Neukonzeption OSiP – Begleitdokument 02

Architekturentscheidungen

[Unteruntertitel]

Version: 1.00

Stand: 27.04.2026

Version	Datum	Autor:in	Aktion
1.0	27.04.2026	Dr. George-Petru Ciordas-Hertel	Überführung Arbeitsdokument in FITKO-Vorlage

Inhaltsverzeichnis

1 ADR-000 Dokumentation von Architekturentscheidungen

Sprache: Deutsch

Status: Vorgeschlagen

Datum: 18.11.2025

Entscheidende: Architektur-Workstream

Beratende: Keine

Informierte: Keine

1.1 Kontext und Problemstellung

Die getroffenen Architekturentscheidungen müssen formell festgehalten werden, insbesondere wenn diese die Architektur im engeren Sinne oder andere grundlegende Aspekte betreffen.

Dieser ADR regelt, welchem Format und welcher inhaltlichen Struktur diese Aufzeichnungen folgen sollen.

1.2 Entscheidungsfaktoren

- Implizite Annahmen in Entscheidungsprozessen sollten durch transparente Dokumentation von Entscheidungstreibern explizit gemacht werden.
- Die Dokumentation von Design- und Entscheidungsprozessen sowie zentralen Argumenten ist wichtig, damit ein ausreichend qualifizierter Beobachter die Entscheidungen zu einem späteren Zeitpunkt nachvollziehen kann.
- Die transparente Dokumentation von insbesondere verworfenen Handlungsoptionen schafft Vertrauen und Legitimität, insbesondere bei betroffenen Parteien.

1.3 Betrachtete Optionen

- Option 1: MADR 4.0.0 - The Markdown Architectural Decision Records (deutsche Vorlage)
- Option 2: Michael Nygards ADR-Vorlage - Die erste Inkarnation des Begriffs "ADR"
- Option 3: Sustainable Architectural Decisions - The Y-Statements
- Option 4: Eine andere der [hier](https://github.com/joelparkerhenderson/architecture_decision_record) aufgelisteten ADR-Vorlagen
- Option 5: Formlos - Keine Konventionen für Dateiformat und Struktur

1.4 Entscheidung

Gewählte Option: Option 1: MADR 4.0.0 - The Markdown Architectural Decision Records (deutsch Vorlage)

1.4.1 Konsequenzen

Gut, weil

- MADR ermöglicht die strukturierte Erfassung verschiedenartiger Entscheidungen
- Das MADR-Format ist schlank und passt zu unserem Arbeitsstil
- Die MADR-Struktur ist nachvollziehbar und erleichtert die langfristige Nutzung und Pflege
- Das MADR-Projekt ist aktiv MADR ein verbreitetes Dokumentationsformat für ADRs

1.4.2 Prüfung

- Der Aufbau jeder ADR wird gemäß der deutschen Vorlage aus der Option 1 begutachtet

1.5 Weitere Informationen

- Deutsche Vorlage für MADR 4.0
  - https://github.com/adr/madr/blob/develop/template/i18n/de/adr-template.md

2 ADR-001 Topologie der backendseitigen Kommunikationsinfrastruktur

Sprache: Deutsch

Status: Vorgeschlagen

Datum: 2025-12-02

Entscheidende: Architektur-Workstream

Beratende: ITS/DS Workstream, Fachvertreter:innen EKS und Genehmigungsbehörden, FIT-AB, FITKO-AM, Lenkungsausschuss

Informierte: IT-PLR

2.1 Kontext und Problemstellung

Die Topologie der backendseitigen Kommunikationsinfrastruktur stellt eine grundlegende Architekturentscheidung dar, da sie bestimmt, wie die Kommunikation zwischen den betrachteten Backend-Systemen strukturell organisiert ist und in welchem Maß zentrale oder dezentrale Kommunikationsmechanismen zum Einsatz kommen.

Die Zielarchitektur von OSiP stellt ein föderales System-of-Systems dar, in dem eine große Anzahl von organisatorisch autonomer Fachverfahren verschiedener Behörden miteinander kommunizieren müssen. Im Kontext dieses ADR werden die angebundenen Fachverfahren als kommunizierende Backend-Systeme betrachtet. Die beteiligten Organisationen betreiben ihre Backend-Systeme eigenständig und unterliegen unterschiedlichen technischen, organisatorischen und rechtlichen Rahmenbedingungen.

Betrachtet werden unterschiedliche Ausprägungen der Kopplung zwischen den Backend-Systemen, die von direkter Punkt-zu-Punkt-Kommunikation bis hin zu einer vollständig oder teilweise zentralisierten Kommunikationsinfrastruktur reichen. Im Kontext dieses ADR bezeichnet Kommunikationsinfrastruktur die strukturelle Organisation der Kommunikation zwischen Backend-Systemen. Die konkrete technische Realisierung dieser Kommunikationsinfrastruktur erfolgt in OSiP durch die sogenannte Transportinfrastruktur. Die Wahl der Topologie hat dabei wesentlichen Einfluss auf Skalierbarkeit, Komplexität, Betriebsstrukturen sowie auf die Möglichkeit, föderale Anforderungen und unterschiedliche organisatorische Rahmenbedingungen abzubilden.

Die Kommunikationsinfrastruktur verbindet die folgenden Backend-Systeme: Fachverfahren von Antragserfassungsstellen (AES), Genehmigungsbehörden (GB) und Erkenntnisstellen (EKS) sowie perspektivisch Register.

Die Kommunikationsinfrastruktur ist ausschließlich für den Transport und die adressierungsbasierte Weiterleitung von Nachrichten verantwortlich und übernimmt keine fachliche Verarbeitung der übermittelten Inhalte.

Dieses ADR trifft keine Aussagen zur konkreten technischen Umsetzung der eingesetzten Kommunikationskomponenten. Ebenso sind weitere Infrastrukturkomponenten innerhalb der Zielarchitektur, die nicht Teil der reinen Kommunikationsinfrastruktur sind, nicht Gegenstand dieser Entscheidung.

2.2 Entscheidungsfaktoren

Funktionale Anforderungen

- FA_1077: Das System ermöglicht es, Online-Sicherheitsüberprüfungen AWBs-/Bundeslands-übergreifend zu übertragen und anzuerkennen. Nachberichte werden an die neue Fachbehörde gesendet. Falls nicht mit ursprünglicher Anfrage geschehen, werden relevante EKS des neuen Bundeslandes/AWBs automatisch zusätzlich angefragt.
- FA_1108: Das System ermöglicht Erkenntnisanfragen an alle für die Genehmigungsbehörde relevanten und gesetzlich vorgegebenen Stelle.
- FA_791: Das System ermöglicht die Anbindung von sekundären EKS zur direkten Kommunikation (z.B. Aktenanforderungen) über OSiP.
- FA_440: Das System ermöglicht die Weiterleitung von Anhörungsergebnissen an EKS.
- FA_116.1: Das System ermöglicht das Teilen von bereits abgerufenen Akten und Informationen der EKS durch eine GB mit anderen GBs.
- ÜFA_60: Das System erstellt automatisch Statistik- und ESTA-Meldungen und übermittelt Ergebnisse der Online-Sicherheitsüberprüfung an externe Register.
- FA_150: Das System ermöglicht die Rückmeldung des Ergebnisses der Online-Sicherheitsprüfung an das Bewacherregister.
- FA_573.1: Das System ermöglicht die Rückmeldung des Ergebnisses der Online-Sicherheitsprüfung an das Bundeszentralregister.
- FA_785: Das System ermöglicht die Rückmeldung des Ergebnisses der Online-Sicherheitsprüfung an das IMI (Binnenmarktinformationssystem).

Nicht-funktionale Anforderungen

- ASD_6: Die Transportinfrastruktur kann unabhängig vom OSiP-Fachverfahren genutzt werden, um Daten mit Erkenntnisstellen und Registern auszutauschen.

- ASD_6.1: Die Transportinfrastruktur ist fachlich, technisch und betrieblich vollständig unabhängig vom OSiP-Fachverfahren zu konzipieren und zu betreiben.
- ASD_10: Das System ermöglicht eine klare Abgrenzung der Systemgrenzen und eine saubere Entkopplung zwischen der Transportinfrastruktur und den angebundenen Fachverfahren.
- ASD_28: Im Rahmen der Neuentwicklung wird das Ziel einer weitreichenden Anbindung von Genehmigungsbehörden verfolgt.
- ASD_50: Das System übermittelt Daten ohne zentrales Mapping (Pass-Through). Notwendige Transformationen liegen in der Verantwortung der angebundenen Systeme.
- ASD_79: Die OSiP-Transportinfrastruktur soll als zentrale Basiskomponente bereitgestellt werden, mit verpflichtender Nutzung durch die Behörden.
- ASD_80: Der zentralisierte Betrieb eines OSiP-Fachverfahrens wird angestrebt, dennoch soll ein dezentraler Betrieb für einzelne Länder möglich sein.
- ASD_90: Das System unterstützt eine wachsende Zahl an Mandanten performant und wartbar. Neue Mandanten können ohne grundlegende Systemänderungen ergänzt werden.
- ASD_411: Die Routing-Regeln müssen basierend auf der Kombination von BL und AWB definierbar sein.
- ASD_413: Das System stellt sicher, dass das definierte Routing-Regeln nicht von angebundenen Fachverfahren oder anderen externen Systemen umgangen oder manipuliert werden kann.
- ASD_414: Die Transportinfrastruktur erzwingt die Adressierung basierend auf den zentral hinterlegten Regeln und akzeptiert keine abweichenden Adressaten, die von einem Fachverfahren übermittelt werden.

2.3 Betrachtete Optionen

- Option 1: Punkt-zu-Punkt-Kommunikation
- Option 2: Zentrale Kommunikationsinfrastruktur
- Option 3: Föderierte Kommunikationsinfrastruktur

2.4 Entscheidung

Gewählte Option: „Option 2: Zentrale Kommunikationsinfrastruktur"

Ausschlaggebend für diese Entscheidung war, dass eine zentrale Kommunikationsinfrastruktur den Integrations-, Betriebs- und Koordinationsaufwand bei der gegebenen großen und heterogenen Anzahl von Backend-Systemen gering hält. Bei einer direkten Punkt-zu-Punkt-

Kommunikation wächst die Anzahl notwendiger Integrationen zwischen Systemen mit zunehmender Systemanzahl stark an (n*(n-1) Kommunikationsbeziehungen). Dies führt zu einer schwer beherrschbaren Integrations- und Betriebslandschaft. Zudem müssen die Backend-Systeme nur eine zentrale Komponente erreichen können und untereinander keine direkten Beziehungen etablieren.

Darüber hinaus ermöglicht eine zentrale Kommunikationsinfrastruktur die konsistente Durchsetzung zentral definierter Adressierungs- und Routingregeln. Diese Regeln können innerhalb der Infrastruktur technisch erzwungen werden und sind damit unabhängig von der Implementierung einzelner Backend-Systeme.

Die Alternativen der Punkt-zu-Punkt-Kommunikation sowie eines föderierten Betriebs wurden verworfen, da sie entweder zu einer stark steigenden Anzahl direkter Integrationen oder zu einer erheblichen zusätzlichen architektonischen und organisatorischen Komplexität führen. Der Entwicklungs- und Betriebsaufwand der zentralen Komponente wird bewusst in Kauf genommen, da er im Gesamtsystem als beherrschbar und geringer eingeschätzt wird als die verteilten Aufwände der Punkt-zu-Punkt-Topologie. Die Souveränität der Backend-Systeme in der direkten Kommunikation dieser wird bewusst zugunsten der Reduktion der Gesamtsystemkomplexität aufgegeben.

2.4.1 Konsequenzen

Gut, weil

- Backend-Systeme von der direkten Integration mit anderen Backend-Systemen entlastet werden.
- Änderungen an Protokollen, Sicherheitsmechanismen oder Schnittstellen zentral umgesetzt und ausgerollt werden können.
- zentrale Authentifizierungs-, Adressierungs- und Routingmechanismen innerhalb der zentralen Komponente konsistent umgesetzt und kontrolliert werden können.

Neutral, weil

- die zentrale Komponente zu einer kritischen Kernkomponente der Gesamtarchitektur wird und entsprechend hochverfügbar, skalierbar und sicher ausgelegt werden muss.
- die Kommunikationsinfrastruktur eine zentrale Betriebs- und Governance-Struktur erfordert, einschließlich definierter Prozesse für Onboarding, Release-Management, Incident-Handling und Monitoring

Schlecht, weil

- die Entwicklung, Betrieb und Weiterentwicklung der Kommunikationsinfrastruktur erhöhten initialen und laufenden Aufwand verursachen, der zentral getragen werden muss.
- der zentrale Betrieb klare Governance-Regelungen, insbesondere für Betrieb, Weiterentwicklung, Release-Management und Incident-Handling erfordert.
- Fehlkonfigurationen oder Sicherheitsprobleme innerhalb der zentralen Komponente potenziell Auswirkungen auf alle angebundenen Systeme haben können.

Föderale oder datenschutzrechtliche Vorbehalte einzelner Genehmigungsbehörden gegenüber einem zentralen Betrieb werden im Rahmen von ADR-004 Ende-zu-Ende-Verschlüsselungsschicht adressiert.

2.5 Vor- und Nachteile der Optionen

2.5.1 Option 1: Punkt-zu-Punkt-Kommunikation

Bei dieser Option erfolgt die Kommunikation direkt zwischen den beteiligten Backend-Systemen. AES, GB und EKS kommunizieren unmittelbar miteinander, ohne dass ein zentraler Akteur als vermittelnde Instanz genutzt wird. Jede Kommunikationsbeziehung wird dabei als eigenständige Integration umgesetzt, einschließlich der technischen Anbindung, der Konfiguration der Schnittstellen sowie der notwendigen Sicherheits- und Vertrauensbeziehungen.

Die Aufnahme weiterer Backend-Systeme führt dazu, dass neue direkte Anbindungen zu den jeweils relevanten Gegenstellen in beide Richtungen aufgebaut werden müssen.

Gut, weil

- die Kommunikationsbeziehungen direkt zwischen den beteiligten Systemen erfolgen und dadurch klar nachvollziehbar sind.
- keine zentrale Infrastrukturkomponente existiert, deren Ausfall alle Kommunikationsbeziehungen gleichzeitig beeinträchtigen würde.
- Genehmigungsbehörden eine hohe Autonomie bei der Ausgestaltung ihrer jeweiligen Kommunikationsbeziehungen behalten.

Neutral, weil

- Sicherheitsmechanismen, Protokolle und Schnittstellen zwischen den beteiligten Parteien abgestimmt werden müssen, diese aber grundsätzlich standardisiert vorgegeben werden könnten.

Schlecht, weil

- mit zunehmender Anzahl angebundener Genehmigungsbehörden und EKS die Anzahl der notwendigen Integrationen stark ansteigt, da jede Kommunikationsbeziehung separat umgesetzt werden muss.
- sich Betriebs-, Wartungs- und Pflegeaufwände für Schnittstellen, Zertifikate und Vertrauensbeziehungen auf viele beteiligte Systeme und Organisationen verteilen.
- eine konsistente und einheitliche Umsetzung über alle Beteiligten hinweg bei heterogenen technischen und organisatorischen Rahmenbedingungen nur schwer sicherzustellen ist.
- die Anbindung neuer Mandanten oder zusätzlicher Kommunikationspartner wiederkehrende Anpassungen an mehreren bestehenden Systemen erfordert, da kein zentraler Anbindungspunkt existiert.
- alle Backend-Systeme angepasst werden müssen, wenn ein neues Backend-System der Kommunikationsinfrastruktur hinzugefügt wird.
- eine zentrale Durchsetzung der Routing-Regeln gemäß ASD_411 und ASD_414 nicht sichergestellt werden kann.

2.5.2 Option 2: Zentrale Kommunikationsinfrastruktur

Der Nachrichtenaustausch zwischen den beteiligten Backend-Systemen erfolgt über eine zentrale Kommunikationsinfrastruktur, die von einem Akteur für alle zur Verfügung gestellt wird. Die Backend-Systeme kommunizieren nicht direkt miteinander, sondern nutzen die zentrale Komponente für den Austausch von Nachrichten. Die Anbindung der Backend-Systeme erfolgt jeweils an die zentrale Komponente.

Gut, weil

- die Fachverfahren jeweils nur an eine zentrale Komponente angebunden werden müssen.
- die zentrale Kommunikationsinfrastruktur eine einheitliche Umsetzung von Protokollen, Schnittstellen und Sicherheitsmechanismen ermöglicht.
- Integrations- und Änderungsaufwände an einer zentralen Stelle gebündelt werden können und nicht auf alle beteiligten Fachverfahren verteilt sind.
- neue Fachverfahren oder Mandanten über eine bestehende Infrastruktur angebunden werden können, ohne andere Fachverfahren anpassen zu müssen.
- innerhalb der Kommunikationsinfrastruktur die Einhaltung der Routing-Regeln sichergestellt werden kann.

Neutral, weil

- die zentrale Komponente selbst hochverfügbar, skalierbar und betrieblich robust ausgelegt werden muss, um die Anforderungen aller angebundenen Fachverfahren zu erfüllen.
- die Fachverfahren in ihrer Kommunikation von der zentralen Infrastruktur abhängig sind, ohne dass dies per se eine funktionale Einschränkung darstellt.

Schlecht, weil

- die zentrale Komponente ein kritischer Bestandteil der Gesamtarchitektur ist, dessen Ausfall oder Fehlfunktion potenziell alle Kommunikationsbeziehungen betrifft.
- die Bündelung der Kommunikationsbeziehungen an einer zentralen Stelle zu hohen Anforderungen an Betrieb, Monitoring und Governance führt.
- föderale oder datenschutzrechtliche Vorbehalte einzelner Genehmigungsbehörden gegen eine zentrale Infrastruktur berücksichtigt werden müssen und zu Akzeptanzproblemen führen können.
- die Entwicklung der zentralen Komponente selbst einen initialen Aufwand verursacht, da sie generisch, skalierbar, sicher und mandantenfähig ausgelegt werden muss.
- der Betrieb der zentralen Komponente dauerhaft erhöhte Aufwände mit sich bringt, insbesondere für Hochverfügbarkeit, Monitoring, Incident Management, Wartung und Weiterentwicklung.
- fachliche und technische Änderungen an der Kommunikationsinfrastruktur sorgfältig koordiniert werden müssen, da sie potenziell Auswirkungen auf alle angebundenen Fachverfahren haben.

2.5.3 Option 3: Föderierte Kommunikationsinfrastruktur

Grundsätzlich kann die Kommunikation zwischen den beteiligten Backend-Systemen über eine zentral zur Verfügung gestellte Komponente der Kommunikationsinfrastruktur erfolgen, welche von einem Akteur bereitgestellt wird. Weitere Akteure können jedoch eigene Komponenten der Kommunikationsinfrastruktur in eigener Verantwortung betreiben und in das Gesamtsystem einbinden. In diesem Fall erfolgt die Kommunikation zwischen den Backend-Systemen der jeweiligen Akteure über die von diesen angebundenen Komponenten. Dadurch können im Gesamtsystem mehrere autonome Komponenten existieren, welche ein Kommunikationsnetzwerk aufbauen. Backend-Systeme können sich in diesem Szenario an eine der unterschiedlichen im Gesamtsystem genutzte Komponenten anbinden. Wobei es ihnen obliegt dies zu organisieren und sicherzustellen.

Gut, weil

- Genehmigungsbehörden mit hohen Anforderungen an Datenschutz oder digitale Souveränität die Möglichkeit haben, eine eigene Komponente in eigener Verantwortung zu betreiben.
- die Backend-Systeme nur an wenige zentrale Komponenten angebunden werden müssen.
- die Kommunikationsinfrastruktur eine einheitliche Umsetzung von Protokollen, Schnittstellen und Sicherheitsmechanismen ermöglicht.
- Integrations- und Änderungsaufwände gebündelt werden können und nicht auf alle beteiligten Fachverfahren verteilt sind.
- neue Fachverfahren oder Mandanten über eine bestehende Infrastruktur angebunden werden können, ohne andere Fachverfahren anpassen zu müssen.

Neutral, weil

- die Kommunikationsinfrastruktur verteilt hochverfügbar, skalierbar und betrieblich robust ausgelegt werden muss, um die Anforderungen aller angebundenen Backend-Systeme zu erfüllen.
- die Backend-Systeme in ihrer Kommunikation von der Kommunikationsinfrastruktur abhängig sind, ohne dass dies per se eine funktionale Einschränkung darstellt.

Schlecht, weil

- im Gesamtsystem mehrere parallel betriebene Komponenten existieren können, was die architektonische Komplexität deutlich erhöht. Somit muss auch eine Kommunikation zwischen Komponenten vorgesehen werden.
- die Backend-Systeme indirekt an alle im Gesamtsystem genutzten Komponenten angebunden werden müssen, um eine vollständige Kommunikation sicherzustellen.
- eine einheitliche Governance, ein konsistentes Sicherheitsniveau und ein gemeinsames Betriebsmodell über mehrere Komponenten hinweg nur mit erheblichem Abstimmungsaufwand durchsetzbar sind.
- organisatorisch sichergestellt werden muss, dass eigenverantwortlich betriebene Komponenten dauerhaft kompatibel sind, sicherheitsrelevante Updates zeitnah umsetzen und auf einem abgestimmten Versionsstand betrieben werden.

3 ADR-002 Kommunikationskonzept

Sprache: Deutsch

Status: Vorgeschlagen

Datum: 2026-03-11

Entscheidende: Architektur-Workstream

Beratende: Fachvertretungen EKS und Genehmigungsbehörden, FIT-AB, FITKO-AM

Informierte: Lenkungsausschuss, IT-PLR

3.1 Kontext und Problemstellung

Die Architektur umfasst mehrere miteinander interagierende Fachverfahren. Darunter Fachverfahren der Antragserfassungsstellen, der Genehmigungsbehörden und der Erkenntnisstellen. In ADR-001 wurde entschieden, dass diese Systeme über eine zentrale Transportinfrastruktur miteinander kommunizieren sollen. Die Transportinfrastruktur fungiert dabei als zentraler Vermittlungs- und Transportmechanismus für den Nachrichtenaustausch zwischen den Fachverfahren.

Für die weitere Ausgestaltung der Architektur ist nun festzulegen, wie die angebundenen Fachverfahren mit dieser zentralen Transportinfrastruktur interagieren. Hierfür kommen unterschiedliche Kommunikationsmuster in Betracht, die sich insbesondere hinsichtlich Latenz, Robustheit, Netzverträglichkeit, Skalierbarkeit, Zustellsemantik sowie Integrationsaufwand unterscheiden. Darüber hinaus unterscheiden sie sich hinsichtlich der zeitlichen Kopplung zwischen sendendem und empfangendem Fachverfahren.

Die Wahl eines einheitlichen Kommunikationskonzepts ist notwendig, um Schnittstellenverträge, Routinglogik, Sicherheitsmechanismen, Zustellgarantien und Betriebsprozesse konsistent und langfristig stabil definieren zu können. Ohne eine solche Entscheidung besteht das Risiko einer heterogenen Kommunikationslandschaft, die sowohl die Wartbarkeit als auch die Einhaltung der Sicherheits- und Netzanforderungen erheblich erschwert. Darüber hinaus beeinflusst das Kommunikationskonzept maßgeblich die Robustheit des Gesamtsystems, insbesondere im Umgang mit temporär nicht verfügbaren Fachverfahren, Netzrestriktionen zwischen Verwaltungsnetzen sowie Lastspitzen im Nachrichtenaufkommen. Zusätzlich ist zu berücksichtigen, dass die angebundenen Fachverfahren sich teilweise in unterschiedlich abgesicherten Netzen befinden können und daher nicht jedes System von jedem anderen System direkt erreichbar ist.

3.2 Entscheidungsfaktoren

- ASD_6.1: Die Transportinfrastruktur ist fachlich, technisch und betrieblich vollständig unabhängig vom OSiP-Fachverfahren zu konzipieren und zu betreiben.
- ASD_10: Das System ermöglicht eine klare Abgrenzung der Systemgrenzen und eine saubere Entkopplung zwischen der Transportinfrastruktur und den angebundenen Fachverfahren.
- ASD_25: Standardisierte Schnittstellen sind bereitzustellen, um Fachverfahren und EKS interoperabel anzubinden.
- ASD_17: Es werden aktuelle Standards und Protokolle eingehalten.
- ASD_18: Das System verwendet offene, dokumentierte Schnittstellen und bewusst offene Datenformate für Austausch und Export.
- ASD_50: Das System übermittelt Daten ohne zentrales Mapping (Pass-Through). Notwendige Transformationen liegen in der Verantwortung der angebundenen Systeme.
- ASD_56: Die Transportinfrastruktur ermöglicht die Benachrichtigung über Events/Webhooks.
- ASD_57: Das System ist skalierbar, um dynamisch auf Lastspitzen reagieren zu können.
- ASD_72: Das System ermöglicht Echtzeitüberprüfungen für die Online-Sicherheitsüberprüfungen.

Zusätzliche architektonische Anforderungen

- Vereinbarkeit mit Kommunikationsbeziehungen über unterschiedlich abgesicherte Netze
- Sicherer und stabiler Versand von Nachrichten auch bei temporärer Nichtverfügbarkeit einzelner Fachverfahren
- Unterstützung eines föderalen Betriebsmodells mit organisatorisch autonomen Fachverfahren
- Minimierung der Integrationskomplexität für angebundene Fachverfahren

3.3 Betrachtete Optionen

- Option 1: Synchrone Vermittlungsschicht
- Option 2: Asynchrone Vermittlungsschicht
- Option 3: Asynchrone Vermittlungsschicht mit ereignisbasierter Kommunikation

3.4 Entscheidung

Gewählte Option: Option 2: Zentrale asynchrone Vermittlungsschicht, denn diese Kommunikationsform bildet die fachlichen und technischen Randbedingungen am konsistentesten ab.

Die asynchrone Kommunikation entkoppelt sendende und empfangende Fachverfahren zeitlich und verhindert, dass Verfügbarkeits- oder Latenzprobleme einzelner Systeme unmittelbar auf andere durchschlagen. Die Transportinfrastruktur übernimmt dabei die Rolle eines Systems, das Nachrichten entgegennimmt, persistiert und für empfangende Fachverfahren zur Abholung bereitstellt. Sie ist mit den bestehenden Netzrestriktionen vereinbar, da Verbindungen ausschließlich vom empfangenden Fachverfahren initiiert werden müssen. Lastspitzen werden durch die Zwischenspeicherung abgefedert, wodurch die Skalierbarkeit des Gesamtsystems erhöht wird.

Die Anforderung nach Echtzeitüberprüfungen wird bei dieser Option nicht ausgeschlossen, da auch asynchrone Kommunikationsmodelle bei geeigneter Systemauslegung sehr geringe Latenzen ermöglichen.

Die synchrone Kommunikation wurde verworfen, da sie eine durchgängige synchrone Erreichbarkeit aller Fachverfahren voraussetzt und mit den Netz- und betrieblichen Rahmenbedingungen nur eingeschränkt vereinbar ist. Die ereignisbasierte Kommunikation wurde nicht gewählt, da sie für die antrags- und zustandsorientierten Kernprozesse einen deutlich höheren Integrations- und Governance-Aufwand erfordert. Zudem stellt ereignisbasierte Kommunikation eine Spezialisierung asynchroner Kommunikation dar, die primär für lose gekoppelte Ereignisverarbeitung geeignet ist, während die betrachteten Prozesse überwiegend explizite Nachrichtenbeziehungen zwischen konkreten Kommunikationspartnern aufweisen.

3.4.1 Konsequenzen

Gut, weil

- die zeitliche Entkopplung der Kommunikation die Robustheit des Gesamtsystems erhöht und temporäre Ausfälle einzelner Fachverfahren nicht unmittelbar auf andere Systeme durchschlagen.
- die Kommunikation netzkonform umgesetzt werden kann und keine aktiven Verbindungen aus weniger vertrauenswürdigen Netzen in stärker geschützte Netze erforderlich sind.
- Lastspitzen durch Zwischenspeicherung abgefedert werden können.

- zentrale Mechanismen für Routing, Protokollierung, Monitoring und Tracing etabliert werden können.
- Wiederholungsmechanismen und Zustellsemantiken zentral umgesetzt werden können.

Neutral, weil

- fachliche Prozesse nicht mehr als unmittelbare Request-Response-Interaktionen modelliert werden können, sondern explizit mit asynchronen Zuständen umgehen müssen.

Schlecht, weil

- Fachverfahren keine unmittelbare Antwort erhalten und Status- sowie Korrelation von Nachrichten explizit modelliert werden müssen.
- die Transportinfrastruktur eine temporäre Persistierung von Nachrichten erfordert und somit zusätzliche Anforderungen an Betrieb und Datenhaltung entstehen.
- ein zentrales Konzept zur eindeutigen Korrelation fachlich zusammengehöriger Nachrichten erarbeitet werden.
- festgelegt werden muss , welche Zustellsemantiken unterstützt werden und wie mit Wiederholungen, Duplikaten und Fehlerfällen umzugehen ist.

3.5 Vor- und Nachteile der Optionen

3.5.1 Option 1 – Synchrone Vermittlungsschicht

Bei der synchronen Kommunikation interagieren die Fachverfahren im klassischen Request-Response-Modell mit der zentralen Transportinfrastruktur.
Ein Fachverfahren sendet eine Anfrage an die Transportinfrastruktur und wartet aktiv auf eine unmittelbare Antwort, die im selben technischen Aufruf zurückgeliefert wird. Kann die Transportinfrastruktur das Zielsystem nicht erreichen, wird dem sendenden System dies mitgeteilt. Es muss später erneut ein Übermittlungsversuch erfolgen. Die Transportinfrastruktur fungiert dabei als synchroner Vermittler zwischen aufrufendem und adressiertem System.
Gut, weil

- die Kommunikationssemantik einfach, etabliert und für Fachlichkeit wie Entwicklung leicht nachvollziehbar ist.
- aufrufende Fachverfahren unmittelbar eine fachliche oder technische Rückmeldung erhalten.
- fachliche Echtzeiterwartungen direkt technisch abgebildet werden können.

Schlecht, weil

- Verfügbarkeit und Antwortzeiten der Zielsysteme direkt auf das aufrufende Fachverfahren durchschlagen.
- diese Kommunikationsform nur eingeschränkt mit unterschiedlich abgesicherten Netzen vereinbar ist. An relevanten Netzübergängen wie müssen Lösungen eingerichtet werden, um den Übergang zu ermöglichen.
- bei temporärer Nichtverfügbarkeit einzelner Fachverfahren Anfragen unmittelbar fehlschlagen. Die technische Komplexität für die Wiederholung von Übermittlungsversuchen liegt bei den Fachverfahren.
- Skalierung bei Lastspitzen eine gleichzeitige Skalierung beteiligter Systeme erfordert.

3.5.2 Option 2 – Asynchrone Vermittlungsschicht

Bei der asynchronen Kommunikation übermitteln die Fachverfahren ihre Nachrichten an die Transportinfrastruktur, die diese entgegennimmt und bis zur Abholung bereitstellt. Empfangende Fachverfahren rufen die für sie bestimmten Nachrichten aktiv ab. Versand und fachliche Verarbeitung sind somit zeitlich entkoppelt.

Gut, weil

- Versand und Verarbeitung zeitlich entkoppelt sind und die Verfügbarkeit einzelner Fachverfahren nicht unmittelbar auf andere Systeme durchschlägt.
- die Kommunikation gut mit unterschiedlich abgesicherten Netzen vereinbar ist, da Verbindungen ausschließlich vom empfangenden System initiiert werden müssen.
- Lastspitzen durch Zwischenspeicherung abgefedert werden können und nicht unmittelbar alle beteiligten Systeme gleichzeitig belasten.
- Wiederholungslogik, Zustellgarantien und Fehlerbehandlung zentral in der Transportinfrastruktur umgesetzt werden können.
- die Anbindung der Transportinfrastruktur weit verbreitete Technologien einsetzt und somit leicht integriert werden kann.

Schlecht, weil

- keine unmittelbare fachliche Antwort an das aufrufende Fachverfahren erfolgt.
- zusätzliche Mechanismen zur Statusverfolgung und Korrelation von Nachrichten erforderlich sind.
- die fachliche Prozesslogik explizit mit asynchronen Abläufen umgehen muss.

- eine zusätzliche Komplexität entsteht, da der funktionale Umfang der Transportinfrastruktur steigt, u.a. durch die Notwendigkeit einer Datenhaltung.
- die Transportinfrastruktur temporär Nachrichten speichern und verantworten muss.

3.5.3 Option 3 – Asynchrone Vermittlungsschicht mit ereignisbasierter Kommunikation

Bei der ereignisbasierten Kommunikation veröffentlichen Fachverfahren Ereignisse oder Nachrichten bei der Transportinfrastruktur. Andere Fachverfahren abonnieren relevante Ereignisse und verarbeiten diese asynchron. Die Kommunikation erfolgt nach dem Publish-Subscribe-Prinzip.

Gut, weil

- Versand und Verarbeitung zeitlich entkoppelt sind und die Verfügbarkeit einzelner Fachverfahren nicht unmittelbar auf andere Systeme durchschlägt.
- die Kommunikation gut mit unterschiedlich abgesicherten Netzen vereinbar ist, da Verbindungen ausschließlich vom empfangenden System initiiert werden müssen.
- Lastspitzen durch Zwischenspeicherung abgefedert werden können und nicht unmittelbar alle beteiligten Systeme gleichzeitig belasten.
- Wiederholungslogik, Zustellgarantien und Fehlerbehandlung zentral in der Transportinfrastruktur umgesetzt werden können.

Neutral, weil

- fachliche Prozesse als Ereignisfolgen modelliert werden können.
- das Publish-Subscribe-Prinzip technisch weit verbreitet ist, jedoch für stark zustandsorientierte Prozesse zusätzliche Modellierungsentscheidungen erfordert

Schlecht, weil

- zusätzliche Mechanismen zur Statusverfolgung erforderlich sind.
- der Nachrichtenfluss schwerer nachvollziehbar ist.
- eine klare Governance von Ereignistypen erforderlich ist.
- höhere Anforderungen an Monitoring und Tracing entstehen.
- eine ereignisbasierte Kommunikation für stark antragsorientierte, zustandsbehaftete Prozesse schnell an Komplexität gewinnt.

4 ADR-003 Festlegung des Endpunkts der Ende-zu-Ende-Verschlüsselung für das zentrale Fachverfahren

Sprache: Deutsch

Status: Vorgeschlagen

Datum: 11.03.2026

Entscheidende: Architektur-Workstream

Beratende: ITS/DS Workstream, Fachvertretungen EKS und Genehmigungsbehörden, Lenkungsausschuss, FIT-AB

Informierte: IT-PLR

4.1 Kontext und Problemstellung

Im Projekt soll eine Ende-zu-Ende-Verschlüsselung implementiert werden, die den Schutz fachlicher Daten auf dem Übertragungsweg sicherstellt. Damit diese Lösung tragfähig entworfen werden kann, muss zunächst eindeutig festgelegt werden, wo sich die kryptografischen Endpunkte der Ende-zu-Ende-Verschlüsselung befinden. Die Festlegung dieses kryptografischen Endpunkts ist von zentraler Bedeutung, da er bestimmt, wo fachliche Daten im Klartext verarbeitet werden, welche Systemkomponenten Zugriff auf Klartext erhalten und welche organisatorischen sowie betrieblichen Konsequenzen sich daraus ergeben. Gleichzeitig beeinflusst er, wie komplex Schlüsselverwaltung, Integrationsaufwände, Protokollierung und Monitoring sowie Fehlerbehandlung und Betriebsprozesse. Darüber hinaus bestimmt diese Entscheidung, ob zentrale Systemkomponenten des Fachverfahrens fachliche Daten im Klartext verarbeiten können oder ausschließlich verschlüsselte Daten speichern und weiterleiten. Die Definition dieses Endpunkts bildet deshalb die Grundlage für die Ausgestaltung der späteren Verschlüsselungsschicht.

4.2 Entscheidungsfaktoren

- ASD_14: Der Zero-Trust-Ansatz wird im System durchgängig umgesetzt.
- ASD_63: Die OSiP-Transportinfrastruktur kann durch E2EE ohne Mandantentrennung betrieben werden.
- ASD_161: Das System stellt eine Ende-zu-Ende-Verschlüsselung für alle Kommunikations- und Datenverarbeitungsvorgänge im System sicher.
- ASD_162: Das System stellt Mandantenfähigkeit mit kryptographischer Datenisolation sicher: Daten pro Land/ Behörde werden mandantenspezifisch verschlüsselt (separate Mandantenschlüssel/KMS/HSM), mit strikter RBAC-Trennung und ohne Einsicht zwischen Mandanten.

- ASD_163: Das System ist so ausgelegt, dass keine zentralen Entschlüsselungsmechanismen vorhanden sind.
- FA_142.1: Das System ermöglicht den automatischen Versand eines positiven Bescheids bei einer positiven Auto-Entscheidung
- FA_138.1: Das System ermöglicht eine Auto-Entscheidung, die vorsieht, eine Entscheidung auf Basis der Rückmeldung der EKS automatisch zu treffen, wenn keine Erkenntnisse vorliegen. Ein Bescheid wird in diesem Fall ebenfalls automatisch versandt.
- ASD_144: Das System verfügt über ein IT-Sicherheitskonzept gemäß IT-Grundschutz auf Basis von ISO/IEC 27001.
- ASD_203: Serverseitige Systeme erhalten keinen Zugriff auf private oder symmetrische Schlüssel im Klartext.
- ASD_204: Mehrere Endgeräte eines Nutzers können am Verschlüsselungsprozess teilnehmen, ohne die Gesamtsicherheit zu beeinträchtigen.
- ASD_207: Neue Geräte werden in den Schlüsselbestand eines Nutzers nur nach erfolgreicher Autorisierung integriert.
- ASD_209: Kompromittierte oder veraltete Schlüssel können entzogen und ersetzt werden.

Zukünftig zu berücksichtigende Anforderungen aus dem Geheimschutz

- ASD_416: Das System wahrt stets den Grundsatz "Kenntnis nur, wenn nötig", sodass nur Personen von VS Kenntnis erhalten, die auf Grund ihrer Aufgabenerfüllung von ihr Kenntnis haben müssen.
- ASD_418: Das System nutzt zur Verarbeitung von VS nur VS-IT, die hierfür freigegeben ist.
- ASD_445: Das System muss sicherstellen, dass geheime und private Schlüssel durch einen Hardware-Sicherheitsanker geschützt werden und niemals außerhalb eines Hardware-Sicherheitsankers dauerhaft im Klartext gespeichert werden dürfen.

Zusätzlich sind folgende architektonische Aspekte zu berücksichtigen:

- Schutz sensibler personenbezogener Daten und ggf. VS-klassifizierter Informationen
- Vertrauensannahmen gegenüber zentral betriebenen Systemkomponenten
- Komplexität der kryptografischen Schlüsselverwaltung
- Betriebliche Anforderungen wie Monitoring, Fehlersuche und Support

4.3 Betrachtete Optionen

- Option 1: Endpunkt im Backend des zentralen Fachverfahrens
- Option 2: Endpunkt auf den autorisierten Endgeräten

4.4 Entscheidung

Gewählt wurde Option 2 Endpunkt auf den autorisierten Endgeräten, denn nur diese Option erfüllt die Anforderungen an eine konsequente Ende-zu-Ende Verschlüsselung (ASD_63) und stellt sicher, dass Klartext ausschließlich auf autorisierten kryptografischen Endpunkten entsteht.

Sie ermöglicht die konsequente Umsetzung des Zero Trust Ansatzes (ASD_14), gewährleistet eine strikte mandantenspezifische kryptografische Isolation und reduziert die Angriffsflächen in Transportinfrastruktur und Fachverfahren erheblich. Darüber hinaus erfüllt sie die Anforderungen an den Schutz sensibler und VS-klassifizierter Informationen, da keine zentrale oder serverseitige Komponente fachliche Inhalte entschlüsseln kann. Das Backend des zentralen Fachverfahren speichert und verarbeitet fachliche Inhalte ausschließlich in verschlüsselter Form. Die zugehörigen kryptografischen Schlüssel befinden sich ausschließlich an den definierten kryptografischen Endpunkten.

Diese Vorteile übersteigen den geringeren Implementierungsaufwand und die geringere Komplexität von Option 1.

4.4.1 Konsequenzen

Gut, weil

- fachliche Inhalte ausschließlich auf kryptografischen Endpunkten im Klartext vorliegen, wodurch die Angriffsfläche auf zentrale Systeme erheblich reduziert wird.
- der Zero Trust Ansatz konsequent umgesetzt wird und weder Transportinfrastruktur noch Fachverfahren Klartext empfangen.
- eine strikte kryptografische Mandantenisolation möglich ist.
- Anforderungen an den Geheimschutz und den Umgang mit VS einfacher erfüllbar werden.
- das zentrale Fachverfahren auch durch Betreiber ohne Zugriff auf fachliche Inhalte betrieben werden kann

Neutral, weil

- bei Fremd-Fachverfahren der kryptografische Endpunkt auch serverseitig liegen kann. Dies liegt im Verantwortungsbereich der jeweiligen Organisation.

Schlecht, weil

- zusätzliche Komplexität im Schlüsselmanagement entsteht, insbesondere bei Gerätewechseln, Mehrgerätebetrieb und Wiederherstellungsszenarien.
- Support, Fehlersuche und Monitoring erschwert werden.
- der Schutz der Endgeräte stark an Bedeutung gewinnt und erhöhte Anforderungen an Betrieb, Härtung und organisatorische Maßnahmen entstehen.
- zusätzliche Komponenten wie mandantenspezifische Agenten erforderlich werden können, um automatische Prozesse zu ermöglichen, zu deren Betrieb Mandanten ggf. nicht in der Lage sind.

4.5 Vor- und Nachteile der Optionen

4.5.1 Option 1: Endpunkt im Backend des zentralen Fachverfahrens

Bei dieser Option liegt der Endpunkt der Verschlüsselung in den Backend-Komponente des zentralen Fachverfahrens. Alle Übertragungsstrecken zwischen den externen Fachverfahren und dem zentralen Fachverfahren sind verschlüsselt, jedoch werden die Daten zentral mandatenübergreifend im Backend entschlüsselt und dort im Klartext weiterverarbeitet. Die Transportinfrastruktur braucht nur für das Routing relevante Informationen in Form von Meta-Daten im Klartext, alle inhaltlichen Daten bleiben verschlüsselt.

Gut, weil

- bestehende fachliche Prüfmechanismen, Validierungen und Automatisierungsprozesse zentral leichter umsetzbar sind.
- Integrationen mit Umsystemen einfacher gestaltet werden können, da diese serverseitig erfolgen können.
- Querschnittsfunktionen wie Validierung, Virenprüfung und Transformation zentral umgesetzt werden können

Schlecht, weil

- die Vertraulichkeit zwar auf der Transportebene gegeben ist, aber im Backend des zentralen Fachverfahrens nicht.
- Ende-zu-Ende Verschlüsselung auf fachlicher Ebene nicht erreicht wird und damit zentrale Anforderungen an E2EE nur teilweise erfüllt werden.
- VS-Anforderungen schwieriger umzusetzen sind, da Klartext in serverseitigen Komponenten verarbeitet wird, welche im Verantwortungsbereich des zentralen Betreibers liegen.

- ein kompromittiertes zentrales Fachverfahren Zugang zu allen fachlichen Daten der jeweiligen Mandanten ermöglichen könnte, ohne kryptografische Barrieren zwischen Verarbeitung und Transport.
- mandantenspezifische kryptografische Isolation nur eingeschränkt möglich ist, da Klartext zwingend serverseitig entsteht.

4.5.2 Option 2: Endpunkt auf den autorisierten Endgeräten

Bei dieser Option befinden sich die kryptografischen Endpunkte auf den autorisierten Endgeräten der Nutzer oder auf dedizierten automatisierten Agenten. Alle beteiligten Zwischensysteme und Umsysteme – einschließlich des zentralen Backends des Fachverfahrens und der Transportinfrastruktur – verarbeiten ausschließlich verschlüsselte Daten, wobei für das Routing benötigte Meta-Daten von der Verschlüsselung ausgenommen sind.

Gut, weil

- echte Ende-zu-Ende-Verschlüsselung erreicht wird und Klartext ausschließlich auf den autorisierten Endgeräten entsteht.
- Vertraulichkeit strikt eingehalten wird, da kein Zwischensystem fachliche Inhalte entschlüsseln kann.
- Angriffsflächen in Transportinfrastruktur und zentralem Fachverfahren erheblich reduziert werden, da dort ausschließlich verschlüsselte Daten vorliegen.
- VS-Anforderungen besser erfüllbar sind, da Klartext nur in minimalen, eindeutig kontrollierbaren Zonen erscheint.
- mandantenspezifische kryptografische Isolation vollständig durchsetzbar ist und keine Klartextüberlappungen entstehen können.
- Betreiber keinen Zugriff auf fachliche Inhalte erhalten.

Neutral, weil

- automatisierte Prozesse durch dedizierte kryptografische Agenten umgesetzt werden können (bspw. für Auto-Entscheide, Virenprüfung, Quittierung und Validierung)

Schlecht, weil

- die Endgeräte der Nutzer evtl. zusätzliche Funktionen wie bspw. Virenprüfungen erfüllen müssen und hieraus eine Abhängigkeit von der lokalen Endgeräteeinrichtung entsteht.
- für mandantenspezifische Agenten zusätzliche Implementierungsaufwände entstehen.

- Mandanten evtl. keinen Agenten eigenverantwortlich betreiben können und diese dann evtl. in der Verantwortung eines zentralen Betreibers betrieben werden müssten.
- die Komplexität der Schlüsselverwaltung steigt, insbesondere bei Gerätewechseln, Mehrgerätebetrieb, Vertretungen, Mandantenwechseln und Wiederherstellungsfällen.
- Support, Monitoring und Fehlersuche erschwert werden.
- der Schutz der Endgeräte deutlich an Bedeutung gewinnt und damit neue Anforderungen an Härtung, BYOD-Ausschluss und Betriebskonzepte entstehen. Maßnahmen bei bspw. Geräteverlust müssen ergriffen werden.

5 ADR-004 Auswahl der Ende-zu-Ende-Verschlüsselungsschicht

Status: Vorgeschlagen

Datum: 17.03.2026

Entscheidende: Architektur-Workstream

Beratende: ITS/DS Workstream, Fachvertreter:innen EKS und Genehmigungsbehörden, Lenkungsausschuss

Informierte: IT-PLR

5.1 Kontext und Problemstellung

Der Auftrag des IT-PLR forciert eine Ende-zu-Ende-verschlüsselte Lösungsarchitektur (Beschluss 2025/20[1]). Des Weiteren ergibt sich aus datenschutzrechtlichen und Geheimschutzanforderungen die Notwendigkeit, eine geeignete Verschlüsselungsschicht zu wählen.

Dieser ADR trifft dabei keine Entscheidung über die Verschlüsselung ruhender Daten in den Fachverfahren oder Backend-Systemen. Er baut auf ADR-003 „Definition des Endpunkts der Ende-zu-Ende-Verschlüsselung für das zentrale Fachverfahren“ auf und fokussiert sich ausschließlich auf die Auswahl eines geeigneten Protokolls bzw. Protokolltyps zur Umsetzung der Anforderungen an die systemübergreifende Ende-zu-Ende-Verschlüsselung der übertragenen fachlichen Daten.

Ziel dieser Entscheidung ist die Auswahl einer E2EE-Schicht, die unabhängig von der gewählten Transportschicht eingesetzt werden kann oder diese zumindest nicht unnötig architektonisch vorbestimmt. Darüber hinaus muss die gewählte Lösung mit asynchroner Kommunikation, dynamischen Kommunikationsbeziehungen, Mehrgerätefähigkeit und einer möglichen Erweiterung um zusätzliche autorisierte kryptographische Endpunkte (z. B. Bots oder Agenten) vereinbar sein.

Nicht Gegenstand dieser Entscheidung sind die konkrete Ausgestaltung des Schlüsselmanagements, die Identitätsbindung kryptographischer Schlüssel, die Vertrauensdienste für Authentisierung und Zertifikatsprüfung sowie die Verarbeitung verschlüsselter Daten außerhalb des Kommunikationskanals. Diese Aspekte sind in nachgelagerten ADRs bzw. im Architekturkonzept konkretisiert.

5.2 Entscheidungsfaktoren

[1] https://www.it-planungsrat.de/beschluss/beschluss-2025-20

- ASD_14: Der Zero-Trust-Ansatz wird im System durchgängig umgesetzt.
- ASD_121: Die Entwicklung soll quelloffene standardisierte Entwicklungswerkzeuge mit adäquatem Support (Programme, Frameworks, Bibliotheken) verwenden.
- ASD_160: Die kryptografische Architektur und Implementierung ist extern überprüfbar und dokumentiert.
- ASD_163: Das System ist so ausgelegt, dass keine zentralen Entschlüsselungsmechanismen vorhanden sind.
- ASD_168: Das System nutzt aktuelle TLS-Konfigurationen (mindestens Version 1.2), verschlüsselt Daten im Ruhezustand (AES-256) und im Transit.
- ASD_169: Die Zertifikatsvalidierung erfolgt gemäß aktueller kryptografischer Sicherheitsstandards. Veraltete, schwache oder unsichere Protokolle und Chiffren sind ausgeschlossen.
- ASD_175: Das System ermöglicht eine zertifikatsbasierte Übermittlung der Daten mit Ende-zu-Ende Verschlüsselung zwischen dem Endgerät der antragstellenden Person bzw. dem Online-Dienst bzw. dem Portal auf dem der Dienst betrieben wird und der zuständigen Behörde. Die Verschlüsselung reicht mindestens bis zu einem von der nachnutzenden Behörde zu definierenden Endpunkt.
- ASD_177: Alle Datenübermittlungen unterliegen einer automatisierten Zertifikatsprüfung.
- ASD_178: Das System hält kryptographische Verfahren, Parameter und Cipher Suites austauschbar und führt ein zentrales Krypto-Kataster (Algorithmen, Schlüssellängen, Einsatzorte, Lebenszyklus).
- ASD_179: Das System setzt kryptographische Protokolle, Verschlüsselungsalgorithmen und -Modi nach aktuellem Stand der Technik ein.
- ASD_180: Die Verschlüsselung des Systems basiert auf Authenticated Encryption (AEAD), um Vertraulichkeit und Integrität sicherzustellen.
- ASD_181: Das System verwendet asymmetrische Verschlüsselung für Schlüsselverteilung.
- ASD_184: Das System unterstützt die Rotation kryptografischer Schlüssel in festgelegten Intervallen und stellt sicher, dass abgelaufene Schlüssel nicht mehr verwendet werden können.
- ASD_190: Es werden ausschließlich starke, öffentlich geprüfte Verschlüsselungs- und Signaturalgorithmen verwendet.
- ASD_192: Das Kryptokonzept unterstützt Verfahren, die nach einer Kompromittierung eine Wiederherstellung des Systems ermöglichen.

- ASD_193: Wiederholte oder manipulierte Nachrichten werden erkannt und ausgeschlossen.
- ASD_197: Schlüssel werden in sicherer Umgebung erzeugt und verwaltet.
- ASD_202: Die Zuordnung zwischen Identität und öffentlichem Schlüssel ist überprüfbar und vertrauenswürdig.
- ASD_203: Serverseitige Systeme erhalten keinen Zugriff auf private oder symmetrische Schlüssel im Klartext.
- ASD_204: Mehrere Endgeräte eines Nutzers können am Verschlüsselungsprozess teilnehmen, ohne die Gesamtsicherheit zu beeinträchtigen.

Zukünftig zu berücksichtigende Anforderungen aus dem Geheimschutz:

- ASD_449: Das System weist einen höchstmöglichen Grad an Kryptoagilität auf, um auf Entwicklungen im Bereich der Post-Quanten-Kryptografie reagieren, kommende Empfehlungen und Normen umsetzen und künftig geschwächte Algorithmen austauschen zu können.

Zusätzlich sind für diese Entscheidung folgende architektonische Kriterien relevant:

- Unterstützung asynchroner Kommunikation
- Unterstützung dynamischer Gruppenkommunikation
- Unterstützung autorisierter zusätzlicher kryptographischer Endpunkte (z. B. Bots/Agenten)
- Geringe Kopplung an ein konkretes Nachrichtenformat oder Transportprotokoll
- Gute Integrierbarkeit in heterogene Fachverfahrenslandschaften

5.3 Betrachtete Optionen

- Option 1: Einsatz von E-Mail-Verschlüsselungsstandards
- Option 2: Einsatz von nachrichtenformatnahen Verschlüsselungsverfahren
- Option 3: Einsatz von Messenger Verschlüsselungsverfahren

5.4 Entscheidung

Gewählte Option: "Option 3: Einsatz von Messenger Verschlüsselungsverfahren" unter Einsatz von MLS.

MLS ist als IETF-Standard für sichere Gruppenkommunikation veröffentlicht. Das Protokoll selbst ist in RFC 9420[2] spezifiziert. Die zugehörige Architektur in RFC 9750[3].

[2] https://www.rfc-editor.org/info/rfc9420
[3] https://www.rfc-editor.org/info/rfc9750

Diese Option wird gewählt, weil sie die Anforderungen an systemübergreifende Ende-zu-Ende-Verschlüsselung im gegebenen Zielbild am besten erfüllt. MLS unterstützt dynamische Gruppen, Mehrgerätefähigkeit, asynchrone Kommunikation sowie moderne kryptographische Eigenschaften wie Forward Secrecy (FS) und Post-Compromise Security (PCS).

Im Unterschied zu nachrichtenformatnahen Verschlüsselungsverfahren ist MLS nicht auf ein bestimmtes Transportprotokoll oder Nachrichtenformat festgelegt. Somit kann die Wahl einer geeigneten Transportschicht weitgehend unabhängig getroffen werden. Außerdem erlaubt es die Kommunikation mit mehreren Kommunikationsparteien (Gruppen, Mehrgerätefähigkeit).

Das BSI hat MLS bereits im Zusammenhang mit sicheren Messengern und dem Austausch von VS-NfD Material betrachtet (siehe BSI-VS-AP-0024-2024 | Version 2.0[4]). Dies wird als positives Indiz für die Eignung von MLS im sicherheitssensiblen Umfeld gewertet, ersetzt jedoch keine eigenständige Bewertung der Gesamtlösung im konkreten Nutzungskontext.

Zur Abdeckung relevanter Anforderungen können zusätzliche Dienstleistungen zentral bereitgestellt werden, zum Beispiel kann die Virenprüfung in einem zentralen Bot-Client erfolgen. Die Messaging Layer Security (MLS) Architektur soll verwendet werden. Für die Authentisierung der Kommunikationspartner und die Bindung von Identitäten an kryptographische Schlüssel sind zusätzliche Vertrauensdienste erforderlich. Eine (V-)PKI könnte hierbei unter anderem als zentraler Vertrauensanker dienen. Die konkrete Ausgestaltung ist Gegenstand nachgelagerter Entscheidungen (siehe ADR-006 und ADR-007).

MLS wird in der Zielarchitektur als E2EE-Schicht für fachliche Nutzdaten verwendet. Die Transportschicht, Zustelldienste sowie Authentisierungs- und Vertrauensdienste bleiben hiervon logisch getrennt und sind ergänzend ausgestaltet bzw. auszugestalten.

[4] https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Zulassung/VS-Anforderungsprofile/Anforderungsprofile/BSI-VS-AP-0024.html

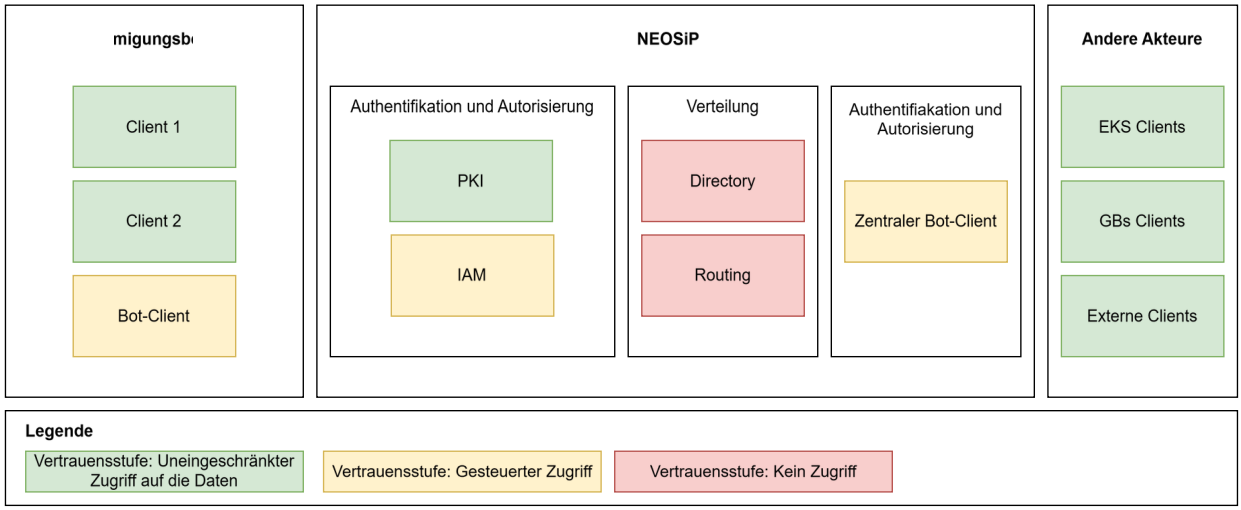

Abbildung: Trust- und Komponentenmodell für MLS-basierte Verschlüsselung

5.4.1 Konsequenzen

Gut, weil

- MLS auch in anderen deutschen und europäischen Projekten Einsatz findet und somit Synergieeffekte genutzt werden können. Diese Aussage ist als Erwartungshaltung zu verstehen und muss im weiteren Projektverlauf konkret erarbeitet werden.
- MLS die Anforderungen in den Entscheidungsfaktoren weitgehend erfüllt, da es keine direkte Kopplung an ein Transportprotokoll oder Nachrichtenformat bewirkt und die Einbindung zusätzlicher autorisierter kryptographischer Endpunkte wie Bots oder Agenten grundsätzlich unterstützt

Neutral, weil

- eine Auswahl einer geeigneten Transportschicht getroffen werden muss.
- MLS zusätzliche Komponenten wie z. B. Authentication Services und Delivery Services erfordert, um neben dem E2E-verschlüsselten Kanal auch die Authentizität der Nachrichten und Kommunikationspartner sicherzustellen.

Schlecht, weil

- die Umsetzung der E2EE komplex ist und besondere Expertise erfordert.

Zusätzliche Punkte:

- Es muss ein Kryptokonzept erarbeitet werden, welches die Verschlüsselung der im zentral zur Verfügung gestellten Fachverfahren abgelegten Daten festlegt. Dabei müssen die bereits in diesem ADR als Entscheidungsfaktoren hinterlegten Anforderungen, aber auch weitere wie beispielsweise FA_19, FA_535.1, ASD_115, FA_287.1, FA_529 und FA_632 berücksichtigt werden.
- Es muss außerdem ein Betriebs- und Schlüsselmanagementkonzept erarbeitet werden, das insbesondere Gruppenlebenszyklus, Geräteverwaltung, Schlüsselrotation, Sperrung, Wiederherstellung, Auditierung und die Behandlung automatisierter Endpunkte regelt.

5.5 Vor- und Nachteile der Optionen

5.5.1 Option 1: Einsatz von E-Mail-Verschlüsselungsstandards

Die Standards OpenPGP (RFC 9580[5]) und S/MIME (RFC 8551[6]) gehören zu den etablierten Standards zur Realisierung einer Inhaltsdatenverschlüsselung. Sie basieren technisch auf vergleichsweise einfachen kryptographischen Verfahren, insbesondere zur asymmetrischen Verschlüsselung, weisen jedoch für das vorliegende Zielbild funktionale und kryptographische Grenzen auf.

Gut, weil

- OpenPGP und S/MIME sind bewährte, praxiserprobte Verschlüsselungsstandards, die auch außerhalb der öffentlichen Verwaltung eingesetzt werden.
- OpenPGP und S/MIME haben den strengen Standardisierungsprozess der IETF durchlaufen.
- OpenPGP und S/MIME sind geeignet, um Inhaltsdaten verschlüsselt auch über intermediäre Systeme hinweg durchgehend verschlüsselt zu übermitteln.
- OpenPGP und S/MIME sind auch in asynchronen Kommunikationsszenarien nutzbar (die Kommunikationsparteien müssen nicht gleichzeitig online sein).

Neutral, weil

- sie transportunabhängig einsetzbar sind.

Schlecht, weil

- OpenPGP und S/MIME keine Kommunikation in dynamischen Gruppen vorsieht.

[5] https://www.rfc-editor.org/rfc/rfc9580
[6] https://www.rfc-editor.org/rfc/rfc8551

- Die für das Zielbild besonders relevanten modernen kryptographischen Eigenschaften wie Perfect Forward Secrecy (PFS) und Post-Compromise Security (PCS, auch: Future Secrecy) nicht unterstützt werden.
- Mehrgerätefähigkeit, Gruppenlebenszyklus und autorisierte zusätzliche kryptographische Endpunkte nur mit erheblichem zusätzlichem Architektur- und Implementierungsaufwand realisierbar wären.

5.5.2 Option 2: Einsatz von nachrichtenformatnahen Verschlüsselungsverfahren

Viele Transportinfrastrukturen bringen bereits eigene Verfahren zur Ende-zu-Ende-Verschlüsselung mit. So nutzt etwa OSCI XML Encryption, während FIT-Connect auf JSON Web Encryption (JWE) setzt. Diese Ansätze können technisch ausgereift und praxistauglich sein, binden die Verschlüsselung jedoch eng an das jeweilige Nachrichtenformat. Dies kann zu Lock-in-Effekten führen, determiniert die Transportschicht und reduziert dadurch die Architekturfreiheit.

5.5.2.1 Option 2a Einsatz von XML-Encryption

Der XML-Encryption-Standard[7] spezifiziert Methoden zur Anwendung kryptographischer Algorithmen im XML-Umfeld. u.a. zur asymmetrischen Verschlüsselung.

Gut, weil

- XML-Encryption ist ein bewährter, praxiserprobter Verschlüsselungsstandard, der auch außerhalb der öffentlichen Verwaltung eingesetzt wird.
- XML-Encryption hat den strengen Standardisierungsprozess des W3C durchlaufen.
- XML-Encryption ist geeignet, um Inhaltsdaten verschlüsselt auch über intermediäre Systeme hinweg durchgehend verschlüsselt zu übermitteln.
- XML-Encryption ist auch in asynchronen Kommunikationsszenarien nutzbar (die Kommunikationsparteien müssen nicht gleichzeitig online sein).

Schlecht, weil

- Die für das Zielbild relevanten modernen kryptographischen Eigenschaften wie Perfect Forward Secrecy (PFS) und Post-Compromise Security (PCS, auch: Future Secrecy) nicht unterstützt werden.
- XML Encryption ist für moderne Web-/Frontend-Szenarien nur eingeschränkt geeignet, weil die Umsetzung im Browser- und JavaScript-Umfeld vergleichsweise aufwändig ist.

[7] https://www.w3.org/TR/xmlenc-core/

- es in der Vergangenheit häufig zu Sicherheitslücken aufgrund von fehlerhaften Implementierungen oder unsicheren Anwendungsmustern des XML-Encryption-Standards kam.
- XML-Encryption konzeptionell nur die direkte Kommunikation zwischen zwei Kommunikationsparteien und nicht den Einsatz mit mehr als zwei Enden vorsieht. Dies schränkt nicht nur auf fachlicher Ebene Gruppenkommunikation, sondern auch Mehrgerätefähigkeit stark ein bzw. erfordert zusätzliche Maßnahmen zur Realisierung dieser Funktionalität.
- XML-Encryption keine Kommunikation in dynamischen Gruppen vorsieht.

5.5.2.2 Option 2b: Einsatz von JSON Web Encryption

Der JSON Web Encryption-Standard (RFC 7516[8]) spezifiziert Methoden zur Anwendung kryptographischer Algorithmen im JSON-Umfeld. Gemeinsam mit weiteren RFCs der IETF-Arbeitsgruppe „Javascript Object Signing and Encryption"[9] spezifiziert RFC 7516 Methoden u.a. zur asymmetrischen Verschlüsselung.

Gut, weil

- JSON Web Encryption ist ein bewährter, praxiserprobter Verschlüsselungsstandard, der auch außerhalb der öffentlichen Verwaltung eingesetzt wird.
- JSON Web Encryption hat den strengen Standardisierungsprozess der IETF durchlaufen.
- JSON Web Encryption ist geeignet, um Inhaltsdaten verschlüsselt auch über intermediäre Systeme hinweg durchgehend verschlüsselt zu übermitteln.
- JSON Web Encryption ist auch in asynchronen Kommunikationsszenarien nutzbar (die Kommunikationsparteien müssen nicht gleichzeitig online sein).
- JSON Web Encryption ist aufgrund der guten Verfügbarkeit von Bibliotheken und der Nähe zu modernen Web-Technologien grundsätzlich gut in Web- und API-Umgebungen integrierbar.

Schlecht, weil

- die für das Zielbild relevanten modernen kryptographischen Eigenschaften wie Perfect Forward Secrecy (PFS) und Post-Compromise Security (PCS, auch: Future Secrecy) nicht durch den Standard selbst bereitgestellt werden.

[8] https://www.rfc-editor.org/rfc/rfc7516
[9] https://datatracker.ietf.org/wg/jose/documents/

- JSON Web Encryption konzeptionell nur die direkte Kommunikation zwischen zwei Kommunikationsparteien und nicht den Einsatz mit mehr als zwei Enden vorsieht. Dies schränkt nicht nur auf fachlicher Ebene Gruppenkommunikation, sondern auch Mehrgerätefähigkeit stark ein bzw. erfordert zusätzliche Maßnahmen zur Realisierung dieser Funktionalität.
- der JSON Web-Encryption-Standard keine Kommunikation in dynamischen Gruppen vorsieht.

5.5.3 Option 3: Einsatz von Messenger Verschlüsselungsverfahren

Die Entwicklung von Ende-zu-Ende-Verschlüsselung im Bereich Messenger hat in den letzten Jahren erhebliche Fortschritte gemacht. Beginnend mit Protokollen wie OTR (Off-the-Record) über moderne Ansätze wie Signal, OMEMO bzw. Olm/Megolm bis hin zu dem aktuellen Standard Messaging Layer Security (MLS) zeigt sich eine Entwicklung hin zu sicheren, skalierbaren und nutzerfreundlichen Lösungen. Diese Technologien sind speziell darauf ausgelegt, asynchrone Kommunikation mit mehreren Teilnehmern in Gruppen zuverlässig und vertraulich zu ermöglichen.

Wir betrachten im weiteren Verlauf nur MLS, welches stark von OTR, OMEMO, Olm/Megolm und dem Signal-Protokoll inspiriert ist. Es unterstützt Forward Secrecy und Post-Compromise Security und wurde aber nicht spezifisch für den Einsatz in einem bestimmten Kommunikationsprotokoll (wie XMPP oder Matrix) entwickelt.

Gut, weil

- MLS ist ein international standardisierter Verschlüsselungsstandard, der auch außerhalb der öffentlichen Verwaltung eingesetzt werden kann.
- MLS hat den strengen Standardisierungsprozess der IETF durchlaufen.
- MLS wurde bereits in der internationalen wissenschaftlichen Community auf mögliche Schwachstellen untersucht, auch wenn es sich in einer Frühphase der praktischen Einführung befindet.
- MLS ist geeignet, um Inhaltsdaten verschlüsselt auch über intermediäre Systeme hinweg durchgehend verschlüsselt zu übermitteln.
- MLS ist auch in asynchronen Kommunikationsszenarien nutzbar (die Kommunikationsparteien müssen nicht gleichzeitig online sein).
- moderne kryptographische Eigenschaften wie Perfect Forward Secrecy (PFS) und Post-Compromise Security (PCS, auch: Future Secrecy) unterstützt werden.
- es stehen (u.a. aufgrund der Vorgaben des IETF-Standardisierungsprozess und der

Förderung durch die EU-Kommission und des Bundesministeriums für Bildung und Forschung (BMBF)) gleich mehrere frei verfügbare Implementierungen bereit[10][11][12].

- MLS ist nicht spezifisch für den Einsatz in einem bestimmten Kommunikationsprotokoll entwickelt worden.
- MLS sieht auch die Kommunikation in dynamischen Gruppen vor (Join/Leave-Rekeying) inkl. der Mehrgerätefähigkeit.
- die Kommunikation mit mehreren Parteien die Möglichkeit bietet Schemavalidierung bzw. Schadsoftwareprüfung durch die Nutzung eines speziellen Agenten zu ermöglichen, ohne die E2EE aufbrechen zu müssen. Diese Agenten können optional innerhalb der Verantwortungsbereiche der Kommunikationsparteien betrieben werden und müssen nicht zwingend zentral betrieben werden.

Neutral, weil

- die Unterstützung von MLS in Kommunikationslösungen/-protokollen befindet sich derzeit noch in der Umsetzung. Es existieren jedoch bereits nutzbare Implementierungen[13][14], die eine Integration in prinzipiell beliebige Kommunikationslösungen/-protokolle ermöglichen.
- die moderne kryptographische Eigenschaft der Plausible Deniability aktuell nicht unterstützt wird.
- MLS als Protokollentscheidung ein belastbares Gruppen-, Geräte- und Schlüsselmanagement sowie geeignete Betriebsprozesse voraussetzt

Schlecht, weil

- es sich um eine sehr moderne Technik handelt, deren Integration komplex ist und Expertise erfordert.

5.6 Weitere Informationen

Der durch MLS geschützte Kommunikationskanal eignet sich gut, um den Nachrichtenaustausch vom Sachbearbeiter bis hin zur Erkenntnisstelle und zurück abzusichern. Für eine Daten- und Geheimschutz-konforme Speicherung von Antragsdaten und Erkenntnissen im Backend des zentral zur Verfügung gestellten Fachverfahrens und zur Sicherstellung einer Mandantentrennung können neben der Beibehaltung der Verschlüsselung

[10] https://github.com/mlswg/mls-implementations/blob/main/implementation_list.md
[11] https://github.com/cisco/mlspp
[12] https://openmls.tech/
[13] https://arewemlsyet.com/
[14] https://www.ietf.org/blog/support-for-mls-2023/

des durch MLS aufgebauten Kommunikationskanals ggf. andere Methoden gewählt werden. Hier muss im Rahmen eines Konzepts ein Ansatz erarbeitet werden, der den Anforderungen an die Anwendung genügt (siehe Konsequenzen).

Die Entscheidung für MLS trifft ausdrücklich keine Vorfestlegung darüber, wie verschlüsselte Fachdaten außerhalb des eigentlichen Kommunikationskanals gespeichert, indiziert, validiert oder durch automatisierte Prozesse verarbeitet werden. Diese Aspekte sind in einem nachgelagerten Kryptokonzept sowie in den ADRs zu Schlüsselmanagement, Identitätsbindung und Vertrauensdiensten zu konkretisieren

6 ADR-005 Authentizität und Integrität in der Ende-zu-Ende-Nachrichtenübermittlung

Sprache: Deutsch

Status: Vorgeschlagen

Datum: 2026-03-17

Entscheidende: Architektur-Workstream

Beratende: FIT-AB, FITKO-AM

Informierte: Lenkungsausschuss, IT-PLR

6.1 Kontext und Problemstellung

Im System werden fachliche Nachrichten zwischen verteilten Endpunkten ausgetauscht, wobei Backend-Komponenten und die Transportinfrastruktur als potenziell kompromittierbar zu betrachten sind. Für die Ende-zu-Ende-Verschlüsselungsschicht ist in ADR-004 Messaging Layer Security (MLS[15]) entschieden worden. Daraus ergibt sich die Frage, welche Ebene als Anker für die Authentizität und Integrität von Nachrichten herangezogen wird und welche Rolle Transport- und Backendkomponenten dabei spielen dürfen.

Dieser ADR legt fest, auf welcher Schicht die fachliche Absenderbindung und die kryptografische Integritätssicherung von Nachrichten verbindlich verankert werden.

Nicht Gegenstand dieses ADR sind die konkrete Ausgestaltung der Identitätsbindung an kryptografische Schlüssel, Vertrauensdienste zur Schlüsselverifikation sowie Detailfestlegungen zu Geräteverwaltung und Betriebsprozessen. Diese Aspekte sind in nachgelagerten ADRs bzw. dem Architekturkonzept konkretisiert bzw. noch zu konkretisieren.

6.2 Entscheidungsfaktoren

- ARC_004: Ein Zero-Trust-Ansatz ist durchgängig zu verfolgen, inklusive Identitätsprüfung und Zugriffskontrolle.
- ARC_075: Das System soll nach dem Zero-Trust-Prinzip arbeiten, d. h. jede Anfrage wird authentifiziert und autorisiert.
- ASD_211: Das System verfügt über ein Identitäts- und Berechtigungsmanagement, das an die Geschäftsprozesse, Organisationsstrukturen sowie an den hohen Schutzbedarf ausgerichtet ist.
- ASD_317: Das System integriert Security by Design mit Nachweisdokumentation in den Entwicklungsprozess.

[15] https://datatracker.ietf.org/doc/html/rfc8446

- ASD_208: Nutzer können die Vertrauenswürdigkeit von Kommunikationspartnern über Schlüsselprüfungen bestätigen.
- ASD_202: Die Zuordnung zwischen Identität und öffentlichem Schlüssel ist überprüfbar und vertrauenswürdig.
- ASD_159: Das System stellt über abgesicherte Kommunikationskanäle den vertrauenswürdigen Informationsaustausch zwischen Genehmigungsbehörden, Erkenntnisstellen und weiteren Stellen sicher.
- ASD_160: Die kryptografische Architektur und Implementierung ist extern überprüfbar und dokumentiert.
- ASD_163: Das System ist so ausgelegt, dass keine zentralen Entschlüsselungsmechanismen vorhanden sind.
- ASD_173: Das System setzt digitale Signaturen zur Sicherstellung der Datenintegrität beim Datenaustausch mit Erkenntnisstellen und Genehmigungsbehörden ein.
- ASD_180: Die Verschlüsselung des Systems basiert auf Authenticated Encryption (AEAD), um Vertraulichkeit und Integrität sicherzustellen.
- ASD_178: Das System hält kryptographische Verfahren, Parameter und Cipher Suites austauschbar und führt ein zentrales Krypto-Kataster (Algorithmen, Schlüssellängen, Einsatzorte, Lebenszyklus).
- ASD_179: Das System setzt kryptographische Protokolle, Verschlüsselungsalgorithmen und -modi nach aktuellem Stand der Technik ein.
- ASD_192: Das Kryptokonzept unterstützt Verfahren, die nach einer Kompromittierung eine Wiederherstellung des Systems ermöglichen.
- ASD_193: Wiederholte oder manipulierte Nachrichten werden erkannt und ausgeschlossen.
- ASD_200: Änderungen oder Neuregistrierungen von Schlüsseln sind überprüfbar und nachvollziehbar.
- ASD_203: Serverseitige Systeme erhalten keinen Zugriff auf private oder symmetrische Schlüssel im Klartext.

Zusätzlich sind für diese Entscheidung folgende architektonische Kriterien relevant:

- Intermediäre Komponenten dürfen nicht als Vertrauensanker für fachliche Absicherung fungieren.
- Fachliche Nachrichten müssen auch bei fehlverhaltender oder kompromittierter Transportinfrastruktur kryptografisch abgesichert bleiben.

- Transportschutz ist weiterhin erforderlich, darf aber nicht mit fachlicher Ende-zu-Ende-Authentizität und -Integrität gleichgesetzt werden.

6.3 Betrachtete Optionen

- Option 1: Keine explizite Authentizität und Integrität in der Nachrichtenübermittlung
- Option 2: Herstellung der Authentizität und Integrität ausschließlich auf der Transportebene
- Option 3: Herstellung der Authentizität und Integrität auf der fachlichen Ende-zu-Ende-Verschlüsselungsschicht

6.4 Entscheidung

Gewählte Option: "Option 3: Herstellung der Authentizität und Integrität auf der fachlichen Ende-zu-Ende-Verschlüsselungsschicht", denn beim Einsatz von MLS ist Ende-zu-Ende-Authentizität und Ende-zu-Ende-Integrität konzeptionell und technisch Bestandteil der Protokollebene. Transport- oder Backend-Authentizität und Integrität kann diese E2E-Eigenschaften weder ersetzen noch auf sichere Weise emulieren. Der ADR stellt damit verbindlich klar, dass die fachliche Authentizität und Integrität von Nachrichten maßgeblich durch die MLS-Schicht abgesichert und von Endpunkten geprüft wird, während TLS lediglich ergänzende Betriebssicherheit liefert.

Der Transportschutz bleibt für die Absicherung von Kommunikationskanälen, Komponentenidentitäten (bspw. durch Einsatz von mTLS) und betrieblicher Missbrauchsreduktion weiterhin erforderlich. Er wird jedoch ausdrücklich nicht als Sicherheitsanker für die fachliche Ende-zu-Ende-Absenderbindung und Nachrichtenintegrität definiert.

6.4.1 Konsequenzen

Gut, weil

- die Authentizität und Integrität von Nachrichten für Endpunkte kryptografisch überprüfbar ist, auch wenn Backends/Transportinfrastruktur kompromittiert oder fehlverhaltend sind.
- das Architekturprinzip, dass Backends nicht Vertrauensanker für E2E-Sicherheit sind verbindlich und prüfbar festgelegt wird. Dies ist wichtig für die Anbindung von Drittimplementierungen.

Neutral, weil

- Transport-Security weiterhin genutzt werden kann und soll, ohne die E2E-Sicherheitsgarantien zu relativieren.
- für Interoperabilität und Drittanbindungen unterstützende Artefakte wie SDKs zweckmäßig werden
- Endpunkte die kryptografische Prüfung, Fehlerbehandlung und korrekte Verarbeitung von Vertrauensinformationen zuverlässig umsetzen müssen

Schlecht, weil

- zusätzliche Anforderungen an Fachverfahrens-Implementierungen entstehen.

6.5 Vor- und Nachteile der Optionen

6.5.1 Option 1: Keine explizite Authentizität und Integrität in der Nachrichtenübermittlung

Diese Option verzichtet auf kryptografische Verfahren zur Überprüfung von Absendern und Nachrichtenintegrität auf der fachlichen Ende-zu-Ende-Ebene

Schlecht, weil

- Integrität und Authentizität nicht überprüfbar sind und aktive Angriffe wie bspw. Injection, Manipulation, Umleitung nicht zuverlässig erkannt werden können.
- die Sicherheitsziele des Systems verfehlt werden und MLS als gewählte E2EE-Schicht damit faktisch nicht korrekt eingesetzt werden kann.
- Endpunkte keine belastbare kryptografische Absenderbindung hätten und damit fachliche Vertrauensentscheidungen nicht sicher treffen könnten

6.5.2 Option 2: Herstellung der Authentizität und Integrität ausschließlich auf der Transportebene

Authentizität wird als Eigenschaft eines abgesicherten Transportkanals zwischen Komponenten interpretiert.

Gut, weil

- bspw. mTLS und Service-to-Service Authentisierung für Betriebssicherheit, Netzwerksegmentierung und Missbrauchsreduktion sinnvoll und etabliert sind.

Neutral, weil

- Transportauthentizität ein notwendiges Grundprinzip sein sollte, aber nicht als Ende zu Ende-Sicherheitsanker definiert sein sollte.

Schlecht, weil

- auch intermediäre Komponenten zu Sicherheitsankern für Absenderbindung und Integritätsannahmen würden, was dem Zero-Trust-Prinzip widerspricht
- Transportauthentizität und –integrität die fachliche Ende-zu-Ende-Kette nicht ersetzen kann. Eine kompromittierte intermediäre Komponente könnte weiterhin Teilnehmer täuschen oder Nachrichtenflüsse manipulieren. Endpunkte hätten keine kryptografisch belastbare Absenderbindung.

6.5.3 Option 3: Herstellung der Authentizität und Integrität auf der fachlichen Ende-zu-Ende-Verschlüsselungsschicht

Authentizität und Integrität werden kryptografisch direkt zwischen den fachlichen Endpunkten umgesetzt und durch diese geprüft.

Gut, weil

- die fachliche Authentizität und Integrität integraler Bestandteil der fachlichen Schicht ist und unabhängig von Backend- und Transportkompontenten funktioniert
- die Rollenverteilung klar ist. Transport-Level-Security schützt den Betrieb. MLS schützt die fachlichen Nachrichteninhalte und deren Absenderbindung.
- Endpunkte auch bei kompromittierten intermediären Plattformen kryptografisch belastbare Aussagen über Nachrichtenursprung und Unverändertheit treffen können

Neutral, weil

- betriebliche Komplexität nicht zwingend steigt, jedoch Implementierungskomplexität in Endpunkten zunimmt. Diese Komplexität kann jedoch durch unterstützenden Artefakte wie bspw. SDKs mitigiert werden.
- weil ergänzende Vertrauensdienste zur Identitätsbindung weiterhin erforderlich bleiben.

6.6 Weitere Informationen

Dieser ADR legt die Sicherheitsanker für Authentizität und Integrität fest und soll damit Fehlinterpretationen wie bspw. „mTLS allein würde für fachliche Authentizität und Integrität genügen" verhindern.

Der ADR trifft keine Aussage dahingehend, dass Transportschutz entbehrlich ist. Vielmehr wird festgelegt, dass Transportschutz und fachliche Ende-zu-Ende-Sicherheitsgarantien

unterschiedliche Sicherheitsfunktionen erfüllen und deshalb getrennt betrachtet werden müssen.

7 ADR-006 Authentizität: Identität öffentlicher Stellen

Sprache: Deutsch
Status: Vorgeschlagen
Datum: 19.03.2026
Entscheidende: Architektur-Workstream
Beratende: FIT-AB, FITKO-AM
Informierte: Lenkungsausschuss, IT-PLR

7.1 Kontext und Problemstellung

Gemäß ADR-005 wird Authentizität und Integrität in der Ende-zu-Ende-Nachrichtenübermittlung durch eine effektive Bindung fachlicher Identitäten an kryptografische Identitäten im Kommunikationskanal erreicht.

Im vorliegenden ADR wird beschrieben, wie sich öffentliche Stellen gegenüber anderen Kommunikationsparteien authentisieren können, um ihre organisatorische Identität kryptographisch an den Ende-zu-Ende-geschützten Kommunikationskanal zu binden.

Durch die in ADR-005 beschriebene Bindung dieser Authentisierung an den Ende-zu-Ende-geschützten Kommunikationskanal weisen öffentliche Stellen gegenüber ihren Kommunikationspartnern die Autorenschaft der von ihnen im Kanal gesendeten Nachrichten nach. Die Vertraulichkeit des Kanals wird dabei durch die E2EE-Schicht hergestellt. Dieser ADR fokussiert sich auf die Identitätsbindung und Authentizität öffentlicher Stellen.

Gegenstand dieses ADR ist die technische Identitätsquelle für öffentliche Stellen als organisatorische Kommunikationsparteien. Die fachliche Berechtigungsprüfung, die vollständige Ausgestaltung des IAM sowie die Authentisierung natürlicher Personen, ist jedoch nicht Gegenstand dieses ADRs. Diese Sachverhalte werden in weiteren ADRs definiert oder zu definieren sein.

7.2 Entscheidungsfaktoren

- ARC_004: Ein Zero-Trust-Ansatz ist durchgängig zu verfolgen, inklusive Identitätsprüfung und Zugriffskontrolle.
- ASD_8.1: Das OSiP-Fachverfahren wird als reguläres, extern angebundenes Fachverfahren behandelt und unterliegt denselben verbindlichen Anschlussbedingungen, Sicherheitsanforderungen, Authentifizierungs-, Autorisierungs- und Kommunikationsmechanismen wie alle übrigen angebundenen Drittsysteme.

- ASD_10: Das System ermöglicht eine klare Abgrenzung der Systemgrenzen und eine saubere Entkopplung zwischen der Transportinfrastruktur und den angebundenen Fachverfahren.
- ASD_246: Das System soll nach dem Zero-Trust-Prinzip arbeiten, d. h. jede Anfrage wird authentifiziert und autorisiert.
- ASD_211: Das System verfügt über ein Identitäts- und Berechtigungsmanagement, das an die Geschäftsprozesse, Organisationsstrukturen sowie an den hohen Schutzbedarf ausgerichtet ist.
- ASD_317: Das System integriert Security by Design mit Nachweisdokumentation in den Entwicklungsprozess.
- ASD_208: Nutzer können die Vertrauenswürdigkeit von Kommunikationspartnern über Schlüsselprüfungen bestätigen.
- ASD_202: Die Zuordnung zwischen Identität und öffentlichem Schlüssel ist überprüfbar und vertrauenswürdig.
- ASD_156: Betreiber des Systems müssen ein gemeinsames Vertrauensmodell definieren (z. B. PKI, Web of Trust).
- ASD_198: Das System setzt eine einheitliche Public-Key-Infrastructure (PKI) als zentralen Vertrauenanker ein.
- ASD_202: Die Zuordnung zwischen Identität und öffentlichem Schlüssel ist überprüfbar und vertrauenswürdig.
- ASD_219: Die IAMs stellen für administrative und sonstige privilegierte und sensible Benutzerkonten eine Authentifizierung auf Vertrauensniveau "hoch" gemäß BSI TR-03107-1 sicher.
- ASD_169: Die Zertifikatsvalidierung erfolgt gemäß aktueller kryptografischer Sicherheitsstandards. Veraltete, schwache oder unsichere Protokolle und Chiffren sind ausgeschlossen.
- ASD_177: Alle Datenübermittlungen unterliegen einer automatisierten Zertifikatsprüfung.
- ASD_178: Das System hält kryptographische Verfahren, Parameter und Cipher Suites austauschbar und führt ein zentrales Krypto-Kataster (Algorithmen, Schlüssellängen, Einsatzorte, Lebenszyklus).
- ASD_179: Das System setzt kryptographische Protokolle, Verschlüsselungsalgorithmen und -Modi nach aktuellem Stand der Technik ein.
- ASD_181: Das System verwendet asymmetrische Verschlüsselung für Schlüsselverteilung (z.B. RSA).

- ASD_183: Das System verwaltet kryptographische Schlüssel über den gesamten Lebenszyklus (Generierung, Distribution, Nutzung, Rotation, Archivierung, Widerruf, Löschung) zentral und revisionssicher.
- ASD_184: Das System unterstützt die Rotation kryptografischer Schlüssel in festgelegten Intervallen und stellt sicher, dass abgelaufene Schlüssel nicht mehr verwendet werden können.
- ASD_190: Es werden ausschließlich starke, öffentlich geprüfte Verschlüsselungs- und Signaturalgorithmen verwendet.
- ASD_192: Das Kryptokonzept unterstützt Verfahren, die nach einer Kompromittierung eine Wiederherstellung der Systems ermöglichen.
- ASD_199: Die verwendeten Zertifikate stammen aus der Verwaltungs-PKI.
- ASD_201: Die Schlüsselverwaltung erfolgt rollengetrennt und revisionssicher.
- ASD_206: Das System verwaltet alle Schlüssel und Passwörter zentral in einem Secrets-Vault (KMS) mit Rotation, Trennung von Code/Config, rollenbasierter Zugriffskontrolle und Protokollierung und verhindert die Ablage in Klartext-Konfigurationsdateien.
- ASD_213: Das IAM der OSiP-Transportinfrastruktur und das OSiP-Fachverfahrens unterstützen föderale Authentifizierungs- und Autorisierungsverfahren.
- ASD_226: Passwort- und Authentifizierungsverfahren (Basic Auth, SSO und Zertifikate) erfüllen aktuelle Sicherheitsstandards.
- ASD_247: Die IAMs stellen für Maschinen und APIs eine zertifikatsbasierte Authentifizierung bereit.
- ASD_250: Das System übermittelt die Informationen nur an zugelassene Fachverfahren, Mandanten und Unternehmensanwendungen.

Zusätzlich sind für diese Entscheidung folgende architektonische Kriterien relevant:

- Nicht-interaktive und automatisierbare Authentisierung für System-zu-System-Kommunikation
- Direkte kryptographische Bindbarkeit der Organisationsidentität an den Ende-zu-Ende-geschützten Kommunikationskanal
- Möglichst geringe Abhängigkeit von einer zentralen, laufzeitkritischen Identitätsvermittlungsinstanz
- Klare organisatorische Abgrenzung des Teilnehmerkreises öffentlicher Stellen

7.3 Betrachtete Optionen

- Option 1: Identifikation mittels X.509-Zertifikaten aus der Verwaltungs-PKI (V-PKI)

- Option 2: Identifikation mittels X.509-Zertifikaten aus einer öffentlichen PKI
- Option 3: Identifikation mittels Organisationskonto gemäß § 3 OZG
- Option 4: Identifikation mittels European Digital Identity Wallet (EUDI-Wallet)

7.4 Entscheidung

Es wurde die Option „Option 1: Identifikation mittels X.509-Zertifikaten aus der Verwaltungs-PKI (V-PKI)" gewählt, denn diese Option realisiert den Zero-Trust-Ansatz sowie die automatisierte Authentisierung öffentlicher Stellen, für die nicht-interaktive organisatorische Identitätsbindung an den Ende-zu-Ende-geschützten Kommunikationskanal.

Gegenüber Option 2 weist die V-PKI eine bewusste und im vorliegenden Anwendungsfall gewünschte Beschränkung des Nutzendenkreises auf, auch wenn sie funktional nicht alle Eigenschaften moderner öffentlicher PKI-Ökosysteme bereitstellt.

Option 1 ist gegenüber Option 3 zu bevorzugen, da das zertifikatsbasierte Design der V-PKI ggü. dem Organisationskonto als zentraler Vermittlungsplattform für Identifikationsvorgänge die Realisierung des Zero-Trust-Ansatzes ermöglicht und insbesondere für automatisierte, asynchrone Systemkommunikation besser geeignet ist.

Option 4 (Identifikation mittels EUDI-Wallet) kann perspektivisch realisiert werden, sofern die Voraussetzungen zum Einsatz der EUDI-Wallet für Organisationen vorliegen und diese für öffentliche Stellen nutzbar werden.

Die Entscheidung für die V-PKI legt dabei ausschließlich die technische Quelle der organisatorischen Authentisierung fest. Die fachliche Berechtigungsprüfung und die Zuordnung von Rollen, Zuständigkeiten und Mandatsbeziehungen erfolgen weiterhin über Governance-, Onboarding- und IAM-/Trust-Register-Prozesse.

7.4.1 Konsequenzen

Gut, weil

- eine nicht-interaktive, vollautomatisierte Authentisierung öffentlicher Stellen möglich ist und sich daher auch für System-zu-System-Kommunikation eignet.
- die Organisationsidentität direkt kryptografisch an den Ende-zu-Ende-verschlüsselten Kommunikationskanal gebunden werden kann und keine laufende Abhängigkeit von einer zentralen Identitätsvermittlungsinstanz besteht.
- der Teilnehmendenkreis bewusst auf öffentliche Stellen beschränkt ist und damit eine klare Abgrenzung gegenüber privaten Organisationen und Dritten erfolgt.

- bestehende Verwaltungsstrukturen und etablierte Vertrauensannahmen genutzt werden können, ohne neue zentrale Identitätsdienste einzuführen.

Neutral, weil

- die V-PKI die Organisationsidentität attestiert, deren fachliche Bedeutung jedoch erst im Kontext des Systems entsteht.
- die Entscheidung für die V-PKI zukünftige Ergänzungen durch alternative Identifikationsmechanismen nicht ausschließt. Sie setzt jedoch voraus, dass diese in das bestehende Governance- und IAM-Modell integrierbar sind und keine zusätzliche zentrale Abhängigkeit im Authentisierungsvorgang erzeugen.
- die beteiligten öffentlichen Stellen einen aufwendigen Zertifizierungsprozess durchlaufen müssen.

Schlecht, weil

- die V-PKI derzeit keine modernen PKI-Funktionalitäten wie automatisierte Zertifikatserneuerung, kurze Zertifikatslaufzeiten oder flächendeckende Transparenzmechanismen unterstützt.

Zusätzlich sind gemäß dieser Entscheidung folgende architektonischen Konsequenzen relevant:

- Die Wahl der V-PKI setzt voraus, dass die Definition und Zulassung öffentlicher Stellen weiterhin durch vorgelagerte Governance- und Onboarding-Prozesse erfolgt und systemintern im IAM/Trust Register abgebildet wird. Die PKI dient ausschließlich der technischen Authentisierung, nicht der fachlichen Berechtigungsentscheidung.
- Das Lebenszyklus-Management von Zertifikaten erfordert klare Zuständigkeiten für Ausstellung, Widerruf und Sperrung, insbesondere bei Sicherheitsvorfällen oder organisatorischen Änderungen von Behörden. Diese Verantwortung besteht unabhängig vom gewählten Identifikationsmittel und ist betrieblich abzusichern.

7.5 Vor- und Nachteile der Optionen

7.5.1 Option 1: Identifikation mittels X.509-Zertifikaten aus der Verwaltungs-PKI (V-PKI)

Zur Herstellung von Authentizität auf Ende-zu-Ende Verschlüsselungsebene können sich öffentliche Stellen mit Hilfe eines Zertifikats aus der V-PKI gegenüber einem anderen Kommunikationsteilnehmenden identifizieren. Dieses Verfahren erlaubt ein hohes Maß an Sicherheit und Vertraulichkeit auf dem Vertrauensniveau der V-PKI.

Die Identitätsdaten öffentlicher Stellen weisen anders als bei Identitätsdaten von Privatpersonen kein besonderes Schutzniveau hinsichtlich des Schutzziels der Vertraulichkeit auf. Daher ist das Abfragen der Identität öffentlicher Stellen zur Authentisierung eines Kommunikationskanals für alle Teilnehmenden möglich. Die Authentisierung des Kommunikationskanals durch ein IT-System der jeweiligen Fachbehörde kann damit ohne die Erforderlichkeit einer Nutzendeninteraktion automatisch und auch im Hintergrund durchgeführt werden.

Um eine effektive Authentisierung des Ende-zu-Ende-verschlüsselten Kanals zu erreichen, muss das im genutzten X.509-Zertifikat hinterlegte Schlüsselmaterial mit Hilfe der von der Ende-zu-Ende-Verschlüsselungsschicht bereitgestellten Funktionen an den kryptographischen Kanal gebunden werden und die im Zertifikat enthaltenen Identitätsdaten der Kommunikationspartei dargestellt werden, gegenüber der sich die öffentliche Stelle authentisiert.

Zusätzlich muss zwingend die Gültigkeit des Zertifikats inkl. Prüfung des Zertifikatspfad und des Revokationsstatus geprüft werden.

Es wird angenommen, dass alle öffentlichen Stellen einen praktikablen Zugang zur V-PKI besitzen und dort Zertifikate beantragen können.

Gut, weil

- X.509-Zertifikate einen sehr verbreiteten und sehr etablierten Mechanismus zur Authentisierung darstellen.
- der Einsatz von X.509-Zertifikaten auch nicht-interaktiv, d.h. ohne Nutzendeninteraktionen auf Seiten der öffentlichen Stelle, möglich ist.
- der Einsatz von X.509-Zertifikaten ohne Abhängigkeiten zu einem zentralen IDP wie dem Organisationskonto auskommt und somit grundsätzlich auch eingeschränkt offline möglich wäre.
- die Beschränkung auf Zertifikate aus der V-PKI die organisatorische Eingrenzung auf öffentliche Stellen technisch unterstützt.

Neutral, weil

- für die fachliche Einordnung der authentisierten Stelle ergänzende Register- bzw. IAM-Informationen erforderlich bleiben.

Schlecht, weil

- die V-PKI moderne Funktionalitäten wie eine automatische Zertifikatserneuerung mittels ACME oder Transparency Logs nicht unterstützt.
- es innerhalb der V-PKI derzeit keinen Mechanismus gibt, um spezifische Attribute öffentlicher Stellen wie bspw. maschinenlesbare Organisations-IDs oder Behördentypen gesichert in Zertifikaten zu hinterlegen.
- der Prozess zur Beantragung von Zertifikaten mitunter aufwändig sein kann.
- die Beantragung von Zertifikaten aus der V-PKI für öffentliche Stellen kostenpflichtig ist, was zusätzliche organisatorische Hürden mit sich bringt und zu einer geringeren Akzeptanz führen könnte.

7.5.2 Option 2: Identifikation mittels X.509-Zertifikaten aus einer öffentlichen PKI

Analog zur Nutzung der V-PKI könnte auch eine öffentliche, d.h. nicht auf öffentliche Stellen beschränkte PKI-Infrastruktur genutzt werden. Bestehende privatwirtschaftlich organisierte PKIs bieten moderne Funktionalitäten wie automatische Zertifikatserneuerung mittels ACME, Transparency Logs oder die Möglichkeit zur Hinterlegung gesicherter Attribute in Zertifikaten.

Privatpersonen und private Organisationen müssen bei der Kommunikation mit öffentlichen Stellen anhand der genutzten Zertifikate jederzeit zweifelsfrei feststellen können, dass sie gerade mit einer offiziellen Behörde kommunizieren, deren Identität sie zweifelsfrei prüfen können. Hierbei sind zusätzliche Maßnahmen nötig, um den Teilnehmendenkreis auf eindeutig identifizierte öffentliche Stellen zu beschränken und damit eine missbräuchliche Nutzung zu vermeiden. Denkbar wären beispielsweise Vorgaben zur Hinterlegung spezifischer gesicherter Attribute in Zertifikaten, insb. Organisations-ID sowie ein Nachweis der Prüfung, dass es sich um eine offizielle öffentliche Stelle handelt.

Gut, weil

- X.509-Zertifikate einen sehr verbreiteten und sehr etablierten Mechanismus zur Authentisierung darstellen.
- der Einsatz von X.509-Zertifikaten auch nicht-interaktiv, d.h. ohne Nutzendeninteraktionen auf Seiten der öffentlichen Stellen, möglich ist.
- X.509-Zertifikate eingeschränkt auch offline und ohne aktive Kommunikationsverbindung zu einem zentral betriebenen IDP genutzt werden können.
- moderne Funktionalitäten wie automatische Zertifikatserneuerung mittels ACME oder Transparency Logs unterstützt werden können.
- auch private Organisationen Zertifikate erhalten können.

Neutral, weil

- ein entscheidender Sicherheitsfaktor auf den Betreiber der öffentlichen PKI gelegt wird. Es erfordert einen klaren Entscheidungsprozess, um die Auswahl einer vertrauenswürdigen öffentlichen PKI zu gewährleisten.
- die Definition öffentlicher Stellen im Rahmen eines vorgelagerten Governance-Prozesses abgebildet werden muss und die Berechtigung über das zentrale IAM erfolgen muss.

Schlecht, weil

- eine öffentliche PKI den Teilnehmerkreis nicht inhärent auf öffentliche Stellen beschränkt und deshalb zusätzliche Governance-, Prüf- und Nachweismechanismen erforderlich wären, um die Eigenschaft „öffentliche Stelle" belastbar festzustellen.
- Produkt-, Policy- und Preismodelländerungen eines externen PKI-Anbieters schwerer steuerbar sein können.

7.5.3 Option 3: Identifikation mittels Organisationskonto gemäß § 3 OZG

Zur Herstellung von Authentizität auf Ende-zu-Ende Verschlüsselungsebene können sich öffentliche Stellen mit einem Organisationskonto gegenüber einem anderen Kommunikationsteilnehmenden identifizieren. Dieses Verfahren erlaubt Sicherheit und Vertraulichkeit auf dem Vertrauensniveaus „substantiell".

Zur Authentisierung wird ein von der Organisationskonto-Infrastruktur ausgestelltes (SAML-) Token vertraulich im Kontext des Ende-zu-Ende verschlüsselten Kommunikationskanals übermittelt und durch einen anderen Kommunikationsteilnehmenden geprüft. Entsprechend ist für die Prüfung eine Vertrauensstellung gegenüber dem Organisationskonto-Server erforderlich. Dies macht das Organisationskonto jedoch für die hier betrachtete nicht-interaktive, kryptographisch an den Kommunikationskanal gebundene Authentisierung organisationaler Kommunikationsparteien ungeeignet. Um eine kryptografisch sichere Bindung zu erreichen, muss der (SAML-) Token auf den betreffenden Kommunikationskanal limitiert sein.

Neutral, weil

- alle öffentlichen Stellen gemäß § 3 OZG zur Nutzung des Organisationskontos verpflichtet sind, die von OSIP abgebildeten Geschäftsprozesse derzeit jedoch keinen OZG-Leistungen entsprechen.

Schlecht, weil

- die Nutzung des Organisationskontos zwingend eine Nutzendeninteraktion auf Seiten der öffentlichen Stelle für jeden Authentisierungsvorgang erfordert, da es keine nicht-interaktive Authentisierung für den automatisierten Nachrichtenaustausch mit der zentralen Transportinfrastruktur gibt.
- Kommunikationsparteien auf die korrekte Authentifizierung durch die Organisationskonto-Infrastruktur vertrauen müssen und dieses Modell keinen geeigneten E2E-Identitätsanker für asynchrone, automatisierte Systemkommunikation darstellt.
- die Funktionsfähigkeit des Systems direkt an die korrekte Funktion des Organisationskontos geknüpft ist, womit bei Ausfall des Organisationskontos keine Möglichkeit zur Authentifizierung mehr besteht.
- anhand des temporären (SAML-) Tokens vom Empfänger die Identität des Absenders nicht dauerhaft kryptographisch kanalgebunden geprüft werden kann und kein alternatives kryptographisches Material gestellt wird.

Diese Option widerspricht insbesondere der Entscheidung in ADR-005 und wurde hier aus Gründen der Vollständigkeit und Transparenz aufgeführt.

7.5.4 Option 4: Identifikation mittels European Digital Identity Wallet (EUDI-Wallet)

Perspektivisch sollen sich öffentliche Stellen zur Herstellung von Authentizität auf Ende-zu-Ende Verschlüsselungsebene direkt mit einem entsprechenden Nachweis aus der European Digital Identity Wallet gegenüber einem anderen Kommunikationsteilnehmenden identifizieren können. Dieses Verfahren erlaubt zukünftig ein hohes Maß an Sicherheit und Vertraulichkeit.

Gut, weil

- mit der EUDI-Wallet perspektivisch ein hohes Sicherheitsniveau im Sinne einer Zero-Trust-Architektur erreicht werden kann.
- die EUDI-Wallet zukunftssicher, einfach nutzbar und in Europa interoperabel gestaltet ist.

Schlecht, weil

- die EUDI-Wallet für diesen Anwendungsfall derzeit noch nicht verfügbar ist.
- von Empfängern die Identität des Absenders nicht geprüft werden kann, da kein kryptographisches Material gestellt wird.

- nicht klar ist, ob öffentliche Stellen eine Identität innerhalb der EUDI-Wallet erhalten.
- die Befähigung für nicht-interaktive, asynchrone System-zu-System-Kommunikation organisatorischer Kommunikationsparteien derzeit nicht hinreichend geklärt ist[16].

[16] https://digital-strategy.ec.europa.eu/en/policies/business-wallets

8 ADR-007 Authentizität: Identität privater Organisationen

Sprache: Deutsch
Status: Vorgeschlagen
Datum: 19.03.2026
Entscheidende: Architektur-Workstream
Beratende: FIT-AB, FITKO-AM
Informierte: IT-PLR, Lenkungsausschuss

8.1 Kontext und Problemstellung

Gemäß ADR-005 wird Authentizität und Integrität in der Ende-zu-Ende-Nachrichtenübermittlung durch eine effektive Bindung fachlicher Identitäten an kryptografische Identitäten im Kommunikationskanal erreicht.

Im vorliegenden ADR wird beschrieben, wie sich private Organisationen gegenüber anderen Kommunikationsparteien authentisieren können. Dabei gelten grundsätzlich die gleichen Entscheidungsfaktoren wie in ADR-006, allerdings steht die V-PKI nicht als Option zu Verfügung, da sie keine Zertifikate an private Organisationen ausstellt.

Durch die in ADR-005 beschriebene Bindung der Authentisierung an den Ende-zu-Ende-geschützten Kommunikationskanal weisen private Organisationen die Autorenschaft der von ihnen im Kanal gesendeten Nachrichten gegenüber anderen Kommunikationsparteien nach. Die Vertraulichkeit des Kanals wird dabei durch die E2EE-Schicht hergestellt. Dieser ADR fokussiert sich auf die Identitätsbindung und Authentizität privater Organisationen.

Gegenstand dieses ADR ist die technische Identitätsquelle für private Organisationen als organisatorische Kommunikationsparteien. Die fachliche Berechtigungsprüfung, die vollständige Ausgestaltung des IAM sowie die Authentisierung natürlicher Personen sind jedoch nicht Gegenstand dieses ADRs. Diese Sachverhalte werden in weiteren ADRs definiert oder noch zu definieren sein.

8.2 Entscheidungsfaktoren

Die nachfolgenden Entscheidungsfaktoren orientieren sich an ADR-006. Anforderungen, die exklusiv auf die Verwaltungs-PKI verweisen, werden für private Organisationen nicht übernommen.

- ARC_004: Ein Zero-Trust-Ansatz ist durchgängig zu verfolgen, inklusive Identitätsprüfung und Zugriffskontrolle.

- ARC_075: Das System soll nach dem Zero-Trust-Prinzip arbeiten, d. h. jede Anfrage wird authentifiziert und autorisiert.
- ASD_211: Das System verfügt über ein Identitäts- und Berechtigungsmanagement, das an die Geschäftsprozesse, Organisationsstrukturen sowie an den hohen Schutzbedarf ausgerichtet ist.
- ASD_317: Das System integriert Security by Design mit Nachweisdokumentation in den Entwicklungsprozess.
- ASD_208: Nutzer können die Vertrauenswürdigkeit von Kommunikationspartnern über Schlüsselprüfungen bestätigen.
- ASD_202: Die Zuordnung zwischen Identität und öffentlichem Schlüssel ist überprüfbar und vertrauenswürdig.
- ASD_156: Betreiber des Systems müssen ein gemeinsames Vertrauensmodell definieren (z. B. PKI, Web of Trust).
- ASD_198: Das System setzt eine einheitliche Public-Key-Infrastructure (PKI) als zentralen Vertrauensanker ein.
- ASD_202: Die Zuordnung zwischen Identität und öffentlichem Schlüssel ist überprüfbar und vertrauenswürdig.
- ASD_219: Die IAMs stellen für administrative und sonstige privilegierte und sensible Benutzerkonten eine Authentifizierung auf Vertrauensniveau "hoch" gemäß BSI TR-03107-1 sicher.
- ASD_169: Die Zertifikatsvalidierung erfolgt gemäß aktuellem kryptografischem Sicherheitsstandard. Veraltete, schwache oder unsichere Protokolle und Chiffren sind ausgeschlossen.
- ASD_177: Alle Datenübermittlungen unterliegen einer automatisierten Zertifikatsprüfung.
- ASD_178: Das System hält kryptographische Verfahren, Parameter und Cipher Suites austauschbar und führt ein zentrales Krypto-Kataster (Algorithmen, Schlüssellängen, Einsatzorte, Lebenszyklus).
- ASD_179: Das System setzt kryptographische Protokolle, Verschlüsselungsalgorithmen und -Modi nach aktuellem Stand der Technik ein.
- ASD_181: Das System verwendet asymmetrische Verschlüsselung für Schlüsselverteilung (z.B. RSA).
- ASD_183: Das System verwaltet kryptographische Schlüssel über den gesamten Lebenszyklus (Generierung, Distribution, Nutzung, Rotation, Archivierung, Widerruf, Löschung) zentral und revisionssicher.

- ASD_184: Das System unterstützt die Rotation kryptografischer Schlüssel in festgelegten Intervallen und stellt sicher, dass abgelaufene Schlüssel nicht mehr verwendet werden können.
- ASD_190: Es werden ausschließlich starke, öffentlich geprüfte Verschlüsselungs- und Signaturalgorithmen verwendet.
- ASD_192: Das Kryptokonzept unterstützt Verfahren, die nach einer Kompromittierung eine Wiederherstellung der Systems ermöglichen.
- ASD_201: Die Schlüsselverwaltung erfolgt rollengetrennt und revisionssicher.
- ASD_206: Das System verwaltet alle Schlüssel und Passwörter zentral in einem Secrets-Vault (KMS) mit Rotation, Trennung von Code/Config, rollenbasierter Zugriffskontrolle und Protokollierung und verhindert die Ablage in Klartext-Konfigurationsdateien.
- ASD_213: Das IAM der OSiP-Transportinfrastruktur und das OSiP-Fachverfahrens unterstützen föderale Authentifizierungs- und Autorisierungsverfahren.
- ASD_226: Passwort- und Authentifizierungsverfahren (Basic Auth, SSO und Zertifikate) erfüllen aktuelle Sicherheitsstandards.
- ASD_247: Die IAMs stellen für Maschinen und APIs eine zertifikatsbasierte Authentifizierung bereit.

Zusätzlich sind für diese Entscheidung folgende arcitektonische Kriterien relevant:

- Nicht-interaktive und automatisierbare Authentisierung für System-zu-System-Kommunikation
- Direkte kryptographische Bindbarkeit der Organisationsidentität an den Ende-zu-Ende-geschützten Kommunikationskanal
- Möglichst geringe Abhängigkeit von einer zentralen, laufzeitkritischen Identitätsvermittlungsinstanz
- Ergänzbare Einbindung in ein zentrales IAM bzw. Trust Register für fachliche Rollen- und Berechtigungszuordnung

8.3 Betrachtete Optionen

- Option 1: Identifikation mittels X.509-Zertifikaten aus einer öffentlichen PKI
- Option 2: Identifikation mittels Organisationskonto gemäß § 3 OZG
- Option 3: Identifikation mittels European Digital Identity Wallet (EUDI-Wallet)
- Option 4: Identifikation über OIDC

8.4 Entscheidung

Gewählte Option: "Option 1: Identifikation mittels X.509-Zertifikaten aus einer öffentlichen PKI", denn diese Option stellt eine organisationsbezogene Authentizität mit hoher Aussagekraft unmittelbar im kryptographischen Kommunikationsbeweis sicher.

Die Identität der privaten Organisation ist dabei an das verwendete Zertifikat gebunden und für alle Kommunikationsteilnehmenden dezentral prüfbar, sofern die zugrunde liegende PKI, die Zertifikatsprüfung und der vorgelagerte Governance- und Onboarding-Prozess als vertrauenswürdig ausgestaltet sind.

Auch unter der Annahme eines gegenüber öffentlichen Stellen reduzierten Schutzbedarfs überwiegen die Vorteile einer dezentral überprüfbaren Organisationsidentität. Insbesondere die klare Nachweisbarkeit der Autorenschaft, die Unabhängigkeit von zentralen Autorisierungsinstanzen sowie die Möglichkeit einer revisionssicheren externen Beweisführung sprechen für diese Option.

Option 4 wurde trotz geringerer Einstiegshürden nicht gewählt, da sie die organisationsbezogene Authentizität nur vermittelt über eine zentrale Vertrauensinstanz herstellt und damit bewusst auf eine kryptografisch nachweisbare Organisationsautorenschaft verzichtet. Diese Einschränkung wird im vorliegenden Kontext als nicht ausreichend tragfähig bewertet, insbesondere im Hinblick auf langfristige Nachvollziehbarkeit und Haftungsfragen.

Option 2 und Option 3 werden nicht gewählt, da sie entweder primär auf Zugangsvermittlung statt auf kryptografische Organisationsidentität ausgelegt sind oder derzeit noch keine hinreichend belastbare Grundlage für organisationsbezogene, automatisierte Kommunikation im vorliegenden Anwendungsfall bieten.

Mit der Wahl von Option 1 wird ein konsistentes, robustes und langfristig tragfähiges Identitätskonzept umgesetzt, das sich nahtlos in die bestehenden Architekturentscheidungen und den Zero-Trust-Ansatz einfügt.

Die Entscheidung legt dabei ausschließlich die technische Identitätsquelle für private Organisationen fest. Die fachliche Berechtigungsprüfung und die Zuordnung zu Rollen, Zuständigkeiten und Mandatsbeziehungen erfolgen weiterhin über Governance-, Onboarding- und IAM-/Trust-Register-Prozesse.

8.4.1 Konsequenzen

Gut, weil

- eine nicht-interaktive, vollautomatisierte Authentisierung privater Organisationen möglich ist und sich daher auch für System-zu-System-Kommunikation eignet.
- die Organisationsidentität direkt kryptografisch an den Ende-zu-Ende-verschlüsselten Kommunikationskanal gebunden werden kann und keine laufende Abhängigkeit von einer zentralen Identitätsvermittlungsinstanz besteht.
- ein zu ADR-006 konsistentes, zertifikatsbasiertes Identitätsmodell für organisationale Kommunikationsparteien entsteht.
- das Identitätsmodell konsistent zu den bestehenden Architekturentscheidungen und Zero Trust bleibt.
- revisionssichere und externe Nachweisbarkeit der Urheberschaft auch langfristig gewährleistet ist.

Neutral, weil

- die Entscheidung für die PKI zukünftige Ergänzungen durch alternative Identifikationsmechanismen nicht ausschließt. Sie setzt jedoch voraus, dass diese in das bestehende Governance- und IAM-Modell integrierbar sind und keine zusätzliche zentrale Abhängigkeit im Authentisierungsvorgang erzeugen.
- der reduzierte Schutzbedarf privater Organisationen nicht zu einer Reduktion der technischen Anforderungen an die Identitätsprüfung führt, sondern bewusst ein höheres Sicherheitsniveau beibehalten wird.

Schlecht, weil

- private Organisationen eigene kryptografische Schlüssel verwalten und Zertifikatsprozesse durchlaufen müssen, was insbesondere für kleinere Organisationen einen erhöhten initialen Aufwand bedeutet.

Zusätzlich sind gemäß dieser Entscheidung folgende architektonischen Konsequenzen relevant:

- Die Wahl setzt voraus, dass die Definition und Zulassung privater Organisationen weiterhin durch vorgelagerte Governance- und Onboarding-Prozesse erfolgt und systemintern im IAM/Trust Register abgebildet wird. Die PKI dient ausschließlich der technischen Authentisierung, nicht der fachlichen Berechtigungsentscheidung.

- Das Lebenszyklus-Management von Zertifikaten erfordert klare Zuständigkeiten für Ausstellung, Widerruf und Sperrung, insbesondere bei Sicherheitsvorfällen oder organisatorischen Änderungen von privaten Organisationen. Diese Verantwortung besteht unabhängig vom gewählten Identifikationsmittel und ist betrieblich abzusichern.

8.5 Vor- und Nachteile der Optionen

8.5.1 Option 1: Identifikation mittels X.509-Zertifikaten aus einer öffentlichen PKI

Zur Herstellung von Authentizität auf Ende-zu-Ende Verschlüsselungsebene können sich private Organisationen mit Hilfe eines Zertifikats aus einer PKI gegenüber einem anderen Kommunikationsteilnehmenden identifizieren. Dieses Verfahren erlaubt ein hohes Maß an Sicherheit und Vertraulichkeit auf dem Vertrauensniveau der genutzten PKI. Bestehende privatwirtschaftlich organisierte PKIs bieten moderne Funktionalitäten wie automatische Zertifikatserneuerung mittels ACME, Transparency Logs oder die Möglichkeit zur Hinterlegung gesicherter Attribute in Zertifikaten.
Gut, weil

- X.509-Zertifikate einen sehr verbreiteten und sehr etablierten Mechanismus zur Authentisierung darstellen.
- der Einsatz von X.509-Zertifikaten auch nicht-interaktiv (d. h. ohne Nutzendeninteraktion auf Seiten der privaten Organisation) möglich ist.
- X.509-Zertifikate (eingeschränkt) auch offline und ohne aktive Kommunikationsverbindung zu einem zentral betriebenen IDP genutzt werden können.
- moderne Funktionalitäten wie automatische Zertifikatserneuerung mittels ACME oder Transparency Logs unterstützt werden können.

Neutral, weil

- ein entscheidender Sicherheitsfaktor auf den Betreiber der öffentlichen PKI gelegt wird. Es erfordert einen klaren Entscheidungsprozess, um die Auswahl einer vertrauenswürdigen öffentlichen PKI zu gewährleisten.
- die Aussagekraft der organisationsbezogenen Identität zusätzlich von der Qualität der vorgelagerten Identitätsprüfung und des Onboardings abhängt.

Schlecht, weil

- Produkt-, Policy- und Preismodelländerungen eines öffentlichen PKI-Anbieters schwerer steuerbar sein können.

8.5.2 Option 2: Identifikation mittels Organisationskonto gemäß § 3 OZG

Zur Herstellung von Authentizität auf Ende-zu-Ende Verschlüsselungsebene können sich private Organisationen mit einem Organisationskonto gegenüber einem anderen Kommunikationsteilnehmenden identifizieren. Dieses Verfahren erlaubt Sicherheit und Vertraulichkeit auf dem Vertrauensniveau „substantiell".

Zur Authentisierung wird ein von der Organisationskonto-Infrastruktur ausgestelltes (SAML-) Token vertraulich im Kontext des Ende-zu-Ende verschlüsselten Kommunikationskanals übermittelt und durch einen anderen Kommunikationsteilnehmenden geprüft. Entsprechend ist für die Prüfung eine Vertrauensstellung gegenüber dem Organisationskonto-Server erforderlich. Dies macht das Organisationskonto jedoch für die hier betrachtete nicht-interaktive, kryptographisch an den Kommunikationskanal gebundene Authentisierung organisationaler Kommunikationsparteien ungeeignet. Um eine kryptografisch sichere Bindung zu erreichen, muss der (SAML-) Token auf den betreffenden Kommunikationskanal limitiert sein.

Gut, weil

- viele private Organisationen das Organisationskonto bereits zur digitalen Beantragung von Verwaltungsleistungen nutzen.

Schlecht, weil

- die Nutzung des Organisationskontos für den hier betrachteten automatisierten Nachrichtenaustausch eine Nutzendeninteraktion oder eine davon abgeleitete, zentral vermittelte Authentisierung voraussetzt, da es keine nicht-interaktive Authentisierung für den automatisierten Nachrichtenaustausch mit der zentralen Transportinfrastruktur gibt.
- Kommunikationsparteien auf die korrekte Authentifizierung durch die Organisationskonto-Infrastruktur vertrauen müssen und dieses Modell keinen geeigneten E2E-Identitätsanker für asynchrone, automatisierte Systemkommunikation darstellt.
- die Funktionsfähigkeit des Systems direkt an die korrekte Funktion des Organisationskontos geknüpft ist, womit bei Ausfall des Organisationskontos keine Möglichkeit zur Authentifizierung mehr besteht.

- anhand des temporären (SAML-) Tokens vom Empfänger die Identität des Absenders nicht dauerhaft kryptographisch kanalgebunden geprüft werden kann und kein alternatives kryptographisches Material gestellt wird.

Diese Option widerspricht insbesondere der Entscheidung in ADR-005 und wurde hier aus Gründen der Vollständigkeit und Transparenz aufgeführt.

8.5.3 Option 3: Identifikation mittels European Digital Identity Wallet (EUDI-Wallet)

Perspektivisch sollen sich private Organisationen zur Herstellung von Authentizität auf Ende-zu-Ende Verschlüsselungsebene direkt mit einem entsprechenden Nachweis aus der European Digital Identity Wallet gegenüber einem anderen Kommunikationsteilnehmenden identifizieren können. Dieses Verfahren erlaubt zukünftig ein hohes Maß an Sicherheit und Vertraulichkeit.

Gut, weil

- mit der EUDI-Wallet perspektivisch ein hohes Sicherheitsniveau im Sinne einer Zero-Trust-Architektur erreicht werden kann.
- die EUDI-Wallet zukunftssicher, einfach nutzbar und in Europa interoperabel gestaltet ist.

Schlecht, weil

- die EUDI-Wallet für diesen Anwendungsfall derzeit noch nicht verfügbar ist.
- von Empfängern die Identität des Absenders nicht geprüft werden kann, da kein kryptographisches Material gestellt wird.
- die Befähigung für nicht-interaktive, asynchrone System-zu-System-Kommunikation organisatorischer Kommunikationsparteien derzeit nicht hinreichend geklärt ist[17].

8.5.4 Option 4: Identifikation über OIDC

Diese Option basiert auf der Annahme, dass für private Organisationen ein geringerer Schutzbedarf besteht als für öffentliche Stellen, da sie ausschließlich Anträge stellen und Verfahrensentscheidungen empfangen sowie keinen Zugriff auf als VS eingestufte Informationen haben.

Unter dieser Annahme verfügt jede Organisation über einen eigenen registrierten Klienten, der eindeutig der jeweiligen Organisation zugeordnet ist.

[17] https://digital-strategy.ec.europa.eu/en/policies/business-wallets

Die Authentisierung erfolgt gegenüber einem zentralen Authentifizierungsserver, der typischerweise Bestandteil einer IAM-Lösung ist oder an diese angebunden ist. Die Organisation weist den Besitz der dem Klienten zugeordneten Zugangsdaten oder kryptografischen Schlüssel nach und erhält ein signiertes Zugriffs-Token.

Diese Option verzichtet somit bewusst auf eine organisationsbezogene Ende-zu-Ende-Authentizität auf Nachrichtenebene zugunsten geringerer organisatorischer und technischer Einstiegshürden, auch wenn die Übermittlung sich in das E2EE-Konzept eingliedert. Die Bindung des kryptografischen Identitätsmaterials des organisationsbezogenen Clients an die jeweilige Organisation erfolgt im Rahmen des zentralen Onboardings und der Identitätsverwaltung, typischerweise innerhalb des IAM oder einer angebundenen Registrierungsinstanz.

Gut, weil

- die Einstiegshürden für private Organisationen geringer sind, da keine Zertifikatsprozesse durchlaufen werden müssen.
- die Authentisierung auf etablierten und verbreitete Standards wie OAuth 2.0 und OpenID Connect basiert.
- die organisationsbezogene Identifikation ausreichend ist, um Anträge eindeutig einer Organisation zuzuordnen, sofern keine organisationsbezogene Ende zu Ende Autorenschaft auf Nachrichtenebene erforderlich ist.
- die Vertraulichkeit der fachlichen Inhalte unabhängig von der Identifikationsmethode weiterhin durch Einbindung in das Ende-zu-Ende-Verschlüsselungskonzept sichergestellt werden kann.

Neutral, weil

- der organisatorische und technische Aufwand nicht entfällt, sondern in den zentralen Betrieb des IAM und des Autorisierungsservers verlagert wird.
- die Aussagekraft der Organisationsidentität maßgeblich von der Qualität der Onboarding und Governance Prozesse abhängt und weniger von kryptografischen Eigenschaften.
- die Nachvollziehbarkeit der Autorenschaft primär über zentrale Protokollierung und nicht über kryptografische Beweise erfolgt.

Schlecht, weil

- keine organisationsbezogene Ende-zu-Ende-Authentizität auf Nachrichtenebene erreicht wird und die Autorenschaft der Organisation nur mittelbar über den Authentifikationsserver nachgewiesen werden kann.
- eine zentrale Vertrauensinstanz entsteht, deren Fehlkonfiguration, Ausfall oder Kompromittierung unmittelbare Auswirkungen auf alle angebundenen privaten Organisationen haben kann.
- die externe und revisionssichere Nachweisbarkeit der Urheberschaft gegenüber Dritten eingeschränkt ist, da die Identitätsbindung nicht Bestandteil des kryptografischen Kommunikationsbeweises ist.
- Empfänger die Organisationsidentität nicht unmittelbar aus einem organisationsbezogenen, dezentral prüfbaren kryptographischen Nachweis ableiten können, sondern auf zentrale Token- und Registrierungslogik angewiesen bleiben.

Diese Option widerspricht insbesondere der Entscheidung in ADR-005 und wurde hier aus Gründen der Vollständigkeit und Transparenz aufgeführt.

9 ADR-008 Hilfsmodule zur vereinfachten Anbindung von Fachverfahren

Status: Vorgeschlagen
Datum: 2026-03-19
Entscheidungsträger: Architektur-Workstream
Beratende: Fachvertreter:innen EKS und Genehmigungsbehörden
Informiert: IT-PLR, Lenkungsausschuss

9.1 Kontext und Problemstellung

Dieser ADR erörtert und regelt, ob und inwiefern Hilfsmodule für die Anbindung an die Kommunikationsinfrastruktur als zentral bereitgestellter Baustein entwickelt und angeboten werden, insbesondere die Bereitstellung von Werkzeugen und Bibliotheken in der Form von integrierten und integrierbaren Software Development Kits (SDK).

Mit Blick auf die Kommunikationsinfrastruktur könnten SDKs zentrale Funktionen für die Anbindung kapseln, insbesondere die Umsetzung der Ende-zu-Ende-Verschlüsselung inklusive Schlüsselverwaltung, die Adressierung von Kommunikationsparteien, die Validierung von Identitäten, eine konsistente Fehlerbehandlung sowie die korrekte Nutzung der standardisierten Schnittstellen.

Dieser ADR regelt nicht, für welche Programmiersprachen und Umgebungen Hilfsmodule wie SDKs zur Verfügung gestellt werden. Dieser ADR regelt zudem nicht, welchen konkreten Funktionsumfang etwaige bereitgestellte Hilfsmodule abbilden sollen.

Im Rahmen dieses ADRs wird über Hilfsmodule zur vereinfachten Anbindung von Fachverfahren an die Transportinfrastruktur entschieden. Adressaten dieser Hilfsmodule sind insbesondere die Entwicklungsteams von Fachverfahren der Antragserfassungsstellen, der Genehmigungsbehörden und der Erkenntnisstellen.

SDKs sind dabei als unterstützende Integrationsartefakte zu verstehen. Sie ersetzen weder die standardisierten Schnittstellen selbst noch die fachliche Verantwortung der anbindenden Stellen für die korrekte Nutzung der Infrastruktur.

9.2 Entscheidungsfaktoren

- ÜFA_35: Das System übermittelt Daten an EKS basierend auf einem Datenstandard.
- ASD_6: Die Transportinfrastruktur kann unabhängig vom OSiP-Fachverfahren genutzt werden, um Daten mit Erkenntnisstellen und Registern auszutauschen.
- ASD_15: Alle Schnittstellen des Systems werden nach dem API-First Ansatz konzipiert.
- ASD_17: Es werden aktuelle Standards und Protokolle eingehalten.

- ASD_18: Das System verwendet offene, dokumentierte Schnittstellen und bewusst offene Datenformate für Austausch und Export.
- ASD_21: Technische und fachliche Dokumentation werden standardisiert erstellt und aktuell gehalten.
- ASD_25: Standardisierte Schnittstellen sind bereitzustellen, um Fachverfahren und EKS interoperabel anzubinden.
- ASD_28: Im Rahmen der Neuentwicklung wird das Ziel einer weitreichenden Anbindung von Genehmigungsbehörden verfolgt.
- ASD_33: Das System unterstützt semantische Versionierung der APIs, Deprecation-Hinweise und maschinenlesbare Schemas inkl. Validierung (JSON Schema).
- ASD_35: Das System ermöglicht die Anbindung von neuen AWBs ohne Programmieraufwand.
- ASD_44: Das System stellt standardisierte Adapter mit Versionierung, Kompatibilitätstests und Referenzimplementierungen bereit.
- ASD_46: Das Produktmanagement stellt SDKs zur Integration von Fachverfahren und EKS in den gängigsten Programmiersprachen bereit
- ASD_68: Das System erzwingt für ausgetauschte Daten valide Schemas (OpenAPI/JSON Schema), inklusive Pflichtfelddefinitionen, Enumerationen, Datentypen und mehrsprachiger Beschreibungen.
- ASD_376: Das System ermöglicht eine automatisierte, skalierbare und fehlerfreie Migration von Daten aus Altsystemen.
- ASD_391: Das Produktmanagement gewährleistet Support für die Erstanbindung neuer Fachverfahren, um Verzögerungen und Mehraufwand zu vermeiden.
- ASD_403: Für die Neuentwicklung NEOSiP wird gewährleistet, dass die Meldung sowie die Nachvollziehbarkeit der Bearbeitung von Fehlern und Anforderungen ermöglicht wird.

Zusätzlich sind für diese Entscheidung folgende architektonische Kriterien relevant:

- Reduktion des Integrationsaufwands bei heterogenen technischen Umgebungen
- Unterstützung einer konsistenten und sicheren Implementierung anspruchsvoller Querschnittsfunktionen
- Vermeidung wiederkehrender Implementierungsfehler bei Schnittstellen, Identitätsprüfung und Kryptografie
- Wahrung des API-First-Prinzips, d. h. direkte Nutzung der standardisierten Schnittstellen muss grundsätzlich weiterhin möglich bleiben

9.3 Betrachtete Optionen

- Option 1: Bereitstellung von SDKs
- Option 2: Keine Bereitstellung von Hilfsmodulen

9.4 Entscheidung

Gewählte Option: „Option 1: Bereitstellung von SDKs", denn diese Option unterstützt auch unter ggf. technisch anspruchsvollen Voraussetzungen die einfache, sichere und konsistente Anbindung einer großen Anzahl von Fachverfahren wirksam und fördert so die Skalierbarkeit und Entwicklungsfreundlichkeit des gesamten Systems.

Etwaige Nachteile in Form von zusätzlichen Entwicklungskosten sowie die technische Heterogenität unter den anzubindenden Systemen wiegen diese Vorzüge nicht auf.

Die Bereitstellung von SDKs erfolgt ergänzend zu den standardisierten Schnittstellen und ersetzt nicht deren direkte Nutzbarkeit.

9.4.1 Konsequenzen

- Es ist weiterführend zu entscheiden, für welche Programmiersprachen und Plattformen SDKs angeboten werden sollen. Hierfür ist der Bedarf bei den Entwicklungsteams von möglichen anzubindenden Fachverfahren empirisch belastbar zu ermitteln.
- Die Entwicklung und langfristige Pflege entsprechender SDKs muss durch eine verantwortliche Stelle geplant und umgesetzt, organisatorisch verankert und belastbar finanziert werden.
- Die SDKs sollten mindestens die Anbindung der Schnittstellen und die Verschlüsselung/Entschlüsselung kapseln. Darüber hinaus wäre auch eine Validierung der ausgetauschten Daten möglich. Der genaue Funktionsumfang muss noch definiert werden.
- Für die SDKs sind Versionierungs-, Kompatibilitäts- und Sicherheitsupdate-Prozesse festzulegen.

9.5 Vor- und Nachteile der Optionen

9.5.1 Option 1: Bereitstellung von SDKs

Als zentral bereitgestellte Integrationsartefakte werden an zentraler Stelle SDKs für die einschlägigen Programmiersprachen und Plattformen entwickelt und unter einer offenen Lizenz bereitgestellt. Diese SDKs kapseln wesentliche Funktionen für die Anbindung an und

Nutzung der Transportinfrastruktur. Diese SDKs können durch Dritte in deren jeweils eigener Umgebung integriert und so die Anbindung an die Transportinfrastruktur vereinfacht werden.

Gut, weil

- dies die Anbindung von Fachverfahren vereinfacht und beschleunigt. Dies senkt die Schwelle für den Anschluss an die Transportinfrastruktur und begünstigt damit deren Akzeptanz und die zügige Verbreitung im unter den Fachverfahren.
- dies die Konsistenz der Anbindung erhöht und die Wahrscheinlichkeit von Entwicklungsfehlern im technischen Anbindungsprozess verringert.
- eine hohe Anzahl an Fachverfahren in Eigenverantwortung durch separate Entwicklungsteams angebunden werden muss und zentrale Hilfsmodule diesen dezentralen Implementierungsaufwand wirksam reduzieren können.
- sicherheitskritische und technisch anspruchsvolle Querschnittsfunktionen wie Schnittstellennutzung, Identitätsprüfung und kryptographische Einbindung zentral konsistenter umgesetzt werden können.

Neutral, weil

- zusätzliche Kosten und Aufwände zur Entwicklung und fortlaufenden bedarfsorientierten Weiterentwicklung entstehen. Dies ist jedoch planbar und kann sich langfristig durch geringere Wartungs- und Betriebskosten amortisieren.
- nicht alle anzubindenden Fachverfahren gleichermaßen durch SDKs adressiert werden können und daher Priorisierungsentscheidungen erforderlich sind.

9.5.2 Option 2: Keine Bereitstellung von Hilfsmodulen

Es werden keine dedizierten Hilfsmodule von zentraler Stelle entwickelt und zur Verfügung gestellt. Die Anbindung von Fachverfahren wird unter Zuhilfenahme der verfügbaren Dokumentationen, Standards und Spezifikationen durch Entwicklungsteams des anzuschließenden Fachverfahrens eigenverantwortlich umgesetzt. Dafür greifen diese direkt auf die APIs der Infrastruktur zu.

Neutral, weil

- keine zusätzlichen Kosten, Aufwände und keine zusätzlichen zentralen Entwicklungs- und Wartungsaufwände entstehen. Dies kann aber zu höherem Support-Bedarf bei der Anbindung von Fachverfahren durch separate Entwicklungsteams führen.
- das API-First-Prinzip unmittelbar umgesetzt wird, da alle Anbindungen direkt auf Basis der Spezifikationen erfolgen.

Schlecht, weil

- Geschwindigkeit, Einfachheit und Qualität der Anbindung von Fachverfahren beeinträchtigt werden könnten, wodurch die Verfügbarkeit im Gesamtsystem geschwächt werden würde.
- im Bereich der Schnittstellen und der Ende-zu-Ende-Verschlüsselung auf moderne offene Standards gesetzt wird, deren korrekte Implementierung ohne die Nutzung einschlägiger Hilfsmodule herausfordernd sein kann.
- ohne zentrale Hilfsmodule die Wahrscheinlichkeit steigt, dass Querschnittsfunktionen uneinheitlich implementiert werden und dadurch Interoperabilitäts-, Sicherheits- und Supportprobleme entstehen.

10 ADR-009 Anschluss von externen Bestandssystemen an die Transportinfrastruktur

Status: Vorgeschlagen

Datum: 2026-03-20

Entscheidungsträger: Architektur-Workstream

Beratende: ITS/DS Workstream, Fachvertretungen Behörden, Lenkungsausschuss

Informiert: IT-PLR

10.1 Kontext und Problemstellung

In ADR-001 wurde entschieden, dass eine zentrale Transportinfrastruktur zur Verfügung gestellt werden wird. An diese werden zahlreiche externe Bestandssysteme angebunden werden. Diese externen Bestandssysteme sind unterschiedlich ausgeprägt und unterliegen jeweils eigenen fachlichen, organisatorischen und technischen Rahmenbedingungen. Die Anpassungen an diesen Bestandssystemen werden auf deren Seite Aufwände erzeugen und Vorlaufzeiten benötigen.

Aktuell existieren keine verbindlichen einheitlichen Anschlussbedingungen an die Transportinfrastruktur. In der Transportinfrastruktur des Bestandssystems sind daher zahlreiche Schnittstellen umgesetzt, welche uneinheitlich gestaltet und unterschiedlich abgesichert sind. Insbesondere werden verschiedene Verfahren zur Authentisierung und Autorisierung eingesetzt. Diese Heterogenität führt zum einen zu einem erhöhten Integrations- und Wartungsaufwand und macht die Transportinfrastruktur mit jedem Anschluss komplexer und fehleranfälliger. Zum anderen ergibt sich aus dieser Heterogenität insbesondere eine komplexe und uneinheitliche Sicherheitsarchitektur, die aufgrund der Sensibilität und Kritikalität der übermittelten Daten unverantwortbar ist.

Ziel dieses ADRs ist es, eine verbindliche Strategie festzulegen, wie ext. Bestandssysteme übergangsweise mit niedrigem Anpassungsaufwand auf Seiten der externen Systeme an die Transportinfrastruktur angebunden werden können. Die diskutierten Optionen sind dabei nicht als Absenkung von Anforderungen, sondern als temporäres technisches Hilfsmittel zu verstehen. Die Einhaltung der Anschlussbedingungen ist auch dann sicherzustellen, wenn die externen Bestandssysteme diese nicht unmittelbar umsetzen.

Das angestrebte Ziel ist ein einheitlicher, sicherer und planbarer Anschluss der bestehenden ext. Systeme, ohne die Konsistenz der Zielarchitektur zu kompromittieren.

SDKs oder andere Hilfsmodule für die reguläre Zielanbindung gemäß ADR-008 sind inhaltlich von diesem ADR abzugrenzen. Die hier vorgeschlagenen Optionen dienen ausschließlich der befristeten Überbrückung von Zielabweichungen bei Bestandssystemen.

10.2 Entscheidungsfaktoren

- FA_42.1: Das System ermöglicht den Eingang von Anträgen über eine Schnittstelle (z.B. SOAP, V2) aus angrenzenden Systemen.
- ÜFA_35: Das System übermittelt Daten an EKS basierend auf einem Datenstandard.
- ASD_10: Das System ermöglicht eine klare Abgrenzung der Systemgrenzen und eine saubere Entkopplung zwischen der Transportinfrastruktur und den angebundenen Fachverfahren.
- ASD_11: Das System ermöglicht eine medienbruchfreie Abwicklung des Prozesses der Online-Sicherheitsüberprüfung für alle beteiligten Stakeholder.
- ASD_14: Der Zero-Trust-Ansatz wird im System durchgängig umgesetzt.
- ASD_16: Das System ist modular aufgebaut, um Wartbarkeit und Erweiterbarkeit zu gewährleisten.
- ASD_18: Das System verwendet offene, dokumentierte Schnittstellen und bewusst offene Datenformate für Austausch und Export.
- ASD_28: Im Rahmen der Neuentwicklung wird das Ziel einer weitreichenden Anbindung von Genehmigungsbehörden verfolgt.
- ASD_31: Im Rahmen der Neuentwicklung wird ein NEOSiP-spezifischer Datenstandard aufgebaut und genutzt und als XÖV-Standard publiziert
- ASD_44: Das System stellt standardisierte Adapter mit Versionierung, Kompatibilitätstests und Referenzimplementierungen bereit.
- ASD_50: Das System übermittelt Daten ohne zentrales Mapping (Pass-Through). Notwendige Transformationen liegen in der Verantwortung der angebundenen Systeme.
- ASD_25: Standardisierte Schnittstellen sind bereitzustellen, um Fachverfahren und EKS interoperabel anzubinden.
- ASD_144: Das System verfügt über ein IT-Sicherheitskonzept gemäß IT-Grundschutz auf Basis von ISO/IEC 27001
- ASD_159: Das System stellt über abgesicherte Kommunikationskanäle den vertrauenswürdigen Informationsaustausch zwischen FITKO, Genehmigungsbehörden, Erkenntnisstellen und weiteren Stellen sicher.
- ASD_161: Das System stellt eine Ende-zu-Ende-Verschlüsselung für alle Kommunikations- und Datenverarbeitungsvorgänge im System sicher.

- ASD_163: Das System ist so ausgelegt, dass keine zentralen Entschlüsselungsmechanismen vorhanden sind.
- ASD_168: Das System nutzt aktuelle TLS-Konfigurationen (mindestens Version 1.2), verschlüsselt Daten im Ruhezustand (AES-256) und im Transit.
- ASD_193: Wiederholte oder manipulierte Nachrichten werden erkannt und ausgeschlossen.
- ASD_251: Das Netz des Systems ist an das Verbindungsnetz des Bundes oder ein gleichwertig gesichertes Bundesnetz angebunden.
- ASD_252: Die Kommunikation aller an dem System beteiligten Behörden und Stellen erfolgt über das Verbindungsnetz des Bundes.
- ASD_323: Das System stellt sicher, dass bei der Verarbeitung personenbezogener Daten die Vorgaben der DSGVO, des BDSG, der einschlägigen Datenschutzgesetze der Bundesländer sowie sonstiger bereichsspezifischer Datenschutzbestimmungen in der jeweils geltenden Fassung eingehalten werden.
- ASD_327: Das System erfüllt die Anforderungen an Datenschutz durch Technikgestaltung (Data Protection by Design).
- ASD_330: Das System implementiert und unterstützt angemessene technische und organisatorische Maßnahmen (TOMs) entsprechend dem Schutzbedarf personenbezogener Daten.
- ASD_331: Das System stellt sicher, dass Vertraulichkeit, Integrität, Verfügbarkeit und Geschäftsprozesskontinuität bei der Verarbeitung von personenbezogenen Daten gewahrt bleiben.
- ASD_408: Das Produktmanagement verfolgt eine saubere Migrationsstrategie, bei der nur aktuelle Versionen migriert werden können.
- ASD_410: Das System bietet einen Migrationsplan, um die Integration und Umstellung strukturiert und risikoarm durchzuführen.

Zukünftig zu berücksichtigende Anforderungen aus dem Geheimschutz:

- ASD_416: Das System wahrt stets den Grundsatz „Kenntnis nur, wenn nötig", sodass nur Personen von VS Kenntnis erhalten, die auf Grund ihrer Aufgabenerfüllung von ihr Kenntnis haben müssen.
- ASD_418: Das System nutzt zur Verarbeitung von VS nur VS-IT, die hierfür freigegeben ist.

- ASD_419: Das System gibt VS über technische Kommunikationsverbindungen grundsätzlich nur durch IT-Sicherheitsprodukte nach Vorgaben des BSI verschlüsselt weiter.
- ASD_437: Werden auf einem der Server des Systems auch VS-Daten verarbeitet, muss dieser Server für die Verarbeitung dieser VS-Daten zugelassen sein.
- ASD_438: Das System gewährleistet die durchgängig verschlüsselte Kommunikation zwischen den Endgeräten, einschließlich der sicheren gegenseitigen Authentifizierung, für die gesamte Kommunikation, bei der Nutzerdaten involviert sind.
- ASD_440: Das System muss seine Metadaten durch geeignete Maßnahmen schützen. Verbindungen zwischen Clients und Servern müssen durch einen Mechanismus wie TLS geschützt werden, wenn dadurch die Menge der für Angreifer sichtbaren Metadaten reduziert wird.

Zusätzlich sind für diese Entscheidung folgende architektonische Kriterien relevant:

- Ein geordneter Übergang von Bestandssystemen zur Zielanbindung muss planbar und steuerbar sein.
- Temporäre Anschlusskomponenten dürfen in der Zielarchitektur nicht dauerhaft Architekturbrüche verursachen.
- E2EE-, Identitäts- und Sicherheitsanforderungen dürfen durch Adapter nur in explizit geregelten Übergangsszenarien berührt werden.
- Die durch Adapter entstehende technische Schuld muss zeitlich und organisatorisch begrenzt werden.

10.3 Betrachtete Optionen

- Option 1: Keine Bereitstellung von intermediären Anschlusskomponenten
- Option 2: Übergangsweise Bereitstellung von Adaptern für externe Bestandssysteme

10.4 Entscheidung

Gewählte Option: „ Option 2: Übergangsweise Bereitstellung von Adaptern für externe Bestandssysteme “, denn die übergangsweise Bereitstellung von Adaptern kann aufgrund der besseren Planbarkeit von Migrationspfaden für Bestandssysteme die Zielerreichung des Gesamtprojekts verbessern.

Die Entscheidung ist ausdrücklich als Transitionsentscheidung zu verstehen. Adapter sind kein Bestandteil des angestrebten Zielbilds, sondern ein zeitlich befristetes Hilfsmittel zur Migration bestehender externer Systeme.

Adapter werden nur dort eingesetzt, wo ein unmittelbarer Anschluss eines Bestandssystems an die Anschlussbedingungen kurzfristig nicht realistisch umsetzbar ist, die fachliche Anbindung aber für die Zielerreichung des Gesamtprojekts erforderlich bleibt.

Im Kontext dieses ADRs sind Adapter als temporäre, technische Anschlusskomponenten zu verstehen, die Bestandssystemen einen mittelbaren Anschluss an die Transportinfrastruktur ermöglichen. Die fachlichen Endpunkte bleiben die jeweiligen Bestandssysteme. Adapter können keine eigenständigen fachlichen Teilnehmer der Zielarchitektur sein.

10.4.1 Konsequenzen

- Es müssen kurzfristig Mehrkosten und Zusatzaufwände für die Entwicklung und Weiterentwicklung von Adaptern berücksichtigt werden.
- Es ist zu klären, ob und wie Entwicklungs- und Supportkosten der Adapter verursachergerecht auf die Bestandssysteme umgelegt werden.
- In der Umsetzungsphase müssen für die jeweiligen Bestandssysteme zusätzliche parallele Teilprojekte in Zusammenarbeit mit den jeweiligen Behörden umgesetzt werden.
- Es besteht die Gefahrt, dass Bestandssysteme sich ohne Druck nicht ausreichend um eine Anpassung an die neuen Anschlussbedingungen bemühen.
- Es muss strikt kommuniziert und durchgesetzt werden, dass jedes Bestandssystem, das einen fachlichen Endpunkt darstellt, eine eigene Instanz eines Adapters aufstellen muss. Es können sich somit nicht mehrere Bestandssysteme einen Adapter teilen.
- Adapter dürfen nur in der Sicherheits- und Vertrauenszone des angebundenen Bestandssystems betrieben werden. Ein Betrieb außerhalb dieser Zone wird ausgeschlossen, um Vertraulichkeit, Integrität und Verfügbarkeit nicht zu gefährden.
- Jeder Adapter erhält einen Einführungs-, Übergangs- und Abschalttermin. Verlängerungen sollten nur vom Lenkungsausschuss mit Risiko- und Kostenentscheid gewährt werden.
- Adapter werden nur bereitgestellt, wenn ein Migrationsplan des Bestandssystems vorliegt.
- Betriebshoheit, Supportgrenzen und die datensicherheitsrechtliche Verantwortung für die Adapter sind vertraglich geregelt.
- Für Adapter gelten gegenüber der Transportinfrastruktur die gleichen verbindlichen Anschlussbedingungen wie für alle anderen angebundenen Systeme.
- Für jeden Adapter existiert ein Dekommissionierungsplan.

- Soweit Adapter eine fachliche Transformation oder eine Entschlüsselung erfordern (davon ist im Kontext des OSiP-Bestandssystems stark auszugehen), ist dies als sicherheitsrelevante Abweichung jeweils isoliert zu bewerten und nur innerhalb der Sicherheits- und Vertrauenszone des jeweilig angebunden Bestandssystems zulässig.

10.5 Vor- und Nachteile der Optionen

10.5.1 Option 1: Keine temporäre Bereitstellung von intermediären Anschlusskomponenten

Es werden keine intermediären Anschlusskomponenten wie bspw. Adapter für den Anschluss von externen Bestandssystemen angeboten. Die Bereitstellung von SDKs (siehe ADR-008) ist davon unberührt. Bestandssysteme müssen die erforderlichen Schnittstellen, Sicherheitsmechanismen und Kommunikationsprotokolle selbst implementieren und setzen damit sämtliche in den Anschlussbedingungen definierten Prinzipien, Modelle und Anforderungen unmittelbar in ihren Systemen um.

Die Verantwortung für die technische Umsetzung der Anschlussbedingungen sowie für die Einhaltung der sicherheitsrelevanten und betrieblichen Vorgaben liegt vollständig bei den jeweiligen Bestandssystemen.

Gut, weil

- keine Wartungs- und Entwicklungsaufwände im Projektteam entstehen.
- kein fachliches Domänenwissen aus den externen Bestandssystemen in das Projektteam übernommen werden muss.
- technische Komplexität und Abhängigkeiten durch zusätzliche intermediäre Komponenten vermieden werden.
- das Schutzziel Vertraulichkeit nicht durch den Betrieb intermediärer Anschlusskomponenten gefährdet wird.
- das Schutzziel Integrität nicht durch den Betrieb intermediärer Anschlusskomponenten gefährdet wird.
- das Schutzziel Verfügbarkeit nicht durch den Betrieb intermediärer Anschlusskomponenten gefährdet wird.
- die Verantwortung für notwendige Anpassungen aufgrund von Änderungen in den Bestandssystemen nicht im Projektteam liegt.

Schlecht, weil

- der Anschluss von Bestandssystemen zeitlich verzögert werden könnte.
- das Gesamtprojekt in seiner Migrations- und Rolloutfähigkeit stärker von den Anpassungsgeschwindigkeiten externer Bestandssysteme abhängig wird.

- einige fachlich notwendige Anbindungen kurzfristig nicht realisierbar sein könnten, obwohl die Zielarchitektur dies langfristig vorsieht.

10.5.2 Option 2: Übergangsweise Bereitstellung von Adaptern für externe Bestandssysteme

Es werden übergangsweise Adapter bereitgestellt, die externen Bestandssystemen einen mittelbaren Anschluss ermöglichen. Die Bestandssysteme können zunächst unverändert weiterbetrieben werden, müssen jedoch innerhalb eines festgelegten Zeitraums angepasst werden. Nach Ablauf der Übergangsphase wird die Weiterentwicklung der Adapter nicht weiter unterstützt. Es wird bei der Entwicklung sichergestellt, dass die Anschlussbedingungen an die Transportinfrastruktur eingehalten werden. Es wird ausgeschlossen, dass neuen bisher nicht angebundenen Systemen ein Adapter bereitgestellt wird.

Gut, weil

- Bestandssysteme zeitnah angebunden werden können und damit die fachliche ZSÜ-Arbeit ununterbrochen fortgeführt werden kann.
- eine Migration planbarer und steuerbarer erfolgt.
- Risiken im laufenden Betrieb durch einen parallelen Übergang minimiert werden.

Neutral, weil

- der Integrationsaufwand für Bestandssysteme für diese zeitlich gestreckt wird.
- Adapter Migrationsaufwände nicht beseitigen, sondern zeitlich verschieben.

Schlecht, weil

- im Projektteam zusätzlicher Entwicklungs- und Wartungsaufwand für die Adapter entsteht.
- das Schutzziel Verfügbarkeit im Gesamtsystems von der Verfügbarkeit dieser weiteren Komponente abhängt.
- im Gesamtsystem während der Übergangsphase eine erhöhte technische Komplexität durch die Adapter besteht.
- im Gesamtsystem während der Übergangsphase mehr unnötige Komponenten verantwortet werden müssen und damit die Angriffsmöglichkeiten steigen.
- das Risiko besteht, dass Übergangsfristen verlängert werden und technische Altlasten vom Projektteam länger getragen werden müssen als geplant.

- der Transformationsprozess im Adapter eine Entschlüsselung der Daten erfordert und damit das Schutzziel Vertraulichkeit gefährdet wird.
- aufgrund der Entschlüsselung von Daten in den Adaptern, diese Adapter im Verantwortungsbereich der Bestandssystems betrieben werden müssen und damit der Support durch das Projektteam aufwendig wird.
- fachliches Domänenwissen aus den externen Bestandssystemen in das Projektteam übernommen werden muss, um Datentransformationen implementieren zu können.
- Adapter eine architektonische Übergangsabweichung vom Zielbild darstellen und deshalb einer strikten Governance, Fristsetzung und Dekommissionierung bedürfen

11 Vorlage für MADR 4.0

Siehe Vorlage:

- ***https://github.com/adr/madr/***
- ***https://github.com/adr/madr/blob/develop/template/i18n/de/adr-template.md***

Sprache: Deutsch

Status: Vorgeschlagen, Abgelehnt, Akzeptiert, Überholt, Ersetzt durch ADR-XXX

Datum:

Entscheidende:

Beratende:

Informierte:

11.1 {Kurzer Titel, der das gelöste Problem und die gefundene Lösung beschreibt}

11.2 Kontext und Problemstellung

{Beschreibt den Kontext und die Problemstellung, z.B. in zwei bis drei Sätzen freiem Text oder in der Form einer Geschichte, die das Problem veranschaulicht. Eine gute Form, das Problem auszudrücken, ist auch eine Frage. Ggf. noch Links zu Boards oder Ticketing System.}

11.3 Entscheidungsfaktoren

- {Entscheidungsfaktor 1, z.B. ein Einfluss, ein Bedenken, …}
- {Entscheidungsfaktor 2, z.B. ein Einfluss, ein Bedenken, …}
-

11.4 Betrachtete Optionen

- {Titel der Optionen 1}
- {Titel der Optionen 2}
- {Titel der Optionen 3}
- …

11.5 Entscheidung

Gewählte Option: "{Titel der Optionen 1}", denn {Begründung, z.B. die einzige Option, die kein Ausschlusskriterium beinhaltet | … | am besten abschneidet (siehe unten)}.

11.5.1 Konsequenzen

- Gut, weil {positive Konsequenz, z.B. Verbesserung einer oder mehrerer gewünschter Eigenschaften, …}

- Schlecht, weil {negative Konsequenz, z.B. Einschränkung einer oder mehrerer gewünschter Eigenschaften, …}
- …

11.5.2 Prüfung

{Beschreibt, wie die Implementierung/Einhaltung geprüft werden kann/wird. Entspricht das gewählte Design und seine Implementierung der Entscheidung? Z.B. kann eine Design-/Code-Review oder ein Test mit einer Bibliothek wie ArchUnit dabei helfen, dies zu prüfen. Beachtet, dass wir dieses Element zwar als optional einstufen, es aber in vielen ADRs enthalten ist.}

11.6 Vor- und Nachteile der Optionen

11.6.1 {Titel der Option 1}

{Beispiel | Beschreibung | Verweis auf weitere Informationen | …}

- Gut, weil {Argument a}
- Gut, weil {Argument b}
-
- Neutral, weil {Argument c}
- Schlecht, weil {Argument d}
- …

11.6.2 {Titel einer anderen Option}

{Beispiel | Beschreibung | Verweis auf weitere Informationen | …}

- Gut, weil {Argument a}
- Gut, weil {Argument b}
- Neutral, weil {Argument c}
- Schlecht, weil {Argument d}
- …

11.7 Weitere Informationen

{Hier können zusätzliche Hinweise/oder die Zuversichtlichkeit bzgl. des Entscheidungsergebnisses angeführt und/oder die Zustimmung des Teams zur Entscheidung dokumentiert und/oder festlegt werden, wann/wie diese Entscheidung umgesetzt werden soll und ob/wann die Entscheidung erneut überprüft werden sollte. Links zu anderen Entscheidungen und Ressourcen können hier ebenfalls erscheinen.}