

**Anleitung
für
Teilnehmerservice-Mitarbeiter
zur Nutzung
der
JAVA RA-Oberfläche
der
DFN-PKI**

Kontakt:

Allgemeine Fragen zur DFN-PKI: pki@dfn.de

Technische Fragen zur DFN-PKI: dfnpca@dfn-cert.de

Einführung	3
1 Voraussetzungen	4
2 Einrichten der CA mit dem TS-Operator Zertifikat	4
3 Arbeiten mit der Java RA-Oberfläche	4
4 Assistenten	8
5 Weitere Dokumentationen	8

Einführung

Mit der JAVA RA-Oberfläche steht Ihnen ein Werkzeug zur Verfügung, das Sie bei den Aufgaben des DFN-PKI Teilnehmerservice (TS) unterstützt, wie zum Beispiel bei der

- Genehmigung von Zertifikatanträgen;
- Sperrung von Zertifikaten;
- Freischaltung zusätzlicher Domains für Zertifikate;
- Benennung und Abmeldung von Teilnehmerservice-MitarbeiterInnen; sowie der
- Erstellung von Schulungsnachweisen für Teilnehmerservice-MitarbeiterInnen

Die Oberfläche bietet Ihnen dazu unterhalb der CA vier verschiedene Menüpunkte zur Bearbeitung an – Zertifikatanträge, Sperranträge, Zertifikate, Administration.

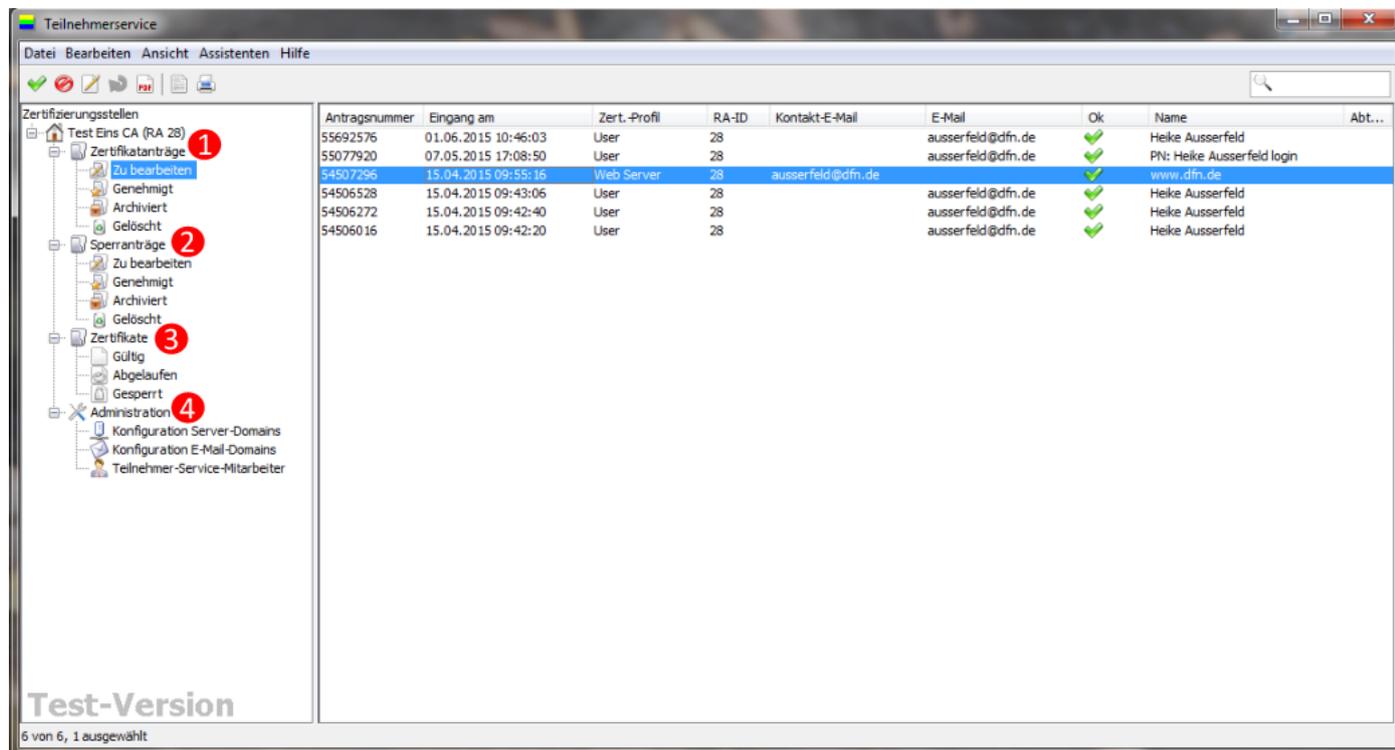


Abbildung 1: JAVA RA-Oberfläche

1 Voraussetzungen

Für die Nutzung der JAVA RA-Oberfläche (im Folgenden kurz RA-Oberfläche genannt) benötigen Sie eine installierte Oracle Java Runtime Environment (JRE) Version 7 oder 8. Falls Sie spezielle angepasste Assistenten in der RA-Oberfläche im Einsatz haben, die eine Schlüsselgenerierung durch die RA-Oberfläche vornehmen und dabei eine Schlüssel hinterlegung in einer zentralen Datenbank durchführen, müssen zusätzlich die Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Dateien installiert sein.

Außerdem benötigen Sie ein Teilnehmerservice-Operator Zertifikat aus der DFN-PKI in Form einer PKCS#12-Datei (üblicherweise mit .p12 oder .pfx Dateiendung) inklusive der vollständigen CA-Kette. Die Anleitung zur Beantragung dieses Zertifikats erhalten Sie mit einer E-Mail nach der vollständigen Konfiguration des Teilnehmerservice für Ihre Einrichtung.

2 Einrichten der CA mit dem TS-Operator Zertifikat

Beim ersten Aufruf der RA-Oberfläche startet automatisch ein Assistent, der Sie bei der Konfiguration der RA-Oberfläche für Ihre Einrichtung unterstützt. Dabei werden Sie aufgefordert, die PKCS#12-Datei anzugeben, die Ihr Teilnehmerservice-Operator Zertifikat enthält.

Sofern Sie weitere Teilnehmerservice-Operator Zertifikate für andere CAs aus der DFN-PKI erhalten haben, können Sie über den Menüpunkt **Datei→neue CA** weitere Teilnehmerservice-Konfigurationen anlegen. Über den Menüpunkt **Bearbeiten→Einstellungen** können bereits angelegte Teilnehmerservicekonfigurationen bearbeitet werden.

3 Arbeiten mit der Java RA-Oberfläche

Die RA-Oberfläche ist in Form einer Baum-Hierarchie strukturiert. Sie enthält für jeden konfigurierten Teilnehmerservice die Kategorien Zertifikatanträge (1), Sperranträge (2), Zertifikate (3) und Administration (4) (siehe Abbildung 1). Die voreingestellte RA hängt vom konfigurierten TS-Operator-Zertifikat ab. Bei der Konfiguration der Domains (4) kann über eine Dropdown-Liste unterhalb der Menüleiste die zu konfigurierende RA ausgewählt werden, sofern das genutzte TS-Operator-Zertifikat der Haupt-RA zugeordnet ist und unter dieser CA mehrere RAs für die Einrichtung konfiguriert wurden.

Sofern ein TS-Operator Zertifikat der Haupt-RA konfiguriert wurde, werden sowohl die Einträge der Haupt-RA als auch aller Unter-RAs angezeigt.

Durch Navigation im Zertifizierungsstellenbaum werden die einzelnen Kategorien geöffnet und angezeigt. Folgende Aktionen sind möglich:

Icon	Kategorie	Aktion	auch im Kontextmenü verfügbar	Mehrfachauswahl
	Zertifikatanträge→ Zu bearbeiten	Antrag genehmigen	ja	ja
	Sperranträge→ Zu bearbeiten			
	Zertifikatanträge→ Zu bearbeiten	Antrag als PDF anzeigen	ja	ja
	Zertifikate→ gültig	Zertifikat sperren	ja	ja
	Administration→ Teilnehmer-Service-Mitarbeiter	TS-Operator-Zertifikat sperren		
	Administration→ Teilnehmer-Service-Mitarbeiter	Formular (PDF) zur Benennung von TS-Mitarbeitern anzeigen	ja	nein
	Administration→ Konfiguration Server-Domains Konfiguration E-Mail-Domains	Neue Domain zur Freischaltungsprüfung eintragen - siehe auch Prüfung von Domainnamen in der DFN-PKI	ja	ja
	Zertifikatanträge (alle)	Antrag anzeigen / bearbeiten	ja	nein
	Sperranträge (alle)			
	Administration → Konfiguration ServerDomains Konfiguration E-Mail-Domains	Domain-Eintrag bearbeiten	ja	nein
	Zertifikate (alle)	Exportiert die ausgewählten Zertifikate in eine Datei	ja	ja

Icon	Kategorie	Aktion	auch im Kontextmenü verfügbar	Mehrfachauswahl
	Zertifikatanträge→ Zu bearbeiten	Antrag löschen	ja	ja
	Sperranträge→ Zu bearbeiten			
	Administration→ Teilnehmer-Service-Mitarbeiter	Formular (PDF) zum Abmelden eines/r TS-MitarbeiterIn erstellen und gleichzeitig TS-Operator-Zertifikat sperren	ja	ja
	Administration → Konfiguration Server-Domains Konfiguration E-Mail-Domains	Domain-Eintrag löschen	ja	ja
	Zertifikatanträge (alle)	Listenansicht drucken	ja	ja
	Sperranträge (alle)			
	Zertifikate (alle)			
	Administration → Teilnehmer-Service-Mitarbeiter	TS-Schulungsnachweis (PDF) erstellen		
	Zertifikatanträge→ Archiviert Gelöscht	Antrag erneuern	ja	ja

Icon	Kategorie	Aktion	auch im Kontextmenü verfügbar	Mehrfachauswahl
	Zertifikatanträge (alle)	Listenselektion in eine CSV-Datei exportieren	ja	Ja
	Sperranträge (alle)			
	Zertifikate (alle)			
	Administration → Konfiguration ServerDomains Konfiguration E-Mail-Domains			
	Zertifikate (alle)	Zeigt Details über das ausgewählte Zertifikat an	ja	nein
	Administration → Teilnehmer-Service-Mitarbeiter			

4 Assistenten

In der Standardkonfiguration der RA-Oberfläche gibt es einen Assistenten (Menüpunkt Assistenten) zum Erstellen von Server-Zertifikaten samt zugehörigem privaten Schlüssel. Dieser Assistent fragt zunächst die gängigen Zertifikatparameter ab:

- FQDN des Servers (CN-Attribut)
- Optionale zusätzliche Namen (FQDNs) für den SubjectAlternativeName
- Abteilungsname (OU-Attribut)
- Name des Antragstellers
- E-Mail-Adresse des Antragstellers
- Art des Servers (Auswahl des Zertifikatprofils)
- Namensraum für den SubjectDN (C-, ST-, L- und O-Attribute, ggf. vordefinierte OU-Attribute)
- Passwort zum Schutz des erzeugten geheimen Schlüssels
- Format- und Speicheroptionen für das ausgestellte Zertifikat und das Schlüsselmaterial

Danach erzeugt der Assistent mit diesen Angaben einen Zertifikatantrag samt Antragsformular (PDF) zum Ausdrucken, Unterschreiben und Archivieren, genehmigt diesen und speichert Schlüssel und Zertifikat in ein auszuwählendes Verzeichnis.

5 Weitere Dokumentationen

- [FAQs](#)
- [Aufgaben des Teilnehmerservice \(TS\) in der DFN-PKI im Sicherheitsniveau Global](#)
- [DFN-PKI Blog](#)
- [Prüfung von Domainnamen in der DFN-PKI](#)
- [DFN-PKI Zertifikatsprofile](#)