Bundesverwaltungsamt

Referat D III 1: Registermodernisierung; Anschlussunterstützung

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

Version 2.2
11.09.2026

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

Ansprechpartner/-in:

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

Inhaltsverzeichnis

1. Einleitung

Dieses Dokument gibt betrieblich verantwortlichen Stellen eines **Data Consumer (DC)** 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 für die NOOTS-Registrierung und technische NOOTS-Kommunikation 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.

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

Die Rollen und Zuständigkeiten gliedern sich dabei wie folgt:

- Fachlich Verantwortliche sind die für das technische Verfahren verantwortlichen nachweisanfordernden oder -liefernden Stellen.

- Die das technische Verfahren im Auftrag der fachlich Verantwortlichen Betreibenden sind die betrieblich Verantwortlichen. Sie verantworten den technisch korrekten Betrieb des DC/DP 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. Das NOOTS 1.0, dessen Produktivsetzung für den 30.11.2026 geplant ist, wird aus den technischen Komponenten Identity und Access Management für Behörden (IAM-B), Registerdatennavigation (RDN) und Vermittlungsstelle (VS) bestehen sowie den Abruf der Identifikationsnummer (IDNr.-Abruf) über das Identity Management für Personen (IDM-P) beinhalten.

Darüber hinaus werden Sichere Anschlussknoten (SAK) für DC (SAK-DC) und DP (SAK-DP) zur Verfügung gestellt (Abbildung 1). In der

aktuellen Iteration sind nur Onlinedienste als DC vorgesehen. Die Darstellung ist zur Übersichtlichkeit und Verständlichkeit in ihrer Komplexität vereinfacht.

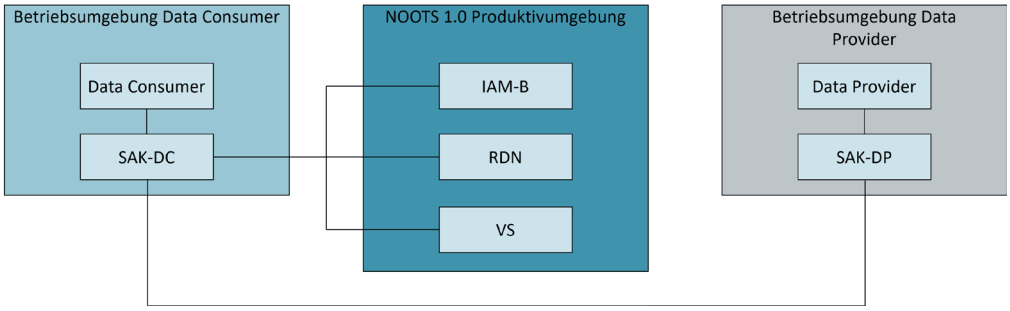

Abbildung 1- Grobübersicht NOOTS 1.0

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

Es gibt drei NOOTS-Umgebungen, an die DC 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 betrieblich Verantwortlichen in Abstimmung mit bzw. im Auftrag der fachlich Verantwortlichen. Für ein Zertifikat ist abweichend vorgesehen, dass die Beschaffung durch die fachlich Verantwortlichen erfolgt.

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

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 DC und DP unterschiedliche Zertifikate; nachfolgend finden Sie einen Überblick für die NOOTS Produktivumgebung:

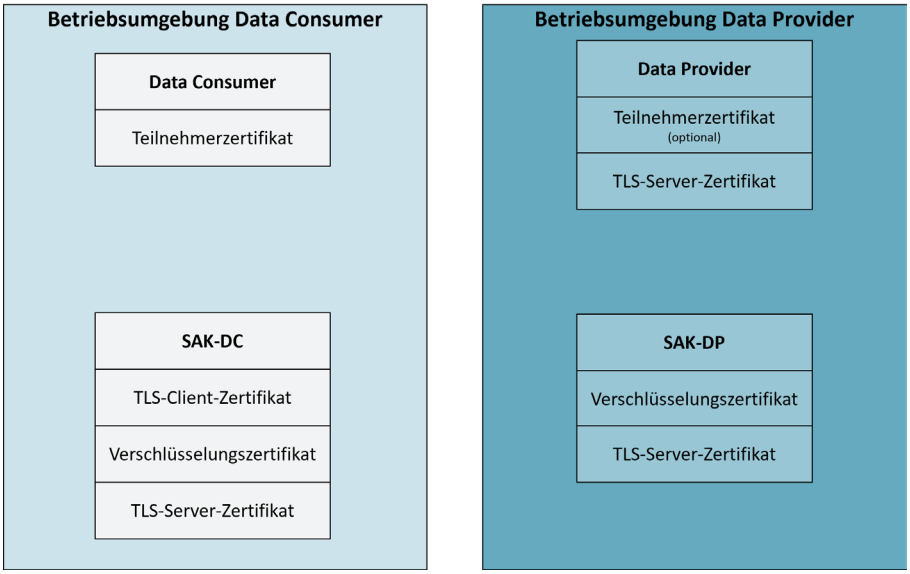

Abbildung 2 - Übersicht Zertifikate NOOTS Produktivumgebung

Für einen **DC** werden für die Kommunikation mit dem NOOTS insgesamt 11 Zertifikate benötigt, von denen jedoch drei für Sie bereitgestellt werden. Somit ist die Beschaffung von acht Zertifikaten zwingend durch Sie erforderlich. Bei dem TLS-Server-Zertifikat für die NOOTS Referenzumgebung handelt es sich um ein zusätzliches optionales Zertifikat, welches nicht zwingend beschafft werden muss. Alle weiteren Zertifikate für die NOOTS Referenzumgebung werden Ihnen zur Verfügung gestellt.

NOOTS Referenzumgebung	**NOOTS Testumgebung**	**NOOTS Produktivumgebung**
Teilnehmerzertifikat des DC (wird bereitgestellt)	Teilnehmer-zertifikat des DC	Teilnehmerzertifikat des DC
TLS-Server-Zertifikat des SAK-DC (optional)	TLS-Server-Zertifikat des SAK-DC	TLS-Server-Zertifikat des SAK-DC
TLS-Client-Zertifikat des SAK-DC (wird bereitgestellt)	TLS-Client-Zertifikat des SAK-DC	TLS-Client-Zertifikat des SAK-DC

Verschlüsselungs-zertifikat des SAK-DC (wird bereitgestellt)	Verschlüsselungs-zertifikat des SAK-DC	Verschlüsselungs-zertifikat des SAK-DC

Tabelle 1 - Übersicht Zertifikate DC

- Mit dem Teilnehmerzertifikat siegelt der DC das Anfragetoken, welches er bei der Initiierung des Nachweisabrufs an den SAK-DC übergibt.

- Das TLS-Server-Zertifikat des SAK-DC dient ausschließlich der Kommunikation zwischen DC und SAK-DC innerhalb der Betriebsumgebung des DC.

- Das TLS-Client-Zertifikat des SAK-DC wird für die Authentisierung des DC 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.

- Das Verschlüsselungszertifikat des SAK-DC ermöglicht zusätzlich zur sicheren mTLS-Verbindung eine Verschlüsselung des vom SAK-DP zum SAK-DC übermittelten Nachweises.

Bei der Registrierung über noots.gov.de müssen Sie für die NOOTS Test- und Produktivumgebung das Teilnehmerzertifikat des DC und das TLS-Client-Zertifikat des SAK-DC im PEM-Format angeben.

Die Beschaffung des Teilnehmerzertifikats des DC ist durch die fachlich Verantwortlichen vorgesehen.

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	Teilnehmerzertifikat des DC	Bereitstellung durch Dataport
	TLS-Server-Zertifikat des SAK-DC (optional)	geeignetes TLS-Zertifikat zur Gewährleistung der Transportverschlüsselung (TLS 1.3)
	TLS-Client-Zertifikat des SAK-DC	Bereitstellung durch Dataport
	Verschlüsselungszertifikat des SAK-DC	Bereitstellung durch Dataport
NOOTS Testumgebung	Teilnehmerzertifikat des DC	Für Siegelung geeignetes Zertifikat (Hash-Algorithmus: SHA256, Schlüsseltyp (Signatur): ECC NIST P-256, Cipher Suite: ecdsa_secp256r1_sha256 (0x0403))
	TLS-Server-Zertifikat des SAK-DC	geeignetes TLS-Zertifikat zur Gewährleistung der Transportverschlüsselung (TLS 1.3)
	TLS-Client-Zertifikat des SAK-DC	gruppenbezogenes Zertifikat (Test) der V-PKI/DOI-CA (CN: GRP: „Name der Einrichtung“:SAK-DC:“Spezifikation des SAK-DC“, Hash-Algorithmus: SHA256, Schlüsseltyp (Signatur): ECC NIST P-256, Cipher Suite:

		ecdsa_secp256r1_sha256 (0x0403), TLS 1.3)
	Verschlüsselungs-zertifikat des SAK-DC	gruppenbezogenes Zertifikat (Test) der V-PKI/DOI-CA (CN: GRP: „Name der Einrichtung“:SAK-DC:“Spezifikation des SAK-DC“, Hash-Algorithmus: SHA256, Schlüsseltyp (Signatur): ECC NIST P-256, Cipher Suite: ecdsa_secp256r1_sha256 (0x0403))
NOOTS Produktivumgebung	Teilnehmerzertifi-kat des DC	Für Siegelung geeignetes Zertifikat (Hash-Algorithmus: SHA256, Schlüsseltyp (Signatur): ECC NIST P-256, Cipher Suite: ecdsa_secp256r1_sha256 (0x0403))
	TLS-Server-Zertifikat des SAK-DC	geeignetes TLS-Zertifikat zur Gewährleistung der Transportverschlüsselung (TLS 1.3)
	TLS-Client-Zertifikat des SAK-DC	gruppenbezogenes Zertifikat der V-PKI/DOI-CA (CN: GRP: „Name der Einrichtung“:SAK-DC:“Spezifikation des SAK-DC“, Hash-Algorithmus: SHA256, Schlüsseltyp (Signatur): ECC NIST P-256, Cipher Suite: ecdsa_secp256r1_sha256 (0x0403), TLS 1.3)
	Verschlüsselungs-zertifikat des SAK-DC	gruppenbezogenes Zertifikat der V-PKI/DOI-CA (CN: GRP: „Name der Einrichtung“:SAK-DC:“Spezifikation des SAK-DC“, Hash-Algorithmus: SHA256, Schlüsseltyp (Signatur): ECC NIST P-256, Cipher Suite:

	ecdsa_secp256r1_sha256 (0x0403))

Tabelle 2 – Übersicht Anforderungen Zertifikate DC

Die nachfolgende Abbildung 3 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.

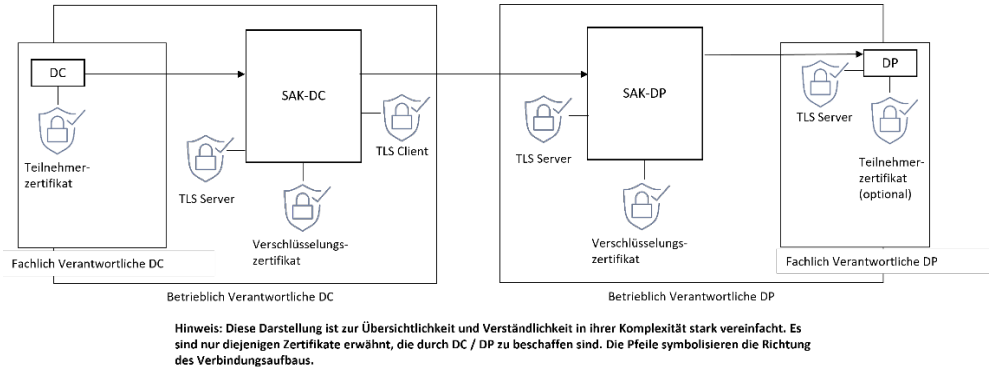

Abbildung 3– Übersicht Komponenten und Zertifikate zur Beschaffung durch DC/DP in der NOOTS Produktivumgebung

3.1. Zertifikate für die Kommunikation mit dem NOOTS

HINWEIS: Generell ist zu beachten, dass für jeden Anwendungsfall ein separates Zertifikat zu beschaffen ist. Eine Wiederverwendung desselben Zertifikats für mehrere Anwendungsfälle ist nicht gestattet. Beispielsweise ist es nicht zulässig, dasselbe TLS-Server-Zertifikat des SAK-DC für die NOOTS Test- und Produktivumgebung zu verwenden. Auch ist zum Beispiel ein TLS-Zertifikat entweder als Server-Zertifikat oder als Client-Zertifikat zu verwenden, eine gleichzeitige Verwendung für beide Zwecke ist unzulässig.

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

NOOTS Referenzumgebung

Das **TLS-Server-Zertifikat des SAK-DC** muss ein geeignetes TLS-Zertifikat zur Gewährleistung der Transportverschlüsselung sein. Es ist ausschließlich die Verwendung von TLS 1.3 zulässig. Die Entscheidung über den Zertifikatstyp, die Beschaffung und die Installation obliegt den betrieblich Verantwortlichen. Dieses Zertifikat ist auf der NOOTS Referenzumgebung nicht verpflichtend. Die Entscheidung über die Verwendung liegt in der Verantwortung des DC.

Das **Teilnehmerzertifikat des DC**, das **TLS-Client-Zertifikat des SAK-DC** und das **Verschlüsselungszertifikat des SAK-DC** werden für die NOOTS Referenzumgebung bereitgestellt.

NOOTS Testumgebung

Bei dem **Teilnehmerzertifikat des DC** muss es sich um ein für Siegelung geeignetes Zertifikat handeln. Die Entscheidung über den Zertifikatstyp, die Beschaffung und die Installation obliegt den betrieblich Verantwortlichen. Es sind jedoch folgende kryptographische Vorgaben einzuhalten:

- Hash-Algorithmus: SHA256
- Schlüsseltyp (Signatur): ECC NIST P-256
- Cipher Suite: `ecdsa_secp256r1_sha256 (0x0403)`

Das **TLS-Server-Zertifikat des SAK-DC** muss ein geeignetes TLS-Zertifikat zur Gewährleistung der Transportverschlüsselung sein. Es ist ausschließlich die Verwendung von TLS 1.3 zulässig. Die Entscheidung über den Zertifikatstyp, die Beschaffung und die Installation obliegt den betrieblich Verantwortlichen.

Das **TLS-Client-Zertifikat des SAK-DC** für die sicheren Verbindungen per mTLS zu den zentralen NOOTS-Komponenten und zum SAK-DP und das **Verschlüsselungszertifikat des SAK-DC** sind als gruppenbezogene Zertifikate der V-PKI/DOI-CA zu beziehen. Die Zertifikate verfügen zwar über die gleichen Eigenschaften, dennoch müssen, wie oben beschrieben, zwei separate Zertifikate erworben bzw. verwendet werden. Für den Anschluss an die NOOTS Testumgebung sind in diesem Fall auch gruppenbezogene Test-Zertifikate der V-PKI/DOI-CA zugelassen.

Bei der Beantragung sind als CN, Hash-Algorithmus und Schlüsseltyp folgende Angaben zu machen bzw. auszuwählen:

- CN: *GRP: „Name der Einrichtung“:SAK-DC:“Spezifikation des SAK-DC“*
- Hash-Algorithmus: SHA256
- Schlüsseltyp (Signatur): ECC NIST P-256

Als Cipher Suite ist `ecdsa_secp256r1_sha256 (0x0403)` festzulegen. Weitere Informationen zur Beschaffung der Zertifikate der V-PKI/DOI-CA finden Sie in der Anleitung: „Vertiefungsleitfaden für die Beschaffung von V-PKI Zertifikaten für Data Consumer und Data Provider für den Anschluss an das NOOTS“.

Für das TLS-Client-Zertifikat des SAK-DC ist ausschließlich die Verwendung von TLS 1.3 zulässig.

NOOTS Produktivumgebung

Bei dem **Teilnehmerzertifikat des DC** muss es sich um ein für Siegelung geeignetes Zertifikat handeln. Die Entscheidung über den Zertifikatstyp, die Beschaffung und die Installation obliegt den betrieblich Verantwortlichen.

Es sind jedoch folgende kryptographische Vorgaben einzuhalten:

- Hash-Algorithmus: SHA256
- Schlüsseltyp (Signatur): ECC NIST P-256
- Cipher Suite: `ecdsa_secp256r1_sha256 (0x0403)`

Das **TLS-Server-Zertifikat** muss ein geeignetes TLS-Zertifikat zur Gewährleistung der Transportverschlüsselung sein. Es ist ausschließlich die Verwendung von TLS 1.3 zulässig. Die Entscheidung über den Zertifikatstyp, die Beschaffung und die Installation obliegt den betrieblich Verantwortlichen.

Das **TLS-Client-Zertifikat** und das **Verschlüsselungszertifikat des SAK-DC** sind für die NOOTS Produktivumgebung als gruppenbezogene Zertifikate der V-PKI/DOI-CA zu beziehen. Die Zertifikate verfügen zwar über die gleichen Eigenschaften, dennoch müssen zwei separate Zertifikate erworben bzw. verwendet werden.

Bei der Beantragung sind als CN, Hash-Algorithmus und Schlüsseltyp folgende Angaben zu machen bzw. auszuwählen:

- CN: *GRP: „Name der Einrichtung":SAK-DC:"Spezifikation des SAK-DC"*
- Hash-Algorithmus: SHA256
- Schlüsseltyp (Signatur): ECC NIST P-256

Als Cipher Suite ist `ecdsa_secp256r1_sha256 (0x0403)` festzulegen. Weitere Informationen zur Beschaffung der Zertifikate der V-PKI/DOI-CA finden Sie in der Anleitung: „Vertiefungsleitfaden für die Beschaffung von V-PKI Zertifikaten für Data Consumer und Data Provider für den Anschluss an das NOOTS".

Für das TLS-Client-Zertifikat des SAK-DC ist ausschließlich die Verwendung von TLS 1.3 zulässig.

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
VS	Vermittlungsstelle
ID-Nr.	Identifikationsnummer
IDM-P	Identity Management für Personen
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
SHA	Secure Hash Algorithm
ECC	Elliptic Curve Cryptography
NIST	National Institute of Standards and Technology

5. Abbildungsverzeichnis