Bundesverwaltungsamt

FITKO

IT-PLANUNGSRAT

Datenschutzdokumentation

Sicherer Anschlussknoten Data Consumer (SAK-DC) Sicherer Anschlussknoten Data Provider (SAK-DP)

Version 1.0.5
23. Januar 2026

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

Ansprechpartner/-in:

Herr Michael Lipaczewski
Referatsleitung BVA D III 3
Bundesverwaltungsamt
E-Mail: Michael.Lipaczewski@bva.bund.de

Dokumentinformationen

Speicherdatum:	23.01.2026
Version:	1.0.5
Zustand:	☐ in Bearbeitung seit: ☐ vorgelegt am: ☐ abgenommen
Verfasser:	Dataport RX4

Dokumentenhistorie

Datum	Version	Änderungsgrund	Bearbeiter
12.12.2025	1.0.3	Erstellung im CD des BVA	Dataport RX4
05.01.2026	1.0.4	Überarbeitung	Dataport RX4
23.01.2026	1.0.5	Überarbeitung Kap. 2.3, Verweise auf Anlagen Systemdokumentation 2026-01-22 Ereignisse-SAK-DC und -DP	Dataport RX4

Ggf. Verteiler

Empfänger	Gremium	Erhalten am

Inhaltsverzeichnis

1. Ebene 1 SDM – Verfahren

Die in diesem Dokument gelieferten Informationen für das Modul Sicherer Anschlussknoten (SAK) Data Consumer (DC) und SAK Data Provider (DP) bilden die Basis, dass der datenschutzrechtlich Verantwortliche eine eigene datenschutzrechtliche Prüfung und geeignete Konfiguration seines SAK durchführen, sowie die gesetzlich geforderte datenschutzrechtliche Dokumentation erstellen kann. Diese operative Umsetzung kann im Rahmen der Modulbetrachtung nur durch eine Muster-Dokumentation unterstützt werden. Die folgenden Informationen unterstützen den Verantwortlichen bei der Erstellung der Verarbeitungsschritte, des Verzeichnisses der Verarbeitungstätigkeiten und einer ggf. durchzuführenden Datenschutz-Folgenabschätzung.

Mitgeltend zu dieser Dokumentation sind die vorliegenden Systemdokumentationen für den SAK-DC und den SAK-DP. Ebenso gelten die jeweiligen Installationsanleitungen des Softwareherstellers der SAK mit. An den entsprechenden Stellen wird aus diesen Dokumenten zitiert. Des Weiteren umfasst diese Datenschutz-Dokumentation eine Schwellwertanalyse (siehe Anlage 1), die auch Ausführungen zu den SAK-DC und SAK-DP enthält.

Die Informationen auf der Ebene 1 des Standard-Datenschutzmodells (SDM) werden hier jedoch nur generisch mitgeliefert. Eine vollständige und abschließende Erstellung einer Datenschutz-Dokumentation liegt in der gesetzlichen Pflicht des jeweiligen datenschutzrechtlich Verantwortlichen.

1.1. Beschreibung der Datenverarbeitung

Der SAK ist eine technische Komponente zur Anbindung der IT-Systeme der DC (Online-Dienste und Fachverfahren) sowie der DP (z. B. Register) an die übrigen Komponenten der NOOTS-Transportinfrastruktur wie bspw. an die Registerdatennavigation (RDN). Die SAK-Software sowie eine jeweils dazugehörige Konfigurations-Datei (config-Datei) kann eine Behörde nach vorheriger Registrierung über das NOVA-Webportal herunterladen. Mithilfe der jeweiligen config-Datei wird jede SAK-Version automatisch in eine Standardkonfiguration versetzt. Die Verwendung von SAKs ist für einen Anschluss an die NOOTS-Infrastruktur für die Teilnehmer verpflichtend und technisch notwendig.

Mit einem SAK-DC und einem SAK-DP soll der sichere Anschluss an die NOOTS-Transportinfrastruktur sowie der Transport von Nachrichten im Sinne des § 5 Abs. 2 E-Government-Gesetzes (EGovG) im Rahmen der

Beantragung von Verwaltungsleistungen erreicht werden. Die SAKs stellen hierzu sicher, dass die Verbindung zwischen einem DC und einem DP TLS-verschlüsselt wird und diese Verschlüsselung aufrechterhalten bleibt. Eine TLS-Verschlüsselung erfolgt ebenfalls für die Anbindung des SAK an das jeweilige Register resp. Fachverfahren und einen Online-Dienst. Die über einen Online-Dienst im Wege der Beantragung einer Verwaltungsleistung angefragten Daten werden in Form eines XNachweises (siehe Kap. 1.1.3 dieser Dokumentation) übertragen.

Die Verantwortung für die erfolgreiche Installation und den sichereren Betrieb der SAKs liegt bei der betriebsverantwortlichen Stelle des jeweiligen DCs oder DPs, da der SAK auf deren IT-Systemen betrieben wird. Eine Auslagerung der Betriebsverantwortung an einen Dienstleister ist möglich.

1.1.1 Data Provider

Ein DP (Registerbehörde) ist ein NOOTS-Teilnehmer zur Lieferung von Nachweisen aus seinem Register-Datenbestand. Folgende Merkmale gelten für den DP:

- Es ist ein gegenüber dem Bundesverwaltungsamt (BVA) registriertes technisches Verfahren mit der Teilnahmeart "Data Provider".

- Der DP kann pro Registertyp mehrere Nachweistypen für natürliche Personen oder Unternehmen aus seinem fachlichen Aufgabenbereich und auf Basis einer rechtlichen Grundlage (Behördenfunktion) ausstellen.

- Bei dezentralen Registern können mehrere DP pro Registertyp definiert werden.

- Ein DP muss durch ein Zertifikat und eine Komponenten-ID in der Komponente IAM für Behörden eindeutig identifizierbar sein[1].

- Ein DP verfügt über einen XNachweis-Endpunkt, über den die Lieferung von Nachweisen verschiedener Nachweistypen gemäß XNachweis [2] erfolgt.

[1] Siehe AD-NOOTS-XX/AD-NOOTS-05-+Grobkonzept+IAM+für+Behörden.md · main · NOOTS / Public / AD-NOOTS / Architektur · GitLab
[2] Siehe XÖV-Handbuch der öffentlichen Verwaltung

1.1.2 Data Consumer

Ein DC ist ein NOOTS-Teilnehmer, der im Rahmen des Prozesses zur Antragstellung für eine Verwaltungsleistung den Abruf von Nachweisen zu benötigten Informationen auslöst. Ferner kann auch ein Sachbearbeiter einer Behörde im Rahmen der Bearbeitung eines Verwaltungsverfahrens einen Nachweisabruf initiieren. Somit ist dieser Sachbearbeiter bzw. die Behörde ebenfalls ein DC. Folgende Merkmale gelten für den DC:

- Die für den DC verantwortliche nachweisanfordernde Stelle ist die fachverantwortliche Stelle. Sie verantwortet:
- die Rechtskonformität der veranlassten Nachweisabrufe,
- die Korrektheit der Daten eines Nachweisabrufs, insbesondere der Basisdaten des Nachweissubjekts und deren Vertrauensniveau
- die Weiterleitung abgerufener Nachweise an die für den Antrag verwaltungsrechtlich sachlich und örtlich zuständige Behörde

DC können nationale Onlinedienste, nationale Fachverfahren und die Intermediäre Plattform (als DC) sein.

1.1.3 Nachweis

Nachweise im Sinne des § 5 Abs. 2 EGovG sind Unterlagen und Daten jeder Art, unabhängig vom verwendeten Medium, die zur Ermittlung des Sachverhalts geeignet sind. Nachweisanfordernde Stelle kann die für die Entscheidung über den Antrag zuständige Behörde oder auch eine andere öffentliche Stelle sein, die dafür zuständig ist, Nachweise einzuholen und an die für die Entscheidung über den Antrag zuständige Behörde weiterzuleiten (DC). Eine Nachweisliefernde Stelle ist diejenige öffentliche Stelle, die dafür zuständig ist, den Nachweis auszustellen (DP). Innerhalb der NOOTS-Transportinfrastruktur wird der XNachweis aus dem XML in der öffentlichen Verwaltung (XÖV)-Standard für den Datenaustausch verwendet.

1.1.4 Technische Beschreibung SAK

Die technische Beschreibung der SAK stammt aus den Kapiteln 1 und 2 der Systemdokumentation SAK-DC und SAK-DP und wird im Folgenden abgebildet.

1.1.4.1 Aufgabenstellung

Ein SAK ist eine zentral zum Download bereitgestellte NOOTS-Komponente, die dezentral im Verantwortungsbereich der NOOTS-

Teilnehmer betrieben wird. Ein SAK ermöglicht den NOOTS-Teilnehmern über ein interoperables Anschlussprotokoll einen einfachen und sicheren Anschluss an das NOOTS, sowie den Versand und Empfang von Nachrichten über die NOOTS-Transportinfrastruktur. Der SAK kapselt dabei den Transport zwischen den NOOTS-Teilnehmern DC und DP sowie zu allen zentralen NOOTS-Komponenten. Sowohl der DC als auch der DP kommunizieren ausschließlich mit dem SAK, was bedeutet, dass der Einsatz des SAKs für die NOOTS-Teilnehmer verpflichtend ist. Das Anschlussprotokoll bedient alle erforderlichen Interaktionen zwischen DC und DP. In dieser Hinsicht verbirgt ein SAK die Komplexität des NOOTS-Systems hinter einer standardisierten Schnittstelle. Die SAKs haben Zugriff auf die übermittelten Daten und unterstützen den Teilnehmer bei der Sicherstellung von Vertraulichkeit, Integrität und Authentizität beim Transport der Daten.

1.1.4.2 Stakeholder

Tabelle 1: Stakeholder

Rolle	Erwartung
Fachverantwortliche Stelle des DC/DP	Einhaltung der organisatorischen, gesetzlichen und fachlichen Vorgaben für den Nachweisabruf.
Betriebsverantwortliche Stelle des DC/DP	Sicherer und stabiler Betrieb des SAK-DCs/DPs.

1.1.4.3 Rahmenbedingungen

Die Rahmenbedingungen des SAK-DC/DP ergeben sich aus den folgenden Dokumenten:

- Grobkonzept der Transportinfrastruktur (AD-NOOTS-19) [3]
- High-Level Architektur (AD-NOOTS-03, HLA) [4]
- Anschlusskonzept Data Consumer (AD-NOOTS-01) [5]
- Anschlusskonzept Data Provider (AD-NOOTS-02) [6]
- Schnittstellenspezifikationen für NOOTS-Komponenten [7]

[3] Siehe https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/AD-NOOTS-XX/AD-NOOTS-19_+Grobkonzept+Transportinfrastruktur.md?ref_type=heads
[4] Siehe https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/AD-NOOTS-XX/AD-NOOTS-03_+High-Level-Architecture+_HLA_.md?ref_type=heads
[5] Siehe: https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/AD-NOOTS-XX/AD-NOOTS-01_+Anschlusskonzept+Data+Consumer+_DC_.md?ref_type=heads
[6] Siehe: https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/AD-NOOTS-XX/AD-NOOTS-02_+Anschlusskonzept+Data+Provider+_DP_.md?ref_type=heads
[7] Siehe: NOOTS / Public / AD-NOOTS / SAK APIs · GitLab

Soweit nicht anders vermerkt, gelten die auf den SAK-DC/DP anwendbaren Rahmenbedingungen aus den übergeordneten Architektur- und Anforderungsspezifikationen des NOOTS.

1.2. Benennung der Verarbeitungsschritte

Wie bereits beschrieben ist der SAK eine technische Komponente zur Anbindung der IT-Systeme der DC und DP an die übrigen Komponenten der NOOTS-Transportinfrastruktur. An dieser Stelle wird daher der Gesamtprozess an Verarbeitungsschritten dargestellt und werden entsprechend die technischen Verarbeitungsschritte abgegrenzt.

Vorbedingungen:

- Beantragung einer Verwaltungsleistung über einen Online-Dienst eines DC
- Notwendige fehlende Informationen im Online-Antrag werden erkannt und als XNachweis erfasst.

SAK-Verarbeitungsschritte:

- Anschluss an die NOOTS-Transportinfrastruktur
- Anforderung wird vom IT-System des DC durch den SAK-DC an die RDN gesandt
- Die RDN ermittelt das Ziel-Register, das die erforderlichen Daten enthält, und gibt die notwendigen Token für das Auffinden des Ziel-Registers sowie die Abfrage an den SAK zurück
- Herstellen einer Verbindung zwischen DC und DP zum Abruf und Austausch von XNachweis-Inhalten
- Die XNachweis-Anfrage geht über die NOOTS-Transportinfrastruktur an den SAK-DP des für die Auskunft zuständigen DP und wird dort im angeschlossenen IT-System (Register) verarbeitet.
- Benötigte Daten werden identifiziert und gehen als XNachweis-Antwort über die SAKs denselben Weg zurück an das anfragende System.

Nachbedingung:

- Übertragung der Informationen vom SAK an den Onlinedienst und dort Anzeige im Webformular und ggfs. Verarbeitung der Informationen

Die Beschreibung der Use Cases kann nur rudimentär auf technischer Ebene erfolgen. Dabei handelt es sich um eine Momentaufnahme (IST-Umsetzung). Die Angaben hierzu sind durch den jeweiligen Verantwortlichen in Verarbeitungsschritte nach der SDM-Methode zu überführen und entsprechend der fachlichen Einsatzszenarien, hier die Benennung der über das NOOTS durchgeführten Fälle für Nachweisabrufe, anzupassen.

1.3. Technische Beschreibung der Verarbeitungsschritte, Datenflüsse und Funktionalitäten

Der grundlegende Aufbau der Systeminfrastruktur der SAK-DC und SAK-DP mit den Datenflüssen sowie deren Funktionalitäten wird im Folgenden abgebildet:

1.3.1 Lösungsstrategie

1.3.1.1 Betriebsstrategien

Die Anwendung wird als JAR-File ausgeliefert, inklusive einer Beispielkonfiguration. Genauere Informationen hierzu sind in der Integrationsanleitung aufzufinden [8].

1.3.2 Bausteinsicht DC

1.3.2.1 Consumer-API Implementation

Die Consumer-API Implementation ist eine SAK-DC Server-Schnittstelle, welche die Kommunikation zwischen Data-Consumer und NOOTS ermöglicht. Die Schnittstelle implementiert die Consumer-API Spezifikation und damit die folgenden Endpunkte:

1.3.3 Verteilungssicht Beschreibung

Die Verteilungssicht beschreibt die technische Infrastruktur der SAKs (z.B. Server, Netze, Container) und deren Zusammenspiel. Sie zeigt, wie Software-Bausteine auf dieser Infrastruktur verteilt sind.

Grundsätzlich kann das Laufzeitartefakt (JAR) der Anwendung in einer VM, einem Container oder auf Bare Metal ausgeführt werden. Ein entsprechender Applikationsserver (Tomcat bei SAK-DC, Netty beim SAK-DP) wird, in dem Artefakt eingebettet, mit ausgeliefert. Der Fokus

[8] Siehe: https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/AD-NOOTS-XX/AD-NOOTS-02_+Anschlusskonzept+Data+Provider+_DP_.md?ref_type=heads

des Verteilungsdiagramms liegt somit auf den grundlegenden Anforderungen zum Betrieb des JARs und die Darstellung dient lediglich als ein Beispiel.

1.3.3.1 Ebene 1 Verteilungsschicht

Das Verteilungsdiagramm Ebene 1 zeigt jeweils einen groben Überblick der für SAK-DC und SAK-DP relevanten Systeme, Schnittstellen, Kommunikationswege, Netze, Laufzeitumgebung und Nodes.

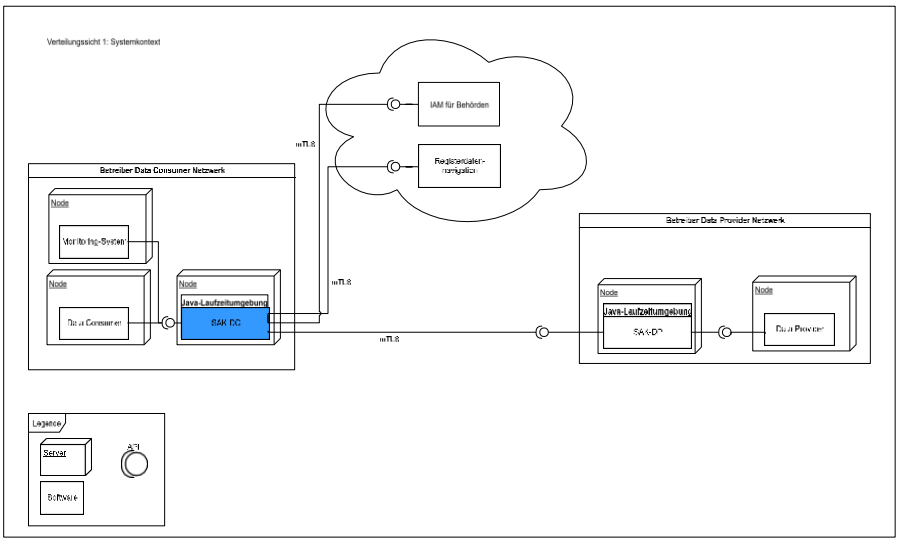

Abbildung 1: Verteilungsdiagramm DC

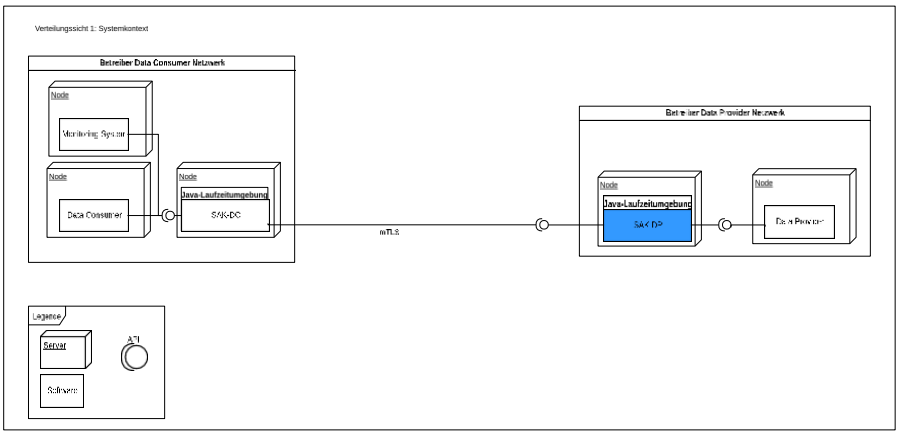

Abbildung 2: Verteilungsdiagramm DP

1.3.3.2 Ebene 2 Verteilungsschicht

Das Verteilungsdiagramm Ebene 2 fokussiert sich auf die Übersicht des SAK-DC und SAK-DP innerhalb des DC- bzw. DP- Betriebs. Dabei werden benötigte weitere Konfigurationsdateien dargestellt, die für den Betrieb notwendig sind. So müssen beispielsweise ein entsprechender Trust- sowie Keystore im verwendeten DC / DP hinterlegt sein. Für den Betrieb des SAK-DC und SAK-DP müssen außerdem umgebungsspezifische

Konfigurationen, beispielsweise über eine application.properties-Datei, zur Verfügung gestellt, und passende Zertifikate und Keystores hinterlegt werden.

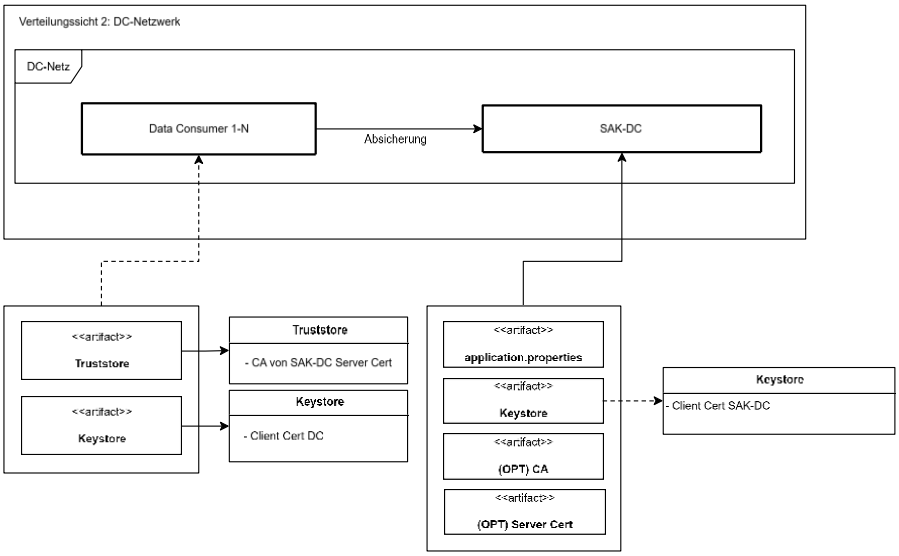

Abbildung 3: Verteilungsdiagramm SAK-DC

Grundsätzlich ist ein Betrieb von mehreren DC über einen SAK-DC möglich. Eine vollständige Mandantenfähigkeit ist derzeit allerdings noch nicht gewährleistet. Mehrere Data-Consumer agieren derzeit als **eine** Anwendung über einen SAK-DC.

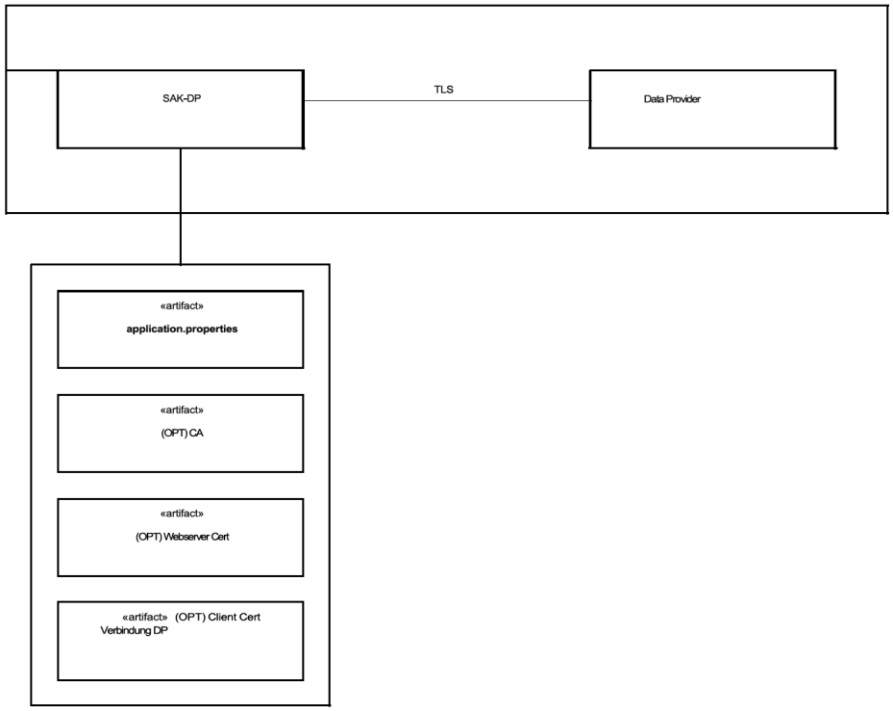

Abbildung 4: Verteilungsschicht SAK-DP

2. Ebene 2 SDM - Umgesetzte Maßnahmen der Anwendungsschicht

Die hier gemachten Angaben beziehen sich auf den Betrieb des SAK-DC und des SAK-DP. Sie werden entsprechend der Funktionalitäten der jeweiligen SAK-Version bereitgestellt. Auch an dieser Stelle sind noch durch den jeweiligen datenschutzrechtlich Verantwortlichen Inhalte, organisatorische und risikominimierende Maßnahmen zu identifizieren und festzulegen, und durch die betriebsverantwortliche Stelle zu implementieren. An entsprechender Stelle wird darauf gesondert hingewiesen.

2.1. Datenkategorien und Betroffenenkategorien

Die Angabe der zu verarbeitenden Kategorien von Daten sowie betroffener Personen erfolgt in generischer Form. Das bedeutet, dass keine abschließende Definition personenbezogener Daten in Bezug auf Inhaltsdaten in dieser Konzeption stattfinden kann. Sie hängt vom jeweiligen Einsatzszenario ab. Hier werden generisch die lt. Gesetz theoretisch möglichen Inhalte genannt. Diese Informationen sind je nach Sachverhalt durch den Verantwortlichen zu ergänzen.

Lfd. Nr.	Beschreibung der Kategorie(n) betroffener Personen
1	Antragsteller:innen
2	Sachbearbeiter:innen Behörde (ist durch betriebsverantwortliche Stelle zu bestimmen)
3	Technische Mitarbeiter:innen Behörde und betriebsverantwortliche Stelle (ist durch betriebsverantwortliche Stelle zu bestimmen)

Tabelle 2: Beschreibung der Kategorien betroffener Personen

Lfd. Nr.	Betroffenen-kategorie (aus Tabelle 1)	Beschreibung der zu verarbeitenden Daten
1	1	Basisdaten gem. § 4 Abs. 2 IDNrG: 1. Identifikationsnummer 2. Familienname 3. frühere Namen 4. Vornamen 5. Doktorgrad 6. Tag und Ort der Geburt 7. Geschlecht 8. Staatsangehörigkeiten 9. gegenwärtige oder letzte bekannte Anschrift 10. Sterbetag 11. Tag des Einzugs und des Auszugs Weitere Daten gem. § 4 Abs. 3 IDNrG: 1. Auskunftssperren nach dem Bundesmeldegesetz 2. Datum des letzten Verwaltungskontakts (Monat, Jahr)
2	2, 3	Für die Administration des SAK können von den Sachbearbeitern/ technischen Mitarbeitern einer Behörde und betriebsverantwortlichen Stelle zum Beispiel die folgenden Daten verarbeitet werden: 3. Vorname 4. Nachname 5. behördliche E-Mail-Adresse 6. behördliche Telefonnummer 7. behördliche Adresse 8. Benutzername 9. Passwort

Tabelle 3: Zuordnung d. Kategorien von zu verarb. Daten zu d. Betroffenenkategorien

Eine Prüfung und Erweiterung dieser Informationen um übertragene Inhalte sowie eine Bewertung, ob die verarbeiteten Inhaltsdaten einem hohen Schutzniveau unterliegen, sind durch den Verantwortlichen in Bezug auf die jeweilige Verarbeitungstätigkeit und die damit verbundenen zu erwartenden Risiken für die EU-Grundrechte und / oder EU-Grundfreiheiten zu ermitteln.

Es wird darauf hingewiesen, dass vorab eine Festlegung zum allgemeinen Schutzbedarf beim Einsatz von SAKs auf dem Level ‚Hoch' aufgrund der Sensitivität einzelner transportierter Datenkategorien erfolgt ist. Die daraus entstehende Dokumentation der zu verarbeitenden personenbezogenen Daten kann dann als Basis für den Eintrag in das Verzeichnis der Verarbeitungstätigkeiten gem. Art. 30 Abs. 1 DSGVO verwendet werden.

2.2. Datenflussdiagramm und Schnittstellen

Die Dokumentationen des SAK-DC und des SAK-DP umfassen ebenso die Schnittstellen (APIs), die in den zu betrachtenden Datenflüssen technisch eingebunden sind. Durch diese Dokumentation werden die Umsetzung der Gewährleistungsziele: Transparenz der Datenverarbeitung sowie Integrität der Daten bei der Übertragung und die Nichtverkettung nachgewiesen.

Nachstehend erfolgt zunächst eine allgemeine Übersicht eines HLA- bzw. *High-Level-Architecture*-Datenflussdiagramms für den Datenaustausch beim Nachweisabruf [9]:

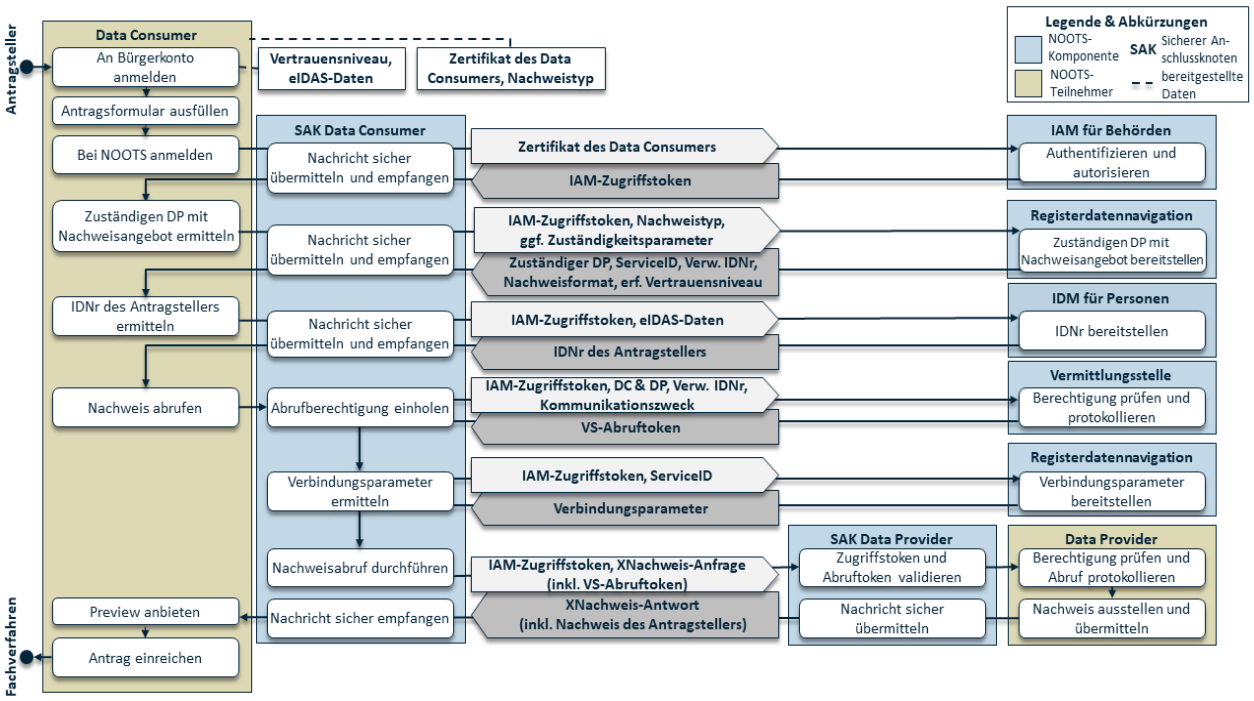

Abbildung 5: Datenflüsse beim Nachweisabruf

[9] Quelle: High-Level-Architecture (HLA) Abbildung 4: https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/AD-NOOTS-XX/AD-NOOTS-03_+High-Level-Architecture+_HLA_.md?ref_type=heads

2.2.1 Fachlicher Kontext SAK-DC

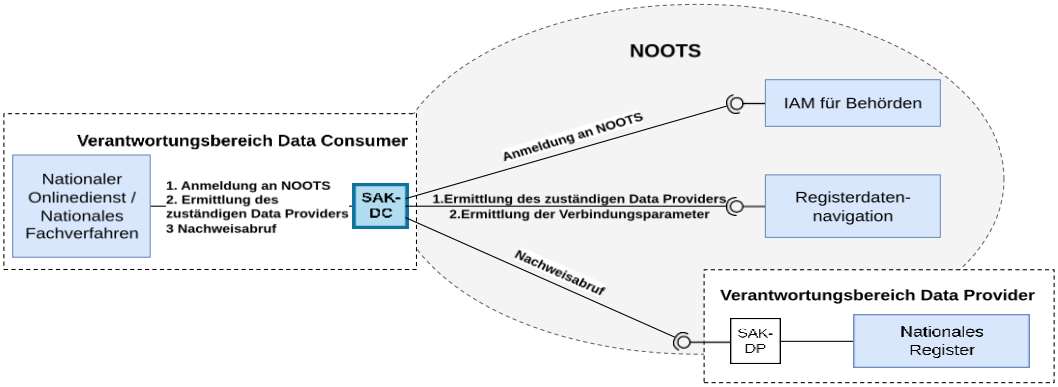

Abbildung 6: Fachlicher Kontext

2.2.2 Fachlicher Kontext SAK-DP

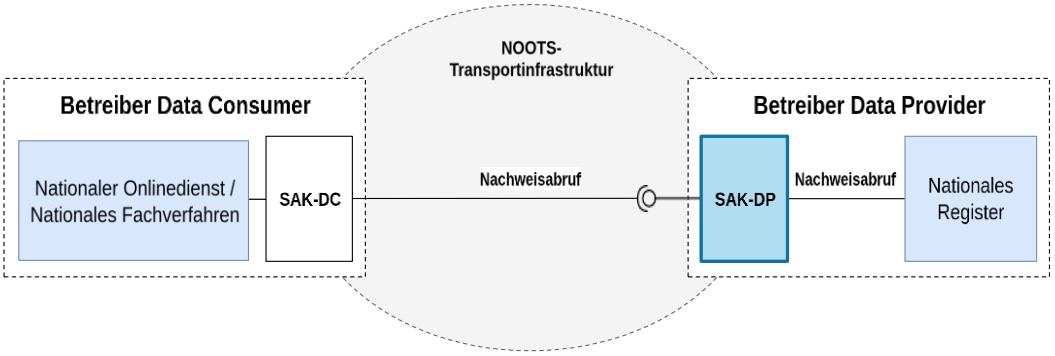

Abbildung 7: SAK-DP Fachlicher Kontext

2.2.3 Technischer Kontext SAK-DC

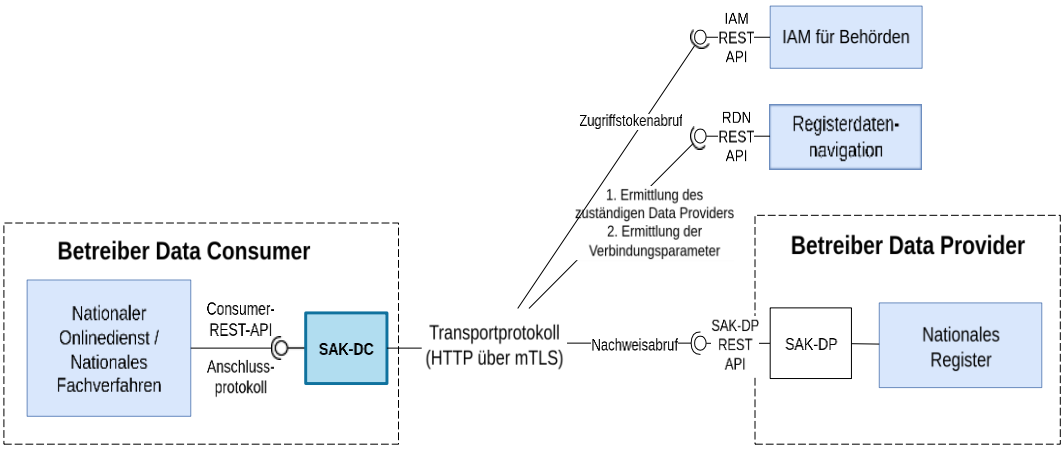

Abbildung 8: SAK-DC: Technischer Kontext

Tabelle 4: SAK-DC: Mapping fachliche auf technische Schnittstellen

Fachliche Schnittstelle	Technische Schnittstelle
Anmeldung an NOOTS DC	Anforderung Zugriffstoken via IAM für Behörden Schnittstelle unter Verwendung des NOOTS-Transportprotokolls
Ermittlung des zuständigen Data Provider / der Verbindungsparameter DC	RDN-Schnittstelle unter Verwendung des NOOTS-Transportprotokolls
Nachweisabruf	Data Provider (passiver Empfänger) Schnittstelle unter Verwendung des NOOTS-Transportprotokolls

2.2.4 Technischer Kontext SAK-DP

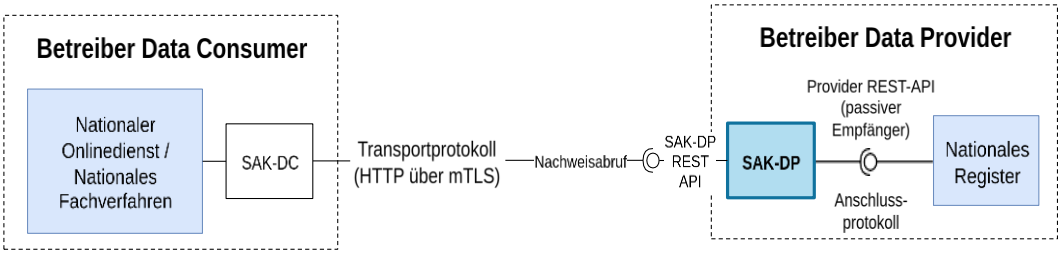

Abbildung 9: SAK-DP Technischer Kontext

Die Abbildung beschreibt die Interaktion zwischen SAK-DP und der NOOTS-Infrastruktur, bzw. Aufruf des SAK-DP durch einen SAK-DC.

Tabelle 5: SAK-DP: Mapping fachliche auf technische Schnittstellen

Fachliche Schnittstelle	Technische Schnittstelle
Nachweisabruf	Data Provider (passiver Empfänger) Schnittstelle unter Verwendung des NOOTS-Transportprotokolls

Die präsentierten Abbildungen und Erläuterungen stützen sich auf das nachfolgende Dokument, in denen umfassendere Informationen zu finden sind:

- High-Level Architektur (AD-NOOTS-03, HLA) [10]

- Architekturkonzept Programm NOOTS, Kapitel "Kontextabgrenzung" [11]

2.2.5 Consumer-API Implementation SAK-DC

Die Consumer-API Implementation ist eine SAK-DC Server-Schnittstelle, welche die Kommunikation zwischen Data-Consumer und NOOTS ermöglicht. Die Schnittstelle implementiert die Consumer-API Spezifikation und damit die folgenden Endpunkte:

Tabelle 6: Endpunkte nach Consumer-API Spezifikation

Endpunkt	http-Methode	Beschreibung
/token	POST	Abruf des Zugrifftoken über das Identitätsmanagement für Behörden anhand einer Komponenten-ID. Notwendig für die Verwendung der weiteren Schnittstellen.
/de/evidence-offer	POST	Abruf der Nachweisangebote für einen bestimmten Nachweistyp anhand des Typen und optionalen Zuständigkeitsparametern (ARS). Gibt eine Liste von Nachweisangeboten mit entsprechenden Service-IDs zurück.
/de/evidence	POST	Abruf des eigentlichen Nachweises anhand einer Service-ID und einer Nachweisanfrage, welche den gewünschten Nachweis weiter einschränkt und definiert.

2.2.6 Laufzeitsicht

Abläufe und Beziehungen zwischen SAK-DC und Nachbarkomponenten werden auf fachlicher und technischer Ebene in folgendem Dokument beschrieben:

[10] Siehe https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/AD-NOOTS-XX/AD-NOOTS-03_+High-Level-Architecture+_HLA_.md?ref_type=heads
[11] Siehe https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/AD-NOOTS-XX/AD-NOOTS-03_+High-Level-Architecture+_HLA_.md?ref_type=heads

- Anschlusskonzept Data Consumer (AD-NOOTS-01) [12], Kapitel "Ablauf eines Nachweisabrufs" beschreibt die Gesamtabläufe unterschiedlicher Nachweisabrufszenarien aus fachlicher Sicht.

- Grobkonzept der Transportinfrastruktur (AD-NOOTS-19) [13], Kapitel "Laufzeitsicht" konkretisiert den Ablauf von Nachweislieferung für den nationalen Nachweisabruf.

2.3. Protokollierung

Der Zweck einer Protokollierung besteht unter anderem sowohl in der Schaffung der Möglichkeit der Transparenz, als auch der Überprüfbarkeit von Verarbeitungstätigkeiten, die bereits in der Vergangenheit liegen. Hierbei wird das Augenmerkt auf den Nachweis der Compliance von Verarbeitungstätigkeiten mit den internen und externen Regularien gerichtet. In einer Dokumentation ist daher nachzuweisen, welche Instanz welche Aktivität zu bestimmten Zeitpunkten an den Verarbeitungstätigkeiten ausgeführt und welche Instanz das Protokoll über diese Tätigkeiten geführt hat.

Vorliegend werden in den SAKs technische Informationen geloggt. Die Informationen enthalten keine personenbezogenen oder personenbeziehbare Werte. Die Speicherung der Protokolle erfolgt nicht innerhalb der SAK und muss durch die betriebsverantwortliche Stelle in Zusammenwirken mit dem jeweils datenschutzrechtlichen Verantwortlichen festgelegt, durchgeführt und in einem Konzept dokumentiert werden.

Eine Übersicht der protokollierten Inhalte für den SAK-DC und den SAK-DP wird im Folgenden abgebildet:

2.3.1 Protokollierung DC

Im weiteren Verlauf wird im Kontext dieses Dokumentes der Begriff "Protokollierung" verwendet, welcher vom Begriff "Protokollierung" der NOOTS High-Level-Architektur abzugrenzen ist. Siehe High-Level Architektur (AD-NOOTS-03, HLA, Entwicklungsstand), Kapitel 2.3.3

Unter Verwendung der ausgelieferten Standard-Konfiguration werden keine sensiblen oder personenbezogenen Daten von den Anwendungen geloggt. Entsprechend verwendete Werte können in dieser angehängten

[12] Siehe: https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/AD-NOOTS-XX/AD-NOOTS-01_+Anschlusskonzept+Data+Consumer+_DC_.md?ref_type=heads
[13] Siehe https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/AD-NOOTS-XX/AD-NOOTS-19_+Grobkonzept+Transportinfrastruktur.md?ref_type=heads

Datei (wird zusammen mit dem Installationsartefakt ausgeliefert) entnommen werden.

Protokollierung (engl. "Logging") umfasst alle Systemfunktionen, um wichtige fachliche und technische Ereignisse und Abläufe zu protokollieren und an ein entsprechendes Speichermedium zu übertragen. Neben der Standardausgabe des Betriebssystems können dies auch Log- Dateien im Dateisystem sein, ein zentrales Sammelsystem im Netzwerk oder eine Kombination davon.

Standardmäßig ist die Anwendungskonsole als Zielmedium für Log-Ausgaben aktiviert. Dies ermöglicht die Anzeige von Anwendungslogs in einer Kubernetes-Umgebung. Das Log-Speichermedium ist allerdings nicht festgelegt; es kann je nach Bedarf individuell konfiguriert werden.

2.3.1.1 Zweck

Die erzeugten Anwendungsprotokolle dienen der Dokumentation von technischen Ereignissen (z.B. Systemstart und -stopp, Auftreten von internen Fehlern), sowie von fachlichen Ereignissen (z.B. Zugriff und Authentifizierung durch ein Client-System, Ausführung von angefragten Aktionen, Fehlermeldungen von nachgelagerten Systemen). Die dokumentierten Ereignisse können zur Überprüfung des ordnungsgemäßen Systembetriebs, der ordnungsgemäßen Nutzung durch Clients, sowie zur Reproduktion von Fehlfunktionen zur Ermittlung von Fehlerursachen hilfreich sein.

2.3.1.2 Abgrenzung

Während bei den Konzepten "Metriken" und "Überwachung" die permanente (teils automatisierte) Überwachung von (Teil-)Systemen im Vordergrund steht, geht es bei der Protokollierung um die Dokumentation und längerfristige Speicherung von wichtigen fachlichen und technischen Ereignissen.

Log-Nachrichten enthalten deshalb mehr fachliche Informationen als Überwachungsmeldungen.

2.3.1.3 Realisierung

SAK-DC verwendet die Logging-Integration von Spring-Boot. Allgemeine Eigenschaften hierzu sind in der Spring-Dokumentation beschrieben.

Es kommt die Logging-Bibliothek Logback zum Einsatz. Die allgemeinen Eigenschaften zur Konfiguration und zum Ausgabe-Format können in der Produktdokumentation von Logback nachgeschlagen werden.

Im Folgenden werden jeweils nur anwendungsspezifische Eigenschaften bei SAK-DC beschrieben.

2.3.1.4 Log-Ausgabeformat

SAK-DC erzeugt Log-Ausgabe standardmäßig im ECS-Format (Elastic Common Schema). ECS ist ein JSON-Schema mit standardisierten Ausgabe-Daten. Diese umfassen neben den üblichen Elementen Log-Nachrichten auch die Trace-ID zur systemweiten Verfolgung von Aktivitäten und Datenflüssen.

ECS kann um zusätzliche Daten erweitert werden. Dies wird momentan allerdings nicht genutzt.

Derzeit wird ein Logformat mit folgenden Fieldsets und Feldern genutzt:

Tabelle 7: Genutzte Felder in den Logausgaben

ECS-Fieldset	Beschreibung	Kontext
Base	Enthält Basis-Felder, welche bei jedem Logeintrag geschrieben werden. - @timestamp: Zeitstempel der Logeintrages - message: Logeintrag	Alle Logeinträge
Log	Informationen über die schreibende Klasse, welche den Logeintrag erzeugt. - log.level: Level des Logeintrages - log.logger: Klasse, welche den Logeintrag erzeugt	Alle Logeinträge
Process	Informationen über den aktuellen Anwendungsprozess und Thread. - process.pid: Prozess-ID der Anwendung - process.thread: Aktiver Thread	Alle Logeinträge
Service	Informationen über die Anwendung. - service.name: Name der Anwendung - service.node: Informationen über die Anwendung, wenn mehrere Instanzen des identischen Service gestartet wurde. Enthält Informationen, die verschiedenen Instanzen unterscheiden können. Im Normalfall ist dieses Feld nicht gesetzt, bzw. leer.	Alle Logeinträge
ECS	Enthält Versionsinformationen über das verwendete Elastic Common Schema. - ecs.version: Verwendete Version des ECS	Alle Logeinträge

Tracing	Enthält Informationen über das Tracing einer Aktion / eines Logs. - traceId: Eindeutige ID des Traces, welche alle Ereignisse einer Anfrage zusammenfasst. - spanId: Eindeutige ID des Spans, welcher ein Ereignis eines Traces identifiziert.	Logeinträge, welche im Rahmen einer externen Anfrage geschrieben werden
Error	Enthält Informationen über eine interne Fehlermeldung, welche durch die Anwendung erzeugt wird. - error.type: Der erkannte Fehlertyp (Typ des Fehlers) - error.message: Fehlernachricht des verknüpften Fehlers	Logeinträge, welche im Rahmen eines Fehlers geschrieben werden

2.3.1.5 Log-Level

Es werden die Log-Level von Logback verwendet: ERROR, WARN, INFO, DEBUG und TRACE.

In der Standard-Konfiguration werden Meldungen mit Log-Level ERROR, WARN und INFO ausgegeben, die Log-Level DEBUG und TRACE sind deaktiviert. Dieses Verhalten kann jedoch bei Bedarf in der Konfigurationsdatei angepasst werden.

2.3.1.6 Protokolle

2.3.1.7 Protokollklassifikation SAK-DC

In den nachfolgenden Beschreibungen der Logausgaben der Anwendung werden diese in mehrere Protokollklassifikationen / Typen aufgeschlüsselt. Diese beschreiben die Art des Logeintrages und Übersichtlichkeit und Filterung für bestimmte Personen- und Verantwortungskreise, welche Zugriff auf die Loginformationen haben.

Es wird zwischen den folgenden Klassifikationen unterschieden:

Tabelle 8: Protokollklassifikation SAK-DC

Typ	Protokoll	Beschreibung
A	Anwendungsnutzung	Protokollierung der Anwendung des Programms zur Sachbearbeitung (im engen Sinne)
B	Anwendungs-administration	Administration der Strukturen auf Anwendungsebene Beispiel: Änderungen von

		Datenfeldern, Nutzerverwaltung, Softwareänderungen/Updates
C	Systemadministration	Administration von Hardware, Betriebssystem, Middleware, Netzinfrastruktur, Speicherungssystemen, auf denen das Anwendungsprogramm aufsetzt
D	Schnittstellennutzung	Protokollierung der Aktivitäten an Schnittstellen (als Beispiel wäre an Übermittlungen von Daten an andere Stellen zu denken, sofern diese über Schnittstellen angeschlossen sind.)
E	Sicherheitsprotokoll	Protokollierung der technischen Schutzmaßnahmen (z.B. Zertifikatsprüfungen, Backupreports)

Der SAK-DC schreibt Protokolle vom Typ **D** und **E**, sowie Log-Ausgaben bei Systemereignissen (Systemstart-/stop, etc.). Diese können Typ **C** zugeordnet werden.

2.3.1.8 Log-Ausgaben

Neben den hier aufgeführten Log-Ausgaben können weitere Log-Nachrichten durch die eingesetzten Bibliotheken und Frameworks abgesetzt werden. Diese werden hier nicht dokumentiert.

2.3.1.9 Schnittstellenereignisse SAK-DC

In der Systemdokumentation SAK-DC werden alle Ereignisse rund um die Anwendung zusammengefasst, die zur Laufzeit durch eine Benutzerinteraktion mit den propagierten Schnittstellen hervorgerufen werden. Sie dienen in erster Linie der fachlichen Nachvollziehbarkeit der Benutzeraktionen, sowie als einfache Möglichkeit, manuell die Performance der Schnittstellen nachvollziehen und deren Verhalten prüfen zu können.

Auf die Anlage Systemdokumentation 2026-01-22 Ereignisse-SAK-DC - Schnittstellenereignisse- als mitgeltend zu dieser Datenschutzdokumentation Seite 1-18 wird verwiesen.

2.3.1.10 Sicherheitsereignisse SAK-DC

Die Tabelle Sicherheitsereignisse fasst alle Ereignisse rund um die Anwendung zusammen, die beim Start oder zur Laufzeit entstehen und einen Bezug zur Authentifizierung und Autorisierung haben.

Diese Tabelle befindet sich auf Seite 18-20 der Anlage Systemdokumentation 2026-01-22 Ereignisse-SAK-DC -Sicherheitsereignisse- (mitgeltend zu dieser Datenschutzdokumentation).

2.3.1.11 Systemereignisse SAK-DC

Die Tabelle Systemereignisse fasst alle Ereignisse rund um die Anwendung zusammen, die nicht zur Laufzeit entstehen und somit nicht im Zusammenhang mit einer Interaktion stehen. Diese Tabelle ist auf Seite 20 der Anlage Systemdokumentation 2026-01-22 Ereignisse-SAK-DC -Systemereignisse- abgebildet (mitgeltend zu dieser Datenschutzdokumentation).

2.3.2 Protokollierung SAK-DP

Im weiteren Verlauf wird im Kontext dieses Dokumentes der Begriff "Protokollierung" verwendet, welcher vom Begriff "Protokollierung" der NOOTS High-Level-Architektur abzugrenzen ist, siehe High-Level Architektur (AD-NOOTS-03, HLA, Entwicklungsstand), Kapitel 2.3.3.

Unter Verwendung der ausgelieferten Standard-Konfiguration werden keine sensiblen oder personenbezogenen Daten von der Anwendung geloggt. Entsprechend verwendete Werte können in dieser angehängten Datei (wird zusammen mit dem Installationsartefakt ausgeliefert) entnommen werden.

Protokollierung (engl. "Logging") umfasst alle Systemfunktionen, um wichtige fachliche und technische Ereignisse und Abläufe zu protokollieren und an ein entsprechendes Speichermedium zu übertragen. Neben der Standardausgabe des Betriebssystems können dies auch Log- Dateien im Dateisystem sein, ein zentrales Sammelsystem im Netzwerk oder eine Kombination davon.

Standardmäßig ist die Anwendungskonsole als Zielmedium für Log-Ausgaben aktiviert. Dies ermöglicht die Anzeige von Anwendungslogs in einer Kubernetes-Umgebung. Das Log-Speichermedium ist allerdings nicht festgelegt; es kann je nach Bedarf individuell konfiguriert werden.

2.3.2.1 Zweck

Fehleridentifikation und technische Diagnose: Durch umfassendes Logging können technische Fehler und Ausnahmen frühzeitig erkannt und analysiert werden. Dies ermöglicht es dem Support, Probleme schnell zu identifizieren, zu beheben und die Stabilität sowie die Zuverlässigkeit des Systems zu gewährleisten. Logs enthalten detaillierte Informationen über Systemereignisse, Fehlercodes,

Stacktraces und andere relevante Metadaten, die für die technische Diagnose unerlässlich sind.

Fachliches Auditlogging: Neben der technischen Fehleranalyse ist es ebenfalls wichtig, ein fachliches Auditlog zu führen. Dieses Log dient der Nachverfolgbarkeit und Transparenz von Geschäftsprozessen und -transaktionen. Es dokumentiert relevante Aktionen und Änderungen, die von Benutzern oder Systemen vorgenommen werden, und stellt sicher, dass alle relevanten Ereignisse nachvollziehbar sind. Dies ist besonders wichtig für Compliance-Anforderungen und interne Audits.

Durch die Kombination dieser beiden Aspekte stellen wir sicher, dass unser System sowohl technisch robust als auch fachlich transparent und nachvollziehbar ist.

2.3.2.2 Abgrenzung

Logging ist ein spezifischer Mechanismus zur Erfassung und Speicherung von Ereignissen und Informationen, die während des Betriebs der Anwendung auftreten. Es dient primär der Fehleridentifikation, der technischen Diagnose und der Erstellung eines fachlichen Auditlogs. Logging unterscheidet sich daher von anderen Überwachungs- und Monitoring-Mechanismen wie Metriken in mehreren Aspekten, z.B. der Verwendung, der Speicherung und dem Detailgrad.

Während daher bei den Konzepten Metriken und Überwachung die permanente, teils automatisierte, Überwachung im Vordergrund steht, handelt es sich bei dem Logging um längerfristige Speicherung von wichtigen fachlichen und technischen Ereignissen.

2.3.2.3 Softwarekomponenten

SAK-DP verwendet die Logging-Integration von Spring-Boot. Allgemeine Eigenschaften hierzu sind in der Spring-Dokumentation beschrieben. Es kommt die Logging-Bibliothek Logback zum Einsatz. Die allgemeinen Eigenschaften zur Konfiguration und zum Ausgabe-Format können in der Produktdokumentation von Logback nachgeschlagen werden.

2.3.2.4 Log-Ausgaben

In der Standard-Konfiguration werden Meldungen mit Log-Level ERROR, WARN und INFO ausgegeben, die Log-Level DEBUG und TRACE sind deaktiviert. Dieses Verhalten kann jedoch bei Bedarf durch Konfiguration angepasst werden. SAK-DP erzeugt Log-Ausgaben standardmäßig im ECS-Format (Elastic Common Schema) welche auf der Konsole ausgegeben werden. ECS ist ein JSON-Schema mit

standardisierten Ausgabe-Daten. Diese umfassen neben den üblichen Elementen von Log-Nachrichten auch die Trace-ID zur systemweiten Verfolgung von Aktivitäten und Datenflüssen.

Alternativ kann das ECS-Format deaktiviert werden. Die Meldungen werden dann im Defaultformat von Spring ausgegeben. Auch ein eigenen Logschema kann über die Anwendungseinstellungen definiert werden.

Sind die Ausgaben in der Konsole nicht gewünscht, besteht die Möglichkeit, die Ausgabe in eine Datei umzuleiten. Sowohl der Ablageort als auch der Name der Datei ist frei konfigurierbar. Das Format entspricht hierbei ebenfalls dem zuvor genannten Spring Standard.

2.3.2.5 Aufbewahrung und Bereitstellung der Daten

Alle Ausgaben werden wie bereits beschrieben auf der Konsole ausgegeben, oder, wenn konfiguriert, als Datei abgelegt.

Die betriebsverantwortliche Stelle ist daher dafür verantwortlich, die Log-Daten in einem angemessenen Rahmen zu speichern (gem. DSGVO), nur berechtigten Akteuren offenzulegen, sowie unter Einhaltung der DSGVO die jeweiligen Löschfristen umzusetzen.

2.3.2.6 Protokollklassifikation SAK-DP

In den nachfolgenden Beschreibungen der Logausgaben der Anwendung werden diese in mehrere Protokollklassifikationen / Typen aufgeschlüsselt. Diese beschreiben die Art des Logeintrages und Übersichtlichkeit und Filterung für bestimmte Personen- und Verantwortungskreise, welche Zugriff auf die Loginformationen haben.

Es wird zwischen den folgenden Klassifikationen unterschieden:

Tabelle 9: Protokollklassifikation SAK-DP

Typ	Protokoll	Beschreibung
A	Anwendungsnutzung	Protokollierung der Anwendung des Programms zur Sachbearbeitung (im engen Sinne)
B	Anwendungsadministration	Administration der Strukturen auf Anwendungsebene Beispiel: Änderungen von Datenfeldern, Nutzerverwaltung, Softwareänderungen/Updates
C	Systemadministration	Administration von Hardware, Betriebssystem, Middleware,

		Netzinfrastruktur, Speicherungssystemen, auf denen das Anwendungsprogramm aufsetzt
D	Schnittstellennutzung	Protokollierung der Aktivitäten an Schnittstellen (als Beispiel wäre an Übermittlungen von Daten an andere Stellen zu denken, sofern diese über Schnittstellen angeschlossen sind.)
E	Sicherheitsprotokoll	Protokollierung der technischen Schutzmaßnahmen (z.B. Zertifikatsprüfungen, Backupreports)

Der SAK-DP schreibt Protokolle vom Typ **D** und **E**, sowie Log-Ausgaben bei Systemereignissen (Systemstart-/stop, etc.). Diese können Typ **C** zugeordnet werden.

2.3.2.7 Schnittstellenereignisse

Die Tabelle Schnittstellenereignisse fasst alle Ereignisse rund um die Anwendung zusammen, die zur Laufzeit durch eine Benutzerinteraktion mit den propagierten Schnittstellen hervorgerufen werden. Sie dienen in erster Linie der fachlichen Nachvollziehbarkeit der Benutzeraktionen, sowie als einfache Möglichkeit, manuell die Performance der Schnittstellen nachvollziehen und deren Verhalten prüfen zu können. Diese Tabelle ist auf den Seiten 1-2 der Anlage Systemdokumentation 2026-01-22 Ereignisse-SAK-DP -Schnittstellenereignisse- abgebildet (mitgeltend zu dieser Datenschutzdokumentation).

2.3.2.8 Sicherheitsereignisse

Die Tabelle Sicherheitsereignisse fasst alle Ereignisse rund um die Anwendung zusammen, die beim Start oder zur Laufzeit entstehen und einen Bezug zur Authentifizierung und Autorisierung haben. Diese Tabelle ist auf den Seiten 2 und 3 der Anlage Systemdokumentation 2026-01-22 Ereignisse-SAK-DP -Sicherheitsereignisse- abgebildet (mitgeltend zu dieser Datenschutzdokumentation).

2.3.2.9 Systemereignisse

Die Tabelle Systemereignisse fasst alle Ereignisse rund um die Anwendung zusammen, die nicht zur Laufzeit entstehen und somit nicht im Zusammenhang mit einer Interaktion stehen. Diese Tabelle ist auf den Seiten 3-4 der Anlage Systemdokumentation 2026-01-22 Ereignisse-SAK-DP -Systemereignisse- abgebildet (mitgeltend zu dieser Datenschutzdokumentation).

2.4. Datenschutzprozesse

Sofern personenbezogene Daten natürlicher Personen verarbeitet werden, leiten sich hieraus für einen Betroffenen subjektive Rechte nach Art. 15 bis 22 DSGVO gegen den Verantwortlichen ab. Ein Verantwortlicher hat deshalb individuelle Prozesse in seiner Behörde zu implementieren, die einem Betroffenen die Wahrnehmung seiner subjektiven Rechte ermöglicht. Auch die Einführung organisatorischer Regeln zur Bearbeitung von Anfragen betroffener Personen ist Aufgabe des Verantwortlichen. So können Datenschutzverletzungen abgemildert und Anforderungen der Gewährleistungsziele der Transparenz und Intervenierbarkeit umgesetzt werden. Sofern Unterstützung bei der Bearbeitung von Anfragen Betroffener hinsichtlich ihrer subjektiven Rechte benötigt wird, steht es einem Verantwortlichen frei, Unterstützung durch einen Auftragsverarbeiter im Rahmen der ihm übertragenen Aufgaben in Anspruch zu nehmen.

Unter Berücksichtigung der Funktionalitäten des SAK sowie des Umstandes, dass die Antragsteller zu keinem Zeitpunkt einen direkten Kontakt mit einem SAK haben, reduzieren sich die hinsichtlich der Rechte zu implementierenden Prozesse. Aufgrund der Funktion eines SAK, Nachweise zu Anfragen und Antworten ohne persistente Speicherung unter Aufrechterhaltung einer TLS-verschlüsselten Verbindung durch- resp. weiterzuleiten, besteht weder die technische noch gesetzliche Möglichkeit der Erfüllung der Rechte der Betroffenen. Eine Beschreibung dazu befindet sich in Unterkapitel 8.4 der Systemdokumentation für den SAK-DP und wird im Folgenden abgebildet:

SAK-DP nutzt keinerlei Persistenz. Die eingehenden Daten werden lediglich verarbeitet und weitergeleitet aber zu keinem Zeitpunkt dauerhaft außerhalb des Arbeitsspeichers gehalten. Zustände von vorherigen Interaktionen zwischen SAK-DC und SAK-DP sowie SAK-DP und Data Provider werden nicht gespeichert oder in irgendeiner Form wiederverwendet. Das System ist zustandslos.

2.5. Rollen- und Rechte

Durch die Vergabe von Rollen und der damit einhergehenden Zuweisung von fachlichen Zuständigkeiten sowie technischen Berechtigungen sollen die Risiken einer unrechtmäßigen Datenverarbeitung, die von unbefugten Zugriffen und von Zugriffen mit zu weitreichenden Rechten ausgehen können, reduziert werden. Ein Rollen- und Rechtekonzept unterstützt die Umsetzung der Gewährleistungsziele der Nichtverkettung, Integrität, Vertraulichkeit, Intervenierbarkeit und Verfügbarkeit.

Die SAK-Instanzen verfügen über keine eigenen Benutzerrollen und -Rechte, da über die Systemadministration hinaus kein persönlicher Benutzerzugriff erfolgt. Eine Beschreibung der Zugriffsmöglichkeiten der Systemadministration ist bisher nicht durch den Hersteller zur Verfügung gestellt worden.

Eine Beschreibung der Zugriffe auf Betriebsebene ist durch die betriebsverantwortliche Stelle zu definieren und in einem eigenen Konzept zu dokumentieren.

Die Beschreibung der Autorisierung für Nachweisabrufe befindet sich in der jeweiligen Systemdokumentation für SAK-DC und SAK-DP im Abschnitt 8.1.2 und wird im Folgenden abgebildet:

Die Berechtigungsprüfung (Autorisierung) eines Aufrufs ist gemäß Übergreifendem Konzept Sicherheitsarchitektur (AD-NOOTS-17) mittels Überprüfung der im Zugriffstoken enthaltenen Berechtigungen umgesetzt.

Bei jedem Aufruf einer der Nachweisabruf-API-Operationen wird überprüft, ob das Zugriffstoken die für die aktuelle API-Operation benötigten Berechtigungen enthält. Die Berechtigungen werden per Konfiguration für jede API-Operation in SAK-DC festgelegt.

Tabelle 10: SAK-DC: Standardkonfiguration mit benötigten Berechtigungen

API-Operation	Benötigte Berechtigungen
findEvidenceOffer	noots.nachweisangebot
getIdNr	noots.identifikationsnummer
getEvidenceDp	Alle folgenden (**UND**): noots.verbindungsparameter noots.abstrakteberechtigung nachweis.national

Berechtigungen sind nur im Zugriffstoken enthalten. Aus diesem Grund wird keine Berechtigungsprüfung für die API-Operation getAccessToken durchgeführt.

Tabelle 11: SAK-DP: Standardkonfiguration mit benötigten Berechtigungen

API-Operation	Benötigte Berechtigungen
findEvidence	Die Konfiguration der Berechtigungen (noots_dp_zugriff) ist in der Integrationsanleitung beschrieben

2.6. Verschlüsselung

Die Implementierung einer Verschlüsselung in IT-Systemen oder in Infrastrukturen zwischen beteiligten IT-Systemen dient der Absicherung gegenüber Zugriffen durch unbefugte Dritte. Sie ermöglicht die Erreichung der Gewährleistungsziele der Integrität und Vertraulichkeit. Derzeit existieren technisch verschiedene Arten der Verschlüsselung, abhängig vom Einsatzzweck sowie der Frage, was verschlüsselt werden soll. Beispielhaft ist vorab zu klären, ob eine Transport- oder Inhaltsverschlüsselung oder beides zur Risikominimierung erforderlich ist.

Vorliegend sind die Netzwerkverbindungen der IT-Systeme der Registerstellen mit dem zugehörigen SAK zu verschlüsseln; dies liegt jedoch in der Verantwortung der betriebsverantwortlichen Stelle in Zusammenwirken mit dem datenschutzrechtlichen Verantwortlichen und muss dort entsprechend dokumentiert werden. Zwischen den jeweiligen SAK und den übrigen Komponenten der NOOTS-Transportinfrastruktur wird eine Transportverschlüsselung auf Basis von TLS oder mTLS aufgebaut. Hierauf wird jeweils in Kapitel 4.1 der Systemdokumentation für SAK-DC und SAK-DP hingewiesen und im Folgenden abgebildet:

Sicherheitstechnisch wird auf das Zero Trust Prinzip gesetzt. Dabei handelt es sich um eine Sicherheitsphilosophie, die davon ausgeht, dass kein Benutzer, Gerät oder Netzwerksegment von Natur aus vertrauenswürdig ist. Es basiert auf der Annahme, dass Bedrohungen sowohl innerhalb als auch außerhalb des Netzwerks lauern können und daher jede Zugriffsanfrage auf Ressourcen streng überprüft und authentifiziert werden muss. Details zur Umsetzung sind im Kapitel 2.5 Authentifizierung und Autorisierung dieser Dokumentation festgehalten.

Als Authentifizierungs- und Autorisierungsverfahren werden OAuth 2.0 und Basic-Auth verwendet. Eine entsprechende Zuordnung zu den betroffenen eingehenden Schnittstellen ist in dem Kapitel Authentifizierung aufzufinden. Zur Verschlüsselung der Übertragung

bei eingehenden und ausgehenden Anfragen selbst werden TLS und mTLS verwendet.

SAK-DC: Dies betrifft sowohl die Anfragen zu den NOOTS-Kernkomponenten, als auch Anfragen gegen einen entsprechenden Data Provider.

2.7. Datensparsamkeit

Folgend dem Ansatz *Privacy by Design* und *Privacy by Default* nach Artikel 25 Abs. 1 u. 2 DSGVO ist eine Datenverarbeitung entsprechend dem Prinzip der Datenminimierung so zu gestalten, dass lediglich der minimal notwendige Umfang an personenbezogenen Daten zur Zweckerfüllung, unter Berücksichtigung der einschlägigen Rechtsvorschriften, verarbeitet wird. Des Weiteren ist ein Prozess zu implementieren, der sicherstellt, dass personenbezogene Daten unverzüglich gelöscht werden, sofern der Zweck entfallen ist, gesetzliche Auffangnormen für eine Anschlussverarbeitung nicht vorliegen, oder gesetzliche Aufbewahrungsfristen einer Löschung nicht entgegenstehen. Die Datensparsamkeit folgt dem Grundsatz der Zweckbindung und der Gewährleistung der Nichtverkettung.

Vorliegend werden personenbezogene Daten in Form von Nachweisen auf dem Transportwege durch einen SAK durchgeleitet und nicht persistent gespeichert (siehe Kapitel 2.4 dieser Dokumentation). Eine entsprechende Dokumentation der abschließenden Implementierung ist durch die betriebsverantwortliche Stelle zu erstellen und vom datenschutzrechtlichen Verantwortlichen entsprechend abzunehmen.

2.8. Datenlöschung

In Bezug auf das europäische Datenschutzrecht definiert der Begriff „Löschen“ die Unkenntlichmachung gespeicherter personenbezogener Daten. Der Vorgang des Löschens bewirkt, dass nach einer Löschung Informationen nicht mehr vorhanden sind, mit denen eine natürliche Person identifiziert werden kann. Eine Löschung hat zu erfolgen, sofern der Zweck einer Datenverarbeitung erfüllt ist und gesetzliche Aufbewahrungsfristen der Löschung nicht entgegenstehen. Die Datenlöschung ist eine Maßnahme zur Datenminimierung.

Vorliegend besteht, wie bereits unter Ziffer 2.7 dieser Dokumentation dargelegt, aufgrund der Art der Verarbeitungstätigkeiten keine Datenspeicherung im SAK und deshalb auch kein rechtlicher Grund für eine Datenlöschung (Siehe Kapitel 2.4 dieser Dokumentation).

3. Ebene 3 SDM – Infrastruktur

SAKs sind eine Schnittstelle zu den dahinterliegenden IT-Systemen. Hinter einem SAK-DC liegt in der Regel ein Online-Dienst oder ein Fachverfahren. Über diesen stellen die Antragsteller einen Antrag aus der Leistungsverwaltung einer Behörde, oder die Sachbearbeiter einer Behörde rufen die für die Bearbeitung eines Verwaltungsverfahrens erforderlichen Daten bei Dritten ab. Der SAK-DC ruft die Teile der NOOTS-Transportinfrastruktur zum Abruf der Daten auf. Dagegen verbindet ein SAK-DP das datenhaltende IT-System einer Registerbehörde (Register) mit der NOOTS-Transportinfrastruktur. Die jeweiligen SAKs werden somit dezentral durch die jeweiligen datenschutzrechtlichen Verantwortlichen betrieben.

3.1. Grundlegendes

Folgend der Beschreibung der verwendeten Fachanwendung sowie der umgesetzten organisatorischen Maßnahmen wird auf Ebene drei die NOOTS-Transportinfrastruktur sowie deren Administration und die Anforderungen an einen sicheren Betrieb in den Modulen betrachtet. Die Auswahl, die Implementierung sowie Konfiguration eines SAK für den Betrieb in einer Infrastruktur liegt jedoch in der abschließenden Verantwortung eines Verantwortlichen einer Registerbehörde oder eines Verantwortlichen für einen Online-Dienst oder Fachverfahren. Folglich können hier keine Aussagen über Art, Struktur, Zusammenwirken der beteiligten IT-Systeme, Position des SAK sowie daraus abgeleitet mögliche Risiken für Betroffene im Rahmen der Beantragung einer Leistung getroffen werden. Dies liegt, wie oben schon erwähnt, im Pflichten- und Zuständigkeitsbereich des jeweiligen Verantwortlichen. An dieser Stelle findet daher lediglich eine Betrachtung der von Seiten der NOOTS-Transportinfrastruktur getroffenen Maßnahmen statt, damit später eine Bewertung der Sicherheit durch den Verantwortlichen erfolgen kann.

Eine umfangreiche Betrachtung hinsichtlich der Gewährleistung eines möglichst störungsfreien Betriebs und einer zügigen Wiederherstellung des Normalbetriebs nach einem Störfall liefert auch das Sicherheitskonzept nach BSI – IT-Grundschutz. Die Ergebnisse des Sicherheitskonzepts können daher als mitgeltend zu dieser Dokumentation betrachtet und für die abschließende datenschutzrechtliche Bewertung durch den Verantwortlichen herangezogen werden.

3.2. Technische und organisatorische Maßnahmen

Das BVA ist Registeroberbehörde und Auftraggeber zur Entwicklung der NOOTS-Transportinfrastruktur sowie der hierfür erforderlichen einzelnen Module, zu denen auch im weiteren Sinne der SAK-DC und SAK-DP gehören. Vom BVA wurden unter dem Gesichtspunkt der Informationssicherheit sowie des Datenschutzes anhand der aus ihrer Sicht im Zusammenhang mit täglichen Arten beantragter Leistungen und übermittelter Daten mögliche Risiken und risikominimierende Maßnahmen definiert. Hieraus leitet sich das Schutzbedarf-Level ‚Hoch' ab. Dieses Level ist ein Basislevel. Die definierten und umgesetzten Maßnahmen dienen ebenfalls teilweise der Gewährleistung des Datenschutzes. Daher werden sie hier dargestellt und einzelnen SDM-Gewährleistungszielen zugeordnet.

Wie zuvor mehrmals dargelegt, ist davon auszugehen, dass ein Verantwortlicher vor Einsatz einer SAK-Version in seinem Verantwortungsbereich eine individuelle Risikobetrachtung vorzunehmen hat. In deren Verlauf hat er zu ermitteln, ob neben den bereits angeführten risikominimierenden Maßnahmen weitere Risiken festgestellt wurden, die gesonderte zusätzliche Maßnahmen zur Risikominimierung erfordern. Nachstehend sind bereits vorliegende risikominimierende Maßnahmen aufgeführt und den datenschutzrechtlichen SDM-Gewährleistungszielen zugeordnet. Die Maßnahmen resultieren aus Anforderungen des BSI-Grundschutzes, wirken sich jedoch ebenfalls risikominimierend im Datenschutz aus.

3.2.1 Vertraulichkeit

- Authentisierung via mTLS und OAuth2 für SAK-DP und SAK-DC
- Ausnahme: An dem Token-Endpunkt für den SAK-DC wird BasicAuth eingesetzt.
- Es wird sichergestellt, dass nur kontrollierte Daten ausgeliefert werden.
- Eingehende Daten werden gegen die OPEN API Spec. geprüft.
- Nur die Anwendung kann Daten im Arbeitsspeicher lesen. Andere Prozesse haben darauf keinen Zugriff (Betriebssystemverschlüsselung der Prozesse).
- Die Verschlüsselung zwischen den jeweiligen SAK-DC und SAK-DP erfolgt mittels mTLS 1.3.

- Es werden nur Funktionen oder Ressourcen aktiviert, die für den Einsatzzweck notwendig sind.

- Der SAK DC / DP erstellt Protokolle / Logs für relevante Ereignisse.

- Die Standardeinstellungen der SAK sehen vor, dass keine Nutzdaten für die betriebsverantwortlichen Stelle geloggt werden.

- Für den Prozess der Entwicklung der Software wurden frühzeitig Sicherheitsanforderungen mit Hilfe der CON.8 und CON.10- Bausteine ermittelt und deren Umsetzung geplant. Das Ergebnis kann im Sicherheitskonzept nachgeprüft werden.

- Die OAuth2-Token-Prüfung stellt sicher, dass nur die Aktionen ausgeführt werden können, zu denen der Inhaber eines Tokens berechtigt ist.

- Zugriffe werden bei fehlerhafter Zugriffskontrolle abgelehnt.

- Installation der jeweiligen SAK DC / DP config-Datei zur Versetzung der SAK nach Installation in eine Standard-Konfiguration

3.2.2 Integrität

- Authentisierung via mTLS und OAuth2 für SAK-DP und SAK-DC

- Ausnahme: An den Token-Endpunkt für den SAK-DC wird BasicAuth eingesetzt.

- Daten im Arbeitsspeicher kann nur die Anwendung lesen. Andere Prozesse haben darauf keinen Zugriff (Betriebssystemverschlüsselung der Prozesse).

- Die Verschlüsselung zwischen den jeweiligen SAK-DC und SAK-DP erfolgt mittels mTLS 1.3.

- Es werden nur Funktionen oder Ressourcen aktiviert, die für den Einsatzzweck notwendig sind.

- Für den Prozess der Entwicklung der Software wurden frühzeitig Sicherheitsanforderungen mit Hilfe der CON.8- und CON.10-Bausteine ermittelt und deren Umsetzung geplant. Das Ergebnis kann im Sicherheitskonzept nachgeprüft werden.

- Die OAuth2-Token-Prüfung stellt sicher, dass nur die Aktionen ausgeführt werden können, zu denen der Inhaber eines Tokens berechtigt ist.

- Zugriffe werden bei fehlerhafter Zugriffskontrolle abgelehnt.

- Installation der jeweiligen SAK DC / DP config-Datei zur Versetzung der SAK nach Installation in eine Standard-Konfiguration.

- Der SAK DC / DP erstellt Protokolle/Logs für relevante Ereignisse.

3.2.3 Verfügbarkeit

- Im Quellcode wird konfiguriert, unter welcher Route eine Ressource zur Verfügung steht. Andere Routen sind ausgeschlossen. Änderungen sind durch statischen Code ausgeschlossen.

- Für den Prozess der Entwicklung der Software wurden frühzeitig Sicherheitsanforderungen mit Hilfe der CON.8- und CON.10-Bausteine ermittelt und deren Umsetzung geplant. Das Ergebnis kann im Sicherheitskonzept nachgeprüft werden.

- Der SAK DC / DP erstellt Protokolle / Logs für relevante Ereignisse.

3.2.4 Nichtverkettung

- Nur die Anwendung kann Daten im Arbeitsspeicher lesen. Andere Prozesse haben darauf keinen Zugriff (Betriebssystemverschlüsselung der Prozesse).

- Die Anwendung benötigt mTLS-Algorithmen. Diese werden anhand der einschlägigen BSI-Empfehlungen hierzu ausgewählt. Siehe hierzu BSI TR-02102. Das Ergebnis kann im Sicherheitskonzept nachgeprüft werden.

- Die OAuth2-Token-Prüfung stellt sicher, dass nur die Aktionen ausgeführt werden können, zu denen der Inhaber eines Tokens berechtigt ist.

- Zugriffe werden bei fehlerhafter Zugriffskontrolle abgelehnt.

3.2.5 Intervenierbarkeit

Wie bereits in dieser Dokumentation beschrieben, besteht im SAK aufgrund der technischen Gegebenheiten weder die technische noch gesetzliche Möglichkeit der Erfüllung der Rechte der Betroffenen nach Artikel 15 bis 22 DSGVO. Das Gewährleistungsziel der Intervenierbarkeit ist bereits vorher bei Antragstellung im Online-Dienst durch den datenschutzrechtlich Verantwortlichen umzusetzen und kann daher an dieser Stelle nicht weiter betrachtet werden.

3.2.6 Transparenz

- Der Einsatzzweck der Software ist definiert und in der HLA des BMI zu NOOTS dokumentiert. Im dort enthaltenen Datenflussdiagramm ist festgehalten, welche Informationen damit verarbeitet werden.

- Die Standardeinstellungen der SAK sehen vor, dass Nutzdaten für die betriebsverantwortlichen Stellen nicht geloggt werden.

3.2.7 Datenminimierung

- Es wird sichergestellt, dass nur kontrollierte Daten ausgeliefert werden. Eingehende Daten werden gegen die OPEN API Spec geprüft.

4. Abkürzungsverzeichnis

Abkürzung	Bezeichnung
Dataport AöR	Dataport Anstalt öffentlichen Rechts
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVA	Bundesverwaltungsamt
CD	Corporate Design
DC	Data Consumer
DP	Data Provider
DSFA	Datenschutz-Folgenabschätzung
DSGVO	Datenschutz-Grundverordnung
HLA	High Level Architecture
IAM-B	Identity Access Management Behörden
IDNrG	Gesetz zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung
NOOTS	National-Once-Only-Technical-System
TOM	Technische und organisatorische Maßnahmen
RDN	Register-Daten-Navigation
SAK	Sicherer-Anschluss-Knoten
SDM	Standard-Datenschutz-Modell

5. Quellenverzeichnis

1 AD-NOOTS-XX/AD-NOOTS-05-+Grobkonzept+IAM+für+Behörden.md · main · NOOTS / Public / AD-NOOTS / Architektur · GitLab

2 XÖV-Handbuch der öffentlichen Verwaltung

3 https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/AD-NOOTS-XX/AD-NOOTS-19_+Grobkonzept+Transportinfrastruktur.md?ref_type=heads

4 https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/AD-NOOTS-XX/AD-NOOTS-03_+High-Level-Architecture+_HLA_.md?ref_type=heads

5 https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/AD-NOOTS-XX/AD-NOOTS-01_+Anschlusskonzept+Data+Consumer+_DC_.md?ref_type=heads

6 https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/AD-NOOTS-XX/AD-NOOTS-02_+Anschlusskonzept+Data+Provider+_DP_.md?ref_type=heads

7 NOOTS / Public / AD-NOOTS / SAK APIs · GitLab

8 https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/AD-NOOTS-XX/AD-NOOTS-02_+Anschlusskonzept+Data+Provider+_DP_.md?ref_type=heads

9 High-Level-Architecture (HLA) Abbildung 4: https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/AD-NOOTS-XX/AD-NOOTS-03_+High-Level-Architecture+_HLA_.md?ref_type=heads

10 https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/AD-NOOTS-XX/AD-NOOTS-03_+High-Level-Architecture+_HLA_.md?ref_type=heads

11 https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/AD-NOOTS-XX/AD-NOOTS-03_+High-Level-Architecture+_HLA_.md?ref_type=heads

12 https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/AD-NOOTS-XX/AD-NOOTS-01_+Anschlusskonzept+Data+Consumer+_DC_.md?ref_type=heads

13 https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/AD-NOOTS-XX/AD-NOOTS-19_+Grobkonzept+Transportinfrastruktur.md?ref_type=heads

6. Abbildungsverzeichnis

7. Tabellenverzeichnis

8. Anhang

- Anlage 1 Schwellwertanalyse SAK

Sicherer Anschlussknoten des Data Consumers: Ereignisse

Schnittstellenereignisse

Tabelle 1. Schnittstellenereignisse

Loglevel	Typ	Log-Name	Ereignis	Beschreibung	Logausgabe
INFO	D	de.bund.bva.noots.sak.dc.controller.ZugriffsberechtigungController	Abruf eines Zugriffstoken war erfolgreich	Der Zugriffstoken für einen DC wurde erfolgreich abgerufen	Zugriffstoken erfolgreich für Data Consumer `component-id` abgerufen
ERROR	D	de.bund.bva.noots.sak.dc.logging.NootsExternalComponentErrorLogger	Abruf eines Zugriffstoken ist fehlgeschlagen	Der Zugriff auf die externe Komponente ist mit dem Fehler "Unauthorized" fehlgeschlagen	Beim Aufruf der Aktion 'Abruf des Zugriffstokens für den Data Consumer' ist ein Fehler aufgetreten: Der Aufruf der Komponente `IAM-B (Identitätsmanagement für Behörden)` war aufgrund eines Client-Fehlers nicht erfolgreich. Es wurde der Fehler-Code 401 mit der Nachricht 'Unauthorized' zurückgegeben.

Loglevel	Typ	Log-Name	Ereignis	Beschreibung	Logausgabe
ERROR	D	de.bund.bva.noots.sak.dc.logging.NootsExternalComponentErrorLogger	Abruf eines Zugriffstoken ist fehlgeschlagen	Der Zugriff auf die externe Komponente ist mit einem Verbindungsfehler fehlgeschlagen	Beim Aufruf der Aktion 'Abruf des Zugriffstokens für den Data Consumer' ist ein Fehler aufgetreten: Die Verbindung zu der Komponente `IAM-B (Identitätsmanagement für Behörden)` konnte nicht aufgebaut werden.
ERROR	D	de.bund.bva.noots.sak.dc.logging.NootsExternalComponentErrorLogger	Abruf eines Zugriffstoken ist fehlgeschlagen	Der Zugriff auf die externe Komponente ist mit einem Clientfehler fehlgeschlagen	Beim Aufruf der Aktion 'Abruf des Zugriffstokens für den Data Consumer' ist ein Fehler aufgetreten: Der Aufruf der Komponente `IAM-B (Identitätsmanagement für Behörden)` war aufgrund eines Client-Fehlers nicht erfolgreich. Es wurde der Fehler-Code `http-statuscode` mit der Nachricht `http-statusmessage` zurückgegeben.

Loglevel	Typ	Log-Name	Ereignis	Beschreibung	Logausgabe
ERROR	D	de.bund.bva.noots.sak.dc.logging.NootsExternalComponentErrorLogger	Abruf eines Zugriffstoken ist fehlgeschlagen	Der Zugriff auf die externe Komponente ist mit einem Serverfehler fehlgeschlagen	Beim Aufruf der Aktion 'Abruf des Zugriffstokens für den Data Consumer' ist ein Fehler aufgetreten: Der Aufruf der Komponente `IAM-B (Identitätsmanagement für Behörden)` war aufgrund eines Server-Fehlers nicht erfolgreich. Es wurde der Fehler-Code `http-statuscode` mit der Nachricht `http-statusmessage` zurückgegeben.
ERROR	D	de.bund.bva.noots.sak.dc.logging.NootsExternalComponentErrorLogger	Abruf eines Zugriffstoken ist fehlgeschlagen	Der Zugriff auf die externe Komponente ist mit einem ungekannten Fehler fehlgeschlagen	Beim Aufruf der Aktion 'Abruf des Zugriffstokens für den Data Consumer' ist ein Fehler aufgetreten: Der Aufruf der Komponente `IAM-B (Identitätsmanagement für Behörden)` war nicht erfolgreich. Es wurde folgender Fehler erzeugt: `error-message`.
ERROR	D	de.bund.bva.noots.sak.dc.controller.ZugriffsberechtigungController	Abruf eines Zugriffstoken ist fehlgeschlagen	IAM-B liefert eine leere Antwort im Response	IAM-B liefert eine leere Antwort.

Loglevel	Typ	Log-Name	Ereignis	Beschreibung	Logausgabe
INFO	D	de.bund.bva.noots.sak.dc.controller.NationalerNachweisabrufController	Abruf eines Zuständigkeitstoken war erfolgreich	Der Zuständigkeitstoken für einen DC wurde erfolgreich abgerufen	Zuständigkeitstoken erfolgreich für Data Consumer `dc-id` abgerufen
ERROR	D	de.bund.bva.noots.sak.dc.logging.NootsExternalComponentErrorLogger	Abruf eines Zuständigkeitstoken ist fehlgeschlagen	Der Zugriff auf die externe Komponente ist mit dem Fehler "Unauthorized" fehlgeschlagen	Beim Aufruf der Aktion 'Abruf der Nachweisangebote für den Data Consumer `dc-id` ' ist ein Fehler aufgetreten: Der Aufruf der Komponente `RDN (Registerdatennavigation)` war aufgrund eines Client-Fehlers nicht erfolgreich. Es wurde der Fehler-Code 401 mit der Nachricht 'Unauthorized' zurückgegeben.
ERROR	D	de.bund.bva.noots.sak.dc.logging.NootsExternalComponentErrorLogger	Abruf eines Zuständigkeitstoken ist fehlgeschlagen	Der Zugriff auf die externe Komponente ist mit einem Verbindungsfehler fehlgeschlagen	Beim Aufruf der Aktion 'Abruf der Nachweisangebote für den Data Consumer `dc-id` ' ist ein Fehler aufgetreten: Die Verbindung zu der Komponente `RDN (Registerdatennavigation)` konnte nicht aufgebaut werden.

Loglevel	Typ	Log-Name	Ereignis	Beschreibung	Logausgabe
ERROR	D	de.bund.bva.noots.sak.dc.logging.NootsExternalComponentErrorLogger	Abruf eines Zuständigkeitstoken ist fehlgeschlagen	Der Zugriff auf die externe Komponente ist mit einem Clientfehler fehlgeschlagen	Beim Aufruf der Aktion 'Abruf der Nachweisangebote für den Data Consumer `dc-id` ' ist ein Fehler aufgetreten: Der Aufruf der Komponente `RDN (Registerdatennavigation)` war aufgrund eines Client-Fehlers nicht erfolgreich. Es wurde der Fehler-Code `http-statuscode` mit der Nachricht `http-statusmessage` zurückgegeben.
ERROR	D	de.bund.bva.noots.sak.dc.logging.NootsExternalComponentErrorLogger	Abruf eines Zuständigkeitstoken ist fehlgeschlagen	Der Zugriff auf die externe Komponente ist mit einem Serverfehler fehlgeschlagen	Beim Aufruf der Aktion 'Abruf der Nachweisangebote für den Data Consumer `dc-id` ' ist ein Fehler aufgetreten: Der Aufruf der Komponente `RDN (Registerdatennavigation)` war aufgrund eines Server-Fehlers nicht erfolgreich. Es wurde der Fehler-Code `http-statuscode` mit der Nachricht `http-statusmessage` zurückgegeben.

Loglevel	Typ	Log-Name	Ereignis	Beschreibung	Logausgabe
ERROR	D	de.bund.bva.noots.sak.dc.logging.NootsExternalComponentErrorLogger	Abruf eines Zuständigkeitstoken ist fehlgeschlagen	Der Zugriff auf die externe Komponente ist mit einem ungekannten Fehler fehlgeschlagen	BBeim Aufruf der Aktion 'Abruf der Nachweisangebote für den Data Consumer `dc-id` ' ist ein Fehler aufgetreten: Der Aufruf der Komponente `RDN (Registerdatennavigation)` war nicht erfolgreich. Es wurde folgender Fehler erzeugt: `error-message`.
ERROR	D	de.bund.bva.noots.sak.dc.rdn.RdnDao	Abruf eines Zuständigkeitstoken ist fehlgeschlagen	RDN liefert eine leere Antwort im Response	RDN-Antwort enthält kein Zuständigkeitstoken im Body
ERROR	D	de.bund.bva.noots.sak.dc.rdn.RdnResponseParser	Abruf eines Zuständigkeitstoken ist fehlgeschlagen	Zuständigkeitstoken konnte nicht geparsed werden	Zuständigkeitstoken konnte nicht validiert und geparsed werden.
ERROR	D	de.bund.bva.noots.sak.dc.rdn.RdnResponseParser	Abruf eines Zuständigkeitstoken ist fehlgeschlagen	Zuständigkeitstoken enthält nicht die geforderten Werte	Claim ist invalide oder keine Liste.
ERROR	D	de.bund.bva.noots.sak.dc.rdn.RdnResponseParser	Abruf eines Zuständigkeitstoken ist fehlgeschlagen	Token konnte nicht validiert oder geparsed werden	Fehler beim Parsen des Zuständigkeitstoken.

Loglevel	Typ	Log-Name	Ereignis	Beschreibung	Logausgabe
ERROR	D	de.bund.bva.noots.sak.dc.rdn.RdnResponseParser	Abruf eines Zuständigkeitstoken ist fehlgeschlagen	Token konnte nicht validiert oder geparsed werden	Fehler beim Laden des Bundles
ERROR	D	de.bund.bva.noots.sak.dc.rdn.RdnResponseParser	Abruf eines Zuständigkeitstoken ist fehlgeschlagen	Token konnte nicht validiert oder geparsed werden	Fehler beim Laden der Zertifikatskette
ERROR	D	de.bund.bva.noots.sak.dc.rdn.RdnResponseParser	Abruf eines Zuständigkeitstoken ist fehlgeschlagen	Token konnte nicht validiert oder geparsed werden	Fehler beim Parsen des JWT
ERROR	D	de.bund.bva.noots.sak.dc.rdn.RdnResponseParser	Abruf eines Zuständigkeitstoken ist fehlgeschlagen	Token konnte nicht validiert oder geparsed werden	Zertifikatskette des JWT konnte nicht durch Truststore validiert werden.
ERROR	D	de.bund.bva.noots.sak.dc.rdn.RdnResponseParser	Abruf eines Zuständigkeitstoken ist fehlgeschlagen	Token konnte nicht validiert oder geparsed werden, da der Truststore nicht gelesen werden konnte	Fehler beim Zugriff auf den Truststore.

Loglevel	Typ	Log-Name	Ereignis	Beschreibung	Logausgabe
ERROR	D	de.bund.bva.noots.sak.dc.logging.NootsExternalComponentErrorLogger	Abruf eines Verbindungstoken ist fehlgeschlagen	Der Zugriff auf die externe Komponente ist mit dem Fehler "Unauthorized" fehlgeschlagen	Beim Aufruf der Aktion 'Abruf der Verbindungstoken für den Data Consumer `dc-id` ' ist ein Fehler aufgetreten: Der Aufruf der Komponente `RDN (Registerdatennavigation)` war aufgrund eines Client-Fehlers nicht erfolgreich. Es wurde der Fehler-Code 401 mit der Nachricht 'Unauthorized' zurückgegeben.
ERROR	D	de.bund.bva.noots.sak.dc.logging.NootsExternalComponentErrorLogger	Abruf eines Verbindungstoken ist fehlgeschlagen	Der Zugriff auf die externe Komponente ist mit einem Verbindungsfehler fehlgeschlagen	Beim Aufruf der Aktion 'Abruf der Verbindungstoken für den Data Consumer `dc-id` ' ist ein Fehler aufgetreten: Die Verbindung zu der Komponente `RDN (Registerdatennavigation)` konnte nicht aufgebaut werden.

Loglevel	Typ	Log-Name	Ereignis	Beschreibung	Logausgabe
ERROR	D	de.bund.bva.noots.sak.dc.logging.NootsExternalComponentErrorLogger	Abruf eines Verbindungstoken ist fehlgeschlagen	Der Zugriff auf die externe Komponente ist mit einem Clientfehler fehlgeschlagen	Beim Aufruf der Aktion 'Abruf der Verbindungstoken für den Data Consumer `dc-id` ' ist ein Fehler aufgetreten: Der Aufruf der Komponente `RDN (Registerdatennavigation)` war aufgrund eines Client-Fehlers nicht erfolgreich. Es wurde der Fehler-Code `http-statuscode` mit der Nachricht `http-statusmessage` zurückgegeben.
ERROR	D	de.bund.bva.noots.sak.dc.logging.NootsExternalComponentErrorLogger	Abruf eines Verbindungstoken ist fehlgeschlagen	Der Zugriff auf die externe Komponente ist mit einem Serverfehler fehlgeschlagen	Beim Aufruf der Aktion 'Abruf der Verbindungstoken für den Data Consumer `dc-id` ' ist ein Fehler aufgetreten: Der Aufruf der Komponente `RDN (Registerdatennavigation)` war aufgrund eines Server-Fehlers nicht erfolgreich. Es wurde der Fehler-Code `http-statuscode` mit der Nachricht `http-statusmessage` zurückgegeben.

Loglevel	Typ	Log-Name	Ereignis	Beschreibung	Logausgabe
ERROR	D	de.bund.bva.noots.sak.dc.logging.NootsExternalComponentErrorLogger	Abruf eines Verbindungstoken ist fehlgeschlagen	Der Zugriff auf die externe Komponente ist mit einem ungekannten Fehler fehlgeschlagen	Beim Aufruf der Aktion 'Abruf der Verbindungstoken für den Data Consumer `dc-id` ' ist ein Fehler aufgetreten: Der Aufruf der Komponente `RDN (Registerdatennavigation)` war nicht erfolgreich. Es wurde folgender Fehler erzeugt: `error-message`.
ERROR	D	de.bund.bva.noots.sak.dc.rdn.RdnDao	Abruf eines Verbindungstoken ist fehlgeschlagen	RDN liefert eine leere Antwort im Response	Es konnte kein Verbindungstoken abgerufen werden für Data Consumer `dc-id`
ERROR	D	de.bund.bva.noots.sak.dc.rdn.RdnDao	Abruf eines Verbindungstoken ist fehlgeschlagen	RDN liefert eine leere Antwort im Response	Fehler beim Abruf des Verbindungstokens
ERROR	D	de.bund.bva.noots.sak.dc.rdn.RdnResponseParser	Abruf eines Verbindungstoken ist fehlgeschlagen	Es wurde kein mTLS-Verbindungsparameter gefunden	mTLS-TransportMode nicht vorhanden!
ERROR	D	de.bund.bva.noots.sak.dc.rdn.RdnResponseParser	Abruf eines Verbindungstoken ist fehlgeschlagen	Verbindungstoken konnte nicht geparsed werden	Verbindungstoken konnte nicht validiert und geparsed werden.

Loglevel	Typ	Log-Name	Ereignis	Beschreibung	Logausgabe
ERROR	D	de.bund.bva.noots.sak.dc.rdn.RdnResponseParser	Abruf eines Verbindungstoken ist fehlgeschlagen	Verbindungstoken enthält nicht die geforderten Werte	Fehler während des Parsens der Verbindungsparameter.
ERROR	D	de.bund.bva.noots.sak.dc.rdn.RdnResponseParser	Abruf eines Verbindungstoken ist fehlgeschlagen	Token konnte nicht validiert oder geparsed werden	Fehler beim Parsen des Verbindungstokens.
ERROR	D	de.bund.bva.noots.sak.dc.rdn.RdnResponseParser	Abruf eines Verbindungstoken ist fehlgeschlagen	Token konnte nicht validiert oder geparsed werden	Fehler beim Laden des Bundles
ERROR	D	de.bund.bva.noots.sak.dc.rdn.RdnResponseParser	Abruf eines Verbindungstoken ist fehlgeschlagen	Token konnte nicht validiert oder geparsed werden	Fehler beim Laden der Zertifikatskette
ERROR	D	de.bund.bva.noots.sak.dc.rdn.RdnResponseParser	Abruf eines Verbindungstoken ist fehlgeschlagen	Token konnte nicht validiert oder geparsed werden	Fehler beim Parsen des JWT
ERROR	D	de.bund.bva.noots.sak.dc.rdn.RdnResponseParser	Abruf eines Verbindungstoken ist fehlgeschlagen	Token konnte nicht validiert oder geparsed werden	Zertifikatskette des JWT konnte nicht durch Truststore validiert werden.
ERROR	D	de.bund.bva.noots.sak.dc.rdn.RdnResponseParser	Abruf eines Verbindungstoken ist fehlgeschlagen	Token konnte nicht validiert oder geparsed werden, da der Truststore nicht gelesen werden konnte	Fehler beim Zugriff auf den Truststore.

Loglevel	Typ	Log-Name	Ereignis	Beschreibung	Logausgabe
INFO	D	de.bund.bva.noots.sak.dc.controller.NationalerNachweisabrufController	Abruf eines Nachweises war erfolgreich	Der Nachweis für einen DC wurde erfolgreich abgerufen	Nachweis erfolgreich für Data Consumer `dc-id` abgerufen
DEBUG	D	de.bund.bva.noots.sak.dc.controller.NationalerNachweisabrufController	Abruf eines Nachweises war erfolgreich	Der Versuch einen Nachweis abzurufen war erfolgreich	Nachweisabruf im `versuch`. Versuch war erfolgreich. Ermittelter-Endpoint: `dp-url`

Loglevel	Typ	Log-Name	Ereignis	Beschreibung	Logausgabe
ERROR	D	de.bund.bva.noots.sak.dc.logging.NootsExternalComponentErrorLogger	Abruf eines Nachweises ist fehlgeschlagen	Der Zugriff auf die externe Komponente ist mit dem Fehler "Unauthorized" fehlgeschlagen	Beim Aufruf der Aktion 'Abruf des Nachweises für Data-Consumer `dc-id` im `versuch`. Versuch über den Data-Provider `dp-id` mit dem ermittelten Endpunkt: `dp-url` ' ist ein Fehler aufgetreten: Der Aufruf der Komponente `SAK-DP (Sicherer Anschlussknoten eines Data-Providers)` war aufgrund eines Client-Fehlers nicht erfolgreich. Es wurde der Fehler-Code 401 mit der Nachricht 'Unauthorized' zurückgegeben. Es wurde die externe Komponente 'SAK-DP (Sicherer Anschlussknoten eines Data-Providers)' mit der Id `dp-id` aufgerufen.

Loglevel	Typ	Log-Name	Ereignis	Beschreibung	Logausgabe
ERROR	D	de.bund.bva.noots.sak.dc.logging.NootsExternalComponentErrorLogger	Abruf eines Nachweises ist fehlgeschlagen	Der Zugriff auf die externe Komponente ist mit einem Verbindungsfehler fehlgeschlagen	Beim Aufruf der Aktion 'Abruf des Nachweises für Data-Consumer `dc-id` im `versuch`. Versuch über den Data-Provider `dp-id` mit dem ermittelten Endpunkt: `dp-url` ' ist ein Fehler aufgetreten: Die Verbindung zu der Komponente `SAK-DP (Sicherer Anschlussknoten eines Data-Providers)` konnte nicht aufgebaut werden. Es wurde die externe Komponente 'SAK-DP (Sicherer Anschlussknoten eines Data-Providers)' mit der Id `dp-id` aufgerufen.

Loglevel	Typ	Log-Name	Ereignis	Beschreibung	Logausgabe
ERROR	D	de.bund.bva.noots.sak.dc.logging.NootsExternalComponentErrorLogger	Abruf eines Nachweises ist fehlgeschlagen	Der Zugriff auf die externe Komponente ist mit einem Clientfehler fehlgeschlagen	Beim Aufruf der Aktion 'Abruf des Nachweises für Data-Consumer `dc-id` im `versuch`. Versuch über den Data-Provider `dp-id` mit dem ermittelten Endpunkt: `dp-url` ' ist ein Fehler aufgetreten: Der Aufruf der Komponente `SAK-DP (Sicherer Anschlussknoten eines Data-Providers)` war aufgrund eines Client-Fehlers nicht erfolgreich. Es wurde der Fehler-Code `http-statuscode` mit der Nachricht `http-statusmessage` zurückgegeben. Es wurde die externe Komponente 'SAK-DP (Sicherer Anschlussknoten eines Data-Providers)' mit der Id `dp-id` aufgerufen.

Loglevel	Typ	Log-Name	Ereignis	Beschreibung	Logausgabe
ERROR	D	de.bund.bva.noots.sak.dc.logging.NootsExternalComponentErrorLogger	Abruf eines Nachweises ist fehlgeschlagen	Der Zugriff auf die externe Komponente ist mit einem Serverfehler fehlgeschlagen	Beim Aufruf der Aktion 'Abruf des Nachweises für Data-Consumer `dc-id` im `versuch`. Versuch über den Data-Provider `dp-id` mit dem ermittelten Endpunkt: `dp-url` ' ist ein Fehler aufgetreten: Der Aufruf der Komponente `SAK-DP (Sicherer Anschlussknoten eines Data-Providers)` war aufgrund eines Server-Fehlers nicht erfolgreich. Es wurde der Fehler-Code `http-statuscode` mit der Nachricht `http-statusmessage` zurückgegeben. Es wurde die externe Komponente 'SAK-DP (Sicherer Anschlussknoten eines Data-Providers)' mit der Id `dp-id` aufgerufen.

Loglevel	Typ	Log-Name	Ereignis	Beschreibung	Logausgabe
ERROR	D	de.bund.bva.noots.sak.dc.logging.NootsExternalComponentErrorLogger	Abruf eines Nachweises ist fehlgeschlagen	Der Zugriff auf die externe Komponente ist mit einem ungekannten Fehler fehlgeschlagen	Beim Aufruf der Aktion 'Abruf des Nachweises für Data-Consumer `dc-id` im `versuch`. Versuch über den Data-Provider `dp-id` mit dem ermittelten Endpunkt: `dp-url` ' ist ein Fehler aufgetreten: Der Aufruf der Komponente `SAK-DP (Sicherer Anschlussknoten eines Data-Providers)` war nicht erfolgreich. Es wurde folgender Fehler erzeugt: `error-message`. Es wurde die externe Komponente 'SAK-DP (Sicherer Anschlussknoten eines Data-Providers)' mit der Id `dp-id` aufgerufen.
WARN	D	de.bund.bva.noots.sak.dc.controller.NationalerNachweisabrufController	Abruf eines Nachweises ist fehlgeschlagen	Der Versuch einen Nachweis abzurufen ergab eine leere Antwort des SAK-DP	Nachweisabruf im `versuch`. Versuch lieferte leere Antwort. Ermittelter-Endpoint: `dp-url`
ERROR	D	de.bund.bva.noots.sak.dc.controller.NationalerNachweisabrufController	Abruf eines Nachweises ist fehlgeschlagen	Alle Versuche einen gültigen Nachweis abzurufen schlugen fehl	Es konnte kein Nachweis abgerufen werden für Data Consumer `dc-id`

Loglevel	Typ	Log-Name	Ereignis	Beschreibung	Logausgabe
ERROR	D	de.bund.bva.noots.sak.dc.controller.NationalerNachweisabrufController	Abruf eines Nachweises ist fehlgeschlagen	Alle Versuche einen gültigen Nachweis abzurufen schlugen fehl	Zugriff auf den SAK Data Consumer über die ermittelten Verbindungsparameter nicht möglich
WARN	D	de.bund.bva.noots.sak.dc.controller.NationalerNachweisabrufController	XNachweis Validierung fehlgeschlagen	Invalide XNachweis Abfrage oder Antwort	Liste der Validierungsfehler

Sicherheitsereignisse

Tabelle 2. Sicherheitsereignisse

Loglevel	Typ	Log-Name	Ereignis	Beschreibung	Logausgabe
INFO	E	de.bund.bva.noots.sak.dc.config.security.BearerTokenAuthenticationLoggerFilter	Erfolgreiche Anmeldung eines Data Consumers	Request von SAK-DC wurde erfolgreich authentifiziert und autorisiert	Erfolgreiche Anmeldung von Data Consumer `data_consumer_id`
DEBUG	E	de.bund.bva.noots.sak.dc.config.security.CustomBasicAuthFilter	Erfolgreiche Anmeldung eines Data Consumers mittels BasicAuth-Header	BasicAuth-Anmeldung wurde erfolgreich durchgeführt	Benutzername und Passwort sind korrekt

Loglevel	Typ	Log-Name	Ereignis	Beschreibung	Logausgabe
DEBUG	E	de.bund.bva.noots.sak.dc.config.security.CustomBasicAuthFilter	Anmeldung eines Data Consumers mittels BasicAuth-Header	Anmeldung wurde gestartet und Header ausgelesen	Ermittelter Authorization Header: `header-value`
DEBUG	E	de.bund.bva.noots.sak.dc.config.security.CustomBasicAuthFilter	Fehlgeschlagene Anmeldung mittels BasicAuth-Header	Basic-Auth ist aktiviert, aber es wurde kein Header gefunden	Basic Auth ist aktiviert, jedoch konnte kein Basic Authorization Schema im Header gefunden werden
DEBUG	E	de.bund.bva.noots.sak.dc.config.security.CustomBasicAuthFilter	Fehlgeschlagene Anmeldung mittels BasicAuth-Header	HTTP-Header konnte nicht korrekt gelesen werden	Fehler beim dekodieren des Basic Auth Headers
DEBUG	E	de.bund.bva.noots.sak.dc.config.security.CustomBasicAuthFilter	Fehlgeschlagene Anmeldung mittels BasicAuth-Header	Falsche Anmeldedaten (Benutzer nicht vorhanden)	Benutzer stimmt nicht überein: `username`
DEBUG	E	de.bund.bva.noots.sak.dc.config.security.CustomBasicAuthFilter	Fehlgeschlagene Anmeldung mittels BasicAuth-Header	Falsche Anmeldedaten (Passwort falsch)	Ermitteltes Passwort für den Benutzer `username` stimmen nicht mit im SAK hinterlegten Werten überein
DEBUG	D, E	de.bund.bva.noots.sak.dc.config.BearerTokenPropagationClientInterceptor	Weiterleiten des Zugriffstoken an externe Systeme (SAK-DP)	Token wird im internen HTTP-Client hinterlegt	Erweitere Request Header: `endpoint-url`

Loglevel	Typ	Log-Name	Ereignis	Beschreibung	Logausgabe
ERROR	E	de.bund.bva.noots.sak.dc.CurrentDataConsumer	System-Interne Verwendung des derzeit angemeldeten Nutzers	Während der Laufzeit der Anwendung konnte, die aktuellen Nutzerdaten nicht geladen werden	Authorization not found

Systemereignisse

Tabelle 3. Systemereignisse

Loglevel	Typ	Log-Name	Ereignis	Beschreibung	Logausgabe
INFO	C	de.bund.bva.noots.sak.dc.logging.SakDcEventListener	Start	Sobald die Anwendung gestartet ist und bereit Anfragen zu verarbeiten.	Komponente SAK-DC erfolgreich gestartet
INFO	C	Framework	Start	Startdauer der Anwendung (wird automatisch erzeugt!)	Started SakDcApplication in `startdauer` seconds (process running for `prozess-lebensdauer`)
INFO	C	de.bund.bva.noots.sak.dc.logging.SakDcEventListener	Ende	Sobald die Anwendung beendet wurde und somit keine Anfragen mehr verarbeiten kann.	Komponente SAK-DC erfolgreich beendet

Sicherer Anschlussknoten des Data Providers: Ereignisse

Tabelle 1. Schnittstellenereignisse

Loglevel	Typ	Log-Name	Ereignis	Beschreibung	Logausgabe
ERROR	D	de.bund.bva.noots.sak.dp.filter.HeaderValidationFilter	Validierung	Entspricht der Traceparent Header dem richtigen Format	Ungültige Traceparent-ID bei Zugriff von Data Consumer `data_consumer_id`
ERROR	D	de.bund.bva.noots.sak.dp.filter.HeaderValidationFilter	Validierung	Entspricht der X-Noots-Service-ID Header dem richtigen Format	Ungültige X-Noots-Service-ID bei Zugriff von Data Consumer `data_consumer_id`
ERROR	D	de.bund.bva.noots.sak.dp.filter.HeaderValidationFilter	Validierung	Entspricht der X-Noots-XNachweis-ID Header dem richtigen Format	Ungültige X-Noots-XNachweis-ID bei Zugriff von Data Consumer `data_consumer_id`
ERROR	D	de.bund.bva.noots.sak.dp.filter.RequestBodyValidationFilter	Validierung	Prüfung, ob ein Request-Body mit gesendet wurde	Leere Anfrage bei Zugriff von Data Consumer `data_consumer_id`
ERROR	D	de.bund.bva.noots.sak.dp.filter.RequestBodyValidationFilter	Validierung	Prüfung, ob alle Felder des Request-Body mit technisch gültigen Werten belegt wurden; detaillierte Fehlermeldungen bekommt nur der Aufrufer als HTTP 4xx Response	Ungültige Anfrage bei Zugriff von Data Consumer `data_consumer_id`

Loglevel	Typ	Log-Name	Ereignis	Beschreibung	Logausgabe
ERROR	D	de.bund.bva.noots.sak.dp.filter.ResponseInspectionFilter	Request an Data Provider	Request von SAK-DP an den Data Provider liefert keine oder eine leere Antwort	Nachweisabruf von Data Provider `data_consumer_id` schlägt fehl: keine Daten vom Data Provider
ERROR	D	de.bund.bva.noots.sak.dp.filter.ResponseInspectionFilter	Request an Data Provider	Request von SAK-DP an den Data Provider liefert einen unerwarteten Fehler	Nachweisabruf von Data Provider `data_consumer_id` schlägt fehl mit Fehlercode `HTTP Fehlercode - 4xx oder 5xx`
WARN	D	de.bund.bva.noots.sak.dp.filter.XNachweisValidationFilter	XNachweis Validierung fehlgeschlagen	Invalide XNachweis Abfrage	Liste der Validierungsfehler
WARN	D	de.bund.bva.noots.sak.dp.filter.ResponseInspectionFilter	ResponseBody konnte nicht geparsed werden	Konnte ResponseBody nicht zu EvidenceResponse parsen.	
WARN	D	de.bund.bva.noots.sak.dp.filter.ResponseInspectionFilter	XNachweis Validierung fehlgeschlagen	Invalide XNachweis Antwort	Liste der Validierungsfehler
INFO	D	de.bund.bva.noots.sak.dp.filter.ResponseInspectionFilter	Request an Data Provider	Der SAK-DP konnte die Nachweisdaten erfolgreich vom Data Provider abrufen	Nachweisabruf von Data Provider `data_consumer_id` erfolgreich

Sicherheitsereignisse

Tabelle 2. Sicherheitsereignisse

Loglevel	Typ	Log-Name	Ereignis	Beschreibung	Logausgabe
INFO	E	de.bund.bva.noots.sak.dp.filter.HeaderValidationFilter	Eingehenden Request verarbeiten	Request von SAK-DC wurde erfolgreich authentifiziert und autorisiert	Erfolgreiche Anmeldung von Data Consumer `data_consumer_id`
ERROR	E	de.bund.bva.noots.sak.dp.exception.handler.GlobalExceptionHandler	Eingehenden Request verarbeiten	Zugriffstoken wurde abgelehnt da entweder die Signatur oder etwaige Token Claims ungültig sind	Zugriffsproblem durch unzureichende Berechtigungen oder Authentifizierungsfehler von Data Consumer `data_consumer_id`
WARN	E	de.bund.bva.noots.sak.dp.config.security.CertificateThumbprintFilter	Eingehenden Request verarbeiten	Der eingehende Request enthält im konfigurierten HTTP Header nicht das Clientzertifikat vom SAK-DC	Kein Header mit SSL Client-Zertifikat gefunden
DEBUG	E	de.bund.bva.noots.sak.dp.config.security.CertificateThumbprintFilter	Eingehenden Request verarbeiten	Information über das Clientzertifikat welches im HTTP Header gefunden wurde	SSL Client-Zertifikat im Header gefunden `header_name`: Subject: `subject`, Issuer: `issuer`
ERROR	E	de.bund.bva.noots.sak.dp.exception.handler.GlobalExceptionHandler	Request an Data Provider	Request von SAK-DP an Data Provider liefert den Response Status **Unauthorized** oder **Forbidden**	Authentifizierung bei Nachweisabruf von Data Consumer `data_consumer_id` schlägt fehl

Systemereignisse

Tabelle 3. Systemereignisse

Loglevel	Typ	Log-Name	Ereignis	Beschreibung	Logausgabe
INFO	C	de.bund.bva.noots.sak.dp.logging.LoggingEventListener	Start	Sobald die Anwendung gestartet ist und bereit Anfragen zu verarbeiten.	Komponente SAK-DP erfolgreich gestartet
INFO	C	Framework	Start	Startdauer der Anwendung (wird automatisch erzeugt!)	Started SakDcApplication in `startdauer` seconds (process running for `prozess-lebensdauer`)
INFO	C	de.bund.bva.noots.sak.dp.logging.LoggingEventListener	Ende	Sobald die Anwendung beendet wurde und somit keine Anfragen mehr verarbeiten kann.	Komponente SAK-DP erfolgreich beendet