Neukonzeption und Neuentwicklung OSiP – NEOSiP

Anforderungserhebung und Architekturkonzeption

Executive Summary

Stand: 27.04.2026

Titel	Dokumentenart	Inhalt
Konzept	Klammerdokument	Übergreifende Zusammenfassung des Vorhabens.
01 Executive Summary	Begleitdokument	Zusammenfassung der Problemstellung, Zielsetzung und der vorgeschlagenen Lösung.
02 Anforderungsliste	Begleitdokument	Detaillierte Beschreibung der für die Neuentwicklung aufgenommenen Anforderungen und deren Quellen.
03 Glossar	Begleitdokument	Übersicht über zentrale Begriffe.

1 Ausgangslage und Auftrag

Das aktuelle Produkt Online-Sicherheitsprüfung (OSIP) weist kritische Sicherheitsmängel auf, die eine rechtssichere Durchführung bundesweiter Zuverlässigkeits- und Sicherheitsprüfungen gefährden. Mit der vorliegenden Neukonzeption von OSiP (NEOSiP) schafft die FITKO eine technologisch rechtskonforme Nachfolgelösung. Durch eine strikte Trennung von Transportweg und Fachdatenverarbeitung wird ein maximales Sicherheitsniveau bei gleichzeitig reduzierter Betriebskomplexität erreicht.

2 Vision und strategische Ziele der Neuentwicklung

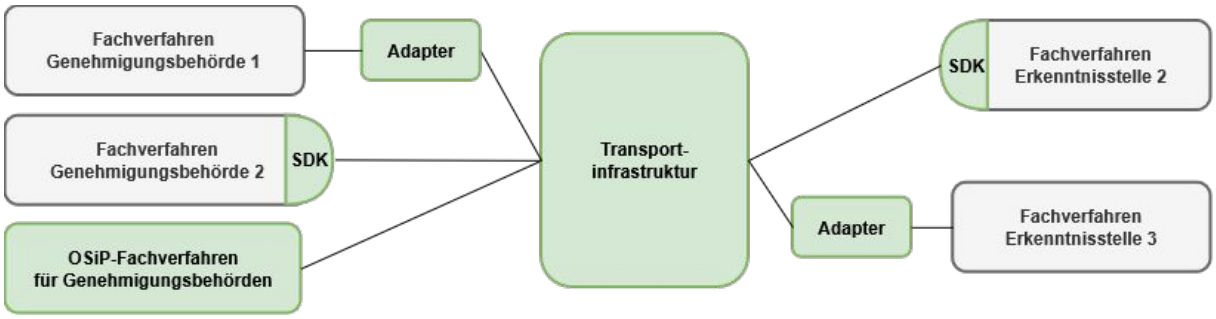
Die Neukonzeption verfolgt die Vision einer zukunftsfähigen, sicheren und skalierbaren Zuverlässigkeits- und Sicherheitsüberprüfung, die bundesweit medienbruchfrei und rechtskonform funktioniert. In Einklang mit dem Beschluss 2025/20 des IT-Planungsrates verfolgt die vorlegende Zielarchitektur insbesondere folgende Ziele:

- Die Transportinfrastruktur wird zukünftig zentral betrieben. Hierdurch werden Betriebs- und Supportaufwände stark reduziert.
- Fachdaten werden erst in den jeweiligen Fachverfahren entschlüsselt. Das System dazwischen ist „blind" und behandelt die Daten damit maximal vertraulich.
- Durch die Ende-zu-Ende-Verschlüsselung zwischen fachlich verantwortlichen Stellen wird der Betrieb der Transportinfrasturkur unter starker Reduktion von Angriffsvektoren ermöglicht.
- Jede Interaktion wird strikt authentifiziert und autorisiert. Das Vertrauen basiert nicht mehr auf impliziten Vertrauensstellungen.
- Die strikte Trennung von Transportfunktionalität und Fachlogik reduziert die Betriebs- und Entwicklungskomplexität massiv.

3 Vorgehen

Im Rahmen des Projekts wurden Anforderungen multi-methodisch über Interviews, Workshops, Dokumentenanalysen und Jira-Auswertungen erhoben. Relevante Stakeholdergruppen, u.a. Genehmigungsbehörden, Erkenntnisstellen, Fachverfahrenshersteller und Mitgliedern des Produktboards, wurden einbezogen, um ein umfassendes Bild fachlicher, technischer und organisatorischer Bedarfe zu erhalten. Es wurden 34 Interviews und 7 Workshops durchgeführt. Zusammen mit einer ausführlichen Bestandsanalyse wurde mit dieser Anforderungserhebung die Grundlage für die Zielarchitektur geschaffen.

4 Zielarchitektur



Die Abbildung zeigt die Komponenten, die von NEOSiP bereit gestellt werden, in grün.

4.1 Transportinfrastruktur für den Nachrichtenaustausch

In der Zielarchitektur ist eine zentral betriebene Transportinfrastruktur die zentrale, vermittelnde Komponente für den regelbasierten Nachrichtenaustausch zwischen allen beteiligten Systemen. Diese übermittelt die Nachrichten zwischen den beteiligten Akteuren asynchron und vollständig Ende-zu-Ende-verschlüsselt.

Die Transportinfrastruktur übernimmt Routing, Zustellung, fachliche Quittierung, Überwachung und Verfahrensstatusübermittlung. Eine Einsicht in die fachlichen Daten ist in dieser Komponente nicht möglich, wodurch die Vertraulichkeit und Integrität der Inhaltsdaten gegenüber der Bestandslösung deutlich zunimmt.

Es wird im weiteren Projektverlauf evaluiert, inwieweit das bestehende IT-PLR-Produkt FIT-Connect als Transportinfrastruktur den von NEOSiP gestellten Anforderungen entspricht, inwieweit das Produkt weiterentwickelt werden muss und somit nachgenutzt werden kann. Die entsprechenden Konsultationsgespräche zwischen den Teams von OSiP und FIT-Connect haben bereits gestartet.

4.2 Fachverfahren für Genehmigungsbehörden

Die Genehmigungsbehörden sollen auch weiterhin ein Referenz-Fachverfahren für Zuverlässigkeits- und Sicherheitsprüfungen auf Basis des bewährten „BO-Clients“ erhalten. Die Zielarchitektur spezifiziert ein solches Referenz-Fachverfahren für einen zentralen Betrieb mit strikter Mandantentrennung. In den nachfolgenden Projektphasen muss noch abschließend geklärt werden, ob die FITKO auch zukünftig die Entwicklung dieses Referenz-Fachverfahrens betreuen soll oder ob damit andere Institutionen mit größerer Nähe zur Fachlichkeit beauftragt werden sollten.

4.3 Geringerer Pflegeaufwand durch modernes Systemdesign

Die Zielarchitektur reduziert die Komplexität des Betriebs erheblich, da durch die verbesserte Sicherheitsarchitektur ein zentraler Betrieb möglich wird. Dieser wird Störungsanalyse, Monitoring und Release-Management absehbar deutlich vereinfachen.

Auch die Wartbarkeit und Erweiterbarkeit des Systems wird durch die vollständige Trennung von Transport- und Fachlogik gesteigert. Denn da die Transportinfrastruktur gegenüber dem Bestandssystem nur essentielle Aufgaben übernimmt, wird diese Systemkomponente in ihrer Komplexität reduziert.

4.4 Homogenisierung der Anschlussbedingungen, Prozesse und Datenformate

Die Zielarchitektur sieht einheitliche Anschlussbedingungen für alle teilnehmenden Kommunikationsparteien vor. Dies ermöglicht eine zentrale Durchsetzung von Sicherheits-, Routing- und Kommunikationsprinzipien, wodurch eine Verbesserung der Nachvollziehbarkeit, der Prüf- und Revisionsfähigkeit sowie eine deutliche Reduktion der Integrationheterogenität erwirkt wird.

Das Konzept diskutiert eine Vereinheitlichung der ZSÜ-Prozesse. Auf diesem Weg soll ein einheitliches Verständnis des ZSÜ-Prozesses geschaffen werden, der derzeit noch fragmentiert, je nach Anwendungsbereich individuell, gehandhabt wird.

Es wird ebenfalls vorgeschlagen, im einen ZSÜ-Datenstandard zu schaffen, der über die gesamte Strecke von Genehmigungsbehörden zu Erkenntnisstellen und zurück Datentransformationen obsolet macht und ein gemeinsames und einheitliches Verständnis schafft.

5 Migration des Bestandssystems

Da die Transportinfrastruktur in der Zielarchitektur keine Einsicht mehr in Inhaltsdaten haben soll und damit umfänglich die Vertraulichkeit der Daten nachhaltig schützt, müssen diverse Aufgaben zukünftig von den Fachverfahren durchgeführt werden:

- Es soll perspektivisch ein einheitliches, gemeinsames **Datenformat** für ZSÜ-Prozesse etabliert werden. Bis dieses Zielbild erreicht ist, müssen die bestehenden Datenformate weiterhin konvertiert werden. Dies muss in den Fachverfahren oder, übergangsweise, in Adaptern durchgeführt werden.
- **Schema-Validierung** und **Routing-Logik** (z.B. wohnortbasierte Anfragenlogik) müssen künftig durch die Fachverfahren übernommen werden, da diese an zentraler Stelle aufgrund der Einsicht in die Inhaltsdaten nicht mehr durchführbar sein werden.In der Zielarchitektur wird die **Authentifizierung und Autorisierung** grundlegend

überarbeitet. Fachverfahren müssen sich zukünftig direkt gegenüber einander authentifizieren können. Die Berechtigungsprüfung wird ebenfalls fachverantwortlich und authentifiziert umgesetzt.

Damit die Migrationsaufwände für die Fachverfahren minimiert werden, ist es Teil des Zielbildes, dass durch das Produkt zukünftig Software Development Kits (SDKs) bereitgestellt werden. Diese SDKs übernehmen einen großen Teil der Prozesslogik, die im Bestandssystem noch im Kern abgebildet ist. SDKs werden als integraler Bestandteil des Produkts dauerhaft bereitgestellt.

Ein **SDK** (**S**oftware **D**evelopment **K**it) ist eine Sammlung von Programmierwerkzeugen und Bibliotheken, die Entwicklern hilft, Software für eine bestimmte Plattform zu erstellen.

Für bestehende Fachverfahren, bei denen eine Migration nicht zeitgerecht möglich ist, könnten Adapter bereitgestellt werden. Diese Adapter sind Systeme, mit denen sich Fachverfahren verbinden könnten und die sich ähnlich zum Bestandssystem verhalten würden. Die Adapter gewährleisten zwar einen reibungslosen Betrieb, dürfen aber aufgrund der damit einhergehenden erhöhten Aufwände und Angriffsfläche unbedingt nur als Übergangslösung und unter festen organisatorischen Rahmenbedingungen betrieben werden. Es muss sichergestellt werden, dass diese keine Dauerlösung darstellen.

Adapter fungieren als technische Vermittler zwischen unterschiedlichen Systemen, die nativ nicht miteinander kommunizieren können. Adapter sind explizit als temporäre Brückenlösung konzipiert.