Bundesverwaltungsamt

Finanziert von der Europäischen Union
NextGenerationEU

Integrationsanleitung
Data Provider / Data Consumer
NOOTS Referenzumgebung

Bundesverwaltungsamt, SEITENBAU GmbH

Version 1.4.1

Inhaltsverzeichnis

1 Änderungshistorie

Version	Änderungen
1.4.1	- Anpassung des Download-Hinweises - Anpassung der weiterführenden Informationen
1.4	- Anpassung der Kontaktdaten des Bundesverwaltungsamtes und des Technischen Supports - Entfernen der Registrierungsinformationen für SAK-DC & SAK-DP - Entfernen der Anleitung für das Hinterlegen eines benutzerdefinierten Testnachweises für SAK-DC - Entfernen der IDNr-Schnittstellenbeschreibung
1.3	- Anpassung des öffentlichen Downloadlinks in Kapitel 7 - Kapitel 4.3 “Zertifikate, Keystores und Truststores” hinzugefügt - Registrierungsdaten für Data Provider angepasst (IP-Adresse wieder eingefügt, Verbindungsparameter Beschreibung angepasst) - Registrierungsdaten für Data Consumer angepasst (Hinweis bei IP-Adresse ergänzt, “Verwendung SAK-DC für DC”-Beschreibung angepasst) - Designanpassungen an Dokumenten-Header und -Footer, sowie an der Darstellung von Tabellen - Anpassung der Kontaktdaten des Bundesverwaltungsamtes
1.2	- Änderungshistorie für dieses Dokument hinzugefügt - Hinzufügen der Kapitel “Technische Anbindungstests für die installierte Umgebung” für Data Provider und Data-Consumer - Hinzufügen des Kapitels “Zertifikat zur Token Verifizierung” - Registrierungsdaten für Data Provider angepasst (IP-Adresse entfernt, Verbindungsparameter Beschreibung angepasst) - Registrierungsdaten für Data Consumer angepasst (Verwaltungsbereich, Behördenfunktion hinzugefügt) - Hinweis beim DP angepasst (nur Zugangs- und Verbindungsdaten) - “NOOTS-Referenzumgebung” angepasst in “NOOTS Referenzumgebung” - Aktualisierung der Schnittstellenbeschreibungen des SAK-DC und SAK-DP auf Version 2.0.0
1.1	- XNachweis Version geändert von 1.2 auf 1.4 - Update des Links zum Download der .jar Dateien für die Installation der SAKs - Bilder (Komponentenansicht und Abläufe) hinzugefügt - Konfigurationsangaben in der Anleitung entfernt und Beispielkonfigurationen bereitgestellt - Generierte values.yaml dokumentiert
1.0	- Initiale Version dieses Dokuments

2 Über dieses Dokument

Dieses Dokument ist eine Integrationsanleitung zur Anbindung eines Data Consumers oder eines Data Providers an die NOOTS Referenzumgebung.

> **Hinweis:** Die Inhalte dieses Dokuments sind **nicht** für die Anbindung an andere NOOTS-Umgebungen geeignet!

3 Überblick über die NOOTS Referenzumgebung

Die NOOTS Referenzumgebung stellt die zentralen NOOTS-Komponenten Identity Access Management für Behörden (IAM-B), Registerdatennavigation (RDN), Identity Management für Personen (IDM-P) und Vermittlungsstelle (VS) als simulierte Komponenten (Mocks) mit einer Basisfunktionalität bereit, die für den exemplarischen Nachweisabruf ausreichend ist. Zusätzlich werden auch Sichere Anschlussknoten (SAK) für Data Consumer (DC) und Data Provider (DP) in der NOOTS Referenzumgebung zur Verfügung gestellt, die einen Nachweisabruf testweise initiieren oder beantworten können, ohne ein externes Testsystem eines Data Consumers oder Data Providers notwendig zu machen. In der unten stehenden Grafik sind die Komponenten, die in der NOOTS Referenzumgebung zur Verfügung stehen, blau gefärbt und die Komponenten, bzw. Systeme, die von anbindungswilligen NOOTS-Teilnehmern betrieben werden, sind orange markiert.

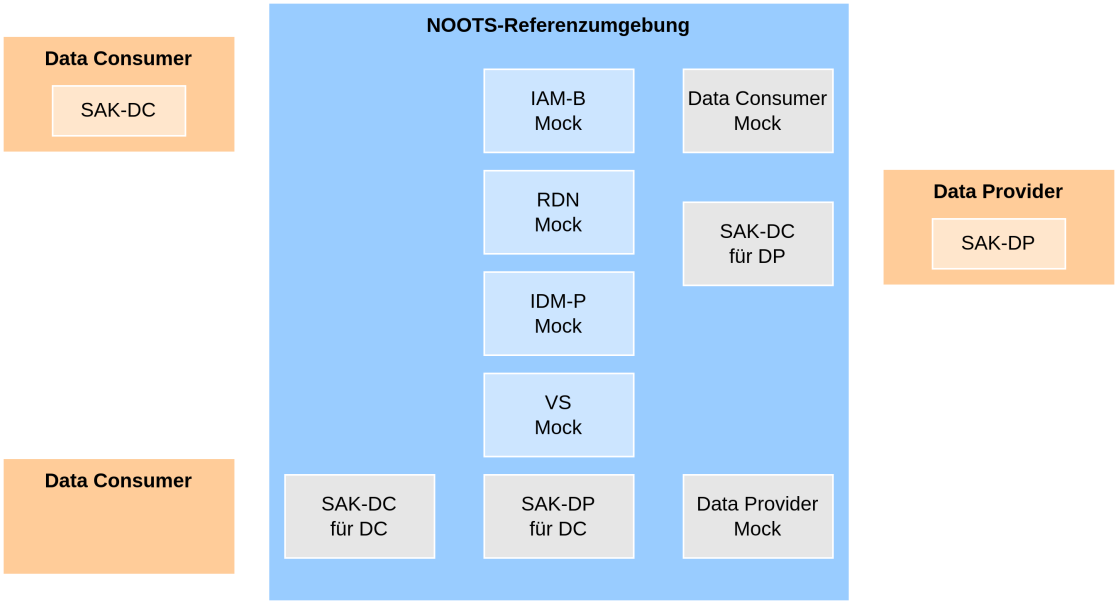

Abbildung 1: NOOTS Referenzumgebung

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.

> **Hinweis:** Im produktiven NOOTS werden SAK-DC und SAK-DP **nicht** zentral betrieben, sondern werden ausschließlich bei den jeweiligen Data Consumern und Data Providern betrieben. Die Bereitstellung solcher SAK-DC und SAK-DP ist ein Service für anbindungswillige NOOTS-Teilnehmer, um unabhängige Tests zu ermöglichen oder den Integrationsaufwand zu minimieren.

4 Integration gegen die NOOTS Referenzumgebung

Hinweis: Vorbedingung für die Anbindung an die NOOTS Referenzumgebung ist die Erstkontaktaufnahme mit dem BVA (siehe “Kontaktinformationen”).

Data Consumer und Data Provider können sich gegen die NOOTS Referenzumgebung anbinden, um den NOOTS-Readiness-Check durchzuführen. In der folgenden Grafik sind die notwendigen Schritte grob skizziert.

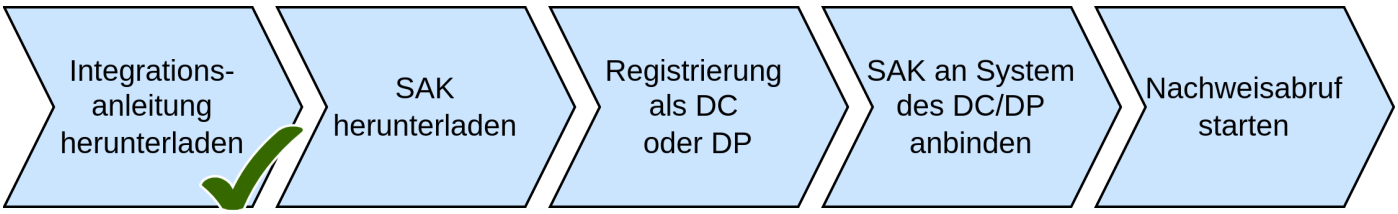

Abbildung 2: Prozessschritte zur Anbindung an die NOOTS Referenzumgebung

Voraussetzung für die Anbindung an die NOOTS Referenzumgebung ist die vorliegende Integrationsanleitung, da in diesem Dokument die wesentlichen Informationen zur Anbindung zusammengefasst dargestellt sind. In einem zweiten Schritt laden Sie den von NOOTS bereitgestellten Sicheren Anschlussknoten herunter (der Download-Link ist hier zu finden). Nachdem Sie die notwendigen Informationen für die Registrierung an den Support (siehe “Kontaktinformationen”) gemeldet haben, richtet das NOOTS-Team die NOOTS Referenzumgebung so ein, dass Sie als Data Consumer oder Data Provider bekannt sind. Zusätzlich werden optional die data-consumer-spezifischen Nachweise bereitgestellt. Währenddessen können Sie den SAK in ihr System einbinden, sodass eine Kommunikation mit dem NOOTS möglich wird. Nachdem die Konfiguration der NOOTS Referenzumgebung und die Einbindung des SAK in Ihr System abgeschlossen ist, können Sie einen Nachweisabruf initiieren und die Integration mit dem NOOTS testen. Können Sie als Data Consumer einen Nachweisabruf erfolgreich durchführen und den gewünschten Nachweis empfangen, haben Sie den Readiness-Check erfolgreich absolviert. Als Data Provider war der Readiness-Check erfolgreich, falls Sie einen Nachweisabruf mit einem passenden generierten Nachweis beantwortet haben.

In den folgenden Abschnitten werden diese Schritte zur Anbindung an die NOOTS Referenzumgebung im Detail aus Sicht der Data Consumer bzw. Data Provider beschrieben.

4.1 Integration als Data Consumer

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 entweder ein Nachweis abgerufen werden, der einem vordefiniertem, generischem Nachweisangebot entspricht, oder es 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.

4.1.1 Registrierung

Um als Data Consumer in der NOOTS Referenzumgebung Nachweise abrufen zu können, muss der Data Consumer in der NOOTS Referenzumgebung registriert werden. Die Registrierung erfolg über NOVA. Das Support-Team richtet anhand der angegebenen Informationen den Data Consumer in der NOOTS Referenzumgebung ein, sodass der Data Consumer im IAM-B bekannt ist, die Vermittlungsstelle die Abrufberechtigungen

des Data Consumers kennt, in der RDN die passenden Verbindungsparameter sowie Nachweisangebot hinterlegt sind und ein passender Mock eines Data Providers die Nachweisabfragen beantworten kann.

4.1.2 Installation

4.1.2.1 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 im Downloadbereich (siehe “Downloadbereich”) zur Verfügung gestellt.

Die Anbindung an die NOOTS Referenzumgebung ist damit wie folgt:

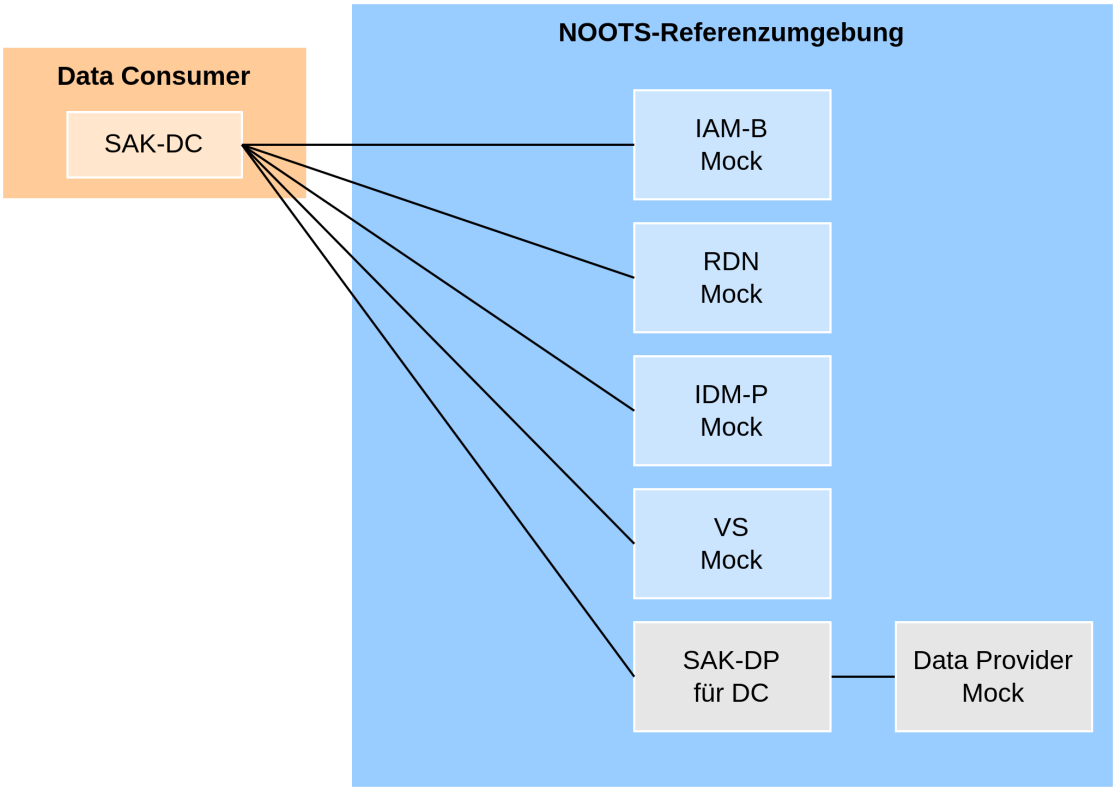

Abbildung 3: Data Consumer mit integriertem SAK-DC

Um den Sicheren 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.

Hinweis: Passwörter, Zugangsdaten und Zertifikat-Truststores, welche über die NOOTS Referenzumgebung ausgegeben werden, erhalten Sie auf Anfrage vom Support (siehe “Kontaktinformationen”).

4.1.2.2 Installation des Sicheren 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.

4.1.2.3 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 den 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.

4.1.3 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.

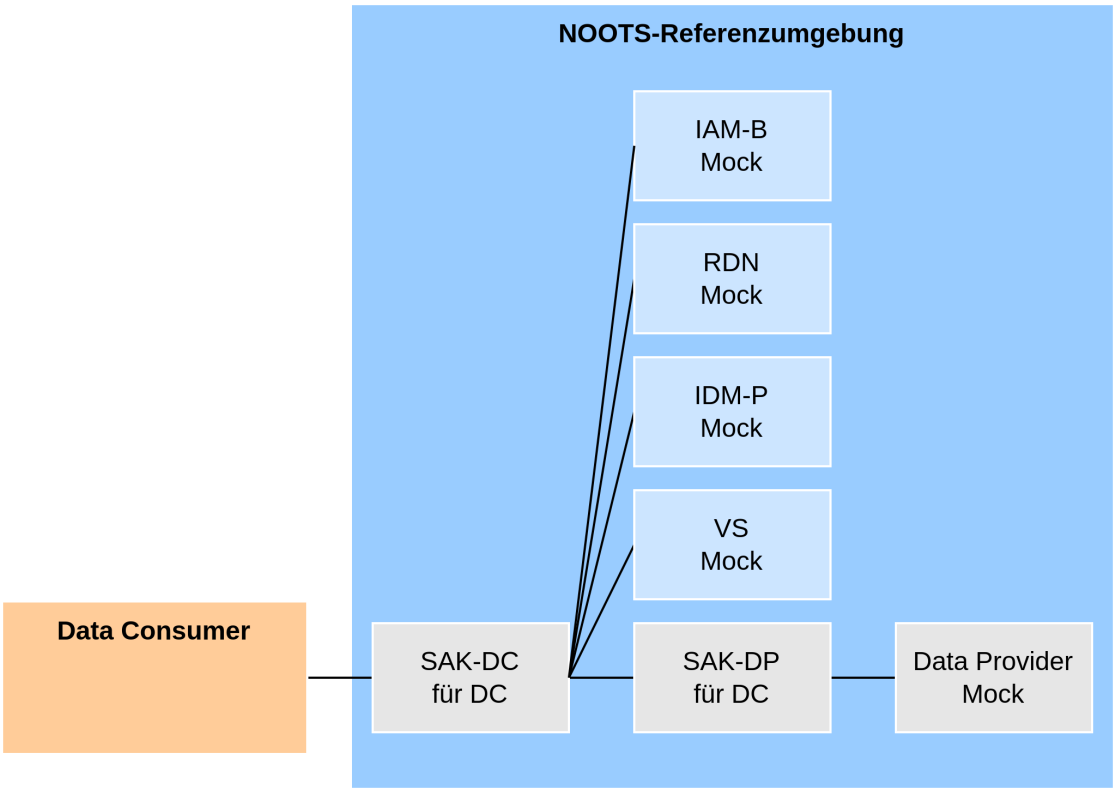

Abbildung 4: Data Consumer ohne integriertem SAK-DC

Diese Art der Betriebsmethode dient lediglich zur Entwicklung gegen die Schnittstellen des SAK-DC und ist nicht zu Produktionszwecken 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!

4.1.4 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.

4.1.5 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 ein 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": "5926157e-dd70-4abc-b6f2-e2e6e31bbc1f",
    "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": "U2FtcGxlIHhuLW5vb3RzOkRFLkV2aWRlbmNlUmVxdWVzdC4wMTAx"
    }
}
```

4.2 Integration als Data Provider

Durch die Anbindung an die NOOTS Referenzumgebung kann ein Data Provider feststellen, ob das eigene System NOOTS-ready ist, d.h. Sie als Data Provider erhalten Nachweiabrufe, auf die Sie mit einem neu erstellten Nachweis antworten.

4.2.1 Registrierung

Um als Data Provider über die NOOTS Referenzumgebung Nachweise bereitstellen zu können, muss der Data Provider in der NOOTS Referenzumgebung registriert werden. Die Registrierung erfolg über NOVA. Das Support-Team richtet anhand der angegebenen Informationen den Data Provider in der NOOTS Referenzumgebung ein, sodass in der RDN die passenden Verbindungsparameter sowie Nachweisangebot hinterlegt sind und ein passender "SAK-DP für DP" eines Data Providers die Nachweisabfragen beantworten kann.

4.2.2 Installation

4.2.2.1 Installation des Sicheren Anschlussknotens als .jar-File

Der Sichere Anschlussknoten für Data Provider muss als eigenständig lauffähige Anwendung mit Zugriff auf das Internet installiert werden. Die aktuelle Version wird als *.jar*-Datei im Downloadbereich (siehe “Download-bereich”) zur Verfügung gestellt.

Die Anbindung an die NOOTS Referenzumgebung ist damit wie folgt:

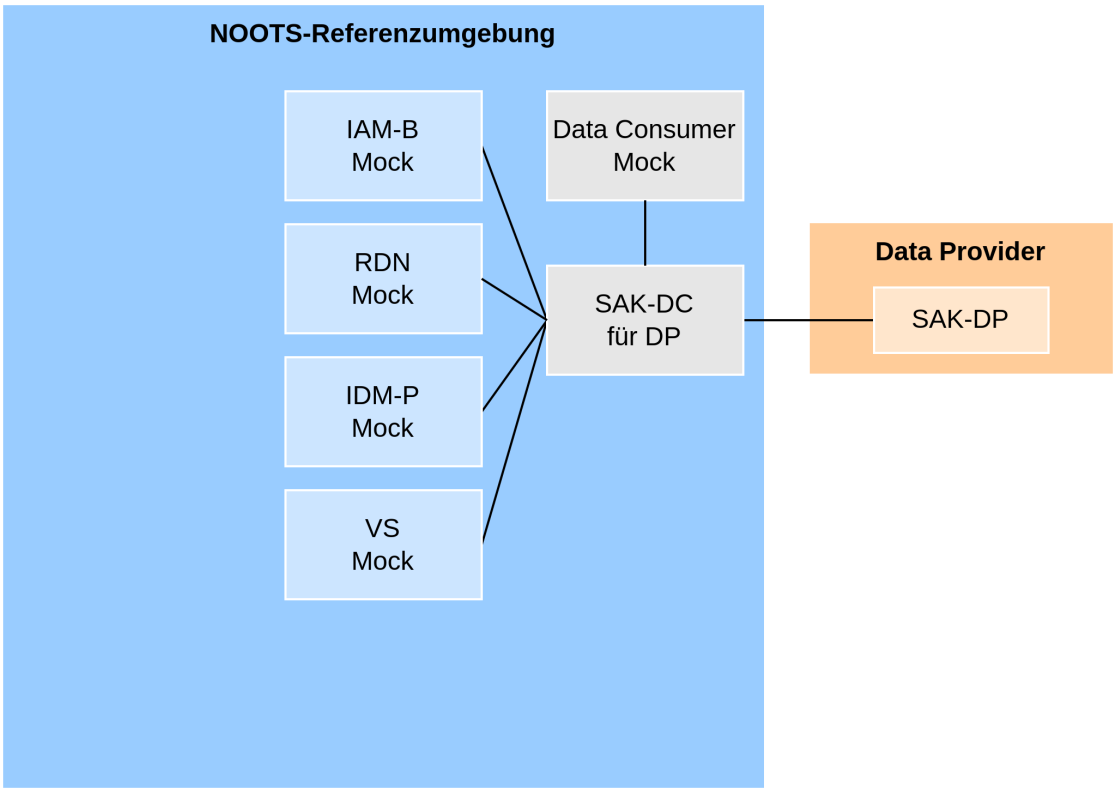

Abbildung 5: Data Provider mit integriertem SAK-DP

Um den Sicheren Anschlussknoten erfolgreich installieren zu können, werden folgenden 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 oder argument-File anzugeben.

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

Hinweis: Zugangs- und Verbindungsdaten, welche über die NOOTS Referenzumgebung ausgegeben werden, erhalten Sie auf Anfrage vom Support (siehe “Kontaktinformationen”).

4.2.2.2 Installation des Sicheren Anschlussknotens mit HELM

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.

4.2.3 Vorgehen für das Testen der Anbindung / Bereitstellung von Nachweisen

Wenn Sie sich als Data Provider an die NOOTS Referenzumgebung anbinden, wird für Sie eine Test-Instanz eines Sicheren Anschlussknotens für Data Consumer (SAK-DC) bereitgestellt (siehe Grafik oben).

Mit Hilfe dieses SAK-DC können Sie Nachweisabrufe, die Ihr System als Data Provider abfragen starten. Die Schritte, welche für den Abruf eines Nachweises notwendig sind, können Sie dem Abschnitt "*Durchlauf eines Nachrichtenabrufs*" entnehmen. Die entsprechende Testinstanz kann nach IP-Freischaltung aufgerufen werden.

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

> **Hinweis:** Es dürfen zu keinem Zeitpunkt Echtdaten für Anfragen oder Nachweisdaten der NOOTS Referenzumgebung verwendet werden!

4.2.4 Grundfunktionstests zur Validierung der technischen und fachlichen Funktionen nach einer lokalen Installation

Nach einer lokalen Installation und Anbindung eines Sicheren Anschlussknotens für Data Provider ist es sinnvoll, diese zu testen. Es empfiehlt sich nach Aktualisierungen, Konfigurationsänderungen oder einer Neuinstallation einen Smoke-Test durchzuführen. Damit dies schnell und möglichst ohne großen Aufwand erfolgen kann, stehen hierzu im "Downloadbereich" mehrere Bash-Skripts und HTTP-Files zur Verfügung. Diese Dateien führen Requests gegen den bereitgestellten SAK-DC sowie den lokalen SAK-DP aus.

Im Folgenden wird für die mitgelieferten Dateien jeweils der Zweck und die für die Zweckerfüllung benötigten Requests erläutert:

- **erreichbarkeitstest.sh**:
  - **Beschreibung:** Dieses Skript testet die allgemeine Erreichbarkeit des lokal installierten SAK-DPs. Dazu wird die URL des SAK_DPs als Aufrufparameter mitgegeben.
  - **Requests:** Es wird ein Request auf die '/evidence'-Schnittstelle ausgeführt mittels cURL ausgeführt.
  - **Zweck:** Es soll die Erreichbarkeit getestet werden.
  - **Ergebnis:** Bei erfolgreicher Durchführung bekommen Sie den Text "Der SAk-DP ist erreichbar" zurück. Sollte die lokale Installation nicht erreichbar sein, wird eine Fehlernachricht mit dem aufgetretenem Status-Code ausgegeben.
  - **Beispielhafter Aufruf**: `./erreichbarkeitstest.sh http://localhost:8080`
- **fachlicher_smoketest.http** und **fachlicher_smoketest.sh**:

- **Beschreibung**: Um zu verifizieren, dass der lokal installierte SAK-DP erfolgreich mit dem Data Provider kommunizieren kann, werden ein bereitgestellter SAK-DC und der lokal installierte SAK-DP in einer fachlichen Reihenfolge abgefragt.
- **Requests**: Es werden insgesamt drei Requests ausgeführt, um die fachliche Grundfunktion testen zu können. Dabei müssen drei Requests an den zur Verfügung gestellten SAK-DC gesendet, da dieser fachlich notwendige Informationen bereitstellt. Zusätzlich wird im dritten SAK-DC Request ein fachlich korrekter Request gegen die '/evidence'-Schnittstelle des lokal installierten SAK-DPs ausgeführt, um die Möglichkeit eines Nachweisabrufs zu testen.
- **Zweck:** Mit diesem fachlichen Grundfunktionstest wird überprüft, ob der lokal installierte SAK-DP eine Verbindung zu dem Data Provider aufbauen und Nachweise abrufen kann.
- **Ergebnis:** Bei erfolgreicher Durchführung wird ein HTTP-Status-Code **200** mit entsprechendem Response-Body erwartet. Sollte es zu einem abweichenden Status-Code kommen, kann dies auf eine Unstimmigkeit in der Konfiguration oder Ähnliches hindeuten. Prüfen Sie in diesem Fall zunächst die Anfragedaten in den Requests, sowie Ihre Zertifikate und Passwörter in der *application.properties*- oder HELM-Konfigurationsdatei. Zusätzlich sollten Sie auch Ihre Netzwerkeinstellungen, Proxies und Firewall-Regeln prüfen.

Hinweis: die angegebenen Platzhalter in den Dateien des fachlichen Smoke-Tests unterscheiden sich von den Ihnen zugewiesenen IDs und Verbindungsparametern. Bitte passen Sie die entsprechenden Parameter der Requests an. Dabei handelt es sich um folgende Parameter:

- *SAK_DC_DOMAIN*: Domain Ihrer eingerichteten NOOTS Referenzumgebung. Dieser Parameter wird vom Support übergeben.
- *COMPONENT_ID*: Die Komponenten-ID des zur Verfügung gestellten SAK-DCs.
- *EVIDENCE_TYPE*: Nachweistyp, der abgerufen werden soll.
- *XNACHWEIS_DATA*: eine valide xNachweisnachricht, die von Ihrem Data Provider verabreitet werden kann. Als base64 String encodiert.

4.3 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.

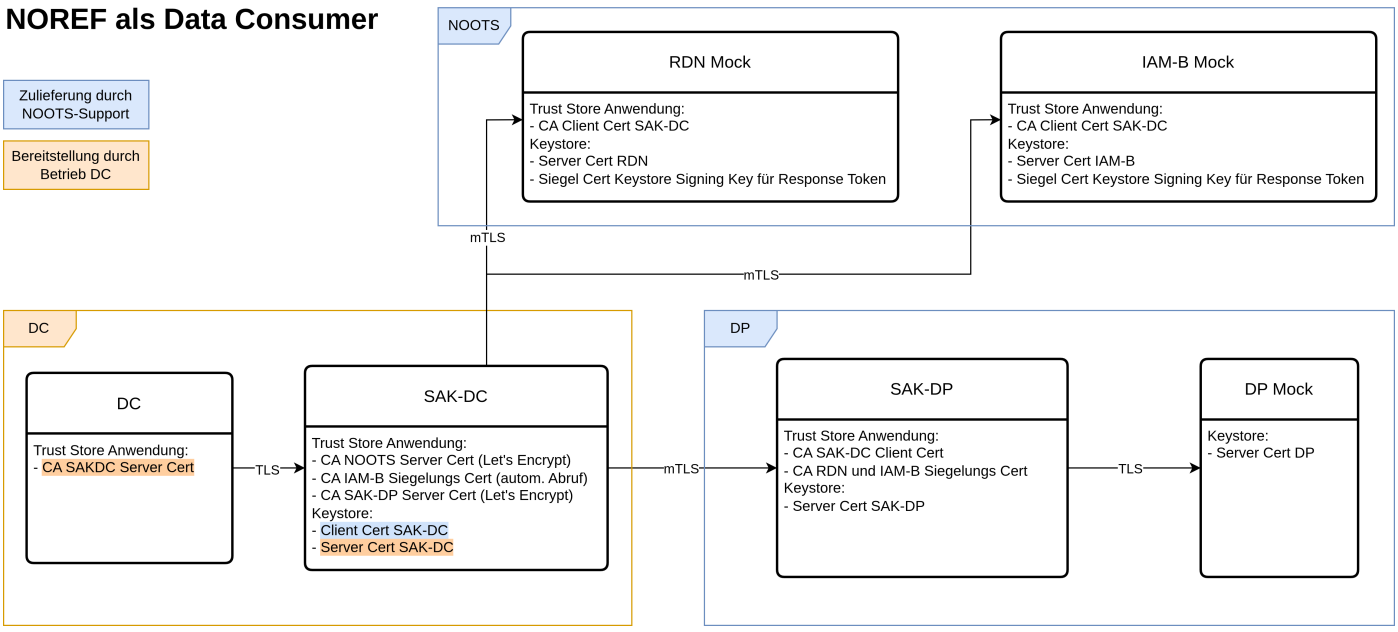

Abbildung 6: Übersicht über die Zertifikate des Data Consumers

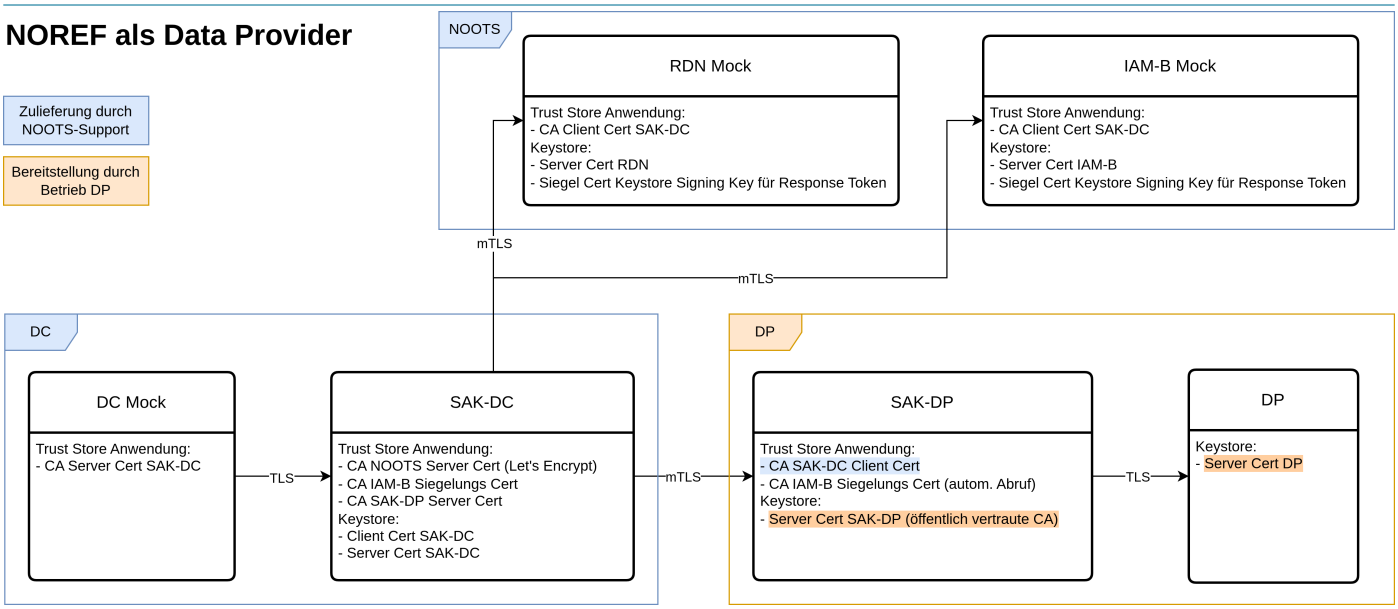

Abbildung 7: Übersicht über die Zertifikate des Data Providers

4.3.1 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 vertrauenswürdiges 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 “Download-bereich”).

5 Übersicht der Schnittstellendefinitionen der NOOTS Referenzumgebung

5.1 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.

5.1.1 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 Stelle laut deren Zertifikat
FV-Anschrift	Anschrift der fachverantwortlichen Stelle laut deren Zertifikat
BV-ID	Vom IAM-Bbei der Registrierung vergebene ID der betriebsverantwortlichen Stelle
BV-Organisation	Organisation der betriebsverantwortlichen Stelle laut deren Zertifikat
BV-Funktionsträger	Funktionsträger der betriebsverantwortlichen Stelle laut deren Zertifikat
BV-Anschrift	Anschrift der betriebsverantwortlichen Stelle laut deren Zertifikat

5.1.1.1 AccessTokenRequest

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

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

5.1.1.2 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)

5.1.1.3 Beispielantwort im Erfolgsfall

Antwort als JSON-Response-Body:

```
{
    "access_token": "mF_9.B5f-4.1JqM",
    "token_type": "Bearer",
    "expires_in": 60
}
```

5.1.1.4 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.

5.1.2 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 zugrifftokenWert`

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

5.1.2.1 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"
    }
}
```

5.1.2.2 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)

5.1.2.3 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"
}
```


5.1.2.4 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.

5.1.3 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 zugrifftokenWert`

Ein Data Consumer kann einen Nachweisabruf aus einem nationalen Data Provider gemäß Nachweisabrufprozess des NOOTS der 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.

5.1.3.1 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": "U2FtcGxlIHhuLW5vb3RzOkRFLkV2aWRlbmNlUmVxdWVzdC4wMTAx",
        "message_type": "DE.EvidenceRequest.0101"
    }
}
```


5.1.3.2 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)

5.1.3.3 Beispielantwort im Erfolgsfall

Antwort als JSON-Response-Body:


```
{
    "mime_type": "application/xml",
    "specification_identifier": "urn:xoev-de:bva:standard:xnachweis_1.4.0",
    "data": "U2FtcGxlIHhuLW5vb3RzOkRFLkV2aWRlbmNlUmVzcG9uc2UuMDEwMg=="
}
```

5.1.3.4 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.

5.2 Endpunkte des Sicheren Anschlussknotens für Data Provider

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.

5.2.1 Bereitstellen eines Nachweises durch den zuständigen Data Provider

`POST /evidence`

Ein Data Provider kann als Antwort auf einen XNachweis-Request eine XNachweis-Response mit Nachweisdaten oder eine XNachweis-ErrorResponse erzeugen. Diese XNachweis-Nachrichten werden mit dem HTTP-Statuscode '200' (OK) an die SAK-API übermittelt.

Diese Operation nutzt den XÖV-Standard XNachweis.

5.2.1.1 GetEvidenceRequest

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


```
{
    "evidence_request": {
        "mime_type": "application/xml",
        "specification_identifier": "urn:xoev-de:bva:standard:xnachweis_1.4.0",
        "message_type": "DE.EvidenceRequest.0101",
        "data": "U2FtcGxlIHhuLW5vb3RzOkRFLkV2aWRlbmNlUmVxdWVzdC4wMTAx"
    }
}
```


5.2.1.2 traceparent

- **Anzugeben in:** HTTP-Request-Header
- **Typ:** TraceParent
- **Pflichtfeld:** ja
- **Beschreibung:** Trace-ID z.B. 4bf92f3577b34da6a3ce929d0e0e4736 zur Verfolgung von Nachrichten über Komponentengrenzen hinweg (siehe W3C Trace Context)

5.2.1.3 x-noots-service-id

- **Anzugeben in:** HTTP-Request-Header
- **Typ:** ServiceId
- **Pflichtfeld:** nein
- **Beschreibung:** Dienstkennung (ServiceID) für den Once-Only-Dienst

5.2.1.4 x-noots-xnachweis-id

- **Anzugeben in:** HTTP-Request-Header
- **Typ:** UUID
- **Pflichtfeld:** nein
- **Beschreibung:** Identifiziert eindeutig die Nachweis-Anfrage

5.2.1.5 Beispielantwort im Erfolgsfall

Antwort als JSON-Response-Body:


```
{
    "mime_type": "application/xml",
    "specification_identifier": "urn:xoev-de:bva:standard:xnachweis_1.4.0",
    "message_type": "DE.EvidenceResponse.0102",
    "data": "U2FtcGxlIHhuLW5vb3RzOkRFLkV2aWRlbmNlUmVzcG9uc2UuMDEwMg=="
}
```


5.2.1.6 Mögliche HTTP-Status-Codes

Die folgenden Fehlerfälle und Status-Codes können nach einem Aufruf der Schnittstelle auftreten und sind nach Schnittstellen-Definition durch den Sicheren Anschlussknoten für Data Provider zurückzugeben, sollten entsprechende Fehler auftreten:

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.

5.3 Endpunkte des Data Providers

5.3.1 Bereitstellen eines Nachweises durch den zuständigen Data Provider

`POST /evidence`

Ein Data Provider kann Nachweise auf Basis einer Nachweis-Anfrage ausstellen. Diese Operation nutzt den XÖV-Standard XNachweis. Konnte der Data Provider keinen Nachweis ausstellen und beantwortet daher die Nachweisabfrage mit einer Fehlermeldung, wird vom SAK-DP eine Fehlermeldung mit dem Code 404 erzeugt, wobei die Original-Fehlerantwort des Data Providers im Element ‘embedded_error’ abgelegt wird.

5.3.1.1 GetEvidenceRequest

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


```
{
    "evidence_request": {
        "mime_type": "application/xml",
        "specification_identifier": "urn:xoev-de:bva:standard:xnachweis_1.4.0",
        "message_type": "DE.EvidenceRequest.0101",
        "data": "U2FtcGxlIHhuLW5vb3RzOkRFLkV2aWRlbmNlUmVxdWVzdC4wMTAx"
    }
}
```


5.3.1.2 traceparent

- **Anzugeben in:** HTTP-Request-Header
- **Typ:** TraceParent
- **Pflichtfeld:** nein
- **Beschreibung:** Trace-ID z.B. 4bf92f3577b34da6a3ce929d0e0e4736 zur Verfolgung von Nachrichten über Komponentengrenzen hinweg (siehe W3C Trace Context)

5.3.1.3 x-noots-service-id

- **Anzugeben in:** HTTP-Request-Header
- **Typ:** ServiceId
- **Pflichtfeld:** nein
- **Beschreibung:** Dienstkennung (ServiceID) für den Once-Only-Dienst

5.3.1.4 x-noots-xnachweis-id

- **Anzugeben in:** HTTP-Request-Header
- **Typ:** UUID
- **Pflichtfeld:** nein
- **Beschreibung:** Identifiziert eindeutig die Nachweis-Anfrage

5.3.1.5 Beispielantwort im Erfolgsfall

Antwort als JSON-Response-Body:


```
{
    "mime_type": "application/xml",
    "specification_identifier": "urn:xoev-de:bva:standard:xnachweis_1.4.0",
    "message_type": "DE.EvidenceResponse.0102",
    "data": "U2FtcGxlIHhuLW5vb3RzOkRFLkV2aWRlbmNlUmVzcG9uc2UuMDEwMg=="
}
```


5.3.1.6 Mögliche HTTP-Status-Codes

Die folgenden Fehlerfälle und Status-Codes können nach einem Aufruf der Schnittstelle auftreten und sind nach Schnittstelle-Definition durch den Data Provider zurückzugeben, sollten entsprechende Fehler auftreten:

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.

6 Kontaktinformationen

Bundesverwaltungsamt
Referat D III 3
Registermodernisierung@bva.bund.de

Technischer Support:
Organisation: Dataport
E-Mail: dataportnootssupport@dataport.de

7 Downloadbereich

Die vorliegende Integrationsanleitung sowie die aktuellen Installationsdateien für die SAKs können in NOVA heruntergeladen werden.

8 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-Platform unter folgender Adresse:

- https://gitlab.opencode.de/noots/public/ad-noots/sak-apis

Ausgewählte Architekturdokumente des NOOTS-System auf OpenCode

- https://gitlab.opencode.de/noots/public/ad-noots/noots-architektur/ad-noots-release

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-Platform des Bundesministeriums des Innern und für Heimat unter folgender Adresse:

- https://bmi.usercontent.opencode.de/noots/Glossar/, öffentlich zugänglich