Bundesverwaltungsamt

Referat D III 3 – Registermodernisierung; Errichtung und Betrieb NOOTS

Zertifikate für den Anschluss von Data Providern an das Nationale Once-Only-Technical-System (NOOTS)

Version 2.2
18.02.2026

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: noots.umsetzung@bva.bund.de

Inhaltsverzeichnis

1. Einleitung

Dieses Dokument gibt betriebsverantwortlichen Stellen eines Data Provider (DP) einen Überblick über die bei dem Anschluss an das NOOTS zu erwerbenden Zertifikate zur NOOTS-Kommunikation. Eine Anleitung zur Beschaffung der V-PKI/DOI-CA (Public Key Infrastruktur der Verwaltung) Zertifikate, welche zur NOOTS-Registrierung benötigt werden sowie ein mögliches Vorgehen zur Signierung des Registrierungsformulars über noots.gov.de, sind dem „Vertiefungsleitfaden für die Beschaffung von V-PKI Zertifikaten für Data Consumer und Data Provider für den Anschluss an das NOOTS“ zu entnehmen. Dieses Dokument wird zur Verfügung gestellt, um eine Beschaffung der Zertifikate, welche teilweise mehrere Wochen in Anspruch nehmen kann, frühzeitig zu unterstützen.

Data Provider sind NOOTS-Teilnehmer zur Lieferung von Nachweisen. Data Consumer sind NOOTS-Teilnehmer zum Abruf von Nachweisen und können Online-Dienste, Fachverfahren und die Intermediäre Plattform sein.

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.

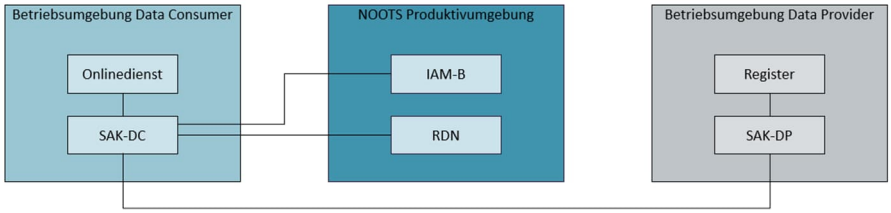

Abbildung 1 - Grobübersicht NOOTS MVP-Phase

In diesem Dokument wird vorausgesetzt, dass das System NOOTS mit seinen Komponenten und Teilnehmenden (z.B. Data Consumer) grundsätzlich bekannt ist. Sofern dies nicht der Fall ist, wird hierzu auf die weitere Begleitdokumentation sowie auf die Informationen des Bundesverwaltungsamt und des Bundesministeriums für Digitalisierung und Staatsmodernisierung verwiesen.

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

- NOOTS Referenzumgebung
- NOOTS Testumgebung
- NOOTS Produktivumgebung

Die zentrale NOOTS-Registrierung der anzuschließenden Teilnehmer und automatisierte Weiterverarbeitung der Anschlussdaten erfolgt über noots.gov.de.

2. Zertifikatsbeschaffung: Übersicht über die Zertifikate

HINWEIS: Für den Anschluss 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 Anschlussvorbereitung anzustoßen.

Für den Anschluss 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.

Für den Anschluss an das NOOTS benötigen Sie Zertifikate für zwei voneinander unabhängige Zwecke:

- Zur NOOTS-Registrierung
- Für die technische NOOTS-Kommunikation

Die Zertifikate für die NOOTS-Registrierung werden ausschließlich im Anschlussprozess benötigt (die Beschaffung der Zertifikate für die NOOTS-Registrierung wird in diesem Leitfaden nicht weiter berücksichtigt. Eine Schritt-für-Schritt-Anleitung ist hier zu finden: „Vertiefungsleitfaden für die Beschaffung von V-PKI Zertifikaten für Data Consumer und Data Provider für den Anschluss an das NOOTS“ .
Die Zertifikate für die technische Kommunikation sind dauerhaft bei erfolgtem Anschluss an das 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.

2.1. 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:

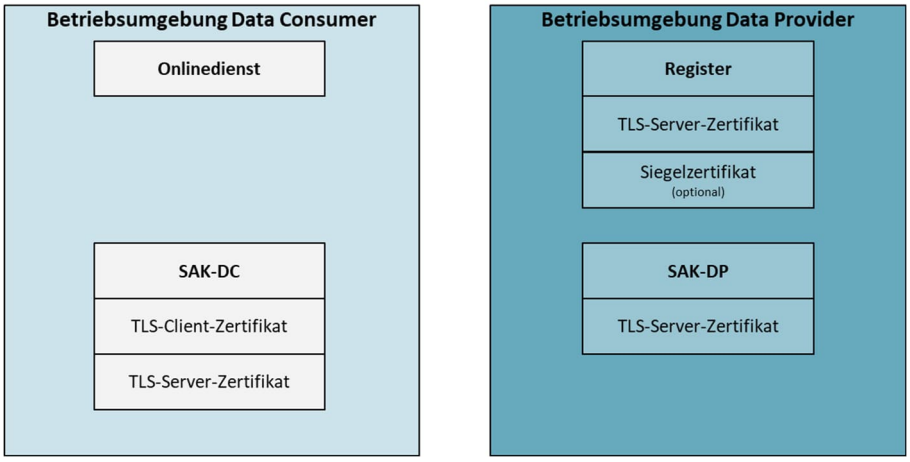

Abbildung 2 - Übersicht Zertifikate NOOTS Produktivumgebung

Für einen Data Provider werden für die Kommunikation mit dem NOOTS insgesamt acht Zertifikate benötigt. Davon sind für die erste Iteration des NOOTS drei Zertifikate optional.

NOOTS Referenzumgebung	NOOTS Testumgebung	NOOTS Produktivumgebung
TLS-Server-Zertifikat des Registers (optional)	TLS-Server-Zertifikat des Registers	TLS-Server-Zertifikat des Registers
TLS-Server-Zertifikat des SAK-DP	TLS-Server-Zertifikat des SAK-DP	TLS-Server-Zertifikat des SAK-DP
	Siegelzertifikat (zunächst optional)	Siegelzertifikat (zunächst optional)

Tabelle 1 - Übersicht Zertifikate Data Provider

Das TLS-Server-Zertifikat des Registers dient ausschließlich der Kommunikation zwischen dem Register und dem SAK-DP innerhalb der Betriebsumgebung des Data Provider. Das TLS-Server-Zertifikat des SAK-DP dient der Authentisierung des SAK-DP gegenüber dem SAK-DC und ermöglicht darüber hinaus eine Transport-verschlüsselung. Das Siegelzertifikat wird für die Siegelung der Nachweisdaten verwendet, ist aber in der ersten Iteration in der NOOTS Test- und Produktivumgebung optional. Bei der Registrierung für die NOOTS Test- und Produktivumgebung müssen Sie das TLS-Server-Zertifikat des SAK-DP im PEM-Format in das Registrierungsformular einfügen.

3. Anforderungen an die Zertifikate

In der nachfolgenden Tabelle finden Sie eine Übersicht über die gestellten Anforderungen, die in den nachfolgenden Abschnitten vertieft werden.

Umgebung	Zertifikat	Anforderung
NOOTS Referenzumgebung	TLS-Server-Zertifikat des Registers (optional)	geeignetes TLS-Zertifikat zur Gewährleistung der Transportverschlüsselung
	TLS-Server-Zertifikat des SAK-DP	geeignetes TLS-Zertifikat zur Gewährleistung der Transportverschlüsselung
NOOTS Testumgebung	TLS-Server-Zertifikat des Registers	geeignetes TLS-Zertifikat zur Gewährleistung der Transportverschlüsselung
	TLS-Server-Zertifikat des SAK-DP	geeignetes TLS-Zertifikat zur Gewährleistung der Transportverschlüsselung
	Siegelzertifikat (zunächst optional)	für Siegelung geeignetes Zertifikat
NOOTS Produktivumgebung	TLS-Server-Zertifikat des Registers	geeignetes TLS-Zertifikat zur Gewährleistung der Transportverschlüsselung
	TLS-Server-Zertifikat des SAK-DP	TLS-Server-Zertifikat vom Typ OV, EV oder QWACs
	Siegelzertifikat (zunächst optional)	fortgeschrittenes elektronisches Siegel gemäß eIDAS Abschnitt 5

Tabelle 2 – Übersicht Anforderungen Zertifikate Data Provider

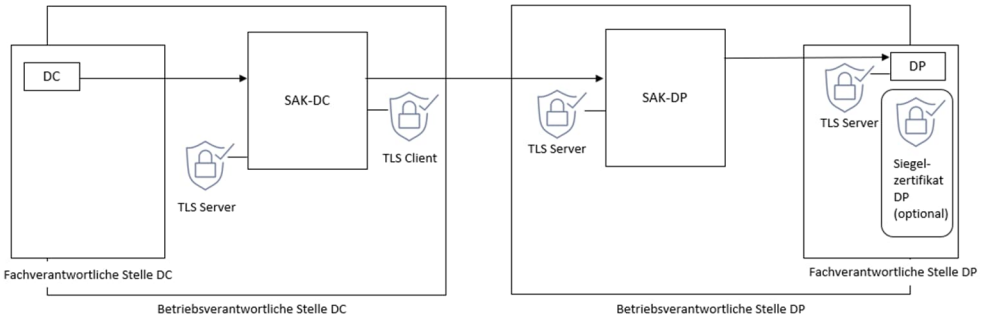

Abbildung 3 – Übersicht Komponenten und Zertifikate zur Beschaffung durch DC/DP in der NOOTS Produktivumgebung

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.

3.1. Zertifikate für die Kommunikation mit dem NOOTS

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

NOOTS Referenzumgebung
Die TLS-Server-Zertifikate des Registers und des SAK-DP müssen geeignete TLS-Zertifikate zur Gewährleistung der Transportverschlüsselung sein. Die Entscheidung über den Zertifikatstyp, die Beschaffung und die Installation obliegen den Betriebsverantwortlichen. Das TLS-Server-Zertifikat des Registers ist in der ersten Iteration des NOOTS für die NOOTS Referenzumgebung optional.

NOOTS Testumgebung
Die TLS-Server-Zertifikate des Registers und des SAK-DP müssen geeignete TLS-Zertifikate zur Gewährleistung der Transportverschlüsselung sein. Die Entscheidung über den Zertifikatstyp, die Beschaffung und die Installation obliegt den Betriebsverantwortlichen.

Bei dem Siegelzertifikat muss es sich um ein für „Siegelung“ geeignetes Zertifikat handeln. Die Entscheidung über den Zertifikatstyp, die Beschaffung und die Installation obliegen den Betriebsverantwortlichen. Das Siegelzertifikat ist in der ersten Iteration des NOOTS optional, da die Siegelung von Nachweisdaten optional ist.

NOOTS Produktivumgebung

Bei dem TLS-Server-Zertifikat des Registers muss es sich um ein geeignetes TLS-Zertifikat zur Gewährleistung der Transportverschlüsselung handeln. Die Entscheidung über den Zertifikatstyp, die Beschaffung und die Installation obliegt den Betriebsverantwortlichen.

Das TLS-Server-Zertifikat des SAK-DP muss mindestens dem Typ „Organisation Validation“ (OV) entsprechen. Weiterhin können auch Zertifikate des Typs „Extended Validation“ (EV) oder „Qualifiziertes Webseitenzertifikat“ (Qualified Website Authentication Certificates, QWACs) als Spezialfall der Extended Validation-Zertifikate genutzt werden. Weitere Informationen zum Thema QWACs finden Sie bei Bedarf hier.

Für die Siegelung von Nachweisdaten wird mindestens ein fortgeschrittenes elektronisches Siegel auf Basis eines qualifizierten Zertifikats gemäß eIDAS Abschnitt 5 „Elektronische Siegel“ benötigt (Siegelzertifikat). Die notwendigen Siegelzertifikate können von allen qualifizierten Vertrauensdiensteanbietern wie z.B. D-Trust bezogen werden. Eine aktuelle Liste ist dem „Trusted List Browser“ der Europäischen Kommission zu entnehmen. Das Siegelzertifikat ist in der ersten Iteration des NOOTS optional, da die Siegelung von Nachweisdaten optional ist.

4. Abkürzungsverzeichnis

BVA	Bundesverwaltungsamt
NOOTS	National-Once-Only-Technical-System
DC	Data Consumer
DP	Data Provider
IAM-B	Identity und Access Management für Behörden
RDN	Registerdatennavigation
SAK	Sicherer Anschlussknoten
SAK-DC	Sicherer Anschlussknoten für Data Consumer
SAK-DP	Sicherer Anschlussknoten für Data Provider
V-PKI	Public Key Infrastruktur der Verwaltung
DOI-CA	Deutschland Online Infrastruktur Certification Authority
RA	Registration Authority
EV	Extended Validation
QWACs	Qualified Website Authentication Certificates
OV	Organisation Validation

5. Abbildungsverzeichnis