DFN CERT

deutsches forschungsnetz

Neues aus der DFN-PKI

71. Betriebstagung | 24.09.2019

Jürgen Brauckmann

Agenda

1. Ablauf der Gen. 1 DFN-PKI
2. Neue Antragsseiten
3. Wildcard-Zertifikate
4. Fazit

Ablauf der 1. Generation der DFN-PKI

Ablauf der 1. Generation der DFN-PKI

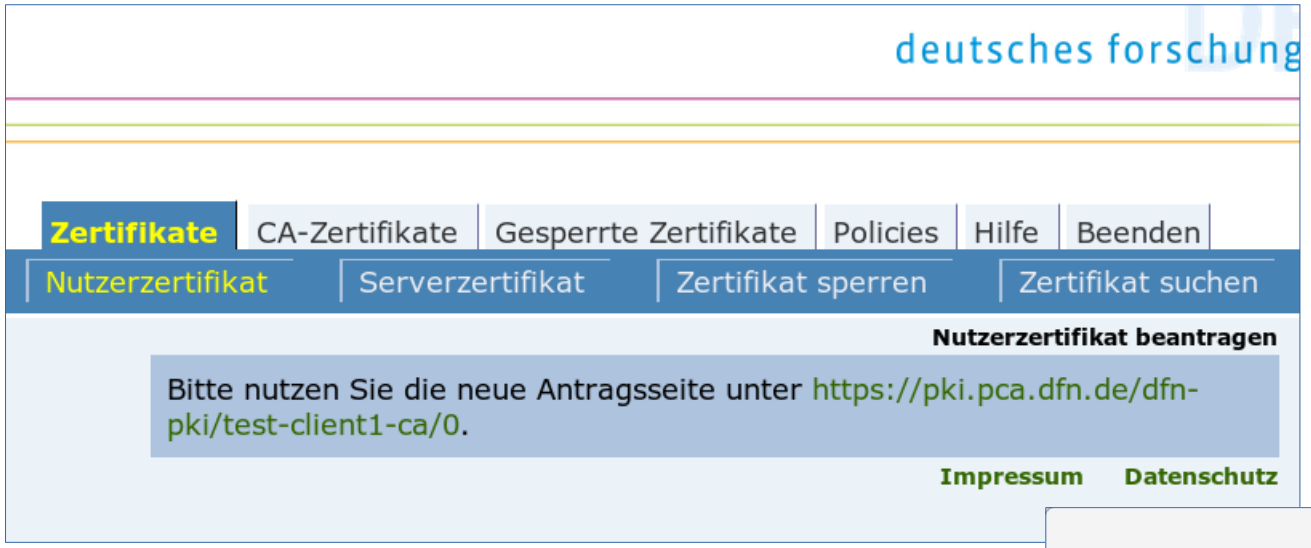
- Keine Katastrophen (bekannt geworden...)
- Danke für Ihre Aufmerksamkeit!
- Abgelaufene CAs:
  - Read-only-Zugang für Teilnehmerservice
    Wird abgeschaltet zum Zeitpunkt X >= H2/2020
  - Kein OCSP
  - Keine neuen CRLs
    Alte (abgelaufene) CRL weiterhin erhältlich

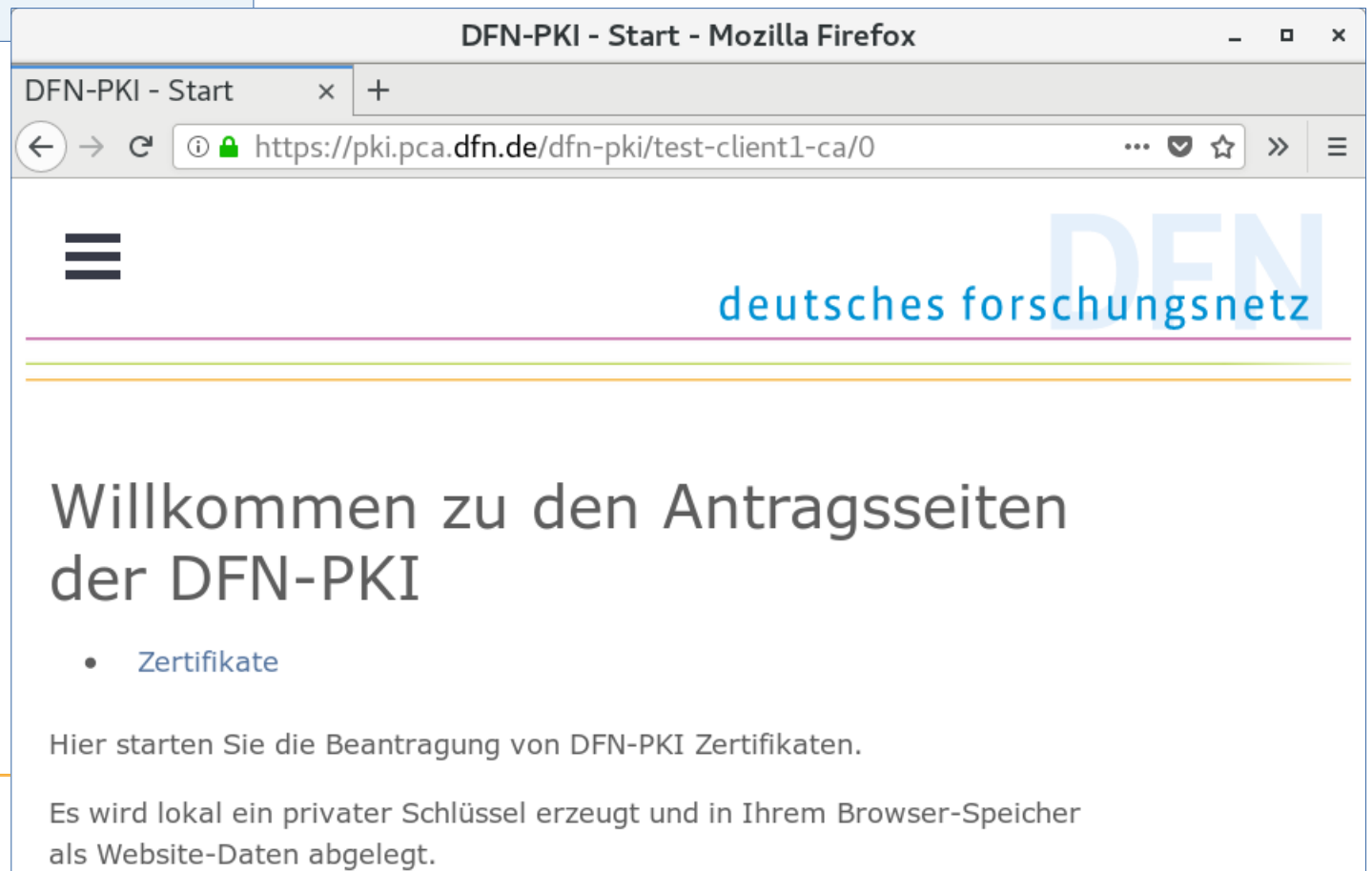
Neue Antragsseiten

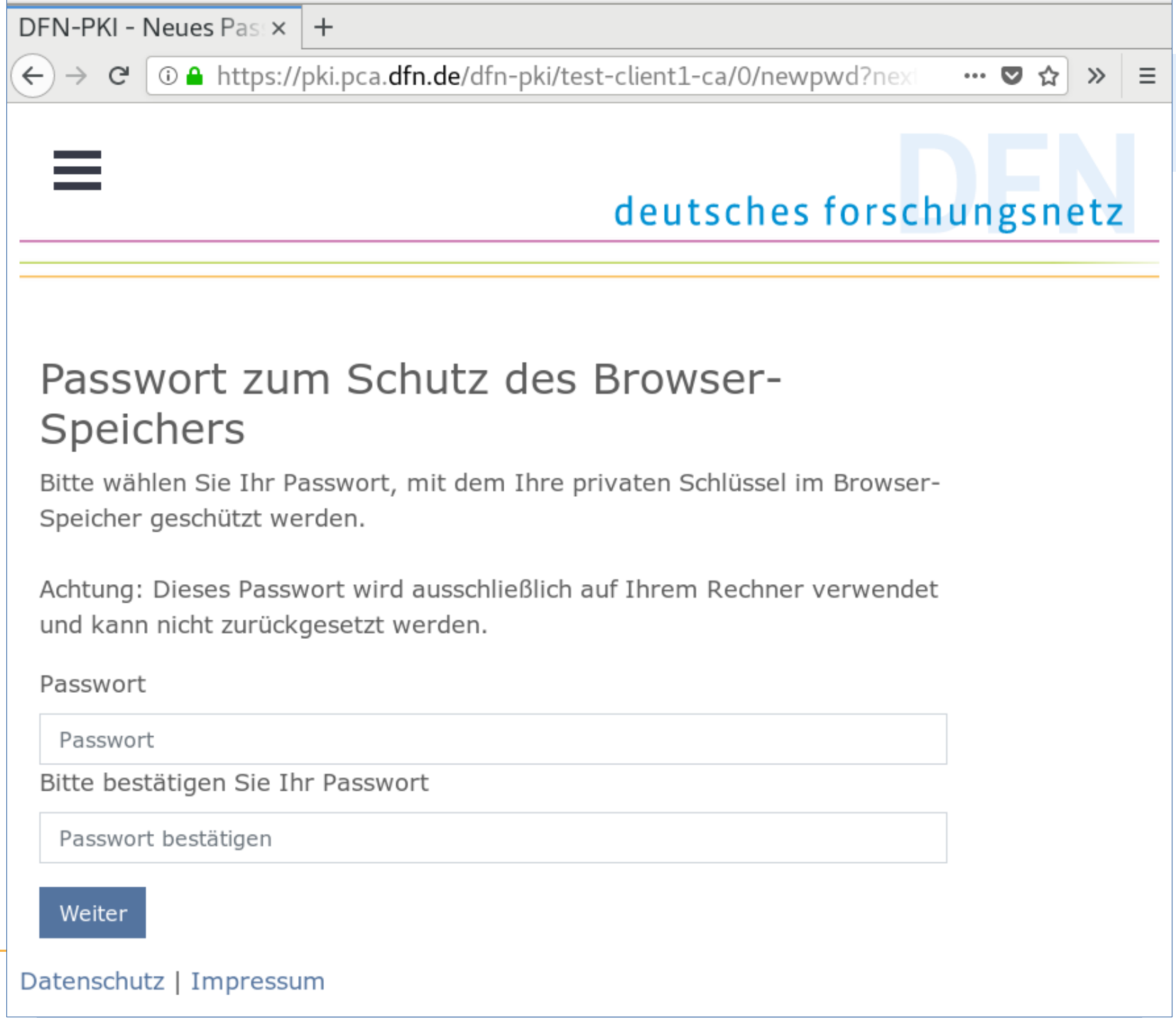
Neue Antragsseiten

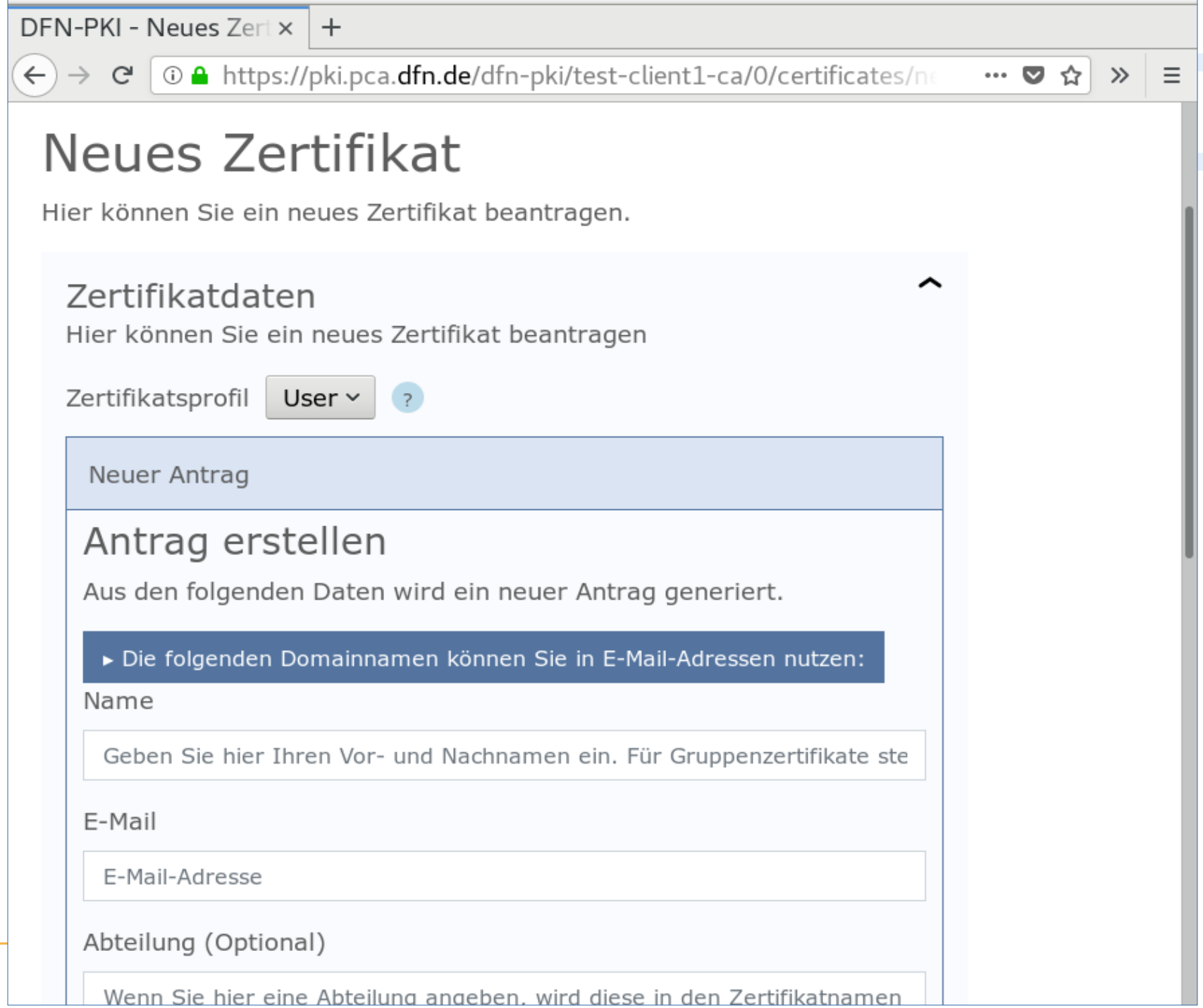
Generell:

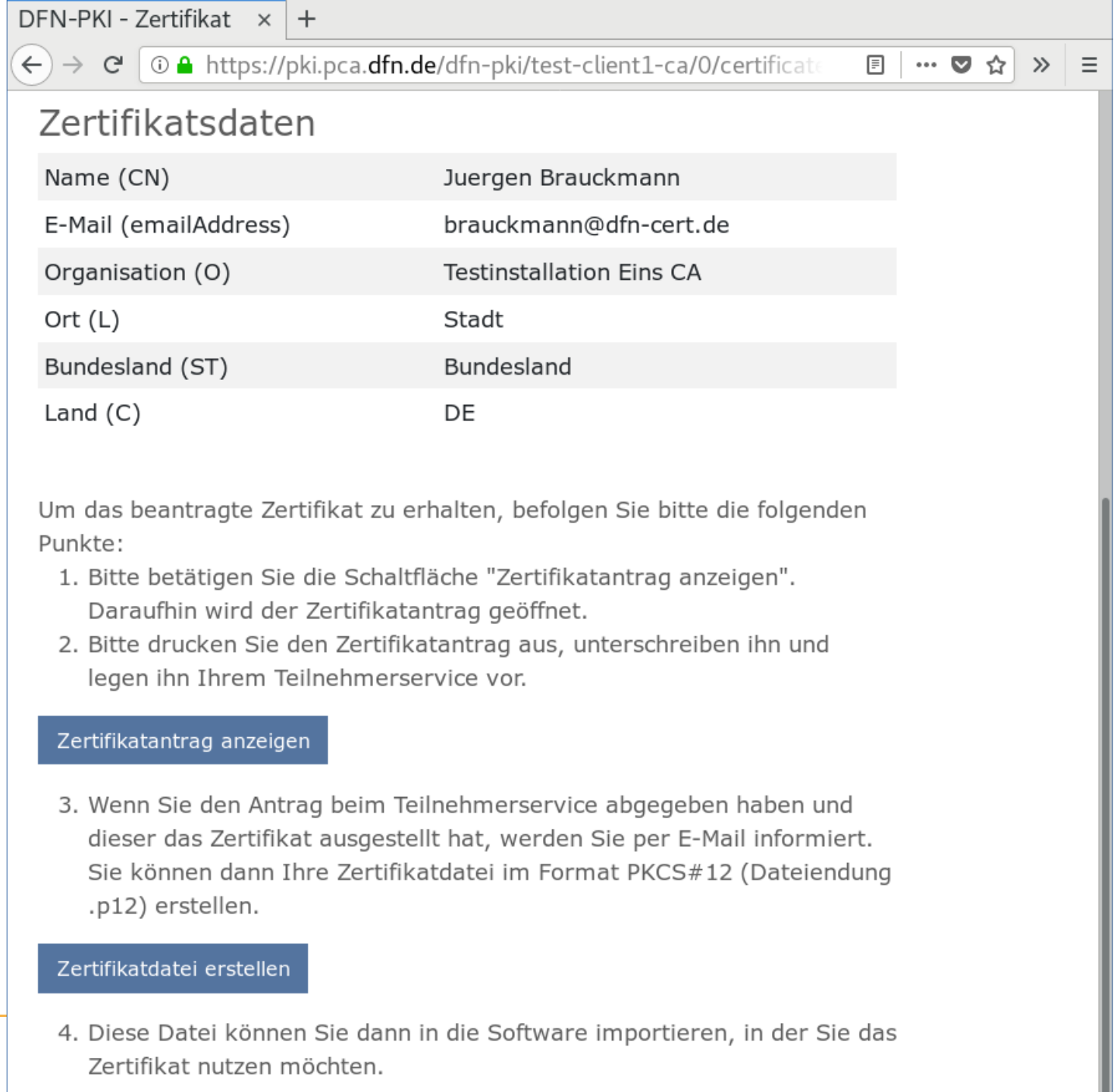
- JavaScript-Anwendung im Browser
- Umstellung u.a. erforderlich, da <KEYGEN> abgeschafft wird
  - Zeitdruck: Firefox 69 Anfang 09/2019, ca. 8 Wochen Vorlauf
- Nutzt SOAP-API der DFN-PKI
- Software-Architektur um Faktor 1000 besser => wartbar
- Unterstützt nicht jeden Konfigurations-Wildwuchs der alten Seiten


deutsches forschung
Zertifikate
CA-Zertifikate
Gesperrte Zertifikate
Policies
Hilfe
Beenden
Nutzerzertifikat
Serverzertifikat
Zertifikat sperren
Zertifikat suchen
Nutzerzertifikat beantragen
Bitte nutzen Sie die neue Antragsseite unter https://pki.pca.dfn.de/dfn-pki/test-client1-ca/0.
Impressum
Datenschutz


DFN-PKI - Start - Mozilla Firefox
DFN-PKI - Start
https://pki.pca.dfn.de/dfn-pki/test-client1-ca/0
deutsches forschungsnetz
Willkommen zu den Antragsseiten der DFN-PKI
Zertifikate
Hier starten Sie die Beantragung von DFN-PKI Zertifikaten.
Es wird lokal ein privater Schlüssel erzeugt und in Ihrem Browser-Speicher als Website-Daten abgelegt.


DFN-PKI - Neues Pas
https://pki.pca.dfn.de/dfn-pki/test-client1-ca/0/newpwd?nex
deutsches forschungsnetz
Passwort zum Schutz des Browser-Speichers
Bitte wählen Sie Ihr Passwort, mit dem Ihre privaten Schlüssel im Browser-Speicher geschützt werden.
Achtung: Dieses Passwort wird ausschließlich auf Ihrem Rechner verwendet und kann nicht zurückgesetzt werden.
Passwort
Passwort
Bitte bestätigen Sie Ihr Passwort
Passwort bestätigen
Weiter
Datenschutz | Impressum


DFN-PKI - Neues Zert
https://pki.pca.dfn.de/dfn-pki/test-client1-ca/0/certificates/ne
Neues Zertifikat
Hier können Sie ein neues Zertifikat beantragen.
Zertifikatdaten
Hier können Sie ein neues Zertifikat beantragen
Zertifikatsprofil
User
?
Neuer Antrag
Antrag erstellen
Aus den folgenden Daten wird ein neuer Antrag generiert.
▸ Die folgenden Domainnamen können Sie in E-Mail-Adressen nutzen:
Name
Geben Sie hier Ihren Vor- und Nachnamen ein. Für Gruppenzertifikate ste
E-Mail
E-Mail-Adresse
Abteilung (Optional)
Wenn Sie hier eine Abteilung angeben, wird diese in den Zertifikatnamen


DFN-PKI - Zertifikat
https://pki.pca.dfn.de/dfn-pki/test-client1-ca/0/certificat
Zertifikatsdaten
Name (CN) Juergen Brauckmann
E-Mail (emailAddress) brauckmann@dfn-cert.de
Organisation (O) Testinstallation Eins CA
Ort (L) Stadt
Bundesland (ST) Bundesland
Land (C) DE
Um das beantragte Zertifikat zu erhalten, befolgen Sie bitte die folgenden Punkte:
1. Bitte betätigen Sie die Schaltfläche "Zertifikatantrag anzeigen". Daraufhin wird der Zertifikatantrag geöffnet.
2. Bitte drucken Sie den Zertifikatantrag aus, unterschreiben ihn und legen ihn Ihrem Teilnehmerservice vor.
Zertifikatantrag anzeigen
3. Wenn Sie den Antrag beim Teilnehmerservice abgegeben haben und dieser das Zertifikat ausgestellt hat, werden Sie per E-Mail informiert. Sie können dann Ihre Zertifikatdatei im Format PKCS#12 (Dateiendung .p12) erstellen.
Zertifikatdatei erstellen
4. Diese Datei können Sie dann in die Software importieren, in der Sie das Zertifikat nutzen möchten.

Neue Antragsseiten

Aktueller Zustand:

- Funktioniert mit den meisten Browsern, auch auf Mobil-Geräten
- Edge inkompatibel

  (Opera/Windows tarnt sich scheinbar als Edge und wird auch abgelehnt)
- IE ebenfalls inkompatibel, altes Verfahren mit ActiveX noch aktiv
- Speicherung von privaten Schlüsseln im LocalStorage
  - vs. Private Fenster, Incognito-Modus, History-Löschen-on-exit, ...

Neue Antragsseiten

Ausblick:

- Beantragung von Serverzertifikaten
- Support für extern erzeugte PKCS#10-Anträge
- Option, die ohne LocalStorage auskommt?
- Fein-Tuning: Optional zweites E-Mail-Feld, OU-Eingabe abschaltbar, ...

Wildcard-Zertifikate

Wildcard-Zertifikate

- In der DFN-PKI seit 2015
- `*.gitlab.uni-pellworm.de`
- Aber **nicht** `www.*.uni-pellworm.de`
  (verboten per CA/Browser-Forum)
- Je nach Situation schlechte Idee: WILDCARD FÜR HAUPT-DOMAIN
  `(*.uni-pellworm.de)`

Wildcard-Zertifikate

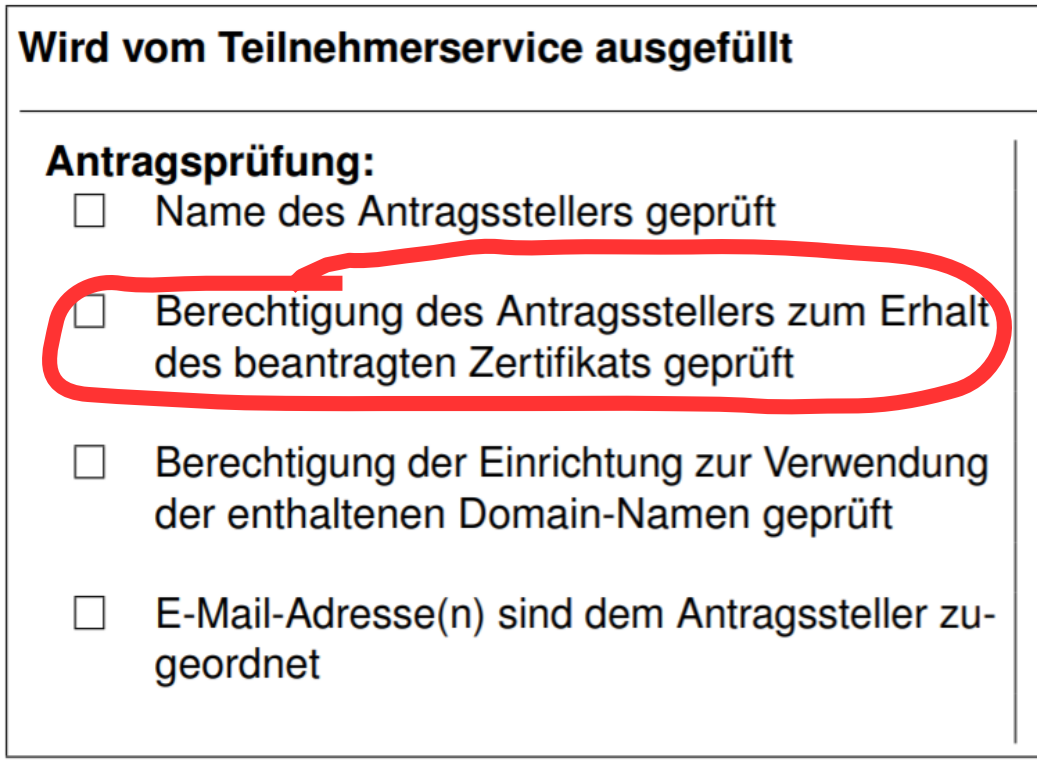
Bisheriger Prozess:

- Papierbasiert (Teilnehmer -> DFN-PCA)
- Nur für Anwendungen, die Wildcard-Zert. unbedingt benötigen
- Spezielle RA
- Unterschrift handlungsberechtigte Person
- Grund: Absprachen mit T-Systems, Erfahrungen sammeln

Wildcard-Zertifikate

Neu (ab Donnerstag, 26.09.):

- Wie normale Serverzertifikate ohne Spezialprozess möglich
- Hinweise Verwendungszweck bleiben (informativ, nur in den FAQ)
- Prüfung der „Berechtigung“ spannend, aber Problem der Teilnehmer



Wildcard-Zertifikate

Möglichkeit zur Steuerung:

- Setzen einer CAA-Policy

```
$ORIGIN hs-musterstadt.de
. CAA 0 issue "pki.dfn.de"
. CAA 0 issuewild ";"
```

- Allerdings: In delegierten Zonen überschreibbar

Fazit

Schnell noch ein Werbeblock.... .

Tutorien des DFN-CERT

- Datenschutz-Grundverordnung
  17.10.2019, Hamburg
- Weiterbildung zum Informationssicherheitsbeauftragten
  12-14.11.+10.-11.12., Hamburg
  12-14.05.+23.-25.06.2020
- 8. DFN-Konferenz Datenschutz
  05.12.-06.12.2019, **Achtung:** Berlin, Park Inn am Alexanderplatz
- 27. DFN-Konferenz „Sicherheit in vernetzten Systemen“
  24.02.-25.02.2020, Hamburg

Anmeldung/Weitere Informationen: https://www.dfn-cert.de

Fazit

- Neue Antragsseiten: In Bewegung!
- Wildcard-Zertifikate ohne Spezial-Prozess
- dfnpki-d@listserv.dfn.de
  Anmelden unter
  https://www.listserv.dfn.de/sympa/info/dfnpki-d =>

Blog: https://blog.pki.dfn.de

Haben Sie noch Fragen?

- Kontakt:

  DFN-PCA

  dfnpca@dfn-cert.de

  https://www.pki.dfn.de

  https://blog.pki.dfn.de