Referat D III 1: Registermodernisierung
Anschlussunterstützung

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

Version 2.4 | 16. Oktober 2026

Inhaltsverzeichnis

Einleitung 3

Zertifikatsbeschaffung: Übersicht über die Zertifikate 4

Anforderungen an die Zertifikate 7

Zertifikate für die Kommunikation mit dem NOOTS 9

NOOTS-Referenzumgebung 9

NOOTS-Testumgebung und NOOTS-Produktivumgebung 10

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

Abbildungsverzeichnis

Abbildung 1 | Übersicht Zertifikate NOOTS-Produktivumgebung....4

Abbildung 2 | Übersicht Komponenten und Zertifikate zur Beschaffung durch DC/DP in der NOOTS-Produktivumgebung....9

Tabellenverzeichnis

Tabelle 1 | Übersicht Zertifikate DP....5

Tabelle 2 | Übersicht Anforderungen Zertifikate DP....8

Einleitung

Dieses Dokument gibt betrieblich und fachlich Verantwortlichen eines **Data Provider (DP)** einen **Überblick** über die bei dem Anschluss an das NOOTS zu erwerbenden **Zertifikate** zur **technischen NOOTS-Kommunikation**.

Es 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 (insbesondere auf „Technischer Leitfaden zum Anschluss von Data Consumern (DP)“) sowie auf die Informationen des Bundesverwaltungsamts und des Bundesministeriums für Digitalisierung und Staatsmodernisierung verwiesen.

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

- zur Anmeldung auf noots.gov.de und Registrierung für die NOOTS-Umgebungen
- für die technische NOOTS-Kommunikation

Die **Zertifikate** zur **Anmeldung** auf **noots.gov.de** und **Registrierung** für die **NOOTS-Umgebungen** werden im Rahmen des **Anschlussprozesses** und gegebenenfalls für eine spätere **Änderung** der im Anschlussprozess **eingegebenen Daten** benötigt. Zur Anmeldung auf noots.gov.de benötigen Sie ein ELSTER-Organisationszertifikat („Mein Unternehmenskonto“) und zur Registrierung für die Test- und Produktivumgebung ein personenbezogenes Zertifikat der V-PKI/DOI CA. Weiterführende Anforderungen an diese Zertifikate sowie deren Beschaffung sind nicht Bestandteil dieses Leitfadens. Informationen hierzu finden Sie im „Leitfaden zur Einrichtung eines ELSTER Benutzerkontos für „Mein Unternehmenskonto““ und im „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** werden von den technischen Systemen genutzt (z.B. DP und SAK-DP) und sind **dauerhaft** bei erfolgtem Anschluss an das NOOTS im Einsatz.

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** (teilweise mehrere Wochen), sodass wir Ihnen empfehlen, den Prozess der Beschaffung frühzeitig (noch in der Phase der technischen Anschlussvorbereitung) anzustoßen.

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 technische Kommunikation mit dem NOOTS benötigen der DC und DP unterschiedliche Zertifikate; nachfolgend finden Sie einen Überblick für die NOOTS-Produktivumgebung:

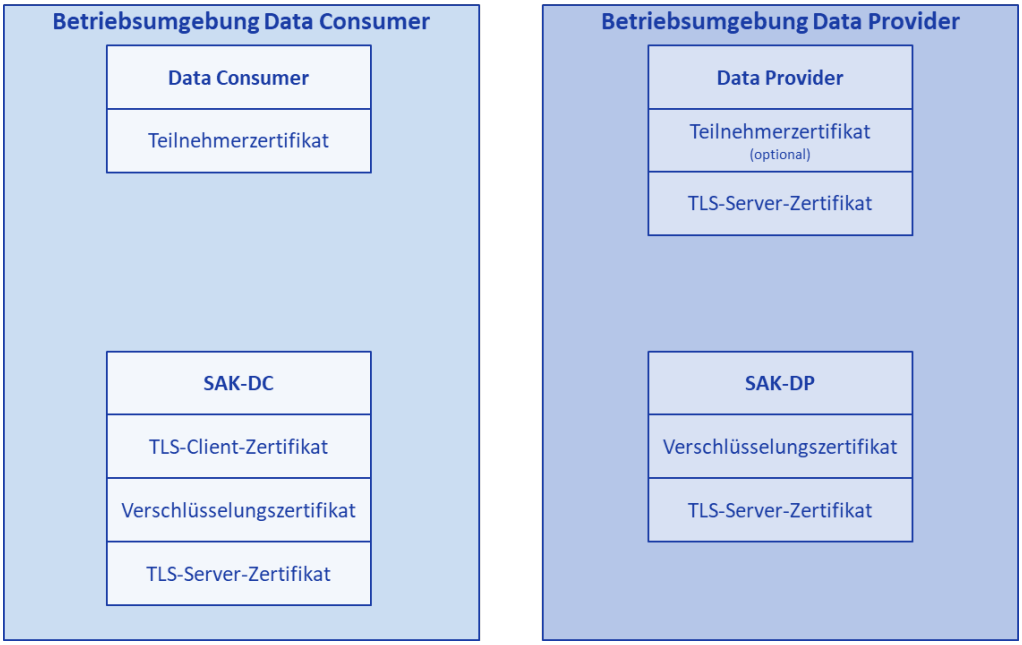


Abbildung 1 | Übersicht Zertifikate NOOTS-Produktivumgebung

Für einen **DP** werden für die Kommunikation mit dem NOOTS insgesamt **acht Zertifikate** verpflichtend benötigt, von denen eines für Sie bereitgestellt wird. Somit ist die Beschaffung von sieben Zertifikaten zwingend durch Sie erforderlich. Bei dem Teilnehmerzertifikat des DP für alle Umgebungen und dem TLS-Server-Zertifikat des DP für die NOOTS-Referenzumgebung handelt es sich um zusätzliche optionale Zertifikate, welche nicht zwingend beschafft werden müssen. Das Verschlüsselungszertifikat des SAK-DP für die NOOTS-Referenzumgebung wird Ihnen zur Verfügung gestellt.

NOOTS-Referenzumgebung	**NOOTS-Testumgebung**	**NOOTS-Produktivumgebung**
Teilnehmerzertifikat des DP (optional)	Teilnehmerzertifikat des DP (optional)	Teilnehmerzertifikat des DP (optional)
TLS-Server-Zertifikat des DP (optional)	TLS-Server-Zertifikat des DP	TLS-Server-Zertifikat des DP
TLS-Server-Zertifikat des SAK-DP	TLS-Server-Zertifikat des SAK-DP	TLS-Server-Zertifikat des SAK-DP
Verschlüsselungszertifikat des SAK-DP (wird bereitgestellt)	Verschlüsselungszertifikat des SAK-DP	Verschlüsselungszertifikat des SAK-DP

Tabelle 1 | Übersicht Zertifikate DP

- Mit dem Teilnehmerzertifikat kann der DP den Nachweis siegeln, bevor er ihn als Bestandteil der Nachweisantwort an den SAK-DP übermittelt.
- Das TLS-Server-Zertifikat des DP dient ausschließlich der Kommunikation zwischen dem DP und dem SAK-DP innerhalb der Betriebsumgebung des DP.
- Das TLS-Server-Zertifikat des SAK-DP ermöglicht eine Transportverschlüsselung bei der Kommunikation mit dem SAK-DC.
- Das Verschlüsselungszertifikat des SAK-DP ermöglicht zusätzlich zur sicheren mTLS-Verbindung eine Verschlüsselung der vom SAK-DC zum SAK-DP übermittelten Nachweisanfrage.

Bei der Registrierung über noots.gov.de müssen Sie für die NOOTS-Test- und Produktivumgebung das Verschlüsselungszertifikat des SAK-DP im PEM-Format angeben.

Die Beschaffung der Zertifikate übernehmen in der Regel die betrieblich Verantwortlichen in Abstimmung mit bzw. im Auftrag der fachlich Verantwortlichen. Für das optionale Teilnehmerzertifikat des DP ist abweichend eine Beschaffung durch die fachlich Verantwortlichen vorgesehen. Es ist auch möglich, die Beschaffung durch die betrieblich Verantwortlichen im Namen der fachlich Verantwortlichen durchzuführen.

Anforderungen an die Zertifikate

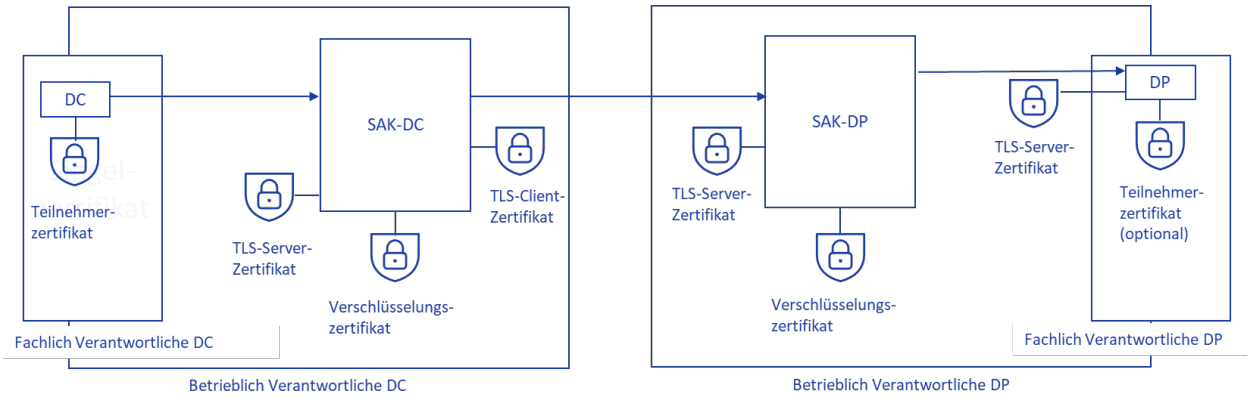
In der nachstehenden Tabelle finden Sie einen Überblick über die an die Zertifikate gestellten Anforderungen, die in den folgenden Abschnitten vertieft werden.

Umgebung	**Zertifikat**	**Anforderung**
NOOTS-Referenzumgebung	Teilnehmerzertifikat des DP (optional)	für Siegelung geeignetes Zertifikat
	TLS-Server-Zertifikat des DP (optional)	geeignetes TLS-Zertifikat zur Gewährleistung der Transportverschlüsselung (TLS 1.3)
	TLS-Server-Zertifikat des SAK-DP	geeignetes TLS-Zertifikat zur Gewährleistung der Transportverschlüsselung (TLS 1.3) (weitere verpflichtende Eigenschaften siehe „Zertifikate für die Kommunikation mit dem NOOTS“)
	Verschlüsselungszertifikat des SAK-DP	*Bereitstellung durch Dataport*
NOOTS-Testumgebung	Teilnehmerzertifikat des DP (optional)	für Siegelung geeignetes Zertifikat
	TLS-Server-Zertifikat des DP	geeignetes TLS-Zertifikat zur Gewährleistung der Transportverschlüsselung (TLS 1.3)
	TLS-Server-Zertifikat des SAK-DP	Vorgabe der TR03190 (DP.13) muss eingehalten werden, Hash-Algorithmus: SHA256, Schlüsseltyp (Signatur): ECC NIST P-256, Cipher Suite:

		ecdsa_secp256r1_sha256 (0x0403), TLS 1.3
	Verschlüsselungszertifikat des SAK-DP	für Verschlüsselung geeignetes Zertifikat (Hash-Algorithmus: SHA256, Schlüsseltyp (Signatur): ECC NIST P-256, Cipher Suite: ecdsa_secp256r1_sha256 (0x0403))
NOOTS-Produktivumgebung	Teilnehmerzertifikat des DP (optional)	für Siegelung geeignetes Zertifikat
	TLS-Server-Zertifikat des DP	geeignetes TLS-Zertifikat zur Gewährleistung der Transportverschlüsselung (TLS 1.3)
	TLS-Server-Zertifikat des SAK-DP	Vorgabe der TR03190 (DP.13) muss eingehalten werden, Hash-Algorithmus: SHA256, Schlüsseltyp (Signatur): ECC NIST P-256, Cipher Suite: ecdsa_secp256r1_sha256 (0x0403), TLS 1.3
	Verschlüsselungszertifikat des SAK-DP	für Verschlüsselung geeignetes Zertifikat (Hash-Algorithmus: SHA256, Schlüsseltyp (Signatur): ECC NIST P-256, Cipher Suite: ecdsa_secp256r1_sha256 (0x0403))

Tabelle 2 | Übersicht Anforderungen Zertifikate DP

Die nachfolgende Abbildung 2 stellt die Kommunikation zwischen DC und DP beispielhaft für die NOOTS-Produktivumgebung dar.



Hinweis: Diese Darstellung ist zur Übersichtlichkeit und Verständlichkeit in ihrer Komplexität stark vereinfacht. Es sind nur diejenigen Zertifikate erwähnt, die durch DC / DP zu beschaffen sind. Die Pfeile symbolisieren die Richtung des Verbindungsaufbaus.

Abbildung 2 | Übersicht Komponenten und Zertifikate zur Beschaffung durch DC/DP in der NOOTS-Produktivumgebung

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-DP 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-Umgebungen (NOOTS-Referenzumgebung, NOOTS-Testumgebung, NOOTS-Produktivumgebung) werden für die Zertifikate des DP in Teilen verschiedene Eigenschaften vorausgesetzt.

NOOTS-Referenzumgebung

Bei dem **Teilnehmerzertifikat des DP** muss es sich um ein für Siegelung geeignetes Zertifikat handeln. Dieses Zertifikat ist auf der NOOTS-Referenzumgebung nicht verpflichtend. Die Entscheidung über die Verwendung liegt in der Verantwortung des DP.

Das **TLS-Server-Zertifikat des DP** 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-Server-Zertifikat des DP ist für die NOOTS-Referenzumgebung optional.

Bei dem **TLS-Server-Zertifikat des SAK-DP** handelt es sich auch um ein geeignetes TLS-Zertifikat zur Gewährleistung der Transportverschlüsselung. Es ist ausschließlich die Verwendung von TLS 1.3 zulässig. Darüber hinaus muss es folgende Anforderungen erfüllen:

- Die Zertifikatskette muss bis zu einer öffentlichen und vertrauenswürdigen Root-Certification-Authority (Root-CA) zurückverfolgt werden.
- Das Zertifikat muss für TLS-Client-Authentifizierung geeignet sein (insbesondere EKU/KeyUsage, sofern vorhanden).
- Schlüssel- und Signaturalgorithmen dürfen nicht durch die Java-Sicherheitsrichtlinien gesperrt sein.

Das **Verschlüsselungszertifikat des SAK-DP** wird für die NOOTS Referenzumgebung bereitgestellt.

NOOTS-Testumgebung und NOOTS-Produktivumgebung

Bei dem **Teilnehmerzertifikat des DP** muss es sich um ein für Siegelung geeignetes Zertifikat handeln. Dieses Zertifikat ist auf der NOOTS-Testumgebung und NOOTS-Produktivumgebung optional. Die Entscheidung über die Verwendung liegt in der Verantwortung des DP.

Das **TLS-Server-Zertifikat des DP** 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.

Bei dem **TLS-Server-Zertifikat des SAK-DP** muss die Vorgabe der TR03190 (DP.13) eingehalten werden: Das Zertifikat muss der V-PKI entstammen, oder von einer öffentlichen Certificate Authority bezogen werden, die zum einen mindestens den CA/B-Forum Basisanforderungen in der aktuell gültigen Fassung genügt und zusätzlich Kryptoverfahren und Schlüssellängen verwendet, die der BSI TR-02102-2 genügen.

Es ist ausschließlich die Verwendung von TLS 1.3 zulässig. Darüber hinaus sind folgende kryptographische Vorgaben einzuhalten:

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

Bei dem **Verschlüsselungszertifikat des SAK-DP** muss es sich um ein für Verschlüsselung der Nachweisanfrage 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)