Bundesverwaltungsamt

D II 4

# NOOTS MVP – Umfang & Abgrenzung

für

## Programmmanagement BVA Programmleitung Dataport

Version 1.4.0
Datum 01. April 2025

Das vorliegende Dokument wurde durch das Bundesverwaltungsamt in Zusammenarbeit mit den Firmen SEITENBAU und Dataport erstellt.


SEITENBAU

**Ansprechpartner/-in**:

Herr André Nollmann
D II 4
Bundesverwaltungsamt
E-Mail: noots.umsetzung@bva.bund.de

## Dokumentinformationen

| | |
|---|---|
| Speicherdatum: | 07.05.2025 |
| Version: | 1.4.0 |
| Zustand: | ☐ in Bearbeitung seit: TT.MM.JJJJ<br><br>☐ vorgelegt am:<br><br>☒ abgenommen |
| Verfasser: | Martina Koch, Harald Krause |
| Projektleiter: | André Nollmann |
| Dokumenten-ID: | NOOTS_MVP_v1.4.0.docx |

## Dokumentenhistorie

| Datum | Version | Änderungsgrund | Bearbeiter |
|---|---|---|---|
| 31.10.2024 | 0.5 | Initiale Erstellung | Martina Koch |
| 01.11.2024 | 0.6 | Fortschreibung | Harald Krause |
| 01.11.2024 | 0.9 | Fortschreibung | Martina Koch, Harald Krause |
| 05.11.2024 | 0.9.1 | Fortschreibung | Martina Koch, Harald Krause |
| 13.11.2024 | 0.9.2 | Fortschreibung | Martina Koch, Harald Krause |
| 20.11.2024 | 1.0.0 | Einarbeitung Reviewkommentare | Martina Koch, Harald Krause |
| 27.11.2024 | 1.0.1 | Fortschreibung | Martina Koch, Harald Krause |
| 13.02.2024 | 1.1.0 | Fortschreibung | Martina Koch, Harald Krause |
| 05.03.2024 | 1.2.0 | Fortschreibung | Martina Koch, Harald Krause |
| 19.03.2024 | 1.3.0 | Einarbeitung Reviewkommentare | Martina Koch |
| 01.04.2025 | 1.4.0 | Aufnahme der Anforderungen aus dem Support-Team | Martina Koch |

# Inhaltsverzeichnis

# 1. Management Summary

Das vorliegende Dokument beschreibt den Umfang des Minimum Viable Products (MVP) von NOOTS. Im Dokument werden die getroffenen Annahmen beschrieben, Abgrenzungen vorgenommen, Rahmenbedingungen definiert und der geplante Zeitrahmen zur Beendigung von MVP festgelegt.

Das produktive NOOTS soll iterativ bis zum vollständigen Funktionsumfang entwickelt werden. In diesem Dokument wird das Minimum Viable Product (MVP) beschrieben. In den folgenden Iterationen wird das NOOTS sukzessive erweitert.

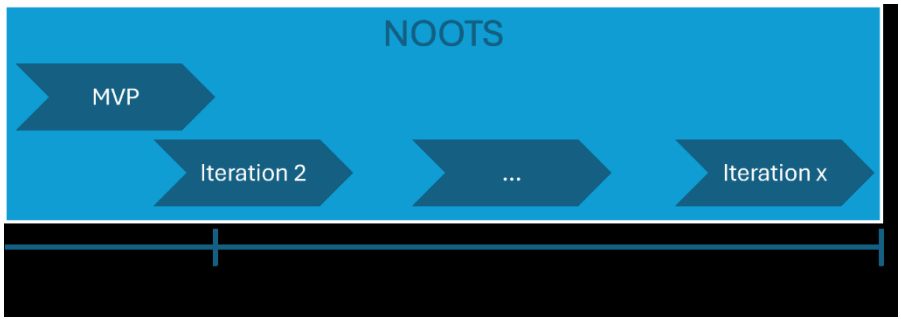


*Abbildung 1: Iterationen des NOOTS bis zur Gesamtfertigstellung in 2028*

Das MVP hat zum Ziel eine minimale, funktionsfähige, produktiv eingesetzte Version des NOOTS bereitzustellen, an die sich Data Consumer und Data Provider produktiv anbinden und Nachweise mit Echtdaten austauschen können. Im MVP steht die Umsetzung der beiden Use Cases NOOTS UP 01_2025 - Bürgerzentriert und NOOTS UP 02_2025 – Wirtschaftszentriert im Fokus. Des Weiteren können zusätzliche Data Consumer oder Data Provider produktiv angeschlossen werden.

## 1.1. Lesehinweise

Die verwendeten Begriffe, insbesondere hinsichtlich der unterstützten Funktionalitäten oder Abgrenzungen, entstammen in der Regel aus den Grobkonzepten der HLA. D.h. falls ein Begriff nicht selbsterklärend ist, sollte der Begriff im entsprechenden Grobkonzept der HLA beschrieben sein.

# 2. MVP-Inhalt

## 2.1. Anforderungen

Die im vorliegenden Dokument aufgeführten Anforderungen entsprechen dem Stand von November 2024. Eine abschließende Liste der zu erfüllenden Anforderungen ist in Jira im Projekt „NOOTSKUN“ dokumentiert. Alle MVP-relevanten Anforderungen sind mit den Schlagworten „MVP“ bzw. „MVP_teilweise“ gekennzeichnet. Anforderungen, die im MVP optional erfüllt werden sollen, werden nicht mit den genannten Schlagworten gekennzeichnet, da das MVP nur das absolute Minimum der zu erfüllenden Anforderungen umfasst. Weitere Anforderungen können erfüllt werden, wenn dies zeitlich und kapazitätsmäßig leistbar ist.

## 2.2. Konzeptions-Basis des MVP

Die Grobkonzepte der HLA (Stand Q3/2024) bilden die Basis für den MVP. Wurden die Grobkonzepte seitdem überarbeitet und können diese Änderungen aufwandsneutral im MVP berücksichtigt werden, wird geprüft, ob die neuere Version der HLA-Konzepte berücksichtigt wird, jedoch ist die Berücksichtigung neuere HLA-Versionen nicht verbindlich vorgegeben.

## 2.3. NOOTS-Komponenten

Im Folgenden werden die im MVP enthaltenen NOOTS-Komponenten und deren Umfang beschrieben, dabei werden bestimmte Annahmen getroffen und Ausschlüsse definiert, die für den MVP gelten.

Die folgenden nichtfunktionalen Anforderungen werden im MVP erfüllt:

- NOOTS-735 - Das NOOTS MUSS alle einschlägigen Datenschutzvorschriften einhalten.
- NOOTS-738 - Das NOOTS MUSS die einschlägigen nationalen IT-Sicherheitsstandards erfüllen.
- NOOTS-739 - Das NOOTS MUSS bei der Übertragung schützenswerter Daten deren Vertraulichkeit sicherstellen.
- NOOTS-741 - Das NOOTS MUSS sicherstellen, dass Nachweise nur in notwendigem Umfang und für die notwendige Dauer innerhalb des NOOTS verarbeitet werden.
- NOOTS-836 Das NOOTS MUSS eine effiziente Lokalisierung und Analyse von Fehlern wirksam unterstützen.
- NOOTS-628 - Das NOOTS MUSS innerhalb von 60s eine Antwort liefern.

Die unten aufgeführten nichtfunktionalen Anforderungen werden optional im MVP erfüllt:

- NOOTS-713 - Das NOOTS SOLL die Migration zu moderneren Transportstandards nicht erschweren.
- NOOTS-628 - Das NOOTS SOLL bei Abrufen von nationalen Nachweisen innerhalb von 40s eine Antwort liefern.

### 2.3.1 Sicherer Anschlussknoten des Data Consumers

Der Sichere Anschlussknoten des Data Consumer (SAK-DC) unterstützt die folgenden Anwendungsfälle der HLA nicht:

- 1a – Interaktiver Nachweisabruf zu einer natürlichen Person über das NOOTS mit IDNr
- 1b – interaktiver Nachweisabruf zu einem Unternehmen über das NOOTS mit beWiNr
- 2 – Nicht-interaktiver Nachweisabruf über das NOOTS
- 3 – Abruf von nationalen Nachweisen aus EU-Mitgliedsstaaten über das EU-OOTS
- 4 – Abruf von europäischen Nachweisen durch nationale Data Consumer über das EU-OOTS

Der SAK-DC unterstützt die folgenden Anwendungsfälle der HLA

- 1a – Interaktiver Nachweisabruf zu einer natürlichen Person über das NOOTS mit Basisdaten ( → NOOTS UP 01_2025 – Bürgerzentriert)
- 1b – interaktiver Nachweisabruf zu einem Unternehmen über das NOOTS mit Basisdaten (→ NOOTS UP 02_2025 – Wirtschaftszentriert)

mit folgenden Einschränkungen:

- Der SAK-DC unterstützt im MVP keine Nachweisabfrage mit IDNr oder beWiNr.
- Der SAK-DC unterstützt im MVP keinen Aufruf zur Intermediäre Plattform.
- Der SAK-DC unterstützt ausschließlich die XNachweis-Version 1.4.0. Andere Versionen von XNachweis werden im MVP nicht unterstützt.
- Der SAK-DC ist im MVP nicht mandantenfähig.
    - Es ist für jeden Data Consumer (DC) ein separater SAK-DC nötig.

- Es findet keine Abstrakte Berechtigungsprüfung und auch kein Aufruf der Vermittlungsstelle statt.
    - Da die Nachweisabfrage mit IDNr bzw. beWiNr im MVP nicht unterstützt wird, ist keine abstrakte Berechtigungsprüfung erforderlich.
- Der SAK-DC prüft die Siegelung der Verbindungs- und Zuständigkeitstokens der RDN nicht, da der SAK-DC die Tokens selbst über eine sichere Verbindung angefordert hat und eine Kompromittierung der Siegel daher nicht erfolgen konnte.
- Bei Zertifikatsprüfungen wird der Revocationstatus nicht geprüft.
- Es wird keine verteilte Nachrichtenverfolgung unterstützt. (Die Trace-ID wird in den Nachrichten und Logs enthalten sein, um eine mögliche Fehleranalyse zu unterstützen.)
- Der SAK-DC unterstützt keinen Parallelbetrieb von unterschiedlichen Versionen von Standards und Schnittstellen.
    - Anforderung NOOTS-717 wird im MVP nicht unterstützt.
- Der SAK-DC wird ausschließlich als jar bereitgestellt.
- Der SAK-DC wird zur Integration in eine bestimmte, vordefinierte Infrastruktur für Überwachung (Protokollierung, Logging, Monitoring) vorgesehen, d.h. es findet keine flexible Unterstützung verschiedener Infrastrukturen im MVP statt
- Eine horizontale Lastverteilung (z.B. durch Load Balancer) obliegt der Verantwortung des Data Consumers. Es wird keine Stickiness unterstützt.
- Die Transportinfrastruktur im MVP ist auf einen Teilnehmeranzahl im niedrigen zweistelligen Bereich ausgelegt.
    - Die Anforderung NOOTS-413 wird noch nicht vollumfänglich unterstützt.
- Der Betrieb im Katastrophenfall wird noch nicht im MVP geleistet.
    - Die Anforderung NOOTS-878 wird im MVP nicht gewährleistet.
- Das technische Log des SAK-DC enthält im Standard-Log-Level keine personenbezogenen Daten.
    - Die Informationen, die je Log-Level enthalten sein dürfen, sind durch das IT-Sicherheitskonzept zu definieren.
- Logs werden auf der Konsole oder in eine Datei ausgegeben.
- Die in den Grobkonzepten der HLA beschriebenen Audit-Logs werden im MVP nicht erstellt.
- Der SAK-DC bietet keine Tracing-API.

- Der SAK-DC unterstützt folgende Fehlerszenarien, für die ein Logeintrag erstellt wird:
  Wenn beim SAK-DC im Rahmen eines Aufrufs durch den DC ein Fehler entstanden ist, dann muss er zu diesem Fehler einen Log-Eintrag schreiben. Der Log-Eintrag soll eine eindeutige Unterscheidung zwischen folgenden Fällen ermöglichen:
    - Der SAK-DC ist nicht in der Lage eine Verbindung zu einer zentralen NOOTS Komponente aufzubauen
      - Benötigte Info: Welche Komponente kann nicht erreicht werden
    - Der SAK-DC konnte eine Verbindung zu einer zentralen NOOTS Komponente aufbauen, dort ist jedoch ein Fehler aufgetreten
      - Benötigte Info: Welche NOOTS Komponente?
      - Benötigte Info: Fehlercodes und -informationen der NOOTS Komponente
    - Der SAK-DC ist nicht in der Lage eine Verbindung zu einem Data Provider aufzubauen
      - Benötigte Info: Welcher DP (service-id)
    - Der SAK-DC konnte eine Verbindung zu einem Data Provider aufbauen, dort ist jedoch ein Fehler aufgetreten
      - Benötigte Info: Welcher DP (service-id)
      - Benötigte Info: Fehlercodes und -informationen des SAK-DP
- Der SAK-DC muss bei jedem Logeintrag in Zusammenhang mit einem Aufruf durch den DC (insbesondere bei dabei auftretenden Fehlern) eine Trace-ID dazu loggen, sofern diese vom DC übermittelt wurde. Wenn der DC keine Trace-ID beim Aufruf des SAK-DC mitgibt, wird keine Trace-ID erzeugt und gelogged.
- Wenn beim Aufruf einer NOOTS Komponente durch einen SAK-DC ein Fehler auftritt und an den SAK-DC zurückgespielt wird, dann muss dieser Fehler geloggt werden. Der Log-Eintrag muss enthalten
  - die Trace-ID, die vom SAK-DC übergeben wurde,
  - die Parameter, mit denen die Komponente aufgerufen wurde (sofern rechtlich zulässig),
  - eine Information zum Fehler.
- Der SAK-DC ermöglicht dem Data Consumer wahlweise unverschlüsselt, mTLS oder TLS-verschlüsselt zu kommunizieren und sich per http-basic-auth zu

authentifizieren. Der NOOTS-Teilnehmer muss in jedem Fall dem Schutzbedarf hoch gerecht werden.
- Der SAK-DC stellt einen Health-Endpunkt zur Verfügung, der für die betriebsverantwortliche Stelle des DC abfragbar ist.
-

Es werden folgenden Annahmen / Rahmenbedingungen zugrunde gelegt:

- Die fachliche und organisatorische Dokumentation für den Data Consumer zur Verwendung des SAK-DC und zum Anschluss an NOOTS wird durch das BVA erstellt.
- Gemäß der Vorgabe des ISB des BVA darf der Code des NOOTS-PoC nicht im MVP wiederverwendet werden, dennoch wird folgende Entwicklungsleistungen des NOOTS-PoC zur Weiterverwendung im MVP vorgesehen:
    - Die Abnahmetests werden aus dem NOOTS-PoC weiterverwendet und nur an ggf. geänderte Schnittstellen bzw. Datenformat angepasst
    - Der Code für Infrastruktur, Buildpipeline, Deployment, etc. darf im MVP wiederverwendet werden.
- Der SAK-DC soll die Vertraulichkeit der Nachrichten für Nachweise sicherstellen sowie die einschlägigen Datenschutzvorschriften und nationalen IT-Sicherheitsstandards einhalten und den Schutzbedarf hoch erfüllen.
    - Die Erfüllung der Anforderungen NOOTS-427, NOOTS-735, NOOTS-738 wird gemäß den Vorgaben aus den Grobkonzepten der HLA umgesetzt.
- Der für den SAK-DC verwendete Technologiestack kann dem des PoC entsprechen oder auf dem von Dataport vorgegebenen Technologiestack basieren.
    - Dataport hat den Technologistack vollständig bis zum 15.11.2024 definiert.
- In der Architektur des SAK-DC werden keine Vorgaben von IsyFact berücksichtigt
- Die Bereitstellung des SAK-DC für Data Consumer erfolgt über das Download-Portal, siehe Kapitel 2.4.2

Die folgenden nichtfunktionalen Anforderungen werden im MVP erfüllt oder teilweise erfüllt:

- NOOTS-413 - Die Transportinfrastruktur MUSS in der Lage sein, Nachrichten zwischen einer großen Anzahl an

Teilnehmern (>100 Data Consumer; >10.000 Data Provider; Komponenten des NOOTS) zu transportieren. (Anforderung wird nicht vollumfänglich erfüllt: Das MVP wird auf eine Teilnehmerzahl im niedrigen zweistelligen Bereich ausgelegt.)
- NOOTS-427 - Die Transportinfrastruktur MUSS die Vertraulichkeit der Nachrichten für Nachweise des Schutzbedarfs hoch sicherstellen.
- NOOTS-428 - Die Transportinfrastruktur MUSS die Authentizität der Teilnehmer bei der Zustellung von Nachrichten sicherstellen.
- NOOTS-429 - Die Transportinfrastruktur MUSS sicherstellen, dass Nachrichten beim Transport nicht verändert werden können.
- NOOTS-436 - Die Transportinfrastruktur MUSS sicherstellen, dass die Sicherheit des Transports durch unsachgemäßen Anschluss der Teilnehmer nicht kompromittiert werden kann.
- NOOTS-440 - Die Transportinfrastruktur MUSS für eine Request-Response Kommunikation eine maximale Zustellzeit von 4 Sekunden sicherstellen.
- NOOTS-712 - Die Transportinfrastruktur MUSS die Anbindung von Teilnehmern erlauben, die selbst keinen direkten Zugang zu den Behördennetzen erhalten.

### 2.3.2 Sicherer Anschlussknoten des Data Providers

Der Sichere Anschlussknoten des Data Providers (SAK-DP) unterstützt die folgenden Anwendungsfälle der HLA nicht:

- 1a – Interaktiver Nachweisabruf zu einer natürlichen Person über das NOOTS mit IDNr
- 1b – interaktiver Nachweisabruf zu einem Unternehmen über das NOOTS mit beWiNr
- 2 – Nicht-interaktiver Nachweisabruf über das NOOTS
- 3 – Abruf von nationalen Nachweisen aus EU-Mitgliedsstaaten über das EU-OOTS
- 4 – Abruf von europäischen Nachweisen durch nationale Data Consumer über das EU-OOTS

Der SAK-DP unterstützt die folgenden Anwendungsfälle der HLA

- 1a – Interaktiver Nachweisabruf zu einer natürlichen Person über das NOOTS mit Basisdaten (→ NOOTS UP 01_2025 – Bürgerzentriert)

- 1b – interaktiver Nachweisabruf zu einem Unternehmen über das NOOTS mit Basisdaten (→ NOOTS UP 02_2025 – Wirtschaftszentriert)

mit folgenden Einschränkungen:

- Der SAK-DP unterstützt im MVP keine Nachweisabfrage mit IDNr oder beWiNr.
- Der SAK-DP unterstützt im MVP keine Abfrage durch die Intermediäre Plattform.
- Der SAK-DP unterstützt ausschließlich die XNachweis-Version 1.4.0. Andere Versionen von XNachweis werden im MVP nicht unterstützt.
- Der SAK-DP ist im MVP nicht mandantenfähig.
    - Es ist für jeden Data Provider (DP) ein separater SAK-DP nötig.
- Der SAK-DP unterstützt als Anschlussprotokoll ausschließlich die Empfangsart „passiver Empfänger“. Die Empfangsart „aktiver Empfänger“ wird nicht unterstützt im MVP.
- Es findet keine Abstrakte Berechtigungsprüfung statt.
    - Da die Nachweisabfrage mit IDNr bzw. beWiNr im MVP nicht unterstützt wird, ist keine abstrakte Berechtigungsprüfung erforderlich.
- Bei Zertifikatsprüfungen wird der Revocationstatus nicht geprüft.
- Es wird keine verteilte Nachrichtenverfolgung unterstützt. (Trace-ID wird in den Nachrichten und Logs enthalten sein, um eine mögliche Fehleranalyse zu unterstützen.)
- Der SAK-DP unterstützt keinen Parallelbetrieb von unterschiedlichen Versionen von Standards und Schnittstellen.
    - Anforderung NOOTS-717 wird im MVP nicht unterstützt.
- Der SAK-DP wird ausschließlich als jar bereitgestellt.
- Der SAK-DP wird zur Integration in eine bestimmte, vordefinierte Infrastruktur für Überwachung (Protokollierung, Logging, Monitoring) vorgesehen, d.h. es findet keine flexible Unterstützung verschiedener Infrastrukturen im MVP statt
- Eine horizontale Lastverteilung (z.B. durch Load Balancer) obliegt der Verantwortung des Data Providers. Es wird keine Stickiness unterstützt.
- Die Transportinfrastruktur im MVP ist auf eine Teilnehmeranzahl im niedrigen zweistelligen Bereich ausgelegt.

    - Die Anforderung NOOTS-413 wird noch nicht vollumfänglich unterstützt.
- Der Betrieb im Katastrophenfall wird noch nicht im MVP geleistet.
    - Die Anforderung NOOTS-878 wird im MVP nicht gewährleistet.
- Das technische Log des SAK-DP enthält im Standard-Log-Level keine personenbezogenen Daten.
- Die Informationen, die je Log-Level enthalten sein dürfen, sind durch das IT-Sicherheitskonzept zu definieren. Logs werden auf der Konsole oder in eine Datei ausgegeben.
- Die in den Grobkonzepten der HLA beschriebenen Audit-Logs werden im MVP nicht erstellt.
- Der SAK-DP bietet keine Tracing-API.
- Der SAK-DP ermöglicht dem Data Provider wahlweise unverschlüsselt, mTLS oder TLS-verschlüsselt zu kommunizieren. Der NOOTS-Teilnehmer muss in jedem Fall dem Schutzbedarf hoch gerecht werden.
- Der SAK-DP stellt einen Health-Endpunkt zur Verfügung, der für die betriebsverantwortliche Stelle des DP abfragbar ist.

Es werden folgenden Annahmen / Rahmenbedingungen zugrunde gelegt:

- Die fachliche und organisatorische Dokumentation für den Data Provider zur Verwendung des SAK-DP und zum Anschluss an NOOTS wird durch das BVA erstellt.
- Gemäß der Vorgabe des ISB des BVA darf der Code des NOOTS-PoC nicht im MVP wiederverwendet werden, dennoch wird folgende Entwicklungsleistungen des NOOTS-PoC zur Weiterverwendung im MVP vorgesehen:
    - Die Abnahmetests werden aus dem NOOTS-PoC weiterverwendet und nur an ggf. geänderte Schnittstellen bzw. Datenformat angepasst.
    - Der Code für Infrastruktur, Buildpipeline, Deployment, etc. darf im MVP wiederverwendet werden.
- Der SAK-DP soll die Vertraulichkeit der Nachrichten für Nachweise sicherstellen sowie die einschlägigen Datenschutzvorschriften und nationalen IT-Sicherheitsstandards einhalten und den Schutzbedarf hoch erfüllen.

    - Die Erfüllung der Anforderungen NOOTS-427, NOOTS-735, NOOTS-738 wird gemäß der Vorgaben aus den Grobkonzepten der HLA umgesetzt.
- Der für den SAK-DP verwendete Technologiestack kann dem des PoC entsprechen oder auf dem von Dataport vorgegebenen Technologiestack basieren.
    - Dataport hat den Technologistack vollständig bis zum 15.11.2024 definiert.
- In der Architektur des SAK-DP werden keine Vorgaben von IsyFact berücksichtigt.
- Die Bereitstellung des SAK-DP für Data Provider erfolgt über das Download-Portal, siehe Kapitel 2.4.2.

#### 2.3.3 IAM für Behörden

Das IAM für Behörden (IAM-B) unterstützt folgende Anwendungsfälle:

- Authentifizierung der IT-Komponente auf Grundlage des Client-TLS-Zertifikat des SAK-DC
- Ausstellung des Zugriffstokens mit Attributen zur IT-Komponente sowie fach- und betriebsverantwortlichen Stelle

mit folgenden Einschränkungen:

- Im MVP unterstützt das IAM-B keine Web-Dialoge für den Self-Service für öffentliche oder sonstige Stellen.
    - Die Registrierung von IT-Komponenten und fach- und betriebsverantwortlichen Stellen sowie die Erfassung von Grunddaten erfolgt durch Mittel des technischen oder fachlichen Verfahrensmanagements (TVM, FVM).
    - Zu den so erfassten Daten zählen insbesondere Client-TLS-Zertifikate der SAK-DC sowie Teilnahmeart und Behördenfunktion der IT-Komponente.
    - Es werden im MVP keine den registrierten fach- und betriebsverantwortlichen Stellen zugeordnete Zertifikate hinterlegt. Entsprechend erfolgt zum Zeitpunkt des Abrufs von Zugriffstoken keine Gültigkeitsvalidierung der zur IT-Komponente assoziierten Stellen.
    - Die durchs TVM oder FVM registrierten Daten zu fach- und betriebsverantwortlichen Stellen wie Organisationsname, Funktionsträger und Anschrift entstammen nicht von Zertifikaten der Stellen.
- Es werden keine Funktionen zur Prüfung hinterlegter Daten durch Fachaufsichten unterstützt.

- Bei Zertifikatsprüfungen wird der Revocationstatus nicht geprüft.

Es werden folgenden Annahmen / Rahmenbedingungen zugrunde gelegt:

- Vor dem IAM-B steht kein SAK. Die mTLS-Terminierung und Tokenprüfung findet für alle zentralen NOOTS-Komponenten in einheitlicher Weise statt (siehe Kapitel **2.4.4**).
- In der Architektur des IAM-B werden keine Vorgaben von IsyFact berücksichtigt.
- Das IAM-B erfüllt den Schutzbedarf hoch.

#### 2.3.4 Registerdatennavigation

Die Registerdatennavigation (RDN) unterstützt die folgenden Anwendungsfälle nicht:

- 2 – Zuständige Intermediäre Plattform ermitteln
- 4 – Zuständigkeiten aktualisieren
- 5 – Once-Only-Dienste aktualisieren

Der RDN unterstützt die folgenden Anwendungsfälle

- 1 – Zuständigen Data Provider ermitteln
- 3 – Verbindungsparameter eines Once-Only-Dienstes ermitteln

mit folgenden Einschränkungen:

- Im MVP muss die RDN für einen Nachweistyp einen vordefinierten Data Provider als zuständig ermitteln und an die aufrufende Stelle zurückgeben. Data Provider können zentrale oder dezentrale Register sein. Im MVP werden ausschließlich Data Provider unterschiedlicher Fachlichkeiten unterstützt, d.h. es ist nicht möglich mehrere Register desselben Registertyps anzubinden.
- Die Ausgestaltung des Datenmodells basiert nicht auf den Vorgaben des FDK.
- Ein Import aus dem Nachweiskatalog (NWK) oder Once-Only-Diensteverzeichnis (OODV) erfolgt nicht.
    - Die von der RDN benötigten Daten werden durch das Projektteam erzeugt und bereitgestellt.
- Die RDN stellt im MVP keine Technische Administration bereit.
- In den von der RDN erzeugten Token ist im MVP keine Sperrliste (CRL) enthalten.

- Bei Zertifikatsprüfungen wird der Revocationstatus nicht geprüft.
- Vor der RDN steht kein SAK. Die mTLS-Terminierung und Tokenprüfung findet zentral für alle zentralen NOOTS-Komponenten, z.B. in einem API-Gateway statt (siehe Kapitel **2.4.4**).
- Die RDN unterstützt keinen Parallelbetrieb von unterschiedlichen Versionen von Standards und Schnittstellen
    - Anforderung NOOTS-717 wird im MVP nicht unterstützt.
- Die in den Grobkonzepten der HLA beschriebenen Audit-Log werden im MVP nicht erstellt.
- Logs werden auf der Konsole oder in eine Datei ausgegeben.
    - Die Struktur von Log-Ausgaben wird von Dataport für die zentralen NOOTS-Komponenten vorgegeben.
- Das IAM-B stellt einen Health-Endpunkt zur Verfügung, der für die betriebsverantwortliche Stelle des IAM-B abfragbar ist.

Es werden folgenden Annahmen / Rahmenbedingungen zugrunde gelegt:

- Die RDN basiert auf dem von Dataport vorgegebenen Technologiestack, dabei wird das Ziel der Herstellerunabhängigkeit und die Verwendung von Open Source berücksichtigt.
    - Dataport hat den Technologistack vollständig bis zum 30.11.2024 definiert.
- In der Architektur der RDN werden keine Vorgaben von IsyFact berücksichtigt.
- Die Registerdatennavigation (RDN) hat kein UI.
- Gemäß der Vorgabe des ISB des BVA darf der Code des NOOTS-PoC nicht im MVP wiederverwendet werden, dennoch wird folgende Entwicklungsleistungen des NOOTS-PoC zur Weiterverwendung im MVP vorgesehen:
    - Die Abnahmetests werden aus dem NOOTS-PoC weiterverwendet und nur an ggf. geänderte Schnittstellen bzw. Datenformat angepasst.
    - Der Code für Infrastruktur, Buildpipeline, Deployment, etc. darf im MVP wiederverwendet werden.
- Die RDN erfüllt den Schutzbedarf hoch.
- Die RDN stellt einen Health-Endpunkt zur Verfügung, der für die betriebsverantwortliche Stelle des RDN abfragbar ist.

Die folgenden nichtfunktionalen Anforderungen werden im MVP erfüllt:

- NOOTS-795 - Die RDN SOLL in 95% der Fälle eine Antwortzeit von unter 2 Sekunden erreichen und MUSS innerhalb von unter 3 Sekunden eine Antwort liefern.

#### 2.3.5 Vermittlungsstelle

Im MVP ist keine Vermittlungsstelle (VS) enthalten.

Da die Nachweisabfrage mit IDNr bzw. beWiNr im MVP nicht unterstützt wird (siehe Kapitel 2.3.1 und 2.3.2), ist keine abstrakten Berechtigungsprüfung erforderlich.

#### 2.3.6 Intermediäre Plattform

Die Intermediäre Plattform (IP) wird im MVP nicht als funktionsfähige Einheit betrieben werden. Stattdessen wird deren Subkomponente „eDelivery Access Point“ (eDAP) als technische Kommunikationsschnittstelle in einer rudimentären Form bereitgestellt, die prinzipiell die Adressierbarkeit durch OOTS-Infrastrukturen der EU-Mitgliedsstaaten gestattet.

Diese rudimentäre Bereitstellung des eDAP genügt folgenden Anforderungen und Restriktionen:

- Der eDAP stellt einen Empfangspunkt für eDelivery-Nachrichten im Internet bereit.
- Der eDAP verarbeitet und speichert keine empfangenen fachlichen Nachrichten (eDelivery-Payload) und somit auch keine personenbezogenen oder -beziehbaren Daten.
- Der eDAP antwortet auf eingehende Nachrichten protokollkonform generell mit einer synchronen Fehlermeldung.
- Der eDAP sendet keine asynchronen Nachrichten an andere Access Points.
- Der eDAP wird bis auf Weiteres in der dSecureCloud betrieben.

Die Umsetzbarkeit der aufgeführten Anforderungen stützt sich dabei auf folgende, gegenwärtig nicht validierte Annahmen:

- Die eDAP-Instanz kann durch das auch von der IP-Implementierung verwendete Produkt Domibus (Sample-Implementierung der EU-Kommission) realisiert und in der dSecureCloud betrieben werden.

- Die binäre Distribution von Domibus kann durch Konfiguration des Produktes oder der Infrastruktur, also ohne Anpassungen im Quelltext, so betrieben werden, dass auf eingehende eDelivery-Nachrichten pauschal mit protokollkonformen (eDelivery) Fehlernachrichten geantwortet wird.
- Als Fehlermeldung bzw. Fehlercode kann eine Information geliefert werden, die eine allgemeine Nichterreichbarkeit o.ä. für anfragende Systeme sinnvoll ausdrückt.
- Bei in dieser Form konfigurierten Domibus-Instanz kann sichergestellt werden, dass keine fachlichen Daten und insb. keine personenbezogenen oder -beziehbaren Daten verarbeitet und gespeichert werden.

Sollte sich bei eingehender Analyse ergeben, dass eine oder mehrere Annahmen nichtzutreffend sind, wäre ein alternatives Vorgehen abzustimmen.

#### 2.3.7 Identity Management für Personen

Im MVP ist kein Identity Management für Personen (IDM-P) enthalten.

- Da die Nachweisabfrage mit IDNr im MVP nicht unterstützt wird (siehe Kapitel 2.3.1 und 2.3.2), ist keine Ermittlung der IDNr erforderlich.

#### 2.3.8 Identity Management für Unternehmen

Im MVP ist kein Identity Management für Unternehmen (IDM-U) enthalten.

- Da die Nachweisabfrage mit beWiNr im MVP nicht unterstützt, ist keine Ermittlung der beWiNr erforderlich.

### 2.4. Sonstige Komponenten und Aspekte

#### 2.4.1 Datenschutzcockpit

Das Datenschutzcockpit (DSC) in der Rolle der Transparenzstelle, die für Bürger nachvollziehbar macht, welche Datenübermittlungen mittels der IDNr stattgefunden haben, ist für den MVP nicht relevant. Die Anbindung des DSC als Data Consumer oder Data Provider bleibt davon unbenommen.

#### 2.4.2 SAK-Bereitstellung

Dataport stellt eine Downloadmöglichkeit für die SAK-DC und SAK-DP zur Verfügung, sodass die NOOTS-Teilnehmer die aktuelle Version der

Komponenten herunterladen können. Die Softwarekomponenten werden signiert.

#### 2.4.3 Zertifizierungsstelle

- Zertifikate der zentralen NOOTS-Komponenten für Server-TLS und Token-Siegelung innerhalb der produktiven Umgebung (NOINF-PROD) werden über kommerzielle Zertifizierungsstellen durch Dataport bereitgestellt.
- Für die Testumgebungen werden die Zertifikate aus der Dataport-PKI erstellt und bereitgestellt.
- Dagegen gilt für die Client-TLS-Zertifikate der SAK:
    - Geeignete Zertifizierungsstellen, über die die Data Consumer ihre Authentisierungszertifikate beziehen, sind durch das BVA festzulegen.
    - Bis zur Festlegung wird von der Nutzung der Verwaltungs-PKI (DOI CA Deutschland) zu diesem Zweck ausgegangen.
    - Ein Wechsel der zulässigen Wurzelzertifizierungsstellen oder koexistierende Alternativen muss möglich sein.

#### 2.4.4 Mutual TLS-Terminierung

Die Terminierung von Mutual TLS (mTLS) vor den zentralen NOOTS-Komponenten (IAM-B, RDN) und die Validierung der Client-TLS-Zertifikate erfolgt für alle Komponenten in einheitlicher Weise. Die genaue Ausgestaltung der technischen Umsetzung (z.B. Terminierung in einem Application Layer Gateway, den Ingress Controllern oder durch die Applikation im Container) wird noch festgelegt.

#### 2.4.5 Last und Performance

Bezüglich Leistungseffizienz (Durchsatz und Antwortzeiten) der NOOTS-Komponenten des MVP gelten folgende Aussagen:

- Die Architektur der MVP-Implementierungen sind skalierungsfähig ausgelegt und gestatten bei entsprechender Auslegung (Sizing) der Produktionsinfrastruktur hohe zweistellige Abrufe von Zugriffstoken pro Sekunde.
- Die Ausstellung der Zugriffs-, Zuständigkeits- und Verbindungstoken werden jeweils innerhalb von maximal drei Sekunden nach Abruf beantwortet.
- Durch Lasttests der Token-Abrufe in der Staging-Umgebung (NOINF-QS-STAGE) wird die grundsätzliche Skalierungsfähigkeit der Komponenten nachgewiesen und

Sizing-Abschätzungen für künftige produktive Lastszenarien ermittelt.
- Für die erste produktive Phase in 2025 mit der initialen Auslegung der Produktionsinfrastruktur wird jedoch keine hohe zweistellige Anzahl von Abrufen je Sekunde garantiert.

#### 2.4.6 Betriebs-Tools

- Es wird ein geeignetes System durch den Betrieb bereitgestellt, das es insbesondere den Support-Mitarbeitern ermöglicht die Logeinträge der zentralen NOOTS-Komponenten anhand der Trace-ID zu durchsuchen. Optional können weitere Suchmöglichkeiten unterstützt werden.
    - Auf die Logeinträge der SAKs wird kein zentraler Zugriff ermöglicht.

- Es wird ein geeignetes System durch den Betrieb bereitgestellt, das die Health-Endpunkte der zentralen NOOTS-Komponenten regelmäßig abfragt und damit die Erreichbarkeit der NOOTS-Komponenten prüft.
    - Die Ergebnisse der Abfragen gegen die Health-Endpunkte werden gespeichert, sodass insbesondere Support-Mitarbeiter die Erreichbarkeit der NOOTS-Komponenten für vergangene Zeiträume nachvollziehen können.

### 2.5. Umgebungen, Softwareanlieferung, Support, Freigabe

#### 2.5.1 Testumgebungen

- In allen Testumgebungen dürfen ausschließlich Testdaten verwendet werden. Die Verwendung von Echtdaten ist unter keinen Umständen erlaubt.
- Dataport hat Testumgebungen (Systemlandschaft NODEV) in der dSecureCloud ab Januar 2025 bereitgestellt. Diese Testumgebungen können von Dataport, BVA und SEITENBAU zur Testausführung verwendet werden.
    - Die Testumgebungen und deren Verwendungszwecke sind in der Umgebungsübersicht[1] beschrieben.
    - Die Testumgebungen sind hinsichtlich der Deployment-, Sicherheits- und

[1] https://confluence.zcdi.dataport.de/pages/viewpage.action?pageId=148211821

Datenschutzanforderungen nahezu identisch mit der späteren Betriebsumgebung im Rechenzentrum.

- Dataport hat Testumgebungen (Systemlandschaft NOINF) im Twin Data Center (Rechenzentrum) ab spätestens 01. August 2025 bereitgestellt. Diese Testumgebungen können von Dataport, BVA, SEITENBAU und, nach Absprache, anschlusswillige Data Consumer und Data Provider Zugriff zur Testausführung verwendet werden.
    - Die Testumgebungen und deren Verwendungszwecke sind in der Umgebungsübersicht[2] beschrieben.
- SEITENBAU baut interne Testumgebungen für die Softwareentwicklungsprojekte im NOOTS-Kontext auf. Auf diese Umgebungen haben ausschließlich SEITENBAU-Mitarbeiter Zugriff.

#### 2.5.2 Betriebsumgebung (Produktivbetrieb)

- Dataport stellt die Betriebsumgebung (NOOTS MVP PROD) im Twin Data Center ab spätestens 01. August 2025 bereit.

#### 2.5.3 Softwareanlieferung

- Die von SEITENBAU entwickelten Softwarekomponenten werden an Dataport geliefert und durch Dataport gebaut. Die Infrastruktur zur Anlieferung und zum Bauen der Software wird von Dataport bereitgestellt
    - Dataport hat die entsprechenden Vorgaben für die Softwareanlieferung inkl. Der einzuhaltenden Sicherheitsstandards bis zum 31.12.2024 definiert.

#### 2.5.4 Support

- Für die anschlusswilligen bzw. angebundenen Data Consumer und Data Provider wird ein Support bereitgestellt.
    - Dataport übernimmt den First und Second Level Support.
    - Dataport, SEITENBAU und BVA können im Third Level Support involviert werden.

#### 2.5.5 Freigabe für Produktivbetrieb

- Um die Erlaubnis für den Produktivbetrieb des MVP zu erhalten sind i.d.R. bestimmte Freigaben durch BSI, BMI, BVA, Dataport und ggf. weitere erforderlich oder auch die

[2] https://confluence.zcdi.dataport.de/pages/viewpage.action?pageId=148211821

Zustimmung auf Gesamtprogrammleitungsebene oder aus politischen Gremien erforderlich.
    - BVA klärt welche Freigaben bzw. Zustimmungen erforderlich sind und welche Leistungen (z.B. erfolgreich absolvierte Tests, Berichte, etc.) dafür bis zu welchem Zeitpunkt zu erbringen sind.
    - Dataport bindet weitere benötigte Beteiligte (z.B. BSI zur Durchführung von Pentests oder zur Erstellung des IT-Sicherheitskonzepts) frühzeitig ein und hat entsprechende Anforderungen mit Auswirkung auf die Softwareentwicklungsprojekte bis spätestens 31.12.2024 formuliert, sodass diese in der Umsetzung adäquat berücksichtigt werden können.

### 2.6. NOOTS-Teilnehmer

- An dem MVP sollen die Data Consumer und Data Provider der Use Cases NOOTS UP 01_2025 - Bürgerzentriert und NOOTS UP 02_2025 - Wirtschaftszentriert angeschlossen werden.
- An dem MVP können weitere Data Consumer oder Data Provider angeschlossen werden.
- Die NOOTS-Teilnehmer müssen einen NOOTS-Readiness-Check auf der NOREF vornehmen. Die NOOTS-Referenzumgebung (NOREF) steht ab Anfang 2025 zur Verfügung.
- Die Registrierung der NOOTS-Teilnehmer in den jeweiligen Umgebungen erfolgt durch das Projektteam (Dataport (und ggf. SEITENBAU)). Es wird kein Self-Service für die Registrierung unterstützt.
- Die NOOTS-Teilnehmer können sich auf einer produktionsnahen Testumgebung (NOOTS MVP TEST) und auf der produktiven Betriebsumgebung des NOOTS (NOOTS MVP PROD) ab September 2025 anbinden.
- Die NOOTS-Teilnehmer schaffen selbständig die Voraussetzungen für den Anschluss an NOOTS und befähigen ihren Onlinedienst bzw. ihr Register für NOOTS.
    - Bei konkreten Fragestellungen können sie sich an den Support (siehe Kapitel 2.5.4) wenden.

Die nichtfunktionalen Anforderungen, die von den NOOTS-Teilnehmern im MVP erfüllt werden müssen, sind nicht in diesem Dokument enthalten.

Mit den angeschlossenen Data Providern und Data Consumern sollen die folgenden Anwendungsfälle realisiert werden:

- Use-Case 1 (NOOTS UP 01_2025 – Bürgerzentriert)
  Nachweisabruf für den Onlinedienst Anwohnerparkausweis aus dem zentralen Fahrzeugregister und bei Bedarf ggfs. dem Spiegelregister BW für das Melderegister
    - Nachweisabruf initiiert durch Bürger
    - Data Provider für MVP Ausbaustufe 1:
        - Zentrales Fahrzeugregister (ZFR)
            - Zuständige Stelle: Kraftfahrtbundesamt (KBA)
            - Zentrales Register
            - Benötigte Information: Zulassungsbescheinigung Teil 1 (Fahrzeugschein)
    - Data Consumer für MVP Ausbaustufe 1:
        - Kommunen in Baden-Württemberg
    - LeiKa-Leistung: 99108001001000 - Bewohnerparkausweis Erteilung
- Use-Case 2 (NOOTS UP 02_2025)
  Unternehmensgründung → Anmeldung eines erlaubnispflichtigen, reglementierten Gewerbes (OZG-ID 10294)
    - Nachweisabruf initiiert durch Unternehmen
    - Data Provider für MVP Ausbaustufe 1:
        - Registerportal der Länder
            - Zuständige Stelle: Ministerium der Justiz des Landes Nordrhein-Westfahlen
            - Zentrales Register
            - Benötigte Information: Handelsregister Auszug
- Data Consumer für MVP Ausbaustufe 1:
    - Wirtschaft-Service-Portal (WSP.NRW)
        - Zuständige Stelle: MWIKE NRW
- LeiKa-Leistung: 99050012104000 Gewerbe Anmeldung – Gewerbe anmelden (OZG-Leistung 10294 Unternehmensanmeldung und -genehmigung)

Die Verantwortung für die Realisierung der Anwendungsfälle obliegt dabei den Data Consumern und Data Providern. Dataport, SEITENBAU und BVA unterstützen die Anbindung an NOOTS bis hin zum

erfolgreichen Nachweisaustausch durch den angebotenen Support (siehe Kapitel 2.5.4).

# 3. Zeitrahmen

- Das MVP inkl. des Anschlusses der Data Consumer und Data Provider für NOOTS UP 01_2025 - Bürgerzentriert und NOOTS UP 02_2025 – Wirtschaftszentriert und optional weiterer Data Consumer oder Data Provider soll bis Ende November 2025 abgeschlossen sein.
- Die Softwareentwicklung startete ab Anfang Januar 2025.
- Der Anforderungs-Freeze erfolgte zum 15.02.2025.
- Der Feature Freeze für die NOOTS-Komponenten des MVP erfolgt bis spätestens 31.05.2025.
- Die NOOTS-Teilnehmer sollen sich ab 01.09.2025 gegen die produktive Betriebsumgebung (NOOTS MVP PROD) anbinden können.