Referat D III 1: Registermodernisierung;
Anschlussunterstützung

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

Version 2.3 | 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 ..... 10

NOOTS-Testumgebung ..... 10

NOOTS-Produktivumgebung ..... 11

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 DC....5

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

# Einleitung

Dieses Dokument gibt betrieblich und fachlich Verantwortlichen eines **Data Consumer (DC)** 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 (DC)“) 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. DC und SAK-DC) 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:

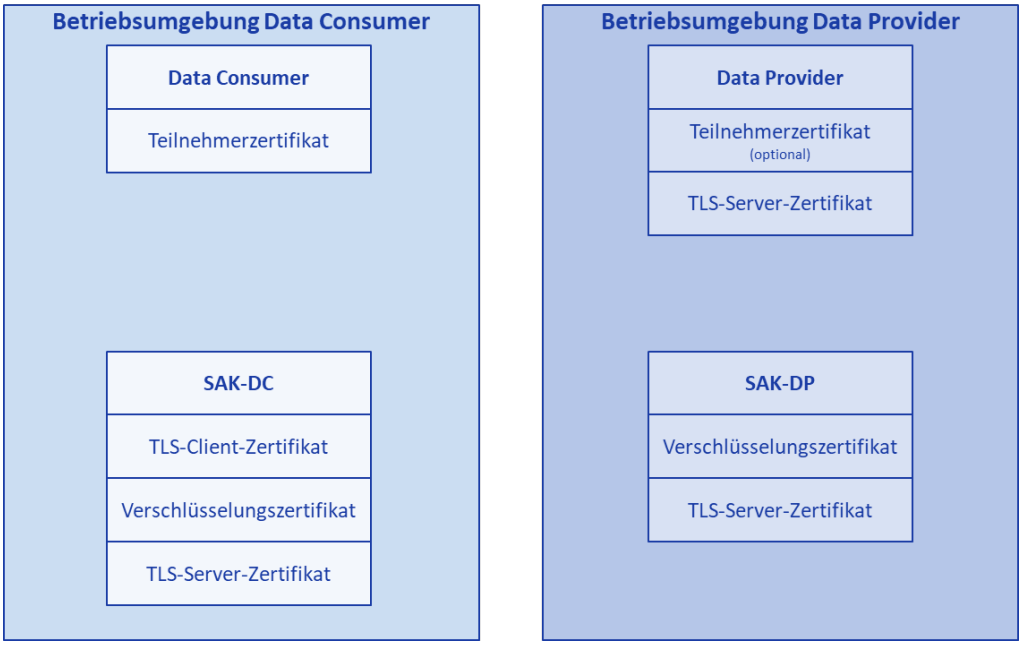



*Abbildung 1 | Übersicht Zertifikate NOOTS-Produktivumgebung*

Für einen **DC** werden für die Kommunikation mit dem NOOTS insgesamt **11 Zertifikate** verpflichtend 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)* | Teilnehmerzertifikat 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 |
| *Verschlüsselungszertifikat des SAK-DC (wird bereitgestellt)* | Verschlüsselungszertifikat des SAK-DC | Verschlüsselungszertifikat 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 Identity und Access Management für Behörden (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 der Zertifikate übernehmen in der Regel die betrieblich Verantwortlichen in Abstimmung mit bzw. im Auftrag der fachlich Verantwortlichen. Für das Teilnehmerzertifikat des DC 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 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) |

| | | |
|---|---|---|
| | Verschlüsselungszertifikat 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 | 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 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) |
| | Verschlüsselungszertifikat 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 2 stellt die Kommunikation zwischen DC und DP beispielhaft für die NOOTS-Produktivumgebung dar.

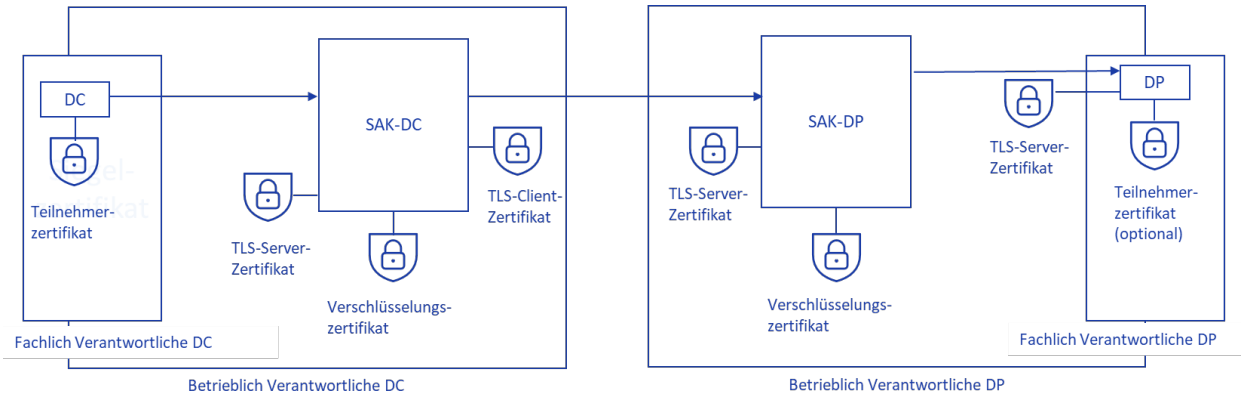



*Abbildung 2 | Übersicht Komponenten und Zertifikate zur Beschaffung durch DC/DP in der NOOTS-Produktivumgebung*

# 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-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-Testumgebung und NOOTS-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 und die Beschaffung obliegt den fachlich Verantwortlichen. Diese Aufgaben können alternativ auch von den betrieblich Verantwortlichen im Namen der fachlich Verantwortlichen übernommen werden. Es sind 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 und die Beschaffung obliegt den fachlich Verantwortlichen. Diese Aufgaben können alternativ auch von den betrieblich Verantwortlichen im Namen der fachlich Verantwortlichen übernommen werden.

Es sind 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.