Bundesverwaltungsamt

Sicherer Anschlussknoten des Data Providers Integrationsanleitung

Bundesverwaltungsamt

Version 0.29.3, Datum 29.10.2026

Inhaltsverzeichnis

Änderungshistorie 1
1. Einleitung 1
2. Überblick 3
2.1. Fachliche Beschreibung 3
2.2. Technische Beschreibung 3
3. Installation der Anwendung für Server-Betrieb 5
3.1. Systemvoraussetzungen 5
3.2. Installation 5
4. Installation in einem Kubernetes-Cluster 10
4.1. Vorbereitung der Systemumgebung 10
4.2. Installation der Anwendung 12
4.3. Konfiguration der Anwendung 13
5. Deinstallation der Anwendung 15
5.1. Deinstallation im Server-Betrieb 15
5.2. Deinstallation in einem Kubernetes-Cluster 15
6. Regulärer Wirkbetrieb 16
6.1. Logging 16
6.2. Statusprüfung der Anwendungen 16
6.3. Monitoring 16
6.4. Backup und Recovery 17
6.5. Hinweise für Störungsdiagnose und -behandlung 17
Anhang 19
Anhang A: Technisches Glossar 19
Anhang B: Fachliches Glossar 19
Anhang C: Betrieblich-Relevante Konfigurationsparameter für Server-Betrieb 20
Anhang D: Helm Chart Values-Datei für Kubernetes-Betrieb 20
Quellen 38

Änderungshistorie

Version	Änderungen
0.1	• Initiale Erstellung des Dokuments
0.2	• Einarbeitung Review Kommentare
0.9	• Dokument finalisiert
1.0	• Dokument abgenommen

1.0.1	• Anpassungen in der Beispiel-Konfigurationsdatei
	  • Hinzufügen von Konfigurationsparametern für das Rate-Limiting der Anwendung
	  • Hinzufügen von Konfigurationsparametern für einen Truststore mit erlaubten Client-Zertifikaten ohne Zertifikatskette (Pinning)
	• Anpassung von neuen Links und Referenzen auf OpenCode

1.0.2	• Hinzufügen der Anleitung für Installation in einem Kubernetes-Cluster inklusive der zugehörigen Konfigurationsparameter
1.0.3	• Hinzufügen der Anleitung für die Deinstallation der Anwendung

1. Einleitung

Das vorliegende Dokument enthält die Integrationsanleitung für die Anwendung "**Sicherer Anschlussknoten des Data Providers**" (*SAK-DP*) in der jeweils aktuell veröffentlichten Version. Es fungiert als Hilfestellung für den Betrieb der Anwendung.

Das Kapitel Überblick bietet einen groben fachlichen, technischen sowie betrieblichen Überblick über die Anwendung und liefert Verweise auf weitergehende Dokumente.

Das Kapitel Installation der Anwendung für Server-Betrieb beschreibt die traditionelle Installation und Konfiguration der Anwendung in einer Server-Umgebung.
`Relevant für Betrieb und Softwareentwicklung`

Das Kapitel Installation in einem Kubernetes-Cluster beschreibt die Installation und Konfiguration der Anwendung in einem Kubernetes-Cluster.
`Relevant für Betrieb und Softwareentwicklung`

Das Kapitel Deinstallation der Anwendung beschreibt die Deinstallation der Anwendung in einer Server-Umgebung sowie in einem Kubernetes-

Cluster.
`Relevant für Betrieb`

Das Kapitel Regulärer Wirkbetrieb liefert Informationen für den Betrieb der Anwendung und gibt Hilfestellung bei der Fehleranalyse
`Relevant für Betrieb und Softwareentwicklung`

Der Anhang enthält ein fachliches und technisches Glossar sowie die Beschreibung der Konfigurationsdaten.

2. Überblick

In diesem Kapitel wird aus fachlicher und technischer Sicht ein Überblick über die Geschäftsprozesse gegeben, die mithilfe des SAK-DP durchgeführt werden.

2.1. Fachliche Beschreibung

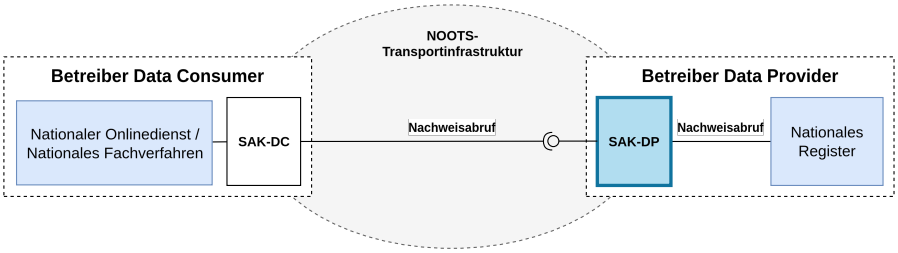


Abbildung 1. SAK-DP: Fachliche Kontextabgrenzung

Die fachlichen Aufgaben von SAK-DP sind:

- Prüfung von Identität und Berechtigung der abfragenden Stelle
- Prüfung und Weitergabe der Abruf-Anfrage an den Data Provider
- Weiterleitung des angefragten Nachweises an die anfragende Stelle

2.2. Technische Beschreibung

SAK-DP stellt Komponenten des NOOTS-Netzwerks einen sicheren Zugang zu einem Data Provider bereit. Hierzu fungiert die Anwendung als "Application Layer Gateway" durch:

- Bereitstellung einer öffentlichen REST-API (Transportprotokoll) für andere SAK-DC im Internet.
- Anbindung des Data Provider via das Anschlussprotokoll.

Zur Absicherung der Zugriffe auf Data Providers via das Anschlussprotokoll kommen "Basic Auth" und "OAuth 2.0" zum Einsatz, zur Absicherung der Netzwerk-Kommunikation "(m)TLS".

Die hierzu benötigten Zugangsdaten und Zertifikate müssen bei der Installation vom SAK-DP bereitgestellt werden.

HINWEIS

- Die Kommunikation des SAK-DP erfolgt direkt mit dessen Data Provider und den SAKs der Dara Consumer.
- Der europäische Datenfluss ist nicht Teil des MVP.

Weitere technische Details können im Anschlusskonzept Data Provider (AD-NOOTS-02)

> nachgelesen werden.

3. Installation der Anwendung für Server-Betrieb

Dieses Kapitel beschreibt die traditionelle Installation der Java-Anwendung auf einem Host-Server.

3.1. Systemvoraussetzungen

Die Systemvoraussetzungen für den Betrieb sind abhängig von der Anzahl der gleichzeitigen Zugriffe auf den SAK-DP. Je nach Mengengerüst können diese erheblich von den Mindestanforderungen abweichen.

Tabelle 1. Systemvoraussetzungen

Name	Mindestanforderungen
Java-JRE	JRE 21, getestet mit Adoptium Temurin
Betriebssystem	nicht vorgegeben, Konformität mit BSI-Grundschutz[1] wird vorausgesetzt
Arbeitsspeicher	1024MB
Speicherplatz	512MB
Prozessor	2 GHz Dual Core, 64-Bit
Netzwerk	Internetverbindung (direkt oder über Proxy) auf Port 443

3.2. Installation

WICHTIG Halten Sie sich hier an Ihre betrieblichen Vorgaben für einen sicheren Betrieb. Die hier beschriebenen Schritte dienen nur als Beispiel.

Der SAK-DP wird als ausführbare JAR-Datei (Java Archive) bereitgestellt.

Die JAR-Datei sollte in der Laufzeitumgebung abgelegt werden, in unserem Beispiel ist das `/opt/sak-dp`

Kopieren Sie die JAR-Datei mit der entsprechenden Version auf den Zielrechner, beispielsweise mit `scp`:

```
scp sak-dp-VERSION-TAG.jar admin@laufzeitumgebungshost:~
```

Loggen Sie sich per `ssh` auf dem Rechner ein:

```
ssh admin@laufzeitumgebungshost:~
```

Die Berechtigung sollte nur auf das Nötigste beschränkt werden, damit nur

der ausführende User der Serveranwendung Leserechte hat. In unserem Beispiel läuft die Serveranwendung mit dem User `sak-dp` der der Linux Gruppe `sak-dp` angehört.

```
sudo mkdir /opt/sak-dp
sudo chown root:sak-dp /opt/sak-dp
sudo chmod 750 /opt/sak-dp

sudo mv ~/sak-dp-VERSION-TAG.jar /opt/sak-dp

sudo chown root:sak-dp /opt/sak-dp/sak-dp-VERSION-
TAG.jar
sudo chmod 640 /opt/sak-dp/sak-dp-VERSION-TAG.jar
```

WICHTIG	Die Anwendung sollte unter keinen Umständen über den `root`-User des Systems, sondern idealerweise mittels eines eigenen Benutzers mit möglichst minimalen Rechten ausgeführt werden.

3.2.1. Start und Konfiguration der Anwendung

Die Konfigurationen des SAK-DP findet mittels einer bereitgestellten `application.properties` statt, welche auf die Laufzeitumgebung angepasst werden muss. Die Parameter sind in der Datei beschrieben und enthalten Beispielwerte, an denen sich orientiert werden kann. Die Konfigurationsdatei muss als Parameter übergeben werden. Die Dateirechte auf die Konfigurationsdatei sollten auch hier so gesetzt werden, sodass nur die Anwendung darauf zugreifen, aber nicht ändern kann.

```
java -jar sak-dp-VERSION-TAG.jar
--spring.config.additional
-location=application.properties
```

Weiterführende Hinweise zur Konfiguration

Im oben genannten Beispiel wird davon ausgegangen, dass die `application.properties`-Datei im identischen Verzeichnis wie die Anwendung (.jar) selbst liegt. Wenn die Konfiguration aus einem anderen Verzeichnis geladen werden soll, kann dieses sowohl relational, sowie absolut angegeben werden. Außerdem können mehrere Dateien, auch *optional* angegeben werden. Hier muss die Reihenfolge beachtet werden. Gleiche Konfigurationsschlüssel aus Dateien, welche früher in der Kette angegeben werden, werden

durch spätere Dateien überschrieben.

```
java -jar sak-dp-VERSION-TAG.jar
--spring.config.additional-location=\

  #Konfigurations-Datei im gleichen Ordner; muss
vorhanden sein
  application.properties,\

  #externe Konfigurations-Datei ; muss vorhanden
sein
  /opt/default.properties,\

  #externe Konfigurations-Datei ; optional,
produziert keinen Fehler, wenn nicht vorhanden
  optional:/opt/optional.properties
```

Weitere Informationen zu der Angabe von externen Konfigurationen können der offiziellen Spring Boot Dokumentation; Kapitel "Externalized Configuration"; Abschnitt "External Application Properties" entnommen werden.

Die Anwendung sollte nun gestartet sein und folgende Meldung in der Ausgabe erscheinen:

```
SAK-Komponente erfolgreich gestartet
```

3.2.2. Endpunkte

In der Standardkonfiguration ist die Serveranwendung über Port **8080** sowie der Managementendpunkt über Port **9000** erreichbar.

WICHTIG	Diese Netzwerkports sollten über geeignete Firewallregeln abgesichert werden, um unbefugten Zugriff zu unterbinden. Halten Sie sich auch hier an Ihre betrieblichen Vorgaben für einen sicheren Betrieb.

In den offiziellen Test- und Produktionsumgebungen von NOOTS ist es verpflichtend, die Endpunkte nicht ungeschützt und unverschlüsselt zu betreiben. Es können hierbei verschiedenen Varianten genutzt werden. Je nach vorhandener Infrastruktur kann auch ein Betrieb hinter einem Proxy sinnvoll sein. In einer lokalen Teststellung ohne Anbindung gegen das NOOTS-System (z.B. mittels Mocks) können die Endpunkte auch weniger abgesichert betrieben werden.

Tabelle 2. Absicherung der Endpunkte

Art	Erklärung
HTTPS	Die Konfiguration erfolgt über die `application.properties`
mTLS	Die Konfiguration erfolgt über die `application.properties`
HTTP Basic-Auth	Die Konfiguration erfolgt über die `application.properties`
Die obigen Methoden können bei Bedarf durch Apache-, Nginx oder einen anderen geeigneten Reverse Proxy abgebildet werden	Die Konfiguration erfolgt über das externe genutzte System

In jedem Fall ist die Nutzung von TLS 1.3 für die Kommunikation zwischen dem Data Provider und dem SAK-DP verpflichtend! Dies wurde in der Technische Richtlinie BSI TR-03190 im Punkt DCDP.6 festgelegt:

> [...] TLS MUSS in der Version 1.3 verwendet werden.
>
> — BSI TR-03190, DCDP.6

3.2.3. Timeouts

Timeouts können für die maximale Dauer einer Anfrage (`connect-timeout`) und die maximale Wartezeit auf die dazugehörige Antwort (`read-timeout`) festgelegt werden. Die Tabelle Timeouts des SAK-DP zeigt den Zusammenhang zwischen den Schritten und Zeiten, welche in Tabelle 9 der High-Level-Architecture (AD-NOOTS-03) spezifiziert sind, und den Konfigurationsparametern in der `application.properties`, über welche sich die Timeouts anpassen lassen.

WICHTIG

Die Konfigurationsparameter sind standardmäßig so eingestellt, dass sie den maximalen Zeiten aus der Anforderung entsprechen. Eine Lockerung der Timeout-Werte widerspricht damit den Anforderungen und beeinflusst das gesamte NOOTS-System, da andere Teilnehmer sich nicht mehr auf die angegebenen Bearbeitungs- und Kommunikationszeiten verlassen können! Diese Teilnehmer geraten dann selbst in Timeout-Probleme und müssten ebenfalls ihre Konfiguration - den Anforderungen widersprechend - anpassen. Im schlimmsten Fall wird das gesamte NOOTS-System stark verlangsamt. Es ist daher von höchster Wichtigkeit, dass die Timeouts nur verschärft, aber nicht gelockert werden.

Für die maximale Dauer einer Anfrage ist nur die Kommunikationsdauer aus der Anforderung relevant. Die Schritte sind entsprechend in der Tabelle gekennzeichnet. Die Timeouts sind nach Server gruppiert, an welche der SAK-DP als Client Anfragen sendet.

WICHTIG

Eine Besonderheit muss bei dem `sakdp.client.connect-timeout` beachtet werden: Der Wert darf in der `application.properties` nicht mit einer Einheit angegeben werden. Stattdessen muss eine positive ganze Zahl gewählt werden, welche immer als Zeit in Millisekunden interpretiert wird. Leider gibt es hier keine andere Konfigurationsmöglichkeit.

Tabelle 3. Timeouts des SAK-DP

Schritt	Server	Timeout	Konfigurationsparameter
5.7 Nachweis abrufen (Kommunikationsdauer)	DP	`0,5s`	`sakdp.client.connect-timeout`
5.8 Nachweis bereitstellen		`3,5s`	`sakdp.client.read-timeout`

3.2.4. Start und Stop

Damit die Anwendung nicht immer manuell über die Konsole gestartet werden muss, können Mittel wie zum Beispiel systemd oder init.d genutzt werden.

Wir empfehlen hierzu die offizielle Spring Boot Dokumentation; Kapitel "Installing Spring Boot Applications".

4. Installation in einem Kubernetes-Cluster

4.1. Vorbereitung der Systemumgebung

Dieses Kapitel beschreibt, welche Vorbereitungen für den Betrieb der Anwendung Sicherer Anschlussknoten des Data Providers (SAK-DP) in der Systemumgebung nötig sind.

4.1.1. Kubernetes Laufzeitumgebung

SAK-DP ist für das Deployment auf einer Kubernetes-konformen Container-Orchestrierungsplattform vorgesehen. Die Laufzeitumgebung muss dem BSI-Grundschutz[1] entsprechen, insbesondere der Baustein "APP4.4 Kubernetes" ist zu beachten.

Falls die "Deutsche Verwaltungscloud"[2] genutzt werden soll, sind die entsprechenden FITKO-Richtlinien[3] zu beachten.

4.1.2. Verifzierung der Attestate am Container-Image

Die SBOMs und CVE-Reporte sind als Metadaten am Container-Image attestiert[4]. Vor einem Deployment müssen die Attestate an jedem Image verifiziert werden, um sicherzustellen, dass das Image unverändert und geprüft ausgeliefert wurde. Das folgende Beispiel zeigt die Verifikation mittels **Cosign**. Dabei müssen der Public-Key und der Repository-Pfad des Images angegeben werden.

Verifizierung attestierter Metadaten.

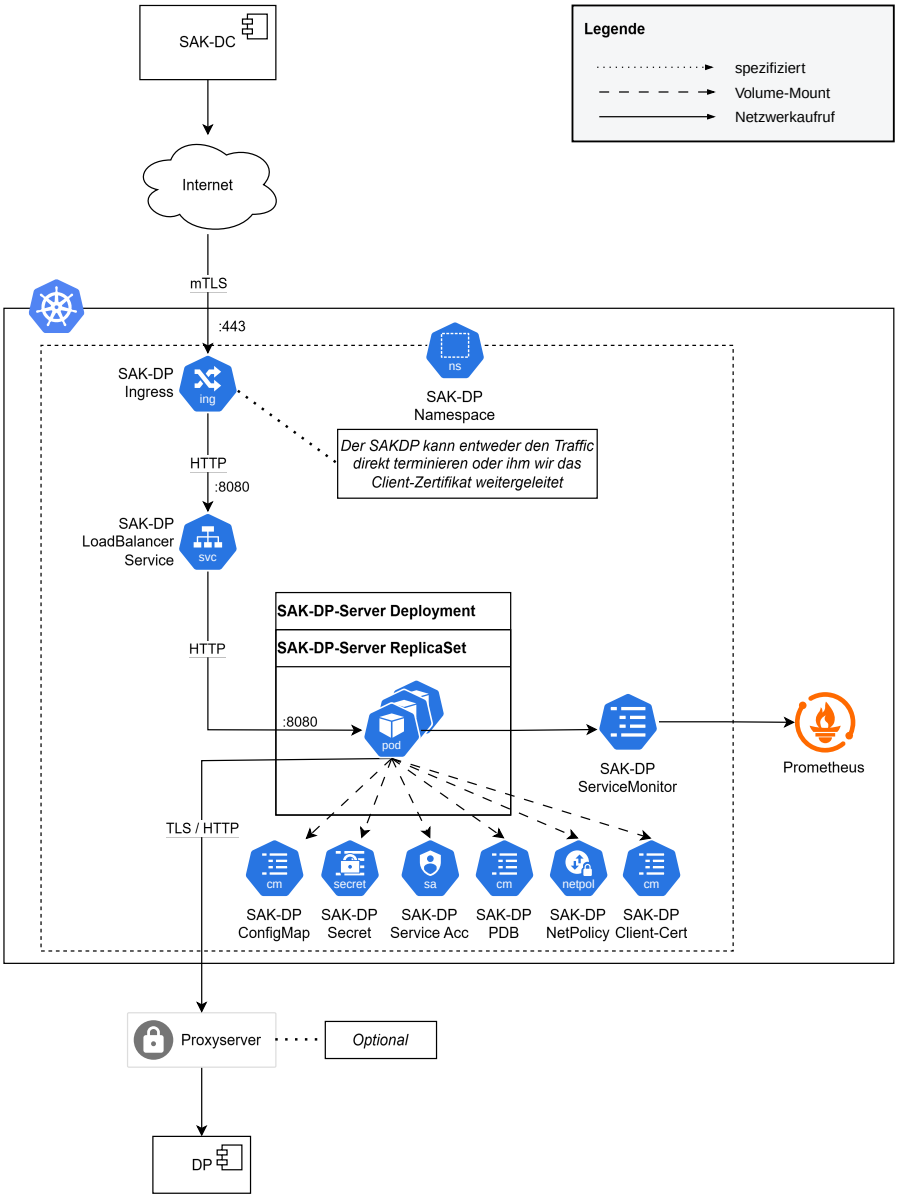
```
cosign verify-attestation \
    --key $PUBLIC_KEY \
    --insecure-ignore-tlog=true \
    --type=vuln \
    $IMAGE_REPOSITORY_PATH
```

> **TIP** Gleichermaßen kann mit der Option `--type=sbom` die SBOM verifiziert werden.

Aktuell wurde der Ablageort des hier verwendeten Public-Keys noch nicht festgelegt. Somit ist die Prüfung mit **Cosign** noch nicht möglich.

4.1.3. Konfiguration des Kubernetes Clusters

Die untere Abbildung zeigt die zur Verfügung gestellten Kubernetes Ressourcen.



Ein Kubernetes Namespace muss für den Sicherer Anschlussknoten des Data Providers angelegt werden. Alternativ, kann der Namespace während der Installation der Anwendung erstellt werden.

Ressourcenlimits

Die Helm-Charts von SAK-DP definieren Standard-Ressourcenlimits. Das Cluster muss dementsprechend ausreichend CPU und RAM bereitstellen.

Verschlüsselung sensibler Daten

Um die Sicherheit sensibler Daten im Cluster zu gewährleisten, muss die Verschlüsselung des `etcd`-Datenspeichers aktiviert werden. `etcd` ist die zentrale Schlüssel-Wert-Datenbank, in der Kubernetes neben anderen Informationen auch vertrauliche Daten wie Secrets ablegt. Ohne aktivierte Verschlüsselung würden diese Daten im Klartext vorliegen. Für weitere

Informationen diesbezüglich kann die Kubernetes Dokumentation[5] herangezogen werden.

Vorbereitung mTLS-Terminierung beim SAK-DP

Es ist möglich, das Helm-Chart des SAK-DP für eine mTLS-Terminierung im Ingress als auch beim SAK-DP selbst zu konfigurieren. Die Konfiguration wird im Abschnitt Konfiguration der mTLS-Terminierung beschrieben. Zusätzlich zur Konfiguration des SAK-DP und des Ingress-Objekts sind möglicherweise auch Konfigurationen am gewählten Ingress-Controller notwendig. Diese sollten in der Dokumentation des entsprechenden Ingress-Controllers nachgelesen werden.

TIP

Wenn die mTLS-Verbindung erst im SAK-DP terminieren soll, muss in der Regel das sogenannte „SSL-Passthrough“ eingerichtet werden. Unter diesem Stichpunkt sollten in der jeweiligen Dokumentation weitere Informationen zu finden sein.

4.2. Installation der Anwendung

SAK-DP wird als OCI Container-Image und Helm-Charts bereitgestellt. Diese befinden sich im Auslieferung-OCI-Repository und können von dort bezogen werden.

Die Installation der Anwendung erfolgt mittels des Kommandozeile-Tools `helm`. Angenommen die Helm-Charts für SAK-DP sind in `$RELEASE_REPOSITORY` vorhanden, zeigt das folgende Beispiel die Installation eins der beiden Anwendungen:

Installation der IT-Systeme

```
helm upgrade "$APP_RELEASE"
"oci://$RELEASE_REPOSITORY/$APP_HELM_CHART_NAME" \
    --version "$APP_HELM_CHART_VERSION" \
    --install \
    --namespace "$APP_NAMESPACE" \
    --values "$APP_VALUES"
```

Weitere Optionen können aus der Dokumentation zum `helm upgrade`[6] entnommen werden.

TIP

Durch die Option `--install` kann der Befehl auch für die erstmalige Installation, verwendet werden.

4.3. Konfiguration der Anwendung

Die Konfigurationen von SAK-DP findet mittels einer Helm Values-Datei[7] statt.

Die Helm Values-Dateien können dem Anhang entnommen werden: Anhang D: Helm Chart Values-Datei für Kubernetes-Betrieb

WICHTIG	Mit "@erforderlich" gekennzeichnete Parameter müssen durch eine überschreibende Values-Datei oder per "--set"-Option gesetzt werden. Zur Anpassung des Deployments in der vorgesehenen Umgebung müssen ggf. auch weitere Parameter angepasst werden.

4.3.1. Timeouts

Die Timeouts können in der Helm Values-Datei über die Konfigurationsparameter `sakdp.client.*` eingestellt werden. Im obigen Abschnitt Timeouts für die Installation des SAK-DP im Server-Betrieb sind weitere Informationen zu finden, welche gleichermaßen auch für den Cluster-Betrieb gelten.

4.3.2. Konfiguration der mTLS-Terminierung

Für die mTLS-Terminierung gibt es die folgenden zwei Konfigurationsmöglichkeiten:

1. Die mTLS-Terminierung findet im Ingress-Controller statt.
2. Die mTLS-Terminierung findet beim SAK-DP statt.

Standardmäßig ist die Terminierung im Ingress-Controller konfiguriert. Für die Umstellung gibt es einen zentralen Parameter in der `values.yaml`:

```
sakdp:
  server:
    ssl:
      enabled: true/false
```

Hier kann mittels `sakdp.server.ssl.enabled: true` die mTLS-Terminierung im SAK-DP aktiviert werden.

In diesem Fall ist es außerdem notwendig, dass der entsprechende Key- und Truststore für den SAK-DP konfiguriert werden. Dies erfolgt über `sakdp.server.keystore.*` bzw. `sakdp.server.truststore.*`. Zusätzlich müssen zwei Ports angepasst werden:

Konfigurationsparameter	Wert
`service.port`	8443
`networkPolicy.ingress[0].ports[0].port`	8443

WICHTIG

Falls die Terminierung zu einem späteren Zeitpunkt wieder im Ingress-Controller und nicht mehr beim SAK-DP erfolgen soll, müssen die Ports auf `8080` zurückgesetzt werden.

Abhängig von dem Ingress-Controller im Cluster muss gegebenenfalls das Ingress-Objekt auch für SSL-Passthrough konfiguriert werden.

5. Deinstallation der Anwendung

Dieses Kapitel beschreibt die Deinstallation des SAK-DP in einer Server-Umgebung sowie in einem Kubernetes-Cluster.

WICHTIG	Denken Sie daran, konfigurative Einstellungen, die Sie für die Installation und den Betrieb vorgenommen haben, rückgängig zu machen. Dies gilt auch für eventuell angelegte Logs.

5.1. Deinstallation im Server-Betrieb

Führen Sie zum Entfernen der Anwendung aus einer Server-Umgebung die folgenden Schritte aus:

1. Stoppen Sie die Anwendung. Sofern die Anwendung als Dienst betrieben wird, stoppen und deaktivieren Sie den Dienst.
2. Entfernen Sie die Anwendungsdateien. Entfernen Sie die JAR-Datei und die dazugehörigen Dateien von der Laufzeitumgebung.
3. Löschen Sie die Konfiguration und die Zertifikate. Dazu gehört die angepasste `application.properties` mit allen darin referenzierten Zertifikaten und Schlüsselspeichern.

5.2. Deinstallation in einem Kubernetes-Cluster

Für die Deinstallation wird der Helm-Release der Anwendung entfernt (gleiche Variablen wie bei der Installation, siehe Installation in einem Kubernetes-Cluster):

```
helm uninstall "$APP_RELEASE" --namespace
"$APP_NAMESPACE"
```

Mit dem Helm-Release werden alle vom Helm-Chart erzeugten Ressourcen entfernt, darunter auch das vom Helm-Chart erzeugte Secret und der ServiceAccount.

Nicht vom Helm-Chart verwaltet und daher separat zu entfernen sind:

- Secrets, die nicht über das Helm-Chart angelegt wurden, z. B. Keystores, Truststores oder Passwörter.
- PersistentVolumes, sofern sie für die Installation angelegt wurden.

6. Regulärer Wirkbetrieb

6.1. Logging

Der SAK-DP verwendet standardmäßig die Konsole für Logausgaben. Das Log-Nachrichtenformat entspricht dem Elastic Common Schema (ECS).

6.2. Statusprüfung der Anwendungen

Der SAK-DP stellt die folgenden Endpunkte über den Management Port zur Statusprüfung bereit:

HINWEIS	Diese Endpunkte sollten nur intern (z.B. hinter einer Firewall) betrieben werden. Eine Freigabe für einen öffentlichen, nicht regulierten Zugriff ist zu vermeiden!

Tabelle 4. Status-Endpunkte

Endpunkt	Beschreibung
`/actuator/health`	Gesamtstatus der Anwendung. Liefert `{"status":"UP|DOWN"}` als Antwort

6.3. Monitoring

Der SAK-DP kann zusätzliche Metriken liefern. Es stehen folgende Endpunkte zur Verfügung:

- `/metrics`
- `/prometheus` (Spring Boot Dokumentation; Kapitel "Prometheus (prometheus)")

Die Endpunkte können über die `application.properties` aktiviert werden und sind über den Management-Port erreichbar.

Es werden folgende Standard-Metriken bereitgestellt:

HINWEIS	Diese Endpunkte sollten nur intern (z.B. hinter einer Firewall) betrieben werden. Eine Freigabe für einen öffentlichen, nicht regulierten Zugriff ist zu vermeiden!

Tabelle 5. Standard-Metriken

Metriken	Beschreibung	Path
JVM	Metriken zum Speicherverbrauch, zur Garbage Collection, Threads und geladenen Klassen.	`/actuator/metrics/jvm/*`
System	Metriken zur CPU-Auslastung, dem Dateisystem und der Uptime der Anwendung.	`/actuator/metrics/disk/` `/actuator/metrics/system/` `/actuator/metrics/process/*`
Application Startup	Metriken zur Startzeit der Anwendung.	`/actuator/metrics/application/*`
Logger	Metriken zu Logging-Events.	`/actuator/metrics/logback/events`
REST Services	Metriken zu aufgerufenen REST-Services.	`/actuator/metrics/http/*`

6.4. Backup und Recovery

Wir empfehlen mindestens folgende Daten zu sichern:

- für Host-Server-Betrieb:
  - Angepasste `application.properties` die für den Betrieb verwendet wird.
  - Logs der Anwendung unter Beachtung der geltenden Datenschutzbestimmungen.
- für Container-Betrieb:
  - Angepasste `values.yaml` die für den Betrieb verwendet wird.

6.5. Hinweise für Störungsdiagnose und -behandlung

6.5.1. Debug-Logging

Die Konfiguration wird mit Log-Level `INFO` ausgeliefert, d.h. das Loggen von Debug-Ausgaben ist ausgeschaltet. Es kann aber per Konfigurationsparameter eingeschaltet werden:

- für Host-Server-Betrieb:
  - In `application.properties`: `logging.level.root=DEBUG` setzen.
- für Container-Betrieb:
  - Für den ausführenden POD die Umgebungsvariable `LOGGING_LEVEL_ROOT` auf den Wert `DEBUG` setzen.

ACHTUNG	Das Logging sollte auf der Produktivumgebung nie auf `DEBUG` gestellt werden. Aufgrund der umfangreichen Datenausgabe könnte es zu Performance-Problemen kommen. Gleichzeitig ist nicht sichergestellt, dass keine sicherheitsrelevanten Daten ausgegeben werden.

6.5.2. Bei Ressourcengrenzenüberschreitung des Anwendungscontainers

Für den Fall, dass im Container-Betrieb ein Container an seine Ressourcengrenzen kommt oder diese überschreitet, gibt es keine anwendungsspezifischen Handlungsempfehlungen. Es sind die üblichen Maßnahmen gemäß Betriebsrichtlinien des Anwendungsbetreibers auszuführen.

Anhang

Anhang A: Technisches Glossar

HINWEIS	Das hier hinterlegte Glossar ist übergreifend für alle Dokumente des SAKs identisch

Tabelle 6. Technisches Glossar für SAK-DP

Begriff	Bedeutung
Laufzeitumgebung	Umgebung, in der ein Service oder eine Anwendung betrieben werden kann.

Anhang B: Fachliches Glossar

HINWEIS	Das hier hinterlegte Glossar ist übergreifend für alle Dokumente des SAKs identisch

Tabelle 7. Fachliches Glossar für SAK-DP

Begriff	Bedeutung
Data Consumer	Ein Data Consumer ist ein NOOTS-Teilnehmer, welcher Nachweise aus dem System, konkret den Data Providern, abrufen möchte.
Data Provider	Ein Data Provider ist ein NOOTS-Teilnehmer der den Data Consumern Nachweise zur Verfügung stellt.
Identity Access Management für Behörden (IAM-B)	Das IAM für Behörden ist eine zentrale Komponente des NOOTS. Sie stellt für den Zugriff auf andere NOOTS-Komponenten und Data Provider vertrauenswürdige und zuverlässige Zugriffstoken für Data Consumer aus, die den Zugriff des DC auf die NOOTS-Komponenten und die DPs autorisiert, die Identität des DCs bestätigt und die Berechtigungen des DCs gegenüber den NOOTS-Komponenten und DPs beinhaltet.
Registerdatennavigation (RDN)	Die Registerdatennavigation ist eine zentrale Komponente des NOOTS. Sie liefert auf Anfrage die Information, von welchem technischen Dienst einer Behörde ein gesuchter Nachweistyp abgerufen werden kann. Dazu übermittelt die RDN notwendige Verbindungsparameter an den anfragenden Data Consumer.
Nachweis	Nachweise sind Unterlagen und Daten in elektronischer Form, die zur Ermittlung des Sachverhaltes in Verwaltungsverfahren geeignet sind.

Begriff	Bedeutung
National-Once-Only-Technical-System (NOOTS)	Das NOOTS ist ein gemeinsames informationstechnisches System aus IT-Komponenten, Schnittstellen und Standards, das öffentlichen Stellen den Abruf und die Übermittlung von elektronischen Nachweisen und Daten national und grenzüberschreitend aus Datenbeständen öffentlicher Stellen, zur Erfüllung öffentlicher Aufgaben ermöglicht.
Sicherer Anschlussknoten (SAK)	Ein sicherer Anschlussknoten (SAK) ist eine für Data Consumer - und Provider bereitgestellte NOOTS-Komponente, die dezentral im Verantwortungsbereich der NOOTS-Teilnehmer betrieben wird. Er ermöglicht den NOOTS-Teilnehmern über ein interoperables Anschlussprotokoll einen einfachen und sicheren Zugriff auf die NOOTS Transportinfrastruktur.

Anhang C: Betrieblich-Relevante Konfigurationsparameter für Server-Betrieb

```
include::../../../../../../{anwendung-abbv-
lc}/src/main/dist/application.properties
```

Anhang D: Helm Chart Values-Datei für Kubernetes-Betrieb

```yaml
# Standardwerte für das Chart des Sicheren
Anschlussknotens für Data Provider
# Mit @erforderlich gekennzeichnete Parameter müssen
durch eine überschreibende Values-Datei oder per "--
set"-Option gesetzt werden.
# Zur Anpassung des Deployments in der vorgesehenen
Umgebung müssen ggf. auch weitere Parameter angepasst
werden.

# replicaCount -- definiert die Anzahl der Replikate für
das Deployment. Weitere Informationen:
https://kubernetes.io/docs/concepts/workloads/controller
s/replicaset/
replicaCount: 1

# image -- konfiguriert das Container-Image für das
Deployment. @erforderlich
image:
  # image.repository -- definiert das Repository des
Container-Images. @erforderlich
  repository: null
```

```
  # image.tag -- definiert den Tag des Container-Images.
@erforderlich
  tag: null
  # image.pullPolicy -- legt die Pull-Richtlinie für das
Container-Image fest.
  pullPolicy: IfNotPresent

# imagePullSecrets -- enthält Referenzen auf Secrets,
die für den Zugriff auf private Container-Image-
Repositories benötigt werden.
imagePullSecrets: null
# nameOverride -- überschreibt den Standardnamen des
Charts.
nameOverride: null
# fullnameOverride -- überschreibt den vollständigen
Namen des Charts.
fullnameOverride: null

# serviceAccount -- konfiguriert den Kubernetes
ServiceAccount, der für das Deployment verwendet wird.
serviceAccount:
  # serviceAccount.create -- gibt an, ob ein neuer
ServiceAccount erstellt werden soll.
  create: true
  # serviceAccount.automount -- legt fest, ob das
ServiceAccount-Token automatisch in den Pod gemountet
wird.
  automount: false
  # serviceAccount.annotations -- definiert
Annotationen, die dem ServiceAccount hinzugefügt werden.
  annotations: { }
  # serviceAccount.name -- legt den Namen des zu
verwendenden ServiceAccounts fest. Wenn nicht gesetzt
und create auf true steht, wird ein Name generiert.
  name: ""

# podAnnotations -- definiert Kubernetes-Annotationen,
die auf die Pods angewendet werden.
podAnnotations: { }

# podLabels -- definiert Kubernetes-Labels, die auf die
Pods angewendet werden.
podLabels: { }

# podSecurityContext -- konfiguriert den Pod-weiten
SecurityContext, einschließlich Dateisystem- und
Gruppenrechten.
```

```yaml
podSecurityContext:
  # podSecurityContext.fsGroup -- legt die Dateisystem-
Gruppe für Dateien im Pod fest.
  fsGroup: 1000
  # podSecurityContext.supplementalGroups -- definiert
zusätzliche Gruppen, die dem Pod zugewiesen werden.
  supplementalGroups:
    - 1000

# securityContext -- konfiguriert den SecurityContext
für den Container, einschließlich Benutzer- und
Gruppenrechten.
securityContext:
  # securityContext.capabilities.drop -- entfernt alle
Linux-Kernel-Fähigkeiten, um erweiterte Systemrechte zu
entziehen.
  capabilities:
    drop:
      - ALL
  # securityContext.readOnlyRootFilesystem -- aktiviert
ein schreibgeschütztes Root-Dateisystem.
  readOnlyRootFilesystem: true
  # securityContext.runAsNonRoot -- erzwingt, dass der
Container nicht als Root-Benutzer ausgeführt wird.
  runAsNonRoot: true
  # securityContext.runAsUser -- legt die Benutzer-ID
fest, unter der der Container ausgeführt wird.
  runAsUser: 1000
  # securityContext.runAsGroup -- legt die Gruppen-ID
fest, unter der der Container ausgeführt wird.
  runAsGroup: 1000
  # securityContext.allowPrivilegeEscalation --
verhindert Privilegienerhöhungen innerhalb des
Containers.
  allowPrivilegeEscalation: false
  # securityContext.privileged -- verhindert, dass der
Container im privilegierten Modus ausgeführt wird.
  privileged: false

# javatoolOptionsExtra -- definiert zusätzliche
Optionen, die der Anwendung als JAVA_TOOL_OPTIONS
übergeben werden.
javatoolOptionsExtra: ""

# env -- ist eine Liste zusätzlicher Environment-
Variablen, die dem Container übergeben werden können.
env: [ ]
```

```
# sakdp -- enthält die Hauptkonfiguration für den
Sicheren Anschlussknoten für Data Provider (SAK-DP).
sakdp:
  features:
    # sakdp.features.include -- enthält eine Liste von
Feature-Flags
    include: "feature.apiV2,feature.apiV3"

  # sakdp.dataprovider -- enthält die Konfiguration für
den Data Provider.
  dataprovider:
    # sakdp.dataprovider.componentId -- ist die
Komponenten-ID (UUID) des Data Providers aus DAMAS.
    # @erforderlich, wenn "feature.apiV3" aktiv
    componentId:
    endpoints:
      apiV2:
        # sakdp.dataprovider.endpoints.apiV2.url -- ist
die komplette URL der v2 Evidence-Endpunkt des Data-
Providers.
        # @erforderlich, wenn "feature.apiV2" aktiv
        url:
        basicAuth:
          #
sakdp.dataprovider.endpoints.apiV2.basicAuth.enabled --
aktiviert die Basic-Authentifizierung für den v2
Evidence-Endpunkt.
          enabled: true
          #
sakdp.dataprovider.endpoints.apiV2.basicAuth.username --
ist der Benutzername für die Basic-Authentifizierung für
den v2 Evidence-Endpunkt.
          # @erforderlich, wenn "feature.apiV2" und
Basic-Auth aktiv
          username:
          #
sakdp.dataprovider.endpoints.apiV2.basicAuth.password --
ist das Passwort für die Basic-Authentifizierung für den
v2 Evidence-Endpunkt.
          # @erforderlich, wenn "feature.apiV2" und
Basic-Auth aktiv
          password:
      apiV3:
        # sakdp.dataprovider.endpoints.apiV3.url -- ist
die komplette URL der v3 Evidence-Endpunkt des Data-
Providers.
```

```
        # @erforderlich, wenn "feature.apiV3" aktiv
        url:
        basicAuth:
          #
sakdp.dataprovider.endpoints.apiV3.basicAuth.enabled --
aktiviert die Basic-Authentifizierung für den v3
Evidence-Endpunkt.
          enabled: true
          #
sakdp.dataprovider.endpoints.apiV3.basicAuth.username --
ist der Benutzername für die Basic-Authentifizierung für
den v3 Evidence-Endpunkt.
          # @erforderlich, wenn "feature.apiV3" und
Basic-Auth aktiv
          username:
          #
sakdp.dataprovider.endpoints.apiV3.basicAuth.password --
ist das Passwort für die Basic-Authentifizierung für den
v3 Evidence-Endpunkt.
          # @erforderlich, wenn "feature.apiV3" und
Basic-Auth aktiv
          password:

  # sakdp.server -- konfiguriert serverseitige
Einstellungen des SAK-DP
  server:
    ssl:
      # sakdp.server.ssl.enabled -- konfiguriert, ob
beim SAK-DP ('enabled: true') oder beim Ingress
('enabled: false') die mTLS-Terminierung stattfinden
soll.
      # Folgende zusätzliche Konfigurationen müssen
vorgenommen werden, wenn mTLS beim SAK-DP terminieren
soll:
      #  * der eingesetzte Ingress Controller muss so
konfiguriert werden, dass das Client-Zertifikat an den
SAK-DP in einem HTTP-Header weitergeleitet wird.
      #  * 'sakdp.server.keystore.*' muss konfiguriert
werden.
      #  * 'sakdp.server.truststore.*' muss konfiguriert
werden.
      #  * 'networkPolicy.ingress[0].ports[0].port:
8443'
      #  * 'service.port: 8443'
      # Der Ort der mTLS-Terminierung wirkt sich auch
auf andere Konfigurationswerte aus, welche mit einem
entsprechenden Hinweis versehen sind.
```

```
      enabled: false
    # sakdp.server.keystore -- konfiguriert den Keystore
für die mTLS-Verbindung zum SAK-DP wenn
'sakdp.server.ssl.enabled: true'.
    # Der Keystore muss eine PKCS#12-Datei sein.
    # Die Konfiguration wird ignoriert, wenn
'sakdp.server.ssl.enabled: false'.
    keystore:
      # sakdp.server.keystore.secretRef -- ist die
Referenz auf ein Secret, das den Keystore enthält.
      secretRef: "sakdp-server-keystore-secret"
      # sakdp.server.keystore.secretRefKey -- ist der
Key innerhalb des Secrets, der den Keystore enthält.
      secretRefKey: "server-keystore.p12"
      # sakdp.server.keystore.passwordSecretRef -- ist
die Referenz auf ein Secret, das das Passwort für den
Keystore enthält.
      # Wenn der Keystore nicht durch ein Passwort
geschützt ist, muss 'passwordSecretRef: ""' gesetzt
werden.
      passwordSecretRef: ""
      # sakdp.server.keystore.passwordSecretRefKey --
ist der Key innerhalb des Secrets, der das Passwort
enthält.
      # Der Wert wird ignoriert, wenn
'sakdp.server.keystore.passwordSecretRef: ""'.
      passwordSecretRefKey: ""
    # sakdp.server.truststore -- konfiguriert den
Truststore für die mTLS-Verbindung zum SAK-DP wenn
'sakdp.server.ssl.enabled: true'.
    # Der Truststore muss eine PKCS#12-Datei sein.
    # Die Konfiguration wird ignoriert, wenn
'sakdp.server.ssl.enabled: false'.
    truststore:
      # sakdp.server.truststore.secretRef -- ist die
Referenz auf ein Secret, das den Truststore enthält.
      secretRef: "sakdp-server-truststore-secret"
      # sakdp.server.truststore.secretRefKey -- ist der
Key innerhalb des Secrets, der den Truststore enthält.
      secretRefKey: "server-truststore.p12"
      # sakdp.server.truststore.passwordSecretRef -- ist
die Referenz auf ein Secret, das das Passwort für den
Truststore enthält.
      # Wenn der Truststore nicht durch ein Passwort
geschützt ist, muss 'passwordSecretRef: ""' gesetzt
werden.
      passwordSecretRef: ""
```

```
      # sakdp.server.truststore.passwordSecretRefKey --
ist der Key innerhalb des Secrets, der das Passwort
enthält.
      # Der Wert wird ignoriert, wenn
'sakdp.server.truststore.passwordSecretRef: ""'.
      passwordSecretRefKey: ""

  # sakdp.mtlsAuthentication -- konfiguriert die mTLS-
Authentifizierung für ausgehende Verbindungen.
  mtlsAuthentication:
    # sakdp.mtlsAuthentication.enabled -- aktiviert oder
deaktiviert die mTLS-Authentifizierung.
    enabled: true
    keystore:
      # sakdp.mtlsAuthentication.keystore.data --
enthält die einzeilig Base64-kodierten Keystore-Bytes.
Wenn gesetzt, wird secretRef überschrieben.
      data: ""
      # sakdp.mtlsAuthentication.keystore.secretRef --
ist die Referenz auf ein Secret, das den Keystore
enthält.
      secretRef: "sakdp-mtls-keystore"
      # sakdp.mtlsAuthentication.keystore.secretRefKey
-- ist der Key innerhalb des Secrets, der den Keystore
enthält.
      secretRefKey: "sakdp-mtls-keystore.p12"
      # sakdp.mtlsAuthentication.keystore.password --
ist das Passwort für den Keystore. Ein leerer String
("") ist ein gültiges Passwort.
      # Um ein bestehendes Secret mittels
'passwordSecretRef' zu nutzen, muss 'password: null'
gesetzt werden.
      password: null
      #
sakdp.mtlsAuthentication.keystore.passwordSecretRef --
ist die Referenz auf ein Secret, das das Passwort für
den Keystore enthält.
      passwordSecretRef: "sakdp-mtlspassword"
      #
sakdp.mtlsAuthentication.keystore.passwordSecretRefKey
-- ist der Key innerhalb des Secrets, der das Passwort
enthält.
      passwordSecretRefKey: "password"
  client:
    # sakdp.client.connect-timeout -- setzt den Timeout
in Millisekunden für den Verbindungsaufbau zum Data
Provider (Standardwert: 500; Achtung: ohne Einheit).
```

```
    connectTimeout: null
    # sakdp.client.read-timeout -- setzt den Timeout für
die Bearbeitungsdauer im Data Provider (Standardwert:
3500ms).
    readTimeout: null
  # sakdp.clientTruststore -- konfiguriert den
Truststore für ausgehende TLS-Verbindungen.
  clientTruststore:
    # sakdp.clientTruststore.data -- enthält die
einzeilig Base64-kodierten Truststore-Bytes. Wenn
gesetzt, wird secretRef überschrieben.
    data: ""
    # sakdp.clientTruststore.enabled -- aktiviert die
Verwendung eines benutzerdefinierten Truststores.
    enabled: true
    # sakdp.clientTruststore.secretRef -- ist die
Referenz auf ein Secret, das den Truststore enthält.
    secretRef: "sakdp-client-truststore"
    # sakdp.clientTruststore.secretRefKey -- ist der Key
innerhalb des Secrets, der den Truststore enthält.
    secretRefKey: "sakdp-client-truststore.p12"
    # sakdp.clientTruststore.password -- ist das
Passwort für den Truststore. Ein leerer String ("") ist
ein gültiges Passwort.
    # Um ein bestehendes Secret mittels
'passwordSecretRef' zu nutzen, muss 'password: null'
gesetzt werden.
    password: null
    # sakdp.clientTruststore.passwordSecretRef -- ist
die Referenz auf ein Secret, das das Passwort für den
Truststore enthält.
    passwordSecretRef: "sakdp-clienttruststorepassword"
    # sakdp.clientTruststore.passwordSecretRefKey -- ist
der Key innerhalb des Secrets, der das Passwort enthält.
    passwordSecretRefKey: "password"

  # sakdp.rateLimitation -- konfiguriert die
Ratenbegrenzung für Anfragen.
  rateLimitation:
    # sakdp.rateLimitation.limitForPeriod -- legt die
maximale Anzahl von Anfragen pro Zeitraum fest.
    limitForPeriod: 50
    # sakdp.rateLimitation.limitRefreshPeriod -- legt
den Zeitraum in Millisekunden fest, nach dem die
Anfrageanzahl zurückgesetzt wird.
    limitRefreshPeriod: 1000
```

```
  # sakdp.whitelistTruststore (nur relevant bei
feature.apiV2) -- konfiguriert den Whitelist-Truststore
für Client-Zertifikate (Pinning).
  # @erforderlich, wenn "feature.apiV2" aktiv
  whitelistTruststore:
    # sakdp.whitelistTruststore.data -- enthält die
Base64-kodierten Truststore-Bytes. Wenn gesetzt, wird
secretRef überschrieben.
    data: ""
    # sakdp.whitelistTruststore.secretRef -- ist die
Referenz auf ein Secret, das den Truststore enthält.
    secretRef: "sakdp-whitelisttruststore"
    # sakdp.whitelistTruststore.secretRefKey -- ist der
Key innerhalb des Secrets, der den Truststore enthält.
    secretRefKey: "truststore.p12"
    # sakdp.whitelistTruststore.password -- ist das
Passwort für den Truststore. Ein leerer String ("") ist
ein gültiges Passwort.
    # Um ein bestehendes Secret mittels
'passwordSecretRef' zu nutzen, muss 'password: null'
gesetzt werden.
    password: null
    # sakdp.whitelistTruststore.passwordSecretRef -- ist
die Referenz auf ein Secret, das das Passwort für den
Truststore enthält.
    passwordSecretRef: "sakdp-
whitelisttruststorepassword"
    # sakdp.whitelistTruststore.passwordSecretRefKey --
ist der Key innerhalb des Secrets, der das Passwort
enthält.
    passwordSecretRefKey: "password"

  # sakdp.accessToken -- konfiguriert die Überprüfung
von AccessTokens.
  accessToken:
    # sakdp.accessToken.sslClientCertHeader -- ist der
HTTP-Request-Header mit dem Client-Zertifikat aus der
eingehenden TLS-Verbindung.
    # Dieser Wert wird ignoriert, wenn
'sakdp.server.ssl.enabled = true', da die TLS-Verbindung
dann beim SAK-DP direkt terminiert und somit das
    # Client-Zertifikat nicht über den Header zur
Verfügung gestellt werden muss.
    sslClientCertHeader: "ssl-client-cert"
    # sakdp.accessToken.sslClientCertHeaderEncoding --
ist die Kodierung des HTTP-Request-Headers mit dem
Client-Zertifikat aus der eingehenden TLS-Verbindung.
```

```
    # Dieser Wert wird ignoriert, wenn
'sakdp.server.ssl.enabled = true' (s.
'sakdp.accessToken.sslClientCertHeader').
    sslClientCertHeaderEncoding: "url"
    # sakdp.accessToken.roleGetEvidence -- definiert die
Rollen, die erforderlich sind, um Nachweise abzurufen.
    roleGetEvidence: "nachweis.national"
    # sakdp.accessToken.algorithms -- gibt den
Algorithmus an, mit dem das Token signiert sein muss.
    algorithms: "ES256"
    # sakdp.accessToken.rolesclaimname -- ist der Name
des Claims im Token, der die Rollen enthält.
    rolesclaimname: "scope"
    # sakdp.accessToken.issuer -- ist der erwartete
Aussteller des Tokens.
    issuer:
    # sakdp.accessToken.audiences -- definiert die
erwartete Audience des Tokens.
    audiences: "urn:regmo:components"
    iambTruststore:
      # sakdp.accessToken.iambTruststore.cabundle --
enthält CA-Zertifikate als PEM. Wenn gesetzt, wird
secretRef überschrieben.
      cabundle: ""
      # sakdp.accessToken.iambTruststore.secretRef --
ist die Referenz auf ein Secret, das den Truststore
enthält.
      secretRef: "sakdp-iamb-truststore"
      # sakdp.accessToken.iambTruststore.secretRefKey --
ist der Key innerhalb des Secrets, der den Truststore
enthält.
      secretRefKey: "sakdp-iamb-cabundle.pem"

  # sakdp.rdnTruststore -- konfiguriert die Überprüfung
von Jurisdictiontokens.
  rdnTruststore:
    # sakdp.rdnTruststore.cabundle -- Enthält die CA-
Zertifikate als PEM. Sie ersetzen das secretRef und
zugehörigen secretRefKey.
    cabundle: ""
    # sakdp.rdnTruststore.secretRef -- Ist die Referenz
auf ein Secret, das den Truststore für die RDN enthält.
    secretRef: "sakdp-rdn-truststore"
    # sakdp.rdnTruststore.secretRefKey -- Ist der Key
innerhalb des Secrets, der den Truststore für die RDN
enthält.
    secretRefKey: "sakdp-rdn-cabundle.pem"
```

```
  # sakdp.vsTruststore -- konfiguriert die Überprüfung
von Abruftokens.
  # @erforderlich, wenn "feature.apiV3" aktiv
  vsTruststore:
    # sakdp.vsTruststore.cabundle -- Enthält die CA-
Zertifikate als PEM. Sie ersetzen das secretRef und
zugehörigen secretRefKey.
    cabundle: ""
    # sakdp.vsTruststore.secretRef -- Ist die Referenz
auf ein Secret, das den Truststore für die VS enthält.
    secretRef: "sakdp-vs-truststore"
    # sakdp.vsTruststore.secretRefKey -- Ist der Key
innerhalb des Secrets, der den Truststore für die VS
enthält.
    secretRefKey: "sakdp-vs-cabundle.pem"

  # sakdp.encryptionCertificate -- Konfiguriert das
Verschlüsselungszertifikat für die JWE-Verschlüsselung
mit dem SAK-DC.
  # @erforderlich, wenn "feature.apiV3" aktiv
  encryptionCertificate:
    # sakdp.encryptionCertificate.secretRef -- Ist die
Referenz auf ein bestehendes Secret mit dem
Verschlüsselungszertifikat und privaten Schlüssel.
    secretRef: "noots-sakdp-encrypt-cert-secret"
    # sakdp.encryptionCertificate.secretRefCertKey --
Ist der Key innerhalb des Secrets, der das öffentliche
Zertifikat (PEM) enthält.
    secretRefCertKey: "tls.crt"
    # sakdp.encryptionCertificate.secretRefPrivateKey --
Ist der Key innerhalb des Secrets, der den privaten
Schlüssel (PEM) enthält.
    secretRefPrivateKey: "tls.key"

iamb:
  # iamb.hostname -- IAM-B Hostname
  hostname:

# dataprovider -- enthält die Konfiguration für den Data
Provider.
# @deprecated: s. sakdp.dataprovider
dataprovider:
  # dataprovider.url -- ist die Basis-URL des Data
Providers.
  # @deprecated: sakdp.dataprovider.endpoints.apiV2.url
und sakdp.dataprovider.endpoints.apiV3.url stattdessen
```

```
verwenden
  url:
  # dataprovider.resource -- ist der Pfad innerhalb der
Basis-URL.
  # @deprecated: sakdp.dataprovider.endpoints.apiV2.url
und sakdp.dataprovider.endpoints.apiV3.url stattdessen
verwenden
  resource:
  # dataprovider.componentId -- ist die Komponenten-ID
des Data Providers (UUID). @erforderlich, wenn
"feature.apiV3" aktiv
  # @deprecated: sakdp.dataprovider.componentId
stattdessen verwenden
  componentId:
  credentials:
    basicAuth:
      # dataprovider.credentials.basicAuth.enabled --
aktiviert die Basic-Authentifizierung für den /evidence-
Endpunkt.
      # @deprecated:
sakdp.dataprovider.endpoints.apiV2.basicAuth.enabled und
sakdp.dataprovider.endpoints.apiV3.basicAuth.enabled
stattdessen verwenden
      enabled: true
      # dataprovider.credentials.basicAuth.username --
ist der Benutzername für die Basic-Authentifizierung.
      # Der Benutzername wird ignoriert, wenn 'enabled:
false'.
      # Der Benutzername muss gesetzt werden, wenn
'enabled: true'.
      # @deprecated:
sakdp.dataprovider.endpoints.apiV2.basicAuth.username
und
sakdp.dataprovider.endpoints.apiV3.basicAuth.username
stattdessen verwenden
      username: ""
      # dataprovider.credentials.basicAuth.password --
ist das Passwort für die Basic-Authentifizierung.
      # Das Passwort wird ignoriert, wenn 'enabled:
false'.
      # Das Passwort muss gesetzt werden, wenn 'enabled:
true'.
      # @deprecated:
sakdp.dataprovider.endpoints.apiV2.basicAuth.password
und
sakdp.dataprovider.endpoints.apiV3.basicAuth.password
stattdessen verwenden
```

```
      password: ""

# resources -- konfiguriert CPU- und Speicher-Limits
sowie -Requests für den Pod.
resources:
  # resources.limits -- definiert die maximalen
Ressourcen, die der Container verwenden darf.
  limits:
    # resources.limits.cpu -- gibt das obere CPU-Limit
an.
    cpu: 1000m
    # resources.limits.memory -- gibt obere
Arbeitsspeichergrenze an.
    memory: 1024Mi
  # resources.requests -- definiert die reservierten
Ressourcen, die dem Container garantiert werden.
  requests:
    # resources.requests.cpu -- gibt die garantierte
CPU-Menge an.
    cpu: 500m
    # resources.requests.memory -- gibt den garantierten
Arbeitsspeicher an.
    memory: 1024Mi

# proxy -- konfiguriert einen optionalen HTTP-Proxy für
ausgehende Verbindungen.
proxy:
  # proxy.enabled -- aktiviert oder deaktiviert die
Verwendung des Proxys.
  enabled: true
  # proxy.host -- ist die Adresse des Proxy-Servers. Es
kann eine IP-Adresse oder ein Hostname angegeben werden.
  # Der Parameter ersetzt funktional 'proxy.ip' und wird
bevorzugt verwendet.
  # Hinweis: Für cluster-externe Ziele wie einen Proxy
kann eine NetworkPolicy nur IP-basierte Regeln (ipBlock)
verwenden.
  # Bei Angabe eines Hostnames für den Proxy muss der
Betreiber daher die Egress-Regel der NetworkPolicy
  # selbst definieren (s. 'networkPolicy.egressProxy').
  host: ""
  # proxy.ip -- ist die IP-Adresse des Proxy-Servers.
(deprecated: stattdessen 'proxy.host' verwenden)
  # Wird nur verwendet, wenn 'proxy.host' nicht gesetzt
ist.
  ip: "127.0.0.1"
  # proxy.port -- ist der Port des Proxy-Servers.
```

```
  port: "3128"
  # proxy.noProxy -- listet Hosts auf, die ohne Proxy
direkt erreicht werden sollen.
  # proxy.noProxy Listen-Elemente werden durch `|`
getrennt und können Wildcards mit `*` enthalten.
  noProxy: ""

# networkPolicy -- konfiguriert die NetworkPolicy-Regeln
für das Deployment.
networkPolicy:
  # networkPolicy.enabled -- steuert, ob NetworkPolicies
im Cluster angewendet werden sollen.
  enabled: true
  # networkPolicy.ingress -- definiert eingehende Pod-
Verbindungen, die erlaubt sind.
  ingress:
    # networkPolicy.ingress.ports -- definiert die
erlaubten Ports für eingehenden Traffic.
    - ports:
        - protocol: TCP
          # networkPolicy.ingress[0].ports[0].port --
konfiguriert den Port für eingehenden TCP Traffic.
          # Wenn 'sakdp.server.ssl.enabled: true' muss
'port: 8443' gesetzt werden; sonst 'port: 8080'.
          port: 8080
      # networkPolicy.ingress.from -- definiert die
erlaubten Quellen für eingehenden Traffic.
      from:
        - podSelector:
            matchLabels:
              app.kubernetes.io/name: rke2-ingress-nginx
          namespaceSelector:
            matchLabels:
              kubernetes.io/metadata.name: kube-system
  # networkPolicy.egressDns -- definiert ausgehende
Verbindungen zur Namensauflösung.
  egressDns:
    - to:
        - namespaceSelector:
            matchLabels:
              kubernetes.io/metadata.name: kube-system
          podSelector:
            matchLabels:
              k8s-app: kube-dns
      # networkPolicy.egressDns.ports -- definiert die
Ports, die für DNS-Auflösung benötigt werden.
      ports:
```

```
        - protocol: TCP
          port: 53
        - protocol: UDP
          port: 53
  # networkPolicy.egress -- definiert generelle
ausgehende Pod-Verbindungen.
  egress:
    # networkPolicy.egress.ports -- definiert die
erlaubten Ziel-Ports für ausgehenden Traffic.
    - ports:
        - protocol: TCP
          port: 443
  # networkPolicy.egressProxy -- definiert die
ausgehende Verbindung zum Proxy-Server, wenn
'proxy.enabled: true'.
  # Wird 'networkPolicy.egressProxy' nicht gesetzt
(Standard), bleibt das bisherige Verhalten erhalten:
  # es wird ausschließlich der Proxy im Egress erlaubt,
und zwar als IP-Block 'proxy.host/32' (bzw.
'proxy.ip/32')
  # mit dem Port 'proxy.port' (TCP).
  # Über diese Liste kann der Betreiber die Egress-Regel
an die tatsächliche Umgebung anpassen, z. B. per
  # CIDR-Block, podSelector, namespaceSelector oder mit
abweichenden Ports.
  # Hinweis: Kubernetes-NetworkPolicies unterstützen
ausschließlich IP-basierte Ziele (ipBlock).
  # Bei Angabe eines Hostnames für den Proxy
(proxy.host) muss der Betreiber die Egress-Regel daher
selbst
  # definieren (z. B. per podSelector/namespaceSelector
oder passendem ipBlock).
  egressProxy: null
  # networkPolicy.ingressPrometheus -- erlaubt
eingehende Prometheus-Verbindungen zum Management-Port.
  ingressPrometheus:
    - from:
        - namespaceSelector:
            matchLabels:
              kubernetes.io/metadata.name: kube-
prometheus-stack
      ports:
        - protocol: TCP
          port: 9000

# Dies dient zur Einrichtung eines Dienstes. Weitere
Informationen finden Sie hier:
```

```
https://kubernetes.io/docs/concepts/services-
networking/service/
service:
  # service.create -- bestimmt, ob ein Service-Objekt
erstellt werden soll.
  create: true
  # service.type -- legt den Typ des Service fest (z. B.
ClusterIP, NodePort).
  type: ClusterIP
  # service.port -- ist der Port, über den der Service
den Traffic zum Pod weiterleitet.
  # Wenn 'sakdp.server.ssl.enabled: true' muss 'port:
8443' gesetzt werden; sonst 'port: 8080'.
  port: 8080
  # service.managementPort -- ist der Management-Port
(z. B. für Health/Prometheus).
  managementPort: 9000
  # service.exposeDebuggingPort -- steuert, ob ein
Debugging-Port offen gelegt werden soll.
  exposeDebuggingPort: false

# Dieser Block dient zur Einrichtung des Ingress.
Weitere Informationen finden Sie hier:
https://kubernetes.io/docs/concepts/services-
networking/ingress/
ingress:
  # ingress.enabled -- aktiviert oder deaktiviert das
Erstellen eines Ingress-Objekts.
  enabled: false
  # ingress.className -- legt die Ingress-
Klassenbezeichnung (IngressClass) fest.
  className: ""
  # ingress.annotations -- enthält zusätzliche
Annotationen, die dem Ingress-Objekt hinzugefügt werden.
  annotations: { }
  # ingress.hosts -- listet die Hosts auf, unter denen
die Anwendung erreichbar sein soll.
  hosts:
    # ingress.hosts[0].host -- ist der Hostname für den
ersten Host-Eintrag.
    - host: sicherer-anschlussknoten-dp.local
      # ingress.hosts[0].paths -- definiert Pfade und
Typen für den Host.
      paths:
        # ingress.hosts[0].paths[0].path -- ist der
HTTP-Pfad für den Ingress-Eintrag.
        - path: /
```

```
          # ingress.hosts[0].paths[0].pathType -- gibt
den Pfadtyp für das Ingress an.
          pathType: ImplementationSpecific
  # ingress.tls -- konfiguriert TLS-Einträge für das
Ingress-Objekt.
  tls: [ ]

# Der Servicemonitor sowie der Endpunkt
actuator/prometheus wird aktiviert
servicemonitor:
  # servicemonitor.enabled -- schaltet den
ServiceMonitor ein oder aus.
  enabled: false

# Dies dient zur Einrichtung der Liveness-, Readiness-
und Startup-Probes. Weitere Informationen finden Sie
hier: https://kubernetes.io/docs/tasks/configure-pod-
container/configure-liveness-readiness-startup-probes/
livenessProbe:
  # livenessProbe.httpGet -- definiert die HTTP-GET-
Anfrage zur Prüfung der Liveness.
  httpGet:
    # livenessProbe.httpGet.path -- ist der Pfad, der
für die Liveness-Prüfung aufgerufen wird.
    path: /actuator/health/liveness
    # livenessProbe.httpGet.port -- ist der Port, der
für die Liveness-Prüfung verwendet wird.
    port: 9000
  # livenessProbe.initialDelaySeconds -- legt die
Verzögerung vor der ersten Prüfung fest.
  initialDelaySeconds: 30

# readinessProbe -- konfiguriert die Readiness-Probe des
Containers.
readinessProbe:
  # readinessProbe.httpGet -- definiert die HTTP-GET-
Anfrage zur Prüfung der Readiness.
  httpGet:
    # readinessProbe.httpGet.path -- ist der Pfad, der
für die Readiness-Prüfung aufgerufen wird.
    path: /actuator/health/readiness
    # readinessProbe.httpGet.port -- ist der Port, der
für die Readiness-Prüfung verwendet wird.
    port: 9000
  # readinessProbe.initialDelaySeconds -- legt die
Verzögerung vor der ersten Readiness-Prüfung fest.
  initialDelaySeconds: 30
```

```
# startupProbe -- konfiguriert die Startup-Probe des
Containers.
startupProbe:
  # startupProbe.httpGet -- definiert die HTTP-GET-
Anfrage zur Prüfung des Container-Starts.
  httpGet:
    # startupProbe.httpGet.path -- ist der Pfad für die
Startup-Prüfung.
    path: /actuator/health/liveness
    # startupProbe.httpGet.port -- ist der Port, der für
die Startup-Prüfung verwendet wird.
    port: 9000
  # startupProbe.periodSeconds -- legt das Prüfintervall
für die Startup-Probe fest.
  periodSeconds: 30
  # startupProbe.failureThreshold -- legt fest, nach wie
vielen Fehlversuchen der Pod als nicht startbar gilt.
  failureThreshold: 30

# volumes -- definiert zusätzliche Volumes in der Pod-
Spezifikation.
volumes: [ ]

# volumeMounts -- definiert die Mount-Punkte für
zusätzliche Volumes im Container.
volumeMounts: [ ]

# nodeSelector -- definiert Node-Labels, die zur Auswahl
der Nodes für das Deployment verwendet werden.
# Weitere Informationen:
https://kubernetes.io/docs/concepts/scheduling-
eviction/assign-pod-node/
nodeSelector: { }

# affinity -- konfiguriert Affinity-Regeln für die Pods.
affinity: { }

# tolerations -- definiert Tolerations, um Pods auf
getainteten Nodes zuzulassen.
tolerations: [ ]

# -- pdb konfiguriert das Pod Disruption Budget für das
Deployment.
pdb:
  # -- pdb.enabled aktiviert die Erstellung eines Pod
Disruption Budgets.
```

```
  enabled: false
  # -- pdb.minAvailable definiert die minimale Anzahl an
Pods, die während einer Störung verfügbar bleiben
müssen.
  minAvailable: null
  # -- pdb.maxUnavailable definiert die maximale Anzahl
an Pods, die während einer Störung nicht verfügbar sein
dürfen.
  maxUnavailable: null
```

Quellen

Tabelle 8. Quellen

Name der Quelle	Link	Version
Anschlusskonzept Data Consumer (AD-NOOTS-01)	https://gitlab.opencode.de/noots/public/ad-noots/noots-architektur/ad-noots-release/-/blob/main/AD-NOOTS-XX/AD-NOOTS-01_+Anschlusskonzept+Data+Consumer+_DC_.md	Release Februar 2025
Anschlusskonzept Data Provider (AD-NOOTS-02)	https://gitlab.opencode.de/noots/public/ad-noots/noots-architektur/ad-noots-release/-/blob/main/AD-NOOTS-XX/AD-NOOTS-02_+Anschlusskonzept+Data+Provider+_DP_.md	Release Februar 2025
High-Level-Architecture (AD-NOOTS-03)	https://gitlab.opencode.de/noots/public/ad-noots/noots-architektur/ad-noots-release/-/blob/main/AD-NOOTS-XX/AD-NOOTS-03_+High-Level-Architecture+_HLA_.pdf	Release Februar 2025
Spring Boot Dokumentation ; Kapitel "Installing Spring Boot Applications"	https://docs.spring.io/spring-boot/3.5/how-to/deployment/installing.html	Version 3.5.5

Name der Quelle	Link	Version
Spring Boot Dokumentation ; Kapitel "Externalized Configuration"; Abschnitt "External Application Properties"	https://docs.spring.io/spring-boot/reference/features/external-config.html#features.external-config.files	Version 3.5.5
Spring Boot Dokumentation ; Kapitel "Prometheus (prometheus)"	https://docs.spring.io/spring-boot/api/rest/actuator/prometheus.html	Version 3.5.5
Kubernetes Dokumentation ; Kapitel "Pod Lifecycle"; Abschnitt "Types of probe"	https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle/#types-of-probe	
Technische Richtlinie BSI TR-03190	https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03190/BSI-TR-03190.pdf	Version 1.0

[1] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html

[2] https://deutsche-verwaltungscloud.de

[3] https://docs.fitko.de/dvc

[4] https://helm.sh/docs/chart_template_guide/values_files

[5] https://kubernetes.io/docs/concepts/security/secrets-good-practices

[6] https://helm.sh/docs/helm/helm_upgrade

[7] https://helm.sh/docs/chart_template_guide/values_files