Bundesverwaltungsamt

Referat D III 1 – Registermodernisierung; Anschlussunterstützung

Vertiefungsleitfaden für die Beschaffung von V-PKI Zertifikaten für Data Consumer und Data Provider für die Anbindung an das Nationale Once-Only-Technical-System (NOOTS)

Version 2.0
09.09.2026

Das vorliegende Dokument wurde durch das Bundesverwaltungsamt in Zusammenarbeit mit der Firma Dataport AöR erstellt.

Ansprechpartner/-in:

Referat D III 1: Registermodernisierung; Anschlussunterstützung
Bundesverwaltungsamt
E-Mail: registermodernisierung@bva.bund.de

Inhaltsverzeichnis

1. Übersicht

Im Zuge des Anschlusses an das NOOTS werden aus Gründen der IT-Sicherheit verschiedene Zertifikate der V-PKI/ DOI-CA benötigt.

Data Provider (DP) benötigen mindestens drei Zertifikate:

- ein personenbezogenes Zertifikat der V-PKI/DOI-CA (produktiv) für die Registrierung am NOOTS
- zwei gruppenbezogene Zertifikate der V-PKI/DOI-CA als TLS-Server-Zertifikat des SAK-DP

Data Consumer (DC) benötigen insgesamt mindestens fünf Zertifikate:

- ein personenbezogenes Zertifikat der V-PKI/DOI-CA (produktiv) für die Registrierung am NOOTS
- zwei gruppenbezogene Zertifikate der V-PKI/DOI-CA als TLS-Client-Zertifikat des SAK-DC
- zwei gruppenbezogene Zertifikate der V-PKI/DOI-CA als Verschlüsselungszertifikat des SAK-DC

Hinweis: Der Zeitbedarf für die Zertifikatsbeschaffung beträgt ab dem postalischen Versand des Antrags ca. zwei Wochen. Es wird empfohlen, den Prozess der Beschaffung noch in der Phase des Anschlusses an die NOOTS Referenzumgebung zu beginnen.

2. Einleitung

Dieses Dokument erläutert Ihnen den Prozess der Beschaffung der benötigten V-PKI-Zertifikate sowie die Signierung von PDF-Dateien am Beispiel von Adobe Acrobat Pro. Es stellt eine Vertiefung zu den bereits bestehenden Leitfäden zu Zertifikaten für den Anschluss dar, die eine ganzheitliche Zertifikatsübersicht enthalten.

Die Public Key Infrastruktur der Verwaltung (V-PKI) ist ein technisch organisatorisches Konstrukt zur Ausstellung, Verwaltung und Prüfung digitaler Zertifikate für Bundes- und Landesbehörden, Kommunen sowie öffentliche Institutionen. Ziel der Verwaltungs-PKI ist es, den elektronischen Geschäftsverkehr zwischen Verwaltung und Wirtschaft konform der einschlägigen technischen Richtlinien zu ermöglichen.

Die benötigten Zertifikate erhalten Sie über die Deutschland Online Infrastruktur Certification Authority (DOI-CA), welche in die PKI-Verwaltung des Bundes integriert ist. Die DOI-CA wird durch die Deutsche Telekom Security GmbH im Trust Center betrieben. Die DOI-CA arbeitet bei der Registrierung von Teilnehmern mit sogenannten RA zusammen.

V-PKI-Zertifikate können ohne weiteres von Angehörigen der öffentlichen Verwaltung beantragt werden. Die Beschaffung der Zertifikate übernehmen in der Regel die betrieblich Verantwortlichen in Abstimmung mit bzw. im Auftrag des fachlich Verantwortlichen.

Dritte, die nicht unmittelbar der öffentlichen Verwaltung angehören (z.B. Dienstleister, Vereine, Beliehene etc.) benötigen für die Beantragung eines V-PKI-Zertifikats eine Vollmacht ihrer zuständigen Behörde der öffentlichen Verwaltung. Eine Voransicht der Vollmacht finden Sie in Anhang 1.

In den nachfolgenden Tabellen finden Sie eine Übersicht über die verschiedenen Zertifikate, die in diesem Leitfaden beschrieben werden:

Umgebung/Portal	Zertifikat	Anforderung	Zweck
https://noots.gov.de/	Personenbezogenes Signaturzertifikat	personenbezogenes Zertifikat der V-PKI/DOI-CA **(produktiv)**	Signieren von PDF-Dokumenten für die Registrierung
NOOTS Referenzumgebung	entfällt (alle benötigten V-PKI-Zertifikate werden durch die Referenzumgebung bereitgestellt)		
NOOTS Testumgebung	TLS-Client-Zertifikat des SAK-DC	gruppenbezogenes Zertifikat der V-PKI/DOI-CA **(produktiv oder test)**	Sichere Verbindung per mTLS zu den zentralen NOOTS-Komponenten und zum SAK-DP
	Verschlüsselungszertifikat des SAK-DC	gruppenbezogenes Zertifikat der V-PKI/DOI-CA **(produktiv oder test)**	Verschlüsselung der Nachweislieferung SAK-DP→ SAK-DC
NOOTS Produktivumgebung	TLS-Client-Zertifikat des SAK-DC	gruppenbezogenes Zertifikat der V-PKI/DOI-CA **(produktiv)**	Sichere Verbindung per mTLS zu den zentralen NOOTS-Komponenten und zum SAK-DP
	Verschlüsselungszertifikat des SAK-DC	gruppenbezogenes Zertifikat der V-PKI/DOI-CA **(produktiv)**	Verschlüsselung der Nachweislieferung SAK-DP→ SAK-DC

Tabelle 1 - Übersicht Anforderungen V-PKI-Zertifikate DC

Umgebung/Portal	Zertifikat	Anforderung	Zweck
https://noots.gov.de/	Personenbezogenes Signaturzertifikat	personenbezogenes Zertifikat der V-PKI/DOI-CA **(produktiv)**	Signieren von PDF-Dokumenten für die Registrierung
NOOTS Referenzumgebung	entfällt (alle benötigten V-PKI-Zertifikate werden durch die Referenzumgebung bereitgestellt)		
NOOTS Testumgebung	TLS-Server-Zertifikat des SAK-DP	gruppenbezogenes Zertifikat der V-PKI/DOI-CA **(produktiv oder test)**	TLS-Verschlüsselung zu SAK-DC
NOOTS Produktivumgebung	TLS-Server-Zertifikat des SAK-DP	gruppenbezogenes Zertifikat der V-PKI/DOI-CA **(produktiv)**	TLS-Verschlüsselung zu SAK-DC

Tabelle 2 - Übersicht Anforderungen V-PKI-Zertifikate DP

Sollte ein personenbezogenes Zertifikat der V-PKI/ DOI-CA aus anderen Zusammenhängen bereits vorliegen, kann dieses auch für den Registrierungsprozess im Zuge der Anbindung an das NOOTS genutzt werden (elektronisches Signieren von PDF-Dokumenten).

Die gruppenbezogenen Zertifikate der V-PKI/DOI-CA müssen jeweils exklusiv für ihren Einsatzbereich mit den jeweiligen Umgebungen des NOOTS vorgehalten und dürfen nicht für andere Zwecke zusätzlich eingesetzt werden. Ein gruppenbezogenes Zertifikat, das bereits für die NOOTS Testumgebung verwendet wurde, kann also nicht für die NOOTS Produktivumgebung genutzt werden.

3. Beschaffung von Zertifikaten der V-PKI/DOI-CA

Im Folgenden werden die in der Einleitung genannten Schritte näher erläutert.

3.1. Schritt 1 - Vorbereitende Maßnahmen

Zunächst sollten DP und DC die Person festlegen, die innerhalb des betrieblichen Verantwortlichen eines DC oder DP berechtigt ist, verbindliche Mitteilungen an das Bundesverwaltungsamt bzw. die Firma Dataport AöR im Zuge des Anschlusses an das NOOTS zu tätigen und entsprechende PDF-Dokumente zu signieren. Für diese Person ist ein persönliches V-PKI-Zertifikat zu beantragen. Für den Fall von Abwesenheiten ist es sinnvoll, eine Vertretung festzulegen. Zu beachten ist, dass jede festgelegte Person ein eigenes personenbezogenes Zertifikat benötigt. Daher kann die Anzahl der zu beantragenden personenbezogenen Zertifikate je nach Festlegung variieren und über der Mindestanzahl von eins liegen.

DC oder DP müssen darüber hinaus die Arbeitseinheit für das zu beziehende Zertifikat festlegen, das dementsprechend beantragt werden muss. Für diese Arbeitseinheit muss eine „schlüsselverantwortliche Person“ festgelegt werden, die das Zertifikat beantragt.

Zusätzlich muss die genaue Bezeichnung ihres Gruppen-/Funktionsnamens festgelegt werden (siehe Schritt 3, gruppenbezogenes Zertifikat). Bei Fragen hierzu wenden Sie sich an dataportnootssupport@dataport.de.

Daneben sollte die für Sie zuständige dienstsiegelführende Stelle identifiziert werden, die berechtigt ist, den Antrag auf ein V-PKI-Zertifikat in Papierform mit einem Dienstsiegel zu versehen.

Im Beantragungsvorgang für das V-PKI-Zertifikat werden Sie gebeten, den Antrag auszudrucken und mit einem Dienstsiegel versehen an die angegebene Adresse zu senden. Es sollte daher im Vorfeld mit der siegelführenden Stelle Rücksprache gehalten werden.

Hinweis für Dritte außerhalb der öffentlichen Verwaltung:

Dritte (z.B. Dienstleister, Vereine, Beliehene etc.) versehen den eigentlichen Antrag für das Zertifikat mit dem hauseigenen Stempel. Zusätzlich benötigen sie für die Beantragung eines V-PKI-Zertifikats eine Vollmacht ihrer zuständigen Behörde der öffentlichen Verwaltung, die mit einem Dienstsiegel zu versehen ist. Es sollte daher im Vorfeld mit der zuständigen Behörde diesbezüglich Kontakt aufgenommen werden. Eine Voransicht der Vollmacht finden Sie in Anhang 1. Die ausfüllbare PDF-Version des Vordrucks erhalten Sie als Begleitdokument zum Download auf nova.noots.gov.de.

Weiterhin sollten Sie die zuständige Haushaltsstelle bzw. Finanzabteilung informieren, dass Kosten zu begleichen sein werden. Bei der RA „Öffentliche Verwaltung“ der Deutschen Telekom Security GmbH sind das 81,- Euro je Zertifikat (Stand 07.2026). Die Preise anderer RA können abweichen und müssten ggf. dort erfragt werden.

Die Begleichung der Kosten kann je nach zuständiger RA unterschiedlich sein. Sofern eine vertragliche Beziehung mit einer bestimmten RA existiert, ist die Rechnungsbegleichung ggf. vordefiniert (andernfalls siehe unten).

Es sollte daher geklärt werden, ob es ggf. eine vertragliche Bindung mit einer bestimmten RA für die Beantragung von V-PKI-Zertifikaten gibt. Sollte das der Fall sein, ist die Beantragung vorzugsweise dort vorzunehmen.

In jedem Fall können V-PKI-Zertifikate immer bei der DOI-CA (Deutsche Telekom Security GmbH) beantragt werden. Dies gilt auch dann, wenn es eine vertragliche Bindung mit einer anderen RA gibt. Dies hätte auf die Ausstellung und Gültigkeit des Zertifikats keinen Einfluss. Es ist aber möglich, dass es im Zuge der Rechnungsbegleichung zu Irritationen kommen könnte, wenn die Zertifikate nicht bei einer ggf. vertraglich festgelegten Stelle beantragt wurden. Das wäre jedoch eine reine Frage der Buchhaltung, die keinen Einfluss auf die Wirksamkeit des Zertifikats hätte.

Die Rechnungslegung bei der DOI-CA (Deutsche Telekom Security GmbH) ist ein nachgelagerter Prozess, der in Absprache mit den Antragstellenden verschiedentlich gestaltet werden kann (z.B. Rechnung per PDF oder eRechnung im XML-Format).

3.2. Schritt 2 - Zugangsdaten für das Webportal der Zertifizierungsstelle beantragen

Als DC und DP der Bundesländer Bremen, Hamburg, Sachsen-Anhalt und Schleswig-Holstein wenden Sie sich an dataportzentraleregistrierungsstellepki@dataport.de.

Sofern eine Bindung an eine andere RA bekannt ist, wenden Sie sich bitte an diese (andernfalls siehe unten).

3.2.1 DP

Als DP schreiben Sie eine E-Mail mit folgendem Text, um die Zugangsdaten zum Webportal zu erhalten:

„Sehr geehrte Damen und Herren,
für den Anschluss an das Nationale Once-Only-Technical-System (NOOTS) benötigen wir ein personenbezogenes Zertifikat der V-PKI Produktivumgebung, um damit das Antragsformular im PDF-Format elektronisch signieren zu können.
Für die verschlüsselte Kommunikation mit dem NOOTS benötigen wir zusätzlich zwei gruppenbezogene Zertifikate der V-PKI Produktivumgebung zum Einsatz als TLS Client-Zertifikate.
Es besteht eine vertragliche Bindung an folgende Registrierungsstelle (RA): -> bitte einfügen <-
Bitte übersenden Sie uns die Zugangsdaten für das entsprechende Portal sowie die dazugehörige URL.
Mit freundlichen Grüßen
[Signatur]“

Falls die Bindung an eine bestimmte RA nicht vorhanden oder nicht bekannt ist, wenden Sie sich an den Servicedesk der DOI-CA (Deutsche Telekom Security GmbH). Es wird die Anfrage an die zuständige Stelle weiterleiten. Die E-Mailadresse lautet: smc-berlin.tsi@telekom.de.

Als DP schreiben Sie in diesem Fall eine E-Mail mit folgendem Text:

„Sehr geehrte Damen und Herren,
für den Anschluss an das Nationale Once-Only-Technical-System (NOOTS) benötigen wir ein personenbezogenes Zertifikat der V-PKI Produktivumgebung, um damit das Antragsformular im PDF-Format elektronisch signieren zu können.
Für die verschlüsselte Kommunikation mit dem NOOTS benötigen wir zusätzlich zwei gruppenbezogene der V-PKI Produktivumgebung zum Einsatz als TLS Client-Zertifikate.
Eine vertragliche Bindung an eine Registrierungsstelle (RA) ist nicht vorhanden oder uns nicht bekannt.
Bitte übersenden Sie uns die Zugangsdaten für das entsprechende Portal sowie die dazugehörige URL
Mit freundlichen Grüßen
[Signatur]“

3.2.2 DC

Als DC schreiben Sie eine E-Mail mit folgendem Text, um die Zugangsdaten zum Webportal zu erhalten:

„Sehr geehrte Damen und Herren,
für den Anschluss an das Nationale Once-Only-Technical-System (NOOTS) benötigen wir ein personenbezogenes Zertifikat der V-PKI Produktivumgebung, um damit das Antragsformular im PDF-Format elektronisch signieren zu können.
Für die verschlüsselte Kommunikation mit dem NOOTS benötigen wir zusätzlich vier gruppenbezogene Zertifikate der V-PKI Produktivumgebung zum Einsatz als TLS Client-Zertifikate.
Es besteht eine vertragliche Bindung an folgende Registrierungsstelle (RA): -> bitte einfügen <-
Bitte übersenden Sie uns die Zugangsdaten für das entsprechende Portal sowie die dazugehörige URL.
Mit freundlichen Grüßen
[Signatur]“

Falls die Bindung an eine bestimmte RA nicht vorhanden oder nicht bekannt ist, wenden Sie sich an den Servicedesk der DOI-CA (Deutsche Telekom Security GmbH). Es wird die Anfrage an die zuständige Stelle weiterleiten. Die E-Mailadresse lautet: smc-berlin.tsi@telekom.de.

Als DC schreiben Sie in diesem Fall eine E-Mail mit folgendem Text:

„Sehr geehrte Damen und Herren,
für den Anschluss an das Nationale Once-Only-Technical-System (NOOTS) benötigen wir ein personenbezogenes Zertifikat der V-PKI Produktivumgebung, um damit das Antragsformular im PDF-Format elektronisch signieren zu können.
Für die verschlüsselte Kommunikation mit dem NOOTS benötigen wir zusätzlich vier gruppenbezogene der V-PKI Produktivumgebung zum Einsatz als TLS Client-Zertifikate.
Eine vertragliche Bindung an eine Registrierungsstelle (RA) ist nicht vorhanden oder uns nicht bekannt.
Bitte übersenden Sie uns die Zugangsdaten für das entsprechende Portal sowie die dazugehörige URL
Mit freundlichen Grüßen
[Signatur]“

3.3. Schritt 3 - Antrag für ein V-PKI-Zertifikat online ausfüllen, ausdrucken und unterschreiben

Nach Erhalt der URL und der Zugangsdaten loggen Sie sich entsprechend ein und beginnen die Beantragung.

Hinweis: Die Test- und Produktivumgebung der Telekom Plattform sehen identisch aus. Bitte prüfen Sie die URL. In der Testumgebung ist der Zusatz „test“ enthalten, in der Produktivumgebung nicht. Die folgenden Abbildungen zeigen die produktive Umgebung. Die Beantragung sowohl für die personenbezogenen als auch für die gruppenbezogenen Zertifikate erfolgt aus demselben Portal heraus und verläuft sehr ähnlich.

Stand 08.2026:

Umgebung der Telesec	URL
Test	https://doi.test.telesec.de/doi/ee/new/login/displayLogin.html
Produktiv	https://doi.telesec.de/doi/ee/login/displayLogin.html

Loggen Sie sich mit den bereitgestellten Zugangsdaten auf der Plattform ein.

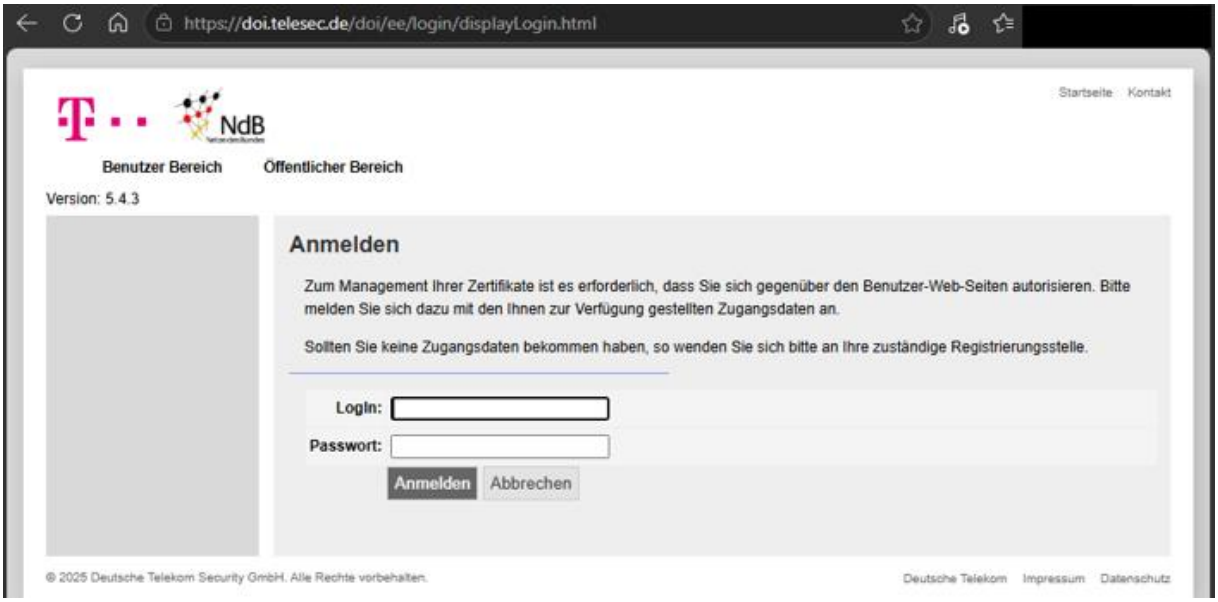

Abbildung 1 - Anmelden im Webportal der Zertifizierungsstelle

Bitte klicken Sie im Menüpunkt „Software-Zertifikat“ auf „beantragen“.

Wählen Sie zunächst als Sub-Domäne „NOOTS“ aus. Wenn die Sub-Domäne nicht wählbar ist, dann kann die RA keine Zertifikate für NOOTS ausstellen. Wenden Sie sich bitte an die für Sie zuständige RA, um diese Sub-Domäne einzurichten. Sollte das nicht möglich sein, können Sie sich an den Servicedesk der DOI-CA (Deutsche Telekom Security GmbH) wenden (smc-berlin.tsi@telekom.de). Die Beantragung des Zertifikats kann als Rückfalloption dort erfolgen.

Abbildung 2 - Auswahl der Domäne

3.3.1 Für personenbezogene Zertifikate:

Als Zertifikatstyp wählen Sie bitte ein „Personenbezogenes Zertifikat“ und bestätigen mit „Weiter“.

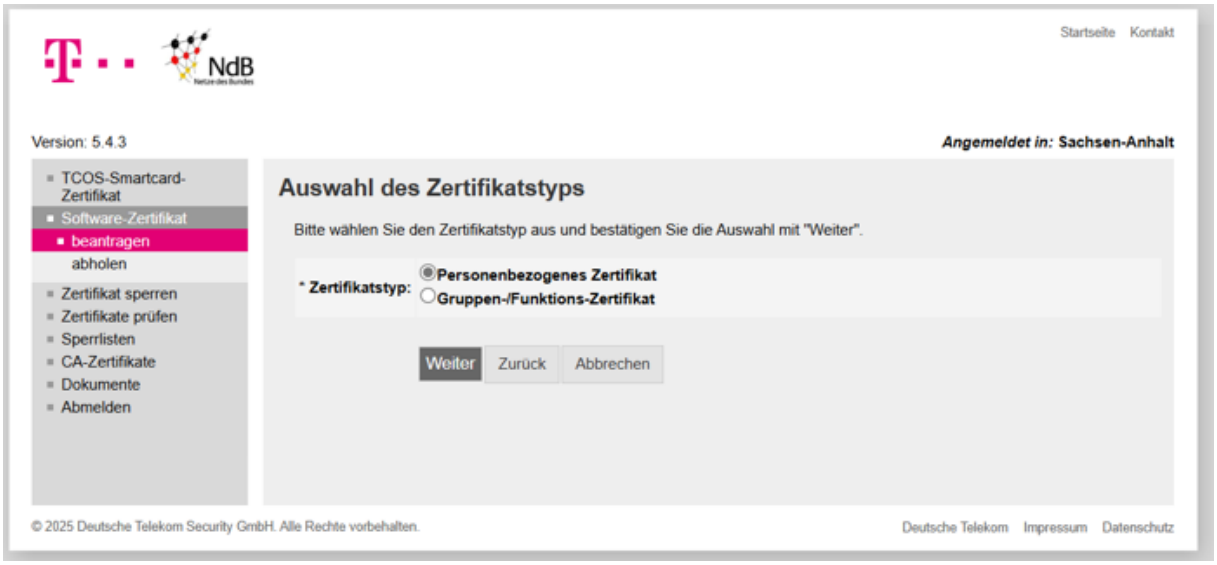

Abbildung 3 - Auswahl des Zertifikatstyps

Geben Sie nun die dienstlichen Daten (Dienstort, dienstliche Telefonnummer und dienstliche E-Mail-Adresse) der antragstellenden Person ein. Die E-Mailadresse muss zu einer natürlichen Person gehören. Die Angabe von E-Mailadressen zu Gruppen-/Funktionspostfächern ist nicht zulässig und führt zur Ablehnung des Antrags.

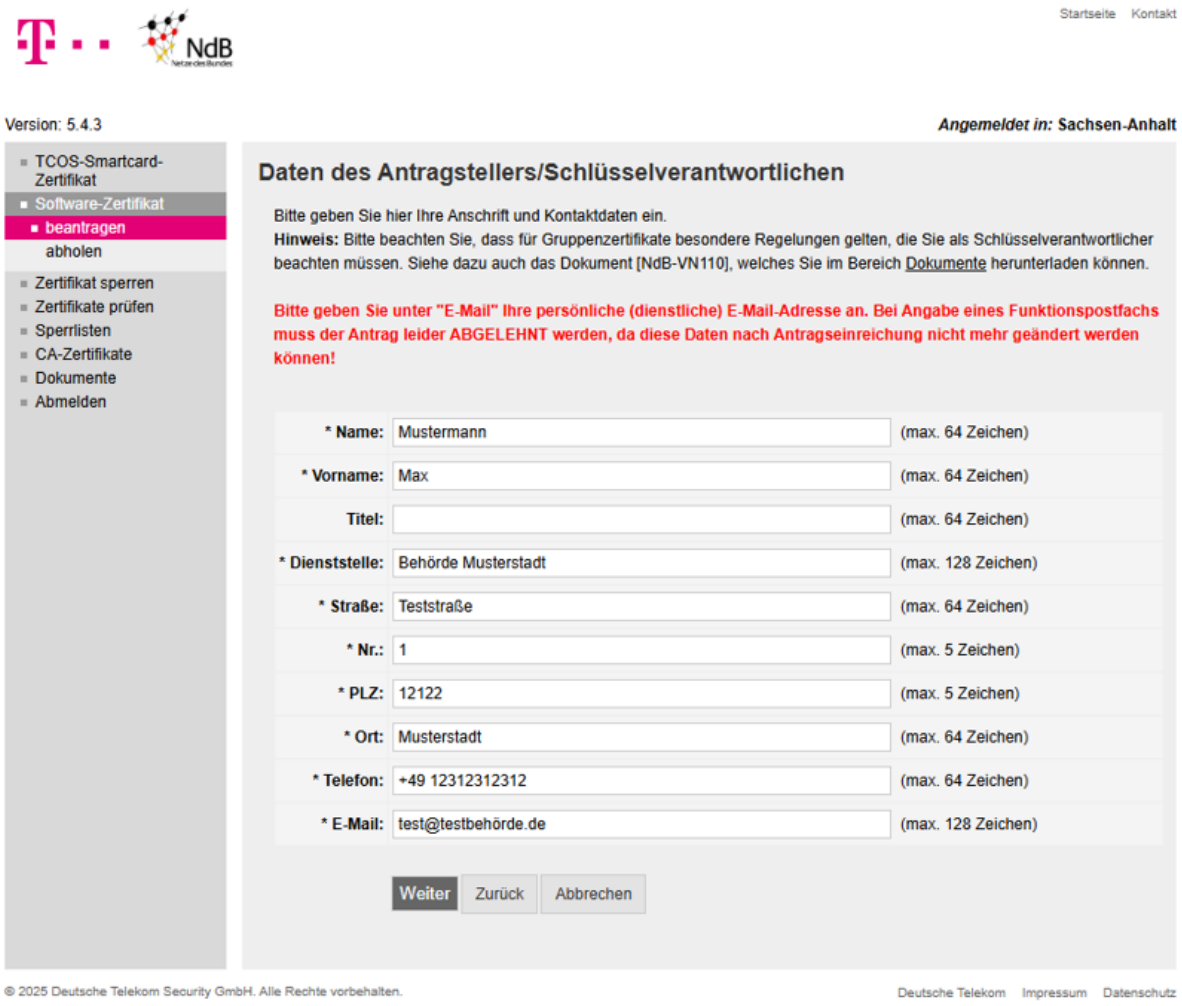

Abbildung 4 - Erfassung der Daten des Antragsstellers

Die Daten „Common-Name“ und „E-Mail-Adresse“ werden automatisch aus den Angaben in der vorigen Maske hinterlegt. Bitte klicken Sie auf „Weiter“.

Abbildung 5 - Erfassung der Zertifikatsdaten für personenbezogenes Zertifikat

Sie können zu Ihrer Organisationseinheit „weitere Angaben“ (Kennung 1 und Kennung 2) machen.

Es wird empfohlen, diese Felder freizulassen, da bei Änderungen der Organisationseinheit das Zertifikat gesperrt werden müsste.

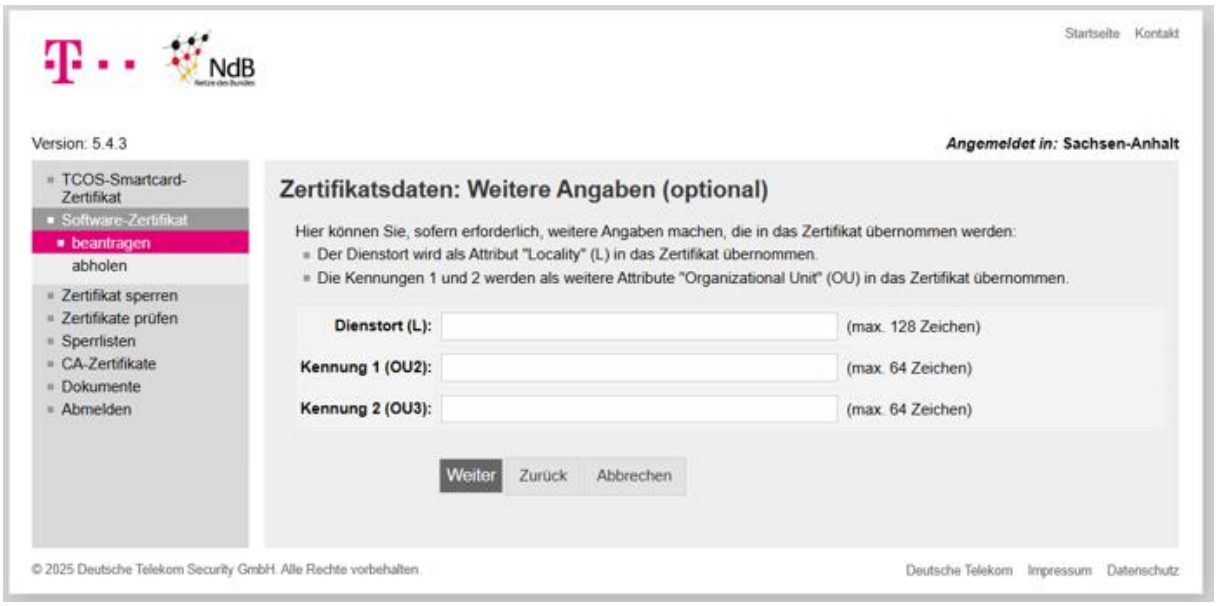

Abbildung 6 - Erfassung der Zertifikatsdaten für personenbezogenes Zertifikat: Weitere Angaben

Sie können auswählen, ob das Zertifikat im DOI-Verzeichnisdienst (VöD) veröffentlicht werden soll. Für das personenbezogene Zertifikat wird die Veröffentlichung im VöD grundsätzlich nicht empfohlen. Ausnahmen können sich ergeben, wenn bereits jetzt schon absehbar ist, dass das personenbezogene V-PKI-Zertifikat für einen Anwendungsfall nachgenutzt werden könnte, bei dem die Veröffentlichung im VöD erforderlich ist. Das dürfte in der Regel jedoch nicht der Fall sein.

Als Hash-Algorithmus und Schlüsseltyp sind die folgenden Angaben auszuwählen:

- Hash-Algorithmus: SHA256
- Schlüsseltyp (Signatur): ECC NIST P-256

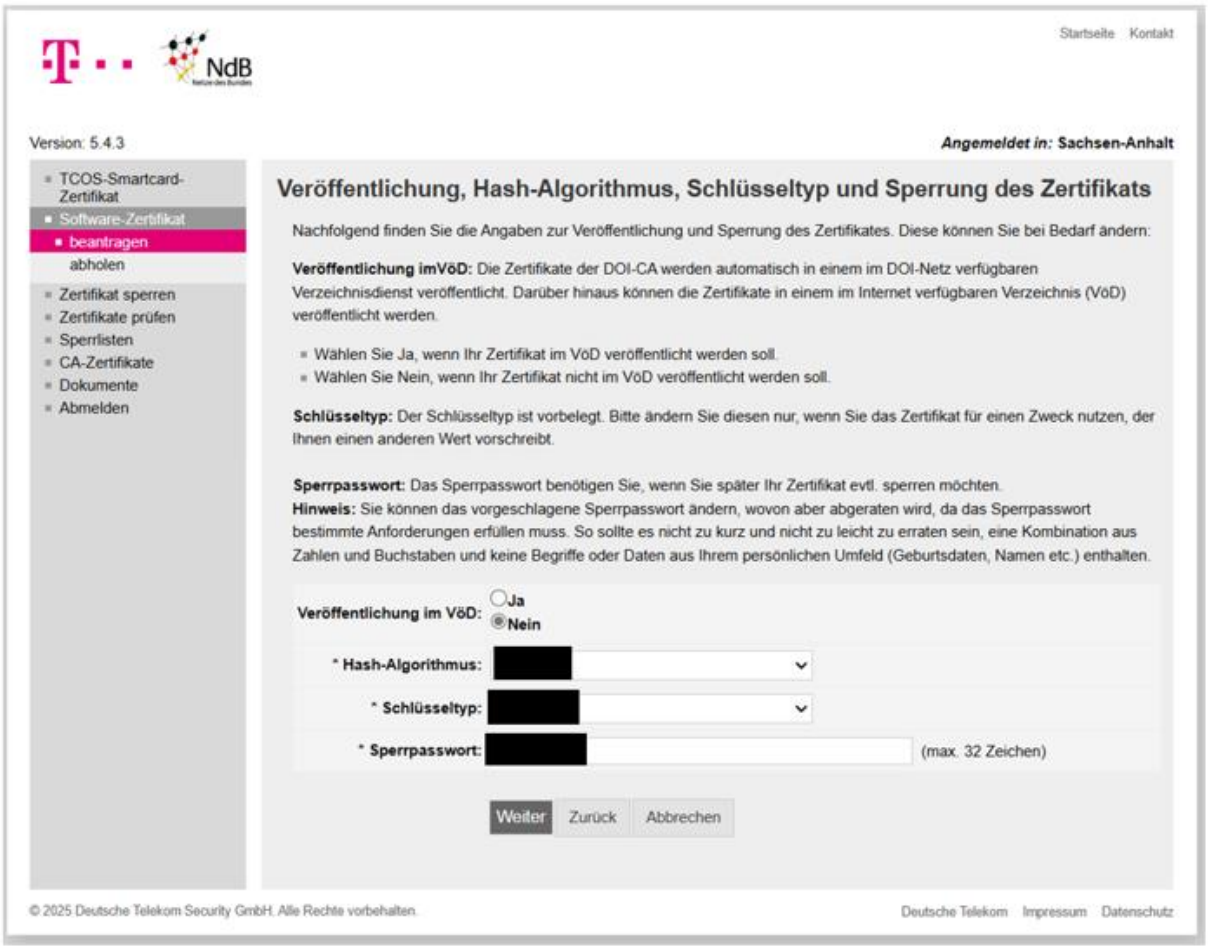

Abbildung 7 - Veröffentlichung und Sperrung des Zertifikats

Die Maske zur Abrechnung des Zertifikats kann ggf. vordefiniert sein und sich je nach RA unterscheiden. Bitte geben Sie die Daten zur Abrechnung an.

Abbildung 8 - Abrechnung des beantragten Zertifikats

Sie können am Ende der Beantragung Mitteilungen an die RA machen. Dieses Feld eignet sich z.B. um auf bestehende Kommunikation, ältere Vorgänge bei der Neubeantragung eines bestehenden Zertifikats, eine vorangegangene Falschbeantragung oder Eilbedürftigkeit hinzuweisen. In der Regel brauchen hier keine Angaben gemacht zu werden.

Abbildung 9 - Mitteilung an die RA

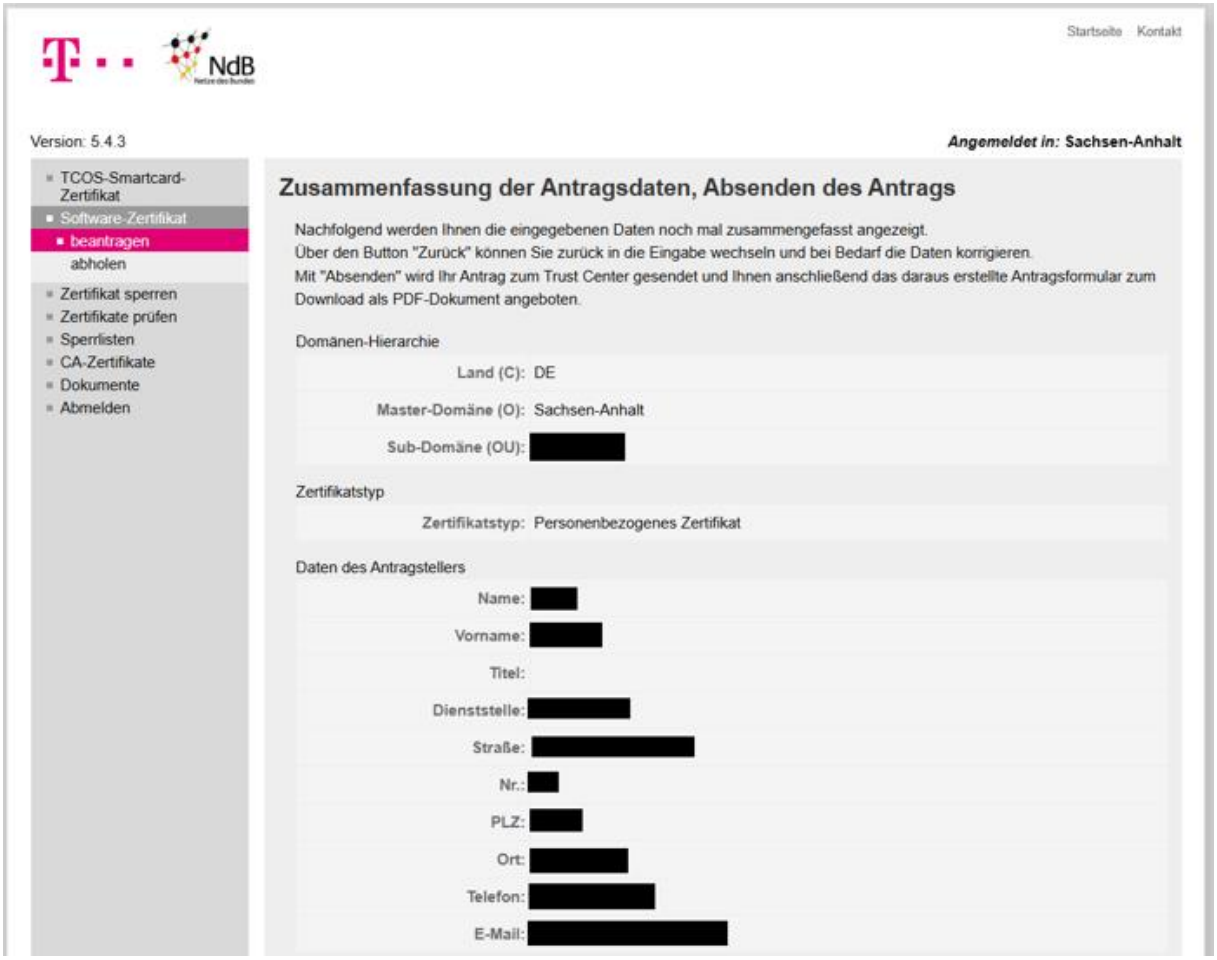

Abbildung 10 - Zusammenfassung der Antragsdaten

3.3.2 Für gruppenbezogene Zertifikate:

Bitte klicken Sie im Menüpunkt „Software-Zertifikat“ auf „beantragen“. Als Nächstes wählen Sie die Sub-Domäne (OU) „NOOTS“ aus und klicken auf „Weiter“.

Abbildung 11 - Erfassung der Zertifikatsdaten für gruppenbezogenes Zertifikat: Auswahl der Domäne

Als Zertifikatstyp wählen Sie bitte ein „Gruppen-/Funktionszertifikat“ und bestätigen mit „Weiter“.

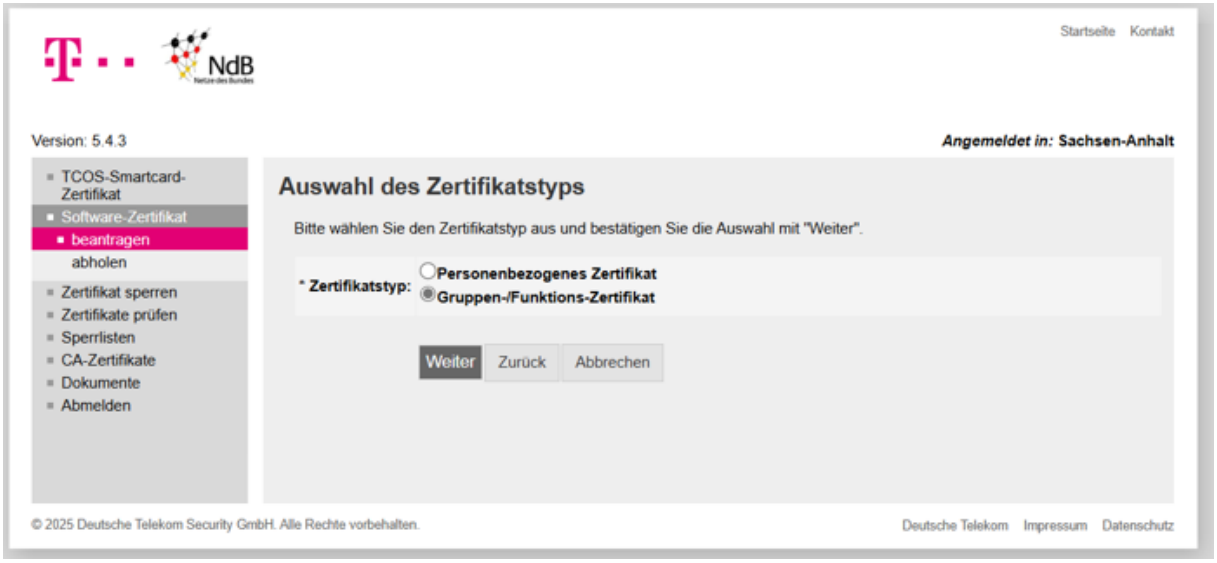

Abbildung 12 - Auswahl des Zertifikatstyps für Gruppen-/Funktionszertifikat

Geben Sie nun die dienstlichen Daten (Dienstort, Diensttelefonnummer und Dienst-E-Mail-Adresse) der antragstellenden Person ein. Diese Daten sind nicht Bestandteil des Zertifikats. Die E-Mailadresse muss zu einer natürlichen Person gehören. Die Angabe von E-Mailadressen zu Gruppen-/Funktionspostfächern ist nicht zulässig und führt zur Ablehnung des Antrags.

Bei Gruppenzertifikaten entspricht die antragstellende Person dem „Schlüsselverantwortlichen“ und muss daher eine natürliche Person sein.

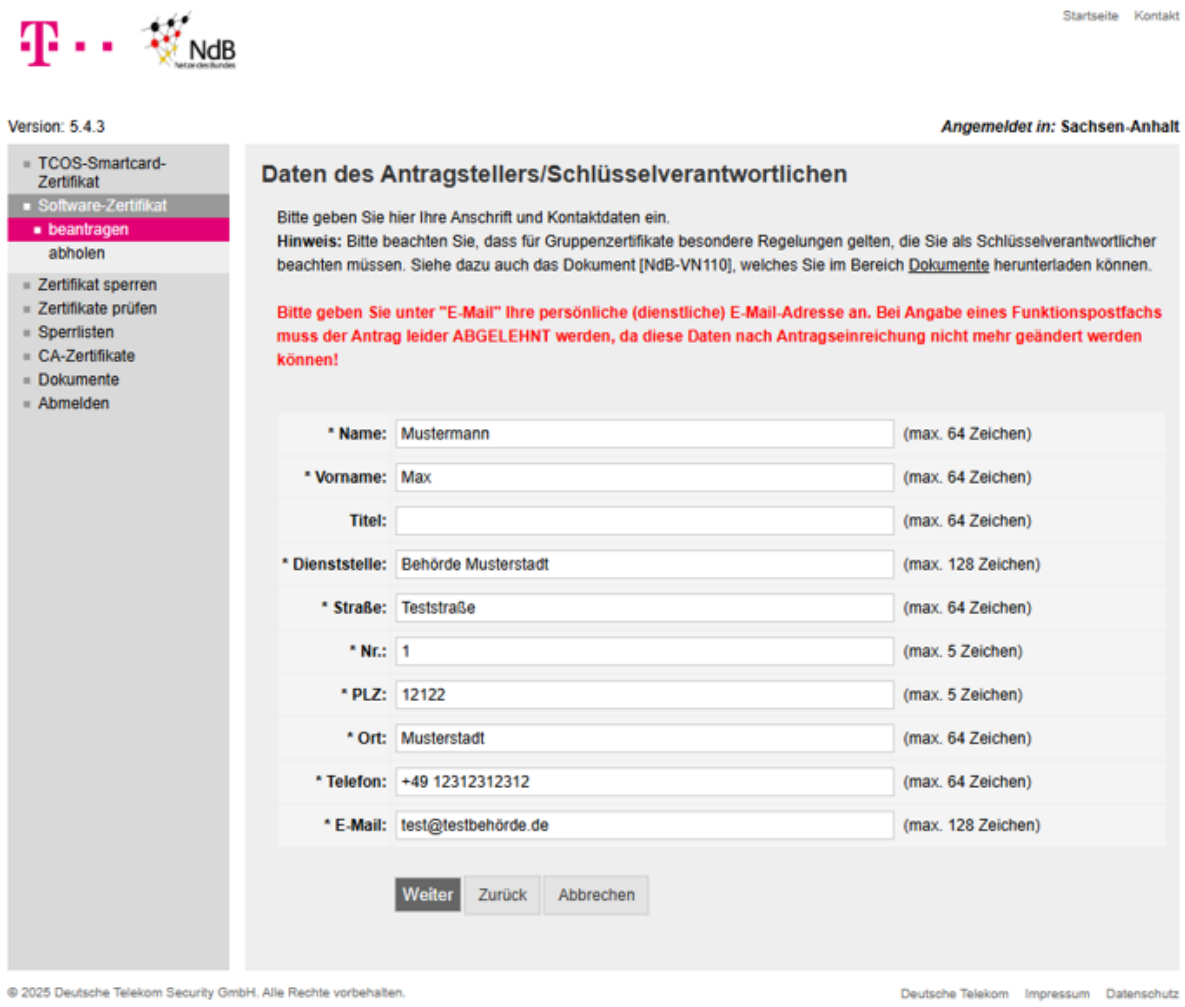

Abbildung 13 - Erfassung der Daten des Antragsstellers für Gruppen-/Funktionszertifikat

Als Nächstes geben Sie die Zertifikatsdaten ein.

Ihre Eingabe im Feld CN muss folgendem Schema entsprechen:

- GRP: „Name der Einrichtung“:SAK-DC:“Spezifikation des SAK-DC“ bzw. „Name der Einrichtung“:SAK-DP:“Spezifikation des SAK-DP

Die Bestandteile „GRP: “ und „:SAK-DC/-DP:“ sind verpflichtend vorgegeben und müssen in dieser Form eingetragen werden.

Tragen Sie darüber hinaus den Namen der beantragenden Einrichtung sowie der Abteilung nach „GRP:“ ein. Die Einrichtung und Abteilung müssen daran eindeutig identifizierbar sein.

Spezifizieren Sie das Einsatzgebiet des SAK-DC/DP am Ende des Feldes. Dies ist vor allem dann wichtig, wenn Sie in ihrer Einrichtung planen, mehrere SAK-DC/-DP zu betreiben.

Beispiel:
Einrichtung: Rechenzentrum Musterstadt AöR
Arbeitseinheit: IT Sicherheit
SAK für Data Consumer: SAK-DC bzw. SAK für Data Provider: SAK-DP
Einsatzgebiet SAK: Online-Dienst XY

Daraus ergibt sich für das Feld CN folgender beispielhafter Eintrag:

- GRP: Rechenzentrum Musterstadt AöR IT Sicherheit:SAK-DC:Online-Dienst XY

Bei Fragen hierzu wenden Sie sich an dataportnootssupport@dataport.de.

Als E-Mailadresse sollten Sie eine möglichst zentrale Adresse wie ein Gruppen-/Funktionspostfach angeben. Klicken Sie anschließend auf „Weiter“.

Abbildung 14 - Erfassung der Zertifikatsdaten für Gruppen-/Funktionszertifikat

Bennen Sie im Feld L den Dienstort der beantragenden Einrichtung. Beispiel: Musterstadt

Sie können zu Ihrer Organisationseinheit „weitere Angaben“ (Kennung 1 und Kennung 2) machen.

Es wird empfohlen, diese Felder frei zu lassen, da bei Änderungen der Organisationseinheit das Zertifikat gesperrt werden müsste

Abbildung 15 - Erfassung der Zertifikatsdaten für Gruppen-/Funktionszertifikat: Weitere Angaben

Sie können auswählen, ob das Zertifikat im DOI-Verzeichnisdienst (VöD) veröffentlicht werden soll.

Als Hash-Algorithmus und Schlüsseltyp sind die folgenden Angaben auszuwählen:

- Hash-Algorithmus: SHA256
- Schlüsseltyp (Signatur): ECC NIST P-256

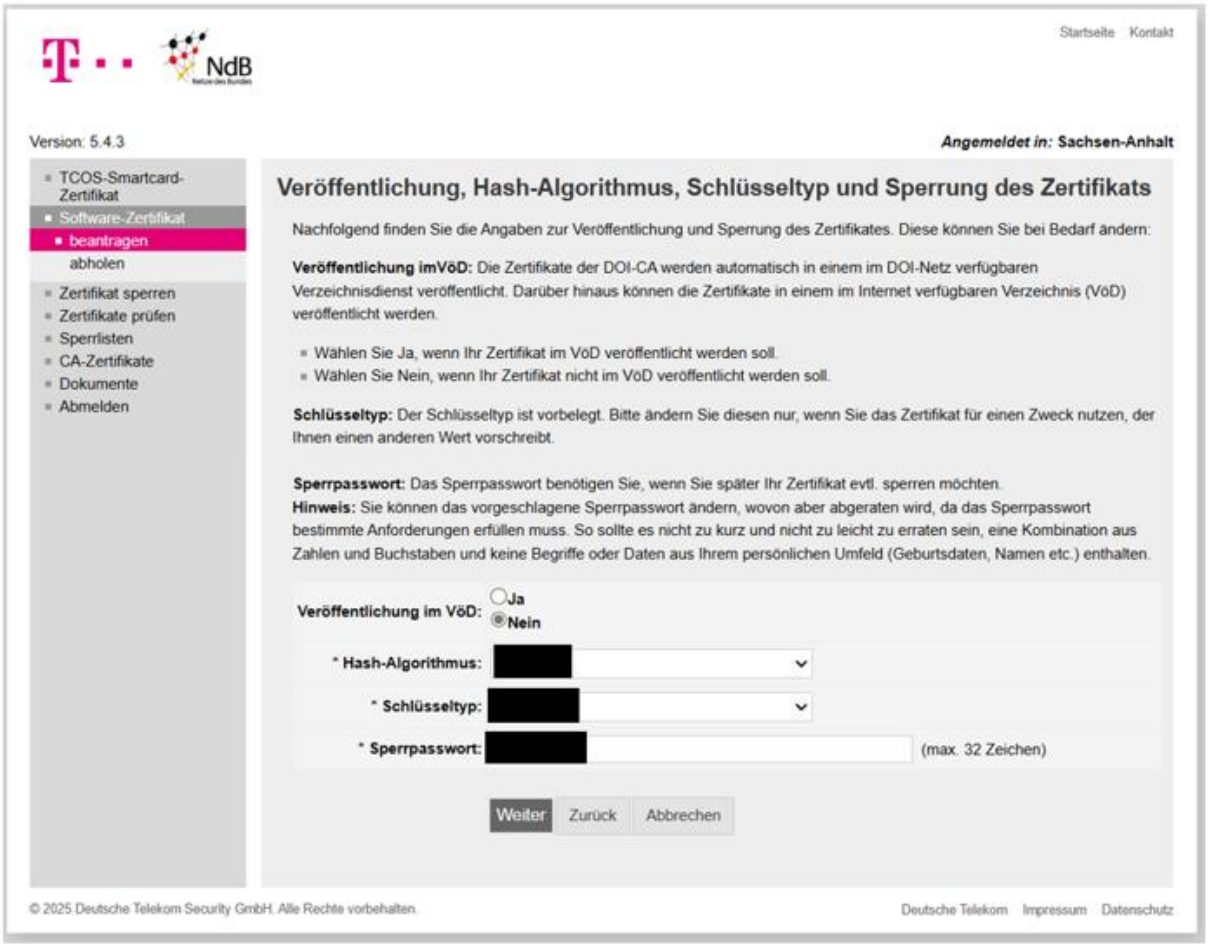

Abbildung 16 - Veröffentlichung und Sperrung des Zertifikats

Die Maske zur Abrechnung des Zertifikats kann ggf. vordefiniert sein und sich je nach RA unterscheiden. Bitte geben Sie die Daten zur Abrechnung an.

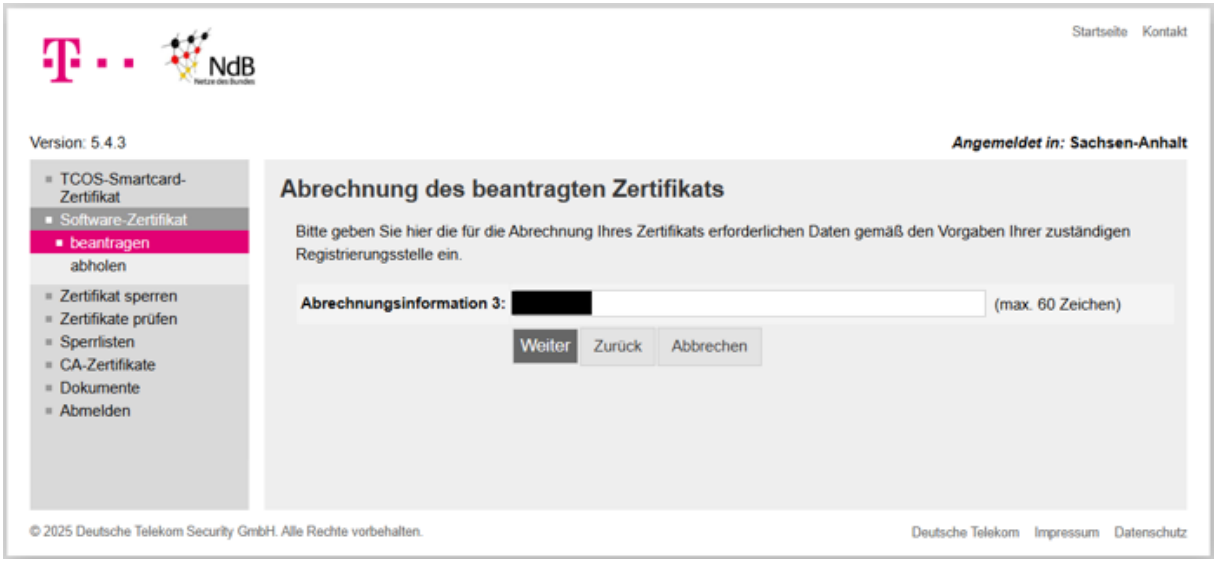

Abbildung 17 - Abrechnung des beantragten Zertifikats

Sie können am Ende der Beantragung Mitteilungen an die RA machen.

Dieses Feld eignet sich z.B. um auf bestehende Kommunikation, ältere Vorgänge bei der Neubeantragung eines bestehenden Zertifikats, eine vorangegangene Falschbeantragung oder Eilbedürftigkeit hinzuweisen.

Abbildung 18 - Mitteilung an die RA

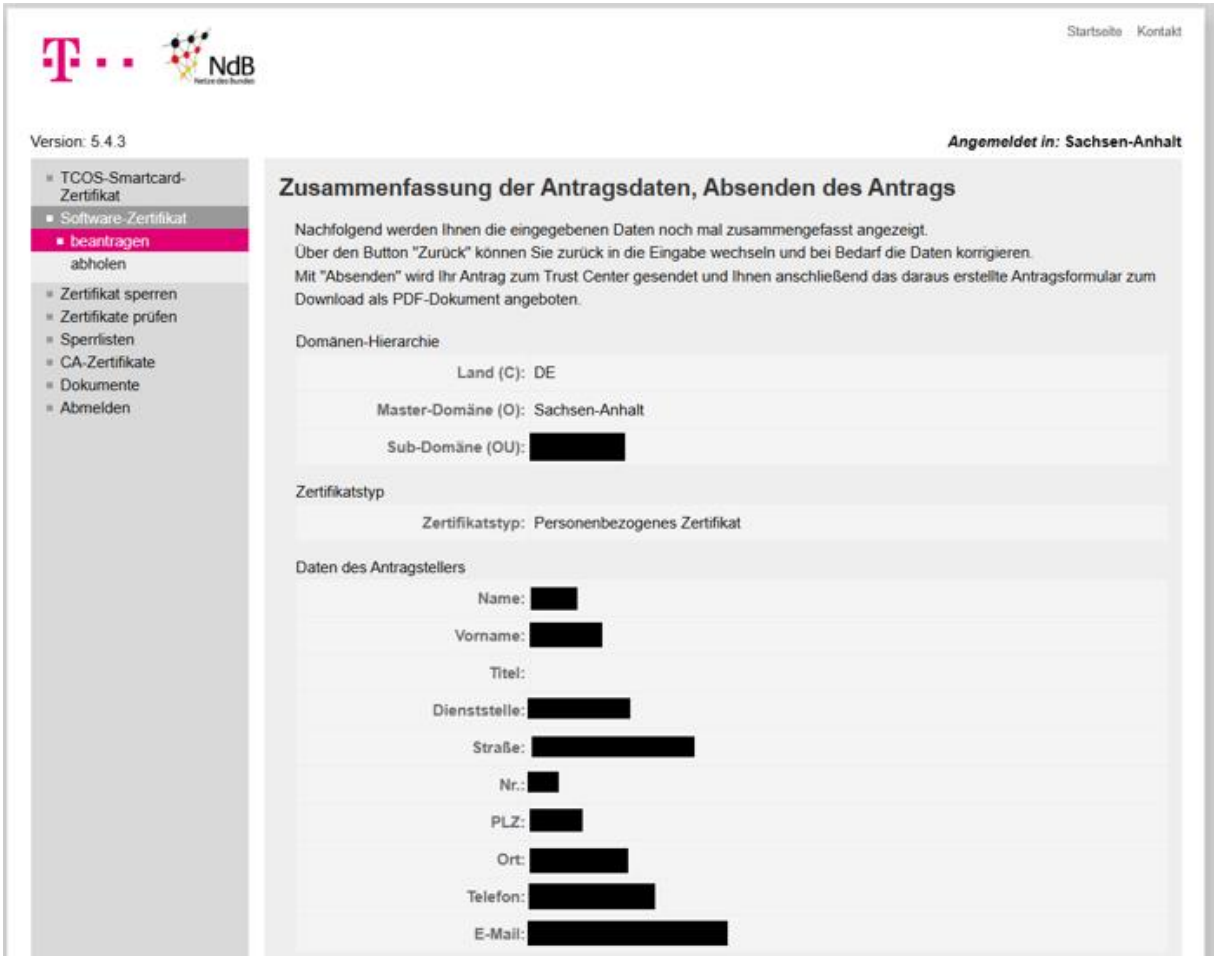

Abbildung 19 - Zusammenfassung der Antragsdaten

DC oder DP, die beabsichtigen sich an die NOOTS Testumgebung und die NOOTS Produktivumgebung anzubinden, benötigen zwei bzw. vier gruppenbezogene Zertifikate. In diesem Fall muss der Prozess für die Beantragung der gruppenbezogenen Zertifikate mehrfach durchlaufen werden. Zur Klarstellung gegenüber der RA kann auf diesen Umstand unter „Mitteilung an die Registrierungsstelle“ hingewiesen werden, um Missverständnisse zu vermeiden. Beispiel:

„Es werden zwei gruppenbezogene Zertifikate benötigt, weshalb der Antrag zweimal eingereicht wird.“

Schließlich werden Ihnen noch einmal alle Ihre Angaben angezeigt. Bitte überprüfen Sie die Daten. Wenn Sie Änderungen vornehmen möchten, können Sie dies über „Zurück“ tun. Sind die Angaben richtig, schicken Sie den Antrag mit „Absenden“ ab.

3.4. Schritt 4 - Siegeln des Antrags mit einem Dienstsiegel und Versand per Post an die RA

Am Ende der Beantragung des personenbezogenen und der gruppenbezogenen Zertifikate muss der Antrag heruntergeladen werden.

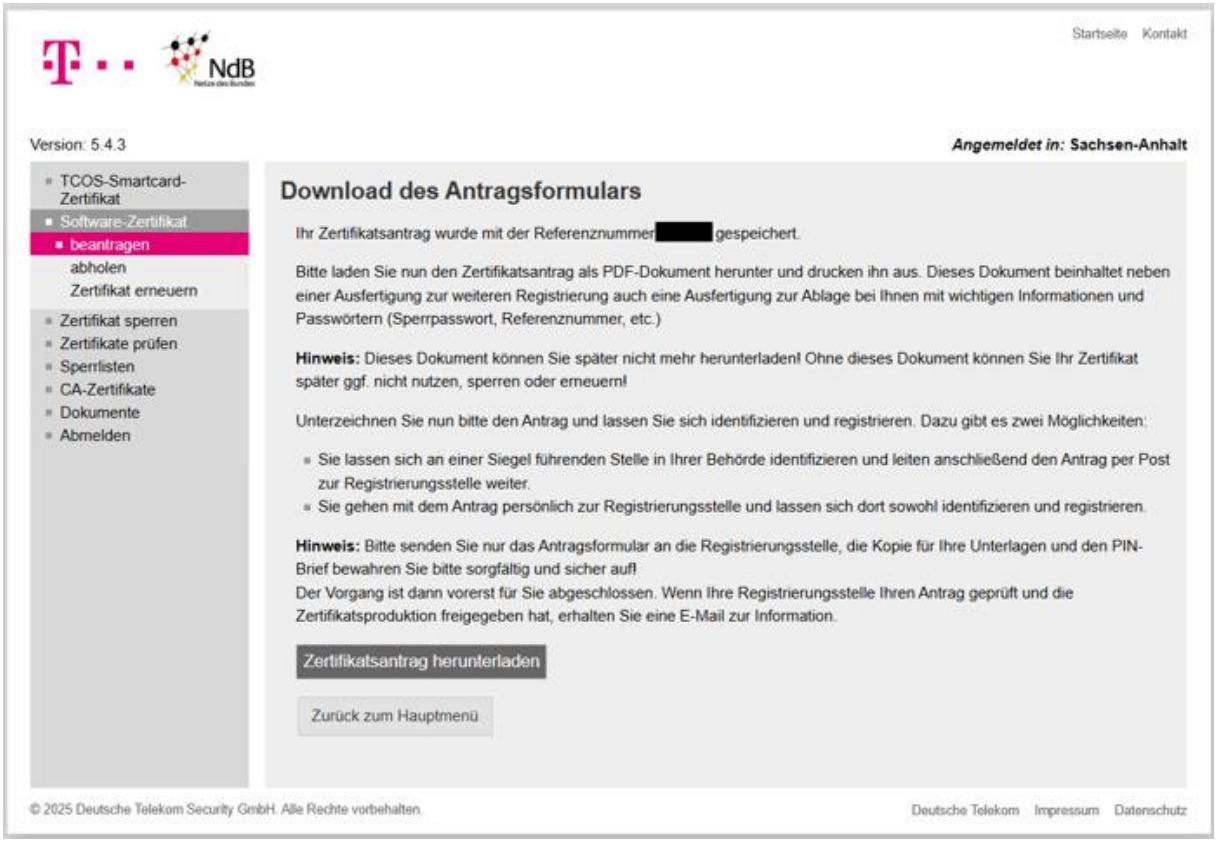

Abbildung 20 - Download des Antragsformulars

Zusätzlich zum eigentlichen Antrag enthält der Download eine Kopie des Antrags für die eigenen Unterlagen, einen PIN-Brief und ggf. weitere Blätter. Der Antrag sollte in digitaler Form über die gesamte Laufzeit des Zertifikats sicher aufbewahrt werden.

Bitte drucken Sie die Zertifikatsanträge aus und unterschreiben sie diese. Im nächsten Schritt müssen die unterschriebenen Dokumente mit einem Dienstsiegel gesiegelt werden. Wenden Sie sich dazu an Ihre siegelführende Stelle und lassen die Dokumente siegeln.

Im Anschluss senden Sie die Anträge per Post an Ihre RA. Die Anschrift finden Sie in den Antragsformularen. Um den Postweg zu beschleunigen, können Sie ggf. den Versand als Einschreiben wählen. Die RA benötigen in der Regel nicht alle Seiten des Antrags. Bitte beachten Sie die Hinweise auf der Webseite und im Download.

Hinweis für Dritte außerhalb der öffentlichen Verwaltung:

Dritte (z.B. Dienstleister, Vereine, Beliehene etc.) versehen den Antrag mit ihrem hauseigenen Stempel. Zusätzlich benötigen sie für die Beantragung eines V-PKI-Zertifikats eine Vollmacht ihrer zuständigen Behörde der öffentlichen Verwaltung. Eine Voransicht der Vollmacht finden Sie in Anhang 1. Die ausfüllbare PDF-Version des Vordrucks erhalten Sie als Begleitdokument zum Download auf nova.noots.gov.de.

Bitte übersenden Sie die entsprechend ausgefüllte und gesiegelte Vollmacht zusammen mit den Anträgen an die RA.

3.5. Schritt 5 - Download des Zertifikats nach Bearbeitung des Antrags durch die RA

Wenn Ihr Zertifikat von der RA genehmigt wurde, werden Sie per E-Mail informiert. Gehen Sie auf den in der E-Mail übersandten Link und unter dem Menüpunkt „Software-Zertifikat“ klicken Sie bitte auf „abholen“.

Bitte geben Sie die Referenznummer und das Download-Passwort ein. Beide Daten finden Sie in Ihrem Antragsformular oder Ihrem PIN-Brief. Bitte klicken Sie anschließend auf „Suchen“.

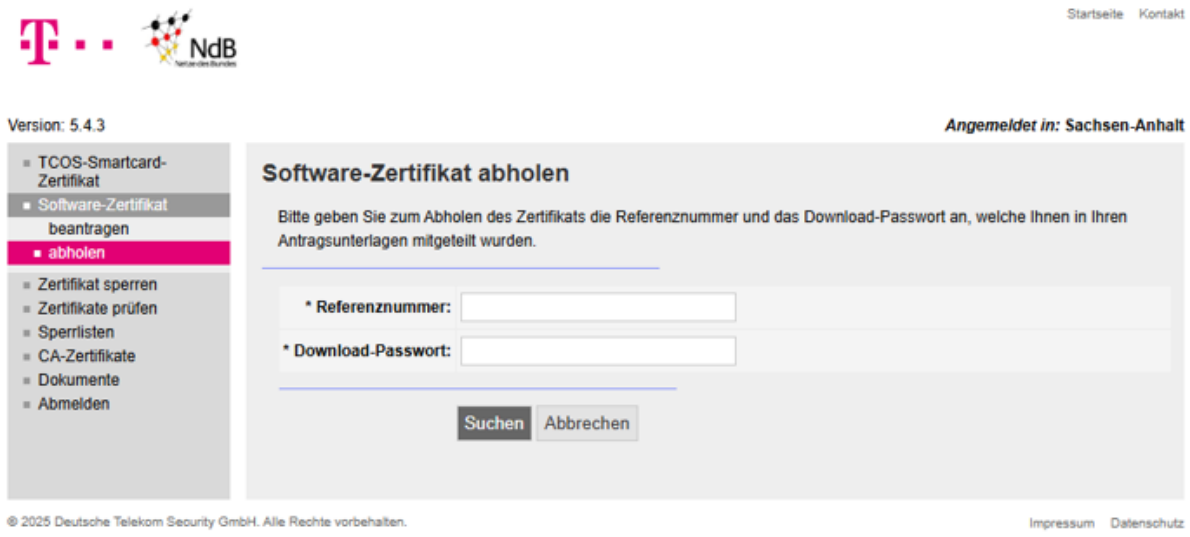

Abbildung 21 - Abholung des Software-Zertifikates Teil I

Bei erfolgreicher Eingabe wird Ihnen eine *.p12-Datei zum Download angeboten. Speichern Sie die *.p12-Datei an geeigneter Stelle ab. Diese Datei beinhaltet den privaten Schlüssel und verbleibt ausschließlich bei Ihnen. Bitte achten Sie auf Maßnahmen der Informationssicherheit gemäß den Vorgaben Ihrer Organisation zum Schutz der Schlüsseldatei. Der erfolgreiche Download der Datei muss bestätigt werden. Nach Bestätigung haben Sie die Möglichkeit, den öffentlichen Schlüssel separat herunterzuladen.

Der Download ist auf drei Versuche limitiert. Wenn Sie nach dem dritten Versuch nicht bestätigt haben, dass Sie die Datei erfolgreich heruntergeladen haben, wird beim nächsten Versuch der Download gesperrt und der private Schlüssel gelöscht. Sie müssen dann einen neuen Antrag stellen.

Nach der Bestätigung wird Ihnen angezeigt, dass das Zertifikat freigeschaltet wurde. Sie können nun noch einmal das Zertifikat nur mit dem öffentlichen Schlüssel als *.der-Datei herunterladen.

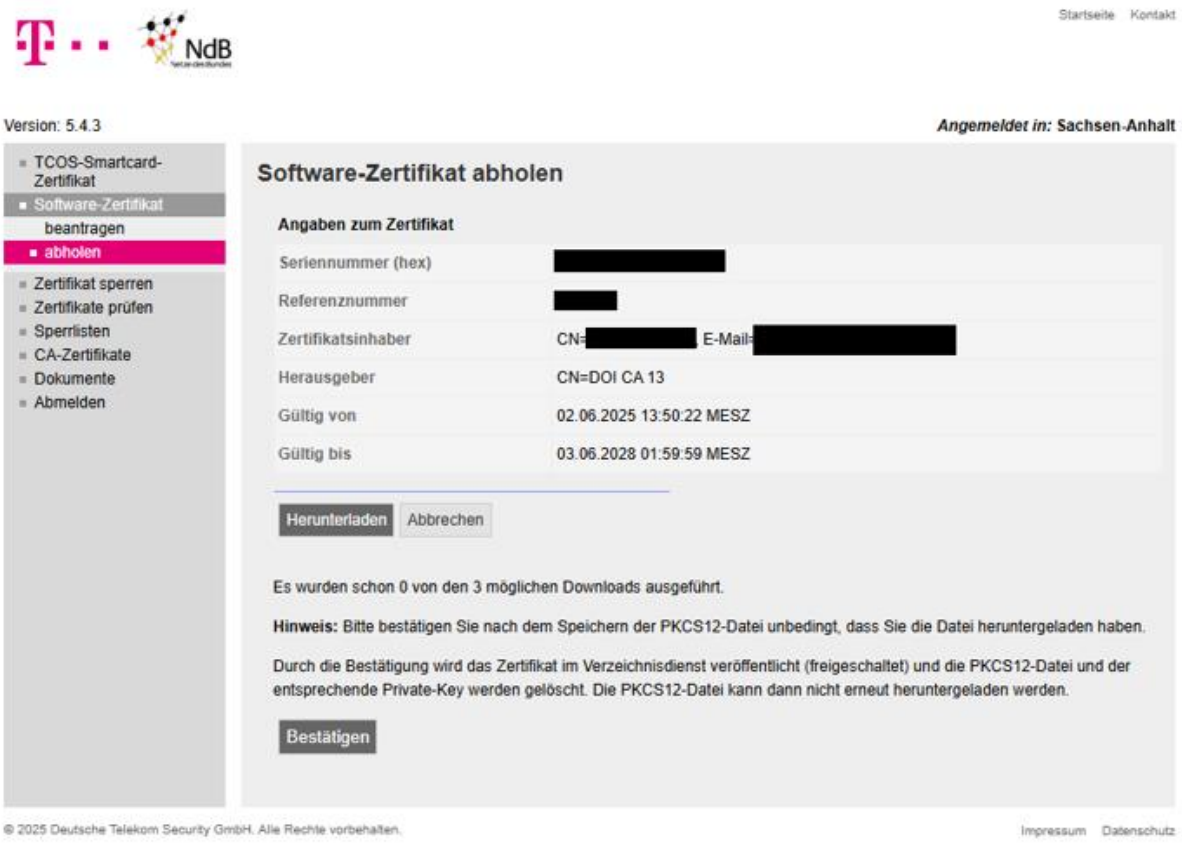

Abbildung 22 - Abholung des Software-Zertifikates Teil II

Abbildung 23 - Abholung des Software-Zertifikates Teil III

4. Darstellung der Signierung von PDF-Dokumenten mit Adobe Acrobat

Wie zuvor oben beschrieben, müssen Sie das Registrierungsformular für die einzelnen Umgebungen mit einem personenbezogenen Signaturzertifikat signieren. Dieses wird im Anschluss vom NOOTS-Support geprüft. Um diese Prüfung zu ermöglichen, übergeben Sie bitte Ihren öffentlichen Schlüssel an das BVA.

4.1. PDF signieren

Generell können Sie für die Signierung jede anerkannte Software verwenden, mit der fortgeschrittene elektronische Signaturen an PDF-Dokumenten angebracht werden können. Die Anwendung muss für das elektronische Signieren mit Softwarezertifikaten zugelassen sein. In diesem Dokument wird beispielhaft das Vorgehen unter Verwendung von Adobe Acrobat Pro erläutert. Mögliche alternative Softwarelösungen sind zum Beispiel Governikus DATA Boreum oder SecSigner von SecCommerce. Bei verschiedenen verfügbaren Varianten einer Softwarelösung empfehlen wir Ihnen die Nutzung einer „offline“-Version, die keine Internetverbindung benötigt.

Bitte halten Sie Ihr personenbezogenes Signaturzertifikat inklusive Passwort zur Durchführung der Signatur bereit.

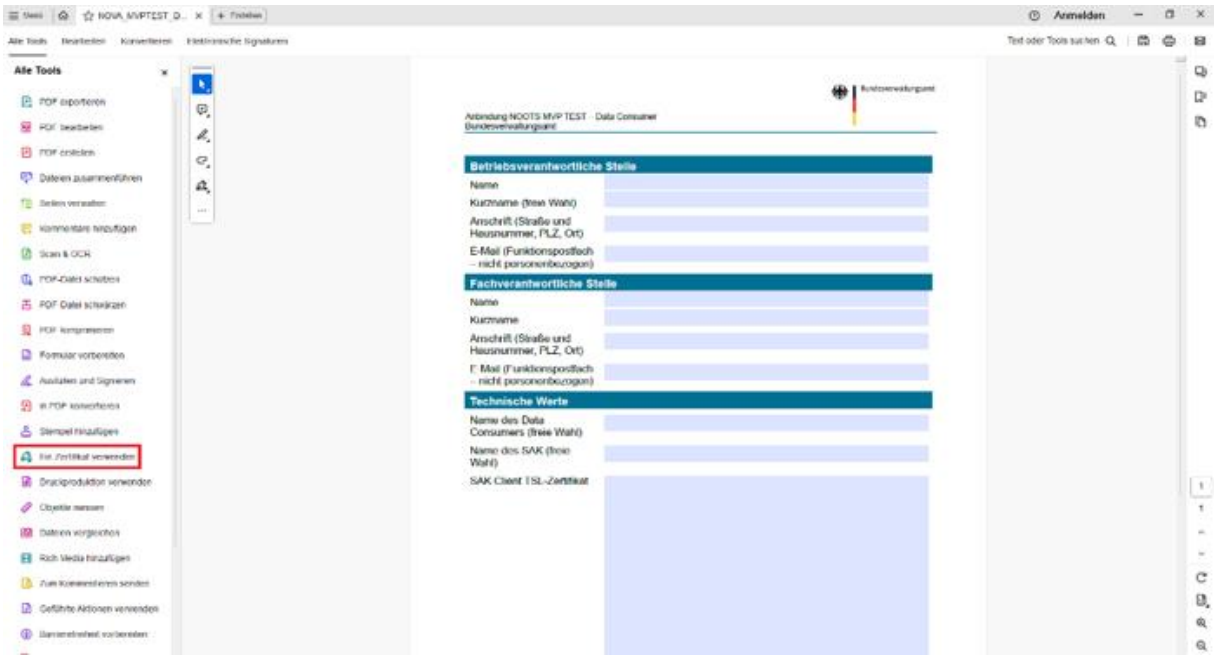

Abbildung 24 - Registrierungsformular in Adobe Acrobat Pro

Als Erstes öffnen Sie bitte das ausgefüllte Registrierungsformular als PDF-Datei mit Adobe Acrobat Pro und wählen unter „Alle Tools“ „Ein Zertifikat verwenden“ aus.

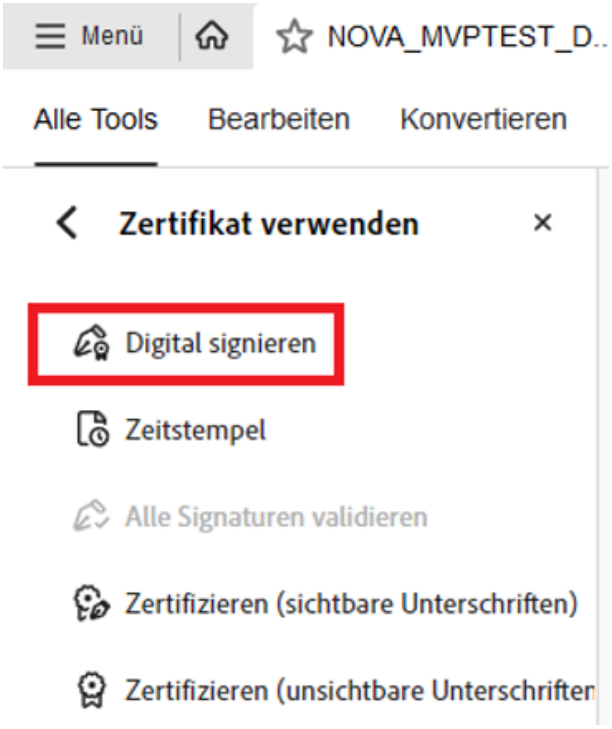

Abbildung 25 - Untermenü "Digital signieren"

In dem sich öffnenden Untermenü klicken Sie bitte auf „Digital signieren“ und wählen einen Platz auf dem Formular aus, auf dem die Signatur stehen soll.

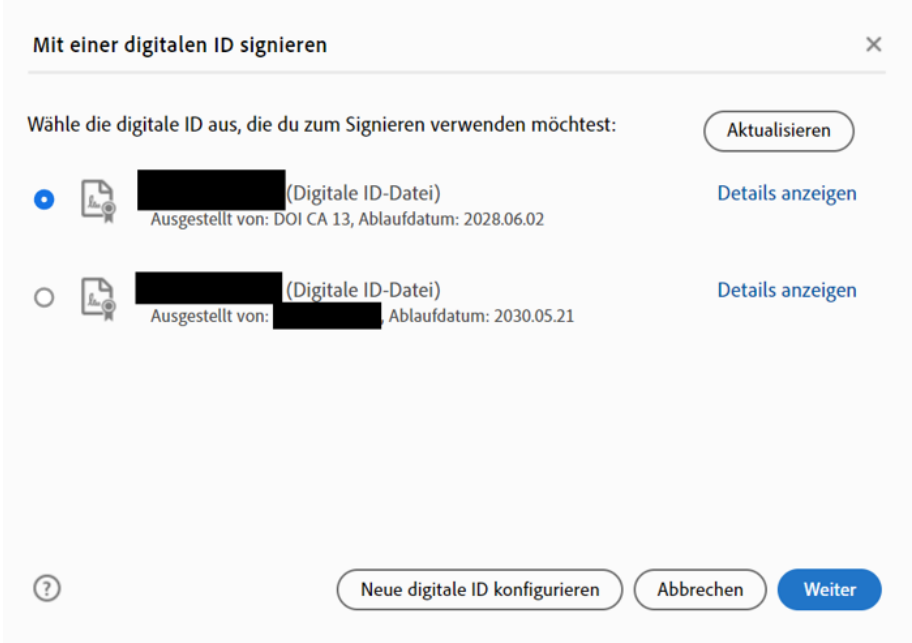

Abbildung 26 - Auswahl der digitalen ID

In dem sich öffnenden Fenster wählen Sie bitte die digitale ID aus, die Sie zum Signieren benutzen möchten und bestätigen mit „Weiter“. Mit der „digitalen ID“ ist ein digitaler Identitätsnachweis gemeint, wie beispielsweise Ihr personenbezogenes Zertifikat der V-PKI/DOI-CA. Wenn Sie dieses noch nicht in Adobe Acrobat Pro hinzugefügt haben, ist ggf. noch keine passende digitale ID vorhanden. Wählen Sie dann bitte „Neue digitale ID konfigurieren“.

4.2. Konfiguration einer neuen digitalen ID

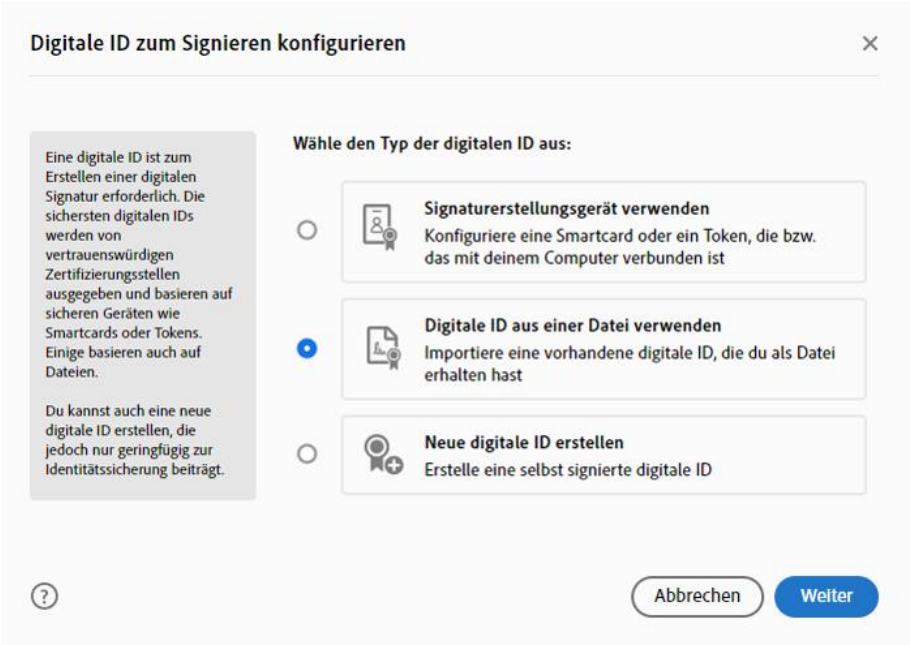

Abbildung 27 - Konfiguration einer digitalen ID zum Signieren

Bitte wählen Sie „Digitale ID aus einer Datei verwenden“ und klicken Sie auf „Weiter“.

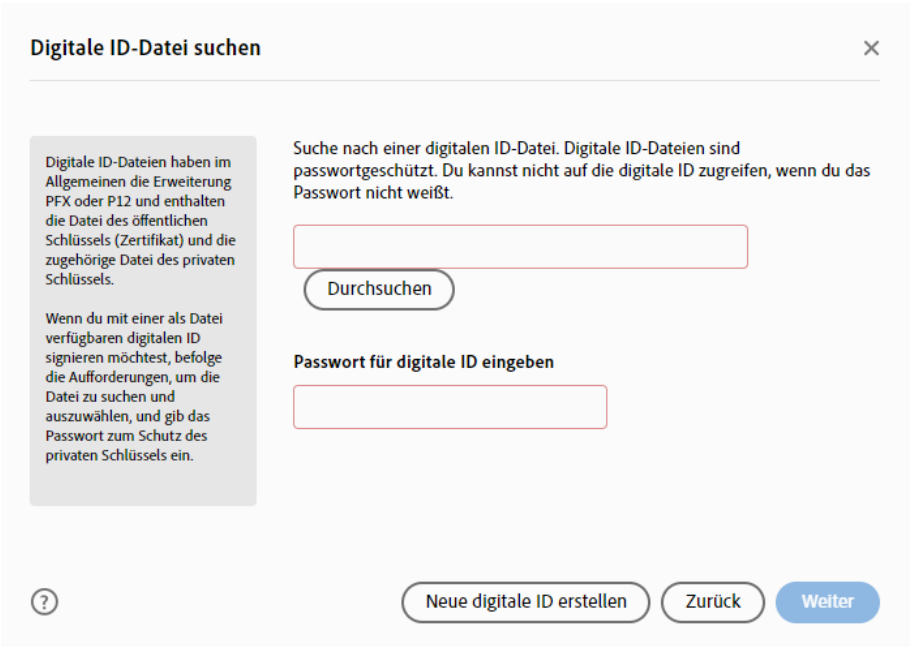

Abbildung 28 - Suchen einer digitalen ID-Datei

Bitte suchen Sie nun nach der Zertifikatsdatei Ihres personenbezogenen Zertifikates der V-PKI/DOI-CA (diese endet auf .p12) und geben Sie das zu dem Zertifikat gehörige Passwort ein. Bestätigen Sie mit „Weiter“.

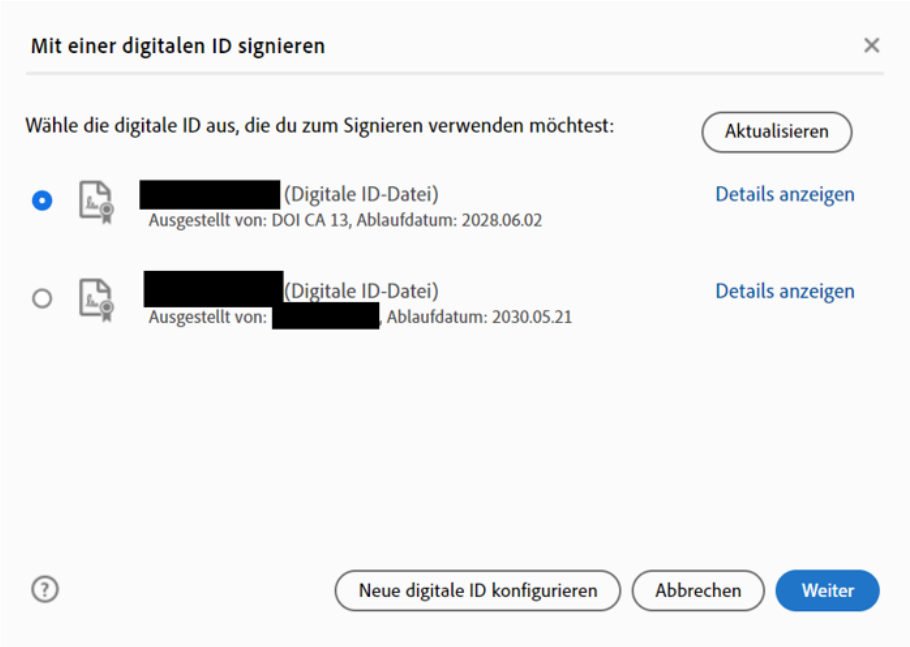

Abbildung 29 - Auswahl der digitalen ID nach Konfiguration

Wählen Sie nun die digitale ID aus, mit der Sie signieren möchten, und bestätigen Sie mit „Weiter“.

4.3. Abschluss

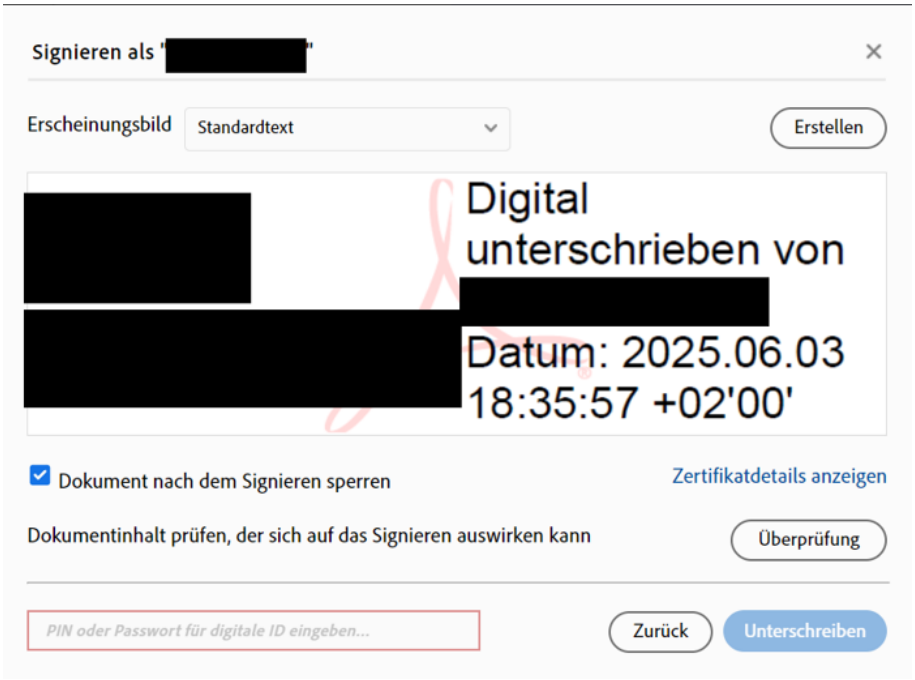

Abbildung 30 - Unterschreiben mit der digitalen ID

Geben Sie nun das Passwort des Zertifikats ein und klicken Sie auf „Unterschreiben“.

Ihr Dokument wurde nun digital von Ihnen signiert.

4.4. Weitergabe des öffentlichen Schlüssels an das BVA

Der öffentliche Teil des Schlüssels bzw. die ausgelesenen Informationen des Schlüssels müssen für die Prüfung der Signatur an das BVA übermittelt werden.

Bitte wenden Sie sich zur Vereinbarung einer Übergabe an folgende E-Mailadresse: registermodernisierung@bva.bund.de. Sofern für die Übergabe aufgrund von internen Vorgaben in Ihrer Organisation spezielle Freigaben nötig sind, setzen Sie sich hierzu im Vorfeld mit Ihrer zuständigen IT-Stelle in Verbindung.

4.5. Öffentlichen Schlüssel auslesen

Das Auslesen der Informationen kann mittels zugelassener Software durchgeführt werden. Für das folgende Beispiel wurde die Open-Source Software Kleopatra verwendet.

Der öffentliche Schlüssel wird importiert und anschließend ausgelesen. Dieser Schritt vermeidet einen erheblichen Aufwand auf der Seite des BVAs.

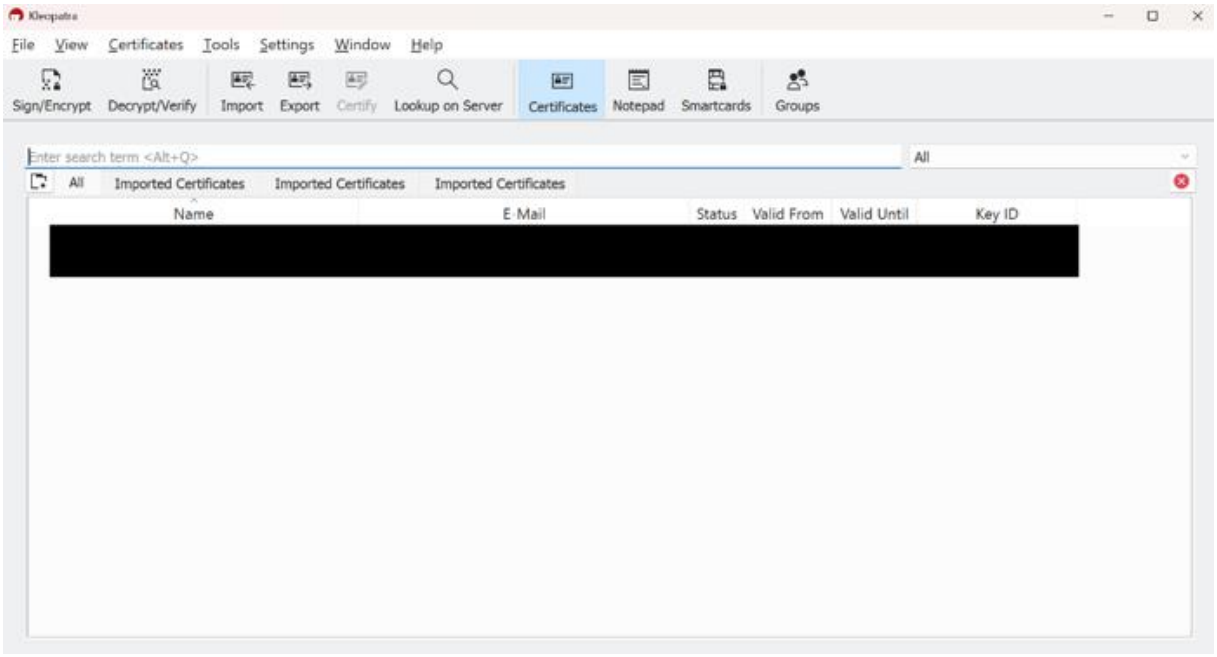

Abbildung 31 - Öffentlichen Schlüssel mittels Kleopatra auslesen

Die relevanten Informationen zur weiteren Verarbeitung können aus der der Zertifikatsdetailansicht extrahiert werden. Je nach verwendeter Software, kann die Darstellung abweichen.

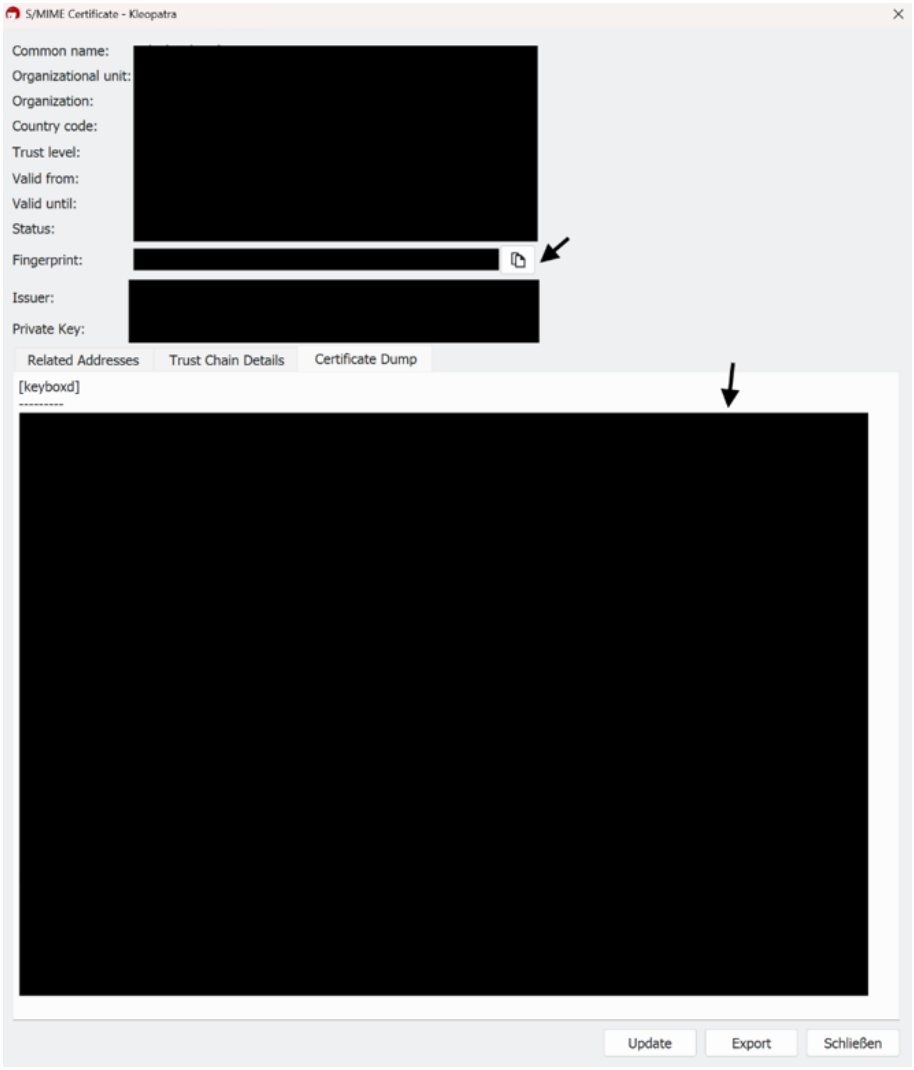

Abbildung 32 - Zertifikatsdetailansicht Kleopatra

Das dargestellte Textfeld „Certificate Dump“ inkl. SHA-Fingerprint wird dann, wie mit dem BVA individuell vereinbart, übergeben.

Anhang 1 – Vollmacht Zertifikatsantrag für Dritte

Die ausfüllbare PDF-Version des Vordrucks erhalten Sie als Begleitdokument zum Download auf nova.noots.gov.de.

Vollmacht

Öffentliche Stelle [„Vollmachtgeber“]:

Behörden-/Stellenname:

Anschrift:

Autorisierte Stelle [„Bevollmächtigter“]:

Institution:

Anschrift:

Diese Vollmacht wird ausgestellt für:

Auflistung der Mitarbeitenden
(nur natürliche Personen, keine Arbeitseinheiten)

Mitarbeitende:

Der Vollmachtgeber bevollmächtigt den Bevollmächtigten, ihn gegenüber der Deutsche Telekom Geschäftskunden GmbH und der Deutsche Telekom Security GmbH zu vertreten.

Diese Vollmacht berechtigt den Bevollmächtigten dazu, im Auftrag des Vollmachtgebers Zertifikate der DOI-CA innerhalb der Subdomäne „NOOTS“ bei der Deutsche Telekom Geschäftskunden GmbH und der Deutsche Telekom Security GmbH zu beantragen.

Der Vollmachtgeber bestätigt hiermit das Bestehen einer Zusammenarbeit mit dem Bevollmächtigten im Rahmen der Registermodernisierung bzw. des NOOTS und das damit einhergehende Erfordernis von Zertifikaten der DOI-CA innerhalb der Subdomäne „NOOTS“.

Der Vollmachtgeber versichert, dass die festgelegten Mitarbeitenden bekannt sind und zur Organisation des Bevollmächtigten gehören.

Die Bestätigung erstreckt sich nur auf die hier festgelegten Mitarbeitenden und ist nicht erweiter- oder übertragbar.

Diese Bestätigung ist gültig bis auf Widerruf.

Datum, Ort, Name, Unterschrift Vollmachtgeber

Dienstsiegel öffentliche Stelle

Abbildung 33 – Vollmacht Zertifikatsantrag für Dritte