



Referat D III 3 – Registermodernisierung; Errichtung und Betrieb NOOTS

Technischer Leitfaden zur Anbindung von Data Consumern an das Nationale Once-Only-Technical-System (NOOTS)

Version 1.0
14.10.2025

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

Ansprechpartner/-in:

Referat D III 3 - Registermodernisierung; Errichtung und Betrieb NOOTS
Bundesverwaltungsamt
E-Mail: registermodernisierung@bva.bund.de

Inhaltsverzeichnis

1. Einleitung	5
2. Anbindung an das NOOTS	7
2.1. Technische Anbindungsvorbereitung.....	8
2.2. Zertifikatsbeschaffung: Übersicht über die Zertifikate	11
2.2.1 Zertifikat zur Registrierung auf NOVA.....	11
2.2.2 Zertifikate für die technische Kommunikation.....	12
2.2.3 Anforderungen an die Zertifikate.....	13
2.2.4 Zertifikat für die Registrierung über NOVA	14
2.2.5 Zertifikate für die Kommunikation mit dem NOOTS	15
2.2.6 Beschaffung eines Zertifikats der V-PKI/DOI-CA	15
2.2.7 Signierung des Registrierungsformulars für NOVA	30
2.3. Anbindungsverprobung.....	36
2.3.1 Registrierung über NOVA	36
2.3.2 Installation und Konfiguration des Sicheren Anschlussknotens.....	37
2.3.3 Testung.....	55
2.3.4 NOOTS-Readiness-Check Referenzumgebung	57
2.4. Anbindung: NOOTS Testumgebung	58
2.4.1 Registrierung über NOVA	58
2.4.2 Installation und Konfiguration des Sicheren Anschlussknotens.....	59
2.4.3 Testung.....	69
2.4.4 NOOTS-Readiness-Check Testumgebung.....	73
2.5. Anbindung: NOOTS Produktivumgebung.....	74
2.5.1 Registrierung über NOVA	74
2.5.2 Installation und Konfiguration des Sicheren Anschlussknotens.....	75
2.5.3 Bestätigung der Anbindung.....	76

3.	Kontaktmöglichkeiten.....	77
4.	Weiterführende Informationen.....	78
5.	Änderungsverzeichnis.....	80
6.	Abkürzungsverzeichnis / Glossar.....	81
7.	Betrieblich-Relevante Konfigurationsparameter.....	83
8.	Abbildungsverzeichnis	88
9.	Tabellenverzeichnis	90

1. Einleitung

Dieser Leitfaden richtet sich an Betriebsverantwortliche eines **Data Consumer (DC)** bei der Anbindung an das Nationale Once-Only-Technical-System (NOOTS). Data Consumer sind NOOTS-Teilnehmer zum Abruf von Nachweisen und können Online-Dienste, Fachverfahren und die Intermediäre Plattform sein. Data Provider sind NOOTS-Teilnehmer zur Lieferung von Nachweisen.

Die Rollen und Zuständigkeiten gliedern sich dabei wie folgt:

- Fachverantwortliche sind die für das technische Verfahren verantwortliche nachweisanfordernde oder -liefernde Stellen.
- Die das technische Verfahren im Auftrag der Fachverantwortlichen betreibenden sind die Betriebsverantwortlichen. Sie verantworten den technisch korrekten Betrieb des Data Consumer/Data Provider und des Sicheren Anschlussknotens.

Das NOOTS ist ein gemeinsames informationstechnisches System, das aus IT-Komponenten, Schnittstellen und Standards besteht. Es ermöglicht öffentlichen Stellen den Abruf sowie die Übermittlung elektronischer Nachweise und Daten aus öffentlichen Datenbeständen – sowohl national als auch EU-weit – zur Erfüllung ihrer öffentlichen Aufgaben. In der funktionsfähigen Iteration besteht es aus den technischen Komponenten Identity und Access Management für Behörden (IAM-B) und Registerdatennavigation (RDN). Darüber hinaus werden Sichere Anschlussknoten (SAK) für Data Consumer (SAK-DC) und Data Provider (SAK-DP) zur Verfügung gestellt (Abbildung 1). In der ersten Iteration sind nur Onlinedienste als Data Consumer vorgesehen.

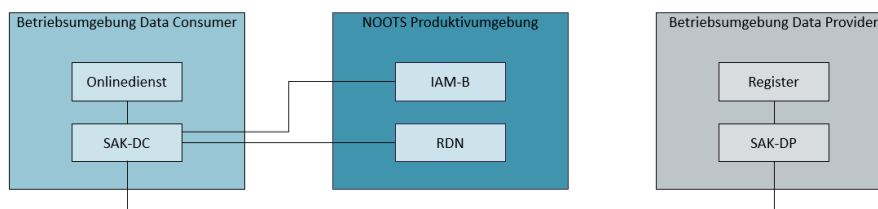


Abbildung 1 - Grobübersicht NOOTS erste Iteration

In diesem Anbindungsleitfaden wird vorausgesetzt, dass das System NOOTS mit seinen Komponenten und Teilnehmenden (z.B. Data Consumer) bekannt ist. Alle weiterführenden Begleitdokumente dazu finden Sie nach der Registrierung auf [NOVA](#). Weitere Links und

Informationen finden Sie im Kapitel 4. Unterstützend finden Sie im Kapitel 6 dieses Dokumentes ein Glossar.

Es gibt drei NOOTS-Umgebungen, an die Data Consumer aufeinanderfolgend angebunden werden müssen:

- NOOTS Referenzumgebung
- NOOTS Testumgebung
- NOOTS Produktivumgebung

Jede Umgebung hat unterschiedliche Eigenschaften und erfüllt im Rahmen der Anbindung eines Data Providers einen bestimmten Zweck:

NOOTS Referenz- umgebung 	• Erste Erprobung der Anbindung des Data Consumer an die NOOTS-Schnittstellen • Erprobung der Anbindung des Data Consumer an die Schnittstelle des SAK-DC • Verwendung generischer bzw. eingespielter Testdaten
NOOTS Test- umgebung 	• Qualifizierte Ende-zu-Ende-Tests unter produktionsähnlichen Bedingungen • Fachliche Tests zwischen Data Consumer und Data Provider (inkl. Fehlerszenarien) möglich • Nur Verwendung von Testdaten
NOOTS Produktiv- umgebung 	• Produktivsystem von NOOTS zum Abruf echter Nachweisdaten • Entwickelte zentrale NOOTS-Komponenten stehen im Echtbetrieb mit ihren Schnittstellen zur Verfügung • Vollumfängliche Wartung und Support

Abbildung 2 - Eigenschaften und Zweck der Umgebungen

2. Anbindung an das NOOTS

Als digitale Anlaufstelle für die NOOTS-Anbindung steht Ihnen während des gesamten Anbindungsprozesses die Webseite [NOVA](#) zur Verfügung. Das Nutzerorientierte Online-Vorregistrierungs- und Anbindungsportal (NOVA) ist das zentrale Anbindungstool für das NOOTS und dient sowohl der Registrierung von anzubindenden Teilnehmern als auch der Weiterverarbeitung der Anbindungsdaten.

Die Anbindung an das NOOTS läuft sequenziell ab. Das heißt, Sie binden Ihren Data Consumer erst an die NOOTS Referenzumgebung, dann an die NOOTS Testumgebung und schließlich an die NOOTS Produktivumgebung an. Die Übergänge zwischen den Umgebungen werden von den sogenannten NOOTS-Readiness-Checks begleitet, sodass ein strukturierter Übergang zwischen den Phasen gewährleistet wird. Insgesamt durchlaufen Sie bei der Anbindung an das NOOTS zwei Readiness-Checks und die Anbindungsbestätigung in der NOOTS Produktivumgebung:

1. NOOTS-Readiness-Check Referenzumgebung

Dieser Check ist abgeschlossen, wenn ein erfolgreicher Testlauf auf der NOOTS Referenzumgebung stattgefunden hat.

2. NOOTS-Readiness-Check Testumgebung

Dieser Check ist abgeschlossen, wenn ein erfolgreicher Testlauf auf der NOOTS Testumgebung stattgefunden hat.

Bestätigung der Anbindung Produktivumgebung

Sie bestätigen, dass eine erfolgreiche Anbindung auf der NOOTS Produktivumgebung stattgefunden hat.

Die einzelnen Schritte zur Anbindung an die NOOTS-Infrastruktur sind in der folgenden Abbildung dargestellt und werden in den weiteren Abschnitten im Detail erläutert.

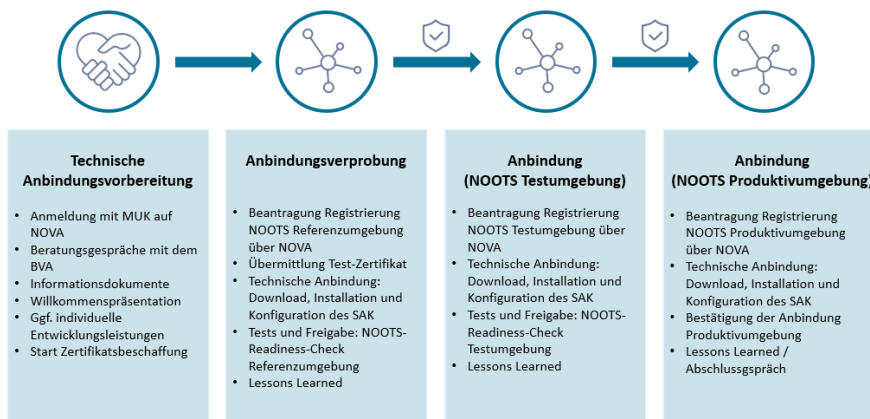
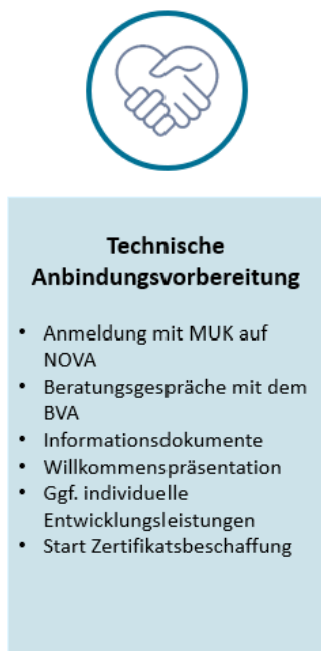


Abbildung 3 - Übersicht Anbindungsprozess

2.1. Technische Anbindungsvorbereitung



Die technische Anbindungsvorbereitung dient der gezielten Vorbereitung Ihrer Anbindung. Dabei werden relevante Informationen gesammelt, bei Bedarf individuelle Entwicklungsleistungen identifiziert und gegebenenfalls weiterführende Beratungsangebote in Anspruch genommen.

Auf der Startseite von NOVA finden Sie allgemeine Informationen zur Anbindung und zum NOOTS. Bei konkretem Interesse an einer Anbindung bitten wir Sie, sich bei NOVA unter [Home - NOVA](#) mit „Mein Unternehmenskonto“ (MUK) anzumelden.

Abbildung 4 – Technische Anbindungsvorbereitung

Bitte nehmen Sie auch Kontakt zum Team Anbindungsbegleitung des BVA unter registermodernisierung@bva.bund.de auf.

Anmelden mit "Mein Unternehmenskonto" (MUK)

Bitte beachten Sie:

Wenn Sie „Zur Anmeldung mit „Mein Unternehmenskonto““ auswählen, werden Sie zum „Serviceportal Gemeinsam Online“ (GO) weitergeleitet. Dort werden Sie um Ihr Einverständnis zur digitalen Zusendung von Bescheiden / der Rückmeldung in das Postfach Ihres „Mein Unternehmenskonto“ gebeten. Nach Zustimmung gelangen Sie zum Login mit ELSTER auf „Mein Unternehmenskonto“ (MUK). Bitte laden Sie dort Ihr persönliches zu Ihrem Unternehmen gehöriges Elster-Unternehmenszertifikat hoch und geben das zugehörige Passwort ein. Daraufhin müssen Sie die Datenweitergabe an NOVA bestätigen. Sie werden danach zurück zu NOVA geleitet. Bitte beachten Sie zusätzlich die Hinweise auf den Seiten des „Serviceportal Gemeinsam Online“ und auf „Mein Unternehmenskonto“.

Zur Anmeldung mit "Mein Unternehmenskonto"

MUK Freischaltung für NOVA

Wenn für Ihre Organisation in der **Berechtigungssteuerung**, die Kontoberechtigung aktiviert ist, muss die Nutzung von NOVA zunächst für Ihr Benutzerkonto freigeschaltet werden. Ansonsten erhalten Sie nach der Anmeldung den Hinweis „Für den Online-Dienst NOVA fehlen Ihnen offenbar die erforderlichen Berechtigungen“.

Wenden Sie sich zur Freischaltung bitte an die Person in Ihrer Organisation mit Administrator-Berechtigung bei MUK.

Weiterführende Informationen für nutzende Organisationen finden Sie [hier](#).

Abbildung 5 - Anmeldung mit MUK

Wenn Sie mehr über die Erstellung eines MUK und die Anmeldung auf NOVA erfahren möchten, finden Sie [hier](#) weiterführende Informationen. Nach der initialen Anmeldung mit Ihrem MUK stehen Ihnen umfangreiche Informationsunterlagen unter dem Abschnitt „Begleitdokumentation“ bereit.

IT-PLANUNGSRAT

GO FIT CO

Dashboard

Hilfe und Support

Begleitdokumente

Login/Logout

Begleitdokumente zur NOOTS-Anbindung

Auf dieser Seite finden Sie relevante Begleitdokumente zur Anbindung an das NOOTS.

Die Dokumente unterstützen Sie bei der Planung, Umsetzung und technischen Integration Ihrer Systeme von der initialen Architekturübersicht bis zur konkreten Schnittstellenbeschreibung.

Dokumentenübersicht

Ausgewählte Architekturdokumente

Ausgewählte Architekturdokumente aus dem Konsultationsprozess zum NOOTS

High-Level-Architecture (HLA)

Anschlusskonzept Data Consumer (DC)

Anschlusskonzept Data Provider (DP)

Technische Arbeitshilfen zur Anbindung

Abbildung 6 - Begleitdokumente zur NOOTS-Anbindung

Unter den Begleitdokumenten auf NOVA finden Sie auch die sogenannte Willkommenspräsentation mit Informationen zu technischen und fachlichen Grundlagen für die Anbindung. Bitte sehen

Sie sich die Willkommenspräsentation für den ersten Einstieg an, ,
bevor Sie dieses Dokument weiterlesen. Sie legt Ihnen folgende Inhalte
dar:

- Wie sich der Anbindungsprozess gestaltet
- Welche Schritte Sie erwarten
- Welche Rolle NOVA dabei spielt
- Wo Sie Unterstützung erhalten können

Wenn Sie Fragen zur Umsetzung der erforderlichen Voraussetzungen
haben, stehen wir Ihnen unter dataportnootssupport@dataport.de
gern zu Verfügung. Zu Beginn des Anbindungsprozesses sollten Sie mit
der Beschaffung der notwendigen Zertifikate für die NOOTS
Testumgebung starten. Die dafür notwendigen Informationen finden
Sie im nächsten Kapitel dieses Dokumentes detailliert aufgeführt.

2.2. Zertifikatsbeschaffung: Übersicht über die Zertifikate

HINWEIS: Für die **Anbindung** an das **NOOTS** benötigen Sie bestimmte **Zertifikate**, die Sie **selbst beschaffen** müssen. Der Erwerb der Zertifikate nimmt eine **gewisse Zeit in Anspruch**, sodass wir Ihnen empfehlen, den Prozess der Beschaffung noch in der Phase der technischen Anbindungsvorbereitung anzustoßen.

Für die Anbindung an das NOOTS benötigen Sie unterschiedliche Zertifikate, deren Beschaffung frühzeitig eingeleitet werden sollte. Die Beschaffung übernehmen in der Regel die Betriebsverantwortlichen in Abstimmung mit bzw. im Auftrag der Fachverantwortlichen.

Als DC benötigen Sie die Zertifikate, die in diesem Dokument beschrieben werden, erst für die Anbindung an die NOOTS Test- und Produktivumgebung.

Für die Anbindung an das NOOTS benötigen Sie Zertifikate für zwei voneinander unabhängige Zwecke:

- Zur Registrierung auf NOVA
- Für die technische Kommunikation

Das **Zertifikat** für die **Registrierung auf NOVA** wird ausschließlich **im Anbindungsprozess** benötigt. Die **Zertifikate** für die **technische Kommunikation** sind **dauerhaft** bei erfolgtem Anschluss an NOOTS im Einsatz.

Hinweis: Bitte berücksichtigen Sie, dass Zertifikate grundsätzlich eine begrenzte Gültigkeitsdauer besitzen. Prüfen Sie daher immer eigenverantwortlich welche Ihrer verwendeten Zertifikate wann ablaufen und welche Schritte für die rechtzeitige Verlängerung erforderlich sind. Für die elektronische Signierung von Dokumenten können Sie 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 (z.B. Adobe Acrobat Pro, Governikus DATA Boreum oder SecSigner von SecCommerce). Sofern Sie noch nicht mit dieser Software ausgestattet sind, leiten Sie bitte deren Installation auf Ihrem PC bzw. Laptop ein.

2.2.1 Zertifikat zur Registrierung auf NOVA

Auf NOVA benötigen Sie als Betriebsverantwortliche ein personenbezogenes Zertifikat, welches eine digitale Signatur unterstützt um sich für die NOOTS-Test- und Produktivumgebung zu

registrieren. Mit diesem Zertifikat signieren Sie die Registrierungsformulare, die Sie auf NOVA ausgefüllt hochladen. Das Signaturzertifikat dient der Authentisierung und ermöglicht eine Prüfung, ob das Dokument während des Transportes verändert wurde. Sie können für beide Registrierungsformulare dasselbe Zertifikat nutzen. Wenn Sie bereits ein personenbezogenes Signaturzertifikat besitzen, welches die im Abschnitt 2.2.3 genannten Anforderungen erfüllt, können Sie auch dieses verwenden.

2.2.2 Zertifikate für die technische Kommunikation

Für die technische Kommunikation mit dem NOOTS benötigen der Data Consumer und Data Provider unterschiedliche Zertifikate.

Hier finden Sie einen Überblick für die NOOTS Produktivumgebung:

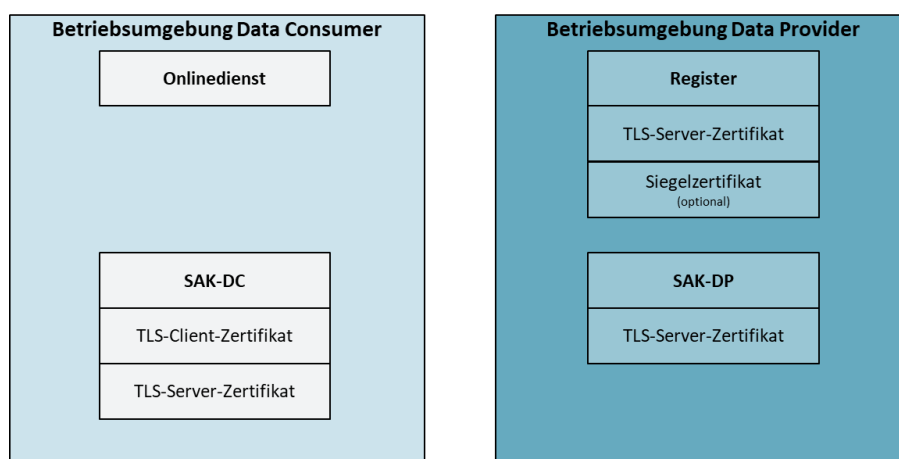


Abbildung 7 - Übersicht Zertifikate NOOTS Produktivumgebung

Für einen **Data Consumer** werden für die Kommunikation mit dem NOOTS insgesamt fünf Zertifikate benötigt, von denen jedoch eines für Sie bereitgestellt wird. Bei dem TLS-Server-Zertifikat für die NOOTS Referenzumgebung handelt es sich um ein zusätzliches optionales Zertifikat, welches nicht zwingend beschafft werden muss. Das TLS-Client-Zertifikat für die NOOTS Referenzumgebung wird Ihnen zur Verfügung gestellt.

NOOTS Referenzumgebung	NOOTS Testumgebung	NOOTS Produktivumgebung
TLS-Server-Zertifikat des SAK-DC (optional)	TLS-Server-Zertifikat des SAK-DC	TLS-Server-Zertifikat des SAK-DC

<i>TLS-Client-Zertifikat des SAK-DC (wird bereitgestellt)</i>	TLS-Client-Zertifikat des SAK-DC	TLS-Client-Zertifikat des SAK-DC
---	-------------------------------------	-------------------------------------

Tabelle 1 - Übersicht Zertifikate Data Consumer

Das TLS-Server-Zertifikat des SAK-DC dient ausschließlich der Kommunikation zwischen Onlinedienst und SAK-DC innerhalb der Betriebsumgebung des Data Consumers. Das TLS-Client-Zertifikat des SAK-DC wird für die Authentisierung des Data Consumers am IAM-B benötigt und ermöglicht in Ergänzung zu den jeweiligen TLS-Server-Zertifikaten eine sichere mTLS-Verbindung mit den zentralen NOOTS-Komponenten und dem SAK-DP. Bei der Registrierung über NOVA müssen Sie für die NOOTS Test- und Produktivumgebung das TLS-Client-Zertifikat des SAK-DC im PEM-Format in das Registrierungsformular einfügen.

2.2.3 Anforderungen an die Zertifikate

Sowohl an das Zertifikat für die Registrierung über NOVA als auch an die Zertifikate für die Kommunikation mit NOOTS werden verschiedene Anforderungen gestellt. In der nachfolgenden Tabelle finden Sie eine Übersicht über die gestellten Anforderungen, die in den nachfolgenden Abschnitten vertieft werden.

Umgebung	Zertifikat	Anforderung
NOVA	Personenbezogenes Signaturzertifikat	Personenbezogenes Zertifikat der V-PKI/DOI-CA
NOOTS Referenzumgebung	TLS-Server-Zertifikat des SAK-DC (optional)	geeignetes TLS-Zertifikat zur Gewährleistung der Transportverschlüsselung
	TLS-Client-Zertifikat des SAK-DC	Bereitstellung durch Seitenbau / Dataport
NOOTS Testumgebung	TLS-Server-Zertifikat des SAK-DC	geeignetes TLS-Zertifikat zur Gewährleistung der Transportverschlüsselung
	TLS-Client-Zertifikat des SAK-DC	gruppenbezogenes Zertifikat (Test) der V-PKI/DOI-CA
NOOTS Produktivumgebung	TLS-Server-Zertifikat des SAK-DC	geeignetes TLS-Zertifikat zur Gewährleistung der Transportverschlüsselung
	TLS-Client-Zertifikat des SAK-DC	gruppenbezogenes Zertifikat der V-PKI/DOI-CA

Tabelle 2 - Übersicht Anforderungen Zertifikate Data Consumer

Die nachfolgende Abbildung stellt die Kommunikation zwischen DC und DP beispielhaft für die NOOTS Produktivumgebung dar. Diese Darstellung ist zur Übersichtlichkeit und Verständlichkeit in ihrer Komplexität stark vereinfacht. Es sind nur diejenigen Zertifikate erwähnt, die durch DC bzw. DP zu beschaffen sind. Die Pfeile symbolisieren die Richtung des Verbindungsaufbaus.

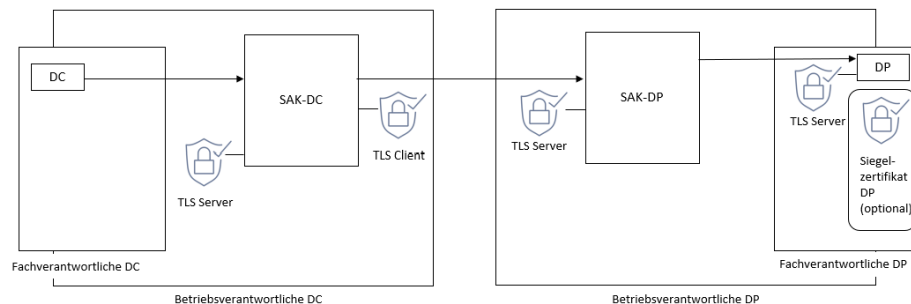


Abbildung 8 - Übersicht Komponenten und Zertifikate zur Beschaffung durch DC/DP in der NOOTS Produktivumgebung

2.2.4 Zertifikat für die Registrierung über NOVA

Für die Registrierung über NOVA für die unterschiedlichen Umgebungen benötigt eine bei den Betriebsverantwortlichen beschäftigte Person ein personenbezogenes Signaturzertifikat. Das Zertifikat muss ein personenbezogenes Zertifikat der V-PKI/DOI-CA sein.

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.

Das benötigte Zertifikat erhalten Sie, sofern noch nicht vorhanden, 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-Stellen (Registration Authority, Registrierungsstellen) zusammen. Die DOI-CA stellt ausschließlich Zertifikate für Teilnehmer der öffentlichen Verwaltung aus. Dritte können Zertifikate erhalten, sofern das Erfordernis von öffentlicher Stelle bestätigt wird.

Eine Anleitung zur Beschaffung von Zertifikaten der V-PKI/DOI-CA ist im Kapitel 2.2.6 zu finden.

2.2.5 Zertifikate für die Kommunikation mit dem NOOTS

Für die NOOTS Referenzumgebung, NOOTS Test- und Produktivumgebung werden für die Zertifikate des Data Consumer in Teilen verschiedene Eigenschaften vorausgesetzt.

NOOTS Referenzumgebung

Das **TLS-Server-Zertifikat des SAK-DC** muss ein geeignetes TLS-Zertifikat zur Gewährleistung der Transportverschlüsselung sein. Die Entscheidung über den Zertifikatstyp, die Beschaffung und die Installation obliegen den Betriebsverantwortlichen. Dieses Zertifikat ist auf der NOOTS Referenzumgebung nicht verpflichtend. Die Entscheidung über die Verwendung liegt in der Verantwortung des DC.

Das **TLS-Client-Zertifikat des SAK-DC** wird für die NOOTS Referenzumgebung bereitgestellt.

NOOTS Testumgebung

Das **TLS-Server-Zertifikat des SAK-DC** muss ein geeignetes TLS-Zertifikat zur Gewährleistung der Transportverschlüsselung sein. Die Entscheidung über den Zertifikatstyp, die Beschaffung und die Installation obliegt den Betriebsverantwortlichen.

Das **TLS-Client-Zertifikat des SAK-DC** für die sicheren Verbindungen per mTLS zum IAM-B, zur RDN und zum SAK-DP ist als gruppenbezogenes Zertifikat/gruppenbezogenes Zertifikat (Test) der V-PKI/DOI-CA zu beziehen. Für die Anbindung an die NOOTS Testumgebung sind in diesem Fall auch gruppenbezogene Test-Zertifikate der V-PKI/DOI-CA zugelassen.

NOOTS Produktivumgebung

Das **TLS-Server-Zertifikat** muss, ein geeignetes TLS-Zertifikat zur Gewährleistung der Transportverschlüsselung sein. Die Entscheidung über den Zertifikatstyp, die Beschaffung und die Installation obliegt den Betriebsverantwortlichen.

Das **TLS-Client-Zertifikat** ist für die NOOTS Produktivumgebung als gruppenbezogenes Zertifikat der V-PKI/DOI-CA zu beziehen.

2.2.6 Beschaffung eines Zertifikats der V-PKI/DOI-CA

Dieser Abschnitt orientiert sich am „Benutzerhandbuch Teilnehmer [NdB-VN104]“ der Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben. Er dient der

Konkretisierung des Prozesses der Beschaffung eines Zertifikats der V-PKI/DOI-CA für diesen speziellen Anwendungsfall. Untenstehend wird erläutert, wie Sie Zugriff auf das Benutzerhandbuch erhalten.

Die Beantragung der Zertifikate der V-PKI/DOI-CA erfolgt durch die Betriebsverantwortlichen bzw. in ihrem Auftrag über die Registrierungsstellen der DOI-CA. Die Fachverantwortlichen sollte die Betriebsverantwortlichen hierbei in fachlichen Rückfragen beratend unterstützen.

Der Prozess beinhaltet folgende Schritte:

1. Zugangsdaten für Webportal der Zertifizierungsstelle beantragen
2. Antrag ausfüllen
3. Antrag einreichen
4. Zertifikat der V-PKI/DOI-CA erhalten

Zu 1.) Zugangsdaten für Webportal der Zertifizierungsstelle beantragen

Wenn Sie bereits Zugangsdaten für den Zugang zum Webportal (und, falls gewünscht, für die Beantragung eines gruppenbezogenen Zertifikats (Test) zur Testumgebung des Webportals) der Zertifizierungsstelle haben, können Sie diesen Schritt überspringen. Anderenfalls beantragen Sie bitte per E-Mail Zugangsdaten bei der für Ihre Organisation zuständigen Registrierungsstelle. Als Data Consumer und Data Provider der Bundesländer Bremen, Hamburg, Sachsen-Anhalt und Schleswig-Holstein wenden Sie sich an dataportzentraleregistrierungsstellepki@dataport.de.

Alternativ bzw. sollte Ihnen Ihre Registrierungsstelle nicht bekannt sein, steht Ihnen die Registrierungsstelle "Öffentliche Verwaltung" (smc-berlin.tsi@telekom.de) zur Verfügung.

Zu 2.) Antrag ausfüllen

Startseite Kontakt

Benutzer Bereich Öffentlicher Bereich

Version: 5.4.3

Anmelden

Zum Management Ihrer Zertifikate ist es erforderlich, dass Sie sich gegenüber den Benutzer-Web-Seiten autorisieren. Bitte melden Sie sich dazu mit den Ihnen zur Verfügung gestellten Zugangsdaten an.

Sollten Sie keine Zugangsdaten bekommen haben, so wenden Sie sich bitte an Ihre zuständige Registrierungsstelle.

Login:

Passwort:

Anmelden Abbrechen

© 2025 Deutsche Telekom Security GmbH. Alle Rechte vorbehalten. Deutsche Telekom Impressum Datenschutz

Abbildung 9 - Anmelden im Webportal der Zertifizierungsstelle

Wenn Ihnen die Zugangsdaten vorliegen, können Sie sich über [DOI | Anmelden](#) im Webportal der Zertifizierungsstelle anmelden. Zur Beantragung eines gruppenbezogenen Zertifikats (Test) der V-PKI/DOI-CA können Sie sich für die Testumgebung des Webportals der Zertifizierungsstelle [hier](#) anmelden. Der dargestellte Prozess gilt für die Produktivumgebung des Webportals der Zertifizierungsstelle. Der Prozess für die Beantragung in der Testumgebung ist sehr ähnlich und kann ebenso über die folgende Beschreibung nachvollzogen werden.

Für die Anbindung an das NOOTS benötigen Sie zum einen ein personenbezogenes Zertifikat der V-PKI/DOI-CA für die Registrierung über NOVA sowie zusätzlich als Data Consumer 2 gruppenbezogene Zertifikate der V-PKI/DOI-CA, von denen eines ein Testzertifikat sein darf.

Beantragung eines personenbezogenen Zertifikats

The screenshot shows the NdB (Netzwerk des Bundes) web interface. On the left is a sidebar menu with options: TCOS-Smartcard-Zertifikat, Software-Zertifikat (highlighted), beantragen (highlighted in red), abholen, Zertifikat sperren, Zertifikate prüfen, Sperrlisten, CA-Zertifikate, Dokumente, and Abmelden. The main content area is titled 'Auswahl der Domäne'. It instructs the user to select a sub-domain and confirm with 'Weiter'. A note states: 'Hinweis: Die Sub-Domäne wird in das Zertifikat als "Organizational Unit (OU)" übernommen.' Below this, there are two dropdown menus: 'Master-Domäne (O): Sachsen-Anhalt' and '* Sub-Domäne (OU):' (which is currently empty). At the bottom of the main area are 'Weiter' and 'Abbrechen' buttons. The footer contains copyright information for Deutsche Telekom Security GmbH and links to Impressum and Datenschutz.

Abbildung 10 - Auswahl der Domäne

Für die Beantragung eines personenbezogenen Zertifikats klicken Sie im Menüpunkt „Software-Zertifikat“ auf „beantragen“ und wählen eine geeignete Sub-Domäne aus. Welche Sub-Domäne zu wählen ist, stimmen Sie bitte mit der für Sie zuständigen Registrierungsstelle ab. Sofern vorhanden empfehlen wir Ihnen jedoch die Sub-Domäne NOOTS auszuwählen.

Bitte klicken Sie auf „Weiter“.

The screenshot shows the NdB web interface at the 'Auswahl des Zertifikatstyps' (Certificate Type Selection) step. The sidebar menu is identical to the previous screenshot. The main content area instructs the user to select a certificate type and confirm with 'Weiter'. It shows two radio button options: 'Personenbezogenes Zertifikat' (selected) and 'Gruppen-/Funktions-Zertifikat'. At the bottom of the main area are 'Weiter', 'Zurück', and 'Abbrechen' buttons. The footer contains the same copyright and link information as the previous screenshot.

Abbildung 11 - Auswahl des Zertifikatstyps

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

The screenshot shows the NdB application interface. On the left is a sidebar menu with options like 'TCOS-Smartcard-Zertifikat', 'Software-Zertifikat', and 'beantragen'. The main area is titled 'Daten des Antragstellers/Schlüsselverantwortlichen'. It contains a form with fields for Name, Vorname, Titel, Dienststelle, Straße, Nr., PLZ, Ort, Telefon, and E-Mail. Each field has a maximum character count. Below the form are buttons for 'Weiter', 'Zurück', and 'Abbrechen'. At the bottom, there is a copyright notice for Deutsche Telekom Security GmbH and links to Impressum and Datenschutz.

Version: 5.4.3

Angemeldet in: Sachsen-Anhalt

Daten des Antragstellers/Schlüsselverantwortlichen

Bitte geben Sie hier Ihre Anschrift und Kontaktdaten ein.

Hinweis: Bitte beachten Sie, dass für Gruppenzertifikate besondere Regelungen gelten, die Sie als Schlüsselverantwortlicher beachten müssen. Siehe dazu auch das Dokument [NdB-VN110], welches Sie im Bereich [Dokumente](#) herunterladen können.

Bitte geben Sie unter "E-Mail" Ihre persönliche (dienstliche) E-Mail-Adresse an. Bei Angabe eines Funktionspostfachs muss der Antrag leider ABGELEHNT werden, da diese Daten nach Antragseinreichung nicht mehr geändert werden können!

* Name: Mustermann (max. 64 Zeichen)

* Vorname: Max (max. 64 Zeichen)

Titel: (max. 64 Zeichen)

* Dienststelle: Behörde Musterstadt (max. 128 Zeichen)

* Straße: Teststraße (max. 64 Zeichen)

* Nr.: 1 (max. 5 Zeichen)

* PLZ: 12122 (max. 5 Zeichen)

* Ort: Musterstadt (max. 64 Zeichen)

* Telefon: +49 12312312312 (max. 64 Zeichen)

* E-Mail: test@testbehörde.de (max. 128 Zeichen)

Weiter Zurück Abbrechen

© 2025 Deutsche Telekom Security GmbH. Alle Rechte vorbehalten. Deutsche Telekom Impressum Datenschutz

Abbildung 12 - Erfassung der Daten des Antragstellers

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 der Behörde gehören. Die Angabe von E-Mailadressen zu Gruppen-/Funktionspostfächern ist nicht zulässig und führt zur Ablehnung des Antrags.

The screenshot shows the NdB application interface for certificate data entry. The sidebar menu is the same as in the previous screenshot. The main area is titled 'Zertifikatsdaten: Name und E-Mail-Adresse'. It contains a form with fields for 'Common-Name (CN)' and 'E-Mail-Adresse (SAN)'. Each field has a maximum character count. Below the form are buttons for 'Weiter', 'Zurück', and 'Abbrechen'. At the bottom, there is a copyright notice for Deutsche Telekom Security GmbH and links to Impressum and Datenschutz.

Version: 5.4.3

Angemeldet in: Sachsen-Anhalt

Zertifikatsdaten: Name und E-Mail-Adresse

Ihre im vorherigen Schritt erfassten Angaben zu Name und E-Mail-Adresse werden wie folgt in das Zertifikat übernommen:

- Der "CommonName" (CN) des Zertifikats wird aus Ihren Namen, Titel und Vornamen gebildet.
- Ihre E-Mail-Adresse wird in das Attribut "SubjectAlternativeName" übernommen.

* Common-Name (CN): (max. 64 Zeichen)

* E-Mail-Adresse (SAN): (max. 128 Zeichen)

Weiter Zurück Abbrechen

© 2025 Deutsche Telekom Security GmbH. Alle Rechte vorbehalten. Deutsche Telekom Impressum Datenschutz

Abbildung 13 - Erfassung der Zertifikatsdaten für personenbezogenes Zertifikat

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

The screenshot shows the NdB web interface. On the left is a sidebar menu with options: TCOS-Smartcard-Zertifikat, Software-Zertifikat (highlighted in pink with a sub-option 'beantragen' also highlighted), Zertifikat sperren, Zertifikate prüfen, Sperrlisten, CA-Zertifikate, Dokumente, and Abmelden. The main content area is titled 'Zertifikatsdaten: Weitere Angaben (optional)'. It contains instructions: 'Hier können Sie, sofern erforderlich, weitere Angaben machen, die in das Zertifikat übernommen werden: Der Dienstort wird als Attribut "Locality" (L) in das Zertifikat übernommen. Die Kennungen 1 und 2 werden als weitere Attribute "Organizational Unit" (OU) in das Zertifikat übernommen.' Below this are three input fields: 'Dienstort (L):' (max. 128 Zeichen), 'Kennung 1 (OU2):' (max. 64 Zeichen), and 'Kennung 2 (OU3):' (max. 64 Zeichen). At the bottom are buttons for 'Weiter', 'Zurück', and 'Abbrechen'. The top right shows 'Angemeldet in: Sachsen-Anhalt' and links for 'Startseite' and 'Kontakt'. The bottom footer contains copyright information: '© 2025 Deutsche Telekom Security GmbH. Alle Rechte vorbehalten.' and links for 'Deutsche Telekom', 'Impressum', and 'Datenschutz'.

Abbildung 14 - Erfassung der Zertifikatsdaten für personenbezogenes Zertifikat: Weitere Angaben

Im nächsten Schritt können Sie optional weitere Informationen eingeben. Bitte klicken Sie anschließend auf „Weiter“.

Die Notwendigen Schritte zur Beantragung eines personenbezogenen Zertifikats sind nun abgeschlossen. Bitte lesen Sie jetzt bei Abschließende Tätigkeiten weiter.

Beantragung eines gruppenbezogenen Zertifikates

The screenshot shows the NdB web interface for domain selection. The sidebar menu is the same as in the previous screenshot, with 'Software-Zertifikat' and 'beantragen' highlighted. The main content area is titled 'Auswahl der Domäne'. It contains instructions: 'Bitte wählen Sie die Sub-Domäne aus und bestätigen Sie die Auswahl mit "Weiter". Hinweis: Die Sub-Domäne wird in das Zertifikat als "Organizational Unit" (OU) übernommen.' Below this are two dropdown menus: 'Master-Domäne (O):' and '* Sub-Domäne (OU):'. At the bottom are buttons for 'Weiter' and 'Abbrechen'. The top right shows 'Angemeldet in: Sachsen-Anhalt' and links for 'Startseite' and 'Kontakt'. The bottom footer contains copyright information: '© 2025 Deutsche Telekom Security GmbH. Alle Rechte vorbehalten.' and links for 'Deutsche Telekom', 'Impressum', and 'Datenschutz'.

Abbildung 15 - Erfassung der Zertifikatsdaten für gruppenbezogenes Zertifikat: Auswahl der Domäne

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

Version: 5.4.3

Angemeldet in: Sachsen-Anhalt

Auswahl des Zertifikatstyps

Bitte wählen Sie den Zertifikatstyp aus und bestätigen Sie die Auswahl mit "Weiter".

* Zertifikatstyp: ☐ Personenbezogenes Zertifikat ☒ Gruppen-/Funktions-Zertifikat

© 2025 Deutsche Telekom Security GmbH. Alle Rechte vorbehalten. Deutsche Telekom Impressum Datenschutz

Abbildung 16 - Auswahl des Zertifikatstyps für Gruppen-/Funktions-Zertifikat

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

Version: 5.4.3

Angemeldet in: Sachsen-Anhalt

Daten des Antragstellers/Schlüsselverantwortlichen

Bitte geben Sie hier Ihre Anschrift und Kontaktdaten ein.
Hinweis: Bitte beachten Sie, dass für Gruppenzertifikate besondere Regelungen gelten, die Sie als Schlüsselverantwortlicher beachten müssen. Siehe dazu auch das Dokument [NdB-VN110], welches Sie im Bereich [Dokumente](#) herunterladen können.

Bitte geben Sie unter "E-Mail" Ihre persönliche (dienstliche) E-Mail-Adresse an. Bei Angabe eines Funktionspostfachs muss der Antrag leider ABGELEHNT werden, da diese Daten nach Antragseinreichung nicht mehr geändert werden können!

* Name:	Mustermann	(max. 64 Zeichen)
* Vorname:	Max	(max. 64 Zeichen)
Titel:		(max. 64 Zeichen)
* Dienststelle:	Behörde Musterstadt	(max. 128 Zeichen)
* Straße:	Teststraße	(max. 64 Zeichen)
* Nr.:	1	(max. 5 Zeichen)
* PLZ:	12122	(max. 5 Zeichen)
* Ort:	Musterstadt	(max. 64 Zeichen)
* Telefon:	+49 12312312312	(max. 64 Zeichen)
* E-Mail:	test@testbehörde.de	(max. 128 Zeichen)

© 2025 Deutsche Telekom Security GmbH. Alle Rechte vorbehalten. Deutsche Telekom Impressum Datenschutz

Abbildung 17 - Erfassung der Daten des Antragstellers für Gruppen-/Funktions-Zertifikat

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 der Behörde 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.

The screenshot shows the 'Zertifikatsdaten: Name und E-Mail-Adresse' form. On the left is a sidebar with a menu: TCOS-Smartcard-Zertifikat, Software-Zertifikat (selected), beantragen (highlighted), abholen, Zertifikat sperren, Zertifikate prüfen, Sperrlisten, CA-Zertifikate, Dokumente, and Abmelden. The main content area has the title 'Zertifikatsdaten: Name und E-Mail-Adresse' and instructions: 'Bitte geben Sie hier einen aussagekräftigen Namen und eine E-Mail-Adresse der Gruppe oder Funktion ein, für die das Zertifikat beantragt wird.' It includes a 'Hinweise' section with two bullet points: 'Der Name ("CommonName", CN) muss gemäß Policy mit dem Zusatz "GRP:" beginnen.' and 'Als E-Mail-Adresse muss eine zentrale E-Mail-Adresse bzw. ein Funktionspostfach eingetragen werden!'. Below this are two input fields: '* Gruppen-/Funktionsname (CN):' with the value 'GRP: Testbehörde' (max. 64 Zeichen) and '* E-Mail-Adresse (SAN):' with the value 'FuPo@testbehoerde.de' (max. 128 Zeichen). At the bottom are three buttons: 'Weiter', 'Zurück', and 'Abbrechen'. The footer contains copyright information and links to 'Deutsche Telekom', 'Impressum', and 'Datenschutz'.

Abbildung 18 - Erfassung der Zertifikatsdaten für Gruppen-/Funktions-Zertifikat

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

Tragen Sie darüber hinaus den Namen der beantragenden Einrichtung sowie der Abteilung nach dem GRP: ein. Die Einrichtung und Abteilung muss anhand dessen eindeutig identifizierbar sein.

Spezifizieren Sie das Einsatzgebiet des SAK-DC am Ende des Feldes.

Dies ist vor allem dann wichtig, wenn Sie in ihrer Einrichtung planen, mehrere SAK-DCs zu betreiben.

Beispiel: GRP: Rechenzentrum Musterstadt AöR IT Sicherheit:SAK-DC:Online-Dienste

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

The screenshot shows the 'Zertifikatsdaten: Weitere Angaben (optional)' form. The sidebar is identical to the previous form. The main content area has the title 'Zertifikatsdaten: Weitere Angaben (optional)' and instructions: 'Hier können Sie, sofern erforderlich, weitere Angaben machen, die in das Zertifikat übernommen werden:'. It includes two bullet points: 'Der Dienstort wird als Attribut "Locality" (L) in das Zertifikat übernommen.' and 'Die Kennungen 1 und 2 werden als weitere Attribute "Organizational Unit" (OU) in das Zertifikat übernommen.' Below this are three input fields: 'Dienstort (L):' (max. 128 Zeichen), 'Kennung 1 (OU2):' (max. 64 Zeichen), and 'Kennung 2 (OU3):' (max. 64 Zeichen). At the bottom are three buttons: 'Weiter', 'Zurück', and 'Abbrechen'. The footer contains copyright information and links to 'Deutsche Telekom', 'Impressum', and 'Datenschutz'.

Abbildung 19 - Erfassung der Zertifikatsdaten für Gruppen-/Funktions-Zertifikat: Weitere Angaben

Nutzen Sie die Felder der weiteren Angaben für die folgenden Informationen:

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

Nutzen Sie die optionalen Felder OU2 und OU3 für die nähere Beschreibung Ihrer konkreten Organisationseinheit bzw. Abteilung innerhalb der im CN angegebenen Einrichtung.

Abschließende Tätigkeiten

The screenshot shows the NdB portal interface. On the left is a sidebar with a menu: TCOS-Smartcard-Zertifikat, Software-Zertifikat (highlighted), beantragen (highlighted), abholen, Zertifikat sperren, Zertifikate prüfen, Sperrlisten, CA-Zertifikate, Dokumente, and Abmelden. The main content area is titled 'Veröffentlichung, Hash-Algorithmus, Schlüsseltyp und Sperrung des Zertifikats'. It contains instructions for publishing and revoking certificates. There are three main sections: 'Veröffentlichung im VoD' with radio buttons for 'Ja' and 'Nein' (selected), 'Hash-Algorithmus' with a dropdown menu, 'Schlüsseltyp' with a dropdown menu, and 'Sperrpasswort' with a text input field (max. 32 Zeichen). At the bottom are buttons for 'Weiter', 'Zurück', and 'Abbrechen'. The footer includes '© 2025 Deutsche Telekom Security GmbH. Alle Rechte vorbehalten.' and 'Deutsche Telekom Impressum Datenschutz'.

Abbildung 20 - Veröffentlichung und Sperrung des Zertifikats

Sie können auswählen, ob Sie Ihr Zertifikat im öffentlichen Verzeichnisdienst der Verwaltung (VoD) im Internet veröffentlichen wollen. Als Hash-Algorithmus und Schlüsseltyp sind die folgenden Angaben auszuwählen:

Hash-Algorithmus: SHA256

Schlüsseltyp (Signatur): ECC NIST P-256

The screenshot shows the NdB portal interface for the 'Abrechnung des beantragten Zertifikats' page. The sidebar is identical to the previous screenshot. The main content area is titled 'Abrechnung des beantragten Zertifikats'. It contains a text input field for 'Abrechnungsinformation 3:' (max. 60 Zeichen). At the bottom are buttons for 'Weiter', 'Zurück', and 'Abbrechen'. The footer includes '© 2025 Deutsche Telekom Security GmbH. Alle Rechte vorbehalten.' and 'Deutsche Telekom Impressum Datenschutz'.

Abbildung 21 - Abrechnung des beantragten Zertifikats

Bitte geben Sie die Daten zur Abrechnung des Zertifikats an und bestätigen Sie mit „Weiter“. Die Maske zur Abrechnung kann sich je nach abgestimmten Abrechnungsprozess unterscheiden. Die Kosten für das Zertifikat müssen von den Betriebsverantwortlichen oder

Fachverantwortlichen getragen werden. Dies müssen Sie mit den Fachverantwortlichen abstimmen.

The screenshot shows the NdB web interface. At the top left, there are logos for 'T' and 'NdB'. The version '5.4.3' is displayed. The user is logged in as 'Sachsen-Anhalt'. The left sidebar contains a menu with options: 'TCOS-Smartcard-Zertifikat', 'Software-Zertifikat' (highlighted), 'beantragen', 'abholen', 'Zertifikat sperren', 'Zertifikate prüfen', 'Sperrlisten', 'CA-Zertifikate', 'Dokumente', and 'Abmelden'. The main content area is titled 'Mitteilung an die Registrierungsstelle' and contains the text: 'Hier können Sie optional der zuständigen Registrierungsstelle eine Kurzmitteilung (bis max. 170 Zeichen) zur Bearbeitung Ihres Antrags eingeben.' Below this is a text input field labeled 'Mitteilungen an die RA:'. At the bottom of the form are three buttons: 'Weiter', 'Zurück', and 'Abbrechen'. The footer contains the copyright notice '© 2025 Deutsche Telekom Security GmbH. Alle Rechte vorbehalten.' and links to 'Deutsche Telekom', 'Impressum', and 'Datenschutz'.

Abbildung 22 - Mitteilung an die Registrierungsstelle

Wenn Sie möchten, können Sie eine Mitteilung an Ihre Registrierungsstelle verfassen. Bitte bestätigen Sie mit „Weiter“.

Version: 5.4.3

Angemeldet in: Sachsen-Anhalt

Zusammenfassung der Antragsdaten, Absenden des Antrags

Nachfolgend werden Ihnen die eingegebenen Daten noch mal zusammengefasst angezeigt.
Über den Button "Zurück" können Sie zurück in die Eingabe wechseln und bei Bedarf die Daten korrigieren.
Mit "Absenden" wird Ihr Antrag zum Trust Center gesendet und Ihnen anschließend das daraus erstellte Antragsformular zum Download als PDF-Dokument angeboten.

Domänen-Hierarchie

Land (C): DE

Master-Domäne (O): Sachsen-Anhalt

Sub-Domäne (OU): [redacted]

Zertifikatstyp

Zertifikatstyp: Personenbezogenes Zertifikat

Daten des Antragstellers

Name: [redacted]

Vorname: [redacted]

Titel: [redacted]

Dienststelle: [redacted]

Straße: [redacted]

Nr.: [redacted]

PLZ: [redacted]

Ort: [redacted]

Telefon: [redacted]

E-Mail: [redacted]

Zertifikatsdaten: Name und E-Mail-Adresse

Common-Name (CN): [redacted]

E-Mail-Adresse (SAN): [redacted]

Zertifikatsdaten: Weitere Angaben (optional)

Dienstort (L): [redacted]

Kennung 1 (OU2): [redacted]

Kennung 2 (OU3): [redacted]

Veröffentlichung, Hash-Algorithmus und Sperrung des Zertifikats

Veröffentlichung im VöD: Nein

Hash-Algorithmus: [redacted]

Schlüsseltyp: [redacted]

Sperrpasswort: [redacted]

Abrechnung des beantragten Zertifikats

Abrechnungsinformation 3: [redacted]

Mitteilung an die Registrierungsstelle

Mitteilungen an die RA: [redacted]

☐ Hiermit erkläre ich mich mit den **Nutzungsbedingungen** einverstanden und ich habe die **Datenschutzhinweise** zur Kenntnis genommen.

Absenden **Zurück** **Abbrechen**

© 2025 Deutsche Telekom Security GmbH. Alle Rechte vorbehalten. Deutsche Telekom Impressum Datenschutz

Abbildung 23 - Zusammenfassung der Antragsdaten

Schließlich werden Ihnen noch einmal alle Ihre Angaben angezeigt (Hinweis: es handelt sich in den Abbildungen um ein Beispiel für ein personenbezogenes Zertifikat). 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.

Zu 3.) Antrag einreichen

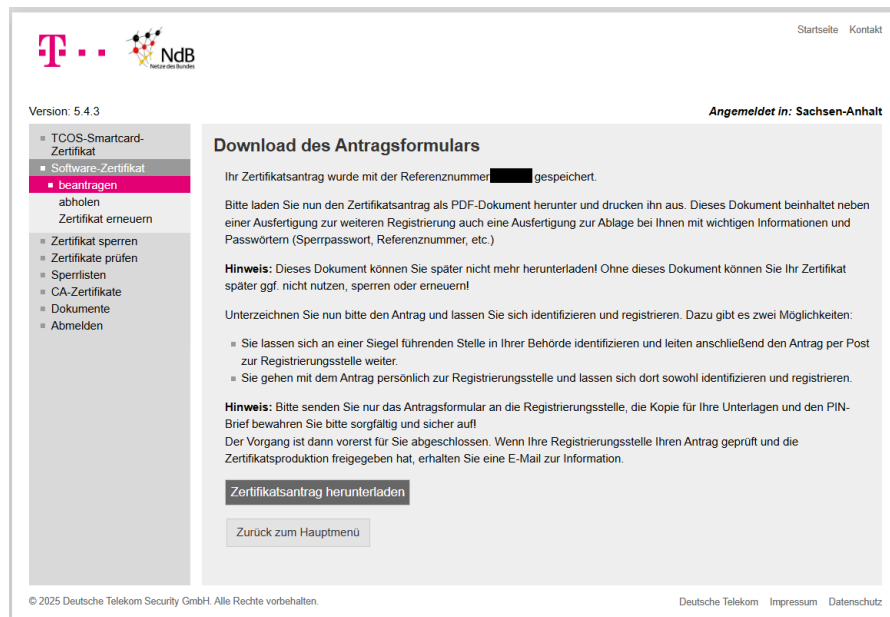


Abbildung 24 - Download des Antragsformulars

Bitte klicken Sie nun auf „Zertifikatsantrag herunterladen“, um den Antrag als PDF zu downloaden. Zusätzlich zum eigentlichen Antrag enthält der Download eine Kopie des Antrags für die eigenen Unterlagen, einen PIN-Brief und ggf. weitere Blätter. Bitte beachten Sie die Hinweise auf der Webseite und im Download.

Bitte drucken Sie den Zertifikatsantrag aus und unterschreiben ihn. Im nächsten Schritt muss das unterschriebene Dokument mit einem Dienstsiegel gesiegelt werden. Lassen Sie sich dazu von Ihrer siegelführenden Stelle identifizieren und das Dokument siegeln.

Im Anschluss senden Sie den Antrag per Post an Ihre Registrierungsstelle. Die Anschrift finden Sie im Antragsformular. Um den Postweg zu beschleunigen können Sie ggf. den Versand als Einschreiben wählen.

Zu 4.) Zertifikat der V-PKI/DOI-CA erhalten



Version: 5.4.3 Angemeldet in: Sachsen-Anhalt

Software-Zertifikat abholen

Bitte geben Sie zum Abholen des Zertifikats die Referenznummer und das Download-Passwort an, welche Ihnen in Ihren Antragsunterlagen mitgeteilt wurden.

* Referenznummer:

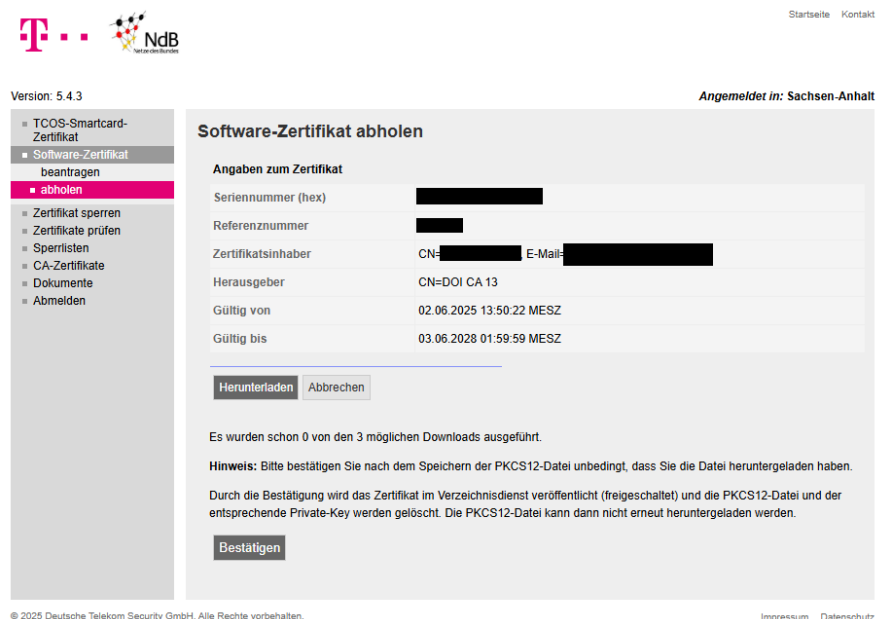
* Download-Passwort:

© 2025 Deutsche Telekom Security GmbH. Alle Rechte vorbehalten. Impressum Datenschutz

Abbildung 25 - Abholung des Software-Zertifikates Teil I

Wenn Ihr Zertifikat von der Registrierungsstelle genehmigt wurde, werden Sie per E-Mail informiert. Gehen Sie wieder auf [DOI](#) [Anmelden](#). 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“.



Version: 5.4.3 Angemeldet in: Sachsen-Anhalt

Software-Zertifikat abholen

Angaben zum Zertifikat

Seriennummer (hex)

Referenznummer

Zertifikatsinhaber CN= E-Mail=

Herausgeber CN=DOI CA 13

Gültig von 02.06.2025 13:50:22 MESZ

Gültig bis 03.06.2028 01:59:59 MESZ

Es wurden schon 0 von den 3 möglichen Downloads ausgeführt.

Hinweis: Bitte bestätigen Sie nach dem Speichern der PKCS12-Datei unbedingt, dass Sie die Datei heruntergeladen haben.

Durch die Bestätigung wird das Zertifikat im Verzeichnisdienst veröffentlicht (freigeschaltet) und die PKCS12-Datei und der entsprechende Private-Key werden gelöscht. Die PKCS12-Datei kann dann nicht erneut heruntergeladen werden.

© 2025 Deutsche Telekom Security GmbH. Alle Rechte vorbehalten. Impressum Datenschutz

Abbildung 26 - Abholung des Software-Zertifikates Teil II

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 gem. 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.



Abbildung 27 - Abholung des Software-Zertifikates Teil III

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.

2.2.7 Signierung des Registrierungsformulars für NOVA

Wie zuvor beschrieben, müssen Sie das Registrierungsformular für die einzelnen Umgebungen, welches Sie über NOVA hochladen, 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.

2.2.7.1 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.

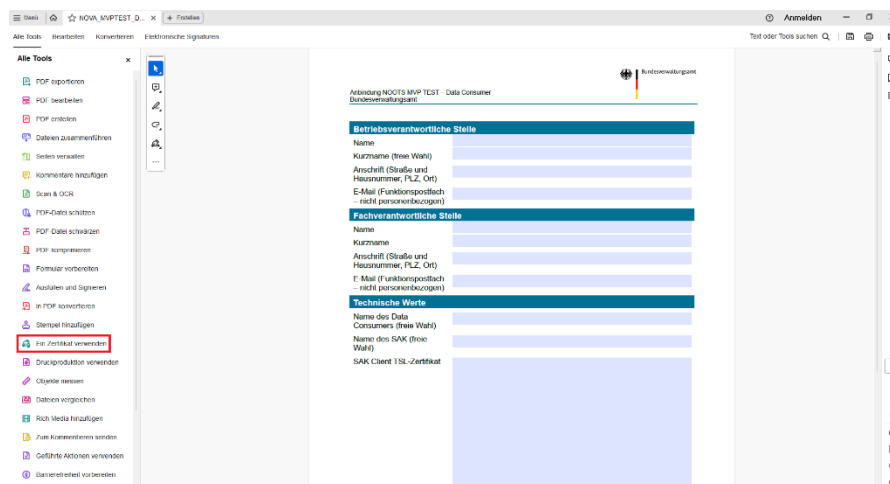


Abbildung 28 - Registrierungsformular in Adobe Acrobat Pro

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

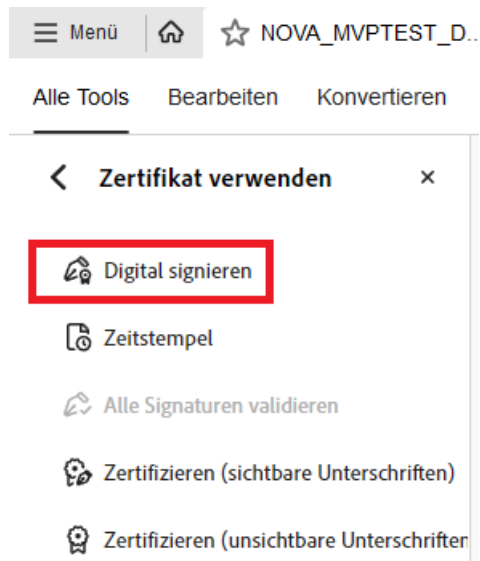


Abbildung 29 - Untermenü "Digital signieren"

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.

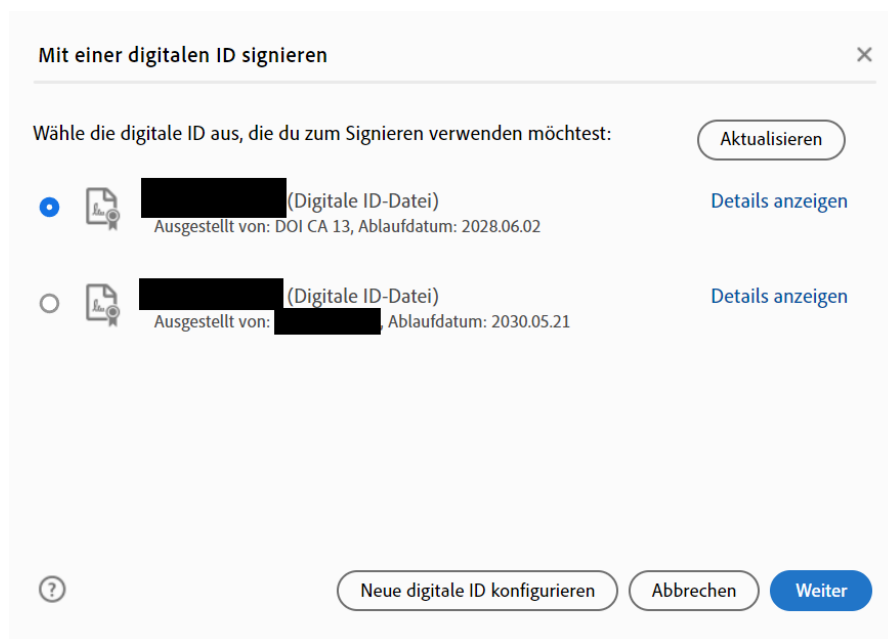


Abbildung 30 - Auswahl der digitalen ID

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“.

Konfiguration einer neuen digitalen ID

Digitale ID zum Signieren konfigurieren [X]

Eine digitale ID ist zum Erstellen einer digitalen Signatur erforderlich. Die sichersten digitalen IDs werden von vertrauenswürdigen Zertifizierungsstellen ausgegeben und basieren auf sicheren Geräten wie Smartcards oder Tokens. Einige basieren auch auf Dateien.

Du kannst auch eine neue digitale ID erstellen, die jedoch nur geringfügig zur Identitätssicherung beiträgt.

Wähle den Typ der digitalen ID aus:

- ☐ **Signaturerstellungsgesamt verwenden**
Konfiguriere eine Smartcard oder ein Token, die bzw. das mit deinem Computer verbunden ist
- ☒ **Digitale ID aus einer Datei verwenden**
Importiere eine vorhandene digitale ID, die du als Datei erhalten hast
- ☐ **Neue digitale ID erstellen**
Erstelle eine selbst signierte digitale ID

[?] [Abbrechen] [Weiter]

Abbildung 31 - Konfiguration einer digitalen ID zum Signieren

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

Digitale ID-Datei suchen [X]

Digitale ID-Dateien haben im Allgemeinen die Erweiterung PFX oder P12 und enthalten die Datei des öffentlichen Schlüssels (Zertifikat) und die zugehörige Datei des privaten Schlüssels.

Wenn du mit einer als Datei verfügbaren digitalen ID signieren möchtest, befolge die Aufforderungen, um die Datei zu suchen und auszuwählen, und gib das Passwort zum Schutz des privaten Schlüssels ein.

Suche nach einer digitalen ID-Datei. Digitale ID-Dateien sind passwortgeschützt. Du kannst nicht auf die digitale ID zugreifen, wenn du das Passwort nicht weißt.

[Textfeld für Dateipfad]

[Durchsuchen]

Passwort für digitale ID eingeben

[Textfeld für Passwort]

[?] [Neue digitale ID erstellen] [Zurück] [Weiter]

Abbildung 32 - 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“.

Mit einer digitalen ID signieren [X]

Wähle die digitale ID aus, die du zum Signieren verwenden möchtest:

☒ [Redacted] (Digitale ID-Datei)
Ausgestellt von: DOI CA 13, Ablaufdatum: 2028.06.02 [Details anzeigen](#)

☐ [Redacted] (Digitale ID-Datei)
Ausgestellt von: [Redacted], Ablaufdatum: 2030.05.21 [Details anzeigen](#)

[?]

Abbildung 33 - Auswahl der digitalen ID nach Konfiguration

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

Abschluss

Signieren als [Redacted] [X]

Erscheinungsbild

☒ Dokument nach dem Signieren sperren [Zertifikatdetails anzeigen](#)

Dokumentinhalt prüfen, der sich auf das Signieren auswirken kann

Abbildung 34 - 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.

2.2.7.2 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.

2.2.7.3 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.

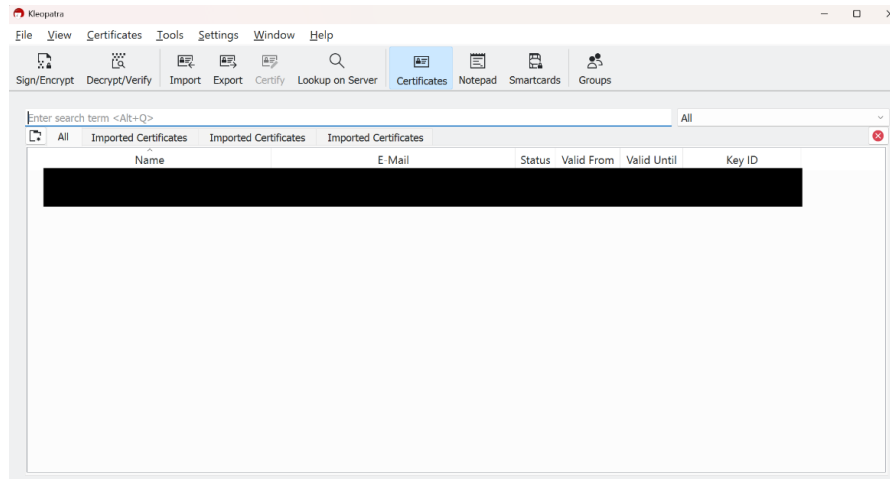


Abbildung 35 - Öffentlichen Schlüssel mittels Kleopatra auslesen

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

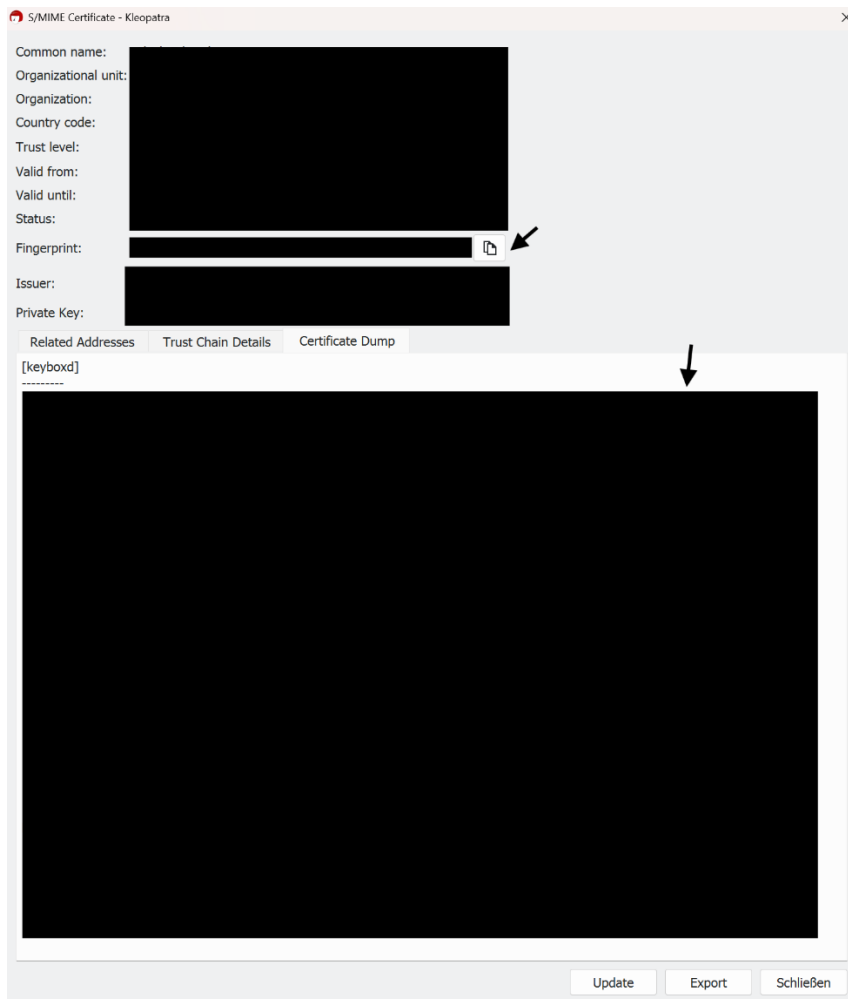


Abbildung 36 - Zertifikatsdetailansicht Kleopatra

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

2.3. Anbindungsverprobung

HINWEIS: Bitte beachten Sie, dass ausschließlich Testdaten an die NOOTS Referenzumgebung gesendet werden dürfen. **Es dürfen zu keinem Zeitpunkt Echt Daten für Anfragen an die NOOTS Referenzumgebung verwendet werden!**

Im Rahmen der Anbindungsverprobung binden Sie Ihren Data Consumer an die NOOTS Referenzumgebung an. Die einzelnen Schritte zur Anbindung an die NOOTS Referenzumgebung sind in der folgenden Abbildung dargestellt und werden in den weiteren Abschnitten im Detail erläutert.

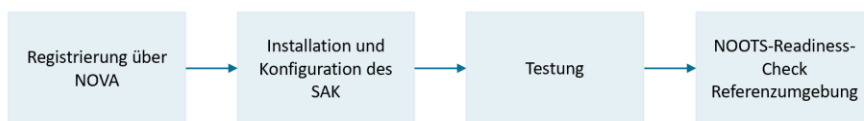


Abbildung 37 – Schritte zur Anbindung an die NOOTS Referenzumgebung

2.3.1 Registrierung über NOVA



Um Ihren Data Consumer in der NOOTS Referenzumgebung zu registrieren, werden einige Informationen benötigt (u.a. zu Fach- und Betriebsverantwortlichen). Bitte melden Sie sich dafür zunächst bei NOVA an. Wählen Sie anschließend das „Dashboard“ aus.

Anbindungsverprobung

- Beantragung Registrierung NOOTS Referenzumgebung über NOVA
- Übermittlung Test-Zertifikat
- Technische Anbindung: Download, Installation und Konfiguration des SAK
- Tests und Freigabe: NOOTS-Readiness-Check Referenzumgebung
- Lessons Learned

Abbildung 38 – Anbindungsverprobung: NOOTS Referenzumgebung

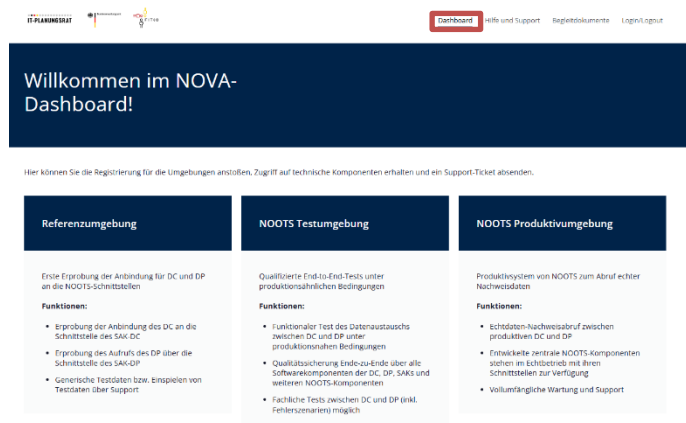


Abbildung 39 - NOVA Dashboard

Beachten Sie bitte auf dem NOVA-Dashboard, dass Sie die Registrierung für die NOOTS Referenzumgebung als Data Consumer vornehmen wollen. Wenn Sie die Registrierung für Data Consumer für die NOOTS Referenzumgebung auswählen, öffnet sich ein neues Formular. Füllen Sie nun die angefragten Informationen im Formular vollständig aus und klicken Sie auf „Zusammenfassung“. Bitte überprüfen Sie in der Zusammenfassung nochmals Ihre eingegebenen Daten. Wenn alles korrekt ist klicken Sie auf „Formular absenden“. Sie erhalten eine Bestätigung über den Formularversand per E-Mail.

2.3.2 Installation und Konfiguration des Sicheren Anschlussknotens

Nach Ihrer Registrierung für die NOOTS Referenzumgebung können Sie über NOVA auf dem [Dashboard](#) den Sicheren Anschlussknoten für die NOOTS Referenzumgebung herunterladen. Wählen Sie hierzu unter „Referenzumgebung“ und „Für Data Consumer“ das Feld „Download SAK-Software“ aus. Laden Sie den SAK runter und führen Sie die Installation durch.

Hinweis: Im produktiven NOOTS werden SAK-DC und SAK-DP nicht zentral betrieben, sondern ausschließlich bei den jeweiligen Data Consumern und Data Providern. Die Bereitstellung dieser SAK-DC und SAK-DP ist ein Service für anbindungswillige NOOTS-Teilnehmer, um unabhängige Tests zu ermöglichen oder den Integrationsaufwand zu minimieren. Die angebunden Data Consumer und Data Provider kommunizieren ausschließlich mit Komponenten der NOOTS Referenzumgebung. Es wird keine Kommunikation zwischen angebundenen Data Consumern und angebundenen Data Providern unterstützt.

Nach der Absendung Ihrer Registrierungsanfrage für die NOOTS Referenzumgebung erhalten Sie eine Termineinladung von Dataport für ein Beratungsgespräch. In diesem Termin werden Ihnen die

weiteren Anbindungsschritte erläutert. Zudem erhalten Sie nochmals Informationen zu den notwendigen Zertifikaten für die weitere Anbindung.

Parallel führt Dataport Ihre Freischaltung für die Nutzung der NOOTS Referenzumgebung durch. Sobald diese Freischaltung erfolgt ist, werden Sie darüber per E-Mail informiert. Zusätzlich wird Dataport Ihnen ein Test-Zertifikat für Ihren SAK-DC übermitteln. Sobald Ihnen die Information über die durchgeführte Freischaltung und das Test-Zertifikat vorliegen, können Sie mit der Konfiguration des SAK-DC beginnen.

2.3.2.2 Integration gegen die NOOTS Referenzumgebung

Durch die Anbindung an die NOOTS Referenzumgebung kann ein Data Consumer feststellen, ob das eigene System NOOTS-ready ist, d.h. ob ein Data Consumer erfolgreich einen Nachweisabruf initiieren und den generierten Nachweis empfangen kann. Dabei kann ein Nachweis abgerufen werden, der einem vordefiniertem, generischem Nachweisangebot entspricht. Alternativ kann ein Nachweis abgerufen werden, der zu einem fachlich relevanten Nachweisangebot gehört, sofern der Data Consumer in den Registrierungsinformationen auch Angaben hinsichtlich fachlich relevanter Nachweisangebote gemacht hat. Können Sie als Data Consumer einen Nachweisabruf erfolgreich durchführen und den gewünschten Nachweis empfangen, haben Sie den Readiness-Check Referenzumgebung erfolgreich absolviert. Bitte folgen Sie nun den nachstehenden Anweisungen, um Ihren SAK zu installieren.

Installation

Installation des Sicheren Anschlussknotens als .jar-File

Der Sichere Anschlussknoten für Data Consumer muss als eigenständig lauffähige Anwendung mit Zugriff auf das Internet installiert werden. Die aktuelle Version der Komponente wird als .jar -Datei wie beschrieben über das NOVA-Dashboard zur Verfügung gestellt.

Die Anbindung an die NOOTS Referenzumgebung ist damit wie folgt:

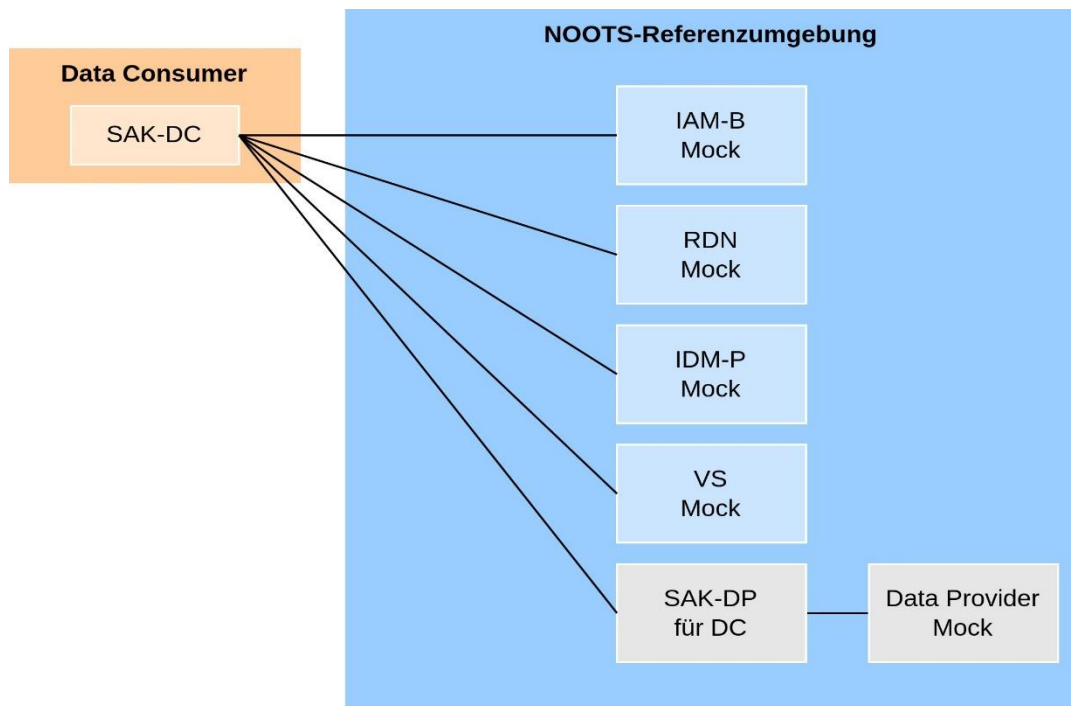


Abbildung 40 - Data Consumer mit integriertem SAK-DC

Um den Sicherem Anschlussknoten erfolgreich installieren zu können, werden folgende Einstellungen und Abhängigkeiten vorausgesetzt:

- Java/JVM 21

Das Starten des SAKs kann mittels des gelieferten .jar-File ausgeführt werden. Es empfiehlt sich die benötigten Konfigurationsparameter als Laufzeit-Parameter anzugeben.

```
java -Dquarkus.config.locations=application.properties -jar sak-dc.jar
```

Die für die Konfiguration benötigte Property-Datei liegt der jar-Datei bei. In dieser Datei müssen die entsprechenden umgebungsspezifischen Einstellungen hinterlegt werden. Die vorhandenen Beispieldaten müssen hierbei durch echte Werte ersetzt werden.

Installation des Sicherem Anschlussknotens als HELM-File

Als Alternative zu einer klassischen Installation via .jar-File ist außerdem eine Installation via HELM möglich. Sie benötigen hierfür eine eigene Registry in der Sie das Container Image importieren müssen. Die aktuelle Version des HELM Charts sowie das Container Image wird im Downloadbereich (siehe "Downloadbereich") zur Verfügung gestellt.

Die für die Konfiguration benötigte Values-Datei, die als Helm Parameter - f übergeben werden muss, liegt den HELM Charts bei. In dieser Datei müssen die entsprechenden umgebungsspezifischen Einstellungen hinterlegt werden. Beachten Sie auch hier die Hinweise innerhalb der Datei. Die vorhandenen Beispieldaten müssen hierbei durch echte Werte ersetzt werden.

Technische Anbindungstests für die installierte Umgebung

Um als Data Consumer die Installation und Anbindung schnell und ohne größeren Aufwand testen zu können, empfiehlt es sich, nach erfolgreichem Starten der Anwendung und nach entsprechenden Änderungen an der Konfiguration oder Installation, einen Smoke-Test manuell durchzuführen. Hierzu steht im "Downloadbereich" ein einfaches Bash-Script zur Verfügung, mit welchem ein Request auf die '/token'-Schnittstelle mittels CURL durchgeführt werden kann.

Mittels diesem Request können schnell und einfach folgende Kriterien, welche für einen erfolgreichen Betrieb der Anwendung notwendig sind getestet werden:

- Erreichbarkeit des SAK-DC in der lokalen Installation
- Erfolgreiche Kommunikation zwischen SAK-DC und NOOTS-Kernkomponenten der Referenzumgebung (Firewall-Regeln/Proxies/IP-Freischaltung)
- Fachliche Freigabe des DC in der Referenzumgebung

Im Falle einer erfolgreichen Durchführung wird ein HTTP-Status-Code des Typs 200 mit einem entsprechenden Response-Body (beschrieben in der Smoketest-Datei) erwartet.

Hinweis: ggfs. können die angegebenen Test-Daten des CURL-Requests von der Ihnen zugewiesenen IDs und Verbindungsdaten abweichen. Sollte dies der Fall sein, passen Sie diese bitte den CURL-Befehl entsprechend an.

Abweichende Status-Codes (!2XX) können auf einen Fehler in der Konfiguration, Umgebung oder Registrierung hinweisen. Bitte prüfen Sie hier zunächst Ihre angegebenen Daten, Zertifikate und Passwörter in der entsprechenden application.properties- oder HELM-Konfigurationsdatei. Prüfen Sie bitte außerdem Ihre Netzwerkeinstellungen, Proxies und ggfs. Firewall-Regeln, ehe Sie sich an den Support wenden.

Nutzung des “SAK-DC für DC” der NOOTS Referenzumgebung

Ein weiterer Weg für eine Anbindung an die NOOTS Referenzumgebung ist die Nutzung des vorinstallierten SAK-DC der NOOTS Referenzumgebung. Eine Installation des SAK-DC im eigenen System entfällt somit.

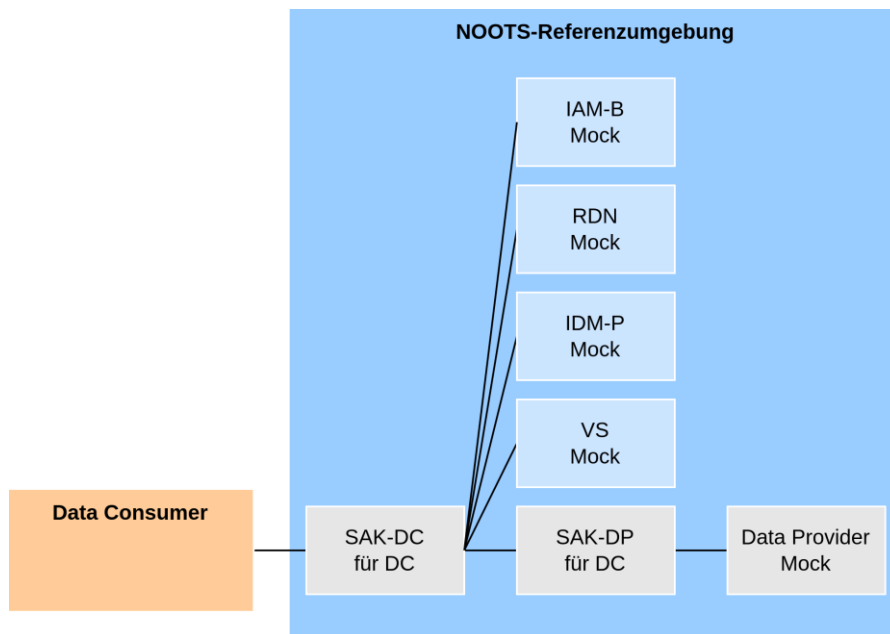


Abbildung 41 - Data Consumer ohne integrierten SAK-DC

Diese Art der Betriebsmethode dient lediglich zur Entwicklung gegen die Schnittstellen des SAK-DC und ist nicht zu Produktivzwecken geeignet. Die Nutzung der Schnittstellen bleibt identisch.

Hinweis: Diese Art der Nutzung des Sicheren Anschlussknotens wird nur in der NOOTS Referenzumgebung angeboten. Bei einer produktiven Anbindung an NOOTS ist eine On-Premise-Installation zwingend erforderlich!

Bereitstellung von Test-Data-Providern

In der Referenzumgebung werden Test-Data-Provider (Data Provider Mock) zur Verfügung gestellt. Die Information zu den aktuell verfügbaren Nachweistypen, welche den grundlegenden Datenumfang abdecken, erhalten Sie bei der Registrierung Ihres Systems. Sollten Sie spezielle Testdaten benötigen, setzen Sie sich bitte mit dem Support (siehe “Kontaktinformationen”) in Verbindung.

Durchlauf eines Nachrichtenabrufs

Um als Data Consumer nach der Installation und Integration des SAK-DC und der Registrierung als Data Consumer einen Nachweis abrufen zu können, sind die nachfolgenden Schritte notwendig (eine weiterführende Schnittstellendokumentation finden Sie unter "Endpunkte des SAK-DC").

Bitte beachten Sie, dass ausschließlich Testdaten an die NOOTS Referenzumgebung gesendet werden dürfen.

Hinweis: Es dürfen zu keinem Zeitpunkt Echtdaten für Anfragen an die NOOTS Referenzumgebung verwendet werden!

1: Anfordern des Zugriffstoken

In einem ersten Schritt ist es notwendig, einen Zugriffstoken für die Nutzung der Schnittstellen anzufordern. Die Anforderung eines solchen Zugriffstokens erfolgt über die Schnittstelle "Anfordern des Zugriffstoken".

Aufruf der Schnittstellen `https://<>/token` mit dem HTTP-Request-Body:

Beispiel:

```
{  
  "component_id": "9151f21f-43ae-43b4-92f3-f4af67cdf544"  
}
```

Als "component_id" ist die zugewiesene Komponenten-ID des Data Consumers zu verwenden. Den Wert dieses Feldes erhalten Sie nach der Registrierung (siehe Registrierung als Data Consumer) vom Support- Team.

Hinweis: Der Zugriffstoken hat eine Gültigkeit von einer Minute und muss daher vor jedem Request geprüft und ggf. neu angefordert werden!

2: Suche nach einem Nachweisangebot

Nach dem erfolgreichen Anfordern eines Zugriffstoken kann eine Suche nach einem passenden Nachweisangebot begonnen werden. Die Suche erfolgt über die Schnittstelle "Suche nach einem Nachweisangebot eines Nachweistyps".

Aufruf der Schnittstellen <https://<>/de/evidence-offer> mit dem HTTP-Request-Body:

Beispiel für den Abruf eines Geburtsnachweises:

```
{  
  "evidence_type": "4b70194e-  
ae5a-417b-b8de-6b92f8b044e3",  
  "jurisdictions": {  
    "ars": "012345678901",  
    "bundesland": "BY",  
    "hochschule": "LMU"  
  }  
}
```

Beispiel für den Abruf einer Meldebescheinigung:

```
{  
  "evidence_type": "4b70194e-  
ae5a-417b-b8de-6b92f8b044e3",  
  "jurisdictions": {  
    "ars": "012345678901",  
    "bundesland": "BY",  
    "hochschule": "LMU"  
  }  
}
```

3: Anfordern des Nachweises

Mit dem Ergebnis der Nachweisangebotssuche kann nun eine Anfrage für einen bestimmten Nachweis gestellt werden. Die Anfrage erfolgt über die Schnittstelle "Anfordern eines Nachweises des zuständigen Data Providers".

Aufruf der Schnittstellen <https://<>/de/evidence> mit dem HTTP-Request-Body:

Beispiel:

```
{  
  "evidence_request": {  
    "mime_type": "application/xml",  
    "specification_identifier": "urn:xoev-  
de:bva:standard:xnachweis_1.4.0",  
    "message_type": "DE.EvidenceRequest.0101",  
  }  
}
```

```
"data":  
"U2FtcGx1IHhuLW5vb3Rz□kRFLkV2aWR1bmN1UmVxdWVzdC4wMT  
Ax"  
}  
}
```

2.3.2.3 Zertifikate, Keystores und Truststores

In diesem Kapitel erfahren Sie, welche Keystores und Truststores in der NOOTS Referenzumgebung konfiguriert sind. Diese Komponenten sind entscheidend für die sichere Kommunikation und Authentifizierung innerhalb Ihres Systems.

Zertifikate sind digitale Dokumente, die die Identität einer Entität (z.B. eines Servers, einer Anwendung oder eines Benutzers) bestätigen. Sie werden von einer vertrauenswürdigen Zertifizierungsstelle (CA, Certificate Authority) ausgestellt und enthalten öffentliche Schlüssel, die zur Verschlüsselung und Authentifizierung verwendet werden. Zertifikate gewährleisten, dass die Kommunikation zwischen zwei Parteien sicher und vertrauenswürdig ist.

- **Keystore (Schlüsselcontainer):**
 - **Inhalt:** Enthält private Schlüssel und die zugehörigen Zertifikate der eigenen Entität.
 - **Verwendung:** Wird verwendet, um die eigenen Identitätsinformationen und Verschlüsselungsschlüssel sicher zu speichern.
 - **Beispiel:** Ein Webserver verwendet einen Keystore, um sein eigenes SSL/TLS-Zertifikat und den privaten Schlüssel zu speichern.
- **Truststore (Vertrauenscontainer):**
 - **Inhalt:** Enthält öffentliche Zertifikate von vertrauenswürdigen Drittanbietern oder Zertifizierungsstellen.
 - **Verwendung:** Wird verwendet, um die Identität von entfernten Entitäten zu überprüfen und zu validieren.
 - **Beispiel:** Ein Client verwendet einen Truststore, um die Zertifikate von vertrauenswürdigen Zertifizierungsstellen zu speichern, die zur Validierung der Zertifikate von Servern verwendet werden.

NOREF als Data Consumer

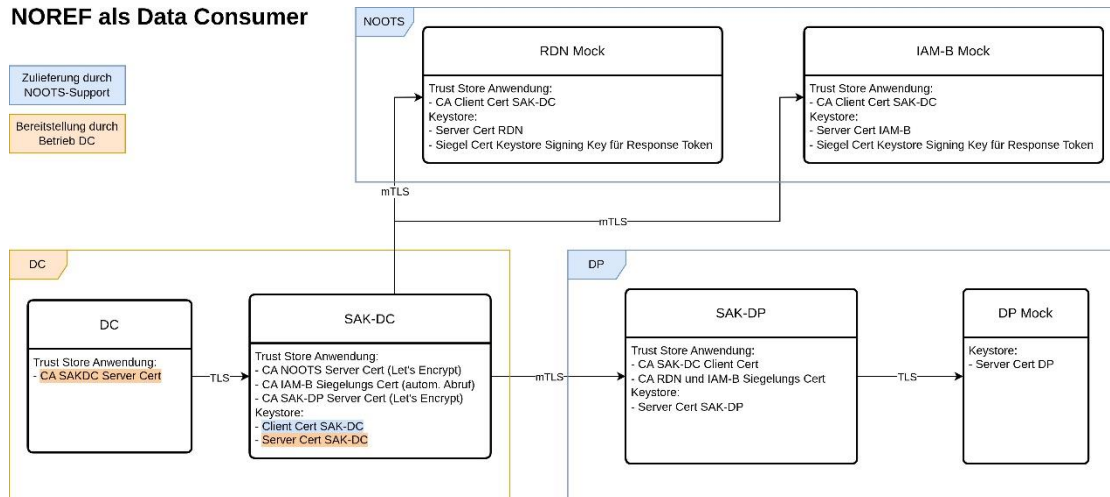


Abbildung 42 - Übersicht über die Zertifikate des Data Consumers

Zertifikat zur Token-Verifizierung

Der Datenaustausch zwischen den NOOTS-Teilnehmern erfolgt teilweise mittels gesiegelter bzw. signierter Webtokens, welche sich besonders für die Übertragung sensibler Daten eignen. Zur Sicherstellung der Datenintegrität können alle NOOTS-Teilnehmer die Siegelung überprüfen, insbesondere:

- dass der Inhalt des Webtokens seit der Siegelung nicht verändert wurde, und
- dass der Teilnehmer, welcher die Siegelung angebracht hat, ein vertrauenswürdigen Zertifikat verwendet, also der ist, für den er sich ausgibt.

Letztes erfordert, dass das Siegel-Zertifikat von einer öffentlichen Stelle ("Trust-Center") bestätigt wird oder dass dem Token-Empfänger das zugrunde liegende Ursprungszertifikat ("root certificate authority", kurz: "root-CA") bekannt ist.

Um dem Data-Provider und -Consumer in jedem Fall die Verifizierung der Token-Siegelung zu ermöglichen, wird das entsprechende Ursprungszertifikat als Datei `ca.crt` zum Download bereitgestellt (siehe "Downloadbereich").

2.3.2.4 Übersicht der Schnittstellendefinitionen der NOOTS

Referenzumgebung: Endpunkte des Sicheren Anschlussknotens für Data
Consumer

Hinweis: In der NOOTS Referenzumgebung erfolgt **keine** Datenhaltung. Alle, durch die NOOTS Referenzumgebung verarbeiteten Daten, sind statisch generiert oder werden nur zur Laufzeit der Anfrage gehalten.

Anfordern des Zugriffstoken

POST /token

Für den Zugriff auf alle anderen Operationen der Consumer-API benötigt ein Data Consumer ein gültiges Zugriffstoken vom 'IAM für Behörden'. Das erhaltene Zugriffstoken muss bei diesen Operationen der Consumer-API als Bearer-Token im HTTP-Header "Authorization" gemäß RFC6750 angegeben werden. Vor jedem Aufruf der Consumer-API ist zu überprüfen, ob das Zugriffstoken noch gültig ist (Gültigkeitsdauer: 1 Minute). Sollte das Token abgelaufen sein, muss ein neues Zugriffstoken angefordert werden.

Ein Zugriffstoken besteht aus folgenden fachlichen Bestandteilen:

Bestandteil	Beschreibung
Komponenten-ID	Vom IAM-B bei der Registrierung vergebene ID der IT-Komponente
Bezeichnung	Bezeichnung der IT-Komponente
Behördenfunktion	Behördenfunktion der IT-Komponente
Verwaltungsbereich	Verwaltungsbereich der Behördenfunktion der IT-Komponente
Teilnahmeart	Teilnahmeart der IT-Komponente
Rollen	Menge von Rollen gemäß der Teilnahmeart
FV-ID	Vom IAM-B bei der Registrierung vergebene ID der fachverantwortlichen Stelle
FV-Organisation	Organisation der fachverantwortlichen Stelle laut deren Zertifikat

FV-Funktionsträger	Funktionsträger der Fachverantwortlichen laut deren Zertifikat
FV-Anschrift	Anschrift der Fachverantwortlichen laut deren Zertifikat
BV-ID	Vom IAM-B bei der Registrierung vergebene ID der Betriebsverantwortlichen
BV-Organisation	Organisation der Betriebsverantwortlichen laut deren Zertifikat
BV-Funktionsträger	Funktionsträger der Betriebsverantwortlichen laut deren Zertifikat
BV-Anschrift	Anschrift der Betriebsverantwortlichen laut deren Zertifikat

Tabelle 3 - Bestandteile von Zugriffstoken

AccessTokenRequest

- **Anzugeben in:** HTTP-Request-Body
- **Typ:** AccessTokenRequest
- **Pflichtfeld:** ja
- **Beispiel:**

```
{  
  "component_id": "9151f21f-43ae-43b4-92f3-f4af67cdf544"  
}
```

traceparent

- **Anzugeben in:** HTTP-Request-Header
- **Typ:** TraceParent
- **Pflichtfeld:** ja
- **Beschreibung:** Trace-ID z.B.
0af7651916cd43dd8448eb211c80319c zur Verfolgung von
Nachrichten über Komponentengrenzen hinweg (siehe W3C
Trace Context)

Beispielantwort im Erfolgsfall

Antwort als JSON-Response-Body:

```
{  
  "access_token": "mF_9.B5f-4.1JqM",
```

```
"token_type": "Bearer"  
"expires_in": 60  
}
```

Mögliche HTTP-Status-Codes

Die folgenden Fehlerfälle und Status-Codes können nach einem Aufruf der Schnittstelle auftreten und sind durch den Data Consumer zu verarbeiten:

Status	Beschreibung
200 OK	Erfolgreiche Anfrage
400 Bad Request	Die Anfrage konnte nicht bearbeitet werden, da ein Fehler durch den Anfragenden vermutet wird (z. B. fehlerhafte Anfragesyntax).
401 Unauthorized	Zugriffstoken fehlt, ist ungültig oder die Authentifizierung der IT-Komponente ist fehlgeschlagen.
403 Forbidden	IT-Komponente wurde erfolgreich authentifiziert, hat jedoch aufgrund ihrer Berechtigungen keinen Zugriff auf die angeforderte Ressource.
404 Not Found	Unter der angeforderten URI ist keine Ressource verfügbar.
422 Unprocessable Entity	Die Anfrage ist syntaktisch korrekt, kann jedoch aufgrund semantischer Fehler nicht verarbeitet werden. Weitere Informationen sind in der Fehlernachricht enthalten (siehe Definition von ErrorMessage für Einzelheiten).
500 Internal Server Error	Unerwartete Serverfehler
503 Service Unavailable	Der Service steht temporär nicht zur Verfügung.

Tabelle 4 - Mögliche HTTP-Status Codes

Suche nach einem Nachweisangebot eines Nachweistyps

POST /de/evidence-offer

Hinweis: Für die Ausführung dieses Endpunktes ist ein Zugriffstoken (siehe [IAM-B Zugriffstoken](#)) erforderlich. Dieser Token ist bei der Anfrage als "Authorization"-Header vom Typ "Bearer" anzugeben.

Beispiel: Authorization: Bearer zugriffstokenWert

Es wird nach einem Nachweisangebot aus der Registerdatennavigation gesucht, basierend auf dem Nachweistyp und gegebenenfalls weiteren Zuständigkeitsparametern. Bei zentralisierten Registern reicht der Nachweistyp allein aus, um den zuständigen Data Provider zu bestimmen. Für dezentralisierte Register werden zusätzliche Zuständigkeitsparameter wie zum Beispiel der amtliche Regionalschlüssel (ARS) benötigt. Ein Nachweisangebot enthält Informationen für den Abruf eines Nachweises von einem Data Provider, der für den spezifischen Nachweistyp und das Nachweissubjekt zuständig ist.

Hier sind die Informationen, die als Suchergebnis zurückgeliefert werden:

- Zuständiger Data Provider samt dessen Dienstkennung (Service-ID)
- Für den Nachweisabruf nötiges Vertrauensniveau. Es bestimmt, wie hoch das Vertrauensniveau des authentifizierten Nachweissubjekts oder dessen Vertreters mindestens sein muss, um einen Nachweis dieses Typs abrufen zu können.
- Für den Nachweistyp angebotene Nachweisformate. Sie bestimmen, in welchen Formaten (z.B. Fachstandard-XML in Version x.y der Data Consumer einen Nachweis beziehen kann. Der Data Consumer muss eines der angebotenen Nachweisformate im Nachweisabruf angeben.
- Angabe, ob ein Nachweis dieses Typs mit IDNr (natürliche Person) bzw. beWiNr (Unternehmen) abgerufen werden kann. **(Die Abrufe mit IDNr bzw. beWiNr werden in der NOOTS Referenzumgebung nicht unterstützt.)**
- Zuständigkeitstoken mit Nachweisangeboten in gesiegelter Form

FindEvidenceOffersRequest

- **Anzugeben in:** HTTP-Request-Body
- **Typ:** FindEvidenceOffersRequest
- **Pflichtfeld:** ja

- **Beispiel:**

```
{  
  "evidence_type": "9151f21f-43ae-43b4-92f3-f4af67cdf544",  
  "jurisdictions": {  
    "ars": "012345678901",  
    "bundesland": "BY",  
    "hochschule": "LMU"  
  }  
}
```

traceparent

- **Anzugeben in:** HTTP-Request-Header
- **Typ:** TraceParent
- **Pflichtfeld:** ja
- **Beschreibung:** Trace-ID z.B.
0af7651916cd43dd8448eb211c80319c zur Verfolgung von
Nachrichten über Komponentengrenzen hinweg (siehe W3C
Trace Context)

Beispielantwort im Erfolgsfall

Antwort als JSON-Response-Body:

```
{  
  "evidence_offers": [  
    {  
      "evidence_type": "9151f21f-  
43ae-43b4-92f3-  
f4af67cdf544",  
      "evidence_type_name":  
      "Geburtsnachweis",  
      "provider_id": "23a9e938-  
6677-432a-a9e9-  
386677032af2",  
      "provider_name":  
      "Standesamt Hamburg",  
      "service_id": "73c32bb9-  
d973-46b8-832b-  
b9d973b6b8cb",  
      "level_of_assurance":  
      "Low",  
      "subject_id_usage": [ "idnr"  
    ],  
      "evidence_formats": [  
        {  
          "oots_media_type": "application/xml",  

```

```
    "conforms_to":  
    "https://sr.oots.tech.ec.europa.eu/distributions/  
    birthcert-1.0.0", "transformation": "string"  
  }  
]  
}  
],  
  "jurisdiction_token": "string"  
}
```

Status	Beschreibung
200 OK	Erfolgreiche Anfrage
400 Bad Request	Die Anfrage konnte nicht bearbeitet werden, da ein Fehler durch den Anfragenden vermutet wird (z. B. fehlerhafte Anfragesyntax).
401 Unauthorized	Zugriffstoken fehlt, ist ungültig oder die Authentifizierung der IT-Komponente ist fehlgeschlagen.
403 Forbidden	IT-Komponente wurde erfolgreich authentifiziert, hat jedoch aufgrund ihrer Berechtigungen keinen Zugriff auf die angeforderte Ressource.
404 Not Found	Unter der angeforderten URI ist keine Ressource verfügbar.
422 Unprocessable Entity	Die Anfrage ist syntaktisch korrekt, kann jedoch aufgrund semantischer Fehler nicht verarbeitet werden. Weitere Informationen sind in der Fehlernachricht enthalten (siehe Definition von ErrorMessage für Einzelheiten).
500 Internal Server Error	Unerwartete Serverfehler
503 Service Unavailable	Der Service steht temporär nicht zur Verfügung.

Tabelle 5 - Mögliche HTTP-Status Codes

Anfordern eines Nachweises des zuständigen Data Providers

POST /de/evidence

Hinweis: Für die Ausführung dieses Endpunktes ist ein Zugriffstoken (siehe [IAM-B Zugriffstoken](#)) erforderlich. Dieser Token ist bei der Anfrage als "Authorization"-Header vom Typ "Bearer" anzugeben.

Beispiel: Authorization: Bearer zugriffstokenWert

Ein Data Consumer kann einen Nachweisabruf aus einem nationalen Data Provider gemäß Nachweisabrufprozess des NOOTS der High Level Architektur (HLA) durchführen. Diese Operation verwendet den XÖV-Standard XNachweis zur Übermittlung von Nachweisen zu Personen und Unternehmen. XNachweis-Antworten mit Nachweisdaten sowie XNachweis-Fehlernachrichten werden mit dem HTTP-Code 200 (OK) übermittelt.

GetEvidenceRequest

- **Anzugeben in:** HTTP-Request-Body
- **Typ:** GetEvidenceRequest
- **Pflichtfeld:** ja
- **Beispiel:**

```
{
  "service_id": "a31d115a-12c3-
4f27-9d11-5a12c3bf2727",
  "evidence_request": {
    "mime_type": "application/xml",
    "specification_identifier":
    "urn:xoev-
de:bva:standard:xnachweis_1.4.0",
    "data":
    "U2FtcGx1IHhuLW5vb3RzKkRFLkV2aWR1
bmNlUmVxdWVzdC4wMTAx",
    "message_type":
    "DE. EvidenceRequest. 0101"
  }
}
```

traceparent

- **Anzugeben in:** HTTP-Request-Header
- **Typ:** TraceParent
- **Pflichtfeld:** ja

- **Beschreibung:** Trace-ID z.B.
0af7651916cd43dd8448eb211c80319c zur Verfolgung von
Nachrichten über Komponentengrenzen hinweg (siehe W3C
Trace Context)

Beispielantwort im Erfolgsfall

Antwort als JSON-Response-Body:

```
{  
  "mime_type": "application/xml",  
  "specification_identifier": "urn:xoev-  
de:bva:standard:xnachweis_1.4.0",  
  "data":  
    "U2FtcGx1IHhuLW5vb3RzKkRFLkV2aWR1bmN1  
UmVzcG9uc2UuMDEwMg=="  
}
```

Die folgenden Fehlerfälle und Status-Codes können nach einem Aufruf
der Schnittstelle auftreten und sind durch den Data Consumer zu
verarbeiten:

Status	Beschreibung
200 OK	Erfolgreiche Anfrage
400 Bad Request	Die Anfrage konnte nicht bearbeitet werden, da ein Fehler durch den Anfragenden vermutet wird (z. B. fehlerhafte Anfragesyntax).
401 Unauthorized	Zugriffstoken fehlt, ist ungültig oder die Authentifizierung der IT-Komponente ist fehlgeschlagen.
403 Forbidden	IT-Komponente wurde erfolgreich authentifiziert, hat jedoch aufgrund ihrer Berechtigungen keinen Zugriff auf die angeforderte Ressource.
404 Not Found	Unter der angeforderten URI ist keine Ressource verfügbar.
422 Unprocessable Entity	Die Anfrage ist syntaktisch korrekt, kann jedoch aufgrund semantischer Fehler nicht verarbeitet werden. Weitere Informationen sind in der

	Fehlernachricht enthalten (siehe Definition von ErrorMessage für Einzelheiten).
500 Internal Server Error	Unerwartete Serverfehler
503 Service Unavailable	Der Service steht temporär nicht zur Verfügung.

Tabelle 6 - Mögliche HTTP-Status Codes

2.3.3 Testung

Um die erfolgreiche Anbindung an die NOOTS Referenzumgebung sicherzustellen, führen Sie nach der Integration eine Testung durch, die aus drei Teilschritten besteht. Den Ablauf der Teilschritte für die Testung finden Sie in der nachfolgenden Abbildung beschrieben. Im ersten Schritt überprüfen Sie die notwendigen Vorbedingungen. Anschließend durchlaufen Sie selbstständig mindestens die im Rahmen dieses Dokumentes definierten Testfälle. Im Erfolgsfall buchen Sie einen Termin zur Testabnahme.

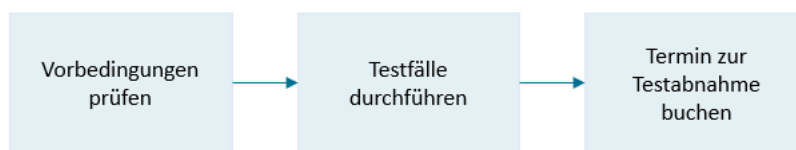


Abbildung 43 - Ablauf Testung NOOTS Referenzumgebung

2.3.3.1 Vorbedingungen

Folgende Vorbedingungen müssen mindestens erfüllt sein, damit Sie einen Termin zur Testabnahme mit Dataport durchführen können:

1. Ein funktionsfähiger, eigens installierter SAK-DC für die Referenzumgebung ist eingerichtet.
2. Der im nachfolgenden Kapitel beschriebene Testfall 1 ist vorbereitet und erfolgreich durchlaufen worden.
3. Es besteht Zugang zu den Logdateien des SAK-DC. Dieser Zugang kann im Rahmen der Testabnahme über eine Videokonferenz via Bildschirmübertragung live mit dem Support-Team von Dataport geteilt werden.

Wenn Sie Rückfragen zur Erfüllung dieser Voraussetzungen haben, eröffnen Sie bitte ein Supportticket über [NOVA](#) oder wenden Sie sich an dataportnootssupport@dataport.de.

2.3.3.2 Testfälle

Wenn Sie alle Vorbedingungen, die mindestens erfüllt sein müssen, erreichen, fahren Sie mit der Durchführung der Testfälle fort. Diese werden im Rahmen der Testabnahme (s. Kapitel 2.3.3.3) erneut überprüft. Bitte dokumentieren Sie die Ergebnisse Ihrer Testfälle. Die hier abgebildeten Testfälle stellen die Mindestanforderungen dar und können individuell im Rahmen Ihres Testkonzeptes ergänzt verwendet werden.

Nr.	Testfall	Durchführung	Erwartetes Ergebnis
1	Es wird geprüft, ob über den eigenen SAK-DC die Abrufe /token, /evidence-offer und /evidence nachvollziehbar und fehlerfrei sind.	Der Test kann in der Bash z.B. über cURL, in Powershell oder mit dem eigenen Online-Dienst durchgeführt werden.	Die Abrufe /token, /evidence-offer und /evidence sind nachvollziehbar und fehlerfrei. Die Logs des SAK-DC zeigen keine Fehler. In den Logs der Referenzumgebung kann unter Verwendung der TraceId nachvollzogen werden, dass alle Aufrufe des SAK-DC gegen das IAM-B, RDN und den SAK-DP fehlerfrei waren.

Tabelle 7 - Testfälle NOOTS Referenzumgebung DC

2.3.3.3 Testabnahme

Wenn Sie alle Testfälle erfolgreich abgeschlossen haben, buchen Sie per E-Mail an dataportnootssupport@dataport.de einen Termin zur Testabnahme beim Support-Team von Dataport. In dem Termin prüfen Sie dann gemeinsam mit Dataport, ob die Vorbedingungen erfolgreich erfüllt sind. Anschließend durchlaufen Sie gemeinsam mit dem Support-Team den geschilderten Testfall.

Außerdem müssen Sie im Rahmen des Termines zur Testabnahme folgende Fragen beantworten:

- Welche testverantwortlichen Personen sind auf dem Readiness-Check namentlich zu erwähnen (1-4 Personen)?
- Wie lautet der Anwendungsfall auf dem Readiness-Check (Beispiel: Erprobung des nationalen Nachweisdatenaustauschs und Anbindung des Nachweises XXX aus dem Register YYY an den Onlinedienst ZZZ (UC-Kürzel))?

2.3.4 NOOTS-Readiness-Check Referenzumgebung

Wenn der Testlauf ohne Fehler erfolgt ist, bereitet Dataport den NOOTS-Readiness-Check Referenzumgebung für Sie vor. Anschließend erhalten Sie von Dataport eine Einladung zu einem Lessons Learned-Gespräch. In diesem Gespräch möchten wir gern von Ihnen erfahren, was im Rahmen der Anbindung an die NOOTS Referenzumgebung gut funktioniert hat und wo es noch Optimierungspotentiale gibt. Danach können Sie mit der Anbindung an die NOOTS Testumgebung fortfahren.

2.4. Anbindung: NOOTS Testumgebung

HINWEIS: In der NOOTS Testumgebung dürfen **ausschließlich Testdaten** verwendet werden. Es dürfen in **keinem** Falle **Echtdaten** zum Einsatz kommen! Darüber hinaus dürfen **keine Produktivzertifikate** benutzt werden!

Die einzelnen Schritte zur Anbindung an die NOOTS Testumgebung sind in der folgenden Abbildung dargestellt und werden in den weiteren Abschnitten im Detail erläutert.

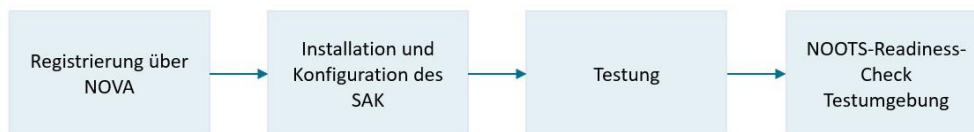


Abbildung 44 - Anbindung an die NOOTS Testumgebung

2.4.1 Registrierung über NOVA



Zur Registrierung im IAM-B der NOOTS Testumgebung benötigen wir von Ihnen als Data Consumer unterschiedliche Informationen. Bitte melden Sie sich hierzu erneut mit Ihrem MUK-Konto bei NOVA an. Wählen Sie anschließend das „Dashboard“ aus.

Anbindung (NOOTS Testumgebung)

- Beantragung Registrierung NOOTS Testumgebung über NOVA
- Technische Anbindung: Download, Installation und Konfiguration des SAK
- Tests und Freigabe: NOOTS-Readiness-Check Testumgebung
- Lessons Learned

Abbildung 45 - NOOTS Testumgebung

Beachten Sie bitte auf dem NOVA-Dashboard, dass Sie die Registrierung für die NOOTS Testumgebung als Data Consumer vornehmen wollen. Wenn Sie die Registrierung für Data Consumer für die NOOTS Testumgebung auswählen, öffnet sich ein neues Formular. Hier können Sie das benötigte Registrierungsformular als PDF herunterladen. Bitte füllen Sie das PDF-Formular vollständig aus. Dies beinhaltet auch den Upload des öffentlichen Schlüssels Ihres erworbenen TLS-Client-Zertifikats für die NOOTS Testumgebung. Der private Schlüssel muss bei Ihnen verbleiben und geheim gehalten

werden. Anschließend ist es aus Sicherheitsgründen erforderlich, dass Sie das Registrierungsformular mit einem personenbezogenen Zertifikat der V-PKI/DOI-CA signieren. Eine Schritt-für-Schritt Anleitung hierzu finden Sie in Abschnitt 2.2.7 dieses Dokumentes.

Wenn Sie das Registrierungsformular signiert haben, speichern Sie es ab. Füllen Sie die erforderlichen Angaben auf der Website aus und klicken Sie auf „Weiter zum Datei-Upload“. Laden Sie nun das signierte Registrierungsformular hoch und klicken Sie auf „Weiter zur Zusammenfassung“.

Bitte überprüfen Sie in der Zusammenfassung Ihre eingegebenen Daten. Wenn alles korrekt ist, klicken Sie auf „Formular absenden“. Sie erhalten eine Bestätigung über den Formularversand per E-Mail.

2.4.2 Installation und Konfiguration des Sicheren Anschlussknotens

In den beiden nachfolgenden Kapiteln finden Sie eine fachliche und technische Beschreibung des Sicheren Anschlussknotens. Um unmittelbar mit der Installation und Konfiguration der Software fortzufahren, widmen Sie sich bitte dem Kapitel 2.4.2.3 „Installation der Anwendung“.

2.4.2.1 Fachliche Beschreibung

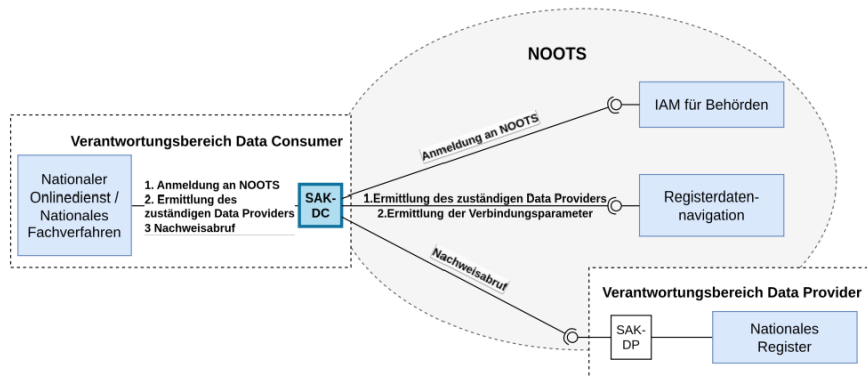


Abbildung 46 - SAK-DC: Fachlicher Kontext

Die fachlichen Aufgaben des SAK-DCs sind die Durchführung des Nachweisabrufs unter Einhaltung des obligatorischen Sicherheitsprotokolls.

Im Einzelnen:

- der Abruf des NOOTS-Zugriffstokens vom IAM für Behörden
- die Abfrage des Data Providers und der benötigten Verbindungsparameter

- der eigentliche Nachweisabruf.

2.4.2.2 Technische Beschreibung

Der SAK-DC ermöglicht via Anschlussprotokoll (bestehend aus REST-APIs) den sicheren Zugang zum NOOTS-Netzwerk für einen Data Consumer.

- Zur Absicherung der Zugriffe auf SAK-DC kommen **Basic Auth** und **OAuth 2.0** zum Einsatz
 - Bei einer gleichzeitigen Nutzung von **Basic Auth** und **OAuth 2.0** (Zugriffstoken) auf den Schnittstellen /evidence-offer und /evidence müssen beide Header-Werte in **einem** HTTP-Header angegeben werden:

Beispiel 1. Nutzung von Bearer- und Basic-Schemas in einem Header

```
Authorization: Bearer [[Zugriffstoken]],Basic  
[[Basic-Auth]]
```

- Zur Absicherung der Netzwerk-Kommunikation zwischen DC und SAK-DC kommt **(m)TLS** zum Einsatz

In der folgenden Matrix sind die Sicherheitsmechanismen in einer Matrix aufgeschlüsselt. Hier kann eingesehen werden, welcher Sicherheitsmechanismus wann eingesetzt werden sollte oder muss.

Endpunkt	mTLS	OAuth 2.0	Basic Auth
/token	optional (empfohlen)	-	optional
/de/evidence-offer	optional (empfohlen)	erforderlich	optional
/de/evidence	optional (empfohlen)	erforderlich	optional

Tabelle 8 – Aktivierung / Erzwingung der Sicherheitsmechanismen je Endpunkt

Die hierzu benötigten Zugangsdaten und Zertifikate müssen bei der Installation bereitgestellt und konfiguriert werden. Die benötigten

Zugriffstoken für die OAuth 2.0 Authentifizierung müssen zur Laufzeit über die `/token`-Schnittstelle abgerufen werden.

Hinweis:

- Die Übertragung der Nachweisdaten erfolgt ausschließlich über den geschützten Weg zwischen SAK-DC und SAK-DP
- Der Anbindung an den EU-Kontext ist derzeit nicht Teil der Anwendung

2.4.2.3 Installation der Anwendung

Nach Ihrer Registrierung für die NOOTS Testumgebung können Sie über NOVA auf dem [Dashboard](#) den Sicheren Anschlussknoten für die NOOTS Testumgebung herunterladen. Wählen Sie hierzu unter „NOOTS Testumgebung“ und „Für Data Consumer“ das Feld „Download SAK-Software“ aus. Laden Sie den SAK herunter.

Entpacken Sie die ZIP-Datei und installieren Sie den SAK. Die Details der spezifischen Installation und Konfiguration Ihres SAKs entnehmen Sie bitte den nachfolgenden Anweisungen und der Dokumentation der Konfigurationsdatei.

Für die Konfiguration der NOOTS-Anbindung an die Testumgebung benötigen Sie weitere individuelle Angaben, die Sie nach Versand des Registrierungsformulars automatisch per E-Mail vom Dataport Support erhalten und anschließend in Ihren Systemen eintragen:

- Die Komponenten-ID tragen Sie in den DC (nicht SAK-DC) ein.
- Die SAK-DC-ID tragen Sie in die Konfiguration des SAK-DC ein.

Zusätzlich finden Sie auf NOVA die für den SAK-DC in der jeweiligen Umgebung notwendigen Truststores. Diese müssen im Rahmen der Konfiguration ihres SAKs eingebunden werden, damit der SAK eine Kommunikation zum zentralen NOOTS und zum SAK-DP herstellen kann. In der ersten Iteration des NOOTS müssen SAK-DC und SAK-DP, die miteinander kommunizieren sollen, auch gegenseitige Zertifikate eingebunden haben. Das bedeutet: Wenn sich ein neuer SAK-DP an das NOOTS anbindet, und Sie als DC mit diesem neuen DP kommunizieren möchten, müssen Sie Ihren Truststore entsprechend aktualisieren. Der aktualisierte Truststore mit dem Zertifikat eines neu hinzugekommenen DPs wird im Rahmen der Anbindung dieses DPs auf NOVA bereitgestellt.

Installation des SAK-DC

Die nachfolgende Installationsanleitung beschreibt die Erstinstallation auf einem Linux-Server (keine Benutzeroberfläche) mit Zugriff mittels `ssh`.

Wichtig: Halten Sie sich auch hier an Ihre betrieblichen Vorgaben für einen sicheren Betrieb. Die hier beschriebenen Schritte dienen nur als Beispiel!

Der SAK-DC wird als ausführbare JAR-Datei (Java Archive) bereitgestellt.

Die JAR-Datei sollte in der Laufzeitumgebung abgelegt werden, in unserem Beispiel ist das `/opt/sak-dc`

Kopieren Sie die JAR-Datei mit der entsprechenden Version auf den Zielrechner, beispielsweise mit `scp`:

```
scp sak-dc-VERSION-TAG.jar admin@laufzeitumgebungshost:~
```

Loggen Sie sich per `ssh` auf dem Rechner ein:

```
ssh admin@laufzeitumgebungshost:~
```

Die Berechtigung sollte nur auf das Nötigste beschränkt werden, damit nur der ausführende User der Serveranwendung Leserechte hat. In unserem Beispiel läuft die Serveranwendung mit dem User `sak-dc` der der Linux Gruppe `sak-dc` zugehört.

```
sudo mkdir /opt/sak-dc
sudo chown root.sak-dc /opt/sak-dc
sudo chmod 750 /opt/sak-dc

sudo mv ~/sak-dc-VERSION-TAG.jar /opt/sak-dc

sudo chown root.sak-dc /opt/sak-dc/sak-dc-VERSION-TAG.jar
sudo chmod 640 /opt/sak-dc/sak-dc-VERSION-TAG.jar
```

Wichtig: Die Anwendung sollte unter keinen Umständen über den `root`-User des Systems, sondern idealerweise mittels eines eigenen Benutzers mit möglichst minimalen Rechten ausgeführt werden.

Systemvoraussetzungen

Die Systemvoraussetzungen für den Betrieb sind abhängig von der Anzahl der gleichzeitigen Zugriffe auf den SAK-DC. Je nach Mengengerüst können diese erheblich von den Mindestanforderungen abweichen.

Name	Mindestanforderungen
Java-JRE	JRE 21, getestet mit Adoptium Temurin
Betriebssystem	Linux amd64
Arbeitsspeicher	1024MB
Speicherplatz	512MB
Prozessor	2 GHz Dual Core, 64-Bit
Netzwerk	Internetverbindung (direkt oder über Proxy) auf Port 443

Tabelle 9 - Systemvoraussetzungen

Start und Konfiguration der Anwendung

Die Konfigurationen des SAK-DC findet mittels einer bereitgestellten `application.properties` statt, welche auf die Laufzeitumgebung angepasst werden muss. Die Parameter sind in der Datei beschrieben und enthalten Beispielwerte, an denen sich orientiert werden kann. Die Konfigurationsdatei muss als Parameter übergeben werden. Die Dateirechte auf die Konfigurationsdatei sollten auch hier so gesetzt werden, sodass nur die Anwendung darauf zugreifen kann.

```
java -jar sak-dc-VERSION-TAG.jar --  
spring.config.location=application.properties
```

Weiterführende Hinweise zur Konfiguration

Im oben genannten Beispiel wird davon ausgegangen, dass die `application.properties`-Datei im identischen Verzeichnis wie die Anwendung (.jar) selbst liegt. Wenn die Konfiguration aus einem anderen Verzeichnis geladen werden soll, kann dieses sowohl relational, sowie absolut angegeben werden. Außerdem können mehrere Dateien, auch *optional* angegeben werden. Hier muss die Reihenfolge beachtet werden. Dateien, welche früher in der Kette angegeben werden, werden durch spätere Dateien überschrieben (je nach Konfigurationsschlüssel)

```
java -jar sak-dc-VERSION-TAG.jar --
spring.config.location=\

#Konfigurations-Datei im gleichen Ordner; muss
vorhanden sein
    application.properties,\

#externe Konfigurations-Datei ; muss vorhanden sein
    /opt/default.properties,\

#externe Konfigurations-Datei ; optional, produziert
keinen Fehler, wenn nicht vorhanden
    optional:/opt/optional.properties
```

Weitere Informationen zu der Angabe von externen Konfigurationen können der offiziellen [Spring Boot Dokumentation](#); Kapitel "Externalized Configuration"; Abschnitt "External Application Properties" entnommen werden.

Die Anwendung sollte nun gestartet sein und folgende Meldung in der Ausgabe erscheinen:

Komponente SAK-DC erfolgreich gestartet

Proxykonfiguration

Wird für die Kommunikation nach Außen ein Proxyserver benötigt, muss dieser beim Start der Anwendung konfiguriert werden, nicht in der `application.properties`.

```
java -Dhttps.proxyHost=IP/HOSTPROXY  
-Dhttps.proxyPort=PROXYPORT  
-Dhttp.nonProxyHosts=PROXYAUSNAHMEN -jar sak-dc-VERSION-  
TAG.jar --spring.config.location=application.properties
```

Endpunkte

In der Standardkonfiguration ist die Serveranwendung über Port 8080 sowie der Managementendpunkt über Port 9000 erreichbar.

Wichtig: Diese Netzwerkports sollten über geeignete Firewallregeln abgesichert werden, um unbefugten Zugriff zu unterbinden. Halten Sie sich auch hier an Ihre betrieblichen Vorgaben für einen sicheren Betrieb.

In den offiziellen Test- und Produktionsumgebungen von NOOTS ist es verpflichtend, die Endpunkte nicht ungeschützt und unverschlüsselt zu betreiben. Es können hierbei verschiedenen Varianten genutzt werden. Je nach vorhandener Infrastruktur kann auch ein Betrieb hinter einem Proxy sinnvoll sein. In einer lokalen Teststellung ohne Anbindung gegen das NOOTS-System (z.B. mittels Mocks) können die Endpunkte auch weniger abgesichert betrieben werden.

Art	Erklärung
HTTPS	Die Konfiguration erfolgt über die <code>application.properties</code>
mTLS	Die Konfiguration erfolgt über die <code>application.properties</code>
HTTP Basic-Auth	Die Konfiguration erfolgt über die <code>application.properties</code>
Die obigen Methoden können bei Bedarf durch Apache-, Nginx oder einen anderen geeigneten Reverse Proxy abgebildet werden	Die Konfiguration erfolgt über das externe genutzte System

Tabelle 10 – Absicherung der Endpunkte

Start und Stop

Damit die Anwendung nicht immer manuell über die Konsole gestartet werden muss, können Mittel wie zum Beispiel `systemd` oder `init.d` genutzt werden.

Wir empfehlen hierzu die offizielle [Spring Boot Dokumentation](#); Kapitel "Installing Spring Boot Applications".

2.4.2.4 Regulärer Wirkungsbetrieb

2.4.2.4.1 Logging

Der SAK-DC verwendet standardmäßig die Konsole für Logausgaben. Das Log-Nachrichtenformat entspricht dem [Elastic Common Schema \(ECS\)](#).

2.4.2.4.2 Statusprüfung der Anwendungen

Der SAK-DC stellt die folgenden Endpunkte über den Management Port zur Statusprüfung bereit:

Hinweis: Diese Endpunkte sollten nur intern (z.B. hinter einer Firewall) betrieben werden. Eine Freigabe für einen öffentlichen, nicht regulierten Zugriff ist zu vermeiden!

Endpunkt	Beschreibung
<code>/actuator/health</code>	Gesamtstatus der Anwendung. Liefert <code>{"status": "UP DOWN"}</code> als Antwort

Tabelle 11 - Status-Endpunkte

2.4.2.4.3 Monitoring

Der SAK-DC kann zusätzliche Metriken liefern. Es stehen folgende Endpunkt zur Verfügung:

- `/metrics`
- `/prometheus` ([Spring Boot Dokumentation](#); Kapitel "Prometheus (prometheus)")

Die Endpunkte können über die `application.properties` aktiviert werden und sind über den Management-Port erreichbar.

Es werden folgende Standard-Metriken bereitgestellt:

Hinweis: Diese Endpunkte sollten nur intern (z.B. hinter einer Firewall) betrieben werden. Eine Freigabe für einen öffentlichen, nicht regulierten Zugriff ist zu vermeiden!

Metriken	Beschreibung	Path
JVM	Metriken zum Speicherverbrauch, zur Garbage Collection, Threads und geladenen Klassen.	<code>/actuator/metrics/jvm/*</code>
System	Metriken zur CPU-Auslastung, dem Dateisystem und der Uptime der Anwendung.	<code>/actuator/metrics/disk/</code> <code>/actuator/metrics/system/</code> <code>/actuator/metrics/process/*</code>
Application Startup	Metriken zur Startzeit der Anwendung.	<code>/actuator/metrics/application/*</code>
Logger	Metriken zu Logging-Events.	<code>/actuator/metrics/logback/events</code>
REST Services	Metriken zu aufgerufenen REST-Services.	<code>/actuator/metrics/http/*</code>

Tabelle 12 - Standard-Metriken

2.4.2.4.4 Backup und Recovery

Wir empfehlen mindestens folgende Daten zu sichern:

- Angepasste `application.properties` die für den Betrieb verwendet wird.
- Logs der Anwendung unter Beachtung der geltenden Datenschutzbestimmungen.

2.4.2.4.5 Hinweise für Störungsdiagnose und -behandlung

Debug-Logging

Die Konfiguration wird mit Log-Level **INFO** ausgeliefert, d.h. das Loggen von Debug-Ausgaben ist ausgeschaltet. Es kann aber mittels der `application.properties logging.level.root=DEBUG` eingeschaltet werden.

Achtung: Das Logging sollte auf der Produktivumgebung nie auf **DEBUG** gestellt werden. Aufgrund der umfangreichen Datenausgabe könnte es zu Performance- Problemen kommen. Gleichzeitig ist nicht sichergestellt, dass keine sicherheitsrelevanten Daten ausgegeben werden.

2.4.3 Testung

Wie bei der Anbindung an die NOOTS Referenzumgebung müssen Sie für Ihren Data Consumer auch in der NOOTS Testumgebung eine Testung durchführen, die aus drei Teilschritten besteht. Den Ablauf der Teilschritte für die Testung finden Sie in der nachfolgenden Abbildung beschrieben. Im ersten Schritt überprüfen Sie die notwendigen Vorbedingungen. Anschließend durchlaufen Sie selbstständig mindestens die im Rahmen dieses Dokumentes definierten Testfälle. Im Erfolgsfall buchen Sie einen Termin zur Testabnahme.

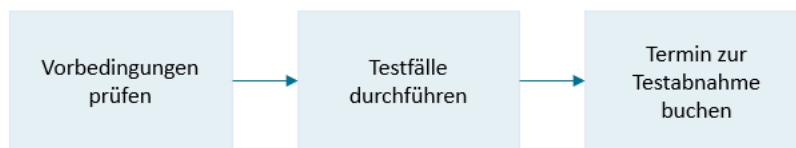


Abbildung 47 - Ablauf Testung NOOTS Testumgebung

2.4.3.1 Vorbedingungen

Folgende Vorbedingungen müssen mindestens erfüllt sein, damit Sie die Testabnahme mit Dataport durchführen können:

1. Der anzusprechende DP ist für die NOOTS Testumgebung eingerichtet, funktionsfähig und hat den NOOTS Readiness-Check Testumgebung bereits erfolgreich absolviert.
2. Ein funktionsfähiger SAK-DC für NOOTS Testumgebung ist gemäß der Anweisungen im vorausgehenden Kapitel dieses Dokumentes installiert und konfiguriert worden.
3. Ein DC-Client ist vorhanden, funktionsfähig und für den Tester verfügbar. Dies muss ein Online-Dienst sein, der denselben Stand hat, wie er in der Produktion eingesetzt wird.
4. Mindestens vier Nachweisabrufe für den DC-Client sind vorbereitet. Dabei handelt es sich um
 - Zwei unterschiedliche gültige Nachweisabrufe, die vom DP erfolgreich bedient werden.
 - Zwei unterschiedliche ungültige Nachweisabrufe, für die der DP einen Fehler zurückgibt (z.B. Nachweissubjekt unbekannt). Die Fehler müssen sich unterscheiden.
5. Es besteht Zugang zu den Logdateien des SAK-DC. Dieser Zugang kann im Rahmen der Testabnahme über eine Videokonferenz via Bildschirmübertragung live mit dem Support-Team von Dataport geteilt werden.
6. Folgende Angaben sind bekannt und können gegenüber dem Support-Team von Dataport im Rahmen der Testabnahme benannt werden:

- DC-Client
 - Name der Software oder des Online-Dienstes:
 - URL (nur im Falle eines Online-Dienstes oder eines Web-Clients):
 - IP-Adresse:
 - Version der Softwarekomponente:
- SAK-DC
 - URL:
 - IP-Adresse:
 - Version der Softwarekomponente:

Hilfreich für den Test ist es, wenn ein Vertreter der DP-Seite am Test teilnehmen kann.

Wenn Sie Rückfragen zur Erfüllung dieser Voraussetzungen haben, eröffnen Sie bitte ein Supportticket über NOVA [hier](#) oder wenden Sie sich an dataportnootssupport@dataport.de.

2.4.3.2 Testfälle

Wenn Sie alle Vorbedingungen, die mindestens erfüllt sein müssen, erreicht haben, fahren Sie mit der Durchführung der Testfälle fort. Diese werden im Rahmen der Testabnahme (s. Kapitel 2.4.3.3) erneut überprüft. Bitte dokumentieren Sie die Ergebnisse Ihrer Testfälle. Die hier abgebildeten Testfälle stellen die Mindestanforderungen dar und können individuell im Rahmen Ihres Testkonzeptes ergänzt verwendet werden.

Nr.	Testfall	Durchführung	Erwartetes Ergebnis
1	Es wird geprüft, ob für den ersten gültigen Nachweisabruf eine gültige und erfolgreiche Antwort vom DP zurückgegeben und in einer Vorschau (menschenslesbar) im DC angezeigt wird.	Der gültige Nachweisabruf wird vom DC-Client abgesetzt.	Im DC-Client wird die Zustimmung zum Nachweisabruf eingeholt. Der DC-Client erhält einen gültigen Nachweis als Antwort, welcher menschenlesbar in einer Vorschau dargestellt wird. Die Logs des SAK-DC zeigen keine Fehler.
2	Es wird geprüft, ob für den zweiten gültigen Nachweisabruf eine gültige und erfolgreiche Antwort vom DP zurückgegeben und in einer Vorschau (menschenslesbar) im DC angezeigt wird. Sie muss sich vom ersten Testfall unterscheiden!	Der gültige Nachweisabruf wird vom DC-Client abgesetzt.	Im DC-Client wird die Zustimmung zum Nachweisabruf eingeholt. Der DC-Client erhält einen gültigen Nachweis als Antwort, welcher menschenlesbar in einer Vorschau dargestellt wird. Die Logs des SAK-DC zeigen keine Fehler.
3	Es wird geprüft, ob für den ersten ungültigen Nachweisabruf eine gültige Antwort mit der passenden Fehlermeldung vom DP zurückgegeben wird.	Der erste ungültige Nachweisabruf wird vom DC-Client abgesendet.	Der DC-Client erhält eine gültige Nachweisantwort. Der fachliche Fehler wird in sprechender und nachvollziehbarer Weise auf der Oberfläche des DC angezeigt.
4	Es wird geprüft, ob für den zweiten ungültigen Nachweisabruf eine gültige Antwort mit der passenden Fehlermeldung vom DP zurückgegeben wird. Sie muss sich vom ersten Testfall unterscheiden!	Der zweite ungültige Nachweisabruf wird vom DC-Client abgesendet.	Der DC-Client erhält eine gültige Nachweisantwort. Der fachliche Fehler wird in sprechender und nachvollziehbarer Weise auf der Oberfläche des DC angezeigt
5	Der DC wird so konfiguriert, dass die IAM-B-Abfrage scheitert	Der gültige Nachweisabruf wird vom DC-	Der DC-Client behandelt den Fehler aktiv und gibt auf der Oberfläche einen sprechenden

	(falsche Komponenten-ID). Es wird geprüft, ob der Fehler korrekt behandelt wird, wenn die IAM-B-Abfrage scheitert.	Client abgesendet.	Fehler aus (z.B. "Nachweisabruf nicht möglich"). In den Logs des DC erscheint die Fehlermeldung über den gescheiterten Token-Zugriff mit der dazugehörigen Trace-ID.
6	Der DC wird so konfiguriert, dass die RDN-Abfrage scheitert (falsche Evidence-Type-ID). Es wird geprüft, ob der Fehler korrekt behandelt wird, wenn die RDN-Abfrage scheitert.	Der gültige Nachweisabruf wird vom DC-Client abgesendet.	Der DC-Client behandelt den Fehler aktiv und gibt auf der Oberfläche einen sprechenden Fehler aus (z.B. "Nachweisabruf nicht möglich"). In den Logs des DC erscheint die Fehlermeldung über den gescheiterten Token-Zugriff mit der dazugehörigen Trace-ID.

Tabelle 13 - Testfälle NOOTS Testumgebung DC

Wenn Sie Rückfragen zur Erfüllung dieser Voraussetzungen haben, eröffnen Sie bitte ein Supportticket über NOVA [hier](#) oder wenden Sie sich an dataportnootssupport@dataport.de.

2.4.3.3 Testabnahme

Wenn Sie alle Testfälle erfolgreich abgeschlossen haben, buchen Sie per E-Mail an dataportnootssupport@dataport.de einen Termin zur Testabnahme beim Support-Team von Dataport. Sie können den Termin zur Testabnahme verkürzen, wenn Sie die informativen Vorbedingungen aus Kapitel 2.4.3.1 (Stichpunkt 6.) bereits bei der Terminbuchung per E-Mail angeben.

In dem Termin prüfen Sie dann gemeinsam mit Dataport, ob die Vorbedingungen erfolgreich erfüllt sind. Anschließend durchlaufen Sie gemeinsam mit dem Support-Team die geschilderten Testfälle.

Außerdem müssen Sie im Rahmen des Termines zur Testabnahme folgende Fragen beantworten:

- Welche testverantwortlichen Personen sind auf dem Readiness-Check namentlich zu erwähnen (1-4 Personen)?
- Wie lautet der Anwendungsfall auf dem Readiness-Check (Beispiel: Erprobung des nationalen Nachweisdatenaustauschs und Anbindung des Nachweises)

XXX aus dem Register YYY an den Onlinedienst ZZZ (UC-Kürzel))?

2.4.4 NOOTS-Readiness-Check Testumgebung

Wenn die Testabnahme erfolgt ist, stellt Dataport den NOOTS-Readiness-Check Testumgebung für Sie aus. Dieser wird dem BVA und Ihnen per E-Mail bereitgestellt. Anschließend erhalten Sie von Dataport eine Einladung zu einem Lessons Learned-Gespräch. In diesem Gespräch möchten wir gern von Ihnen erfahren, was im Rahmen der Anbindung an die NOOTS Testumgebung bereits gut funktioniert hat und wo es noch Optimierungspotentiale gibt. Danach können Sie mit der Anbindung an die NOOTS Produktivumgebung fortfahren.

2.5. Anbindung: NOOTS Produktivumgebung

Die einzelnen Schritte zur Anbindung an die NOOTS Produktivumgebung sind in der folgenden Abbildung dargestellt und werden in den weiteren Abschnitten im Detail erläutert.

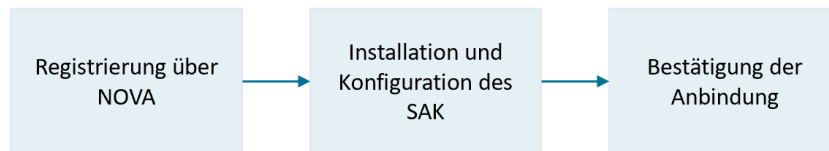


Abbildung 48 - Anbindung an die NOOTS Produktivumgebung

2.5.1 Registrierung über NOVA



Anbindung (NOOTS Produktivumgebung)

- Beantragung Registrierung NOOTS Produktivumgebung über NOVA
- Technische Anbindung: Download, Installation und Konfiguration des SAK
- Bestätigung der Anbindung Produktivumgebung
- Lessons Learned / Abschlussgespräch

Für die Registrierung im IAM-B benötigen wir von Ihnen als Data Consumer unterschiedliche Informationen. Bitte melden Sie sich hierzu erneut mit Ihrem MUK-Konto bei NOVA an. Wählen Sie anschließend das „Dashboard“ aus.

Abbildung 49 - NOOTS Produktivumgebung

Beachten Sie bitte auf dem NOVA-Dashboard, dass Sie die Registrierung für die NOOTS Produktivumgebung als Data Consumer vornehmen wollen.

Wenn Sie die Registrierung für Data Consumer für die NOOTS Produktivumgebung auswählen, öffnet sich ein neues Formular. Hier können Sie das benötigte Registrierungsformular als PDF herunterladen. Bitte füllen Sie das PDF vollständig aus. Dies beinhaltet auch den Upload des öffentlichen Schlüssels Ihres erworbenen TLS-Client-Zertifikats für die NOOTS Produktivumgebung. Der private Schlüssel muss bei Ihnen verbleiben und geheim gehalten werden. Anschließend ist es aus Sicherheitsgründen erforderlich, dass Sie das Registrierungsformular mit einem personenbezogenen Zertifikat der V-PKI/DOI-CA signieren. Eine Schritt-für-Schritt Anleitung hierzu finden Sie in Abschnitt 2.2.7 dieses Dokumentes.

Wenn Sie das Registrierungsformular signiert haben, speichern Sie es ab. Füllen Sie die erforderlichen Angaben auf der Website aus und klicken Sie auf „Weiter zum Datei-Upload“. Laden Sie nun das signierte Registrierungsformular hoch und klicken Sie auf „Weiter zur Zusammenfassung“.

Bitte überprüfen Sie in der Zusammenfassung Ihre eingegebenen Daten. Wenn alles korrekt ist klicken Sie auf „Formular absenden“. Sie erhalten eine Bestätigung über den Formularversand per E-Mail.

2.5.2 Installation und Konfiguration des Sicheren Anschlussknotens

Nach Ihrer Registrierung für die NOOTS Produktivumgebung können Sie über NOVA auf dem [Dashboard](#) den Sicheren Anschlussknoten für die NOOTS Produktivumgebung herunterladen. Wählen Sie hierzu unter „NOOTS Produktivumgebung“ und „Für Data Consumer“ das Feld „Download SAK-Software“ aus. Laden Sie den SAK runter.

Entpacken Sie die ZIP-Datei und installieren Sie den SAK. Die Details der spezifischen Installation und Konfiguration Ihres SAKs entnehmen Sie bitte dem Kapitel 2.4.2.1 und der Dokumentation der Konfigurationsdatei.

Für die Konfiguration der NOOTS-Anbindung benötigen Sie weitere individuelle Angaben, die Sie nach Versand des Registrierungsformulars automatisch per E-Mail vom Dataport Support erhalten und anschließend in Ihren Systemen eintragen:

- Die Komponenten-ID tragen Sie in den DC (nicht SAK-DC) ein.
- Die SAK-DC-ID tragen Sie in die Konfiguration des SAK-DC ein.

Zusätzlich finden Sie auf NOVA die für den SAK-DC in der jeweiligen Umgebung notwendigen Truststores. Diese müssen im Rahmen der Konfiguration ihres SAKs eingebunden werden, damit der SAK eine Kommunikation zum zentralen NOOTS und zum SAK-DP herstellen kann. In der ersten Iteration des NOOTS müssen SAK-DC und SAK-DP, die miteinander kommunizieren sollen, auch gegenseitige Zertifikate eingebunden haben. Das bedeutet: Wenn sich ein neuer SAK-DP an das NOOTS anbindet, und Sie als DC mit diesem neuen DP kommunizieren möchten, müssen Sie Ihren Truststore entsprechend aktualisieren. Der aktualisierte Truststore mit dem Zertifikat eines neu hinzugekommenen DPs wird im Rahmen der Anbindung dieses DPs auf NOVA bereitgestellt.

Folgen Sie zur Installation des SAK-DC nun dem Abschnitt „Installation des SAK-DC“ im Kapitel 2.4.2.3 dieses Dokumentes. Kehren Sie anschließend zum nachfolgenden Kapitel 2.5.3 zurück.

2.5.3 Bestätigung der Anbindung

Wenn Sie den SAK gemäß den Angaben im vorherigen Kapitel installiert und konfiguriert haben, überprüfen Sie im eigenen Ermessen, ob in der NOOTS Produktivumgebung ein erfolgreicher Durchlauf stattgefunden hat. Im Erfolgsfall teilen Sie das Ergebnis Dataport via E-Mail an dataportnootssupport@dataport.de mit. Dataport stellt Ihnen dann die „Bestätigung der Anbindung Produktivumgebung“ aus. Diese wird dem BVA und Ihnen per E-Mail zur Verfügung gestellt. Anschließend erhalten Sie von Dataport eine Einladung zu einem Lessons Learned-Gespräch bzw. zum Abschlussgespräch. In diesem Gespräch möchten wir gern von Ihnen erfahren, wie der gesamte Anbindungsprozess aus Ihrer Sicht verlaufen ist, welche Herausforderungen oder Verbesserungsmöglichkeiten Sie identifiziert haben und welche Erfahrungen Sie im Rahmen der Anbindung an zukünftige Data Consumer weitergeben möchten.

3. Kontaktmöglichkeiten

Themenbereich / Anliegen	Kontakt
Allgemeine Informationen zur Anbindung	https://nova.noots.gov.de/
Allgemeine Fragen zur Anbindung	registermodernisierung@bva.bund.de
Rückfragen zu	dataportnootssupport@dataport.de
• Anbindungstests • Anbindungsprozess • Zertifikaten und zur Zertifikatsbeschaffung • Installation und Konfiguration des SAK • Sonstigen technischen Themen	

4. Weiterführende Informationen

Schnittstellendefinitionen der SAKs (SAK-DP & SAK-DC auf OpenCode)

In diesem Dokument wurden bereits die wichtigsten Endpunkte der SAK beschrieben, die aktuelle Version aller Schnittstellendefinitionen der SAK-DP, sowie SAK-DC finden Sie auf der OpenCode-Plattform unter folgender Adresse:

<https://gitlab.opencode.de/noots/public/sak-apis> (öffentlich zugänglich)

Ausgewählte Architekturdokumente des NOOTS-Systems

Ausgewählte Architekturdokumente finden Sie unter folgender Adresse:

<https://bmi.usercontent.opencode.de/noots/> (öffentlich zugänglich)

<https://www.nrw-connect-extern.nrw.de/confluence/pages/viewpage.action?pageId=281904724>
(nicht öffentlich zugänglich)

XNachweis

Der XÖV-Standard XNachweis wird in der NOOTS Referenzumgebung aktuell in der Version 1.4.0 unterstützt. XNachweis kann über das XRepository eingesehen werden:

XÖV-Standard <https://www.xrepository.de/details/urn:xoev-de:bva:standard:xnachweis>

Glossar

Begriffserläuterungen und Abkürzungen finden Sie im Glossar des NOOTS-Projektes auf der OpenCode-Plattform unter folgender Adresse:

<https://bmi.usercontent.opencode.de/noots/Glossar/> (öffentlich zugänglich)

NOVA

Für weitere Begleitdokumente zum NOOTS-Anbindungsprozess
besuchen Sie NOVA:

<https://nova.noots.gov.de/startseite> (öffentlich zugänglich)

<https://nova.noots.gov.de/begleitdokumente> (nicht öffentlich
zugänglich)

5. Änderungsverzeichnis

Version	Änderungs- datum	Gliederungs- punkt	Erläuterung der Änderung
0.1	28.02.2025		Erster Entwurf
0.2	18.03.2025		Kommentare von BVA, SEITENBAU, BearingPoint und msg
0.3	10.04.2025		Kommentare, sofern möglich, eingearbeitet
0.4-0.9	10.07.2025 – 30.09.2025		Grundlegende Überarbeitungen im Rahmen des definierten Anbindungsprozesses; Integration von Dokument zur Zertifikatsbeschaffung sowie der Integrationsanleitungen von Seitenbau
1.0	13.- 14.10.2025		Kommentare von BVA, SEITENBAU, BearingPoint und msg eingearbeitet

6. Abkürzungsverzeichnis / Glossar

Kürzel	Bedeutung	Inhaltliche Erläuterung
API	Application Programming Interface	Schnittstelle, die es Software ermöglicht, miteinander zu kommunizieren und Funktionen auszutauschen
BVA	Bundesverwaltungsamt	Bundesoberbehörde im Geschäftsbereich des Bundesministeriums des Innern (BMI)
DC	Data Consumer	NOOTS-Teilnehmer zum Abruf von Nachweisen (nationale Online-Dienste und Fachverfahren)
DOI-CA	Deutschland Online Infrastruktur Certification Authority	Zertifizierungsstelle (CA) für die Ausstellung von Zertifikaten für die Deutschland Online Infrastruktur (DOI)
DP	Data Provider	NOOTS-Teilnehmer zur Lieferung von Nachweisen (nationale Register)
EV	Extended Validation	Höchste Validierungsstufe eines SSL-Zertifikats
IAM	Identity und Access Management	Zentrales System zur Zuordnung und zum Abruf berechtigungsrelevanter Informationen für Zugriffe auf Ressourcen gemäß rechtlicher Vorgaben
MUK	Mein Unternehmenskonto	Staatlich bereitgestelltes Nutzerkonto mit der Möglichkeit, digitale Verwaltungsleistungen über einen deutschlandweit einheitlichen Zugang zu nutzen
NOOTS	Nationales Once-Only- Technical-System	System aus technischen Komponenten, Schnittstellen und Standards sowie organisatorischen und rechtlichen Regelungen, das öffentlichen Stellen den rechtskonformen Abruf von elektronischen Nachweisen aus den Registern der deutschen Verwaltung ermöglicht

NOVA	Nutzerorientiertes Online-Vorregistrierungs- und Anbindungsportal	Webseite die den Anbindungsprozess für Data Provider/Consumer und den Support für NOOTS abbildet
QWACs	Qualified Website Authentication Certificates	Spezialfall der Extended Validation-Zertifikate und ein Vertrauensdienst gemäß der eIDAS-Verordnung der Europäischen Union.
RDN	Registerdaten-navigation	NOOTS-Komponente und zentraler Routingdienst; liefert auf Anfrage Information von welchem Register ein gesuchter Nachweis abgerufen werden kann
SAK	Sicherer Anschlussknoten	Dezentrale NOOTS-Komponente über die Data Consumer und Data Provider an eine NOOTS-Instanz angebunden werden müssen, um den Transport zwischen den Data Consumern, Data Providern und allen NOOTS-Komponenten zu kapseln
TLS	Transport Layer Security	Protokoll zur sicheren Verschlüsselung von Daten bei der Internetkommunikation
V-PKI	Public Key Infrastruktur der Verwaltung	Zertifikatsbasierte Infrastruktur für elektronische Signatur und Verschlüsselung in der digitalen Kommunikation

7. Betrieblich-Relevante Konfigurationsparameter

```
# -----  
# SAK-DC Transportprotokoll Einstellungen  
# -----  
# Zugewiesene NOOTS-Komponenten-ID des Sicheren  
Anschlussknotens  
sakdc.id =  
  
# SAK-Client TLS-Auth  
# Hardware-basierte Schlüsselspeicher (empfohlen)  
spring.ssl.bundle.jks.client.keystore.type = PKCS11  
spring.ssl.bundle.jks.client.keystore.password =  
spring.ssl.bundle.jks.client.key.alias = sakdc-client-  
crt  
# Datei-basierte Schlüsselspeicher (nicht empfohlen,  
bitte nur PKCS12 in diesem Fall verwenden)  
#spring.ssl.bundle.jks.client.keystore.type = PKCS12  
#spring.ssl.bundle.jks.client.keystore.location =  
sakdc-client-cert.pl2  
#spring.ssl.bundle.jks.client.keystore.password  
  
# Truststore mit Zertifikaten, die der SAK bei  
ausgehenden Aufrufen vertrauen darf.  
# Optional; das System-Truststore des JRE wird  
verwendet, falls nicht gesetzt.  
#spring.ssl.bundle.jks.client.truststore.type = PKCS12  
#spring.ssl.bundle.jks.client.truststore.location =  
sakdc-client-truststore.pl2  
  
#spring.ssl.bundle.jks.client.truststore.password =
```

```
# Truststore-Konfiguration für die NOOTS-Zugriffstoken-
Validierung
spring.ssl.bundle.jks.iamsigncert.truststore.type =
PKCS12
spring.ssl.bundle.jks.iamsigncert.truststore.location =
iam-sign-cert.p12
spring.ssl.bundle.jks.iamsigncert.truststore.password =
#spring.ssl.bundle.pem.iamsigncert.truststore.certificat
e = iam-sign-cert.crt
#spring.ssl.bundle.pem.iamsigncert.truststore.certificat
e = -----BEGIN CERTIFICATE-----....

# Truststore-Konfiguration für die NOOTS-Zuständigkeit-
/Verbindungstoken (RDN-Token) Validierung
spring.ssl.bundle.jks.rdnsigncert.truststore.type =
PKCS12
spring.ssl.bundle.jks.rdnsigncert.truststore.location =
rdn-sign-cert.p12
spring.ssl.bundle.jks.rdnsigncert.truststore.password =
#spring.ssl.bundle.pem.rdnsigncert.truststore.certificat
e = rdn-sign-cert.crt
#spring.ssl.bundle.pem.rdnsigncert.truststore.certificat
e = -----BEGIN CERTIFICATE-----....

# NOOTS IAM Hostname
noots.iam.hostname = iam.noots.gov.de
# NOOTS RDN Hostname
noots.rdn.hostname = rdn.noots.gov.de

# -----
# SAK-DC Anschlussprotokoll Einstellungen
# -----

# SAK-Server Adresse
server.address = localhost
#SAK-Server Port
server.port = 8443
```

```
# Optionale Basic-Auth Authentifizierung der
Schnittstellen des SAKs
# Schnittstellen des SAKs können laut der
Schnittstellenspezifikation optional via
# Basic-Auth gesichert werden. Sollte dies der Fall
sein, muss hier
# "basicauth.token.active" muss auf "true" gesetzt

werden, um den Token-Endpunkt abzusichern.
basicauth.token.active = true
# "basicauth.other.active" muss auf "true" gesetzt
werden, um die Evidence- und Evidence-Offer-Endpunkte
mit Basic-Auth abzusichern.
basicauth.other.active = true
# Username + Passwort muss angegeben werden, sobald
mindestens einer der oberen Werte auf "true" gesetzt
sind.
basicauth.username =
basicauth.password =

# SAK-Server TLS
# Hardware-basierte Schlüsselspeicher (empfohlen)
spring.ssl.bundle.jks.server.keystore.type = PKCS11
spring.ssl.bundle.jks.server.keystore.password =
spring.ssl.bundle.jks.server.key.alias = sakdc-server-
crt
# Datei-basierte Schlüsselspeicher (nicht empfohlen,
bitte nur PKCS12 in diesem Fall verwenden)
#spring.ssl.bundle.jks.server.keystore.type = PKCS12
#spring.ssl.bundle.jks.server.keystore.location = sakdc-
server-cert.p12
#spring.ssl.bundle.jks.server.keystore.password =
# Separate TLS Server-Zertifikaten, falls der SAK unter
unterschiedlichen Hostnames exponiert ist
#server.ssl.server-name-bundles[0].server-name = sak-
dcl.example.com #server.ssl.server-name-
bundles[0].bundle = sakdcl
```

```
#spring.ssl.bundle.jks.sakdc1.keystore.type = PKCS11
#spring.ssl.bundle.jks.sakdc1.keystore.password =
#spring.ssl.bundle.jks.sakdc1.key.alias = sakdc1-server-
crt #spring.ssl.bundle.jks.sakdc1.options.enabled-
protocols = ${sakdc.server.ssl.enabled-protocols}
#spring.ssl.bundle.jks.sakdc1.options.ciphers =
${sakdc.server.ssl.enabled-ciphers}

# SAK-Server TLS Client-Auth
# Einkommentieren, falls DCs ohne Client-Zertifikat den
SAK aufrufen
#server.ssl.client-auth = none
# Truststore mit vertrauenswürdigen Client-Cert-CAs
# Auskommentieren, falls DCs ohne Client-Zertifikat den
SAK aufrufen
spring.ssl.bundle.jks.server.truststore.type = PKCS12
spring.ssl.bundle.jks.server.truststore.location =
sakdc-server-truststore.pl2
spring.ssl.bundle.jks.server.truststore.password =

# SAK-Server TLS deaktivieren (nicht empfohlen, bitte
sicherstellen, dass DCs nur über verschlüsselten Wege
den SAK aufrufen).
# ACHTUNG: 'server.port' wird standardmäßig auf 8080
gesetzt.
# In diesem Fall, alle 'spring.ssl.bundle.jks.server.*'
Properties auskommentieren.
#spring.profiles.active = plain-http
# -----
# SAK-DC Allgemeine Anwendungskonfiguration
# -----
# Arbeitsordner des Webservers
# Dieser muss für die Anwendung lesbar und beschreibbar
sein.
# Andere User und Anwendungen sollen nicht darauf
zugreifen können.
server.tomcat.basedir = /var/run/sak-d
```

```
# Monitoring-Endpunkte der Anwendung
# Die folgenden Endpunkte werden über die URL
"http://{{management.server.address}}:{{management.server.port}}/actuator/{{endpoint}}" auf dem
# konfigurierten Management-Port standardmäßig zur
Verfügung gestellt und können über den
Konfigurationswert
# "management.endpoints.web.exposure.include"
selektiv aktiviert und damit exponiert werden:
# - health: Der Health-Endpunkt stellt Informationen
über die Readiness und Liveness der Anwendung bereit
# - prometheus: Der Prometheus-Endpunkt stellt eine
Vielzahl an Metriken im Prometheus-Format zur
Verfügung
# - info: Der Info-Endpunkt liefert interne
Informationen der Anwendung, z.B. Daten zum Build
oder zur aktuellen Laufzeitumgebung
# - sbom: Der SBOM-Endpunkt liefert eine Auflistung
aller Abhängigkeiten und Bibliotheken im SAK-DC
management.endpoints.web.exposure.include =
health,prometheus
# Verbindungseinstellungen für die Management-
Endpoints
management.server.address = localhost
management.server.port = 9000

# Logging-Einstellungen
# Mögliche Log-Level: ERROR, WARN, INFO, DEBUG, TRACE
# In einer Produktivumgebung sollte immer min. WARN
gesetzt werden
# Basis-Level für alle Logmeldungen der Anwendung
# (spezifische Log-Level überschreiben die Basis)
logging.level.root = INFO
```

8. Abbildungsverzeichnis

Abbildung 1 - Grobübersicht NOOTS erste Iteration	5
Abbildung 2 - Eigenschaften und Zweck der Umgebungen	6
Abbildung 3 - Übersicht Anbindungsprozess	8
Abbildung 4 – Technische Anbindungsvorbereitung	8
Abbildung 5 - Anmeldung mit MUK	9
Abbildung 6 - Begleitdokumente zur NOOTS-Anbindung.....	9
Abbildung 7 - Übersicht Zertifikate NOOTS	
Produktivumgebung	12
Abbildung 8 - Übersicht Komponenten und Zertifikate zur	
Beschaffung durch DC/DP in der NOOTS	
Produktivumgebung	14
Abbildung 9 - Anmelden im Webportal der	
Zertifizierungsstelle.....	17
Abbildung 10 - Auswahl der Domäne.....	18
Abbildung 11 - Auswahl des Zertifikatstyps.....	18
Abbildung 12 - Erfassung der Daten des Antragsstellers	19
Abbildung 13 - Erfassung der Zertifikatsdaten für	
personenbezogenes Zertifikat.....	19
Abbildung 14 - Erfassung der Zertifikatsdaten für	
personenbezogenes Zertifikat: Weitere Angaben.....	20
Abbildung 15 - Erfassung der Zertifikatsdaten für	
gruppenbezogenes Zertifikat: Auswahl der Domäne.....	20
Abbildung 16 - Auswahl des Zertifikatstyps für Gruppen-	
/Funktions-Zertifikat	21
Abbildung 17 - Erfassung der Daten des Antragsstellers für	
Gruppen-/Funktions-Zertifikat	21
Abbildung 18 - Erfassung der Zertifikatsdaten für Gruppen-	
/Funktions-Zertifikat	22
Abbildung 19 - Erfassung der Zertifikatsdaten für Gruppen-	
/Funktions-Zertifikat: Weitere Angaben.....	22
Abbildung 20 - Veröffentlichung und Sperrung des	
Zertifikats	24
Abbildung 21 - Abrechnung des beantragten Zertifikats	24
Abbildung 22 - Mitteilung an die Registrierungsstelle	25
Abbildung 23 - Zusammenfassung der Antragsdaten	26
Abbildung 24 - Download des Antragsformulars	27
Abbildung 25 - Abholung des Software-Zertifikates Teil I ...	28
Abbildung 26 - Abholung des Software-Zertifikates Teil II..	28
Abbildung 27 - Abholung des Software-Zertifikates Teil III	29

Abbildung 28 - Registrierungsformular in Adobe Acrobat Pro	30
Abbildung 29 - Untermenü "Digital signieren"	31
Abbildung 30 - Auswahl der digitalen ID	31
Abbildung 31 - Konfiguration einer digitalen ID zum Signieren	32
Abbildung 32 - Suchen einer digitalen ID-Datei	32
Abbildung 33 - Auswahl der digitalen ID nach Konfiguration	33
Abbildung 34 - Unterschreiben mit der digitalen ID	33
Abbildung 35 - Öffentlichen Schlüssel mittels Kleopatra auslesen	34
Abbildung 36 - Zertifikatsdetailansicht Kleopatra	35
Abbildung 37 - Schritte zur Anbindung an die NOOTS Referenzumgebung	36
Abbildung 38 - Anbindungsverprobung: NOOTS Referenzumgebung	36
Abbildung 39 - NOVA Dashboard	37
Abbildung 40 - Data Consumer mit integriertem SAK-DC	40
Abbildung 41 - Data Consumer ohne integrierten SAK-DC	42
Abbildung 42 - Übersicht über die Zertifikate des Data Consumers	46
Abbildung 43 - Ablauf Testung NOOTS Referenzumgebung	55
Abbildung 44 - Anbindung an die NOOTS Testumgebung	58
Abbildung 45 - NOOTS Testumgebung	58
Abbildung 46 - SAK-DC: Fachlicher Kontext	59
Abbildung 48 - Ablauf Testung NOOTS Testumgebung	69
Abbildung 49 - Anbindung an die NOOTS Produktivumgebung	74
Abbildung 50 - NOOTS Produktivumgebung	74

9. Tabellenverzeichnis

Tabelle 1 - Übersicht Zertifikate Data Consumer	13
Tabelle 2 - Übersicht Anforderungen Zertifikate Data Consumer	13
Tabelle 3 - Bestandteile von Zugriffstoken	48
Tabelle 4 - Mögliche HTTP-Status Codes.....	49
Tabelle 5 - Mögliche HTTP-Status Codes.....	52
Tabelle 6 - Mögliche HTTP-Status Codes.....	55
Tabelle 7 - Testfälle NOOTS Referenzumgebung DC.....	56
Tabelle 8 - Aktivierung / Erzwingung der Sicherheitsmechanismen je Endpunkt.....	60
Tabelle 9 - Systemvoraussetzungen	63
Tabelle 10 - Absicherung der Endpunkte	66
Tabelle 11 - Status-Endpunkte	66
Tabelle 12 - Standard-Metriken	67
Tabelle 12 - Testfälle NOOTS Testumgebung DC	72