deutsches forschungsnetz

Version 5 (Dezember 2019)

Prüfung von Domainnamen und E-Mail-Adressen in der DFN-PKI

- Sicherheitsniveau Global -

Inhaltsverzeichnis

1 Einleitung....1
1.1 Domainnamen in Serverzertifikaten....1
1.1.1 Mögliche E-Mail-Adressen für die Domain-Freischaltung per E-Mail-Challenge-Response....2
1.1.2 Ablauf des E-Mail-Challenge-Response Verfahrens....2
1.1.3 Revalidierung von Domains....2
1.2 E-Mail-Adressen in Server- und Nutzerzertifikaten....3
1.2.1 Variante 1: Alle E-Mail-Adressen möglich....3
1.2.2 Variante 2: Nur E-Mail-Adressen auf der Liste der E-Mail-Domains sind möglich....3
2 Konfiguration....3
2.1 Download und Installation der Java RA-Oberfläche....3
2.2 Starten der Java RA-Oberfläche....3
2.3 Einrichten Ihres Zugangs....3
2.4 Hinzufügen eines neuen Domainnamens....4
2.5 Erlaubte Domainnamen für untergeordnete Teilnehmerservice-Stellen....5

1 Einleitung

1.1 Domainnamen in Serverzertifikaten

Jeder Teilnehmer der DFN-PKI kann Serverzertifikate nur für Domains ausstellen, für die der Inhaber oder der technische Ansprechpartner der Zertifikatvergabe zugestimmt hat. Um dies technisch sicherzustellen, wird von der DFN-PCA für jeden Teilnehmerservice (TS) eine Liste der zulässigen Domains vorgehalten. TS-Mitarbeiter haben die Möglichkeit, diese Liste einzusehen und zu bearbeiten, z. B. wenn eine Einrichtung eine neue Domain nutzt. Zertifikatanträge mit Domainnamen, die nicht auf dieser Liste stehen, werden bereits bei der Antragstellung mit einer Fehlermeldung abgewiesen.

Vor dem Eintragen eines neuen Domainnamens für Serverzertifikate muss der Teilnehmerservice sicherstellen, dass er berechtigt ist, diesen Domainnamen zu verwenden. Informationen hierzu finden sich in dem Dokument „Aufgaben des Teilnehmerservice in der DFN-PKI im Sicherheitsniveau Global[1]“ insb. in Abschnitt 4.1. Nach der Zustimmung des Domaininhabers kann der neue Domainname von allen Antragstellern verwendet werden.

Die Zustimmung des Domaininhabers wird über ein E-Mail-Challenge-Response-Verfahren eingeholt. Die technischen Systeme der DFN-PKI versenden eine E-Mail mit einem einmal verwendbaren, 30 Tage lang gültigen Link. Dieser muss vom Empfänger der E-Mail aufgerufen werden, damit der Teilnehmer die Domain in Serverzertifikaten der DFN-PKI verwenden kann.

Die Zustimmung ist 825 Tage lang gültig und berechtigt zur Ausstellung von beliebig vielen

1 https://www.pki.dfn.de/fileadmin/PKI/anleitungen/Aufgaben-TS-DFN-PKI.pdf

Zertifikaten. Vor Ablauf dieser Frist muss der Teilnehmerservice die E-Mail-Challenge-Response wiederholen lassen („Revalidierung"), wenn die Domain weiterhin in neuen Zertifikaten in der DFN-PKI verwendet werden soll. Bereits ausgestellte Zertifikate behalten auch nach Ablauf der 825 Tage ihre Gültigkeit (im Rahmen der im Zertifikat angegebenen Laufzeit).

1.1.1 Mögliche E-Mail-Adressen für die Domain-Freischaltung per E-Mail-Challenge-Response

Für die zu verwendende E-Mail-Adresse des Domaininhabers oder technischen Ansprechpartners gibt es mehrere, in der Zertifizierungsrichtlinie festgelegte Möglichkeiten:

1. Es kann die E-Mail-Adresse im SOA-Record der DNS-Zone, in der die Domain liegt, verwendet werden.

2. Es kann eine E-Mail-Adresse aus `administrator@`, `admin@`, `webmaster@`, `postmaster@`, `hostmaster@` verwendet werden. Der Domain-Teil kann dabei der angefragte Domainteil bis zur Ebene direkt unter einer Top-Level-Domain sein. Zum Beispiel sind für `sub1.example.org` möglich: `admin@sub1.example.org` und `admin@example.org`

3. Ausnahmsweise kann die DFN-PCA Kontakt- oder Tech-C E-Mail-Adressen aus den verfügbaren WHOIS-Systemen ermitteln. Diese Methode ist allerdings mit hohem manuellem Aufwand verbunden und aufgrund der zunehmenden Einschränkungen beim Zugriff auf WHOIS immer seltener möglich.

Andere E-Mail-Adressen sind nicht zulässig.

Die zu verwendende E-Mail-Adresse wird in den Fällen 1. und 2. direkt beim Eintragen einer neuen Domain in die Java RA-Oberfläche durch den Teilnehmerservice-Mitarbeiter bestimmt.

1.1.2 Ablauf des E-Mail-Challenge-Response Verfahrens

Das technische System der DFN-PKI verschickt ausschließlich an die eingetragene Adresse eine E-Mail (kein Cc: an den Teilnehmerservice o.ä.). In dieser E-Mail ist ein Link enthalten, der vom Empfänger, also dem Domaininhaber oder technischen Ansprechpartner, aufgerufen werden muss.

Nach Aufruf des Links und Anwahl des Buttons „Bestätigen" in der daraufhin dargestellen Web-Seite kann die Domain sofort in Anträge für Serverzertifikate aufgenommen werden.

Über die Bestätigung (oder Ablehnung) wird an die bei der DFN-PKI hinterlegte Teilnehmerservice-Kontakt-Mailadresse, an die auch Kopien der Zertifikatauslieferungs- und Ablaufwarnmails verschickt werden, eine Nachricht versandt.

1.1.3 Revalidierung von Domains

Eine Freischaltung einer Domain ist für 825 Tage gültig, d.h. innerhalb dieses Zeitraumes kann der Teilnehmer beliebig viele Zertifikate mit dieser Domain ausstellen. Nach Ablauf dieser Zeit ist keine Ausstellung von neuen Zertifikaten mehr möglich. Bereits ausgestellte Zertifikate behalten ihre Gültigkeit.

Um eine Revalidierung von bestehenden Domains anzustoßen, muss der Teilnehmerservice selbst tätig werden. In der Java RA-Oberfläche findet sich in der Liste der freigeschalteten Domains auch das Datum, bis wann die jeweilige Domain verwendet werden kann. Der Teilnehmerservice muss regelmäßig in dieser Liste für ablaufende Domains erneut eine E-Mail-Adresse auswählen, an die dann eine Challenge-Response-E-Mail verschickt wird.

Der Vorgang stellt sich für den Empfänger der E-Mail genau wie bei der ersten Freischaltung dar.

1.2 E-Mail-Adressen in Server- und Nutzerzertifikaten

1.2.1 Variante 1: Alle E-Mail-Adressen möglich

In der DFN-PKI können standardmäßig alle E-Mail-Adressen in Zertifikate aufgenommen werden, die dem Antragsteller zugeordnet sind. Die Zuordnung muss stets zum Zeitpunkt der Genehmigung des Zertifikatantrags durch den Teilnehmerservice sichergestellt werden. Es gibt grundsätzlich keine Einschränkung der Domains, aus denen die E-Mail-Adressen stammen können.

Der Teilnehmerservice wird bei seiner Prüfaufgabe technisch unterstützt, indem für E-Mail-Adressen aus Domains, die nicht in einer vorab zu konfigurierenden Liste der zugelassenen E-Mail-Domains enthalten sind, je Zertifikatantrag individuelle Bestätigungs-E-Mails verschickt werden. Ohne Aufruf des in der E-Mail enthaltenen Bestätigungs-Links durch den Antragsteller können die zugehörigen Zertifikatanträge nicht genehmigt werden.

Möchte der Teilnehmerservice E-Mail-Adressen aus bestimmten Domains auf andere Art als mit einer individuellen Bestätigungs-E-Mail prüfen, so kann er diese Domains auf die Liste der zugelassenen E-Mail-Domains setzen. Ein Beispiel für eine Domain, bei der sich dieses anbietet, ist die Haupt-Domain einer Einrichtung, bei der der Teilnehmerservice z. B. über interne Adresslisten die Zuordnung einer E-Mail-Adresse zum Antragssteller einfach nachschlagen kann.

Die Aufnahme von Domains in die Liste der zugelassenen E-Mail-Domains geschieht analog zur Freischaltung von Domainnamen für Serverzertifikate, siehe Abschnitt 1.1.

1.2.2 Variante 2: Nur E-Mail-Adressen auf der Liste der E-Mail-Domains sind möglich

Alternativ zur Variante 1 kann das technische System von der DFN-PCA auch so konfiguriert werden, dass ausschließlich E-Mail-Adressen aus Domains von der Liste der zugelassenen E-Mail-Domains von den Antragsseiten akzeptiert werden. In diesem Fall ist der Mechanismus zur Versendung von Bestätigungs-E-Mails deaktiviert.

Wenn Sie hieran Interesse haben, wenden Sie sich bitte an dfnpca@dfn-cert.de.

2 Konfiguration

2.1 Download und Installation der Java RA-Oberfläche

- Sie benötigen eine Java-Laufzeitumgebung OpenJDK ab Version 11. Sie können diese unter jdk.java.net herunterladen.
- Die aktuelle Version der Java RA-Oberfläche können Sie als ZIP-Datei von https://blog.pki.dfn.de/tag/guira-releases herunterladen. Die ZIP-Datei enthält Installationshinweise für Windows, Linux und MacOSX.

2.2 Starten der Java RA-Oberfläche

- Gestartet wird die Java RA-Oberfläche über ein/e in der ZIP-Datei enthaltene/s Shell-Script (Linux, MacOSX) bzw. Batch-Datei (Windows).
- Gegebenenfalls muss die verwendete Startdatei vor dem Start noch an die lokalen Gegebenheiten angepasst werden, siehe Installationshinweise.

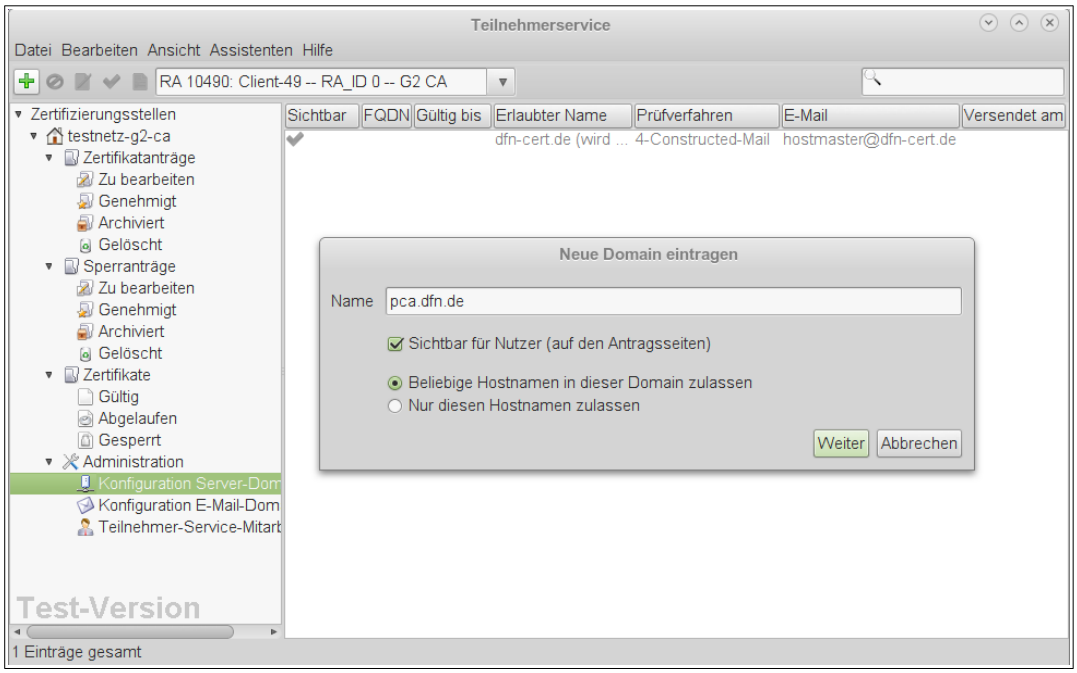
2.3 Einrichten Ihres Zugangs

- Beim ersten Start der Software werden Sie nach dem TS-Mitarbeiter-Zertifikat gefragt, das entweder in Form einer PKCS#12-Datei oder auf einer Smartcard/USB-Crypto-To-

ken vorliegen muss.

- Um Ihr TS-Mitarbeiter-Zertifikat im PKCS#12-Format zu verwenden, exportieren Sie dieses aus Ihrem Webbrowser:
  - *Firefox:* Bearbeiten → Einstellungen → Erweitert → Verschlüsselung → Zertifikate anzeigen → Ihre Zertifikate → TS-Mitarbeiter-Zertifikat auswählen → Sichern...
  - *Internet Explorer:* Extras → Internetoptionen → Inhalte → Zertifikate → Eigene Zertifikate → TS-Mitarbeiter-Zertifikat auswählen → Exportieren... → Weiter → „Ja, privaten Schlüssel exportieren"
- Um Ihr TS-Mitarbeiter-Zertifikat alternativ von einer Smartcard/Crypto-Token zu nutzen, geben Sie den Pfad zu der PKCS#11-Bibliothek des Herstellers ein (z. B. *etpkcs11.dll* für ein eToken unter Windows).
- Wenn Sie kein TS-Mitarbeiter-Zertifikat haben oder ein neues benötigen, melden Sie sich bitte unter dfnpca@dfn-cert.de. Dazu muss uns eine Benennung zum Teilnehmerservice-Mitarbeiter vorliegen.

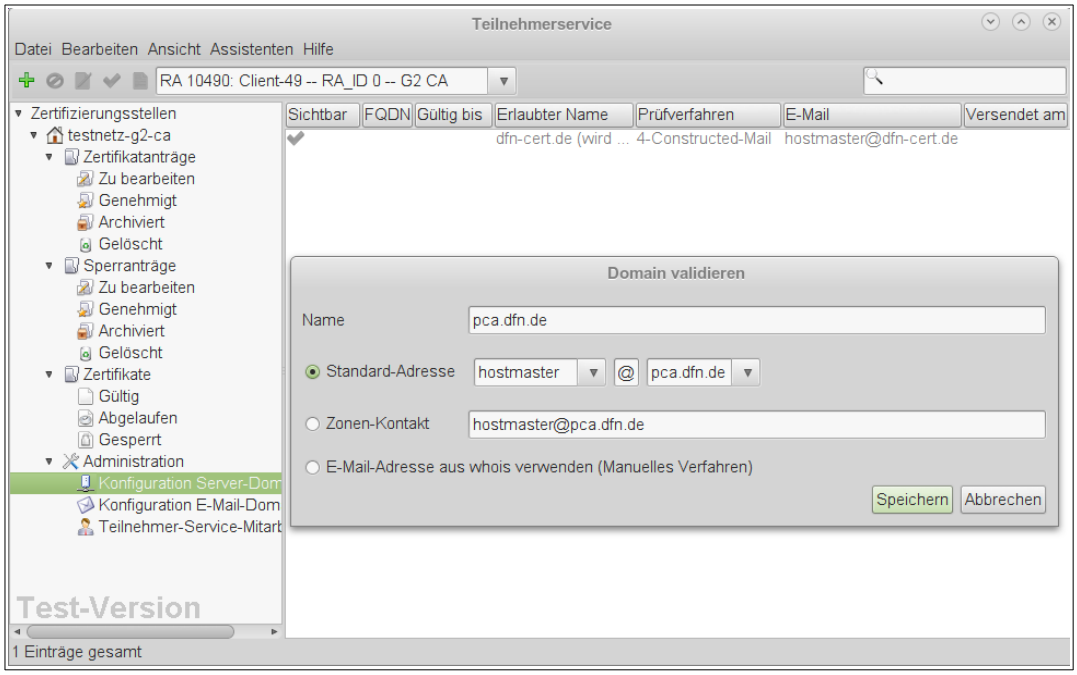
2.4 Hinzufügen eines neuen Domainnamens



1. Wählen Sie unter "Administration" die entsprechende Kategorie aus:
   - Unter "**Konfiguration Server-Domains**" tragen Sie Domainnamen ein, die im SubjectDN (CN-Attribut) oder im alternativen Namen (SubjectAlternativeName vom Typ „DNS") von Serverzertifikaten verwendet werden dürfen.
   - Unter "**Konfiguration E-Mail-Domains**" tragen Sie Domainnamen ein, die in E-Mail-Adressen im SubjectDN (emailAddress-Attribut) oder im alternativen Namen (SubjectAlternativeName vom Typ „email") von Nutzer- bzw. Serverzertifikaten verwendet werden können, *ohne dass* je Zertifikatantrag eine individuelle Bestätigungs-E-Mail an diese versendet wird.
2. Betätigen Sie die Schaltfläche mit dem Pluszeichen, oder klicken Sie mit der rechten Maustaste in die freie Fläche des rechten Fensters.
3. Tragen Sie den neuen Domainnamen in dem erscheinenden Dialog ein.
4. Wählen Sie, ob der Domainname auf den Antragsseiten sichtbar sein soll. Ein nicht

sichtbarer Domainname kann trotzdem beantragt werden und ist hilfreich, wenn dieser nur intern verwendet wird oder aus anderen Gründen nicht publik werden soll. (Bitte beachten: Diese Option legt nicht die Veröffentlichung der zu der Domain ausgestellten Zertifikate fest!)

5. Legen Sie fest, ob dem eingetragenen Namen beliebige Subdomains und/oder Hostnamen vorangestellt werden dürfen. Wenn Sie „nur diesen Hostnamen zulassen" wählen, wird der Eintrag mit einem Haken in der Spalte „FQDN" in der Liste angezeigt. In diesem Fall ist nur die Beantragung mit genau diesem Hostnamen möglich. Es ist nach der Beantragung nicht mehr möglich, diese Einstellung zu ändern. Falls Sie diese Einstellung dennoch ändern möchten, müssen Sie den Eintrag löschen und neu beantragen.



6. Im anschließenden Dialog „Domain validieren" treffen Sie die Auswahl, über welche E-Mail-Adresse die Zustimmung des Domaininhabers oder technischen Ansprechpartners eingeholt werden soll. Eine Erläuterung der möglichen Adressen wird in Abschnitt 1.1.1 gegeben.
7. Speichern Sie den neuen Domainnamen.
8. In der Übersicht werden die konfigurierten Domainnamen angezeigt.
9. Neue Domains können nach der Zustimmung des Domaininhabers verwendet werden. Bis dahin kann der Domainname nicht geändert, sondern nur gelöscht werden und wird mit dem Status „Wird geprüft" angezeigt.

2.5 Erlaubte Domainnamen für untergeordnete Teilnehmerservice-Stellen

Wenn Ihre CA untergeordnete Teilnehmerservice-Stellen enthält, kann standardmäßig nur die Haupt-TS (RA_ID 0) die Domainnamen für alle TS bearbeiten. Diese kann die zu bearbeitende Unter-TS aus einer Liste auswählen.

Sollen untergeordnete TS Domainnamen selbstständig eintragen können, wenden Sie sich bitte an dfnpca@dfn-cert.de.