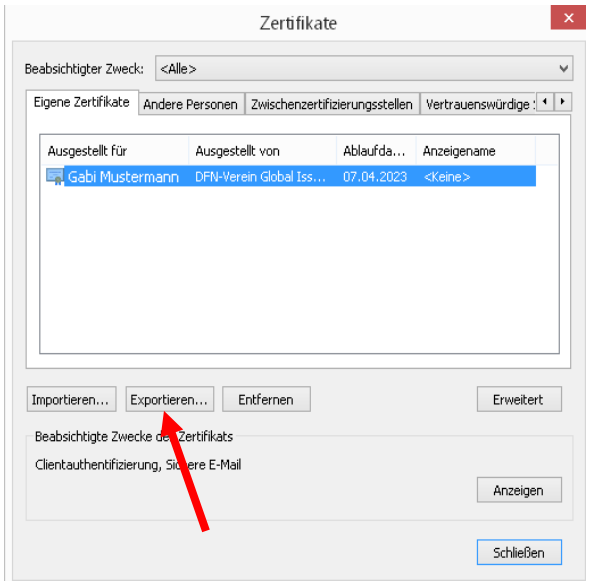


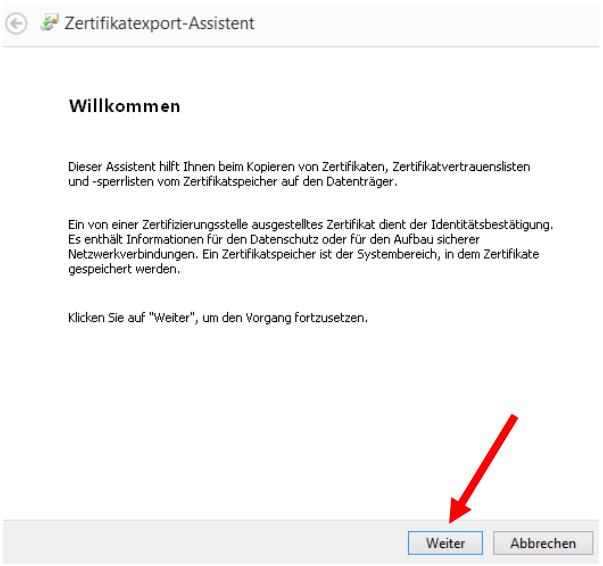


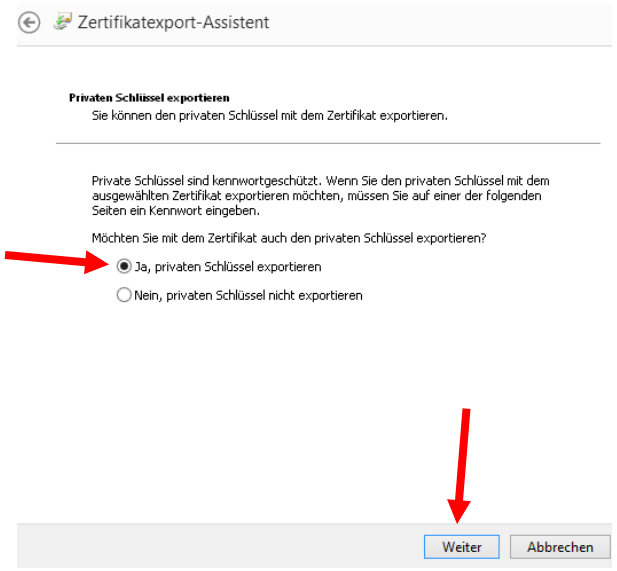
7. Das Zertifikat - einschließlich des geheimzuhaltenden **private Keys -** ist damit in den Windows-Zertifikatsspeicher eingebaut. Es sollte nun unbedingt eine Sicherungskopie dieser sensiblen Daten gemacht werden. Diese Kopie kann auch genutzt werden, um das Zertifikat in anderen Anwendungen oder auf einem weiteren Rechner einzusetzen. Diese Datei muss mit einem sicheren Passwort geschützt werden.
   Die Sicherungskopie erzeugt man am Besten mit dem Internet-Explorer wie in folgenden Bildern zu sehen.

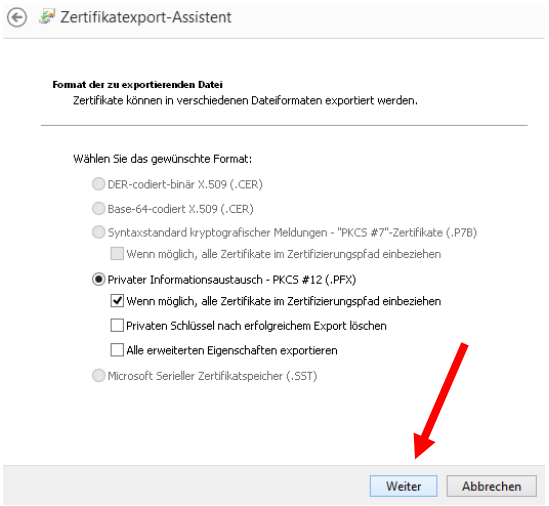

https://www.fz-juelich.de/ias
Forschungszentrum Jülich...
FZJ-CA - G2
FZJ-CA - G2
Datei Bearbeiten Ansicht Favoriten Extras ?
Suchbegriff
DEUTSCH | ENGLISH
Institute for Advanced Simulation (IAS)
Jülich Supercomputing Centre (JSC)
AKTUELLES FORSCHUNG LEISTUNGEN KARRIERE ÜBER UNS
JSC Leistungen Dienstleistungen Zertifikate Global-Zertifikate
Drucken
Datei
Zoom (100 %)
Sicherheit
Website zu „Apps" hinzufügen
Downloads anzeigen Strg+J
Add-Ons verwalten
F12 Entwicklertools
Zu angehefteten Sites wechseln
Einstellungen der Kompatibilitätsansicht
Internetoptionen

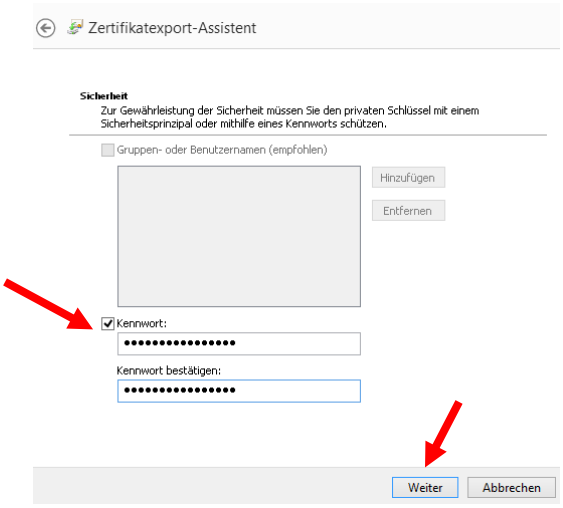

Internetoptionen
Verbindungen Programme Erweitert
Allgemein Sicherheit Datenschutz Inhalte
Family Safety
Steuert die Internetinhalte, die angezeigt werden dürfen.
Family Safety
Zertifikate
Für verschlüsselte Verbindungen und zur Identifizierung werden Zertifikate verwendet.
SSL-Status löschen Zertifikate Herausgeber
AutoVervollständigen
AutoVervollständigen speichert vorherige Eingaben auf Webseiten und schlägt Übereinstimmungen vor.
Einstellungen
Feeds und Web Slices
Feeds und Web Slices bieten aktualisierte Inhalte von Websites, die in Internet Explorer und anderen Programmen gelesen werden können.
Einstellungen
OK Abbrechen Übernehmen


Zertifikate
Beabsichtigter Zweck: <Alle>
Eigene Zertifikate Andere Personen Zwischenzertifizierungsstellen Vertrauenswürdige
Ausgestellt für Ausgestellt von Ablaufda... Anzeigename
Gabi Mustermann DFN-Verein Global Iss... 07.04.2023 <Keine>
Importieren... Exportieren... Entfernen Erweitert
Beabsichtigte Zwecke des Zertifikats
Clientauthentifizierung, Sichere E-Mail
Anzeigen
Schließen


Zertifikatexport-Assistent
Willkommen
Dieser Assistent hilft Ihnen beim Kopieren von Zertifikaten, Zertifikatvertrauenslisten und -sperrlisten vom Zertifikatspeicher auf den Datenträger.
Ein von einer Zertifizierungsstelle ausgestelltes Zertifikat dient der Identitätsbestätigung. Es enthält Informationen für den Datenschutz oder für den Aufbau sicherer Netzwerkverbindungen. Ein Zertifikatspeicher ist der Systembereich, in dem Zertifikate gespeichert werden.
Klicken Sie auf "Weiter", um den Vorgang fortzusetzen.
Weiter
Abbrechen


Zertifikatexport-Assistent
Privaten Schlüssel exportieren
Sie können den privaten Schlüssel mit dem Zertifikat exportieren.
Private Schlüssel sind kennwortgeschützt. Wenn Sie den privaten Schlüssel mit dem ausgewählten Zertifikat exportieren möchten, müssen Sie auf einer der folgenden Seiten ein Kennwort eingeben.
Möchten Sie mit dem Zertifikat auch den privaten Schlüssel exportieren?
Ja, privaten Schlüssel exportieren
Nein, privaten Schlüssel nicht exportieren
Weiter
Abbrechen


Zertifikatexport-Assistent
Format der zu exportierenden Datei
Zertifikate können in verschiedenen Dateiformaten exportiert werden.
Wählen Sie das gewünschte Format:
DER-codiert-binär X.509 (.CER)
Base-64-codiert X.509 (.CER)
Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B)
Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
Privater Informationsaustausch - PKCS #12 (.PFX)
Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
Privaten Schlüssel nach erfolgreichem Export löschen
Alle erweiterten Eigenschaften exportieren
Microsoft Serieller Zertifikatspeicher (.SST)
Weiter
Abbrechen



8. Abschließend legen Sie einen Namen für die Datei und den Ablageort fest.

9. Bitte denken Sie daran, dass Daten, die Ihnen verschlüsselt zugeschickt werden, **ausschließlich mit Ihrem privaten Schlüssel dekodiert werden können**. Aus diesem Grunde dürfen **auch abgelaufene Zertifikate und die dazu gehörenden privaten Schlüssel nicht gelöscht** werden. pfx-Dateien bzw. p12-Dateien sind geeignete Container, um Schlüssel sicher aufzubewahren.
   Generelle Informationen zum Thema Zertifikate und Verschlüsselung finden Sie beispielsweise in der TKI-365.
   https://www.fz-juelich.de/ias/jsc/DE/Leistungen/Dienstleistungen/Zertifikate/Dokumentation/_node.html