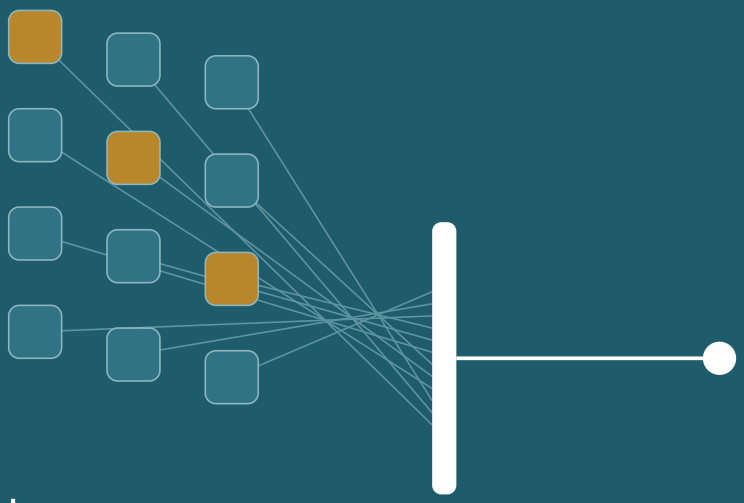
ZERYON

Berichtsformat · ZERYON Systems



AXYON Fleet
Whitepaper

Maschinenidentität für Agentenflotten

Produkt	**AXYON Fleet**
Produktversion	**0.1.0 · Kern-Stand v1.0.1 (983d6e6)**
Fassung	**2.0**
Stand	**2026-11-16**
Dokumentkennung	**AXYON-FLEET-0.1.0-WP-DE-2.0**
Anbieter	**ZERYON Systems · Predrag Gasic**
Erzeugt mit	**reportlab · ZERYON Berichtsformat**

Geltungsbereich

Dieses Papier beschreibt AXYON Fleet in der Version 0.1.0, wie sie gebaut und abgenommen ist. Beschlossene, aber nicht gebaute Erweiterungen sind als solche benannt und nicht als Eigenschaft beschrieben. Es ist kein Angebot und kein Konformitätsnachweis.

Zusammenfassung

Der erste KI-Agent in einem Unternehmen ist ein Sonderfall: Jemand kennt ihn, jemand weiß, was er darf. Ab einer Handvoll Agenten kippt etwas — leise. Es laufen Prozesse, die niemand von Hand gestartet hat, und mehrere Agenten teilen sich Dienstkonten, weil es damals schneller ging. Die Frage „Wer war das?" hat dann meist nur noch eine ehrliche Antwort: *irgendetwas, das den richtigen Schlüssel hatte.*

AXYON Fleet ist ein eigenständiges Produkt neben AXYON: dieselbe Kontroll- und Nachweisschicht zwischen KI und Unternehmenssystemen, für die Einsatzlage, in der sich mehrere autonome Agenten gegenüber dieser Schicht **ausweisen** müssen. Der Agent weist sich mit einem Zertifikat aus, nicht mit einem Geheimnis. Der Zugangstoken ist an das Zertifikat der Verbindung gebunden, über die er kommt. Der Ausweis ist zur Laufzeit entziehbar — Widerruf wird bei **jeder Anfrage** geprüft. Die Identitätsereignisse stehen im selben append-only, hash-verketteten Nachweis wie Freigabe und Ausführung. Und die Freigabe bleibt menschlich: Ein Agent gibt niemals einen Agenten frei — das ist eine geprüfte Abnahmebedingung des Produkts, keine Einstellung.

Dieses Whitepaper beschreibt die Lage, den Mechanismus, die Architektur, die geführten Nachweise und die Grenzen. Alle Aussagen sind gegen den Produktstand vom 16. November 2026 geprüft; die Belegstellen stehen im Anhang.

01

Die Lage: von einem Agenten zur Flotte

KI-Agenten werden 2026 nicht mehr einzeln eingeführt. Sie entstehen in Fachabteilungen, in Automatisierungen, in Pilotprojekten — und sie bleiben. Was dabei schneller wächst als jede andere Zahl in der IT, ist die Menge der **nicht-menschlichen Kennungen**: Dienstkonten, API-Schlüssel, Automatisierungsnutzer, Agenten. In der Fachdiskussion hat sich dafür der Begriff *Non-Human Identities* (NHI) etabliert.

Für die menschliche Belegschaft ist das Problem seit Jahrzehnten gelöst: Ausweise werden ausgestellt, gehören zu genau einer Person, und beim Ausscheiden werden sie eingezogen — der Pförtner hat die Sperrliste noch am selben Tag. Für Agenten gilt in den meisten Häusern etwas anderes: Der „Ausweis" ist ein Geheimnis. Ein Token, ein Schlüssel, ein Zertifikat in einer Datei.

Ein Geheimnis hat drei unangenehme Eigenschaften:

	Geheimnis Token, Schlüssel, Zertifikat in einer Datei	**Ausweis** ausgestellt, gebunden, entziehbar
Welche Frage wird beantwortet?	„Weißt du das Wort?“ Wer es kennt, ist drin.	„Wer bist du?“ Die Identität kommt aus einem ausgestellten Zertifikat.
Wem wird eine Handlung zugerechnet?	Mehrere Agenten teilen sich ein Konto. Der Urheber bleibt offen.	Ein Zertifikat je Maschine; der Fingerabdruck steht im Nachweis.
Wie wird das Recht entzogen?	Gilt bis zum Ablaufdatum, falls es eines gibt.	Sperre zur Laufzeit; sie wirkt bei der nächsten Anfrage.

Abbildung 1 · Geheimnis und Ausweis im Vergleich

Es beantwortet die falsche Frage. Nicht *wer bist du*, sondern nur *weißt du das Wort*. Wer es kennt, ist drin — und Kopieren hinterlässt keine Spur.

Es ist praktisch nicht zurechenbar. Weil Geheimnisverwaltung mühsam ist, wandern in der Praxis mehrere Agenten auf dasselbe Konto. Damit ist die Frage nach dem Urheber einer Handlung endgültig unbeantwortbar.

Es ist kaum entziehbar. Ein Werksausweis wird eingezogen. Eine Schlüsseldatei gilt bis zu ihrem Ablaufdatum — falls sie eines hat. Und anders als ein Mitarbeiter, der geht, hat ein abhandengekommener Agent kein Interesse daran, dass jemand es merkt.

Die Debatte über KI-Agenten dreht sich fast immer um Zuverlässigkeit: Ist das Modell gut genug? Bei mehreren Agenten ist das die **zweite** Frage. Die erste ist unromantischer:

> **Können Sie im Nachhinein sagen, welcher Agent welche Handlung ausgelöst hat — und können Sie ihm das Recht dazu im laufenden Betrieb entziehen?**

Solange die Antwort „nein" lautet, hilft das beste Modell nichts. Man kann den Agenten nicht mehr tun lassen, weil man das Ergebnis niemandem zuordnen kann. Und man kann ihn nicht anhalten, weil es kein Register gibt, in dem er steht.

02
Die Anforderung: ausgestellt, gebunden, entziehbar — und menschlich freigegeben

Der Unterschied zwischen einem Passwort und einem Werksausweis ist nicht die Sicherheit. Es ist die **Verwaltbarkeit**. Ein Ausweis wird ausgestellt, gehört zu genau einem Träger, und er läuft bei jedem Durchgang gegen eine Sperrliste. Steht er darauf, öffnet das Drehkreuz beim nächsten Durchgang nicht mehr.

Übertragen auf Maschinen ergeben sich vier Anforderungen:

1. **Ausgestellt:** Die Identität kommt aus einem ausgestellten Zertifikat, nicht aus einer Angabe, die der Agent über sich selbst macht.
2. **Gebunden:** Ein Zugangstoken trägt nur zusammen mit dem Zertifikat der Verbindung, über die es vorgelegt wird. Ein abgezogenes Token, anderswo eingesetzt, trägt nicht.
3. **Entziehbar:** Der Widerruf wirkt im laufenden Betrieb, bei der nächsten Anfrage — nicht beim nächsten Neustart und nicht erst beim Ablaufdatum.
4. **Menschlich freigegeben:** Auch mit perfekter Maschinenidentität gibt eine Maschine keine Maschine frei. Sonst wäre Maschinenidentität nur eine elegantere Art, sich selbst zu genehmigen.

Die vierte Anforderung wird in Identitätsdiskussionen regelmäßig vergessen — sie ist aber der Punkt, an dem aus einem Identitätssystem eine **Governance**-Schicht wird.

03
Was AXYON Fleet ist

AXYON Fleet ist ein eigenständiges zweites Produkt neben AXYON — kein Ausbaugrad, keine Stufe, kein Zusatzmodul. Beide Produkte teilen denselben Kern-Quellcode, der in AXYON Fleet auf einen abgenommenen Stand **gepinnt** konsumiert wird; die Trennlinie verläuft über die Einsatzlage, nicht über den Preis. Wer einen einzelnen Agenten oder ein Einzelplatz-Szenario betreibt, braucht AXYON Fleet nicht und verliert dadurch nichts.

Was AXYON leistet, gilt in AXYON Fleet unverändert nach identischen Governance-Regeln: Jede KI-Handlung wird geprüft, bei Bedarf durch einen Menschen freigegeben und in einer append-only, hash-verketteten Kette protokolliert, **bevor** geantwortet wird. AXYON Fleet fügt dem die Maschinenidentität hinzu — für die Lage, in der die Gegenseite der Kontrollschicht keine einzelne Anwendung ist, sondern eine Flotte.

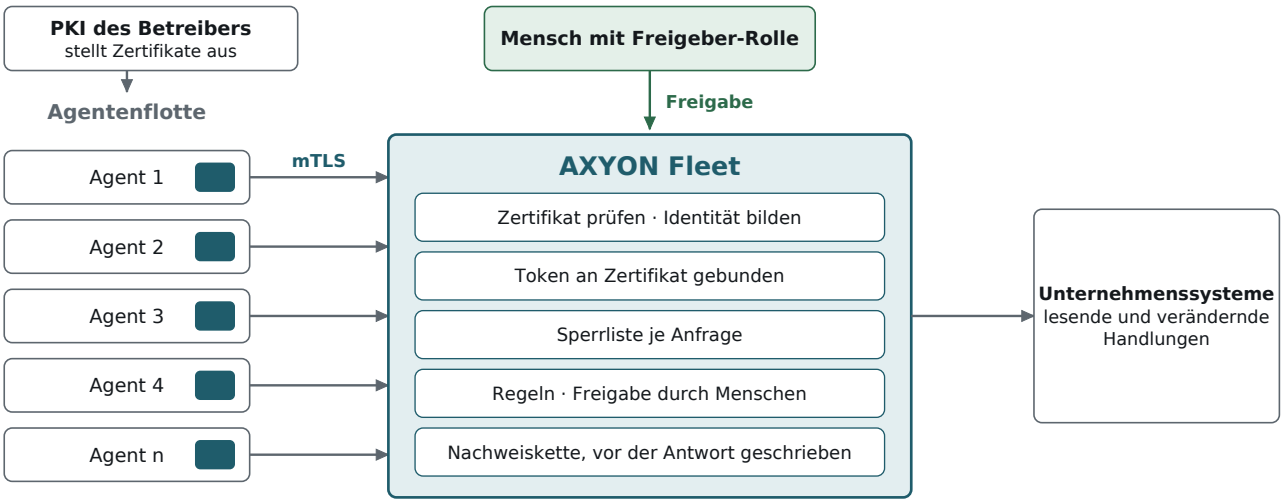


Abbildung 2 · AXYON Fleet zwischen Agentenflotte und Unternehmenssystemen

Ausgeliefert wird AXYON Fleet als Container-Appliance für das eigene Rechenzentrum. Eine notarisierte macOS-Hülle, wie AXYON sie zusätzlich anbietet, gibt es für AXYON Fleet bewusst nicht: Eine Agentenflotte ist kein Einzelplatz-Szenario. AXYON Fleet wird gekauft, nicht abonniert.

04
Der Mechanismus im Einzelnen

4.1 Ausweis statt Schlüsselwort

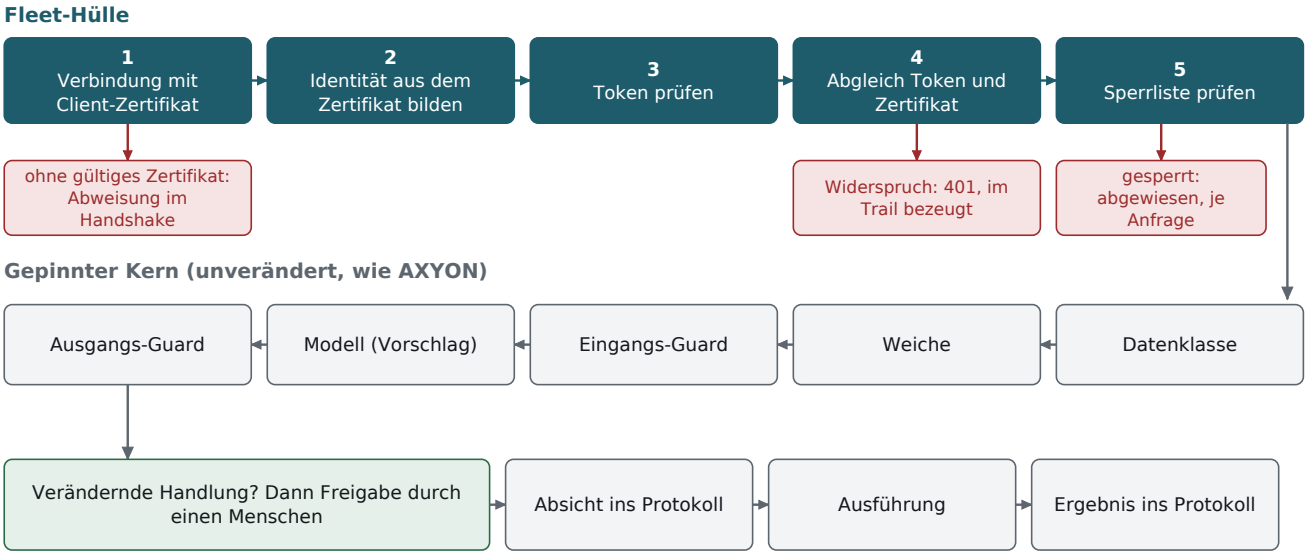


Abbildung 3 · Prüfweg einer Anfrage: fünf Schritte in der Fleet-Hülle, danach der gepinnte Kern

Jede Verbindung zu AXYON Fleet wird beidseitig geprüft (mTLS). Der Agent legt ein Client-Zertifikat vor, das gegen die vom Betreiber festgelegte Zertifikatswurzel geprüft wird; ohne gültiges Zertifikat kommt keine Verbindung zustande — die Abweisung geschieht im Handshake, bevor eine einzige Anfrage das Produkt erreicht.

Die **Identität des Agenten kommt aus dem Zertifikat selbst**: aus einem Namensfeld (SAN URI in der Auslieferungskonfiguration; alternativ SAN DNS oder CN, per Betriebssetzung). Sie ist keine Angabe, die der Agent über sich macht, und kein Header, den eine vorgelagerte Komponente setzt. Eine TLS-Terminierung an einem Reverse Proxy mit Header-Übernahme wurde in der Architekturentscheidung ausdrücklich verworfen: Wo die Identität aus einem Header käme, wäre sie wieder eine Behauptung.

4.2 Ein Token allein genügt nicht mehr

Zugangstokens bleiben nötig — sie tragen Rollen, Mandanten und Berechtigungen. Aber in AXYON Fleet ist der Token an das Zertifikat der Verbindung **gebunden**, über die er vorgelegt wird: Die Kennung im Token muss zur Kennung im Zertifikat passen, und das Zertifikat ist maßgeblich. Ein Widerspruch führt zur Ablehnung.

Die Folge ist genau die, auf die es ankommt: **Ein abgezogenes Token, das anderswo vorgelegt wird, trägt nicht.** Der klassische Diebstahl eines Bearer-Tokens — aus einem Log, einer Umgebungsvariablen, einem kompromittierten Prozess — verliert seinen Wert, weil dem Dieb das gebundene Zertifikat samt privatem Schlüssel fehlt.

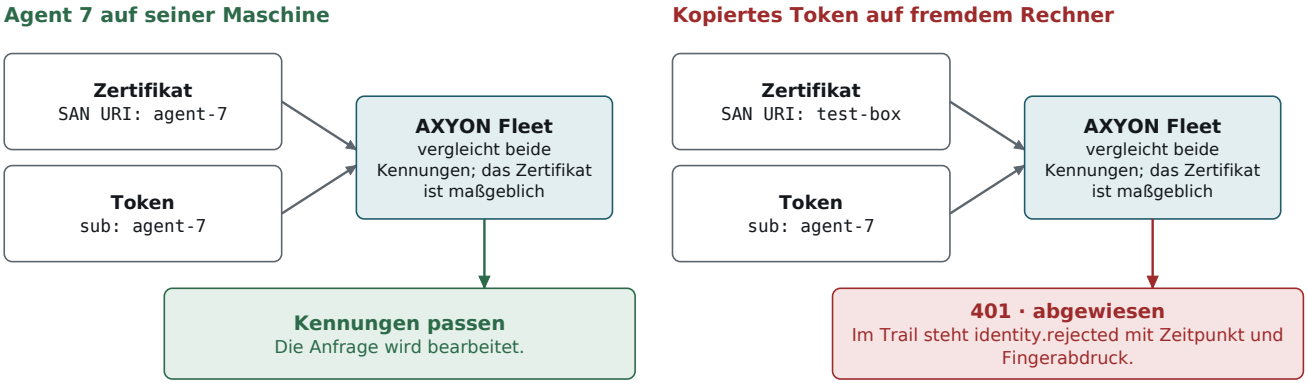


Abbildung 4 · Bindung von Token und Zertifikat: ein kopiertes Token trägt nicht

Diese Bindung ist abschaltbar, aber die Abschaltung ist eine dokumentierte Änderung der Zusage nach außen — keine stille Betriebsoption.

4.3 Widerruf zur Laufzeit, bei jeder Anfrage

Der Unterschied zwischen einer Zertifikatsdatei und einer Maschinenidentität ist der Widerruf. Ohne ihn gilt ein kompromittierter Ausweis bis zu seinem Ablaufdatum.

AXYON Fleet prüft die Sperrliste **bei jeder Anfrage** — nicht beim Verbindungsaufbau, nicht beim Neustart. Ein widerrufener Agent wird mit der nächsten Anfrage abgewiesen, auch auf einer bereits stehenden Verbindung. Die Rücknahme eines Widerrufs ist ebenso möglich und ebenso bezeugt; Widerruf und Rücknahme sind bewusst asymmetrisch abgesichert, damit ein Entzug schnell und eine Wiedereinsetzung eine bewusste Handlung ist. Die Verwaltung läuft über eigene Routen, die derselben Authentifizierungsgrenze unterliegen wie alles andere.

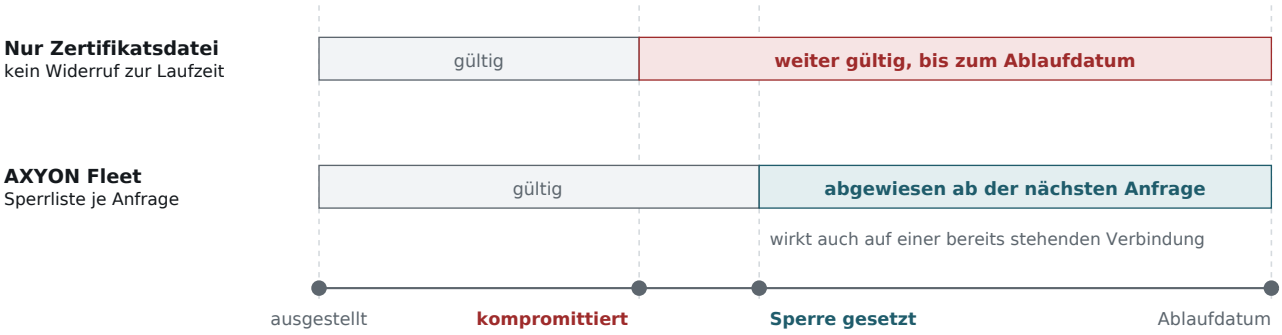


Abbildung 5 · Wirkung des Widerrufs im Zeitverlauf

4.4 Die Identität steht im selben Nachweis wie die Handlung

Ausgewiesen, abgewiesen, widerrufen — das sind Einträge in **derselben** verketteten Kette, in der auch Freigabe und Ausführung stehen. Es gibt kein zweites Protokoll daneben, das man zusätzlich auswerten müsste, und kein Format, das ein Prüfer neu lernen muss: Ein AXYON-Fleet-Protokoll ist dieselbe Kette, die aus AXYON bekannt ist, und wird mit demselben Werkzeug nachgerechnet.

Für die Kette selbst gilt, was für AXYON gilt: Jede Weichenstellung, jede Freigabe, jede ausgeführte Handlung und jede Ablehnung wird geschrieben, bevor geantwortet wird — append-only und hash-verkettet. Eine nachträgliche Änderung an einem Eintrag fällt beim Nachrechnen auf. In der Auslieferungskonfiguration liegt der Trail verschlüsselt auf Platte (AES-256-GCM je Eintrag, Argon2id-Schlüsselableitung); das Betriebs-Compose verweigert den Start ohne Schlüssel. Die Kettenköpfe werden mit einem Ed25519-Schlüssel signiert in einer Ankerdatei festgehalten, und ein Prüfer kann die Kette mit `axyon-verify` gegenprüfen — auf Inhaltsgleichheit und darauf, dass nichts hinten abgeschnitten wurde. Ohne laufendes AXYON Fleet und ohne den Schlüssel des Betreibers.

Nachweiskette: ein Protokoll für Identität und Handlung

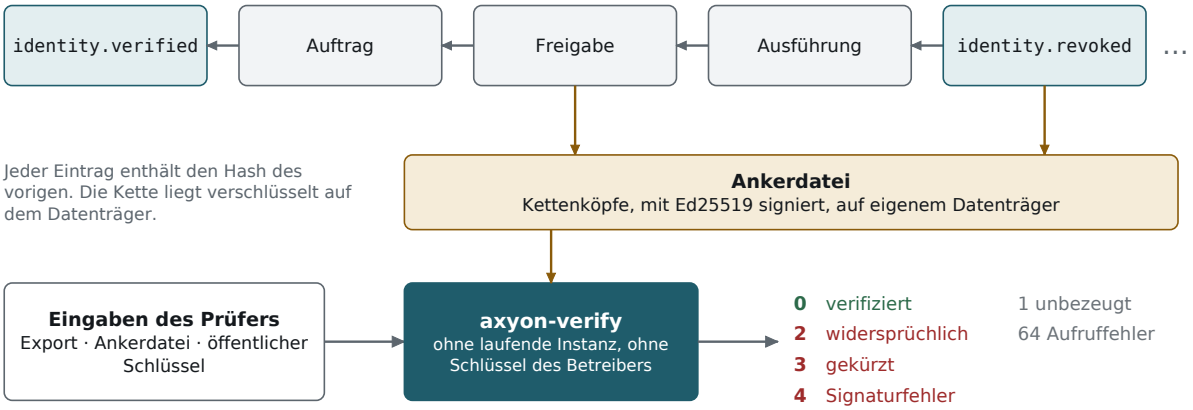


Abbildung 6 · Nachweiskette, Anker und Prüfung durch Dritte

4.5 Die Freigabe bleibt menschlich — und das ist geprüft

Die härteste Abnahmebedingung von AXYON Fleet ist unscheinbar formuliert: **Ein Agent gibt niemals einen Agenten frei.**

Wie ernst das gemeint ist, zeigt der Prüffall, mit dem die Bedingung am 2. September 2026 am gebauten Artefakt belegt wurde. Ein KI-Agent erhielt alles, was technisch zu einer Freigabe berechtigt: ein signiertes Zugangstoken mit der Rolle „approver" und ein Client-Zertifikat, das exakt zu diesem Token gehört. Verbindung einwandfrei, Bindung erfüllt, Rolle vorhanden. Der Freigabe-Antrag wurde abgewiesen:

```
HTTP 403 — „Freigabe erfordert ein menschliches Subjekt"
```

Die Gegenprobe, ohne die dieser Befund nichts wert wäre: derselbe Aufbau mit einem menschlichen Subjekt hinter dem Token — Freigabe erteilt, aufgezeichnet, in der Kette. Die Unterscheidung hängt an der ausgewiesenen Subjektart des Tokens, nicht an einer Konvention; sie ist keine Betriebseinstellung und kein Prompt, den ein Modell übergehen könnte.

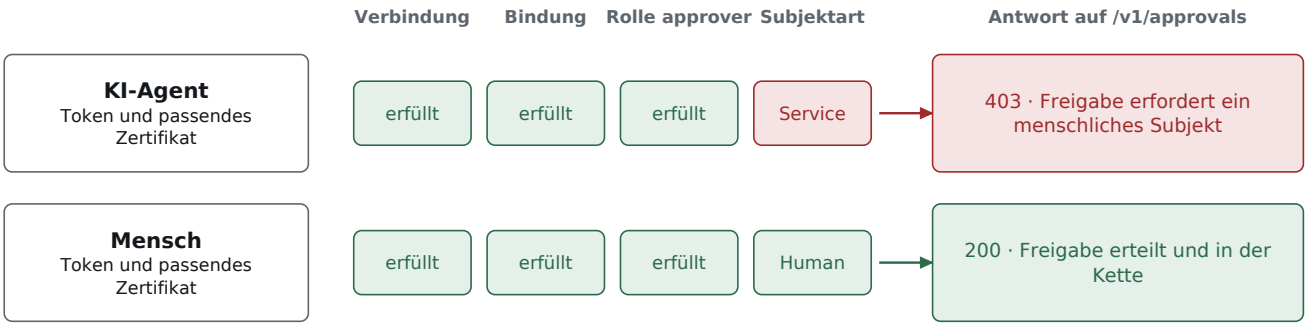


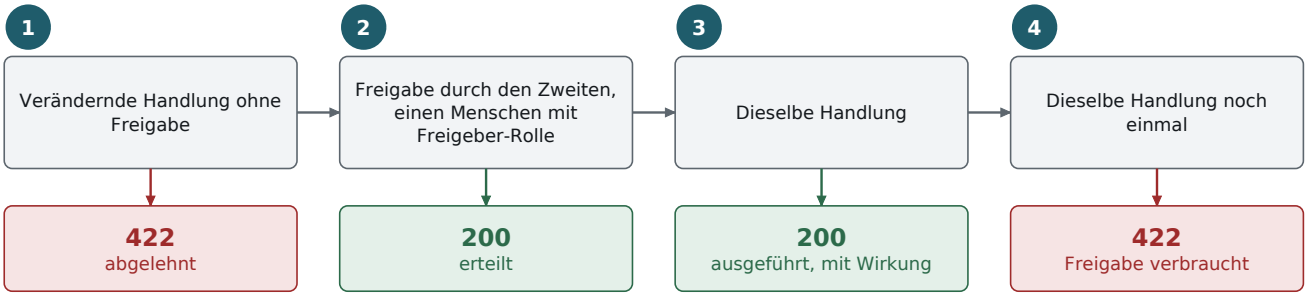
Abbildung 7 · Prüffall vom 2. September 2026: gleiche Rolle, gleiche Bindung, andere Subjektart

Dazu gehört die zweite Regel derselben Familie: **Selbst-Freigabe ist unzulässig.** Wer eine Handlung beantragt hat, kann sie nicht selbst freigeben — auch nicht mit Freigeber-Rolle.

4.6 Freigaben sind gebunden — und verbraucht

Eine Freigabe in AXYON Fleet ist an den konkreten Auftrag **und seinen Inhalt** gebunden und gilt genau einmal:

1. Eine schreibende Handlung ohne Freigabe wird abgelehnt — fail-closed.
2. Ein Mensch mit Freigeber-Rolle gibt den konkreten Auftrag frei.
3. Dieselbe Handlung läuft durch und wird ausgeführt — nachweislich, mit Wirkung.
4. Dieselbe Handlung erneut: abgelehnt. **Die Freigabe ist verbraucht.**



Weitere Antworten aus demselben Lauf: Freigabe ohne Freigeber-Rolle 403 · Selbst-Freigabe 403 · fremdes Token am Zertifikat 401

Abbildung 8 · Lebensweg einer Freigabe, mit den Antworten aus dem Nachweislauf vom 27. Oktober 2026

Schritt 4 ist der, den man weglassen könnte — und der die Zusage erst vollständig macht. Eine Freigabe, die weiterlebt, ist eine Dauervollmacht; genau die soll es nicht geben.

05
Architektur: Hülle und gepinnter Kern

AXYON Fleet ist als eigene **Hülle** um denselben Kern gebaut, der auch AXYON trägt. Die gesamte Identitäts-, Zertifikats- und Widerrufslogik lebt in der Hülle; der Kern bleibt frei von Ein-/Ausgabe, Zeit und Konfiguration und wird auf einen abgenommenen Stand gepinnt konsumiert — **konsumiert, nicht kopiert**, kein Fork.

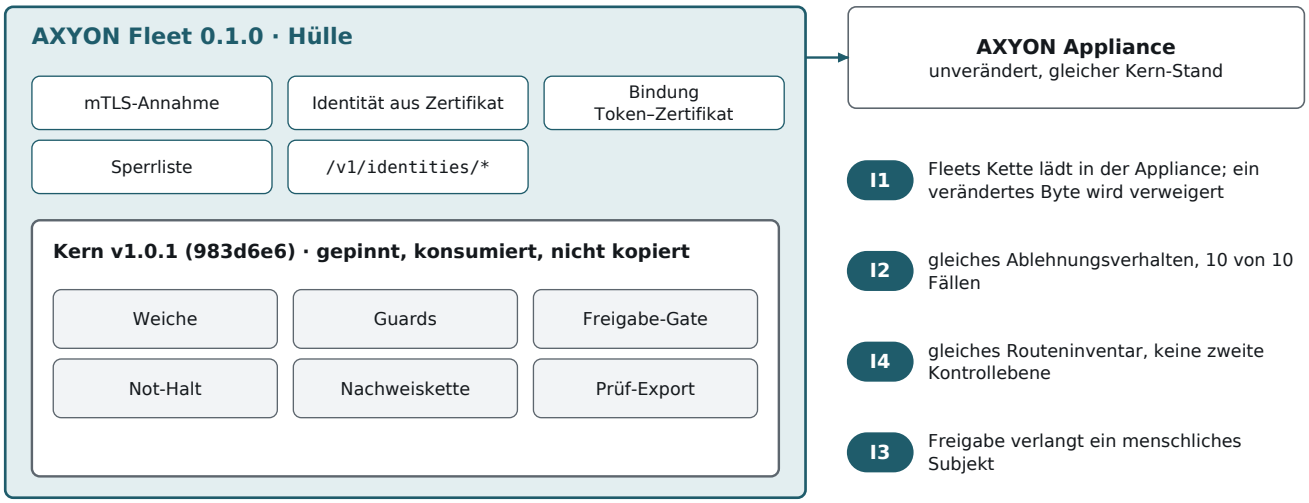


Abbildung 9 · Hülle und gepinnter Kern, mit den vier Invarianten

Vier Invarianten sichern das Verhältnis der beiden Produkte, und alle vier sind Abnahmebedingungen mit geführtem Nachweis am gebauten Artefakt:

Invariante	Inhalt	Beleg (2026-09-02, am gebauten Image)
I1	Ein von AXYON Fleet geschriebenes Protokoll ist formatgleich: Es lädt in einer **unveränderten** AXYON-Appliance des gepinnten Stands	Trail von Fleet geschrieben, von der Appliance geladen und verifiziert; Gegenprobe: ein verändertes Byte, und dieselbe Appliance verweigert den Start
I2	AXYON Fleet lockert keine Prüfung: identisches Ablehnungsverhalten	Deny-Matrix gegen beide Hüllen, 10 von 10 Fällen identisch
I3	Freigabe verlangt ein menschliches Subjekt	Abschnitt 4.5
I4	Keine zweite Kontrollebene neben der bestehenden: deckungsgleiches Routeninventar, Fleets eigene Routen nur hinter der Auth-Grenze	Routeninventar in beiden Richtungen deckungsgleich

Das Artefakt selbst ist auf Angriffsflächen-Minimierung gebaut: distroless (keine Shell, kein Paketmanager), Prozess ohne Root-Rechte, Dateisystem im Betrieb read-only, alle Capabilities abgeworfen, die Operator-Konsole des Bestandsprodukts ist in AXYON Fleet nicht enthalten und ihr Einschalten wird mit Startverweigerung beantwortet. Überhaupt ist **Startverweigerung** das Grundmuster: Eine halbe mTLS-Konfiguration, eine unbekannte Identitätsquelle, eine Bindungsregel ohne mTLS, eine Sperrliste ohne mTLS — jede dieser Lagen beendet den Start, statt einen unklaren Betriebszustand zu erzeugen.

06
Betrieb

Auslieferung. AXYON Fleet wird als architekturreines Container-Archiv mit SHA-256-Prüfsumme übergeben — keine Registry, kein Registry-Konto beim Kunden. Abgenommen ist Version 0.1.0 am Image vom 2. September 2026. Auf Intel (`linux/amd64`) läuft dieselbe Version als Referenzinstanz; ein Kundenarchiv für Intel mit vollständiger Abnahme gibt es noch nicht. Die Grenze, die dazugehört und in jedes Angebot gehört: Die Prüfsumme belegt, dass die Datei unterwegs nicht verändert wurde. Sie belegt **nicht** die Herkunft. Eine Signaturkette und SLSA-Provenance über das Image sind für AXYON wie für AXYON Fleet offen (geplante Auslieferungsstufe 2).

Identitäten. Die Ausstellungshoheit liegt beim Kunden: Welche Stelle im Haus einem Agenten ein Zertifikat ausstellt, entscheidet der Betreiber — AXYON Fleet härtet diese Hoheit, es schafft sie nicht. Kann ein Agent sich selbst ein neues Zertifikat besorgen, hilft kein Mechanismus der Welt; das ist die erste Frage der Inbetriebnahme, und sie ist unbequem.

Auth-Wege. Für die Zugangstokens unterstützt AXYON Fleet OIDC mit vier belegten Erfolgswegen (HS256, RS256 mit PEM-Schlüssel, gepinntes JWKS, Live-JWKS über HTTP), jeweils mit einem abgelaufenen Token als

Gegenprobe. Am ausgelieferten Image selbst ist davon der HS256-Weg geprüft; die drei anderen sind gegen das Programm belegt, aus dem das Image gebaut wird. Ein Dev-Token-Verfahren existiert als dokumentierter Bootstrap für Referenz- und Vorführbetrieb, nicht als Produktionsweg.

Verbund, mit Bedingung. Freigaben und Not-Halt gelten über alle Instanzen hinweg, sobald das geteilte Freigabe- und Halt-Register eingerichtet ist; ohne diese Einrichtung wirkt der Not-Halt knotenlokal. Im geführten Nachweis wurde eine Freigabe auf Knoten 1 erteilt und die Handlung auf Knoten 2 ausgeführt; der Not-Halt auf Knoten 1 hielt Knoten 2 mit an, und das Lösen verlangte die Freigeber-Rolle.

Schlüsselrotationen. Beide Rotationen — Verschlüsselungs- und Kettenschlüssel — sind am Bestand belegt, einschließlich der Gegenprobe: Ein falscher Alt-Schlüssel führt zur Startverweigerung, nicht zu einem stillen Neuanfang.

Betriebspflichten. Das Deployment-Dokument führt zehn Punkte auf, die vor Produktion gesetzt sein müssen — von den Schlüsseln über die Zertifikatswurzel bis zur Ablage der Ankerdatei auf einem anderen Datenträger.

Sicherung. An der Referenzinstanz ist die Sicherung mit einer Rückspielprobe belegt (27. Oktober 2026): Aus den gesicherten Dateien wurde eine zweite Instanz aufgebaut, sie hat alle 21 Einträge der Kette geladen und verifiziert, mit derselben Schlüsselkennung und demselben Ankerschlüssel. Die Rückspielprobe gehört beim Kunden genauso zum Betrieb.

07
Geführte Nachweise

AXYON Fleet ist nach der Doktrin gebaut, dass ein Nachweis, den man einmal von Hand führt, ein Protokoll ist — erst wiederholbar wird er eine Prüfung. Alle folgenden Läufe sind skriptgeführt, wiederholbar und fail-closed; ein übersprungener Fall gilt nicht als bestanden.

Datum	Lauf	Ergebnis
2026-09-02	Werkstor-Gates: Format, statische Analyse ohne Ausnahmen, 31 Tests, Lieferkettenprüfung mit SBOM	grün
2026-09-02	mTLS-Integrationsnachweis: Identität, Bindung, Widerruf/Rücknahme, sieben Startverweigerungs-Varianten	grün
2026-09-02	Betriebsnachweis: Verbund über zwei Knoten, beide Rotationen mit Gegenprobe, vier OIDC-Erfolgswege mit abgelaufenem Token als Gegenprobe, Selbst-Freigabe, I3, Vollkette mit verbrauchter Freigabe	grün
2026-09-02	**Abnahme am gebauten Artefakt**: I1 mit Byte-Gegenprobe, I2 (10/10), I4, Selbst-Freigabe, Vollkette, Rotationen, OIDC und I3 gegen das Image	vollständig grün
2026-09-02	Erste Referenzinstanz (inzwischen abgelöst): Inbetriebnahme mit zehn Prüffällen am laufenden Betrieb	10/10
2026-10-27	Sicherheitsaktualisierung der Abhängigkeiten; Werkstor-Gates danach: Format, statische Analyse, 31 Tests, Lieferkettenprüfung, SBOM	grün
2026-10-27	amd64-Bau auf dem Intel-Bauhost: Format, statische Analyse, 31 Tests dort; Smoke am laufenden Container über mTLS	19/19
2026-10-27	Referenzinstanz auf Intel: Nachweislauf N1–N10 (Handshake ohne Zertifikat abgewiesen, fremdes Token 401, Schreiben ohne Freigabe 422, Selbst-Freigabe 403, Freigabe durch den Zweiten, Handlung ausgeführt, Freigabe verbraucht)	10/10
2026-10-27	Sicherung der Referenzinstanz mit Rückspielprobe	21 von 21 Einträgen verifiziert

Zur Einordnung der Zeilen vom 27. Oktober: Die vollständige Abnahme mit den Invarianten I1, I2 und I4 ist am Image vom 2. September geführt. Am Intel-Image (amd64) sind der Smoke-Lauf und der Nachweislauf N1–N10 belegt, die vollständige Abnahme dort noch nicht. Die Lieferkettenprüfung (Schwachstellen- und Lizenzprüfung) lief für denselben Abhängigkeitsstand auf dem Entwicklungsrechner, nicht auf dem Bauhost.

	Image vom 2. Sept. 2026 erste Abnahme	Intel-Referenz (amd64) 27. Oktober 2026
Werkstor-Gates (Format, statische Analyse, 31 Tests)	grün	grün
Lieferkettenprüfung (Schwachstellen, Lizenzen, SBOM)	grün	grün, auf dem Entwicklungsrechner
Smoke am laufenden Container über mTLS	13 Prüfzeilen	19/19
Vollständige Abnahme: I1 mit Gegenprobe, I2, I4	vollständig grün	nicht geführt
I3: Maschine mit Freigeber-Rolle kann nicht freigeben	am Image belegt	nicht geführt
Nachweislauf an der Referenzinstanz	10/10	N1–N10: 10/10
Sicherung mit Rückspielprobe	nicht belegt	21 von 21 Einträgen
Sicherheitsaktualisierung vom 27. Oktober enthalten	nein	ja
Kundenarchiv mit Prüfsumme	vorhanden, älter als die Aktualisierung	steht aus

Abbildung 10 · Belegstand von Version 0.1.0: was wo geprüft ist

Zwei Eigenheiten dieser Nachweisführung sind erwähnenswert, weil sie über das Übliche hinausgehen. Erstens die **Gegenproben**: Kein Erfolgsfall gilt ohne den zugehörigen Fehlfall — die Appliance, die den unveränderten Trail lädt, muss den um ein Byte veränderten verweigern; das gültige Token muss neben dem abgelaufenen stehen. Zweitens die **Ehrlichkeit der Prüfwerkzeuge selbst**: Mehrere Befunde der Abnahmeläufe waren Fehler in den Prüfskripten, nicht im Produkt — und wurden als solche dokumentiert, statt sie zu Produktbefunden umzudeuten. Ein Prüfwerkzeug, dessen Bezugspunkt neben der Wirklichkeit liegt, meldet zuverlässig Befunde, die keine sind.

08
Regulatorischer Rahmen

Die menschliche Freigabe schreibender Handlungen, die Bindung der Freigabe an Auftrag und Inhalt, ihr Einmal-Charakter und die Bezeugung in einer prüfbaren Kette adressieren die Aufsichts- und Nachvollziehbarkeitserwartungen, wie sie der EU AI Act (insbesondere die menschliche Aufsicht nach Art. 14) und Rahmenwerke wie NIS2 an den produktiven KI-Einsatz stellen. Zu AXYON Fleet gehören eine technische Dokumentation nach dem Muster von Anhang IV, ein Eintrag für das KI-Inventar des Betreibers und ein Benutzerhandbuch, das die Grenzen des Produkts benennt. Die Anhang-IV-Dokumentation ist ein Entwurf (Fassung 0.1); offene Stellen sind darin markiert und nicht gefüllt.

Zur Einordnung: AXYON Fleet ist die Kontroll- und Nachweisschicht um die Modelle des Betreibers herum. Im eigenen KI-Inventar führt der Hersteller das Produkt vorsorglich als eigenen Eintrag. Wie ein Einsatz nach dem EU AI Act einzustufen ist, entscheidet der Anwendungsfall des Betreibers, nicht das Werkzeug; diese Einstufung nimmt dieses Papier nicht vor. Ein Werkzeug erzeugt auch keine Konformität. AXYON Fleet liefert technische Mechanismen und Nachweise, auf die sich die Argumentation des Betreibers stützen kann.

09

Ehrliche Grenzen

Diese Liste steht im Handbuch und im Deployment-Dokument — und gehört in jedes Angebot, weil sie sonst als Enttäuschung zurückkommt.

Keine Häufungsbewertung. AXYON bewertet inzwischen nicht nur die einzelne Handlung, sondern die Folge: Mehrere einzeln erlaubte Handlungen desselben Laufs werden gezählt, und ab einem Band verlangt AXYON eine menschliche Freigabe für den Fortgang. AXYON Fleet 0.1.0 steht auf einem Kernstand **vor** diesem Mechanismus; zwanzig einzeln erlaubte Handlungen ergeben hier keine Schwelle. Der Nachzug ist seit dem 6. November 2026 beschlossen. Gebaut ist er nicht, und ein Termin steht nicht fest. Wer Maschinenidentität kauft und Häufungsschutz erwartet, hat ihn in dieser Version nicht.

Keine Signaturkette über das Image. Die Prüfsumme belegt die Übertragung, nicht die Herkunft (Abschnitt 6).

Noch kein Kundenarchiv für Intel. Auf Intel (amd64) läuft die Referenzinstanz. Ein Kundenarchiv mit vollständiger Abnahme liegt für diese Architektur nicht vor.

Das abgenommene Archiv ist älter als die Sicherheitsaktualisierung. Es stammt vom 2. September 2026. Die Aktualisierung der Abhängigkeiten vom 27. Oktober ist im Quellstand und in der Intel-Referenz enthalten, in diesem Archiv nicht. Ein Auslieferungsbau aus dem aktualisierten Stand steht aus.

Keine Bedienoberfläche. Version 0.1.0 wird über die HTTPS-Schnittstelle und die Betriebswerkzeuge des Hauses bedient. Eine Konsole ist nicht enthalten.

Keine Delegationsketten. Eine Maschine weist sich aus; sie handelt nicht nachweislich *im Auftrag* einer anderen. Die Architektur ist dafür offen, gebaut ist es nicht — und ohne mitziehende Gegenseite beim Kunden wäre es wertlos.

Verbindungshäufigkeit steht nicht im Trail. Die Identitätsbezeugung wird bewusst einmal je Identität und Prozesslauf geschrieben; ein auffälliges Verbindungsmuster ist damit nicht sichtbar. Das hält den Trail lesbar und ist eine dokumentierte Entwurfsentscheidung — keine Lücke, die erst im Betrieb auffällt.

Verbundwirkung nur mit eingerichtetem Register (Abschnitt 6).

Ausstellungshoheit beim Kunden (Abschnitt 6). AXYON Fleet härtet sie, es schafft sie nicht.

10

AXYON und AXYON Fleet nebeneinander

Warum zwei Produkte und nicht eine große Version? Weil eine Stufe das Bestandsprodukt über das definieren würde, was ihm fehlt. AXYON kann alles, was es kann. AXYON Fleet adressiert eine andere Lage: Häuser mit einer Agentenflotte, deren Angehörige sich ausweisen müssen.

	AXYON	AXYON Fleet
Einsatzlage	Eine KI-Anwendung, ein Team, ein Arbeitsplatz	Mehrere autonome Agenten gegenüber einer Kontrollschicht
Identität der Gegenseite	Zugangstoken	Zertifikat (mTLS) + gebundener Token, Widerruf je Anfrage
Häufungsbewertung (Kettentor)	vorhanden	heute nicht (Abschnitt 9)
Auslieferung	Container-Appliance oder native macOS-App	Container-Appliance
Protokollformat	die Kette	dieselbe Kette, formatgleich (I1)
Externe Prüfung	`axyon-verify`	dasselbe Werkzeug
Bedienung	Operator-Konsole	HTTPS-Schnittstelle, keine Oberfläche
Vertragsmodell	siehe Unterlagen zu AXYON	Kauf, kein Abonnement

Beide Produkte laufen im Haus des Betreibers und folgen denselben Governance-Regeln, mit der einen benannten Ausnahme der Häufungsbewertung.

11
Die Prüffrage

Sie hat mit uns nichts zu tun und ist in zehn Minuten zu beantworten:

> **Zählen Sie die nicht-menschlichen Kennungen in Ihrem Haus — Dienstkonten, API-Schlüssel, Automatisierungsnutzer, Agenten. Und markieren Sie dann die, denen Sie das Recht zu handeln heute entziehen könnten. Nicht beim Ablaufdatum — heute.**

Die Differenz zwischen beiden Zahlen ist Ihr eigentliches Thema. Sie wächst schneller als jede andere Zahl in Ihrer IT — und sie wächst, ob Sie KI-Agenten einsetzen oder nicht.

Wenn diese Differenz bei Ihnen groß ist und Sie darüber sprechen wollen, was daraus folgt:
office@zeryon-systems.com

Anhang A
Begriffe

Begriff	Bedeutung in diesem Papier
mTLS	beidseitig geprüfte TLS-Verbindung: auch der Client weist sich mit einem Zertifikat aus
SAN URI	Namensfeld im Zertifikat, aus dem AXYON Fleet die Maschinenkennung liest
Bindung	die Regel, dass Token- und Zertifikatskennung übereinstimmen müssen; das Zertifikat ist maßgeblich
Widerruf	Entzug einer Identität zur Laufzeit, geprüft bei jeder Anfrage
Kette / Trail	append-only, hash-verkettetes Protokoll aller Weichenstellungen, geschrieben vor der Antwort
Anker	signierter Kettenkopf (Ed25519) in einer separaten Datei, Grundlage der externen Prüfung
`axyon-verify`	eigenständiges Prüfwerkzeug: rechnet die Kette nach, ohne laufende Instanz und ohne Betreiberschlüssel
fail-closed	im Zweifel verweigern: unklare Konfiguration verhindert den Start, ungeprüfte Handlung die Ausführung
NHI	Non-Human Identities — nicht-menschliche Kennungen: Dienstkonten, API-Schlüssel, Agenten

Anhang B
Belegstellen

Jede Aussage dieses Papiers ist einem Architektur-Entscheid (ADR), einem Bauabschnitt (Slice) oder einem geführten Nachweislauf zugeordnet. Auswahl:

Aussage	Beleg
Zwei Produkte, keine Stufe; Sprachregel	ADR-048
mTLS, Identität aus dem Zertifikat; Reverse-Proxy-Weg verworfen	SLICE-60; Integrationsnachweis S3
Bindung Token↔Zertifikat, Zertifikat maßgeblich	ADR-062 / SLICE-63
Widerruf je Anfrage, Rücknahme, Asymmetrie, eigene Routen hinter der Auth-Grenze	SLICE-61 / ADR-064; S3-Lauf K61-Reihe
Identitätsereignisse im selben Trail, Bezeugung je Prozesslauf	ADR-063
I1–I4 als Abnahmebedingungen, am Artefakt belegt	ADR-048; Abnahme am Image 2026-09-02
I3-Prüffall (Agententoken mit Freigeber-Rolle → 403, Kontrollfall Mensch → 200)	SLICE-60 Kriterium 6; Betriebsnachweis S4 und Abnahme am Image, je 2026-09-02
Vollkette mit verbrauchter Freigabe	S4 (V1–V5); Referenzinstanz-Inbetriebnahme (N4–N10)
Vier OIDC-Erfolgswege mit Gegenproben	S4, 2026-09-02

Aussage	Beleg
Verbund und Not-Halt über zwei Knoten, mit Bedingung	ADR-037; S4 (A0–A6)
Beide Schlüsselrotationen mit Gegenprobe	S4 (B/C-Reihe)
Externe Prüfung `axyon-verify`, Ed25519-Anker	ADR-049
Gepinnter Kern, konsumiert statt kopiert	ADR-048 / ADR-056
Auslieferung als Archiv mit Prüfsumme; Herkunfts-Grenze	ADR-047 / ADR-075
Distroless, ohne Root, read-only, Konsole verweigert	ADR-053; Artefakt-Eigenschaften im Baulauf
Häufungsbewertung fehlt in Fleet 0.1.0	ADR-075; DEPLOYMENT §8; Handbuch Kap. 21
Keine Delegationsketten	ADR-048
Verbindungshäufigkeit nicht im Trail	ADR-063
Referenzinstanz auf Intel, N1–N10, Smoke 19/19	Ausführungsvermerk Fleet-Intel-Referenz, 2026-10-27
Sicherung mit Rückspielprobe, 21 Einträge	derselbe Vermerk, Paket 3
Sicherheitsaktualisierung der Abhängigkeiten	Fleet-Commit `94295c7`, 2026-10-27
Kein Kundenarchiv für Intel; Archiv vom 2026-09-02	`dist/`-Protokoll zu Commit `fba8ccd`; ADR-079, Bestandstabelle
Nachzug der Häufungsbewertung beschlossen, nicht gebaut	ADR-079 (Accepted 2026-11-06, „nichts implementiert")
OIDC: HS256 am Image, drei Wege gegen das Programm	Risk-Log Fleet, Endstand 2026-09-02

Die vollständigen Nachweisprotokolle und die technische Dokumentation nach Anhang-IV-Muster werden Interessenten im Gespräch offengelegt.

Prüfgrenzen dieses Dokuments

- Geprüft gegen das Fleet-Repo (main `dccb7a7`, Tag `v0.1.0`) und den AXYON-Vault, Stand 16. November 2026. Bauhost und Referenzinstanz wurden an diesem Tag nicht angefasst; Aussagen dazu stammen aus dem Ausführungsvermerk vom 27. Oktober 2026.
- Kein Nachweislauf wurde für dieses Dokument neu gefahren. Alle Ergebnisse tragen das Datum ihres Laufs.
- Die Abbildungen sind Schemazeichnungen. Sie zeigen keine Messwerte außer den im Text belegten Antworten und Zählungen.
- Die kanonische Formatablage ZERYON_GLOBAL wurde nicht eingesehen; gesetzt nach dem Gerüst der AXYON-Kundendokumente v1.2.0.
- Das Dokument ersetzt keine Einstufung eines Anwendungsfalls, keine Rechtsberatung und keine Produktionsabnahme.