Bundesverwaltungsamt

NOREF Integrationsanleitung

Version 1.0, 30.04.2026: NOREF

Inhaltsverzeichnis

Dokumentinformationen

Verfasser	SEITENBAU

Änderungshistorie

Datum	Version	Änderungen	Verfasser
23.02.2026	0.1	• Initiales Aufsetzen des Dokuments in der Version 0.1. Vorherige Versionen sind durch das Einführen einer weiterentwickelten Systemplattform nicht mehr gültig	SEITENBAU
09.04.2026	0.9	• Einarbeitung Review-Anmerkungen	SEITENBAU
30.04.2026	1.0	• Anpassung Version zu 1.0 nach inhaltlicher Abnahme	SEITENBAU

Übersicht

Dieses Dokument ist eine Integrationsanleitung zum Anschluss eines Data Consumers oder eines Data Providers an die Referenzumgebung.

> **HINWEIS** Die Inhalte dieses Dokuments sind nicht für den Anschluss an andere NOOTS-Umgebungen geeignet!

Überblick über die Referenzumgebung

Die Referenzumgebung stellt die zentralen NOOTS-Komponenten Identity Access Management für Behörden (IAM-B), und Registerdatennavigation (RDN) als simulierte Komponenten (Mocks) mit einer Basisfunktionalität bereit, die für den exemplarischen Nachweisabruf ausreichend ist.

Zusätzlich werden auch Sichere Anschlussknoten (SAK) für Data Consumer (DC) und Data Provider (DP) in der Referenzumgebung zur Verfügung gestellt, die einen Nachweisabruf testweise initiieren oder beantworten können, ohne ein externes Testsystem eines Data Consumers oder Data Providers notwendig zu machen.

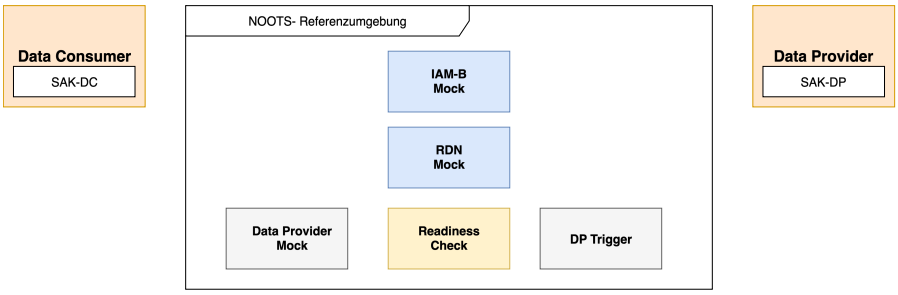
In der unten stehenden Grafik sind die NOOTS-Komponenten, die in der Referenzumgebung zur Simulation zur Verfügung stehen, blau gefärbt. Komponenten, die ausschließlich in der Referenzumgebung verfügbar

sind, sind gelb gefärbt. Grau gefärbte Komponenten sind Komponenten, die von Data Consumer und Data Provider für die Verprobung genutzt werden. Die Komponenten, bzw. Systeme, die von anschlussswilligen NOOTS-Teilnehmern betrieben werden, sind orange markiert.

Data Provider Mock: Der Data Provider Mock ist eine Testkomponetne, die Anstelle eines echten Data Providers verwendet wird. Die Komponente vereint dabei zwei NOOTS Komponenten: SAK-DP und Data Provider. So wird eine unabhängige Verprobung ermöglicht.

Readines-Check: Der Readiness-Check ist zum einen eine technische Komponente, die einen anschlusswilligen NOOTS-Teilnehmer auf einen technisch erfolgreichen Anschluss prüft und Informationen darüber mittels Schnittstelle bereitstellt. Diese technische Komponente wird in der folgenden Komponentenübersicht dargestellt. Zum anderen dient ein erfolgreicher Readiness-Check als Nachweis und Abnahme für weitere Prozessschritte.

DP-Trigger: DP-Trigger ist eine Testkomponetne, die Anstelle eines echten SAK-DC verwendet wird. Die Komponente simuliert dabei die Anfrage eines SAK-DC hin zum SAK-DP. So wird eine unabhängige Verprobung ermöglicht.



Die angebundenen Data Consumer und Data Provider kommunizieren ausschließlich mit der Referenzumgebung. Es wird keine Kommunikation zwischen angebundenen Data Consumern und angebundenen Data Providern unterstützt.

Integration gegen die Referenzumgebung

HINWEIS	Vorbedingung für den Anschluss an die Referenzumgebung ist die Erstkontaktaufnahme mit dem BVA (siehe Kontaktinformationen).

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

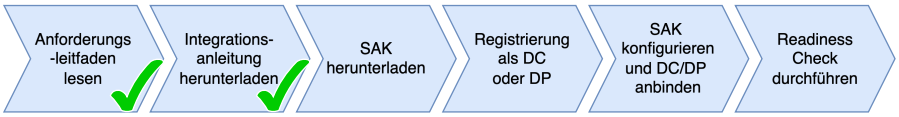


Abbildung 1. Prozessschritte zum Anschluss an die Referenzumgebung

Voraussetzung für den Anschluss an die Referenzumgebung ist die vorliegende Integrationsanleitung, da in diesem Dokument die wesentlichen Informationen zum Anschluss zusammengefasst dargestellt sind. Danach laden Sie den von NOOTS bereitgestellten Sicheren Anschlussknoten herunter und dessen Integrationsanleitung (und ggf. Systemdokumentation) herunter. Folgend registriert Sie das NOOTS-Team in der Referenzumgebung als Data Consumer oder Data Provider und leitet Ihnen alle nötigen Informationen und Daten weiter. Diese Daten verwenden Sie im nächsten Schritt, um den SAK in ihr System einzubinden, sodass eine Kommunikation mit der Referenzumgebung möglich wird. Nachdem die Konfiguration des SAK abgeschlossen ist, können Sie den Readiness-Check initiieren (einen Nachweis abrufen). Somit testen Sie den Anschluss an die Referenzumgebung. Ist der Readiness-Check erfolgreich, so haben Sie diesen absolviert und können die Bestätigung von der Referenzumgebung abrufen. Ein erfolgreicher Readiness-Check ist Vorraussetzung für eine Registrierung auf der Testumgebung.

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

Integration als Data Consumer

Durch den Anschluss an die Referenzumgebung kann ein Data Consumer feststellen, ob das eigene System NOOTS-ready ist, d.h. ob ein Data Consumer erfolgreich einen Nachweisabruf initiieren und den generierten Nachweis empfangen kann. Dabei wird aus Testzwecken sowohl statische Nachweisangebote, als auch ein statischer Nachweis bereitgestellt.

Registrierung

Um als Data Consumer in der Referenzumgebung einen Readiness-Check durchführen zu können, muss der Data Consumer als Client registriert werden. Die Registrierung erfolgt über den Support. Das Support-Team registriert anhand der Informationen den Data Consumer in der Referenzumgebung, sodass der Data Consumer der Anwendung bekannt ist.

Installation

Der Sichere Anschlussknoten für Data Consumer muss als eigenständig lauffähige Anwendung mit Zugriff auf das Internet installiert werden. Wie eine Installation eines SAK-DC durchzuführen ist, ist in der offiziellen

Integrationsanleitung des Sicheren Anschlussknotens zu finden.

HINWEIS	Verwenden Sie bei der Einrichtung des SAK die für Sie bereitgestellten Informationen und Keystores aus der Registrierung.

Bereitstellung von Test-Data-Provider

In der Referenzumgebung wird ein Test-Data-Provider für Data Consumer bereitgestellt. Der Endpunkt liefert dabei einen fest definierten Nachweis für fest definierte Nachweisangebote.

Durchlauf eines Nachweisabrufs (Readiness-Check)

Um als Data Consumer nach der Registrierung und der Installation und Integration des SAK-DC einen Nachweis abrufen zu können, sind die nachfolgenden Schritte notwendig (eine Schnittstellenbeschreibung der Referenzumgebung finden Sie unter Übersicht der Schnittstellendefinitionen der Referenzumgebung).

HINWEIS	Es werden ausschließlich Testdaten innerhalb der Umgebung versendet!

1. Anforderung eines Zugrifftokens

In einem ersten Schritt ist es notwendig ein Zugriffstoken für die Nutzung der Schnittstellen anzufordern. Die Anforderung eines solchen Zugriffstokens erfolgt über die `token`-Schnittstelle des SAK-DC.

Beispiel:

```
POST https://<NOREF_URL>/token
{
  "component_id": "KOMPONENTEN_ID_AUS_REGISTRIERUNG"
}
```

HINWEIS	Sollten Sie auch für diese Schnittstelle Basic Auth aktiviert haben, achten Sie darauf diese mitzusenden. Wie dies genau aussieht, können Sie in der Integrationsanleitung des SAK-DC nachlesen.

Als `component_id` ist die zugewiesene Komponenten-ID des Data Consumers zu verwenden. Den Wert dieses Feldes erhalten Sie nach der Registrierung (siehe Registrierung als Data Consumer) vom Support-Team.

Sollten Sie Basic Auth für die SAK-DC `token`-Schnittstelle bei der Installation und Integration aktiviert haben, müssen Sie beim Anfragen

des Zugrifftokens immer eine Basic Authorization mit spezifischen `username` und `password` mitsenden.

HINWEIS	Der Zugriffstoken hat eine beschränkte Gültigkeit und sollte daher vor jedem Request geprüft und ggf. neu angefordert werden!

2. Suche nach einem Nachweisangebot

Nach dem erfolgreichen Anfordern eines Zugriffstoken kann eine Suche nach einem passenden Nachweisangebot begonnen werden. Die Suche erfolgt über eine SAK-DC Schnittstelle

Beispiel für Geburtsnachweis

```
POST https://<NOREF_URL>/de/evidence-offer
Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI...

{
  "evidence_type": "4b70194e-ae5a-417b-b8de-
6b92f8b044e3",
  "jurisdictions": {
        "ars": "012345678901"
    }
}
```

Beispiel für Meldebescheinigung

```
POST https://<NOREF_URL>/de/evidence-offer
Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI...

{
  "evidence_type": "5926157e-dd70-4abc-b6f2-
e2e6e31bbc1f",
  "jurisdictions": {
        "ars": "012345678901"
    }
}
```

HINWEIS	Sollten Sie auch für diese Schnittstelle Basic Auth aktiviert haben, achten Sie darauf diese zusätzlich zum Zugrifftoken mitzusenden. Wie dies genau aussieht, können Sie in der Integrationsanleitung des SAK-DC nachlesen.

HINWEIS	Die Referenzumgebung sendet unabhängig des abgerufenen Nachweisangebots immer denselben Test-Nachweis zurück.

3. Anfordern des Nachweises

Mit dem Ergebnis der Nachweisangebotssuche kann nun eine Anfrage für einen bestimmten Nachweis gestellt werden. Die Anfrage erfolgt über eine SAK-DC Schnittstelle.

Beispiel:

```
POST https://<NOREF_URL>/de/evidence
Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI...

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

HINWEIS	Sollten Sie auch für diese Schnittstelle Basic Auth aktiviert haben, achten Sie darauf diese zusätzlich zum Zugrifftoken mitzusenden. Wie dies genau aussieht, können Sie in der Integrationsanleitung des SAK-DC nachlesen.

Integration als Data Provider

Registrierung

Um als Data Provider in der Referenzumgebung einen Readiness-Check durchführen zu können, muss der Data Provider registriert werden. Die Registrierung erfolgt über den Support. Das Support-Team registriert anhand der Informationen den Data Provider in der Referenzumgebung, sodass der Data Provider der Anwendung bekannt ist.

Installation

Der Sichere Anschlussknoten für Data Provider muss als eigenständig lauffähige Anwendung mit Zugriff auf das Internet installiert werden. Wie

eine Installation eines SAK-DP durchzuführen ist, ist in der offiziellen Integrationsanleitung des Sicheren Anschlussknotens zu finden.

HINWEIS	Verwenden Sie bei der Einrichtung des SAK die für Sie bereitgestellten Informationen und Keystores aus der Registrierung.

Bereitstellung einer Schnittstelle zum Aufruf eines SAK-DP (DP-Trigger)

In der Referenzumgebung wird ein Endpunkt für Data Provider bereitgestellt, der den Aufruf des SAK-DP durch einen SAK-DC simuliert. Dadurch kann ein Data Provider seinen konfigurierten SAK-DP testen.

Durchlauf eines Nachweisabrufs (Readiness-Check)

Um als Data Provider nach der Registrierung und der Installation und Integration des SAK-DP zu Testen, ob ein Nachweis über den SAK-DP abgerufen werden kann, sind folgende Schritte durchzuführen (eine Schnittstellenbeschreibung der Referenzumgebung finden Sie unter Übersicht der Schnittstellendefinitionen der Referenzumgebung).

Abruf der Trigger-Schnittstelle der Referenzumgebung

Um den Readiness-Check als Data Provider durchzuführen, wird die Trigger-Schnittstelle der Referenzumgebung aufgerufen. Diese Schnittstelle ruft wiederum den installierten und integrierten SAK-DP auf, der einen Nachweis vom registrierten Data Provider bekommt. Dieser Nachweis wird als bei erfolgreichem Durchlauf zurückgegeben.

Beispiel:

```
POST https://<NOREF_URL>/trigger/evidence
traceparent: 00-0af7651916cd43dd8448eb211c80319c-
b7ad6b7169203331-01
```

Zertifikate, Keystores und Truststores

In diesem Kapitel erfahren Sie, welche Keystores und Truststores in der Referenzumgebung konfiguriert sind. Diese Komponenten sind entscheidend für die sichere Kommunikation und Authentifizierung innerhalb Ihres Systems.

Zertifikate sind digitale Dokumente, die die Identität einer Entität (z.B. eines Servers, einer Anwendung oder eines Benutzers) bestätigen. Sie werden von einer vertrauenswürdigen Zertifizierungsstelle (CA, Certificate Authority) ausgestellt und enthalten öffentliche Schlüssel, die zur Verschlüsselung und Authentifizierung verwendet werden. Zertifikate gewährleisten, dass die Kommunikation zwischen zwei Parteien sicher und

vertrauenswürdig ist.

- Keystore (Schlüsselcontainer):
  - **Inhalt:** Enthält private Schlüssel und die zugehörigen Zertifikate der eigenen Entität.
  - **Verwendung:** Wird verwendet, um die eigenen Identitätsinformationen und Verschlüsselungsschlüssel sicher zu speichern.
  - **Beispiel:** Ein Webserver verwendet einen Keystore, um sein eigenes SSL/TLS-Zertifikat und den privaten Schlüssel zu speichern.
- Truststore (Vertrauenscontainer):
  - **Inhalt:** Enthält öffentliche Zertifikate von vertrauenswürdigen Drittanbietern oder Zertifizierungsstellen.
  - **Verwendung:** Wird verwendet, um die Identität von entfernten Entitäten zu überprüfen und zu validieren.
  - **Beispiel:** Ein Client verwendet einen Truststore, um die Zertifikate von vertrauenswürdigen Zertifizierungsstellen zu speichern, die zur Validierung der Zertifikate von Servern verwendet werden.

Die folgende Grafik illustriert die benötigten Zertifikate innerhalb der Referenzumgebung im Zusammenspiel mit den Sicheren Anschlussknoten.

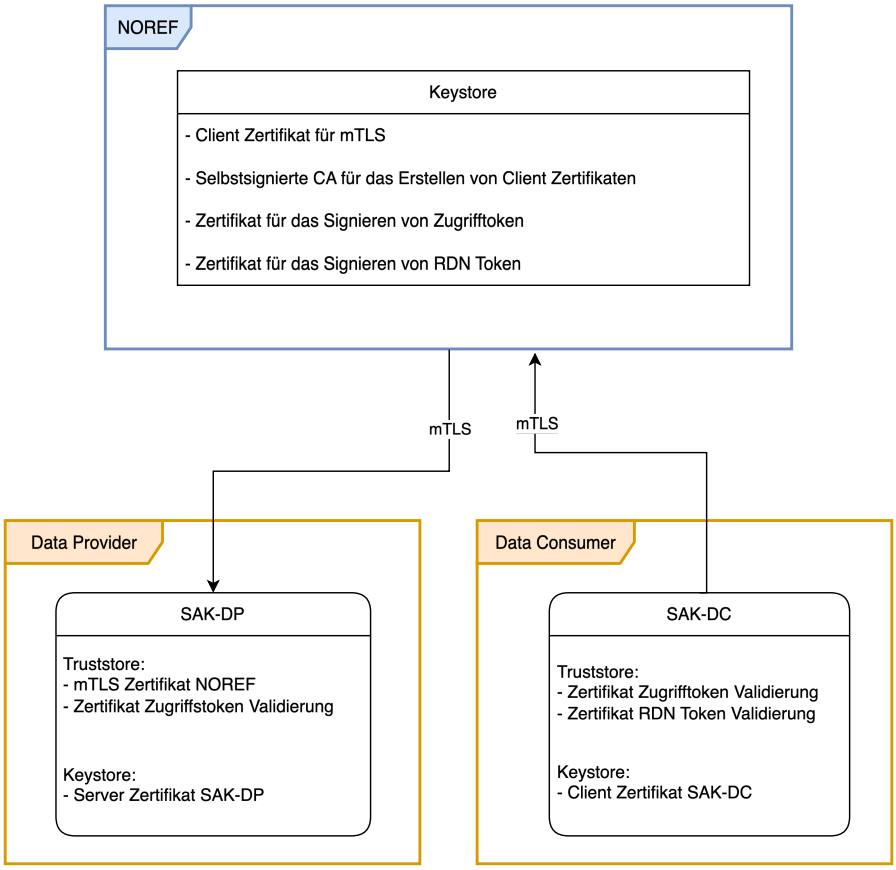


Abbildung 2. NOREF als Data Consumer und Data Provider

Zertifikat zur Token-Verifizierung

Der Datenaustausch zwischen den NOOTS-Teilnehmern erfolgt teilweise mittels gesiegelter bzw. signierter Webtokens, welche sich besonders für die Übertragung sensibler Daten eignen. Zur Sicherstellung der Datenintegrität können alle NOOTS-Teilnehmer die Siegelung überprüfen, insbesondere

- dass der Inhalt des Webtokens seit der Siegelung nicht verändert wurde, und
- dass der Teilnehmer, welcher die Siegelung angebracht hat, ein vertrauenswürdiges Zertifikat verwendet, also der ist, für den er sich ausgibt.

Letztes erfordert, dass das Siegel-Zertifikat von einer öffentlichen Stelle („Trust-Center“) bestätigt wird, oder dass dem Token-Empfänger das zugrunde liegende Ursprungszertifikat („root certificate authority“, kurz: „root-CA“) bekannt ist.

Übersicht der Schnittstellendefinitionen der Referenzumgebung

Endpunkt zum Abrufen des Zugrifftokens

HINWEIS	Dieser Endpunkt simuliert den IAM-B des NOOTS.

```
POST /token
```

Während eines Readiness-Checks wird ein Zugrifftoken benötigt. Dieser ist bei der Referenzumgebung unter dem obigen Endpunkt abzurufen.

Endpunkt zum Abrufen des Nachweises für Data Consumer

HINWEIS	Dieser Endpunkt simuliert den Data Provider für Data Consumer.

```
POST /evidence
```

Während eines Readiness-Checks für Data Consumer wird ein Test-Data-Provider benötigt. Dieser ist bei der Referenzumgebung unter dem obigen Endpunkt anzusprechen.

HINWEIS	Dieser Endpunkt liefert ausschließlich ein Nachweis zurück, unabhängig vom Nachweisangebot.

Endpunkt des Nachweisabrufs für Data Provider

```
POST /trigger/evidence
```

Ein Data Provider kann einen Readiness-Check für dessen konfigurierten SAK-DP starten, indem dieser den oben genannten Endpunkt aufruft. Eine erfolgreiche Antwort dieses Endpunktes nutzt den XÖV-Standard xNachweis.

traceparent

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

Beispielantwort im Erfolgsfall


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


Mögliche HTTP-Status-Codes

Die folgenden Fehlerfälle und Status-Codes können nach einem Aufruf der Schnittstelle auftreten:

Tabelle 1. Status Codes der DP-Trigger Schnittstelle

Status	Beschreibung
200 OK	Erfolgreiche Anfrage
204 No Content	Es konnte kein Readiness-Check über die spezifizierte Client-Id (und ggf. Komponenten-Id) gefunden werden
400 Bad Request	Die Anfrage konnte nicht bearbeitet werden, da ein Fehler durch den Anfragenden vermutet wird (z.B. fehlerhafte Anfragesyntax)
401 Unauthorized	Der Anfrage konnte nicht authorisiert werden. Dies kann z.B. durch ein ungültiges Zertifikat oder Bearertoken passieren
403 Forbidden	Der Anfragende hat nicht die passende Berechtigung den Readiness-Check für die angegebene Client-Id abzufragen
404 Not Found	Unter der angegeben URI ist keine Ressource verfügbar
500 Internal Server Error	Unerwarteter Server Error
503 Service Unavailable	Der Service steht temporär nicht zur Verfügung

Endpunkte des Sicheren Anschlussknotens für Data Consumer

Die Endpunkte des Sicheren Anschlussknotens für Data Consumer ist in dessen Systemdokumentation und Integrationsanleitung beschrieben.

Endpunkte des Sicheren Anschlussknotens für Data Provider

Die Endpunkte des Sicheren Anschlussknotens für Data Provider ist in dessen Systemdokumentation und Integrationsanleitung beschrieben.

Endpunkt des Readiness-Checks

```
POST /readiness
```

HINWEIS	Für die Ausführung dieses Endpunktes ist ein gültiges Client-Zertifikat, welches die spezifische Client-Id aus der Registrierung des Clients enthält.

Nachdem Sie ein Readiness-Check erfolgreich absolviert haben, können Sie die Bestätigung der Absolvierung über den `Readiness`-Endpunkt abrufen.

Folgende Information sollten aus Ergebnis zurückgeliefert werden:

- **client_id**: Die Client-Id des Clients für den der Readiness-Check abgerufen wird.
- **component_id**: Die Komponenten-Id des Clients.
- **client_type**: Information, ob es sich bei dem Client um ein Data Consumer oder Data Provider handelt.
- **entered_at**: Startzeitpunkt des Readiness-Checks.
- **finished_at**: Endzeitpunkt des Readiness-Checks.

ReadinessCheckId

- **Anzugeben in**: HTTP-Request-Body
- **Typ**: ReadinessCheckId

Beispiel:

```
{
  "client_id": "c1afc173-8226-4960-b61f-1bbb790fc7b4",
  "component_id": "c1afc173-8226-4960-b61f-
1bbb790fc7b4",
  "client_type": "DC"
}
```

Beispiel im Erfolgsfall

Antwort als JSON-Response-Body:

```
{
  "client_id": "c1afc173-8226-4960-b61f-1bbb790fc7b4",
  "component_id": "c1afc173-8226-4960-b61f-
1bbb790fc7b4",
  "client_type": "DC",
  "entered_at": "2018-10-29T18:54:50.630Z"
  "finished_at": "2018-10-29T18:55:50.630Z"
}
```

Mögliche HTTP-Status-Codes

Die folgenden Fehlerfälle und Status-Codes können nach einem Aufruf der Schnittstelle auftreten:

Tabelle 2. Status Codes der Readiness-Check Schnittstelle

Status	Beschreibung
200 OK	Erfolgreiche Anfrage
204 No Content	Es konnte kein Readiness-Check über die spezifizierte Client-Id (und ggf. Komponenten-Id) gefunden werden
400 Bad Request	Die Anfrage konnte nicht bearbeitet werden, da ein Fehler durch den Anfragenden vermutet wird (z.B. fehlerhafte Anfragesyntax)
401 Unauthorized	Der Anfrage konnte nicht authorisiert werden. Dies kann z.B. durch ein ungültiges Zertifikat passieren
403 Forbidden	Der Anfragende hat nicht die passende Berechtigung den Readiness-Check für die angegebene Client-Id abzufragen
404 Not Found	Unter der angegeben URI ist keine Ressource verfügbar
500 Internal Server Error	Unerwarteter Server Error
503 Service Unavailable	Der Service steht temporär nicht zur Verfügung

Kontaktinformationen

Kontakt	Information
Bundesverwaltungsamt (Referat D III 3)	Registermodernisierung@bva.bund.de
Technischer Support (Dataport)	dataportnootssupport@dataport.de

Glossar

(siehe "Architekturkonzept Programm NOOTS"[1], Kapitel 12. "Glossar")

[1] https://kundenportal.dataport.de/websites/1159/Architekturboard/Architekturkonzept_Dataport_NOOTS_V1.0.pdf