Systemdokumentation

immo.quick Ökosystem — Architektur, Rechtsgrundlagen, Governance-Prinzipien

immo.quick Global UG

Juli 2026 · Öffentliche Referenzdokumentation

immo.quick
Serverless Edition

Immo.quick Serverless Edition

Systemdokumentation

Diese Dokumentation beschreibt ein System nicht als Produkt, sondern als Antwort auf eine Welt. Sie erklärt zuerst die Welt, in der Compliance heute stattfindet, und leitet aus dieser Welt das System ab. Wer die Welt verstanden hat, versteht das System nicht als Werkzeug, sondern als Haltung.

Erster Teil: Die Welt, in der diese Dokumentation entstanden ist

Bevor ein einziger Algorithmus beschrieben wird, wird beschrieben, warum es einen Algorithmus brauchen kann. Compliance ist heute kein Dokument mehr, das man vorlegt. Compliance ist ein Beweis, den man erbringt. Und dieser Beweis muss Jahre nach dem Ereignis noch erbracht werden können, wenn niemand sich mehr an das Ereignis erinnert.

Kapitel 1: Die Welt der Compliance, wie sie heute ist

Szenario 1: Die verschwundene Grundlage

Drei Jahre nach einer Kreditvergabe sitzt ein Compliance-Beauftragter in einem Zeugenstand. Die Gegenseite fragt, auf welcher Sanktionsliste genau damals geprüft wurde. Der Beauftragte antwortet, auf der EU Liste. Die Gegenseite fragt weiter, welche Fassung der EU Liste. Der Beauftragte antwortet, die, die damals galt. Die Gegenseite fragt, wo stehe, welche Fassung das war. Der Beauftragte schweigt. Das PDF in den Akten sagt Sanktionsprüfung unauffällig. Das PDF sagt nicht, gegen welche Fassung, zu welchem Zeitpunkt, mit welcher Regelversion, auf welche Eingabe bezogen. Das PDF ist eine Behauptung der Abteilung. Es ist kein Beweis.

In diesem Moment zerfällt eine Compliance-Entscheidung, die drei Jahre lang stark war. Nicht weil sie falsch war, sondern weil ihre Grundlage dokumentiert, nicht festgehalten war. Und dieser Unterschied zeigt sich genau dann, wenn es darauf ankommt. In der Nachschau, vor Gericht, in der aufsichtlichen Prüfung, in der forensischen Untersuchung.

Szenario 2: Die glattpolierte Wahrscheinlichkeit

Eine Software sagt, dieser Fall ist mit 92 Prozent unauffällig. Drei Jahre später will ein Forensiker nachrechnen, warum 92 Prozent standen. Er kann es nicht. Die 92 Prozent kamen aus einem Modell, das ein bestimmtes Trainingsdatum hatte, eine bestimmte Konfidenzschwelle, eine bestimmte Version der Klassifikation. Heute ist das Modell anders, die Trainingsdaten sind anders, die Konfidenzschwelle ist anders. Die 92 Prozent von damals sind nicht reproduzierbar. Sie waren eine Momentaufnahme, keine Aussage. Und eine Momentaufnahme hält nicht, was eine Aussage halten muss. Die Reproduzierbarkeit über Zeit.

Szenario 3: Die drei isolierten Notizen

Ein Versicherer prüft eine Auszahlung im Todesfall. Drei Werkzeuge arbeiten nebeneinander. Das AML Werkzeug prüft die Bezugsberechtigte, das Solvency II Werkzeug prüft die Kapitalauswirkung, das IDD Werkzeug prüft die Verhaltenspflicht bei der Anlage des verbleibenden Vermögens. Drei Werkzeuge, drei PDFs, drei Notizen der Berater. Nach zehn Jahren, in einer Versicherungsaufsicht, stehen drei isolierte Dokumente, die nicht miteinander verwandtschaftsverknüpft sind. Die Frage der Aufsicht lautet, haben Sie IDD, Solvency II und AML auf dieselbe Entität, zum selben Zeitpunkt, in derselben Eingabeentscheidung gekoppelt geprüft. Der Versicherer muss antworten, wir haben drei Werkzeuge verwendet und deren Ergebnisse lagen uns separat vor. Die Aufsicht wird fragen, und die Verknüpfung. Schweigen.

Szenario 4: Die nachträgliche Regeländerung

Ein Energieversorger hat im Sommer Energieimporte beschafft. Im Winter kommt die Nachschau, war die beschaffte Herkunft sanktionspflichtig. Der Compliance-Beauftragte sagt, wir haben gegen die damals geltende Sanktionsliste geprüft. Die Aufsicht fragt, welche Fassung. Der Beauftragte sagt, die aktuelle von damals. Die Aufsicht fragt, wo steht die Hash-Referenz auf diese Fassung. Die Antwort ist ein PDF Archiv, in dem die Liste als aktuell ohne Versionsbezug referenziert ist. Niemand kann nachrechnen, welche Liste genau gemeint war. Die Nachschau wird zu einer Glaubensfrage, nicht zu einer Rechenfrage.

Szenario 5: Die unbemerkte Grundrechtskollision

Eine Behörde wendet eine Regel an, die aus einem fachlichen Anliegen entstanden ist, ohne dass im Regelwerk vermerkt wurde, welcher Grundrechtskonflikt darin auf dem Spiel steht. Die Regel wird angewendet, das Ergebnis sieht sauber aus, die Akte wird geschlossen. Jahre später, in einer verfassungsgerichtlichen Auseinandersetzung, stellt sich heraus, dieser Regel fehlt die Grundrechtsdiskussion. Die Grundrechtsdiskussion wurde nie geführt, weil sie niemand angestoßen hat. Die Folge ist nicht eine Korrektur der Entscheidung, sondern eine Rekonstruktionsschwäche, die nachträglich nicht mehr behebbar ist. Die Entscheidung war sauber dokumentiert, aber sie war grundrechtlich blind gewesen.

Szenario 6: Die Struktur, die nur im Querschnitt sichtbar wird

Eine Entität führt über neun Monate vierzehn Vorgänge durch, jeder einzeln unter dem Meldepflicht Schwellenwert. Jede Einzelfallprüfung zeigt, Vorgang unauffällig, nicht meldepflichtig, nächste Prüfung. Niemand sieht das Muster, weil niemand über die Vorgänge hinweg schaut. Am Ende der neun Monate liegt eine Stückelung vor, die niemals als Stückelung erkannt wurde, weil das Werkzeug jeden Vorgang isoliert betrachtete. Anti Structuring Vorschriften existieren, weil diese Querschnittsanforderung real ist. Und kein Einzelfall Werkzeug ist gebaut, um sie zu bearbeiten.

Szenario 7: Die Manipulation, die niemand gesehen hat

Ein Audit Log erlaubt nachträgliche Änderungen. Jemand ändert einen Eintrag, der drei Monate alt ist. Der Eintrag sieht jetzt anders aus, aber niemand kann nachrechnen, dass er geändert wurde, weil das Log nicht append only ist. In einer forensischen Auseinandersetzung fragt die Gegenseite, können Sie nachweisen, dass dieses Log seit drei Monaten unverändert ist. Der Antwortende muss sagen, nein, das Log ist veränderlich. Die Glaubwürdigkeit des gesamten Archives sinkt in einem Satz.

Szenario 8: Die KI Entscheidung, die niemand nachrechnen kann

Eine Software fällt eine Compliance-Entscheidung mit einer KI. Drei Jahre später fragt die Gegenseite, warum genau diese Entscheidung. Die Software kann die Entscheidung nicht reproduzieren, weil die KI von einer Modellversion abhing, die inzwischen nicht mehr existiert. Die Entscheidung ist eine Blackbox geblieben, und die Blackbox ist zugefallen. Die Gegenseite kann die Entscheidung nicht nachrechnen, und das entscheidende Institut kann die Entscheidung nicht verteidigen. In einer gerichtlichen Auseinandersetzung kommt es nicht darauf an, wer behauptet, sondern wer nachweisen kann. Eine KI, die entscheidet, kann nicht nachweisen. Eine Regel, die deterministisch angewendet wird, kann es.

Szenario 9: Der empfangende Prüfer ohne Vorbeziehung

Ein Institut A übergibt einem Institut B ein Compliance Ergebnis. Institut B hat keine Vorbeziehung zu Institut A. Institut B will das Ergebnis verifizieren. Institut A sagt, vertrauen Sie uns, wir haben es geprüft. Institut B fragt, kann ich es selbst nachrechnen. Institut A sagt, nicht ohne unser internes System. Institut B muss sich also entscheiden, entweder vertrauen, ohne nachrechnen zu können, oder ablehnen, weil Nachrechnen nicht möglich ist. Beides ist in einer Compliance Kette unbefriedigend. Eine Entscheidung, die auf blindem Vertrauen beruht, ist keine Entscheidung, die in einer Kette fortgetragen werden kann. Eine Entscheidung, die abgelehnt wird, weil sie nicht nachrechenbar ist, bricht die Kette.

Szenario 10: Die Infrastruktur, die keiner kontrolliert

Ein europäisches Institut führt Compliance Prüfungen in einer Cloud durch, die unter der Hoheit eines US Mutterkonzerns steht. Im Rahmen des CLOUD Act kann diese Cloud auf Anordnung Daten an US Behörden herausgeben, auch die Daten, die im europäischen Rechenzentrum gespeichert sind. In einer Compliance relevanten Auseinandersetzung kann das Institut nicht sicher sagen, dass keine nicht europäische Behörde auf die Daten zugreift. Die Compliance Prüfung selbst wird zu einem Compliance-Risiko. Das ist kein theoretisches Szenario, es ist die Welt, in der jeder lebt, der seine Daten bei einem US Anbieter liegen hat.

Szenario 11: Die Kette, die nicht lückenlos war

Ein Institut dokumentiert jede Prüfung, aber zwischen zwei Dokumentationen klafft eine Lücke, weil ein Wartungsfenster dazwischen lag und in diesem Fenster eine Prüfung nicht versiegelt wurde. Jahre später fragt ein Prüfer, was ist in dieser Lücke passiert. Niemand kann es sagen. Die Lücke ist nicht gefüllt, weil die Kette nicht append only ist und weil es keinen Zwang gibt, jede Prüfung zu versiegeln. Die Lücke ist klein, aber sie ist da, und in einer forensischen Auseinandersetzung genügt eine Lücke, um die ganze Kette infrage zu stellen.

Szenario 12: Der Zeuge, der nicht mehr erreichbar ist

Ein Mitarbeiter hat eine Compliance-Entscheidung begründet. Die Begründung steht in einer E-Mail. Der Mitarbeiter hat das Unternehmen verlassen, die E-Mail ist gelöscht worden, weil die Aufbewahrungsfrist abgelaufen ist. Jahre später kann niemand mehr sagen, worauf die Entscheidung beruhte. Die Entscheidung mag korrekt gewesen sein, aber ihre Begründung ist verschwunden, weil sie nicht in einer versiegelten Kette stand, sondern in einem flüchtigen Medium.

Kapitel 2: Was diese Szenarien gemeinsam haben

Alle zwölf Szenarien haben eine Eigenschaft gemeinsam. Eine Entscheidung wurde getroffen, dokumentiert und abgelegt. Die Entscheidung war in ihrem Moment sauber. Aber in der Nachschau zerfällt sie, weil ihre Grundlage nicht festgehalten, sondern nur behauptet war.

Das ist keine Frage der Compliance-Anstrengung. Es ist eine Frage der Compliance-Methode. Und die Methode ist heute, in fast jedem Institut, dieselbe. Dokumentieren statt Festhalten. Berichten statt Beweisen. Wahrscheinlichkeit statt Determinismus. Isolierte Werkzeuge statt gekoppelter Ketten. Audit Logs statt append only Ketten. KI, die entscheidet, statt Regeln, die deterministisch angewendet werden. Flüchtige Medien statt versiegelter Begründung.

Wer diese Welt verstanden hat, hat verstanden, warum die Frage nicht lautet, wie machen wir noch mehr Compliance. Sondern, wie machen wir Compliance, die in der Nachschau hält.

Kapitel 3: Der rote Faden

Der Satz, der das ganze System trägt, lautet:

> ***Governance ohne Grundlage ist nur eine Meinung.***

Mit Meinung ist hier nicht eine persönliche Stellungnahme gemeint, sondern ein Ergebnis, das im Nachhinein nicht mehr nachrechenbar ist. Eine Compliance-Entscheidung, die nur in einem PDF steht, ist solange stark, bis eine Gegenseite die Nachrechenbarkeit verlangt, und dann fällt sie in sich zusammen. Genau diese Schwäche schließt das System. Und es schließt sie nicht durch ein besseres PDF. Es schließt sie durch eine andere Methode.

Diese Methode hat vier Stützen.

Erste Stütze. Beweis statt Dokumentation. Eine Dokumentation behauptet, was geprüft wurde. Ein Beweis hält kryptografisch versiegelt fest, welche Regel, in welcher Version, mit welchen Daten, zu welchem Zeitpunkt geführt hat.

Zweite Stütze. Determinismus statt Wahrscheinlichkeit. Eine Wahrscheinlichkeitsaussage ist im Nachhinein nicht reproduzierbar. Eine deterministische Regel wendet eine klare Vorschrift auf klare Daten an. Heute dasselbe Ergebnis wie in zehn Jahren.

Dritte Stütze. Prüfung statt Vertrauen. Eine Entscheidung, die auf blindem Vertrauen beruht, kann in einer Kette nicht fortgetragen werden. Eine Entscheidung, die kryptografisch nachrechenbar ist, kann von jedem Dritten ohne Vorbeziehung überprüft werden.

Vierte Stütze. Lückenlosigkeit statt Lückenhaftigkeit. Eine Kette, in der eine Prüfung fehlt, ist keine Kette, sondern eine Ansammlung. Das System zwingt jede Prüfung in die Kette, sodass eine fehlende Prüfung sichtbar wird, nicht unauffällig bleibt.

Wer diese vier Stützen verstanden hat, hat verstanden, warum das System nicht noch ein Compliance-Werkzeug ist. Es ist eine andere Methode.

Kapitel 4: Was diese Methode voraussetzt, und was sie nicht voraussetzt

Die Methode setzt voraus, dass eine Regel existiert, dass eine Eingabe existiert, und dass ein Zeitpunkt existiert. Mehr nicht. Sie setzt nicht voraus, dass die Regel richtig ist, dass die Eingabe vollständig ist, oder dass der Zeitpunkt günstig ist. Sie nimmt das, was ist, versiegelt es, und macht es nachrechenbar.

Das ist wichtig, weil es die Grenze der Methode markiert. Das System kann nicht garantieren, dass eine Regel richtig war. Es kann garantieren, dass die Regel, die angewendet wurde, nachrechenbar ist. Das System kann nicht garantieren, dass eine Eingabe vollständig war. Es kann garantieren, dass die Eingabe, die geprüft wurde, unverändert vorliegt. Das System kann nicht garantieren, dass ein Zeitpunkt glücklich war. Es kann garantieren, dass der Zeitpunkt, an dem geprüft wurde, wahrheitsgemäß festgehalten ist.

Diese Unterscheidung ist entscheidend. Wer das System als Garantie für richtige Entscheidungen liest, hat es missverstanden. Wer es als Garantie für nachrechenbare Entscheidungen liest, hat es verstanden.

Zweiter Teil: Die drei Fundament Standards

Kapitel 5: CDS, Constitutional Divergence Screening

Was es ist. CDS ist ein zweistufiger Scanner, der einen Gesetzestext oder einen Regelentwurf durchsucht, bevor die darin enthaltene Regel überhaupt angewendet wird. Die Prüfung geht nicht auf Fachfragen, sondern auf die Grundrechtsebene. Berührt dieser Text ein Grundrecht, und zwar in einem Muster, das eine Kollision erzeugt, also eine Spannung zwischen zwei Gütern der Rechtsordnung, die im Text selbst nicht vollständig aufgelöst ist.

Der Scanner hat zwei voneinander unabhängige Stufen.

Erste Stufe, Kollisionsmuster Ebene. Welche strukturellen Grundrechtskollisionen erkennt das System. Aktuell sind es 156 Muster, gewachsen aus einer früheren Basis von 47. Diese Zahl gibt an, wie viele solche Muster das System erkennt.

Zweite Stufe, Jurisdiktions Ebene. In wie vielen Rechtsordnungen werden diese Muster angewendet. Aktuell sind es 53 Jurisdiktionen.

Die beiden Zähler werden bewusst nie miteinander verrechnet. Ein Muster kann in vielen Jurisdiktionen gelten, eine Jurisdiktion kann viele Muster enthalten. Eine Mischzahl wie vielleicht einige tausend mögliche Kombinationen wäre täuschend, weil nicht jedes Muster in jeder Jurisdiktion wirklich relevant ist. Die Trennung ist also kein Zufall, sondern Schutz gegen eine solche Verschleierungsarithmetik.

Warum es existiert, im Lichte von Szenario 5. Szenario 5 beschrieb eine Regel, deren Grundrechtskollision niemand angestoßen hat. Die Folge war eine Rekonstruktionsschwäche, die nachträglich nicht mehr behebbar war. CDS schließt genau diese Lücke vorab. Bevor eine Regel angewendet wird, dokumentiert der Scanner die Berührung eines Grundrechtsmusters im entstehenden Beweisstück. Die Grundrechtsdiskussion ist nicht länger dem Zufall überlassen, ob jemand sie anstößt. Sie ist methodisch verankert.

Beispiel. Ein Gesetzgeber erlässt eine Regel, die Internetplattformen verpflichtet, bestimmte Inhalte zu löschen. Fachlich eine Regel über Löschpflichten. Grundrechtlich ein Eingriff in die Meinungsfreiheit, kombiniert mit einer Prüfpflicht, die die Plattform trifft. CDS erkennt das Muster Meinungsfreiheit gegen Löschpflicht und markiert die Berührung im entstehenden Beweisstück. Später, wenn ein künftiges Regelwerk diese Regel anwendet, trägt das Beweisstück die Hash-Referenz auf die grundrechtlich geprüfte Version. Im Ernstfall steht eine Grundrechtsdiskussion zur Verfügung, nicht als umfassendes Gutachten, sondern als dokumentierte Berührung, die eine solche Diskussion sichtbar macht und nicht stillschweigend übersieht.

Wie es zusammenhängt. CDS ist die Eingangsprüfung jeder neuen Regelkatalogversion. Wenn die Pipeline später eine Regel anwendet, trägt das entstehende Beweisstück die Hash-Referenz auf die grundrechtlich geprüfte Version. Ein späterer Prüfer sieht, die Regel war bereits vor ihrer Anwendung auf Grundrechtskollisionen getestet. CDS ist kein fachliches Gate, sondern die Vorab Prüfung der Regel selbst. Es entscheidet nicht, ob die Regel fachlich richtig ist, sondern ob sie grundrechtlich transparent ist.

Erweiterung. CDS ist nicht statisch. Die Musterbibliothek wächst, weil die Grundrechtsdiskussion in den Jurisdiktionen wächst. Eine Kollision, die in einer Jurisdiktion heute noch nicht erkannt wird, kann morgen erkennbar werden, weil ein Gerichtsurteil die Diskussion eröffnet hat. Das System hält die Bibliothek versioniert vor, sodass ein Receipt, der heute erzeugt wird, auf die heute gültige Bibliothek verweist, und ein Receipt, der morgen erzeugt wird, auf die morgen gültige Bibliothek. Auch die Bibliothek ist hashverankert. Niemand kann nachträglich behaupten, ein Receipt sei mit einer anderen Bibliothek geprüft worden als derjenigen, auf die er verweist.

Kapitel 6: STFL, Sovereign Transaction Finance Layer

Was es ist. STFL ist die Schicht, die jedes Compliance Ergebnis mit der kaufmännischen Seite verbindet, mit Abrechnung, Rechnungstellung und Buchung. Jede versiegelte Receipt ist nicht nur ein fachliches Ereignis, sondern auch ein abrechenbares Ereignis. STFL übersetzt die versiegelte Receipt in eine buchungsfähige Struktur.

Warum es existiert, im Lichte von Szenario 3. Szenario 3 beschrieb drei isolierte Werkzeuge, deren Ergebnisse in drei isolierten PDFs standen und die nach zehn Jahren in drei isolierten Notizen verwahrt waren. STFL ist das Gegenmodell. Jede versiegelte Receipt ist eine kryptografisch fixierte Quelle, die in die Buchung einfließt. Nicht die Bezeichnung Compliance erfüllt wird referenziert, sondern die konkrete, nachträglich prüfbare Kette. Die Finanzseite kann die Compliance Seite nicht mehr als Textreferenz übernehmen, sondern nur als hash verankerte Quelle.

Beispiel. Eine Bank führt in einem Monat 247 GLEIF Prüfungen durch. Jede Prüfung erzeugt eine CertifiedReceipt, jede Receipt ist ein versiegeltes, hash verankertes, abrechenbares Ereignis. STFL übersetzt die 247 Receipts in die buchungsrelevante Struktur. Jede Receipt erzeugt einen Eintrag im Receipt Ledger, der abrechenbar ist. Die Monatsabrechnung aggregiert die Receipts zu einer Rechnung, die ihrerseits die Liste der Receipt IDs referenziert. Die Rechnung ist damit nicht eine isolierte Behauptung der Buchhaltung, sondern eine hash referenzierte Aufstellung über die exakt denselben Receipts, die die Compliance Seite erzeugt hat. Ein Auditor prüft Rechnung gegen Receipts, und jeder Eintrag ist eins zu eins nachvollziehbar.

Wie es zusammenhängt. STFL sitzt am Ende der Pipeline. Erst entsteht die Receipt, dann übersetzt STFL sie in Buchungs und Berichtsereignisse. Die Rechnung referenziert die zugrunde liegenden Receipts und ist damit selbst kryptografisch nachprüfbar, nicht eine isolierte Behauptung der Buchhaltung.

Erweiterung. STFL unterstützt mehrere Rechnungswege. Ein Weg ist die Standard PDF per E-Mail, ein Weg ist die XML API Übergabe an ein ERP System, ein Weg ist die Dunkelverarbeitung in einem öffentlichen Beschaffungsnetz, ein Weg ist die E-Rechnung nach der in Europa geltenden Norm für öffentliche Auftraggeber und große Unternehmen. Das System entscheidet nicht, welcher Weg der richtige ist, es stellt alle bereit. Der Empfänger wählt den Weg, der zu seiner Buchhaltung passt. Die Receipt, die hinter der Rechnung steht, ist in allen Wegen dieselbe. Der Weg ändert die Form der Rechnung, nicht die Quelle der Rechnung.

Kapitel 7: SCP 1.0, Sovereign Compliance Proof Standard

Was es ist. SCP 1.0 ist das Datenmodell, das Signaturprotokoll und die Kettenstruktur, das jedes forensisch belastbare Artefakt formal beschreibt. Es legt fest, welche Felder ein Artefakt mindestens enthält, wie die kanonisierte Form aussieht, über die der Hash gebildet wird, wie die Signaturblöcke aufgebaut sind, wie die Merkle Verkettung referenziert wird. SCP 1.0 ist herstellerneutral und offen dokumentiert.

Warum es existiert, im Lichte von Szenario 9. Szenario 9 beschrieb einen empfangenden Prüfer ohne Vorbeziehung, der ein Ergebnis verifizieren will, aber kein System jenseits des erzeugenden Instituts hat, um das zu tun. SCP 1.0 löst das, weil es ein veröffentlichtes, offenes Format vorgibt. Jeder, der es versteht, kann ein Artefakt prüfen, ohne das erzeugende System konsultieren zu müssen.

Beispiel. Ein Portable RDR, das an einen Empfänger übergeben wird, ist ein eigenständiges Dokument in einer offenen Datenstruktur. Es trägt die Receipt ID der zugrunde liegenden CertifiedReceipt, die Regel und ihre Version, das Ergebnis, den Verification Block mit zwei Signaturklassen, den eingebetteten öffentlichen Schlüssel und die Referenz auf den öffentlich veröffentlichten Schlüssel. Der Empfänger, eine Kanzlei, die keine Vorbeziehung zum System hat, kann genau dieses Artefakt verifizieren, ohne ein zweites System konsultieren zu müssen. Sie liest den eingebetteten öffentlichen Schlüssel oder ruft den öffentlich veröffentlichten ab, prüft die Signatur, rechnet die Hashes nach, und bestätigt die Integrität. SCP 1.0 ist das Format, das diese Selbsttragfähigkeit ermöglicht.

Wie es zusammenhängt. Alle Beweisstück Typen bauen auf SCP 1.0 auf. Die CertifiedReceipt, die RelianceDecisionRecord, das T0 Artefakt, die sektorspezifischen Receipts, die Due Diligence Artefakte und die portablen Formate. Wer das Datenmodell einmal verstanden hat, versteht das formale Gerüst in jedem Sektor.

Erweiterung. SCP 1.0 ist versioniert. Das System kann das Datenmodell erweitern, wenn neue Beweisstück Typen hinzukommen. Eine Erweiterung ist nicht rückwirkend, sondern aufgeschichtet. Ein Artefakt, das in Version 1.0 erzeugt wurde, bleibt in Version 1.0. Ein Artefakt, das in Version 1.1 erzeugt wird, trägt die Versionsnummer 1.1. Ein Prüfer, der beide Versionen sieht, weiß, welches Format er vor sich hat, und kann beide prüfen. Das System überschreibt nicht, es schichtet auf.

Dritter Teil: Die zwei Ausführungsmodelle

> ***immo.quick Core ist eine eigenständige Produktlinie mit eigenem Architektur- und Funktionsumfang. Die vorliegende Dokumentation beschreibt ausschließlich die immo.quick Serverless Edition. Aussagen dieser Dokumentation dürfen nicht auf Core übertragen werden.***

Kapitel 8: immo.quick Serverless Edition

Was es ist. Die Serverless Edition ist die API first Ausführung. Ein Kunde ruft ein API Endpunkt auf, die Pipeline läuft, das Ergebnis kommt als Receipt oder als portables Artefakt zurück. Es gibt keinen eigenen Server, den der Kunde zusätzlich betreiben muss.

Warum es existiert. Viele Anwender brauchen Compliance als API, ohne einen Serverbetrieb zu pflegen. Teams, die Compliance Massenprüfungen skalieren, Marktteilnehmer, die Prüfergebnisse in ihre eigene Software einbinden, Integrationen, die eine API an ein eigenes ERP anflanschen.

Beispiel. Ein Fintech, das täglich zehntausend Geschäftspartner Prüfungen durchführt und kein Compliance Team betreibt, das eine eigene Ausführungsumgebung pflegen könnte, ruft die API der Serverless Edition auf. Jede Prüfung kommt als versiegelte Receipt zurück, die abgelegt und bei Bedarf exportiert wird. Das Fintech betreibt keine Infrastruktur, es betreibt nur API Aufrufe.

Wie es zusammenhängt. Jede Receipt, die die Serverless Edition erzeugt, folgt dem in Teil Zwei beschriebenen SCP 1.0 Standard. Die Wahl des Ausführungsmodells für einen konkreten Anwendungsfall ist eine eigene, produktseitige Frage außerhalb des Umfangs dieses Dokuments.

Kapitel 9: Warum die europäische Infrastrukturwahl ein Architekturthema ist

Die Ausführung liegt in europäischen Infrastrukturen, beispielsweise Hetzner, IONOS, OVHcloud. Das ist nicht nur eine Kosten oder Verfügbarkeitsentscheidung, sondern eine Architekturentscheidung mit juristischen Gründen.

Der CLOUD Act ist ein US amerikanisches Bundesgesetz, das US beheimatete Cloud-Anbieter verpflichtet, auf Anordnung Daten an US Behörden herauszugeben, auch wenn die Daten in Europa gespeichert sind. Ein europäischer Kunde, dessen Daten bei einem US Anbieter liegen, kann in einer Compliance relevanten Auseinandersetzung nicht sicher sein, dass keine nicht europäische Behörde Zugriff erhält.

Mit einem europäischen Anbieter, und damit ist ausdrücklich ein Anbieter mit Hauptsitz und Datenhaltung in einer EU-Mitgliedstaat mit eigener Rechtshoheit gemeint, nicht nur ein Anbieter mit europäischem Rechenzentrum aber US Mutterkonzern, ist die Rechtslage eine andere. Eine Herausgabe durch eine EU Behörde läuft über EU Rechtswege und eröffnet keinen automatischen Kanal zu US Behörden. Diese Wahl schützt nicht gegen legitime europäische Anfragen, gibt aber die Kontrolle darüber, unter welchem Rechtsrahmen eine Herausgabe überhaupt stattfindet. Genau deshalb ist die Wahl der europäischen Infrastruktur eine Architekturentscheidung, keine Kosmetik.

Erweiterung. Die Wahl der Infrastruktur ist nicht die einzige Architekturwahl, die juristisch relevant ist. Auch die Frage, wo die Schlüssel liegen, ist relevant. Ein Schlüssel, der in einer US Cloud liegt, unterliegt demselben CLOUD Act. Ein Schlüssel, der in einer europäischen Infrastruktur liegt, unterliegt europäischem Recht. Das System hält die privaten Schlüssel ausschließlich serverseitig und ausschließlich in einer Infrastruktur, die der europäischen Jurisdiktion unterliegt. Das ist nicht Paranoia, sondern die logische Konsequenz aus Szenario 10.

Vierter Teil: Das Innere des Systems

Kapitel 10: Die Gate Pipeline im Detail

Was die Pipeline ist. Die Gate Pipeline ist die Kette von Einzelprüfungen, die ein Eingabedatensatz durchläuft, vom Empfang über verschiedene Regeln bis hin zum ausgelieferten Receipt. Ein Gate ist eine isolierte, eigenständig versionierte Regelanwendung. Ein Gate ist nicht die Compliance, sondern ein konkreter Baustein, der ein konkretes Regelwerk auf eine konkrete Eingabe anwendet. Die Reihenfolge der Gates ist nicht beliebig. Sie folgt einem Ergebnisbegriff. Ein frühes Gate, das auf eindeutig stoppende

Eingabe prüft, etwa einen Sanktions Treffer, macht die späteren Gates für diesen Workflow fachlich hinfällig.

Der vollständige Ablauf. Ein Beispiel. Eine Bank reicht eine Transaktionsprüfungsanfrage ein. Bitte prüfe die Entität mit LEI 5299 in Bezug auf Transaktion T 7741. Was passiert, Schritt für Schritt.

Erster Schritt, Eingang und Eingabe Hash. Die Anfrage wird kanonisiert, der Input Hash wird berechnet. Ab jetzt ist die Eingabe unveränderbar in die Receipt Kette eingebracht. Eine Änderung der Eingabe nach diesem Punkt bricht die Kette sichtbar.

Zweiter Schritt, GLEIF Validierung. Der LEI wird gegen das GLEIF Register geführt. Das Gate erfasst den Status der Entität, die GLEIF Snapshot Version und den GLEIF Snapshot Hash zum Zeitpunkt der Abfrage. Ist der LEI ungültig oder die Entität aufgelöst, dokumentiert das Gate genau diesen Befund, nicht eine Vermutung.

Dritter Schritt, Sanktions Screening. Entität und, sofern vorhanden, gemeldete wirtschaftlich Berechtigte werden gegen die relevanten Sanktionslisten geführt. EU FSF, OFAC SDN, UK HMT, UN SC, FATF. Jede Liste trägt einen Listen Hash. Die Receipt referenziert die Liste und den Hash. Treffer, dokumentiert als BLOCK Anlass. Kein Treffer, dokumentiert als Teil des CLEAR Bildes. Unklar, dokumentiert, nicht verschleiert.

Vierter Schritt, AML Prüfung. Die fachspezifische AML Prüfung, hier nach dem Geldwäschegesetz, wird angewendet. Die AML Prüfung ist nicht die Geldwäsche Wertung an sich. Geldwäsche Strukturerkennung ist CRPG, Teil 7 dieses Dokuments. Sondern die Sorgfaltspflicht und Meldepflichtlogik in Bezug auf den konkreten Vorgang.

Fünfter Schritt, Jurisdiktionskonflikt. Die Transaktion berührt mehrere Jurisdiktionen. Das Gate prüft auf eine Kollision zwischen den anwendbaren Rechtsordnungen, insbesondere die Spannung zwischen der EU Blocking Regulation und der US amerikanischen extraterritorialen Sanktionsanwendung. Wenn eine solche Spannung vorliegt, dokumentiert das Gate das. Die Receipt wird nicht stillschweigend nach der einen oder der anderen Seite entschieden, sondern in der Spannung dokumentiert.

Sechster Schritt, Grundrechtsprüfung. Die anzuwendende Regel wird CDS basiert geprüft. Die Berührung eines Grundrechtsmusters, wenn vorhanden, wird dokumentiert.

Siebter Schritt, Sektorspezifisch. Bankenlogik. Basel III Mindestkapitalprüfung, wenn die Transaktion die Eigenkapitalquote berührt. Oder ein fachspezifisches Gate nach dem Typ der Transaktion, etwa MiFID II Eignung bei einer Anlageentscheidung.

Achter Schritt, Receipt erzeugt. Die CertifiedReceipt entsteht, wird signiert, in die Merkle Kette eingefügt. Die portable Version bekommt bei Bedarf die asymmetrische Signatur. Das Artefakt ist vollständig für die weitere Prüfung bereit.

Kapitel 11: Das Prinzip der versionierten Regelbasis

Jede Regel, die ein Gate anwendet, trägt eine Versionsnummer und einen Hash. Das ist die Antwort auf Szenario 4. Rechtsquellen ändern sich. Ein Urteil kommt hinzu, eine EU Richtlinie wird geändert, einer Sanktionsliste wird ein Eintrag hinzugefügt. Wenn eine Receipt nur sagt Regel X angewendet, dann ist nicht klar, welche Fassung der Regel X angewendet wurde. Im Nachhinein kann niemand rekonstruieren, ob das Ergebnis, das damals erzielt wurde, noch auf der heute aktuellen Fassung beruht.

Deshalb trägt jede Regel eine Versionsnummer, und das System hat eine Katalog Versionierung. Erst wenn eine neue Version des Regelkatalogs mit neuem Hash hinterlegt ist, darf die neue Version angewendet werden. Die Receipt referenziert den Hash der Regel, die sie angewendet hat. So kann ein späterer Prüfer immer feststellen, ob sich die Rechtslage in der Zwischenzeit geändert hat und ob die alte Aussage noch gültig ist.

Beispiel. Eine Receipt referenziert die Sanktionsliste der EU in der Fassung vom 14. Juli 2026 mit Hash X. Drei Jahre später ist die Liste in einer neuen Fassung gültig, mit Hash Y. Der Prüfer kann zwei Fragen beantworten. Stand die damalige Entität auf der damaligen Liste. Ja, nachrechenbar aus Hash X. Und steht die Entität heute auf der heutigen Liste. Das erfordert eine neue Prüfung gegen Hash Y. Beide Fragen sind sauber getrennt, weil die versionierte Regelbasis es erlaubt.

Erweiterung. Die versionierte Regelbasis ist nicht nur ein Schutz gegen Vergessen, sondern ein Schutz gegen die Gegenwart. Wer heute behauptet, eine Prüfung sei nach heutiger Rechtslage korrekt gewesen, obwohl sie vor drei Jahren stattfand, vermischt zwei Zeitebenen. Die versionierte Regelbasis zwingt die Trennung. Die Prüfung war nach der Rechtslage von damals korrekt, gemessen an der damaligen Liste. Ob sie nach der heutigen Rechtslage korrekt wäre, ist eine andere Frage, die eine neue Prüfung verlangt. Das System erlaubt beide Fragen, aber es erlaubt nicht, sie zu vermischen.

Kapitel 12: Die Datenquellen der Pipeline

GLEIF. Das Legal Entity Identifier Register, die internationale Quelle der Unternehmensidentifikation.

Sanktionslisten. EU Consolidated Financial Sanctions, OFAC SDN, UK HMT, UN Security Council, FATF.

Rechtsquellen nach Sektor. BGH Rechtsprechung, Grundgesetz, EU Grundrechtscharta, DORA, Basel III, Solvency II, MiCA, Geldwäschegesetz, Außenwirtschaftsgesetz und verordnung.

Veröffentlichte Regelkataloge. Jede Version mit eigenem Hash, referenzierbar, nicht überschreibend.

Erweiterung. Jede Datenquelle trägt nicht nur einen Hash, sondern auch einen Zeitpunkt der Abfrage. Der Zeitpunkt ist wichtig, weil eine Liste, die heute abgefragt wird, morgen anders aussehen kann. Das System dokumentiert nicht nur, welche Liste geführt wurde, sondern wann sie geführt wurde. Ein Auditor, der die Frage stellt, war diese Liste zum Zeitpunkt der Prüfung die aktuelle, findet die Antwort im Receipt, nicht in einer Vermutung.

Kapitel 13: Gate 0, das Eingangstor der Gesamtpipeline

Gate 0 ist das Eingangsgate der Gesamtpipeline. In der Sektorlogik haben einzelne Sektor Engines eigene Gate Nummern, M0 bis M9 bei Motorsport, aber systemweit ist Gate 0 die grundlegende, systemweite Eingangsprüfung. Alle weiteren Sektor Gates sind nachgeordnet.

Was Gate 0 ist. Gate 0 ist die Prüfung der forensischen Zulässigkeit der Eingabe im Voraus. Es ist kein Fach Gate. Es entscheidet nicht über Foul oder kein Foul, über Sanktionsmeldung oder keine Sanktionsmeldung. Es entscheidet über die Frage, ist die Eingabe überhaupt beweiserzeugend bearbeitbar. Hat die Eingabe die Eigenschaften, die eine forensisch belastbare Receipt zulassen.

Warum Gate 0 existiert. Jede spätere Receipt kann nur so belastbar sein wie die Eingabe, aus der sie entstanden ist. Eine präzise Regel, angewendet auf eine Eingabe, die unvollständig ist, die nicht kryptografisch fixiert ist, die nicht einer verifizierten Entität zugeordnet ist, die ohne NTP Zeitanker erfasst wurde, eine solche Eingabe erzeugt einen Receipt, der alle formellen Eigenschaften erfüllt, aber in einer forensischen Auseinandersetzung zusammenbricht, weil die Eingabe selbst nicht dort stand, wo sie stehen musste. Genau diese Schwäche lässt sich im Nachhinein nicht beheben. Man kann nachträglich keinem Receipt einen verlässlichen Entitätsbezug geben, wenn die Entität bei der Eingabe nicht sauber aufgelöst war. Gate 0 existiert deshalb, um diese Schwäche vorab zu schließen.

Was Gate 0 im Detail prüft. Gate 0 prüft nacheinander und dokumentiert für jeden Schritt einzeln, ob er erfolgreich war, den Status WARNING trug oder fehlgeschlagen ist.

Erste Prüfung, Kanonizität der Eingabe. Die Eingabe wird nach RFC 8785, JSON Canonicalization Scheme, kanonisiert. Das ist die Vorbedingung dafür, dass nachfolgende Hashes reproduzierbar sind. Ohne Kanonizität wäre ein Hash über die Eingabe von der Reihenfolge der Felder, von Leerzeichen oder von der spezifischen Serialisierungsform abhängig, und damit nicht in einem anderen System reproduzierbar. Gate 0 prüft und dokumentiert, dass die Eingabe kanonisiert wurde. Die kanonisierte Form und ihr Hash sind Bestandteil des Vorlaufs.

Zweite Prüfung, Vollständigkeit der Pflichtfelder. Jede Gate Variante hat Pflichtfelder, eine Entitäts Identifikation, einen Transaktionstyp, einen fachlichen Kontext. Gate 0 prüft, dass diese Pflichtfelder vorhanden und nicht leer sind. Fehlt ein Pflichtfeld, stoppt Gate 0, nicht um die Anfrage zu sanktionieren, sondern weil eine forensisch belastbare Receipt mit fehlenden Pflichtfeldern nicht erzeugt werden kann. Der Grund wird dokumentiert, ohne dass ein Receipt erzeugt wird.

Dritte Prüfung, Entitäts Identität, verifiziert, nicht nur behauptet. Zentraler Aspekt von Gate 0. Die Entität, auf die sich die Prüfung bezieht, muss verifiziert sein, nicht nur angegeben. Das bedeutet, der LEI, wenn vorhanden, wird gegen GLEIF geprüft. Ist kein LEI vorhanden, muss eine sekundäre Identifikation vorhanden sein, die Gate 0 ebenfalls verifiziert. Eine nicht verifizierte Entität, Name ist angegeben, aber nicht überprüfbar, ist für eine forensische Receipt untauglich. Genau hier trennt sich das System von zahlreichen Werkzeugen, die eine Entität nur behauptet akzeptieren, weil die Prüfung später ja feststellen würde, ob die Entität real ist. Das ist das Prinzip der Verschiebung. Das System hier macht es

umgekehrt. Verifikation vor der fachlichen Prüfung, weil eine nachträgliche Verifikation an einem Receipt, der fachlich schon basiert hat, zu spät kommt.

Vierte Prüfung, Quellensicherheit der Eingabe. Woher kommen die Eingabedaten. Eine Eingabe kann verschiedene Quellen haben. Eine Transaktion im laufenden Betrieb, eine Regierungsmeldung, ein externer Datenfeed, eine Mitarbeiternotiz. Gate 0 dokumentiert, aus welcher Quelle die Eingabe stammt. Die Quellkennung ist Teil des Vorlaufs. Später, in einer forensischen Auseinandersetzung, ist entscheidend, ob die Eingabe aus einer verifizierbaren Quelle kam oder aus einer Mitarbeiternotiz.

Fünfte Prüfung, NTP Zeitanker der Eingabe. Die Transaktions Zeit ist NTP verankert. Die Zeit ist damit nicht durch das System allein manipulierbar. Gate 0 prüft, ob ein NTP Zeitanker zugewiesen wurde. Fehlt er, dokumentiert Gate 0 das in der Vorlauf Aufzeichnung.

Sechste Prüfung, Divergenz der Eingabe. Wo eine Eingabe aus mehreren Quellen kommt, etwa in einem Sportszenario mit mehreren Kamera Perspektiven, oder einem Transaktionsdatensatz mit mehreren Datenfeeds, prüft Gate 0, ob die Quellen übereinstimmen. Divergiert die Eingabe zwischen Quellen, dokumentiert Gate 0 die Divergenz. Der Receipt wird nicht stillschweigend zugunsten einer Quelle entschieden, sondern der Divergenzfall wird Teil des Vorlaufs, und an das Gate 0 Ergebnis wird eine Markierung divergent angefügt. Spätere Gates können diese Markierung interpretieren. Ein nachgeordnetes Gate kann entscheiden, dass eine divergente Eingabe einer vertieften Prüfung bedarf.

Was Gate 0 tut, wenn es durchläuft. Hat Gate 0 alle sechs Schritte bestanden, Eingabe kanonisiert, Pflichtfelder vollständig, Entität verifiziert, Quelle dokumentiert, NTP Zeitanker gesetzt, Divergenz geklärt, wird ein Gate 0 Ergebnis erzeugt, das aus folgenden Komponenten besteht.

Ein Vorlauf Protokoll, das für jeden der sechs Schritte dokumentiert, ob er bestanden wurde, den Status WARNING trug oder fehlgeschlagen ist.

Ein Gate 0 Verdict, das ausdrücklich kein fachliches Verdict ist, weder PASS noch BLOCK noch Foul oder kein Foul, sondern die Aussage Eingabe forensisch zulässig.

Die übergebene kanonisierte Eingabe und ihr Hash, die ab jetzt für alle nachgeordneten Gates bindend ist.

Die verifizierte Entitäts Identifikation, die ab jetzt für die gesamte Pipeline verbindlich ist.

Was Gate 0 nicht tut. Kein fachliches Urteil. Gate 0 entscheidet nicht über eine Sache, nur über die Forensik der Eingabe. Keine Lückenfüllung. Gate 0 glättet nicht. Wenn ein Pflichtfeld fehlt, stoppt es. Es erfindet keinen Standardwert. Es schließt keine Lücken. Keine KI Entscheidung. Gate 0 wendet deterministische Regeln an. Wo eine Eingabe mehrdeutig ist, dokumentiert Gate 0 die Mehrdeutigkeit und stoppt. Es versucht nicht, sich für eine Interpretation zu entscheiden.

Drei Beispiele für Gate 0.

Beispiel 1, gut durchlaufende Eingabe. Eine Anfrage kommt mit vollständig ausgefüllten Pflichtfeldern. LEI 5299, Transaktionsname, Transaktionstyp, Quelle System Transaktions Feed, NTP verankerter Zeitstempel. Gate 0 kanonisiert die Eingabe und berechnet den Hash. Es prüft alle Pflichtfelder, vollständig. Es verifiziert den LEI gegen GLEIF, Entität aktiv, GLEIF Snapshot Version vorhanden, GLEIF Hash vorhanden. Es dokumentiert die Quelle. Es prüft den NTP Zeitanker, gesetzt. Es gibt keine mehreren Quellen, also kein Divergenz Schritt. Gate 0 durchläuft erfolgreich. Das Gate 0 Ergebnis steht zur Verfügung, und die nachgeordneten fachlichen Gates können arbeiten.

Beispiel 2, stoppende Eingabe. Dieselbe Anfrage, aber der LEI ist ungültig. Gate 0 kanonisiert die Eingabe, stellt fest, dass die Pflichtfelder vollständig sind, verifiziert den LEI gegen GLEIF, LEI nicht gefunden. Gate 0 stoppt. Ein Vorlauf Protokoll wird erzeugt mit dem Eintrag, Schritt 3 fehlgeschlagen, LEI nicht verifizierbar. Keine Receipt erzeugt. Grund, eine forensische Receipt ohne verifizierte Entität ist nicht belastbar. Es gibt keinen Receipt, und es gibt keine fachliche Prüfung. Das ist kein Gesichtspunktensystem, es sind die Bedingungen, ohne die das System nicht arbeitet.

Beispiel 3, divergente Eingabe. Eine Sport Szene mit zwei Kamera Perspektiven, deren Daten einige, aber nicht alle Parameter übereinstimmend liefern. Gate 0 kanonisiert die Eingabe, stellt fest, dass die Pflichtfelder vorhanden sind, verifiziert die sekundäre Identifikation, dokumentiert die Quelle, prüft den NTP Zeitanker und prüft die mehreren Quellen auf Divergenz. Die zwei Kamera Feeds sind übereinstimmend für die Geschwindigkeit, divergent für die Kontaktrichtung. Gate 0 dokumentiert die Divergenz. Das Gate 0 Ergebnis wird mit einer Markierung divergent im Vorlauf Protokoll versehen. Ein nachgeordnetes fachliches Gate kann diese Markierung interpretieren. Etwa kann es eine vertiefte Prüfung veranlassen oder ein Racing Incident nahelegen. Aber die Divergenz ist nicht stillschweigend zugunsten einer Quelle entschieden. Sie ist dokumentiert. Eine forensische Nachprüfung später sieht, diese Eingabe war divergent, und diese Divergenz wurde im Vorlauf festgehalten.

Wie Gate 0 mit dem Rest zusammenhängt. Gate 0 ist das Vor Gate aller fachlichen Gates. Keine Receipt ohne Gate 0. Keine fachliche Prüfung ohne Gate 0. Kein Verfahren ohne Gate 0. In der Schichtung der Pipeline ist Gate 0 der Punkt, an dem die forensische Belastbarkeit aller nachfolgenden Ebenen entscheidet. Gate 0 ist also nicht noch ein Baustein, sondern die begründende Bedingung der gesamten Pipeline.

Gate 0 ist auch der Punkt, an dem die Entitäts Identität als verifiziert hinterlegt wird, eine Eigenschaft, die CRPG zwingend benötigt. Eine Querschnittsanalyse ohne verifizierte Entität ist wertlos. Gate 0 ist damit nicht nur formal nachgeordnet, sondern funktional. Es ist die Stelle, an der die forensische Zulässigkeit und die Entitätsverifikation feststehen, bevor irgend etwas fachlich geschehen darf.

Erweiterung. Gate 0 ist nicht starr, aber es ist bindend. Die sechs Prüfungen können je nach Sektor ergänzt werden. Ein Sektor, der zusätzliche Pflichtfelder verlangt, kann Gate 0 erweitern. Aber die Kernpflichten, Kanonizität, Vollständigkeit, Entitätsverifikation, Quellensicherheit, Zeitanker, Divergenz, sind nicht verhandelbar. Sie sind das Fundament, auf dem alles steht. Wer eine davon aufgibt, gibt die forensische Belastbarkeit auf.

Kapitel 14: Die zwei Verifikationsklassen

Dies ist der Punkt, an dem das System die Linie zwischen wir behaupten es und unabhängig nachprüfbar zieht. Diese Linie verläuft mitten durch die kryptografische Architektur.

Klasse 1, interne Kettenintegrität, HMAC. Die erste Verifikationsklasse ist der HMAC, ein Message Authentication Code auf der Basis einer Hash Funktion, SHA 256. HMAC ist eine symmetrische Kryptografie. Eine Gruppe von beteiligten Parteien teilt vorab ein Geheimnis, den sogenannten Schlüssel. Werden Receipts erzeugt, werden sie mit diesem Schlüssel signiert. Wer denselben Schlüssel besitzt, kann die Signatur nachrechnen und feststellen, dass die Receipt unverändert aus dem erzeugenden System stammt.

Warum es existiert, im Lichte von Szenario 7. Szenario 7 beschrieb ein veränderliches Audit Log, dessen nachträgliche Änderungen niemand nachrechnen konnte. Die append only Merkle Kette mit HMAC ist das Gegenmodell. Die Kette wird in jedem Schritt verlängert. Jede neue Receipt referenziert den Hash der vorherigen, kombiniert beide und berechnet einen Merkle Link, der als Verkettung in der Receipt hinterlegt wird. Eine Receipt kann im Nachhinein nicht verändert werden, ohne die Hashkette zu brechen, und die Brechung ist mit dem gemeinsamen Schlüssel nachprüfbar.

Wie es zusammenhängt. Diese Klasse deckt das interne Beweisbedürfnis ab, also das Nachweisen, dass die Infrastruktur nicht manipuliert wurde. Sie ist nach innen gerichtet, nicht nach außen. Streng genommen gilt sie nur dort, wo der gemeinsame Schlüssel sicher verteilt werden kann, und sie kann das Problem des empfangenden Prüfers, der solchen Schlüssel nicht hat, nicht lösen.

Klasse 2, portable, extern verifizierbare Signatur, ECDSA P256 mit Post Quantum Migrationspfad. Die zweite Verifikationsklasse ist die asymmetrische Signatur. Ein Schlüsselpaar mit einem privaten und einem öffentlichen Schlüssel. Der private Schlüssel signiert, der öffentliche Schlüssel verifiziert. Konkret kommt heute ECDSA P256 zum Einsatz, eine Elliptic Curve Signatur auf der NIST P 256 Kurve. Es existiert ein dokumentierter Migrationspfad auf eine hybride Signatur aus ECDSA P256 plus ML DSA 65, der Post Quantum Signatur aus FIPS 204, sobald eine zertifizierte Bibliothek zur Verfügung steht.

Warum es existiert, im Lichte von Szenario 9. Szenario 9 beschrieb einen empfangenden Prüfer ohne Vorbeziehung, der ein Ergebnis entweder blind vertrauen oder ablehnen musste, weil Nachrechnen nicht möglich war. Die asymmetrische Kryptografie löst das. Die Verifikation durch eine dritte Seite, die den gemeinsamen Schlüssel nicht besitzt und vorher nichts mit dem erzeugenden System zu tun hatte. Eine Kanzlei, ein Gericht, ein Prüfer, ein Aufsichtsorgan des empfangenden Instituts. All diese Parteien können ein portables Artefakt prüfen, indem sie den öffentlichen Schlüssel verwenden, um die Signatur über die Daten nachzuprüfen. Nichts zu dieser Verifikation gehört zu einer laufenden Verbindung, keine andauernde Vertrauensbeziehung, kein geteiltes Geheimnis. Das ist die Grenze. HMAC sagt vertraue mir an dieser Stelle. ECDSA sagt prüfe es selbst.

Wie es zusammenhängt. Die asymmetrische Signatur ist die Klasse, die genau dann in Erscheinung tritt, wenn ein Artefakt die eigene Infrastruktur verlässt. Intern reicht die HMAC Klasse. Für das portable Artefakt, das an einen Empfänger übergeben wird, kommt die ECDSA Klasse zum Einsatz. Die beiden

Klassen sind strikt getrennt. Jede hat ihren eigenen Teil im Verification Block des SCP 1.0 Artefakts, und jede hat ihre eigene semantische Bedeutung. Mehr noch, das System bettet den öffentlichen Schlüssel direkt im portablen Artefakt ein, so dass dieses vollständig selbsttragend ist, und der Prüfer kann zusätzlich gegen den öffentlich veröffentlichten Schlüssel abgleichen. Damit schließt das System eine Angriffsmöglichkeit, die andernfalls bestehen würde. Dass ein Dritter einen eigenen öffentlichen Schlüssel im Artefakt einsetzen würde und damit eine falsche Gültigkeit erzeugen würde.

Beispiel. Eine CertifiedReceipt entsteht intern. Sie trägt eine HMAC Signatur. Die ausstellende Bank und der eigene Audit Service teilen den HMAC Schlüssel. Beide können die Signatur nachrechnen. Das Artefakt verlässt die interne Umgebung nicht. HMAC ist die ausreichende Signaturklasse.

Jetzt wird dieselbe Receipt an eine Empfängerkanzlei übergeben, die keine Vorbeziehung zum System hat, und die eine eigene forensische Prüfung vornimmt. HMAC reicht hier nicht. Die Kanzlei hätte den gemeinsamen Schlüssel, der die Eigenschaft zerstört, dass die Signatur nur dem erzeugenden Kreis bekannt ist. Die Konsequenz wäre, die Kanzlei kann zwar die Signatur prüfen, aber nicht, ob sie vom erzeugenden System stammt oder ob sie von jedem stammt, der den Schlüssel hat, und die Kanzlei kann das mit gesundem Zweifel versehen.

Die Lösung. Das Artefakt, das die eigene Infrastruktur verlässt, bekommt zusätzlich eine asymmetrische Signatur, die mit einem privaten Schlüssel signiert ist, den ausschließlich das System in einem gesicherten, serverseitigen Kontext hält. Die Kanzlei bekommt den öffentlichen Schlüssel, eingebettet im Artefakt und zusätzlich über einen öffentlichen Endpunkt veröffentlicht, und kann die Signatur verifizieren, ohne jemals einen gemeinsamen Schlüssel gehabt zu haben. Das ist der Übergang. HMAC bedeutet vertraut. ECDSA bedeutet prüfbar.

Der entscheidende Unterschied, ausdrücklich. Nur die asymmetrische Signatur erlaubt einem Dritten, der nie zuvor Kontakt zum System hatte, eine Prüfung ohne geteiltes Geheimnis. Das ist die exakte Grenze zwischen wir behaupten es und es ist unabhängig nachprüfbar. Wer den Unterschied zwischen den beiden Klassen verstanden hat, hat verstanden, warum es nicht reicht, eine Receipt nur mit einem HMAC zu versiegeln. Eine solche Receipt mag intern intakt sein, aber sie ist nicht portabel, nicht extern prüfbar und kann ein auswärtiges Prüfbedürfnis nicht befriedigen.

Kapitel 15: Post Quantum Kryptografie und die Wahl des hybriden Ansatzes

Was es ist. Post Quantum Kryptografie umfasst kryptografische Verfahren, die als resistent gegen Angriffe durch Quantencomputer gelten. Die relevanten Standards sind FIPS 203, ML KEM, Schlüsselaustausch, FIPS 204, ML DSA 65, eine modul gitter basierte Digitale Signatur, und FIPS 205, SLH DSA, eine hash basierte alternative Signatur. ML DSA 65 ist die Variante, die von der Standardisierung als Verfahren zur Signatur ausgewählt wurde.

Warum die Hybridwahl. Eine vollständige Migration von ECDSA auf ein reines Post Quantum Verfahren ist heute nicht ratsam, weil die Post Quantum Verfahren noch relativ neu standardisiert sind, ihre Implementierungen in der Praxis noch nicht lange ausbelastet sind, und einige ihrer Sicherheitsannahmen noch nicht so gut etabliert sind wie die klassischer Elliptic Curve Verfahren. Eine

hybride Signatur, also ECDSA P256 plus ML DSA 65, kombiniert die getestete Stärke des klassischen Verfahrens mit der künftigen Quantenresistenz des neuen Verfahrens. Die Signatur gilt, solange mindestens eines der beiden Verfahren hält. Dieser Ansatz ist auch das, was nationale Standardisierungsinstitute in ihren Post Quantum Migrationsleitlinien empfehlen.

Wie es zusammenhängt. Die heute gültigen ECDSA Signaturen bleiben gültig. Die Post Quantum Schicht ist additiv. Eine künftige Version des Portabilitäts Blocks, die die ML DSA 65 Komponente enthalten wird, wird folgenden Verification Block ergeben. Einen klassischen ECDSA Anteil und einen Post Quantum Anteil, die der Prüfer einzeln und gemeinsam überprüft. Das genaue Verfahren und die Zertifizierung der Integration befinden sich noch in Arbeit. Ein Zeitpunkt ist nicht versprochen.

Erweiterung. Die Post Quantum Frage ist keine Zukunftsmusik, sondern eine Frage, die heute entschieden werden muss, weil Receipts, die heute erzeugt werden, in Jahren verifizierbar sein sollen. Wer heute nur ECDSA signiert, und in zwanzig Jahren steht ein Quantencomputer, dessen Signaturen sind angreifbar. Wer heute hybrid signiert, dessen Signaturen bleiben gültig, weil die Post Quantum Schicht hält. Das System entscheidet sich heute für den Migrationspfad, um in zwanzig Jahren noch Beweise zu haben, nicht um heute einen Marketingvorteil.

Kapitel 16: External Validation Record und die Zwei Achsen Logik

Das ist das wichtigste Prinzip im System.

Die zwei Achsen. Jedes forensische Artefakt im System hat, formalisiert im SCP 1.0 Datenmodell, zwei unabhängige Eigenschaften, die niemals miteinander vermengt werden.

Achse 1, technische Integrität. Diese Achse ist ausschließlich eine kryptografische Feststellung. Wurde das Artefakt in der erzeugenden Pipeline vollständig und kryptografisch versiegelt. Stimmen alle Hashes, alle Merkle Links, alle Signaturen. Diese Prüfung ist unabhängig vom fachlichen Ergebnis des Artefakts. Ein Artefakt, das ein BLOCK Ergebnis hat, die Pipeline hat eine Transaktion blockiert, weil eine Sanktionsliste getroffen wurde, ist genauso intakt wie ein Artefakt, das ein CLEAR Ergebnis hat. Integrität ist eine Eigenschaft der Form, nicht des Ergebnisses.

Achse 2, gerichtsfest. Diese Achse wird ausschließlich durch eine versiegelte, extern ausgestellte External Validation Record gesetzt. Ein solcher Record ist eine Validierungsurkunde, die von einer unabhängigen Kanzlei oder einer Prüfstelle ausgestellt wird. Das System selbst kann diese Achse niemals setzen.

Der Kernsatz, der das System am tiefsten beschreibt, lautet:

> ***Das System kann sich nicht selbst für gerichtsfest erklären.***

Warum diese Trennung existiert. Diese Trennung liegt eine harte Lehre aus der Compliance Geschichte zugrunde. Es ist die Versuchung eines jeden Systems, die Selbstaussagen zu erhöhen. Wir sind kryptografisch versiegelt, also ist das gerichtsfest. Der Irrtum in dieser Aussage ist derjenige, dass technische Integrität und gerichtsfester Beweiswert zwei verschiedene Achsen sind. Technische

Integrität beweist, dieses Artefakt ist nicht manipuliert und reproduzierbar. Gerichtsfester Beweiswert beweist, dieses Artefakt kann in einem konkreten gerichtlichen oder aufsichtlichen Verfahren als Beweis vorgelegt werden, weil seine Methode, seine Quelle, seine Verwahrungsdokumentation von einer unabhängigen Stelle begutachtet und anerkannt wurde. Kein Schritt in der ersten Achse führt automatisch zum zweiten.

Das System trennt diese Achsen deshalb hart, weil nur so die nächste Eigenschaft gesichert ist. Dass ein BLOCK Artefakt genauso intakt ist wie ein CLEAR Artefakt. Würden technische Integrität und gerichtsfest zusammengefasst, entstünde eine Versuchung, das System in Richtung einer vorteilhaften Selbstaussage zu konfigurieren, und diese Versuchung schafft Risiken. Das System muss neutral zwischen BLOCK und CLEAR sein.

Beispiel. Eine CertifiedReceipt hat die technische Integrität bestätigt. Alle Hashes, alle Merkle Links, alle Signaturen intakt. Die fachliche Eingabe hat ein BLOCK Ergebnis. Eine Transaktion wurde blockiert, weil die Entität sanktionsrelevant war. Achse 1 gilt. Achse 2, gerichtsfest, gilt nicht, weil es noch keine versiegelte External Validation Record von einer unabhängigen Kanzlei gibt. Die Receipt ist forensisch belastbar, sie ist intakt, reproduzierbar, ihre Entstehung ist nachvollziehbar, sie ist aber noch nicht gerichtsfest, weil vor Gericht die Methode, die Datenerhebung, die Kette der Verwahrung noch nicht begutachtet wurden.

Eine Kanzlei wird beauftragt. Sie begutachtet die Methode, die Datenerhebung und die Kette. Sie stellt eine External Validation Record aus. Methode X ist auf die Eingabedaten angewendet worden. Diese Methode ist im forensischen Rahmen zulässig. Die Datenerhebung ist nachvollziehbar. Der Record wird versiegelt, hinterlegt, in die Merkle Kette der Records eingefügt, und referenziert die entsprechende CertifiedReceipt. Jetzt hat die Receipt die Achse 2 bestätigt, referenziert über den Record. Technische Integrität wurde niemals vermischt. Die beiden Achsen blieben separat, und die zweite Achse wurde ausschließlich von einer externen, unabhängigen Stelle gesetzt.

Wie es zusammenhängt. Die External Validation Record ist ein Artefakt für sich. Sie ist selbst versiegelt, hash verankert und Merkel verkettet. Im SCP 1.0 Artefakt referenziert die zweite Achse den Record über seine ID und seinen Hash. Ohne solche Referenz ist die Achse schlichtweg nicht gesetzt, egal wie intakt das Artefakt ansonsten ist. Jede Setzung der Achse zwei dokumentiert, von wem sie stammt und wann. Auf diese Weise ist der einfache technische Link intakt nicht die mündliche Urkunde eines juristisch gültigen Beweises. Die beiden haben unabhängig voneinander Bestand und werden in Zusammenarbeit geprüft.

Erweiterung. Die External Validation Record hat eine Gültigkeitsdauer. Eine Kanzlei, die eine Methode heute begutachtet, begutachtet sie für die Fassung von heute. In fünf Jahren kann die Methode weiterentwickelt sein, und die Begutachtung muss erneuert werden. Das System dokumentiert die Gültigkeitsdauer im Record. Ein Receipt, der heute auf einen Record verweist, referenziert einen gültigen Record. Ein Receipt, der in sechs Jahren auf denselben Record verweist, referenziert einen abgelaufenen Record. Das System lügt nicht über die Gültigkeit. Es dokumentiert, wann die Gültigkeit beginnt und wann sie endet.

Kapitel 17: CRPG, die Querschnittsebene

Was CRPG ist. CRPG, Cross Receipt Pattern Gate, ist eine zusätzliche Beobachtungsebene, die quer zu den einzelnen Receipts liegt. Wo eine klassische Prüfung fragt, ist dieser einzelne Vorgang über dem Schwellenwert, fragt CRPG, liegt über die letzten Vorgänge einer Entität ein Muster vor, das Structuring, Stückelung, sein könnte.

Warum CRPG existiert, im Lichte von Szenario 6. Szenario 6 beschrieb eine Entität, die über neun Monate vierzehn Vorgänge unter dem Schwellenwert führte, und die in jeder Einzelfallprüfung unauffällig blieb, weil niemand über die Vorgänge hinweg schaute. Die strukturelle Lücke, die CRPG schließt, ist genau die Lücke der reinen Einzelfallprüfung. Eine Einzelfallprüfung prüft jeden Vorgang isoliert. Ein einzelner Vorgang unter dem Schwellenwert ist fachlich unauffällig, also nicht meldepflichtig, also nicht dokumentationswürdig. Aber die Struktur, die eine bewusste Stückelung einer größeren Summe ausmacht, liegt gerade nicht im einzelnen Vorgang, sondern im Querschnitt. Anti Structuring Vorschriften existieren, weil diese Querschnittsanforderung sehr real ist, und kein klassisches Einzelfall Werkzeug ist gebaut, um sie zu bearbeiten.

Rechtliche Verankerung. Paragraph 261 StGB, Geldwäsche, Geldwäschegesetz, FATF Recommendation 1, in den USA 31 USC Section 5324, Structuring Verstoß gegen die Pflicht zur Währungs Transaktionsberichterstattung. Ein wichtiger Hinweis. Einige dieser Einzelzitate sind eingeführt. Vor einer externen Veröffentlichung sollten sie gegen die aktuelle Fassung des Originaltextes geprüft werden.

Die Architektur. CRPG ist eine nicht verändernde Erweiterung der bestehenden Receipt Kette. Das bedeutet. CRPG ändert an den vorhandenen Receipts nichts. Es liest abhängig über die bereits erzeugte Receipt Historie. CRPG ersetzt weder die Einzelfallprüfung noch den Menschen. Es ist eine zusätzliche Beobachtungsebene, die ein kryptografisch versiegeltes CRPGPatternReceipt erzeugt, das angibt, dass ein beobachtetes Muster vorliegen könnte. CRPG ist an die Entitätsidentität gebunden. Vor jedem Quervergleich muss die Identität der Entität, bevorzugt über den LEI, verifizierbar sein. Zwei Vorgänge, die einen ähnlichen Namen aber unterschiedliche Entitäten beschreiben, würden sonst eine falsche Pattern Wolke bilden. Deshalb setzt jeder Vergleich eine erfolgreiche Entitäts Auflösung voraus. Genau hier ist die Gate 0 Bedingung maßgeblich. Ohne Gate 0 gibt es keine verifizierte Entität. Ohne verifizierte Entität hat CRPG kein Fundament.

Single Sector gegen Cross Sector. Zwei Pattern werden unterschieden. Ein Single Sector Pattern, das innerhalb einer Sektor Erhebung auffällt, etwa mehrere Vorgänge in einer Bank, alle knapp unter dem Bank Meldepflicht Schwellenwert, und ein Cross Sector Pattern, das erst im Querschnitt über mehrere Sektoren hinweg erkennbar wird, etwa Vorgänge über Bank, Immobilien und Wealth Management, die für sich nur sektorspezifisch sind, aber in der Summe ein Structuring Muster bilden. Das Cross Sector Signal ist stärker. Es ist auch seltener. Es ist auch technisch anspruchsvoller, da es Daten aus Karten erfordert, die traditionell nicht miteinander reden.

Beispiel. Eine Entität führt über neun Monate 14 Vorgänge durch, jeder einzeln unter dem Bank Meldepflicht Schwellenwert. Die Banken Compliance prüft jeden Vorgang einzeln und sieht, jeder Vorgang unauffällig. CRPG läuft über die 14 Vorgänge und findet, die Vorgänge sind allesamt knapp unter

dem Schwellenwert, zeitlich geclustert, und die Summe übersteigt den Schwellenwert nach einem Multiplikator. CRPG erzeugt ein CRPGPatternReceipt, das das beobachtete Muster dokumentiert. Der Compliance-Officer bewertet das Muster und entscheidet, nicht meldepflichtig oder meldepflichtig. CRPG fällt keinen Meldebescheid, sondern legt eine Beobachtung vor.

Ein Cross Sector Beispiel. Fünf Vorgänge an einer Bank, vier an einem Wealth Manager, drei an einem Immobilien Transaktionsvermittler. Erst die Querschnittsanalyse über die drei Sektoren ergibt ein Structuring Muster, das an jeder einzelnen Stelle sektorspezifisch unauffällig geblieben wäre.

Was CRPG nicht tut. CRPG fällt keinen automatisierten Sanktionsausspruch. Das CRPGPatternReceipt ist eine Beobachtung, kein Meldebescheid. Die Entscheidung, ob das Beobachtungsmuster eine Meldepflicht auslöst, ob eine Meldung folgt, ob Behörden eingeschaltet werden, bleibt bei dem Compliance-Officer, der das Muster bewerten wird, mit der Unterstützung des Receipts.

Erweiterung. CRPG ist ein erster Schritt in eine Welt, in der nicht mehr der einzelne Vorgang zählt, sondern das Muster. Die Aufsichtspraxis bewegt sich in diese Richtung. AMLA, die europäische AML Aufsicht, beginnt, Querschnittsanalysen zu fordern, nicht mehr nur Einzelfallmeldungen. Wer heute CRPG hat, hat einen Beobachtungsraum, den andere sich erst aufbauen müssen. Und der Beobachtungsraum wächst mit jedem Jahr, weil jedes Jahr neue Receipts zur Historie kommt. Ein Institut, das heute mit CRPG beginnt, hat in drei Jahren drei Jahre Musterhistorie. Ein Institut, das in drei Jahren beginnt, hat null.

Fünfter Teil: Die Sektor Engines

Jeder Sektor bekommt hier einen eigenen Abschnitt, der erklärt, was die Engine prüft, ein Beispiel, was bei der Konkurrenz anders ist, und die Frage, was dem Sektor verloren geht, wenn er längere Zeit weiterhin darauf verzichtet.

Kapitel 18: Banken und Finanzdienstleistung

Was die Engine prüft. Basel III Eigenkapitalanforderungen, MiFID II Eignung, DORA betriebliche Widerstandsfähigkeit, AML Pflicht nach dem Geldwäschegesetz und die Standard Gate Pipeline, GLEIF, Sanktionen, Grundrechte.

Beispiel. Ein Kreditinstitut prüft eine Kreditgewährung an eine Firmengruppe. Der Compliance-Lauf erzeugt CertifiedReceipts für LEI Verifikation der Gruppe und aller Töchter, Sanktionsprüfung aller Beteiligten, AML Prüfung des Vorgangs, Basel III Konsolidierungsauswirkung auf die Eigenkapitalquote des Instituts. Alle Ergebnisse in einer SCP 1.0 konformen Kette. Ein Jahr später, im Falle einer Aufsichtsprüfung, kann der Prüfer die Receipts exakt gegen die damals geltenden Regelkatalogversionen nachrechnen.

Was die Konkurrenz anders macht. Banken Compliance-Werkzeuge produzieren Berichte. Sie produzieren fast nie kryptografisch verkettete Receipts mit versions und hashverankerter Regelbasis. Die Aufsichtsprüfung ist zünftiges PDF. Ein Auditor, der die Regellage damals nachrechnen will, kann das nicht, weil die Regelbasis damals nicht hashverankert war, sondern als aktuell geltend angewandt wurde.

Die Konsequenz bei einer Nachprüfung. Er muss sich auf die Compliance-Abteilung verlassen, dass sie die richtige Regel angewendet hat. Er kann es nicht nachrechnen.

Was hier anders gemacht wird. Es bindet die Regelbasis, Basel III, MiFID II, Außenwirtschaftsgesetz, Geldwäschegesetz, in versionsverankerte Regelkataloge ein, deren Hash im Receipt steht. Die Nachrechenbarkeit ist nicht gut gemeint, sondern kryptografisch erzwungen.

Was dem Sektor verloren geht, wenn er längere Zeit weiterhin darauf verzichtet. Institut A hat diese Architektur und kann einer Aufsicht erklären, unsere Compliance Ergebnisse sind kryptografisch nachrechenbar. Die Regellage, die wir damals angewendet haben, ist im Receipt hashverankert. Institut B, das diese Architektur noch nicht einführt, erklärt weiterhin mit PDF und Compliance-Abteilungsnotiz. In einer Aufsichtsprüfung mit drei Jahren Nachschau kann die Aufsicht zwischen einem Institut, das nachrechenbar ist, und einem Institut, das behauptet, dasselbe angewandt zu haben, zunehmend differenzieren. Der erste, der diese Architektur hat, bekommt eine Aufsichtslage, die die anderen sich schwer erarbeiten können. Weil die nachrechenbare Kette eines Instituts, das bereits drei Jahre Receipts hat, nicht mit einem PDF Archiv vergleichbar ist. Und diese Spannung wird in den nächsten ein bis drei Jahren zunehmen, weil die Aufsichtspraxis selbst beginnt, kryptografische Nachrechenbarkeit nicht mehr als Bonus, sondern als Mindestanforderung zu betrachten.

Kapitel 19: Versicherungen

Was die Engine prüft. Solvency II Solvenzkapitalanforderungen, IDD Verhaltenspflichten, AML Pflicht, Grundrechtsberührung, Sanktionsprüfung.

Beispiel. Eine Lebensversicherung mit einem angesparten Vermögen prüft bei einer Auszahlung im Todesfall die Identität des Bezugsberechtigten, die Sanktionswürdigkeit der Bezugsberechtigten, die Solvenzkapitalauswirkung der Auszahlung und ob die Auszahlung mit den IDD Verhaltenspflichten bei der Anlage des verbleibenden Vermögens übereinstimmt. Alle vier Prüfungen als Receipt Set. Nach zehn Jahren kann ein Forensiker nachrechnen, dass die Auszahlung den damaligen Solvency II Anforderungen entsprach.

Was die Konkurrenz anders macht. Versicherungs Compliance-Werkzeuge sind lokal pro Vertrag geführt. Die Verbindung zwischen IDD Verhaltenspflicht, Solvency II Kapitalauswirkung und AML ist nicht in einer gemeinsamen Kette, sondern in drei isolierten Werkzeugen, die drei verschiedene Audits erzeugen, und die nach zehn Jahren in drei isolierten Notizen stehen.

Was dem Sektor verloren geht. Versicherer A hat die Auszahlungsentscheidung in einer Receipt Kette. Versicherer B hat drei Notizen, die nicht miteinander verwandtschaftsverknüpft sind. Im Versicherungsfall bei Uneinigkeit über die IDD Pflicht kann Versicherer A nachweisen, dass IDD, Solvency II und AML auf der gleichen Entität, zum gleichen Zeitpunkt, mit der gleichen Eingabeentscheidung gekoppelt geprüft wurden. Versicherer B hat drei isolierte Notizen. Wer von beiden in einer Versicherungsaufsicht besser darsteht, ist eine Frage der Methode, nicht der Compliance-Anstrengung. Und Versicherungsakten sind langlebig. Eine Lebensversicherung, die heute abgeschlossen wird, kann in dreißig Jahren einen Auszahlungsfall haben. Wer heute beginnt, eine Receipt Kette zu bauen, hat in

dreißig Jahren eine nachrechenbare Auszahlungsentscheidung. Wer das heute nicht tut, hat in dreißig Jahren eine Versicherung und eine Notiz.

Kapitel 20: M&A, Live Due Diligence

Was die Engine prüft. Sechs Prüfdimensionen, sieben Prüfschritte. Das Ausgabe Artefakt heißt MaDDReceipt. Die Schritte sind. AML KYC beidseitig. Beneficial Ownership. FDI Screening. Kartellrecht. Sanktionen. Grundrechtsprüfung. Jurisdiktionskonflikte.

Beispiel. Ein Private Equity Fonds prüft den Kauf einer Industrie Gruppe mit Töchtern in Deutschland, Italien und einer US Beteiligung. Die Engine erzeugt für jeden Prüfschritt eine Receipt. AML KYC für den Fonds als Käufer und die Gruppe als Verkäufer, Beneficial Ownership für alle wirtschaftlich Berechtigten in jeder Jurisdiktion, FDI Screening für jede der drei Jurisdiktionen, Außenwirtschaftsgesetz in Deutschland, Golden Power in Italien, CFIUS in den USA, Kartellprüfung, Sanktionsprüfung, Grundrechtsprüfung und Jurisdiktionskonflikt Prüfung. Am Ende steht ein MaDDReceipt, der das gesamte Bild forensisch festhält.

Was die Konkurrenz anders macht. Traditionelle Due Diligence ist werkzeuggekauft. Ein Beneficial Ownership Werkzeug, ein AML Werkzeug, ein Kartell Werkzeug, ein FDI Werkzeug. Die Einzelergebnisse sind PDFs. Die Synthese ist eine händische Zusammenfassung der Berater. Nach drei Jahren, wenn eine transaktionsrechtliche Auseinandersetzung entsteht, stehen PDFs und Notizen, keine verkettete Kette.

Was dem Sektor verloren geht. Käufer A hat die Ergebnisse in einer forensischen Kette. Jede Receipt referenziert die Regelversion und das Datum. In einer Auseinandersetzung nach drei Jahren über eine angeblich übersehene Sanktionsberührung einer Tochter kann Käufer A nachweisen, dass am damaligen Datum gegen die damals geltende Sanktionsliste geprüft wurde, und dass die Tochter nicht enthalten war. Käufer B, der Sanktionsliste damals als PDF behauptet, muss sich auf die Aussage der Berater verlassen, dass die damals richtige Liste geprüft wurde, und diese Aussage hat keine forensische Kette. Eine M&A Auseinandersetzung mit dreistelligem Millionenbetrag vor Gericht kommt nicht darauf an, wer behauptet, sondern wer nachweisen kann. Wer nachrechenbare Due Diligence hat, hat hier einen materiellen Vorteil.

Kapitel 21: Immobilien

Was die Engine prüft. Beneficial Ownership der Vertragsparteien, Source of Funds Vorprüfung, Sanktionsprüfung, Grundrechtsberührung, insbesondere das Eigentumsgrundrecht, Außenwirtschaftsprüfung bei ausländischem Erwerb, AML Prüfung nach dem Transaktionsvolumen.

Beispiel. Ein ausländischer Investor kauft eine Büroimmobilie in Frankfurt. Die Quelle der Gelder ist durch einen Source of Funds Workflow dokumentiert, der wirtschaftlich Berechtigte des Investors wird ermittelt, Sanktionsprüfung wird auf den Berechtigten angewendet, die Außenwirtschaftsprüfung klärt, ob die Transaktion dem FDI Screening unterliegen könnte. Alle Receipts in einer Kette. Der Notar kann die Kette in der Urkunde referenzieren.

Was die Konkurrenz anders macht. Immobilien Compliance ist oft eine einzelne Liste, die in den Notar Workflow eingebaut wird. Die Geldquelle ist eine Versicherung des Käufers, der wirtschaftliche Berechtigte eine eidesstattliche Erklärung. Sanktionsprüfung ist ein Abgleich gegen eine vielleicht veraltete PDF Liste. Nach Jahren, im Fall einer Verwertungs oder Steuerstraf Auseinandersetzung, gibt es Notiz und Versicherung, aber keine kryptografische Kette.

Was dem Sektor verloren geht. Immobilien Transaktionen sind langlebig wie keine andere Anlage. Die dreijährige Nachschau ist bei Immobilien die zehnjährige Nachschau. Wer heute beginnt, eine Receipt Kette zu bauen, hat in zehn Jahren eine schiere Menge an nachrechenbaren Transaktionen, und die Aufsicht und die Forensik in einer Welt, in der Immobilien zunehmend grenzüberschreitend erworben werden, werden nachvollziehbare Quellen brauchen. Der erste Notar Verbund, der mit einer solchen Architektur arbeitet, hat eine andere Vorlageform für die notarielle Beurkundung als der, der jede Transaktion einzeln in PDF Dokumenten hält. Und wenn der erste Aufsichtsentscheid fällt, der kryptografische Nachrechenbarkeit einer notariellen Beurkundung als Mindestanforderung setzt, wird der Verbund, der heute beginnt, diese Kette zu bauen, derjenige sein, der diesen Entscheid erfüllt.

Kapitel 22: Cloud und digitale Infrastruktur

Was die Engine prüft. DORA betriebliche Widerstandsfähigkeit, C5 und SOC2 Äquivalenz, ISO 27001 Referenz, ENISA Berichterstattungsbereitschaft, Post Quantum Re Attestierung, Cloud Act Konfliktprüfung.

Beispiel. Ein Cloud-Anbieter, der Compliance für europäische kritische Infrastruktur anbietet, führt die DORA Meldungsstruktur durch. Eine ICT Inzident Meldung wird mit einem Receipt dokumentiert, der die Klassifizierung des Inzidents, die betroffenen Kritikalitätsstufen und die anzuwendenden DORA Artikel referenziert.

Was die Konkurrenz anders macht. Cloud Compliance ist urkundenbasiert. Man zertifiziert das eigene System gegen einen Standard. Die Zertifizierung ist eine Urkunde, die jedes Jahr erneuert wird. Die einzelnen Meldungen stehen im Incident Response System, nicht in einer Compliance Kette.

Was dem Sektor verloren geht. Wer DORA mit einer Receipt Kette baut, kann dem Auditor morgen zeigen, jeder Inzident ist referenzierbar, jedes Meldeereignis hat eine Regelbasis, jeder Zustandsübergang ist nachvollziehbar. Wer DORA mit Incident Response Tickets baut, kann das nicht, und der DORA Auditor wird sehr bald nicht mehr nur nach Urkunden fragen, sondern nach der Nachrechenbarkeit einzelner Meldeereignisse. Die DORA Compliance als Urkunde ist die Vergangenheitsform. Die DORA Compliance als Receipt Kette ist die Zukunftsform.

Kapitel 23: Energie

Was die Engine prüft. Grundrechtsberührung des Energierechts, Renewable Energy Directives, Netzausbaubeschleunigungsgesetze, sektorspezifische Sanktionen, insbesondere Sanktionsfolgen bei Energieimporten, ESG Berichterstattung für Energieportfolios.

Beispiel. Ein Energieversorger prüft die Beschaffung vergangener Energieimporte auf Sanktionsberührung. Der Receipt dokumentiert, welche Sanktionsliste, in welcher Fassung, zu welchem Zeitpunkt angewendet wurde. Später, bei einer Nachprüfung der Beschaffungslage, ist nicht wir haben geprüft die Aussage, sondern die Receipt Kette, die alle Beschaffungsentscheidungen bis zum Sanktionslistenstand des jeweiligen Tages referenzierbar macht.

Was dem Sektor verloren geht. Energie ist heute der Sektor, in dem Sanktions Compliance am schärfsten ist, und zugleich der Sektor, in dem die Nachschaulage, Beschaffung im Sommer, Nachschau im Winter, sehr schnell zu einer fünf bis zehnjährigen Frage wird. Der erste Energieversorger, der seine Sanktionsentscheidungen über eine kryptografisch verkettete Kette dokumentiert, hat eine ganz andere Vorlage, wenn die Aufsicht den Einkauf der letzten drei Jahre nachrechnen will, als der, der aktuelle PDF Liste als Prüfgrundlage angegeben hat.

Kapitel 24: Sport, gateSport

Was die Engine prüft. FIFA Laws of the Game, Law 12, Fouls, Law 11, Abseits, Law 10, Spielausgang. Die Engine erzeugt SportDecisionReceipts. Toleranzkorridor und In Dubio Pro Reo als konzeptuelle Stellschrauben. Die genauen Schwellenwerte sind nicht veröffentlicht.

Beispiel. Eine Szene im Strafraum. Drei Kamera Perspektiven. Gate 0 prüft die Divergenz, das sportfachliche Gate wendet Law 12 an, klassifiziert die Indikation, Foul, kein Foul, strittig, dokumentiert die angewandte Law 12 Fassung und alle verwendeten Eingabedaten. Eine SportDecisionReceipt entsteht. Der Schiedsrichter kann die Indikation annehmen oder ablehnen. Die Ablehnung wird im Receipt mit begründet. Das ist ein kalibrierbarer Datensatz.

Was die Konkurrenz anders macht. VAR Werkzeuge produzieren Videos. Sie produzieren selten kryptografisch versiegelte Receipts. Die nachträgliche Kontrolle über eine VAR Entscheidung beruht auf Videowiedergabe und Stellungnahme der Schiedsrichter, nicht auf einer nachrechenbaren Receipt Kette.

Was dem Sektor verloren geht. Sportverbände befinden sich in einer Legitimationsfrage. Eine Gesellschaft, die die Transparenz des Schiedsrichterwesens zunehmend kritisch hinterfragt, wird in naher Zukunft forensische Nachrechenbarkeit einfordern, und ein Verband, der bereits eine solche Architektur hat, hat diese Frage auf eine elegante Weise beantwortet. Nicht mit der Behauptung, dass Schiedsrichter fehlerlos sind, sondern mit dem Beweis, dass jede Entscheidung, die heute fällt, in zehn Jahren nachrechenbar ist.

Kapitel 25: Motorsport, gateMotorsport

Was die Engine prüft. FIA International Sporting Code und analoge Regelwerke der Serien. Neun Gates M0 bis M8 für die motorsportspezifischen Vorfälle. Gate M9 zur BoP Referenzabweichung mit Windschatten Ausschluss, Persistenzprüfung, Windkorrektur, Luftdichtekorrektur nach SAE J1349, und Per Sektor Wettergranularität.

Die drei Schichten der Wetter Normalisierung im Detail. Eine Rundenzeit ist nicht direkt vergleichbar, weil Wind, Temperatur, Druck und Luftfeuchte sie beeinflussen. Wer BoP Abweichungen melden will, muss diese Einflüsse zuerst herausrechnen. Das System macht das in drei streng getrennten Schichten, die niemals zu einem einzigen Korrekturfaktor ausgemischt werden.

Erste Schicht, Verzicht auf Runden, die nicht unter trockenen Bedingungen stattfanden. Nasse oder feuchte Runden sind grip limited, nicht power limited. Sie eignen sich nicht für eine BoP Vergleichbarkeit und werden verworfen, nicht korrigiert. Diese Unterscheidung ist wichtig. Verwerfen heißt, die Runde zählt nicht. Korrigieren hieße, die Runde zählt mit Schätzung. Das System verwirft.

Zweite Schicht, Windvektorprojektion. Der Wind wird nicht als bloße Zahl abgezogen, sondern als Vektor gegen die jeweilige Sektor Fahrrichtung projiziert. Eine Windböe aus der Seite in einem Sektor, in dem geradeaus gefahren wird, hat einen anderen Effekt als die gleiche Böe in einem Sektor, in dem quer zur Windrichtung gefahren wird. Die Vektorprojektion rechnet diesen Effekt korrekt.

Dritte Schicht, Luftdichtekorrektur nach SAE J1349 und DIN 70020. Sie korrigiert die Leistungsabhängigkeit von Temperatur, Luftdruck und Luftfeuchte. Eine kältere Ansaugluft bedeutet mehr Sauerstoff pro Volumen und damit mehr Leistung. Diese Schicht ist physikalisch von der Windkorrektur unabhängig und wird strikt getrennt ausgeführt. Das System mischt keine Schätzungen in einen Fudge Faktor. Die Referenzbedingung ist 99 kPa trockene Luft bei 25 Grad Celsius, nach SAE J1349. Die Korrektur wird auf Basis der tatsächlichen Temperatur, des Drucks und der Luftfeuchte berechnet, mit einer korrekten Dampfkraftkorrektur nach der Magnus Formel, und als multiplikativer Faktor auf die Rundenzeit angewandt, nach der Windkorrektur, niemals zuvor.

Zusätzlich erlaubt das System zwei Wetter Granularitäts Modi. Im Modus Runde wird ein einheitlicher Wetterpunkt pro Runde verwendet, geeignet für Demo und kurze Strecken. Im Modus Sektor wird für jeden Sektor ein eigener Wetterpunkt verwendet, erforderlich für lange Strecken, auf denen die Windbedingungen in einem Sektor völlig anders sein können als in einem anderen. Eine Strecke wie die Nordschleife zwingt in dieser Frage geradezu in die Sektor Granularität, weil von der Döttinger Höhe bis zum Bergwerk meteorologisch verschiedene Welten liegen.

Jedes Receipt dokumentiert genau, welche Korrekturschichten angewandt wurden, mit welcher Methode und mit welcher Granularität. Damit ist der BoP Befund nachträglich vollständig reproduzierbar und nicht von einer stillen Annahme abhängig.

Beispiel. Im Laufe einer Langstrecke prüft Gate M9 die Sektorleistungen der Fahrzeuge. Ein Fahrzeug weicht in den leistungssensitiven Sektoren mehrfach von der BoP Referenz ab. Gate M9 prüft, ob die Abweichung im Windschatten eines anderen Fahrzeugs beginnt, wird ausgeschlossen. Prüft die Persistenz der Abweichung über ein Beobachtungsfenster, wird dokumentiert. Prüft die Wetterdaten, Windkorrektur angewendet, Luftdichtekorrektur angewendet, Per Sektor Granularität angewendet. Gate M9 erzeugt einen Receipt, BoP Referenzabweichung beobachtet, methodisch nachvollziehbar, der an den technischen Kommissar geleitet wird. Die Konsequenz ist eine Entscheidung des technischen Kommissars, nicht ein Urteil der Engine.

Was die Konkurrenz anders macht. BoP Systeme in Motorsport Serien sind serie intern und selten dokumentiert. Die Methodik der Abweichungsanalyse ist nicht öffentlich nachrechenbar. Nach einer Meisterschafts Entscheidung steht das Ergebnis, aber nicht die Methode, die dazu geführt hat.

Was dem Sektor verloren geht. Eine Serie, die gateMotorsport basiert arbeitet, kann nach einer strittigen Meisterschaftsentscheidung eine Receipt Kette vorlegen, die genau dokumentiert, welche Sektorwerte, unter welchen Wetterbedingungen, mit welcher Windschatten Ausschlusslogik, welcher Windkorrektur, welcher Luftdichtekorrektur und welcher Persistenz geprüft wurden. Eine Serie ohne diese Architektur kann das nicht. Der Forensik Wert in strittigen Meisterschaftsentscheidungen ist materiell. In einem Sport, dessen Legitimität zunehmend auf einer nachrechenbaren Methode beruhen wird, wird der erste Verband, der dies hat, einen diskursiven Vorteil haben.

Kapitel 26: Was systemweit anders gemacht wird

Eine gebündelte Aufstellung, die pro Mechanismus zeigt, was anders ist.

Der häufigste Unterschied ist ein kognitiver. Konkurrenz Werkzeuge dokumentieren Compliance. Hier wird sie kryptografisch bewiesen. Das ist kein Optik Unterschied. Es ist ein materieller Unterschied, aus dem alle anderen Differenzen folgen.

Die Konkurrenz arbeitet mit Wahrscheinlichkeit. Hier wird deterministisch geprüft. Die Konkurrenz arbeitet mit isolierten Werkzeugen. Hier wird in einer gekoppelten Kette gearbeitet. Die Konkurrenz arbeitet mit Audit Logs. Hier wird append only gearbeitet. Die Konkurrenz arbeitet mit PDF. Hier wird mit versiegelten Receipts gearbeitet. Die Konkurrenz behauptet Gerichtsfestigkeit. Hier wird die Gerichtsfestigkeit von einer externen Stelle gesetzt. Die Konkurrenz arbeitet mit KI, die entscheidet. Hier entscheidet die Regel, und die KI liest nur.

Sechster Teil: Die Grenzen, die dieses System sich selbst setzt

Kapitel 27: Governance Grenzen, systemweit einheitlich

Ein eigener Abschnitt, der für jedes Gate und jede Engine in diesem System die gleichen Grenzen zusammenfasst, weil sie so wichtig sind, dass sie prominent benannt werden müssen.

Erste Grenze. Kein automatischer Sanktionsausspruch, in keinem Gate, in keinem Sektor. Keine Engine, kein Gate und kein Receipt Typ in diesem System kann selbst eine Sanktion aussprechen. Eine Sanktion,

sei es eine Sportstrafe, eine Meldepflicht, eine Blockadentscheidung, ein Aufhebungsantrag, ist eine menschliche Entscheidung und wird von Menschen getroffen. Das System erzeugt forensische Evidenz, die von Menschen bei ihrer Entscheidung verwendet wird. Es ersetzt keine dieser Entscheidungen.

Beispiel. Ein Compliance-Officer lässt in einer Bank einen Vorgangsstapel laufen. Das System erzeugt eine CertifiedReceipt mit BLOCK Anlass, Sanktionsberührung. Das System kann nicht, und der Architektur nach niemals, eine automatische Freigabe des Vorgangs sperren. Das System erzeugt einen Receipt, der BLOCK dokumentiert. Die Freigabe Entscheidung bleibt beim Compliance-Officer, der den Receipt sieht. Das System ist ein Beweisgeber, kein Entscheider.

Zweite Grenze. Keine KI, die entscheidet. KI, wo im System eingesetzt, und sie ist in klar begrenzten Rollen eingesetzt, etwa in der Textextraktion, in der Quellenkonsolidierung, liest und klassifiziert, entscheidet nicht. Eine Regelentscheidung fällt auf eine deterministische Prüfung zurück, die nicht von Trainingsdaten, nicht von Model Updates und nicht von Konfidenzwerten abhängt. Das ist eine verdeutlichende Bedeutung. Eine Entscheidung, die von einer deterministischen Regel kommt, kann von der Gegenseite nachgerechnet werden. Eine Entscheidung, die aus einem Modell kommt, kann das nicht.

Beispiel. Wo KI die Adverse Media Klassifikation unterstützt, liest die KI Nachrichtenquellen und kennzeichnet eine Nachricht als potenziell relevant. Sie entscheidet nicht Adverse Media bestätigt. Eine solche Aussage kann nur die deterministische Regelklassifizierung ausgeben, die auf eindeutige Quelle und Datum referenzierbar ist.

Dritte Grenze. Jede Unsicherheit wird sichtbar dokumentiert. Eine Eingabe, die nicht vollständig verifizierbar ist, ein Sensor Wert, der divergiert, ein Quorum, das nicht erreicht wird, die Engine verbirgt es nicht zugunsten eines glatten Ergebnisses, sondern dokumentiert es. Das ist für eine spätere forensische Auseinandersetzung wichtiger als ein glattes Ergebnis, das im Nachhinein brüchig wird.

Beispiel. Eine Eingabe hat eine Divergenz in zwei Sensordaten. Einer sagt Kontakt, der andere kein Kontakt. Das System entscheidet nicht zugunsten Kontakt oder kein Kontakt. Es dokumentiert Divergenz vorhanden, eine Quelle sagt A, eine Quelle sagt B. Später kann ein Mensch mit dieser Dokumentation arbeiten. Vertiefte Prüfung, beide Sichten, begründete Entscheidung. Eine andere Engine, die voreilig entscheidet, hätte die Divergenz verdeckt, sich für die eine Seite entschieden, einen Receipt mit Kontakt erstellt, und drei Jahre später wäre die Divergenz spurlos verschollen. Unsichtbarkeit belastet langfristig. Dokumentation entlastet.

Vierte Grenze. Menschliche Entscheidungsträger behalten die volle Entscheidungshoheit. Schiedsrichter, Kommissare, Compliance-Officer, Kanzleien, Aufsichtsorgane, all diese Parteien haben in diesem System eine dokumentierte, nachfolgbare, eigenständige Rolle. Eine Schiedsrichter Entscheidung kann eine Engine Indikation ablehnen. Ein Compliance-Officer kann ein Beobachtungsmuster als nicht meldungspflichtig verwerfen. Eine Kanzlei kann ein Validierungsverfahren abbrechen. Das System hinterlässt jede dieser Entscheidungen als kryptografisches Artefakt und unterlässt keine dieser Entscheidungen.

Diese vier Grenzen gelten einheitlich. Egal ob eine Bank Prüfung, ein Fußball Schiedsspruch, ein Motorsport BoP Monitor, eine M&A Due Diligence, ein CRPG Muster, das System ist in jeder funktionalen Achse an diese Grenze gebunden. Es ist ein Beweis System, kein Entscheidungssystem.

Kapitel 28: Die Aufhebung und die Sichtbarkeit

Eine Aufhebung einer einmal erzeugten Entscheidung ist nur in einem Verfahren möglich, das mindestens so streng ist wie das ursprüngliche Verfahren. Das System verlangt zwei einander unabhängige Prüfer, einen zwingenden Rechtsgrund, mindestens ein Beweismittel, und die Dokumentation im öffentlich zugänglichen Raum.

Es gibt keinen Anruf Override. Wer versucht, eine Aufhebung per informellem Weg zu erreichen, wird automatisch abgelehnt, und der Versuch wird dauerhaft protokolliert. Dieses Protokoll ist kein Zwang, sondern eine Verteidigung der ursprünglichen Entscheidung. Wer die Aufhebungschancen erweitert, ohne die Aufhebungsbedingungen zu erweitern, entwertet die ursprüngliche Entscheidung.

Das System unterscheidet bewusst, welche Rollen einen Antrag auf Aufhebung stellen dürfen. Zulässig sind der Rechtsbeistand des Spielers, der Vereinsverantwortliche, der Verbandsdisziplinar und das unabhängige Berufungsgremium. Nicht zulässig ist ein politischer Akteur. Das ist keine politische Stellungnahme, sondern eine Trennung von Governance und Politik. Wer diese Trennung aufgibt, gibt die Unabhängigkeit der sportrechtlichen Entscheidung auf.

Erweiterung. Die Aufhebung ist nicht das einzige Verfahren, das eine erhöhte Sichtbarkeit verlangt. Auch die ursprüngliche Entscheidung ist sichtbar. Eine Sperre, die ausgesprochen wird, ist öffentlich. Eine Sanktion, die dokumentiert wird, ist referenzierbar. Das System hat keine geheimen Entscheidungen, mit der einzigen Ausnahme der Geheimhaltung, die datenschutzrechtlich geboten ist, etwa die Geheimhaltung persönlicher Daten, die nicht öffentlich gehören. Aber die Entscheidung selbst, ihre Begründung, ihre Regelgrundlage, ihr Zeitpunkt sind öffentlich. Wer Geheimnisse aus dem Verfahren macht, entwertet das Verfahren.

Namenskollisions-Disziplin. Eine eigene, wiederkehrende Grenze, die sich erst bei der Aufnahme der Schweiz als neue Jurisdiktion gezeigt hat, aber grundsätzlicher Natur ist. Verschiedene Rechtsordnungen und Institutionen verwenden identische Abkürzungen für völlig unterschiedliche Rechtsquellen. Das deutsche und das schweizerische Geldwäschereigesetz tragen beide die Abkürzung GwG, sind aber zwei verschiedene Gesetze mit verschiedenen Aufsichtsbehörden. Das Kürzel AMLA bezeichnete im Regelkatalog zunächst fälschlich das materielle EU-Regelwerk, obwohl AMLA korrekt ausschließlich die neue europäische Aufsichtsbehörde meint, das materielle Regelwerk trägt die Bezeichnung AMLR. Beide Verwechslungen wurden erst durch nachträgliche Prüfung aufgedeckt, keine davon durch die ursprüngliche Implementierung selbst. Daraus folgt ein verbindlicher Grundsatz für jede künftige Erweiterung des Regelkatalogs: Jede neue Abkürzung wird vor ihrer Übernahme ausdrücklich gegen die bereits bestehenden Katalog-Kürzel geprüft, nicht erst dann, wenn eine Verwechslung tatsächlich auffällt. Das ist keine einmalige Korrektur zweier Einzelfälle, das ist eine strukturelle Prüfpflicht, die mit jeder neuen Jurisdiktion erneut greift.

Siebter Teil: Rechtsquellen Register, vollständig und namentlich

Kapitel 29: Banking und Finanzdienstleistung

Capital Requirements Regulation, Capital Requirements Directive, Basel III Rahmen, MiFID II, MiFIR, DORA, Geldwäschegesetz, Außenwirtschaftsgesetz, Außenwirtschaftsverordnung, KWG, ZAG, EMIR.

Kapitel 30: Versicherung

Solvency II Rahmenrichtlinie, IDD Richtlinie, VVG, Versicherungsaufsichtsgesetz, VAG.

Kapitel 31: Digitale Vermögenswerte

MiCA Verordnung, DLT Pilot Regulation, eWpG.

Kapitel 32: Öffentliche Hand, Vergabe, FDI

EU Vergaberichtlinie 2014/24/EU, EU Vergaberichtlinie 2014/25/EU, Außenwirtschaftsgesetz, Außenwirtschaftsverordnung, GWB Vergaberegime.

Kapitel 33: Grundrechte und Verfassungsrecht

Grundgesetz, insbesondere Grundrechtsartikel 1 bis 19, EU Grundrechtecharta, EMRK.

Kapitel 34: Sanktionen und AML international

EU Consolidated Financial Sanctions, OFAC SDN, UK HMT, UN Security Council, FATF, GAFI.

Kapitel 35: Sport

FIFA Laws of the Game, UEFA Regulations, DFB Statuten, FIA International Sporting Code, DMSB Regelwerk.

Kapitel 36: Schweiz, nGwV-FINMA 2027

Die Schweiz wurde im Juli 2026 als neue Jurisdiktion aufgenommen, ausgelöst durch die am 12. Mai 2026 eröffnete Anhörung zur Teilrevision der Geldwäschereiverordnung-FINMA, die zum 1. Januar 2027 in Kraft tritt. Ein eigenes Gate deckt sechs verifizierte Bestimmungen ab, jede einzeln gegen die Primärquelle, den Anhörungsbericht der FINMA vom 12. Mai 2026, abgeglichen.

Art. 9b nGwV-FINMA, Nachvollziehbarkeit der Eigentums- und Kontrollstruktur. Art. 10 Abs. 3 GwV-FINMA, Aufhebung der Liechtenstein-Sonderregelung, künftig stets der große Datensatz statt des kleinen. Art. 30 nGwV-FINMA, organisatorische Massnahmen zur Verhinderung von Verstössen gegen das Embargogesetz, SR 946.231. Art. 37 Abs. 3 nGwV-FINMA, Streichung der Formulierung je nach Umständen bei Korrespondenzbankbeziehungen. Art. 37 Abs. 5 nGwV-FINMA, neue Durchlaufkonto-Pflicht bei Korrespondenzbankbeziehungen. Art. 65 Abs. 2 Bst. d nGwV-FINMA, Pflicht zur Einholung einer UBO-Erklärung auch bei Unterkonten.

Zusätzlich referenziert das Gate das Schweizer Geldwäschereigesetz unter der eindeutigen Bezeichnung GwG (CH), um eine Verwechslung mit dem deutschen Geldwäschegesetz auszuschließen, sowie die europäische Geldwäscheaufsicht unter der Bezeichnung AMLA, Verordnung 2024/1620, streng getrennt vom materiellen EU-Regelwerk AMLR, Verordnung 2024/1624. Beide Trennungen sind das Ergebnis nachträglich aufgedeckter Verwechslungen, siehe die Namenskollisions-Disziplin im sechsten Teil.

Kapitel 37: Vorbehalt des Registers

Dieses Register ist vollständig in den Quellen, die das System tatsächlich verwendet. Es ist nicht vollständig in der Rechtslage an sich. Einzelne Artikel Paragrafen Zitate, die im Rahmen der Engine Logik fest hinterlegt sind oder in dieser Dokumentation sinngemäß wiedergegeben wurden, tragen ausdrücklich das Label vor externer Verwendung zu prüfen, wenn der aktuelle Verordnungstext in der Regelbasis noch nicht endgültig konsolidiert wurde. Das ist keine Schwäche, sondern die Praxisform einer ehrlichen Systemdokumentation.

Beispiel Basel III. Ein Gate prüft die CRR Anforderung an die Core Eigenkapitalquote. Der Receipt referenziert die Fassung der CRR, die angewendet wurde, etwa Versions Hash X. Später, wenn die CRR geändert wird, referenziert ein neuer Receipt den Hash der neuen Fassung. Alte Receipts behalten die Hash-Referenz auf ihre damals angewandte Fassung. Die Regelbasisversion wird nicht überschrieben, sondern aufgeschichtet.

Beispiel Außenwirtschaftsverordnung. FDI Screening Aufzeichnung. Die angewandte Fassung ist als Hash im Receipt dokumentiert. Wenn die Verordnung in einer Neufassung die Nachweispflichten schärft, referenzieren künftige Receipts die neue Fassung. Alte bleiben referenzierbar auf die alte Fassung.

Beispiel FIFA Laws of the Game. Eine SportDecisionReceipt referenziert die FIFA Fassung 2024/25. Ein Receipt, der nach der nächsten Regelrevision entsteht, referenziert die FIFA Fassung 2025/26. Die alte Receipt Kette bleibt nachrechenbar auf die angewandte Fassung.

Kapitel 38: Beispiele für die Primitive

Beispiel Kanonizität. Zwei Dokumente. Das eine mit Feld Name vor ID, das andere mit ID vor Name. Semantisch gleich, lexikalisch verschieden. Ohne Kanonizität hätten beide einen unterschiedlichen Hash über sich. RFC 8785 kann diesen Dokumenten eine kanonische Form zuweisen, sodass beide denselben Hash ergeben. Das ist die Bedingung dafür, dass ein Hash in einem anderen System wieder nachrechenbar ist.

Beispiel ECDSA Verifikation im Browser. Ein Empfänger, der ein portables Artefakt erhält, kann die Verifikation lokal im Browser durchführen. Importiert den eingebetteten JWK Schlüssel, nimmt den Signatur String, decodiert ihn, und ruft die Verifikation auf. Das Ergebnis wahr oder falsch. Kein Server Aufruf, keine Vorbeziehung zum System. Die Verifikation ist vollständig lokal.

Beispiel Merkle Kette. Receipt N hat den Payload Hash H N. Receipt N plus 1 hat den Payload Hash H N plus 1. Der Merkle Link von Receipt N plus 1 ist die Kombination beider Hashes. Eine nachträgliche Änderung an Receipt N würde H N ändern, somit den Merkle Link von Receipt N plus 1 brechen, und die

Brechung pflanzt sich in jedem nachfolgenden Receipt fort. Die Kette ist append only. Manipulation ist sichtbar.

Beispiel Verification Block Status. Ist der private Server Schlüssel momentan nicht verfügbar, Rotation im Gange, ist der Status des portablen Beweises nicht verfügbar. Das Artefakt bleibt in seiner internen Integrität korrekt, und der Verifikator weiß, dass die asymmetrische Signatur erst nach der Rotation folgt. Das System verliert niemals die interne Integrität, wenn die asymmetrische Schicht temporär ausfällt.

achter Teil: Fahrplan, was gebaut ist und was als Nächstes kommt

Dieser Abschnitt beschönigt nichts. Jeder Punkt sagt klar, was heute steht und was der nächste konkrete Schritt ist.

Gate M9, alle drei Wetter-Normalisierungsschichten implementiert und aktiv. Die Windkorrektur, Vektorprojektion, ist implementiert und aktiv. Die Luftdichtekorrektur nach SAE J1349, Atmosphärendichtekorrektur, ist implementiert und aktiv, physikalisch unabhängig von der Windkorrektur und niemals mit ihr vermischt. Die Referenzbedingung ist 99 kPa trockene Luft bei 25 Grad Celsius, nach SAE J1349 und DIN 70020. Das System misst die Luftdichte nicht selbst, es empfängt gemessene Umgebungsbedingungen, Temperatur, Druck, relative Feuchte, aus der Strecken-Telemetrie und berechnet daraus den Korrekturfaktor.

Gate M9, Wetterpunkte pro Sektor. Wetterdaten werden pro leistungssensitivem Sektor beigezogen, nicht nur pro Runde. Für Strecken mit starkem Mikroklima, etwa eine lange Strecke mit verschiedenen Höhenlagen wie die Nordschleife, ist das die produktionsgerechte Form. Das Receipt dokumentiert, welche Sektor-Wetterpunkte der Bewertung zugrunde lagen.

External Validation Record, nächster Schritt: Beauftragung einer benannten Kanzlei. Die architektonisch vollständige, kryptografisch vollständige Struktur für External Validation Records steht und ist in Betrieb. Der nächste konkrete Schritt ist, eine externe Kanzlei oder Prüfstelle zu benennen und zu beauftragen, die im laufenden Betrieb solche Records ausstellt. Bis diese Beauftragung erfolgt ist, steht die Achse gerichtsfest für jeden realen Fall zutreffend auf nicht gesetzt. Jede andere Aussage wäre ein Selbstbetrug des Systems, und das System ist gerade so gebaut, dass es diese Aussage nicht selbst treffen kann.

CRPG, Kalibrierungswerte sind Startwerte, Abstimmung mit Aufsichtsorganen ist der nächste Schritt. Die konkreten Zahlenwerte für CRPG, Fenstergröße, Nahbereich-Definition, Mindestanzahl von Ereignissen für die Muster-Auslösung, Summen-Multiplikator, sind technische Startwerte, die mit hoher Sorgfalt gewählt wurden. Der nächste Schritt ist ihre Abstimmung mit den zuständigen Fachbereichen und Aufsichtsorganen. CRPG Receipts, die auf diesen Startwerten basieren, sind schon heute methodisch korrekt erzeugt, die Werte selbst bleiben vorläufig, bis diese offizielle Kalibrierung folgt.

Portable-Proof-Schlüssel, Rotation und Erzeugungsprozess, unter echten Bedingungen bewährt. Der Prozess der Schlüsselerzeugung und Rotation für die asymmetrische Signaturschicht hat eine echte

Bewährungsprobe durchlaufen, keine gestellte. Eine frühere Fassung der Erzeugungszeremonie hatte den privaten Schlüssel in eine Antwort-Rückgabe eingeschlossen, was den geschützten Moment der Erzeugung im strengen Sinne verletzte. Das war kein im Voraus geplantes Testszenario. Es geschah während der aktiven Entwicklung, wurde erkannt und korrigiert, bevor der Schlüssel je produktiv verwendet wurde. Der kompromittierte Schlüssel wurde dauerhaft widerrufen, der Widerruf selbst versiegelt und datiert, und die Zeremonie wurde so neu aufgebaut, dass der private Schlüssel jetzt ausschließlich serverseitig gehalten wird, in einer admin-begrenzten Entität, niemals in Antworten, Logs oder Konfigurationsdokumenten ausgegeben. Was das zeigt, ist nicht, dass ein Fehler nicht passieren kann. Es zeigt, dass die eigene Prüfdisziplin der Architektur ihn findet, benennt und schließt, an einem echten Vorfall, nicht an einer Generalprobe. Der letzte Schritt, die Übergabe an eine hardwaregestützte Schlüsselerzeugung, ist im Gang, vollständig abgeschlossen ist er, sobald dieser Hardware-Schritt steht.

Schutzgutliste, bewusst nicht im Dokument namhaft gemacht. Eine vollständige Namhaftmachung in der Dokumentation mit den konkreten Werten, die in der Erkennungslogik hinterlegt sind, ist aus Sicherheitsgründen nicht geeignet und wird bewusst zurückgehalten, nicht schlicht ausgelassen. Diese Werte werden nicht veröffentlicht. Das betrifft ausdrücklich Windschatten-Distanzen bei Gate M9, Persistenz-Fenstergrößen, CRPG-Nahbereichsprozentsätze und Summen-Multiplikatoren.

Bounding Parameter, bewusst zurückgehalten. Sämtliche numerischen Schwellenwerte, Persistenz-Fenstergrößen, Nahbereich-Definitionen, Summenmultiplikatoren, Windschatten-Distanzen und Persistenzanforderungen sind aus demselben Sicherheitsgrund nicht öffentlich dokumentiert.

Gate 0, Divergenz automatisch aufgelöst. Nein. Gate 0 dokumentiert Divergenzen und löst sie nicht zugunsten einer Quelle. Nachgeordnete fachliche Gates können die Markierung interpretieren.

ML DSA 65 Integration, nächster Schritt: eine zertifizierte Bibliothek. Dokumentierter Migrationspfad, bereit zur Aktivierung. Der Zeitpunkt hängt von der Verfügbarkeit einer zertifizierten Bibliothek ab und wird erst versprochen, sobald diese vorliegt.

Kapitel 39: Technische Grundbegriffe

Datenstrukturen. Receipt Schema, vereinfacht, im SCP 1.0 Datenmodell. Jede Receipt hat einen Identifier, deterministisch erzeugt, etwa RPE für eine Certified Receipt, RDR für eine Reliance Decision Record, CRPG für ein CRPG Pattern Receipt, prefixiert nach Receipt Typ. Einen Input Hash, SHA 256 über die kanonisierte Eingabe. Eine Rule Reference, Regel ID und Hash der angewendeten Regelversion. Ein Verdict, fachliches Ergebnis, PASS, BLOCK, WARN, RACING INCIDENT, OFFSIDE, je nach Sektor. Timestamps, Valid Time, wann die Rechtslage gilt, Transaction Time, wann aufgezeichnet, NTP verankert. Einen Chain Link, den Merkle Link, das ist die Verkettung mit dem Vorgänger. Einen Verification Block.

Verification Block. Der Verification Block in einem SCP 1.0 Artefakt ist so aufgebaut, dass er die zwei Verifikationsklassen strikt trennt. Die interne Integritätssignatur, HMAC SHA 256, verifiable durch Parteien, die den gemeinsamen internen Schlüssel halten. Die portable Beweissignatur, ECDSA P256, mit dem Signaturwert, dem signierten Payload, der Key ID, dem eingebetteten öffentlichen Schlüssel als JWK, der Referenz auf den öffentlich veröffentlichten Schlüssel, und dem Status AVAILABLE oder NOT

AVAILABLE. Die eingebettete public key jwk sorgt dafür, dass das Artefakt selbsttragend ist. Die public key reference erlaubt die Kreuzprüfung gegen den veröffentlichten öffentlichen Schlüssel. Fehlt der aktive private Schlüssel serverseitig, ist portable proof signature status NOT AVAILABLE, die interne Integrität wird jedoch niemals herabgestuft.

Kryptografische Primitive. SHA 256, Hash Standardfunktion, kommt über Kanonizisierung, Merkle Verkettung, Input Hash, Rule Hash zum Einsatz. HMAC SHA 256, Message Authentication Code über SHA 256, Klasse 1 Verifikation. ECDSA P256, Elliptic Curve Signatur auf NIST P 256, Klasse 2 Verifikation heute. Private Schlüssel werden ausschließlich serverseitig in einer admin begrenzten Entität gespeichert und nie in Antworten, Logs oder Konfigurationsdokumenten ausgegeben. ML DSA 65, FIPS 204, Post Quantum Signatur Standard, dokumentierter Migrationspfad zu einer hybriden Signatur neben ECDSA P256, sobald eine zertifizierte Bibliothek integriert ist. RFC 8785, JSON Canonicalization Scheme, standardisierte kanonische Form von JSON, damit Hashes über JSON reproduzierbar sind. Merkle Verkettung, jede Receipt referenziert ihren Vorgänger, append only, Manipulation sichtbar. NTP Zeitanker, Zeitstempel der Receipt sind an NTP verankerte Zeitreferenzen gebunden, die Zeit, zu der ein Ereignis registriert wurde, ist nicht durch das System allein setzbar.

API Grundprinzipien. API First. Alle Ergebnisse sind als API Antwort verfügbar. Die Serverless Edition ist eine API basierte Komposition von Gate Aufrufen. Authentifizierung an jedem Gate. Jeder Funktionsaufruf authentifiziert über Token des aufrufenden Kunden. Öffentliche Endpunkte, etwa der öffentliche Schlüssel, der öffentliche Receipt, sind ohne Authentifizierung in ihrem eingegrenzten Zweck vorgesehen. Keine Secrets in Antworten, keine Umgebungsvariablen Namen in dieser Dokumentation. Sicherheitsrelevante Konfigurationsparameter werden nicht veröffentlicht. Die Namen von internen Umgebungsvariablen und die eigentlichen Secret Werte werden in diesem Dokument nicht ausgeführt. Receipts sind append only. Receipts können im System nicht im Nachhinein verändert werden. Ihre Zustandsübergänge, etwa sealed, verified, disputed, sind dokumentierte Resultate der Prozesse, und die Übergänge reichen selbst im ungünstigsten Zustand nicht aus, um die Hashkette zu brechen. Service Role gegen User Role. Die Wartungs Routine, Abholung eines privaten Schlüssels, Sanktionslisten Synchronisation, geschieht in der Service Role. Fachliche Gate Aufrufe geschehen in der User Role des aufrufenden Kunden.

Kapitel 40: Die Zeit und ihre drei Ebenen

Das System unterscheidet drei Zeitebenen, die niemals vermischt werden.

Transaktionszeit. Das ist der Zeitpunkt, an dem ein Ereignis im System aufgezeichnet wurde. Er ist NTP verankert und nicht durch das System allein manipulierbar.

Gültigkeitszeit. Das ist der Zeitpunkt, ab dem eine Rechtslage gilt. Eine Regel, die am 1. Januar gilt, hat eine Gültigkeitszeit vom 1. Januar, auch wenn sie schon im Dezember vorher veröffentlicht wurde.

Vorlaufzeit. Das ist der Zeitpunkt, an dem die Eingabe in Gate 0 fixiert wurde. Er ist der Beginn der Kette und unabhängig von der Transaktionszeit der späteren fachlichen Gates.

Diese drei Zeitebenen zu trennen, ist wichtig, weil eine forensische Auseinandersetzung oft genau diese drei Zeiten auseinandernehmen muss. Wann wurde die Eingabe fixiert. Wann wurde die Regel angewendet. Wann galt die Rechtslage. Wer diese drei Fragen vermengt, verliert die Nachrechenbarkeit. Wer sie trennt, behält sie.

Kapitel 41: Die Trajektorie der Aufsichtspraxis

Die Aufsichtspraxis in Europa und der Welt bewegt sich in eine Richtung, die kryptografische Nachrechenbarkeit von Compliance-Entscheidungen nicht länger als Bonus, sondern als Mindestanforderung betrachtet. DORA hat für den Finanzsektor Standards gesetzt, die über die reine Zertifikatslogik hinausgehen und die Nachvollziehbarkeit einzelner Meldeereignisse fordern. Die EU AI Act Verordnung beginnt, KI Entscheidungen nicht als Blackbox zu akzeptieren, sondern eine Nachvollziehbarkeit der Entscheidungsgrundlage zu fordern. Die AMLA als europäische AML Aufsicht ist dabei, einen Standard zu setzen, der über die reine Einzelfallmeldung hinausgeht und Querschnittsanalysen fordert.

Diese Trajektorie ist keine Vorhersage. Sie ist bereits im Gange. Und sie läuft unausweichlich auf eine Frage hinaus. Wenn die Aufsicht kryptografische Nachrechenbarkeit zur Mindestanforderung macht, wer hat sie dann, und wer nicht.

In drei Jahren wird der Unterschied zwischen einem Institut, das drei Jahre lang eine Receipt Kette gebaut hat, und einem Institut, das drei Jahre lang PDF Archive geführt hat, nicht mehr ein Unterschied der Compliance-Anstrengung sein. Er wird ein Unterschied der Compliance Methode sein. Und die Methode ist nicht in drei Monaten aufzuholen. Die Kette muss heute beginnen, um in drei Jahren eine drei Jahre alte Kette zu sein.

Kapitel 42: Die Trajektorie der forensischen Praxis

Die forensische Praxis, also die Praxis der Begutachtung von Compliance Entscheidungen durch Kanzleien, Auditoren und Gutachter, bewegt sich parallel. Eine forensische Begutachtung, die vor zehn Jahren ein PDF Archiv durchgesehen hat, wird in drei Jahren kryptografische Nachrechenbarkeit erwarten. Die Frage der Gegenseite, wo steht die Hash Referenz auf die damals geltende Sanktionsliste, ist heute eine höfliche Frage. In drei Jahren wird sie eine Standardfrage sein. Und ein Institut, das auf diese Frage eine Antwort hat, hat einen anderen Stand als ein Institut, das auf diese Frage keine Antwort hat.

In einer gerichtlichen Auseinandersetzung mit dreistelligem Millionenbetrag kommt es nicht darauf an, wer behauptet, sondern wer nachweisen kann. Eine nachrechenbare Kette ist ein Beweis. Eine PDF Notiz ist eine Behauptung. Und der Übergang von einer Welt, in der Behauptungen reichen, zu einer Welt, in der Beweise gefordert werden, ist kein schleichender Übergang. Er ist ein Bruch. Und die Institute, die heute beginnen, eine Kette zu bauen, werden diejenigen sein, die diesen Bruch auf der Seite der Beweise stehen.

Kapitel 43: Was dem verlorengeht, der längere Zeit weiterhin darauf verzichtet

Wenn ein Sektor sich längere Zeit weiterhin darauf verzichtet, eine kryptografisch verkettete Compliance Kette zu bauen, verliert er nicht Compliance-Anstrengung. Er verliert Compliance-Methode. Und der Verlust ist nicht in der Gegenwart spürbar, sondern in der Nachschau. In der Aufsichtsprüfung in drei Jahren, in der gerichtlichen Auseinandersetzung in fünf Jahren, in der forensischen Untersuchung in zehn Jahren.

Die Institute, die heute beginnen, bauen eine Kette, die in drei Jahren drei Jahre alt ist. Die Institute, die in drei Jahren beginnen, bauen eine Kette, die in drei Jahren null Jahre alt ist. Der Unterschied ist nicht aufzuholen, weil die Kette nicht rückwirkend gebaut werden kann. Alte Receipts lassen sich nicht nachträglich erzeugen, weil ihre Zeitstempel NTP verankert sind und ihre Regelversionen nicht im Nachhinein festgelegt werden können. Eine Receipt, die 2026 erzeugt wurde, ist eine Receipt aus 2026. Sie kann nicht 2029 nachträglich erzeugt werden.

Das ist der materielle Grund, warum die Wahl des Beginns nicht beliebig ist. Jedes Jahr, das vergeht, ohne dass die Kette gebaut wird, ist ein Jahr, das in der Kette fehlt. Und das fehlende Jahr ist in der Nachschau nicht mehr herzustellen.

Kapitel 44: Die Preislogik, in Worten, ohne Tabellen

Das System verkauft keine Prüfung. Es verkauft die verbindliche Selbstverpflichtung des Verantwortlichen. Der Wert ist nicht die einzelne Prüfung in sich, sondern der Empfangsbereich dieser Prüfung durch einen verantwortlichen Empfangenden. Der Empfangsverantwortliche ist die Einheit, in der die Prüfung in einer entscheidungsfähigen Form ankommt, bewertet und einer Entscheidung zugeführt wird. Das System unterscheidet daher nicht zwischen Preismodell und Verantwortungsmodell, sondern sieht eine Einheit des Wertstroms. Eine Prüfung ohne Empfangsverantwortlichen ist wertlos. Ein Empfangsverantwortlicher ohne Prüfung ist blind.

Das System lehnt bewusst ein Preismodell, das pro einzelner Feststellung abrechnet. Eine Prüfung ist kein Kaffeebon, der pro Stück verkauft wird. Wer pro Feststellung abrechnet, erzeugt einen Anreiz zur Vermeidung höherer Nutzung und damit zur Vermeidung häufigerer Prüfungen. Das System wählt stattdessen ein institutionelles Lizenzmodell, in dem eine Organisation eine jährliche oder turnierbezogene Lizenz erhält und innerhalb dieser Lizenz die Prüfungen durchführt.

Ein Finanzvorstand wird oft mit der Frage konfrontiert, warum eine Infrastruktur so teuer sei, wenn die einzelne Prüfung doch nach höchstens Sekunden abgeschlossen ist. Die Antwort des Systems ist nicht, dass jede Prüfung viel kostet, sondern dass die Frage falsch ist. Es geht nicht um den Preis pro Prüfung, sondern um den Preis pro verantwortbarem Empfangsbereich, in dem Prüfungen nachweisbar ankommen. Ein angemessener Infrastrukturpreis ist nicht der Preis der Prüfung, sondern der Preis des Nachweises.

Kapitel 45: Die Vermittlung und die Partnerebene

Das System kennt Vermittler. Das sind Organisationen, die das System in ihrem Namen und unter ihrer Verantwortung anwenden. Diese Vermittler erhalten einen eigenen Zugang, einen eigenen Schlüssel, einen eigenen Rechnungsraum. Sie tragen die Verantwortung dafür, dass ihre Endkunden die Receipts in verantworteter Form verwenden.

Die Vermittlertabelle zeichnet jede durchgeführte Prüfung auf, mit ihrem Preis, ihrem Zeitpunkt und ihrer Art. Am Ende eines Abrechnungszeitraums wird daraus eine Rechnung. Diese Rechnung entspricht den örtlich gültigen Rechnungsvorschriften, in Europa der gängigen E Rechnungsnorm für öffentliche Auftraggeber und große Unternehmen.

Das System unterstützt verschiedene Rechnungswege, je nach Bedarf des Empfängers. Die Wege reichen von der Standard PDF per E-Mail über das XML API Angebot an das Empfänger System bis hin zur Dunkelverarbeitung im öffentlichen Beschaffungsnetz. Das System entscheidet nicht über den Weg, es stellt ihn bereit.

Kapitel 46: Die Verlässlichkeit durch Append Only

Das System löscht nichts. Jede Änderung ist ein neues Element in der Kette. Das ist kein Purismus, sondern die Voraussetzung für die Verlässlichkeit des Beweises. Wer ändern kann, kann vertuschen. Wer nur anhängen kann, kann nicht vertuschen, sondern nur korrigieren, und jede Korrektur wird sichtbar.

Kapitel 47: Die Alarme für menschliche Lücken

Das System hat forensische Alarme für Lücken in der Kette. Eine fehlende Versiegelung, eine verpasste Frist, eine unvollständige Begutachtung. Alles das erzeugt einen Alarm, bevor es zu einer Lücke in der Beweiskette kommt. Diese Alarme sind keine kosmetischen Hinweise, sondern Frühwarnzeichen für Gefährdungen des Beweises.

Kapitel 48: Die Interpretationsfreiheit

Das System unterstützt viele Sektoren, aber es interpretiert nicht. Es wendet die Regel an, die im Moment der Prüfung gültig war. Es erfindet keine Regeln. Es liest die vorhandene Regel, fixiert ihre Version und wendet sie an. Das ist die Bedingung, unter der das System forensisch tragfähig bleibt.

Kapitel 49: Beweis ohne Beratung

Das System gibt keine Rechtsberatung. Es erbringt Beweise. Diese Unterscheidung ist nicht nur juristisch, sondern ethisch. Wer Beratung gibt, übernimmt Verantwortung für die Entscheidung. Wer Beweise erbringt, übernimmt Verantwortung für die Nachvollziehbarkeit der Entscheidung. Das ist ein anderer Verantwortungsbegriff, und er ist der richtige für ein System dieser Art.

Kapitel 50: Die Entscheidbarkeit

Das System ist entscheidungsfest. Es lässt sich nicht von Gefühl, nicht von Versprechen, nicht von finanziellen Anreizen leiten. Es lässt sich nur von der Regel und von der Eingabe leiten. Das ist keine Kaltherzigkeit, sondern die Bedingung für Vertrauen. Ein System, das sich von Gefühlen leiten lässt, ist

nicht vertrauenswürdig, weil es unberechenbar wird. Ein System, das sich allein von Regel und Eingabe leiten lässt, ist berechenbar und damit verlässlich.

Kapitel 51: Die Transparenzpflicht

Das System ist transparent. Es dokumentiert seine Regeln, seine Grenzen, seine Lücken, seine Anfragen. Es behauptet keine Fürsorge, die es nicht hat. Es behauptet keine Verlässlichkeit, die es nicht erbringen kann. Diese Transparenz ist keine pädagogische Motivation, sondern eine Beweispflicht. Wer Beweis erbringt, muss auch über die Vertrauensgrenzen dieses Beweises aussagen.

Kapitel 52: Die ethische Stelle

Das System gibt keine Rechtsberatung. Es erbringt Beweise. Diese Unterscheidung ist nicht nur juristisch, sondern ethisch. Wer Beratung gibt, übernimmt Verantwortung für die Entscheidung. Wer Beweise erbringt, übernimmt Verantwortung für die Nachvollziehbarkeit der Entscheidung. Das ist ein anderer Verantwortungsbegriff, und er ist der richtige für ein System dieser Art.

Das System ist entscheidungsfest. Es lässt sich nicht von Gefühl, nicht von Versprechen, nicht von finanziellen Anreizen leiten. Es lässt sich nur von der Regel und von der Eingabe leiten. Das ist keine Kaltherzigkeit, sondern die Bedingung für Vertrauen.

Das System ist transparent. Es dokumentiert seine Regeln, seine Grenzen, seine Lücken, seine Anfragen. Es behauptet keine Fürsorge, die es nicht hat. Es behauptet keine Verlässlichkeit, die es nicht erbringen kann. Diese Transparenz ist keine pädagogische Motivation, sondern eine Beweispflicht.

Kapitel 53: R07, offener Artikelverweis AMLR Technologie

Bei der Aufnahme der EU-Verordnung 2024/1624, AMLR, in den Regelkatalog blieb ein Zitatverweis ausdrücklich offen. Ein internes Referenzdokument hatte Art. 10 als Beleg für eine angebliche Technologie-Bestimmung angeführt. Die Prüfung gegen die tatsächliche Kapitelstruktur der Verordnung ergab, Art. 10 behandelt die unternehmensweite Risikobewertung, nicht Technologie. Ein eindeutiger, einzelner Technologie-Artikel liess sich nicht auffinden, allenfalls verstreute Nebenaspekte in Art. 28 Abs. 3 zu technologischen Entwicklungen bei der Überarbeitung technischer Standards, sowie eine allgemeine Erwägungserwägung. Der Verweis bleibt deshalb bewusst unbesetzt, bis eine tatsächlich zutreffende Bestimmung im Verordnungstext gefunden und verifiziert ist. Das ist dieselbe Disziplin wie bei der Achse External Validation Record, die wahrheitsgemäß auf nicht gesetzt steht, bis eine Kanzlei tatsächlich beauftragt ist, eine sichtbare Lücke statt einer unsicheren Angabe.

Neunter Teil: Die Grenzen

Kapitel 54: Was dieses System nicht kann

Das System kann keine Verantwortung für die Entscheidung des Menschen übernehmen. Es kann dokumentieren, dass die Entscheidung begründet war, aber es kann die Entscheidung nicht treffen.

Das System kann keine externen Begutachtungen erstellen. Es kann sie aufzeichnen, aber nicht herstellen.

Das System kann keine Schlüssel auf ewig garantieren. Es kann Schlüssel rotieren und widerrufen, aber es kann nicht verhindern, dass ein Schlüssel einmal kompromittiert werden kann. Es kann nur dafür sorgen, dass die Kompromittierung erkennbar wird.

Das System kann keine Lücken im rechtlichen Rahmen schließen. Es kann nur belegen, dass im Moment der Prüfung der damals gültige Rahmen eingehalten wurde.

Das System kann keine Wahrheit schaffen. Es kann nur Nachrechenbarkeit schaffen. Wahrheit ist eine menschliche Feststellung. Nachrechenbarkeit ist eine mathematische Feststellung. Das System tut das zweite, nicht das erste.

Kapitel 55: Was dieses System will

Das System will Beweise erbringen, die nach Jahren noch geprüft werden können, ohne dass irgendjemand sich an das Ereignis erinnert.

Das System will Verantwortung zurechenbar machen, nicht verlagern.

Zehnter Teil: Die Akteure und ihre Rollen

Kapitel 56: Der Mensch als entscheidender Akteur

Das System hat eine klare Vorstellung vom Menschen. Der Mensch ist nicht der Störfaktor, der die Determinismus schmälert. Der Mensch ist der entscheidende Akteur, dem das System dient. Alles, was das System erbringt, dient dem Menschen, der eine Entscheidung treffen muss, und der für diese Entscheidung verantwortlich ist. Das System nimmt ihm die Entscheidung nicht ab. Es nimmt ihm die Beweislast ab. Das ist ein anderer Auftrag.

Wer das System versteht, versteht, dass die Deterministik der Maschine und die Freiheit des Menschen kein Widerspruch sind. Die Deterministik stellt sicher, dass der Mensch weiß, worauf er entscheidet. Die Freiheit stellt sicher, dass er entscheidet, nicht die Maschine. Die Deterministik ist die Grundlage der Freiheit, nicht ihr Gegenspieler. Wer die Deterministik aufgibt, um dem Menschen mehr Freiheit zu geben, gibt ihm in Wahrheit mehr Willkür und nimmt ihm die Grundlage, auf der er verantwortlich entscheiden kann.

Kapitel 57: Der Compliance-Officer

Der Compliance-Officer ist der erste Adressat des Systems. Er empfängt die Receipts, bewertet die Befunde, entscheidet über die Freigabe oder Blockade eines Vorgangs. Das System liefert ihm ein Bild, das er in seinem Kontext liest. Es liefert ihm keine fertige Antwort, die er nur abnickt.

Seine Rolle ist dokumentiert. Jede Entscheidung, die er trifft, wird in die Kette eingefügt. Er kann eine Engine Indikation ablehnen, eine Beobachtung als nicht meldungspflichtig verwerfen, eine vertiefte Prüfung veranlassen. Jede dieser Entscheidungen ist forensisch nachvollziehbar. Das System entwertet seine Entscheidungshoheit nicht, es stärkt sie. Der Compliance-Officer, der heute auf Bloße Notizen entscheidet, muss sich verteidigen, wenn seine Entscheidung infrage gestellt wird. Der Compliance-Officer, der auf eine Receipt Kette entscheidet, hat die Verteidigung schon eingebaut.

Kapitel 58: Der Schiedsrichter und der technische Kommissar

Im Sport hat das System zwei Adressaten. Den Schiedsrichter, der das Spiel leitet, und den technischen Kommissar, der die sportrechtlichen Vorgänge bewertet. Beide erhalten Receipts, die ihnen das Bild methodisch nachvollziehbar machen. Beide entscheiden selbst.

Der Schiedsrichter kann eine Indikation des Sport Gates annehmen oder ablehnen. Die Ablehnung wird im Receipt begründet. Das ist keine Schwäche des Systems, sondern seine Stärke. Die Ablehnung ist Datenmaterial, das die Kalibrierung des Systems verbessert. Lehnt ein Schiedsrichter regelmäßig ab, so zeigt das System, dass die Regelindikation und die Schiedsrichterpraxis auseinanderlaufen. Das ist kein Fehler, sondern ein kalibrierbarer Befund, der die weitere Regelentwicklung informiert.

Der technische Kommissar im Motorsport bekommt ein Bild, das die Wetterbedingungen, die Windschattenphase, die Persistenz und die Korrekturschichten dokumentiert. Er entscheidet, ob eine BoP Abweichung vorliegt, die ein Handeln erfordert. Das System liefert ihm die methodische Grundlage, nicht das Urteil.

Kapitel 59: Die Kanzlei

Die Kanzlei ist der externe Akteur, der die Achse 2, Gerichtsfestigkeit, setzt. Sie begutachtet die Methode, die Datenerhebung und die Kette der Verwahrung. Sie stellt die External Validation Record aus. Das System kann diese Aufgabe nicht selbst übernehmen, weil es die Achse 2 nicht selbst setzen darf.

Die Kanzlei ist Akteur des Systems, aber nicht in das System integriert. Das System hat eine Anlage für die Kanzleiarbeit, aber die Kanzlei bleibt unabhängig. Sie wird beauftragt, bezahlt, und sie folgt ihrem eigenen fachlichen Urteil. Das System liefert ihr die methodische Dokumentation, auf der sie ihre Begutachtung aufbaut. Die Begutachtung selbst ist ihr Werk, nicht das Werk des Systems.

Kapitel 60: Der Vermittler

Der Vermittler ist ein Akteur zwischen dem System und dem Endkunden. Er wendet das System in seinem Namen an, unter seiner Verantwortung, für seine Marktteilnehmer. Das System kennt Vermittler, gibt ihnen einen eigenen Zugang und einen eigenen Rechnungsraum, und macht ihre Verantwortung sichtbar.

Der Vermittler ist kein Zwischenhändler im kaufmännischen Sinne. Er ist ein Verantwortlicher, der die Receipts in seinem Namen erzeugt und der dafür haftet, dass seine Endkunden diese Receipts in verantworteter Form verwenden. Das System macht diese Verantwortung forensisch nachvollziehbar. Der Vermittler kann sich nicht hinter dem Endkunden verstecken. Er hat die Receipt erzeugt, er steht dafür.

Kapitel 61: Der Auditor

Der Auditor ist der Nachschauer. Er kommt, wenn die Kette schon steht. Er will wissen, ob das, was dokumentiert ist, auch nachrechenbar ist. Das System ist für ihn gebaut. Er braucht kein Vertrauen, er rechnet nach. Er bekommt die Receipts, die Hashes, die Regelversionen, die Zeitanker. Er prüft die Integrität, die Verkettung, die Signaturen. Das System ist sein Werkzeug, nicht sein Gegner.

Sein Befund wird dokumentiert, in die Kette eingefügt, versiegelt. Ein Auditor, der die Kette geprüft und bestätigt hat, ist selbst Teil der Kette geworden. Wer später die Frage stellt, wurde diese Kette auditiert, findet die Antwort im Receipt, nicht in einer Vermutung.

Kapitel 62: Die Aufsicht

Die Aufsicht ist der Akteur, der die Nachschau des Sektors vornimmt. Sie fragt nach der Compliance-Methode, nicht nach der Compliance Anstrengung. Sie will wissen, ob die Kette belastbar ist, ob die Regelversionen hashverankert sind, ob die Entitätsverifikation stattfand, ob die Lückenlosigkeit gilt.

Das System liefert der Aufsicht ein Bild, das ihren Anforderungen entspricht. Die Aufsicht kann Receipts nachrechnen, kann die Regelbasisversionen vergleichen, kann die Kettenintegrität prüfen. Sie kann feststellen, dass ein Institut eine drei Jahre alte Kette hat, die nachrechenbar ist, und dass ein anderes Institut ein drei Jahre altes PDF Archiv hat, das nicht nachrechenbar ist. Sie wird zwischen beiden zunehmend differenzieren.

Elfter Teil: Die Lebenszyklen eines Artefakts

Kapitel 63: Vom Eingang zur Receipt

Ein Artefakt entsteht nicht in einem Akt, sondern in einer Reihe von Akten. Der erste Akt ist der Eingang. Die Eingabe wird empfangen, kanonisiert, der Hash wird gebildet. Der zweite Akt ist die Gate 0 Prüfung, die die forensische Zulässigkeit feststellt. Der dritte Akt sind die fachlichen Gates, die die Regel anwenden und ein Ergebnis erzeugen. Der vierte Akt ist die Versiegelung, die Signatur, die Verkettung. Der fünfte Akt ist die Ablage, die das Artefakt für die weitere Prüfung bereit hält.

Jeder Akt ist dokumentiert. Jeder Akt hat einen Zeitpunkt. Jeder Akt ist Teil der Kette. Wer das Artefakt später prüft, sieht nicht nur das finale Ergebnis, sondern den ganzen Lebenszyklus, aus dem es entstanden ist. Das ist der Unterschied zwischen einem Dokument und einem Beweis. Das Dokument zeigt das Ergebnis. Der Beweis zeigt die Entstehung.

Kapitel 64: Von der Receipt zum portablen Artefakt

Eine Receipt, die im System entsteht, ist intern intakt. Sie trägt die HMAC Signatur und ist in der Merkle Kette verkettet. Sie ist für die interne Prüfung ausreichend.

Will der Empfänger das Artefakt aus dem System ausführen, um es einem Dritten zu übergeben, dann kommt die zweite Klasse der Signatur hinzu. Die portable Beweissignatur, ECDSA P256, wird hinzugefügt. Der öffentliche Schlüssel wird eingebettet. Das Artefakt wird selbsttragend.

Der Empfänger, der das portable Artefakt erhält, braucht das erzeugende System nicht. Er kann den öffentlichen Schlüssel abrufen, die Signatur verifizieren, die Hashes nachrechnen, die Merkle Verkettung prüfen, die Integrität bestätigen. Das portable Artefakt ist ein Beweisstück für sich. Das System ist nicht mehr nötig, um den Beweis zu erbringen. Das ist die Voraussetzung dafür, dass der Beweis nach Jahren noch erbracht werden kann, wenn das erzeugende System vielleicht bereits archiviert ist.

Kapitel 65: Vom portablen Artefakt zur External Validation Record

Das portable Artefakt ist technisch intakt. Die Achse 1 ist bestätigt. Die Achse 2, Gerichtsfestigkeit, ist noch nicht gesetzt. Die External Validation Record wird hinzugefügt, wenn eine Kanzlei die Begutachtung durchgeführt hat. Sie ist ein weiteres Artefakt, das auf das erste referenziert.

Der Lebenszyklus ist damit nicht abgeschlossen. Die External Validation Record hat eine Gültigkeitsdauer. Sie kann erneuert werden, wenn die Methode in der Zwischenzeit weiterentwickelt wurde. Das System dokumentiert die Gültigkeitsdauer und die Erneuerung. Wer später prüft, sieht, welche Begutachtung galt, und wann sie abgelaufen ist.

Kapitel 66: Vom Receipt zur Entscheidung

Das Receipt ist die Grundlage, nicht die Entscheidung. Die Entscheidung trägt ein Mensch. Das Receipt liefert ihm das Bild, das er bewertet. Die Entscheidung wird dokumentiert, mit Begründung, und in die Kette eingefügt. Damit ist die Entscheidung nicht mehr eine Behauptung, sondern ein kryptografisch verankerter Akt, der auf einem Receipt beruht, das seinerseits auf einer Regel und einer Eingabe beruht.

Wer später die Frage stellt, worauf diese Entscheidung beruhte, findet die Antwort in der Kette. Er findet die Receipt ID, die Regelversion, die Eingabe, die Zeitstempel, die Begründung. Er kann die Entscheidung nachrechnen, auch wenn der Mensch, der sie getroffen hat, nicht mehr erreichbar ist.

Kapitel 67: Vom Receipt zur Aufhebung

Eine Entscheidung, die einmal getroffen wurde, kann aufgehoben werden. Die Aufhebung ist ein eigener forensischer Vorgang, der mindestens so streng ist wie die ursprüngliche Entscheidung. Das System verlangt einen formellen Antrag, einen Rechtsgrund, Beweismittel, und die Begutachtung durch zwei unabhängige Prüfer. Eine informelle Aufhebung wird automatisch abgelehnt, der Versuch wird dokumentiert.

Die Aufhebung ist ein Receipt, das auf das ursprüngliche Receipt referenziert. Das ursprüngliche Receipt bleibt bestehen, es wird nicht gelöscht, es wird nicht geändert. Die Aufhebung ist ein neuer Eintrag, der die Kette fortfeit. Wer später die Frage stellt, wurde diese Entscheidung aufgehoben, findet die Antwort in der Kette, zusammen mit der Begründung, dem Verfahren, und den Prüfern.

Zwölfter Teil: Die Schichten der Verantwortung

Kapitel 68: Die Verantwortung für die Eingabe

Die Eingabe ist die Grundlage jeder Prüfung. Wer die Eingabe liefert, trägt die Verantwortung für ihre Vollständigkeit und Richtigkeit. Das System kann die Eingabe nicht korrigieren, nicht ergänzen, nicht ausgleichen. Es kann nur dokumentieren, was die Eingabe war, und ob sie die forensische Zulässigkeit erfüllt.

Das ist wichtig, weil es die Verantwortung nicht verschiebt. Ein Institut, das eine unvollständige Eingabe liefert, bekommt kein glattes Ergebnis. Es bekommt ein stoppendes Gate 0, das die Unvollständigkeit dokumentiert. Das Institut ist verantwortlich, die Eingabe zu vervollständigen, nicht das System.

Kapitel 69: Die Verantwortung für die Regel

Die Regel Basis ist die Grundlage jeder Anwendung. Wer die Regel Basis pflegt, trägt die Verantwortung für ihre Richtigkeit. Das System wendet die Regel an, die in der versionierten Basis hinterlegt ist. Es interpretiert die Regel nicht, es erfindet sie nicht, es korrigiert sie nicht.

Daraus folgt, dass das System nicht für die Richtigkeit der Regel haftet. Es haftet für die Nachrechenbarkeit der Anwendung. Die Kanzlei, die die Methode begutachtet, haftet für die Anerkennung der Methode. Das System trennt diese Verantwortlichkeiten sauber, weil nur so jede Haftung klar bleibt.

Kapitel 70: Die Verantwortung für die Entscheidung

Die Entscheidung trägt der Mensch. Das System liefert die kryptografische Grundlage, aber die Entscheidung ist menschlich. Das ist keine Ausrede des Systems, sondern eine Bedingung forensischer Klarheit. Wer die Entscheidung auf die Maschine schiebt, gibt die Verantwortung auf, aber er kann sie nicht wirklich abgeben, weil die Maschine nicht haftbar ist. Wer die Entscheidung beim Menschen lässt, hält die Verantwortung erkennbar und kann sie verteidigen.

Das System dokumentiert, dass die Entscheidung menschlich getroffen wurde. Es dokumentiert, wer getroffen hat, wann, mit welcher Begründung, auf welches Receipt bezogen. Die Verantwortung bleibt beim Menschen, und das System macht sie forensisch nachvollziehbar.

Kapitel 71: Die Verantwortung für die Aufhebung

Die Aufhebung ist eine Entscheidung, die eine frühere Entscheidung ersetzt. Auch hier trägt der Mensch die Verantwortung. Das System verlangt das Verfahren, dokumentiert die Begründung, die Prüfer, die Beweise. Die Verantwortung liegt bei den Prüfern, und das System macht ihre Arbeit nachvollziehbar.

Wer die Aufhebung beantragt, trägt ebenfalls eine Verantwortung. Das System dokumentiert, wer beantragt hat, in welcher Rolle, mit welcher Begründung. Ein Antrag, der nicht zulässig ist, etwa von einem politischen Akteur, wird automatisch abgelehnt. Das System macht die Unzulässigkeit sichtbar, es verbirgt sie nicht.

Dreizehnter Teil: Die Schichten der Kryptografie

Kapitel 72: Die Hashfunktion

Die Hashfunktion ist die Grundlage der kryptografischen Integrität. Sie nimmt beliebig große Daten und erzeugt einen festen Fingerabdruck, der die Daten eindeutig identifiziert. Eine kleine Änderung der Daten erzeugt einen vollständig anderen Fingerabdruck. Das System verwendet SHA 256, eine bewährte Hashfunktion, die in zahlreichen kryptografischen Standards etabliert ist.

Die Hashfunktion ist nicht reversibel. Man kann aus dem Fingerabdruck die Daten nicht zurückgewinnen. Das ist wichtig, weil es die Integritätsprüfung von der Vertraulichkeit trennt. Wer den Fingerabdruck hat, kann die Integrität prüfen, ohne die Daten zu kennen. Wer die Daten hat, kann den Fingerabdruck nachrechnen, um die Übereinstimmung festzustellen.

Kapitel 73: Der Message Authentication Code

Der Message Authentication Code, HMAC, ist die symmetrische Signatur, die die interne Kettenintegrität sichert. Er verwendet die Hashfunktion und einen gemeinsamen Schlüssel. Wer den Schlüssel hat, kann die Signatur nachrechnen. Wer die Signatur nachrechnen kann, kann bestätigen, dass die Receipt unverändert aus dem erzeugenden System stammt.

Der HMAC ist Klasse 1 der Verifikation. Er reicht für die interne Prüfung, aber er reicht nicht für die externe Prüfung, weil der Prüfer den gemeinsamen Schlüssel haben müsste, was der Eigenschaft einer asymmetrischen Signatur widerspricht.

Kapitel 74: Die asymmetrische Signatur

Die asymmetrische Signatur, ECDSA P256, ist die Klasse 2 der Verifikation. Sie verwendet ein Schlüsselpaar. Der private Schlüssel signiert, der öffentliche Schlüssel verifiziert. Der private Schlüssel bleibt im System, der öffentliche Schlüssel wird veröffentlicht.

Die asymmetrische Signatur löst das Problem der externen Prüfung. Ein Prüfer, der den öffentlichen Schlüssel hat, kann die Signatur verifizieren, ohne jemals den privaten Schlüssel gehabt zu haben. Das ist die Grundlage der portablen Beweisbarkeit.

Kapitel 75: Die Merkle Verkettung

Die Merkle Verkettung ist die Verkettung der Receipts zu einer append only Kette. Jedes Receipt referenziert seinen Vorgänger. Der Merkle Link ist die Kombination aus dem eigenen Hash und dem Hash des Vorgängers. Eine nachträgliche Änderung eines Receipts würde seinen Hash ändern, den Merkle Link des nachfolgenden Receipts brechen, und die Brechung pflanzt sich in jedem nachfolgenden Receipt fort.

Die Merkle Verkettung ist das Werkzeug, das die Lückenlosigkeit sichert. Sie ist selbst eine bewährte kryptografische Technik, die in Blockketten und anderen append only Systemen etabliert ist. Das System wendet sie konsequent an.

Kapitel 76: Der NTP Zeitanker

Der NTP Zeitanker ist die externe Zeitreferenz, die den Zeitpunkt eines Ereignisses festhält. Das System zieht die Zeit von einer unabhängigen, öffentlichen Zeitquelle. Der Zeitstempel ist somit nicht durch das System allein setzbar. Ein Angreifer, der das System kontrolliert, kann die Daten nicht manipulieren, ohne die Zeit nicht zu fälschen, und die Zeit ist nicht im System, sondern in der Welt.

Der NTP Zeitanker ist die Grundlage der forensischen Belastbarkeit eines Zeitpunkts. Ein Prüfer, der die Frage stellt, wann dieses Ereignis stattfand, findet die Antwort im Receipt, und die Antwort ist nicht durch das System allein erzeugbar, sondern durch die externe Zeitreferenz gesichert.

Kapitel 77: Die kanonische Form

Die kanonische Form, RFC 8785, ist die standardisierte Darstellung von JSON Daten, die es ermöglicht, Hashes über JSON reproduzierbar zu bilden. Ohne kanonische Form hinge ein Hash von der Reihenfolge der Felder, von Leerzeichen, von der Serialisierungsform ab. Mit kanonischer Form sind diese Zufälligkeiten eliminiert.

Die kanonische Form ist die Grundlage der Interoperabilität der Hashbildung. Ein Prüfer, der in einem anderen System denselben Hash nachrechnen will, braucht eine kanonische Form, die dieselbe ist. Das System verwendet RFC 8785, weil es der etablierte Standard für die kanonische Darstellung von JSON ist.

Vierzehnter Teil: Die Schichten der Zeit

Kapitel 78: Die Transaktionszeit

Die Transaktionszeit ist der Zeitpunkt, an dem ein Ereignis im System aufgezeichnet wurde. Sie ist NTP verankert und dokumentiert, wann das Receipt entstanden ist. Die Transaktionszeit ist der Zeitpunkt der Versiegelung.

Kapitel 79: Die Gültigkeitszeit

Die Gültigkeitszeit ist der Zeitpunkt, ab dem eine Rechtslage gilt. Eine Regel, die am 1. Januar gilt, hat eine Gültigkeitszeit vom 1. Januar, auch wenn sie schon im Dezember vorher veröffentlicht wurde. Die Gültigkeitszeit dokumentiert, wann die Regel anwendbar wurde, nicht wann sie dokumentiert wurde.

Kapitel 80: Die Vorlaufzeit

Die Vorlaufzeit ist der Zeitpunkt, an dem die Eingabe in Gate 0 fixiert wurde. Sie ist der Beginn der Kette, die zu einem Receipt führt. Die Vorlaufzeit ist von der Transaktionszeit des späteren fachlichen Gates getrennt. Diese Trennung ist wichtig, weil die forensische Auseinandersetzung oft genau diese Zeiten auseinandernehmen muss. Wann wurde die Eingabe fixiert. Wann wurde die Regel angewendet. Wann galt die Rechtslage.

Kapitel 81: Die Lebenszeit eines Receipts

Ein Receipt hat keine feste Lebenszeit. Es lebt, solange die Kette lebt. Da die Kette append only ist, lebt sie unbegrenzt. Ein Receipt, das 2026 erzeugt wurde, ist 2056 noch nachrechenbar, wenn die Kette gepflegt wurde und die kryptografischen Verfahren noch gelten.

Die Lebenszeit ist durch den kryptografischen Verfall begrenzt. ECDSA P256 gilt heute als sicher, aber in zwanzig Jahren könnte ein Quantencomputer es brechen. Deshalb hat das System den dokumentierten Migrationspfad zur hybriden Signatur aus ECDSA P256 plus ML DSA 65. Wer heute eine Receipt erzeugt, hat in zwanzig Jahren eine Receipt, die unter den damals geltenden kryptografischen Verfahren signiert wurde. Die Migration zu hybriden Signaturen ist additiv, nicht ersetzend. Die alten Signaturen bleiben gültig, die neuen Signaturen kommen hinzu.

Kapitel 82: Die Lebenszeit einer External Validation Record

Eine External Validation Record hat eine dokumentierte Gültigkeitsdauer. Sie ist nicht unbegrenzt. Eine Kanzlei, die eine Methode heute begutachtet, begutachtet sie für die Fassung von heute. In fünf Jahren kann die Methode weiterentwickelt sein, und die Begutachtung muss erneuert werden.

Das System dokumentiert die Gültigkeitsdauer im Record. Ein Receipt, das heute auf einen Record verweist, referenziert einen gültigen Record. Ein Receipt, das in sechs Jahren auf denselben Record verweist, referenziert einen abgelaufenen Record. Das System dokumentiert, wann die Gültigkeit beginnt und wann sie endet. Es lügt nicht über die Gültigkeit.

Kapitel 83: Die Lebenszeit einer Regelversion

Eine Regelversion hat keine Löschung. Sie ist aufgeschichtet, nicht überschrieben. Eine Regel, die 2024 gilt, bleibt in ihrer 2024er Fassung hinterlegt, auch wenn 2025 eine neue Fassung veröffentlicht wird. Ein Receipt, das 2024 erzeugt wurde, referenziert die 2024er Fassung. Wer das Receipt nachrechnen will, findet die 2024er Fassung, hashverankert, nicht überschrieben.

Diese Aufschichtung ist die Grundlage der Nachrechenbarkeit über Zeit. Ein Receipt, das 2024 erzeugt wurde, ist 2034 nachrechenbar, weil die 2024er Fassung 2034 noch hinterlegt ist, mit demselben Hash, an derselben Stelle. Wer die Frage stellt, welche Regel galt 2024, findet die Antwort im Regelkatalog, der die 2024er Fassung noch enthält.

Fünfzehnter Teil: Die Schichten der Transparenz

Kapitel 84: Transparenz nach innen

Das System ist transparent nach innen. Jede Prüfung, die durchgeführt wird, ist im System dokumentiert. Jedes Receipt, das erzeugt wird, liegt vor. Jede Entscheidung, die getroffen wird, ist nachvollziehbar. Wer den Zugang zum System hat, kann die Vollständigkeit der Kette prüfen, kann die Lückenlosigkeit feststellen, kann die Integrität nachrechnen.

Diese Transparenz nach innen ist die Vorbedingung für die Transparenz nach außen. Wer nach innen nicht transparent ist, kann nach außen nichts versichern, was er nicht selbst prüfen kann.

Kapitel 85: Transparenz nach außen

Das System ist transparent nach außen. Der öffentliche Schlüssel ist veröffentlicht. Die Receipts, die das System verlässt, tragen den öffentlichen Schlüssel eingebettet. Wer das Artefakt erhält, kann die Signatur verifizieren, ohne das System zu konsultieren. Das System benötigt keine andauernde Vertrauensbeziehung, keine laufende Verbindung, kein Abonnement.

Diese Transparenz nach außen ist die Grundlage der portablen Beweisbarkeit. Sie ist die Bedingung dafür, dass ein Beweis nach Jahren noch erbracht werden kann, wenn das erzeugende System vielleicht bereits archiviert ist.

Kapitel 86: Transparenz über die Grenzen

Das System ist transparent über seine Grenzen. Es dokumentiert, was es nicht kann, was es nicht leistet, was es nicht versichert. Es behauptet keine Fürsorge, die es nicht hat. Es behauptet keine Verlässlichkeit, die es nicht erbringen kann. Es behauptet keine Gerichtsfestigkeit, die nur eine externe Stelle setzen kann.

Diese Transparenz über die Grenzen ist keine pädagogische Motivation, sondern eine Beweispflicht. Wer Beweis erbringt, muss auch über die Vertrauensgrenzen dieses Beweises aussagen. Wer die Grenzen verschweigt, betrügt den Prüfer, der auf den Beweis vertraut.

Kapitel 87: Transparenz über die Offenheiten

Das System ist transparent über seine offenen Punkte. Es dokumentiert, was noch nicht kalibriert ist, was noch nicht beauftragt ist. Es verschweigt nicht, dass die Kanzleipartnerschaft für External Validation Records aussteht, deren Verfahren jedoch laufen, dass die Kalibrierungswerte für CRPG Startwerte sind, dass der Rotationsprozess für die portable Proof Schlüssel in Überarbeitung ist. Die Luftdichtekorrektur

bei Gate M9 nach SAE J1349 / DIN 70020 ist implementiert und aktiv, sie gehört zu den drei vollständigen Wetter-Normalisierungsschichten.

Diese Transparenz über die Offenheiten ist die Praxisform einer ehrlichen Systemdokumentation. Wer die Offenheiten verschweigt, produziert eine Scheingenauigkeit, die in der forensischen Auseinandersetzung brüchig wird. Wer die Offenheiten dokumentiert, liefert ein Bild, das auch im Ernstfall hält.

Sechzehnter Teil: Die Schichten der Fehler

Kapitel 88: Der fehlerhafte Eingang

Ein fehlerhafter Eingang wird nicht korrigiert, sondern dokumentiert. Das System nicht glättet. Es zeigt, dass die Eingabe fehlerhaft ist, und stoppt. Wer die Eingabe korrigieren will, muss eine neue Eingabe liefern, die in einer neuen Receipt Kette steht. Die fehlerhafte Receipt bleibt in der Kette, dokumentiert, dass sie fehlerhaft war. Die korrigierte Receipt ist ein neuer Eintrag, der auf die fehlerhafte referenziert.

Das ist die append only Methode im Umgang mit Fehlern. Fehler werden nicht gelöscht, sondern korrigiert. Die Korrektur ist sichtbar, und der Fehler ist sichtbar. Wer später die Frage stellt, war dieser Eingang fehlerhaft, findet die Antwort in der Kette, zusammen mit der Korrektur.

Kapitel 89: Die fehlerhafte Regel

Eine fehlerhafte Regel ist eine Regel, die falsch hinterlegt wurde. Das System wendet die Regel an, wie sie hinterlegt ist. Es interpretiert nicht, ob die Regel richtig ist. Es wendet sie an und versiegelt die Anwendung.

Wird später festgestellt, dass die Regel fehlerhaft war, dann ist das keine nachträgliche Korrektur der Receipts, die auf dieser Regel beruhen. Die fehlerhafte Regel bleibt in der versionierten Basis hinterlegt. Eine neue Regelversion wird veröffentlicht, die die fehlerhafte ersetzt, aber nicht überschreibt. Receipts, die auf der fehlerhaften Regel beruhen, referenzieren weiterhin die fehlerhafte Regel. Receipts, die nach der neuen Regelversion erzeugt werden, referenzieren die neue Regelversion.

Wer später die Frage stellt, wurde diese Prüfung mit der fehlerhaften Regel durchgeführt, findet die Antwort in der Kette, referenziert auf die fehlerhafte Regelversion. Die Erkenntnis, dass die Regel fehlerhaft war, ist forensisch nachvollziehbar. Die nachträgliche Korrektur ist dokumentiert, in der neuen Regelversion. Die alte Receipt bleibt nachrechenbar, weil die alte Regelversion hinterlegt bleibt.

Kapitel 90: Die fehlerhafte Entscheidung

Eine fehlerhafte Entscheidung ist eine Entscheidung, die falsch getroffen wurde. Das System kann die Entscheidung nicht korrigieren. Es kann dokumentieren, dass die Entscheidung getroffen wurde, mit Begründung, auf welches Receipt bezogen.

Wird die Entscheidung später als fehlerhaft erkannt, kann eine Aufhebung folgen, in einem Verfahren, das mindestens so streng ist wie das ursprüngliche Verfahren. Die Aufhebung ist ein neuer Eintrag, der

die ursprüngliche Entscheidung referenziert. Die ursprüngliche Entscheidung bleibt in der Kette, dokumentiert, dass sie getroffen wurde, mit Begründung. Die Aufhebung ist ein neuer Eintrag, der dokumentiert, dass die Entscheidung aufgehoben wurde, mit Begründung, mit Prüfern.

Das System löscht nicht. Es korrigiert durch Aufschichtung. Eine fehlerhafte Entscheidung ist sichtbar, und ihre Aufhebung ist sichtbar. Wer später die Frage stellt, war diese Entscheidung fehlerhaft, findet die Antwort in der Kette, zusammen mit der Aufhebung und ihrer Begründung.

Kapitel 91: Der fehlerhafte Schlüssel

Ein fehlerhafter Schlüssel ist ein Schlüssel, der kompromittiert wurde. Das System kann den Schlüssel widerrufen, nicht ungeschehen machen, was mit ihm signiert wurde. Receipts, die mit dem kompromittierten Schlüssel signiert wurden, sind mit der Kenntnis der Kompromittierung zu bewerten. Das System dokumentiert die Kompromittierung und den Widerruf.

Eine neue Schlüsselzeremonie erzeugt ein neues Schlüsselpaar, das den widerrufenen Schlüssel ersetzt. Künftige Receipts werden mit dem neuen Schlüssel signiert. Die alten Receipts, die mit dem kompromittierten Schlüssel signiert wurden, bleiben in der Kette, referenzieren den kompromittierten Schlüssel, und sind forensisch mit der Kenntnis der Kompromittierung zu bewerten.

Das System kann die Vergangenheit nicht ungeschehen machen. Es kann die Zukunft sichern, durch Rotation, durch Widerruf, durch neue Schlüssel. Die Transparenz über die Kompromittierung ist die Voraussetzung dafür, dass ein Prüfer die alten Receipts richtig bewerten kann. Wer die Kompromittierung verschweigt, betrügt den Prüfer.

Siebzehnter Teil: Die Schichten der Unkenntnis

Kapitel 92: Unkenntnis über die Eingabe

Das System kann etwas nicht wissen. Es kann nicht wissen, ob die Eingabe vollständig ist, wenn der Eingangs Akteur etwas verschweigt. Es kann nur dokumentieren, was geliefert wurde, und die forensische Zulässigkeit prüfen.

Diese Unkenntnis ist keine Schwäche, sondern eine Bedingung. Das System ist kein Orakel. Es ist ein Beweisinstrument, das das, was geliefert wurde, forensisch belastbar festhält. Wer etwas verschweigt, trägt die Verantwortung für die Verschwiegenheit. Das System dokumentiert, dass es das Verschwiegene nicht kannte, nicht, dass das Verschwiegene nicht existierte.

Kapitel 93: Unkenntnis über die Regel

Das System kann nicht wissen, ob die Regel richtig ist, die es anwendet. Es kann nur dokumentieren, welche Regel, in welcher Version, angewendet wurde. Die Verantwortung für die Richtigkeit der Regel liegt bei dem, der die Regel hinterlegt hat.

Diese Unkenntnis ist die Grundlage der forensischen Klarheit. Das System wendet die Regel an, wie sie hinterlegt ist. Es versichert nicht, dass die Regel richtig ist, sondern dass die Regel angewendet wurde. Wer die Richtigkeit der Regel bestreitet, wendet sich an den, der sie hinterlegt hat, nicht an das System.

Kapitel 94: Unkenntnis über die Zukunft

Das System kann nicht wissen, welche künftige Rechtslage gelten wird. Es kann nur dokumentieren, welche Rechtslage zum Zeitpunkt der Prüfung galt. Die versionierte Regel Basis ist die Antwort auf diese Unkenntnis. Sie hält fest, was galt, nicht, was gelten wird.

Wer später die Frage stellt, war diese Prüfung nach der damals geltenden Rechtslage korrekt, findet die Antwort im Receipt, nicht im Bauchgefühl. Wer die Frage stellt, wäre diese Prüfung nach der heutigen Rechtslage korrekt, muss eine neue Prüfung durchführen, gegen die heutige Regelversion. Das System erlaubt beide Fragen, aber es erlaubt nicht, sie zu vermischen.

Kapitel 95: Unkenntnis über die KI

Das System kann KI in klar begrenzten Rollen einsetzen, etwa in der Textextraktion oder Quellenkonsolidierung. Die KI liest und klassifiziert, entscheidet nicht. Das System kann nicht wissen, wie die KI zu einer Klassifizierung kam, weil die KI ein Modell ist, das auf Trainingsdaten beruht.

Diese Unkenntnis ist der Grund, warum die KI nicht entscheidet. Eine Entscheidung, die auf einer Unkenntnis beruht, ist forensisch nicht belastbar. Eine Entscheidung, die auf einer deterministischen Regel beruht, ist es. Das System wählt die belastbare Form, weil es die forensische Nachrechenbarkeit sichern muss.

Achtzehnter Teil: Die Schichten der Fairness

Kapitel 96: Fairness gegenüber dem Geprüften

Das System ist fair gegenüber dem Geprüften. Es dokumentiert, was geprüft wurde, auf welche Eingabe, mit welcher Regel, zu welchem Zeitpunkt. Es erfindet keine Anschuldigungen, es glättet keine Befunde. Wer geprüft wird, kann das Receipt sehen, das Befund ist, und er kann es prüfen lassen, durch einen Dritten, ohne Vorbeziehung, ohne Vertrauen.

Diese Fairness ist die Grundlage der Akzeptanz des Systems. Wer das System unfair findet, weil es lückenlos dokumentiert, hat nicht verstanden, dass die Lückenlosigkeit ihm dient. Wer fehlerhaft geprüft wurde, findet den Fehler im Receipt, nicht in einer Vermutung. Wer richtig geprüft wurde, findet die Bestätigung im Receipt. Beide haben dasselbe Werkzeug, dasselbe Beweisstück, dieselbe Nachrechenbarkeit.

Kapitel 97: Fairness gegenüber dem Prüfer

Das System ist fair gegenüber dem Prüfer. Es nimmt ihm die Beweislast ab, nicht die Entscheidungshoheit. Es liefert ihm ein Bild, das er bewertet. Er entscheidet, nicht die Maschine.

Diese Fairness ist die Grundlage der Akzeptanz des Systems beim Prüfer. Wer die Entscheidungshoheit behält, akzeptiert das System als Werkzeug. Wer die Entscheidungshoheit verliert, weil die Maschine entscheidet, lehnt das System als Ersatzentscheider ab. Das System wählt die erste Form, weil sie die forensisch tragfähige ist.

Kapitel 98: Fairness gegenüber dem Auditor

Das System ist fair gegenüber dem Auditor. Es liefert ihm die Receipts, die Hashes, die Regelversionen, die Zeitanker. Er rechnet nach, ohne Vertrauen. Das System ist sein Werkzeug, nicht sein Gegner.

Diese Fairness ist die Grundlage der Akzeptanz des Systems beim Auditor. Wer das System als Werkzeug nutzt, kommt zu einem Befund, der nachrechenbar ist. Wer das System als Gegner betrachtet, kommt zu einem Befund, der an seinem Misstrauen scheitert, nicht am System. Das System wählt die erste Form, weil sie die forensisch belastbare ist.

Kapitel 99: Fairness gegenüber der Aufsicht

Das System ist fair gegenüber der Aufsicht. Es liefert ihr die Methode, die Daten, die Kette. Die Aufsicht kann nachrechnen, differenzieren, beurteilen. Sie kann feststellen, dass ein Institut eine drei Jahre alte Kette hat, die nachrechenbar ist, und dass ein anderes Institut ein drei Jahre altes PDF Archiv hat, das nicht nachrechenbar ist.

Diese Fairness ist die Grundlage der Akzeptanz des Systems bei der Aufsicht. Wer das System hat, hat eine Aufsichtslage, die andernfalls fehlt. Wer das System nicht hat, hat eine Aufsichtslage, die in drei Jahren brüchig wird. Das System wendet sich an die Aufsicht nicht mit der Behauptung, dass Compliance besser wird, sondern mit dem Beweis, dass Compliance nachrechenbar wird.

Kapitel 100: Fairness gegenüber der Gesellschaft

Das System ist fair gegenüber der Gesellschaft. Es dokumentiert die Entscheidungen, die in Compliance Ambiente getroffen werden, in einer Form, die nachrechenbar ist. Die Gesellschaft, die die Transparenz von Entscheidungen zunehmend einfordert, bekommt ein Werkzeug, das diese Transparenz leistet, nicht behauptet.

Diese Fairness ist die Grundlage der Akzeptanz des Systems in der Gesellschaft. Wer das System hat, kann der Gesellschaft eine Antwort geben, die eine Gesellschaft ohne das System nicht geben kann. Die Antwort lautet, dass die Entscheidungen, die in diesem Institut getroffen werden, nach Jahren nachrechenbar sind, nicht nach Behauptungen.

Neunzehnter Teil: Die Schichten der Zukunft

Kapitel 101: Die Zukunft der Aufsichtspraxis

Die Aufsichtspraxis bewegt sich in eine Richtung, die kryptografische Nachrechenbarkeit von Compliance-Entscheidungen nicht länger als Bonus, sondern als Mindestanforderung betrachtet. DORA, EU AI Act, AMLA sind die Indikatoren dieser Bewegung.

Das System ist auf diese Zukunft gebaut. Es hat die Nachrechenbarkeit heute, nicht morgen. Wer heute eine Kette baut, hat in drei Jahren eine drei Jahre alte Kette, die diese Zukunft erfüllt. Wer morgen beginnt, hat in drei Jahren eine null Jahre alte Kette, die diese Zukunft nicht erfüllt.

Kapitel 102: Die Zukunft der forensischen Praxis

Die forensische Praxis bewegt sich parallel. Eine Begutachtung, die vor zehn Jahren ein PDF Archiv durchgesehen hat, wird in drei Jahren kryptografische Nachrechenbarkeit erwarten. Die Frage der Gegenseite, wo steht die Hash-Referenz auf die damals geltende Sanktionsliste, ist heute eine höfliche Frage, in drei Jahren eine Standardfrage.

Das System ist auf diese Zukunft gebaut. Es hat die kryptografische Referenz heute, nicht morgen. Wer heute antworten kann, hat eine andere Verhandlungsposition als der, der morgen Antwort geben muss, aber heute nicht kann.

Kapitel 103: Die Zukunft der Kryptografie

Die Kryptografie bewegt sich in eine_post Quantum. Die heutigen Verfahren, ECDSA P256, gelten heute als sicher, aber der künftige Quantencomputer kann sie brechen. Das System hat den dokumentierten Migrationspfad zur hybriden Signatur aus ECDSA P256 plus ML DSA 65.

Das System ist auf diese Zukunft gebaut. Es hat den Migrationspfad heute, nicht morgen. Wer heute eine Receipt erzeugt, hat in zwanzig Jahren eine Receipt, die unter den damals geltenden kryptografischen Verfahren signiert wurde, plus einer Post Quantum Schicht, die den künftigen Quantencomputer übersteht.

Kapitel 104: Die Zukunft der Sport Governance

Die Sport Governance bewegt sich in eine Richtung, die forensische Nachrechenbarkeit einfordert. Eine Gesellschaft, die die Transparenz des Schiedsrichterwesens zunehmend kritisch hinterfragt, wird in naher Zukunft forensische Nachrechenbarkeit einfordern.

Das System ist auf diese Zukunft gebaut. Es hat die Nachrechenbarkeit heute. Ein Verband, der heute eine Receipt Kette baut, hat in fünf Jahren eine fünf Jahre alte Kette, die diese Zukunft erfüllt. Ein Verband, der morgen beginnt, hat in fünf Jahren eine null Jahre alte Kette, die diese Zukunft nicht erfüllt.

Kapitel 105: Die Zukunft der Compliance-Methode

Die Compliance-Methode bewegt sich von Dokumentation zu Beweis, von Wahrscheinlichkeit zu Determinismus, von Vertrauen zu Prüfung, von Lückenhaftigkeit zu Lückenlosigkeit. Das System ist die Kristallisation dieser Bewegung.

Diese Zukunft ist keine Vorhersage, sondern eine Beschreibung einer Bewegung, die bereits im Gange ist. Das System ist nicht der Treiber dieser Bewegung, sondern ihre Antwort. Wer das System hat, ist auf dieser Bewegung. Wer das System nicht hat, wird von ihr eingeholt.

Zwanzigster Teil: Schluss

Kapitel 106: Was dieses System ist

Dieses System ist ein Beweis System. Es ist kein Entscheidungs System, kein Berichts System, kein Dokumentations System. Es ist ein Beweis System, das forensisch belastbare Beweise erbringt, die nach Jahren noch nachrechenbar sind.

Es kann sich nicht selbst für gerichtsfest erklären. Es entscheidet nicht, es beweist. Es glättet nicht, es dokumentiert. Es vertraut nicht, es prüft. Genau diese vier Linien sind das Gerüst, auf dem jeder Baustein dieses Ökosystems steht.

Kapitel 107: Was dieses System nicht ist

Dieses System ist kein Orakel. Es kennt die Zukunft nicht. Es kennt die Richtigkeit der Regel nicht. Es kennt die Vollständigkeit der Eingabe nicht. Es kennt die Kompetenz des Entscheiders nicht.

Es kennt nur das, was geliefert wurde, die Regel, die angewendet wurde, den Zeitpunkt, an dem geprüft wurde, und es hält das, was geliefert wurde, forensisch belastbar fest. Das ist genug für einen Beweis, aber es ist nicht genug für eine Wahrheit. Wahrheit ist eine menschliche Feststellung. Beweis ist eine mathematische Feststellung. Das System tut das zweite, nicht das erste.

Kapitel 108: Was dieses System will

Dieses System will Beweise erbringen, die nach Jahren noch geprüft werden können, ohne dass irgendjemand sich an das Ereignis erinnert. Es will Verantwortung zurechenbar machen, nicht verlagern. Es will die Lücken in der heutigen Compliance schließen, nicht durch mehr Dokumente, sondern durch bessere Beweise. Es will nicht das erste sein, sondern das verlässlichste.

Kapitel 109: Wer dieses System verstanden hat

Wer dieses System verstanden hat, hat nicht ein Produkt verstanden, sondern eine Haltung. Die Haltung lautet, dass Compliance kein Dokument ist, sondern ein Beweis, und dass dieser Beweis nur dann wertvoll ist, wenn er nach Jahren noch erbracht werden kann.

Wer diese Haltung verstanden hat, hat verstanden, warum die Wahl des Beginns nicht beliebig ist. Jedes Jahr, das vergeht, ohne dass die Kette gebaut wird, ist ein Jahr, das in der Kette fehlt. Und das fehlende Jahr ist in der Nachschau nicht mehr herzustellen.

Kapitel 110: Letzter Satz

Das System ist ein Beweis System, gebaut für eine Welt, in der Beweise heute meist nach drei Jahren verschwunden sind oder auf Vermutungen beruhen. Es erbringt Beweise, die nach Jahren noch stehen. Das ist der entscheidende Unterschied, und es ist genug.

Das System will die Lücken in der heutigen Compliance schließen, nicht durch mehr Dokumente, sondern durch bessere Beweise.

Das System will nicht das erste sein, sondern das verlässlichste.

Das System will, dass eine Entscheidung, die heute fällt, in zehn Jahren noch steht, nicht weil sie unangefochten ist, sondern weil sie nachrechenbar ist.

Das System will, dass die Frage, auf welcher Sanktionsliste, in welcher Fassung, zu welchem Zeitpunkt geprüft wurde, nie wieder mit Schweigen beantwortet werden muss.

Das System will, dass der Übergang von einer Welt der Behauptungen zu einer Welt der Beweise kein Bruch ist, der einige trifft und andere verschont, sondern ein Weg, den gegangen kann, wer heute beginnt.

Schluss

Dieses Dokument beschreibt ein System, das aus der Welt der heutigen Compliance entstanden ist. Es behauptet nicht, diese Welt zu lösen. Es behauptet, in dieser Welt Beweise zu erbringen, die nach Jahren noch stehen. Das ist nicht wenig. In einer Welt, in der Beweise heute meist nach drei Jahren verschwunden sind oder auf Vermutungen beruhen, ist das der entscheidende Unterschied.

Wer dieses System verstanden hat, hat nicht ein Produkt verstanden, sondern eine Antwort. Die Antwort lautet:

> ***Compliance ist kein Dokument, sondern ein Beweis, und dieser Beweis ist nur dann wertvoll, wenn er nach Jahren noch erbracht werden kann.***

Das System ist kein Entscheidungssystem. Es ist ein Beweissystem. Es kann sich nicht selbst für gerichtsfest erklären. Es entscheidet nicht, es beweist. Es glättet nicht, es dokumentiert. Es vertraut nicht, es prüft. Genau diese vier Linien, Beweis statt Entscheidung, externe statt selbst gesetzte Gerichtsfestigkeit, Dokumentation statt Glättung, Prüfung statt Vertrauen, sind das Gerüst, auf dem jeder Baustein dieses Ökosystems steht. Wer dieses Gerüst verstanden hat, hat das System verstanden.**Einundzwanzigster Teil: Technischer Anhang**

Tabelle A1: Reihenfolge der Gate-Pipeline

Pos.	Gate	Typ	Ergebnis
0	Gate 0	Eingang/Hash	Forensische Zulässigkeit
1	GLEIF-Gate	Identität	Entität verifiziert
2	Sanktions-Gate	Identität	CLEAR/BLOCK/UNCLEAR
3	AML-Gate	Sachfrage	Meldepflichtprüfung
4	Jurisdiktions-Gate	Sachfrage	Konflikt dokumentiert
5	Grundrechte-Gate	Sachfrage	Berührung markiert
6	Sektor-Gate	Sachfrage	Sektorbefund
7	Verfahrens-Gate	Verfahren	Frist/Vollständigkeit
8	T0-Gate	Abschluss	Gesamtbild versiegelt

Tabelle A2: Zwei Verifikationsklassen

Eigenschaft	Klasse 1 (HMAC)	Klasse 2 (ECDSA)	Klasse 2+ (PQC)
Kryptografie	Symmetrisch	Asymmetrisch	Hybrid
Schlüssel	Geteilt	Privat/Öffentlich	ECDSA + ML-DSA-65
Richtung	Intern	Extern	Intern + Extern
Portabel	Nein	Ja	Ja
Vertrauen	Geteiltes Geheimnis	Öffentlicher Beweis	Doppelt gesichert
Anwendungsfall	Interne Kette	Export	Post-Quantum-Ära

Tabelle A3: Zwei-Achsen-Logik

Achse	Name	Wer setzt sie?	Bedingung
Achse 1	Technische Integrität	System (Kryptografie)	Hash+Signatur+Kette

Achse	Name	Wer setzt sie?	Bedingung
Achse 2	Gerichtsfest	Externe Kanzlei (EVR)	Gutachten+Signatur

Kernsatz: Das System kann Achse 2 niemals selbst setzen.

Tabelle A4: Wetter-Normalisierungsschichten Gate M9

Schicht	Verfahren	Status	Granularität
1	Nässe verwerfen	Implementiert	pro Sektor
2	Windvektor-Projektion	Implementiert	pro Sektor
3	Luftdichte nach J1349	Implementiert und aktiv	pro Sektor

Schicht 2 und 3 sind strikt getrennt, nie vermischt. Schicht 3 (Luftdichtekorrektur) ist implementiert und aktiv; Referenzbedingung: 99 kPa, 25 °C, trocken, nach SAE J1349 / DIN 70020.

Tabelle A5: Vergleich der Sektor-Engines

Sektor	Primäre Gates	Konkurrenz macht	Hier anders
Banking	GLEIF, Sanktionen, AML, Basel III	PDF-Bericht	Hash-verankerte Kette
Versicherung	Solvency II, IDD, AML	3 Notizen	Receipt-Set
M&A	6 Dimensionen, 7 Schritte	Werkzeug gekauft	MaDDReceipt
Immobilien	BoO, SoF, Sanktionen, AWG	Notarliste	Notar-Kette
Cloud	DORA, C5, ISO 27001	Jährliches Zertifikat	Receipt pro Ereignis
Energie	RE-Richtlinie, AWG, Sanktionen	PDF-Archiv	Tagesreferenz
Sport	FIFA Laws 10, 11, 12	VAR-Video	SportDecisionReceipt
Motorsport	M0–M9, SAE J1349	Serien-intern	BoP-Receipt

Tabelle A6: Akteure und Rollen

Akteur	Rolle	Setzt/Entscheidet
Compliance-Officer	Erstbewertung	Freigabe/Sperre

Akteur	Rolle	Setzt/Entscheidet
Schiedsrichter	Sportentscheidung	Indikation an/aus
Technischer Steward	Motorsport-Bewertung	BoP-Befund
Kanzlei	Externes Gutachten	Achse 2 (EVR)
Vermittler	Zwischen System/Kunde	Receipt im eigenen Namen
Auditor	Nachträgliche Prüfung	Befund-Receipt
Aufsicht	Sektorprüfung	Abweichung festgestellt

Tabelle A7: Zeitebenen

Zeit	Bedeutung	Wann entscheidend
Vorlaufzeit	Eingabe fixiert in Gate 0	Beginn der Kette
Transaktionszeit	Receipt versiegelt	NTP-verankert
Gültigkeitszeit	Rechtslage ab	Welche Regel gilt

Tabelle A8: Receipt-Typ-Präfixe

Präfix	Receipt-Typ	Beispiel
RPE-	Certified Receipt	RPE-SYS-2025-00001
RDR-	Reliance Decision Record	RDR-BNF-2025-00002
CRPG-	Cross-Receipt Pattern	CRPG-ENT-2024-00014
T0-	T-Zero-Artefakt	T0-TEN-2025-00003
GM-	Motorsport-Receipt	GM-SERIE-EVENT-12-0004
GATESPORT-	Sport Decision Receipt	GATESPORT-MATCH-2026003-47-001
EVR-	External Validation	EVR-DE-2025-00001

Tabelle A9: Kryptografische Primitive

Primitiv	Klasse	Verwendung
SHA-256	Hash	Eingabe, Regel, Merkle, Receipt
HMAC-SHA256	MAC, symmetrisch	Interne Integrität
ECDSA-P256	Signatur, asymmetrisch	Portable Nachweisbarkeit
ML-DSA-65	PQ-Signatur (FIPS 204)	Hybrid-Migration (geplant)
RFC 8785	JCS	Kanonische JSON-Form
Merkle-Link	Verkettung	SHA256(vorherige:eigene)
NTP	Zeitquelle	Zeitanker

Tabelle A10: Datenquellen und Hashes

Quelle	Inhalt	Im Receipt
GLEIF	LEI-Register	LEI + Snapshot-Hash
EU FSF	EU-Sanktionen	Listen-Hash
OFAC SDN	US-Sanktionen	Listen-Hash
UK HMT	UK-Sanktionen	Listen-Hash
UN SC	UN-Sanktionen	Listen-Hash
FATF	FATF-Listen	Listen-Hash
Regelkatalog	Regeln (versioniert)	Regel-Hash

Tabelle A11: Systemgrenzen

Nr	Grenze	Hinweis
1	Kein automatischer Sanktionsausspruch	menschliche Handlung
2	Keine KI-Entscheidung	KI liest nur
3	Jede Unsicherheit dokumentiert	nie verborgen

Nr	Grenze	Hinweis
4	Mensch behält Entscheidungshoheit	System beweist
5	Aufhebung mindestens so streng wie Original	Sechs-Augen-Prinzip
6	System setzt Achse 2 (gerichtsfest) nicht selbst	extern: EVR

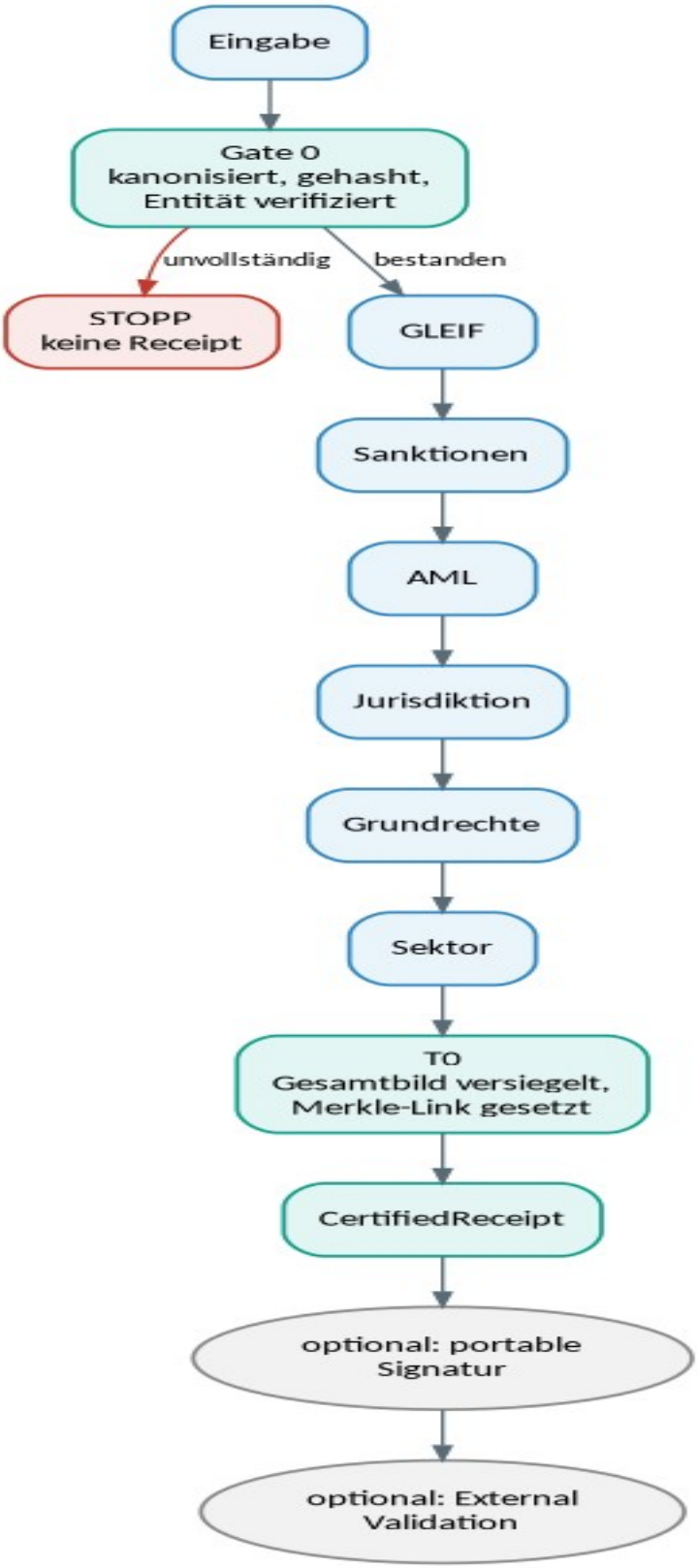
Tabelle A12: Export und Verifikation

Export	HMAC	ECDSA	EVR
Intern	Ja	Optional	Optional
An Vermittler	Ja	Ja	Optional
An externen Empfänger	Ja	Ja	Empfohlen
Öffentliche Prüfung	(unzureichend)	Ja	(+)

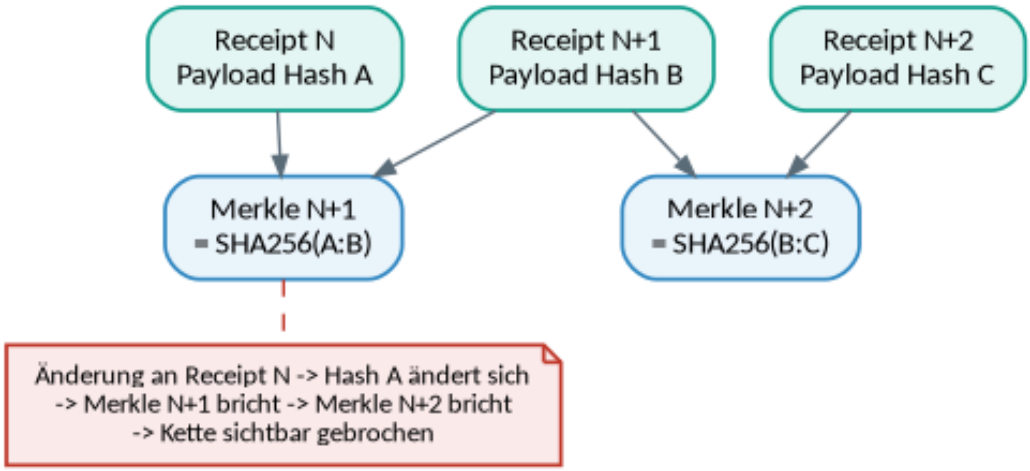
Tabelle A13: Kostenkategorien und Werte

Frage	Antwort des Systems
Preis pro Prüfung?	Falsche Frage
Preis pro Beweis?	Richtige Frage
Abrechnungseinheit	Empfangsgrenze (Verantwortung)
Abrechnung	Jahreslizenz
Vermittler-Rechnung?	Ja

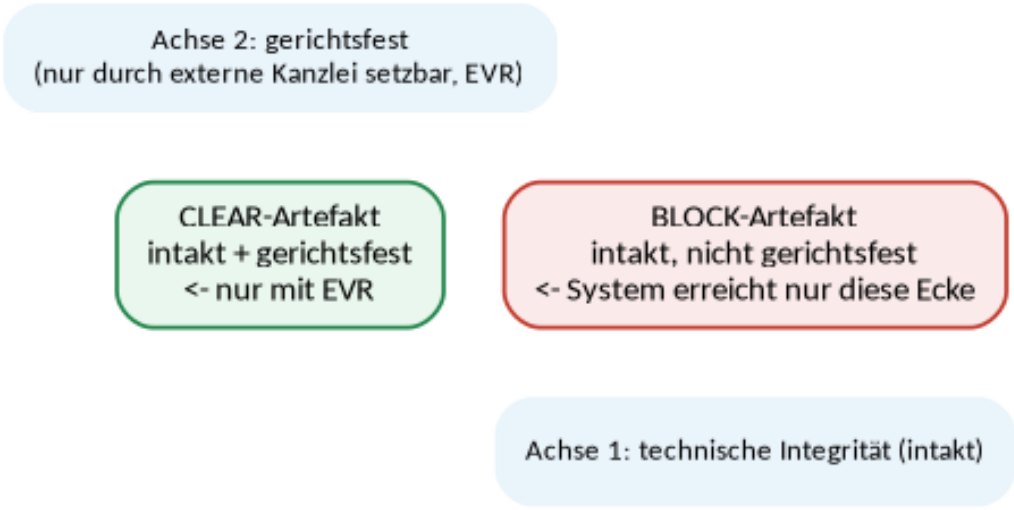
Skizze B1: Gate-Pipeline-Ablauf



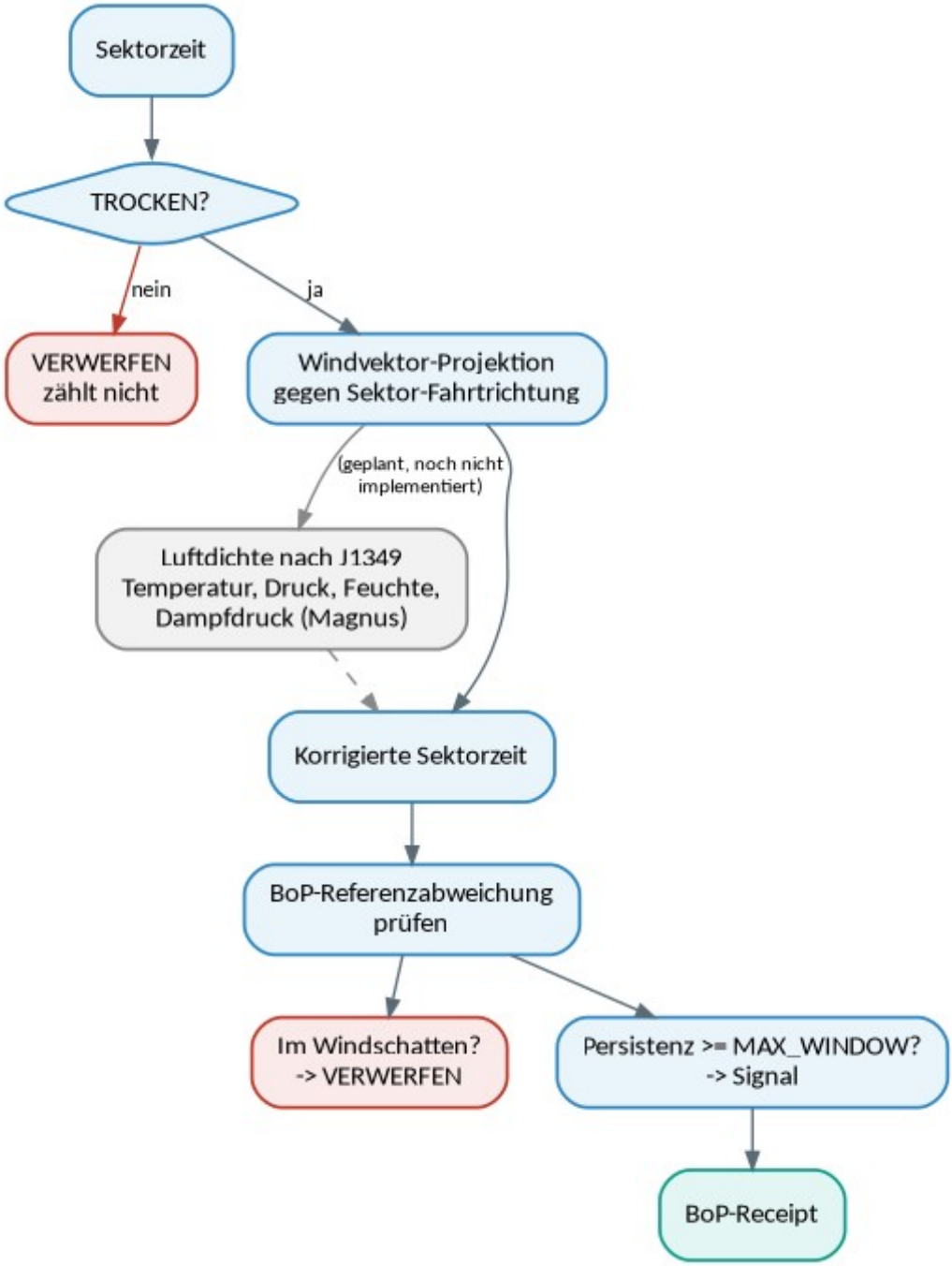
Skizze B2: Merkle-Verkettung



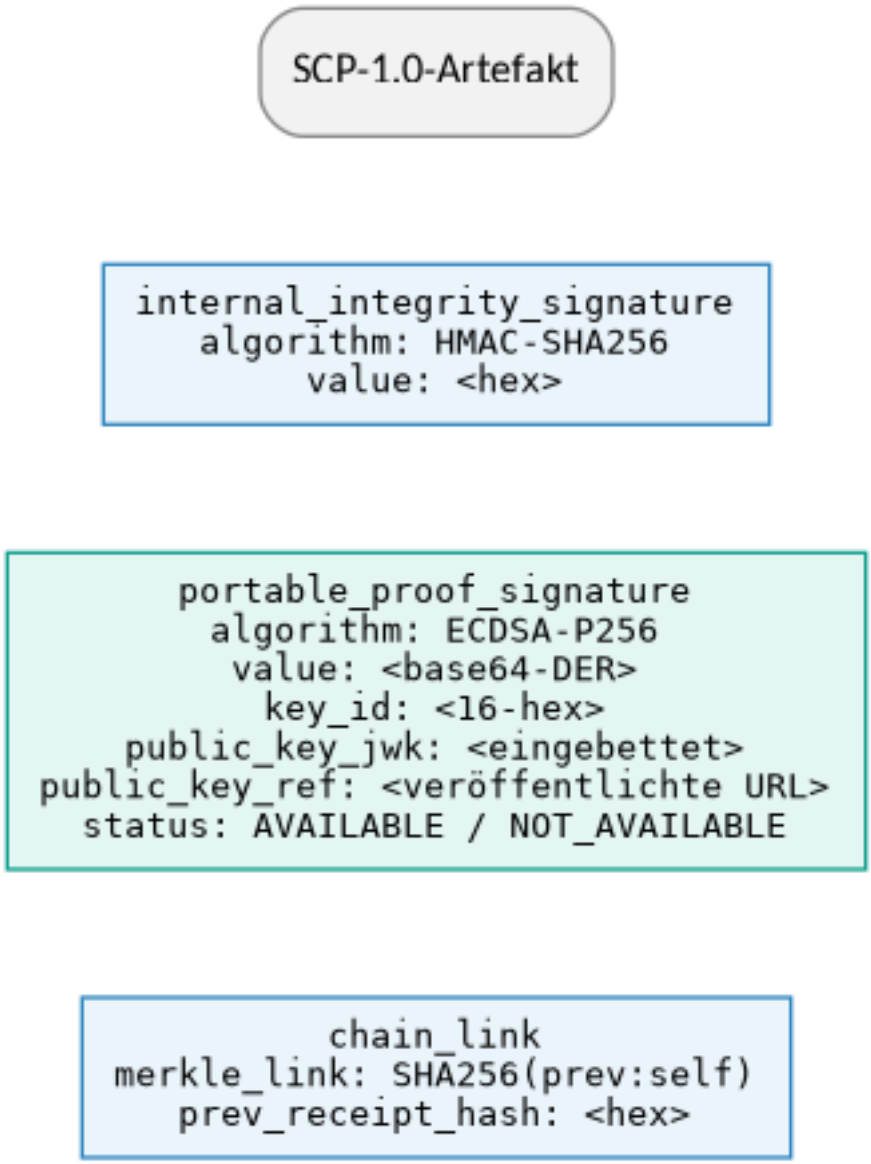
Skizze B3: Zwei-Achsen-Diagramm



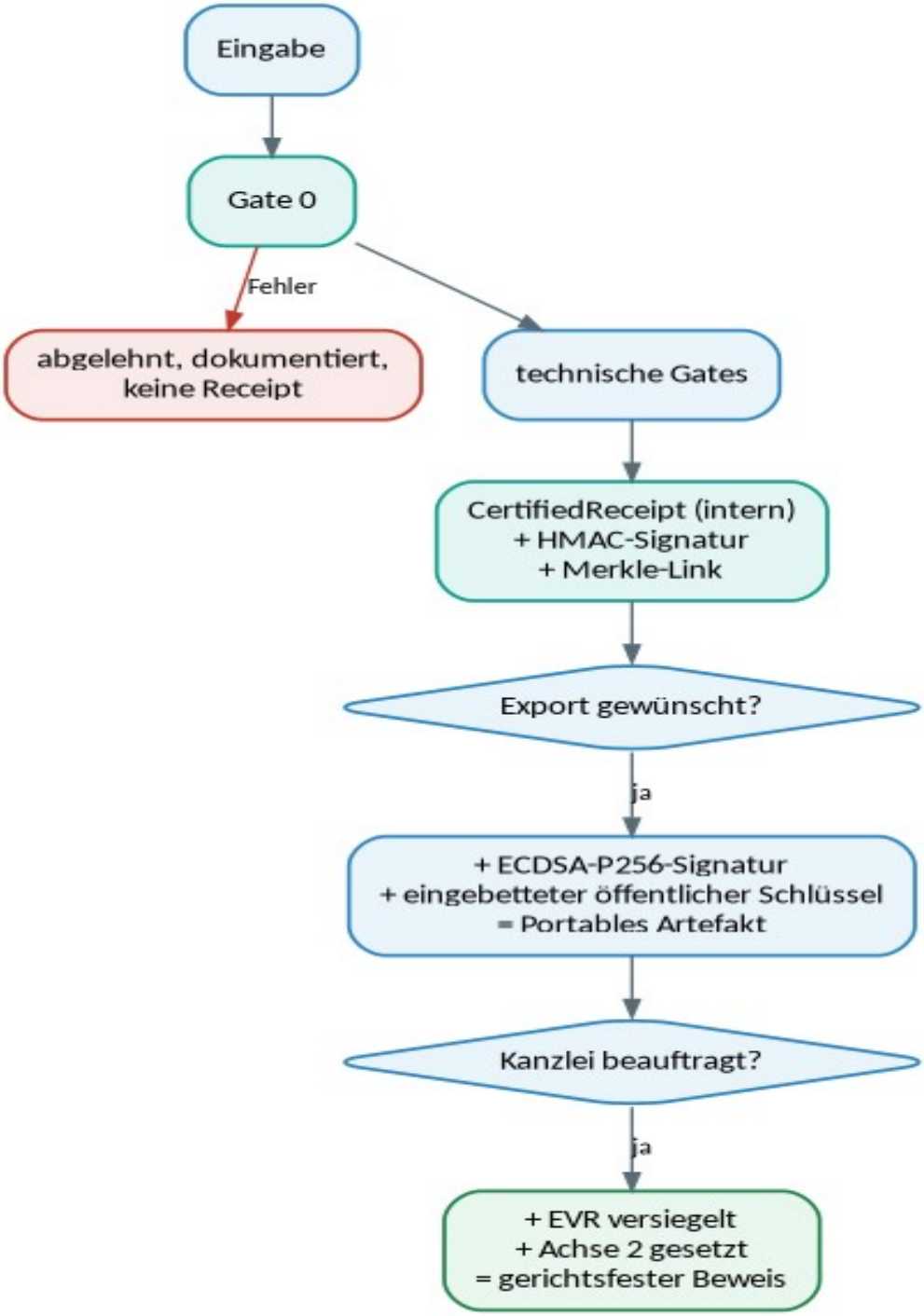
Skizze B4: Wetter-Korrektur-Pipeline Gate M9



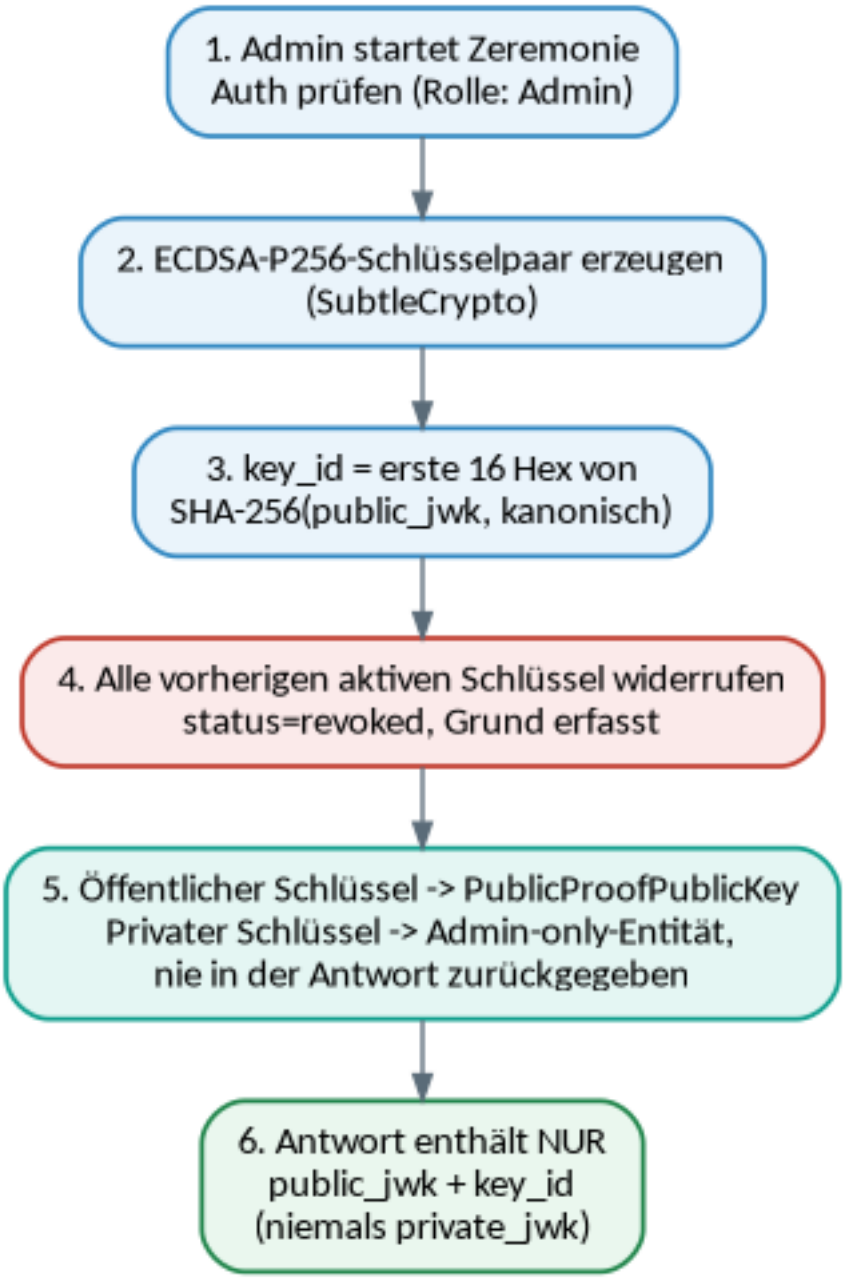
Skizze B5: SCP-1.0 Verifikationsblock



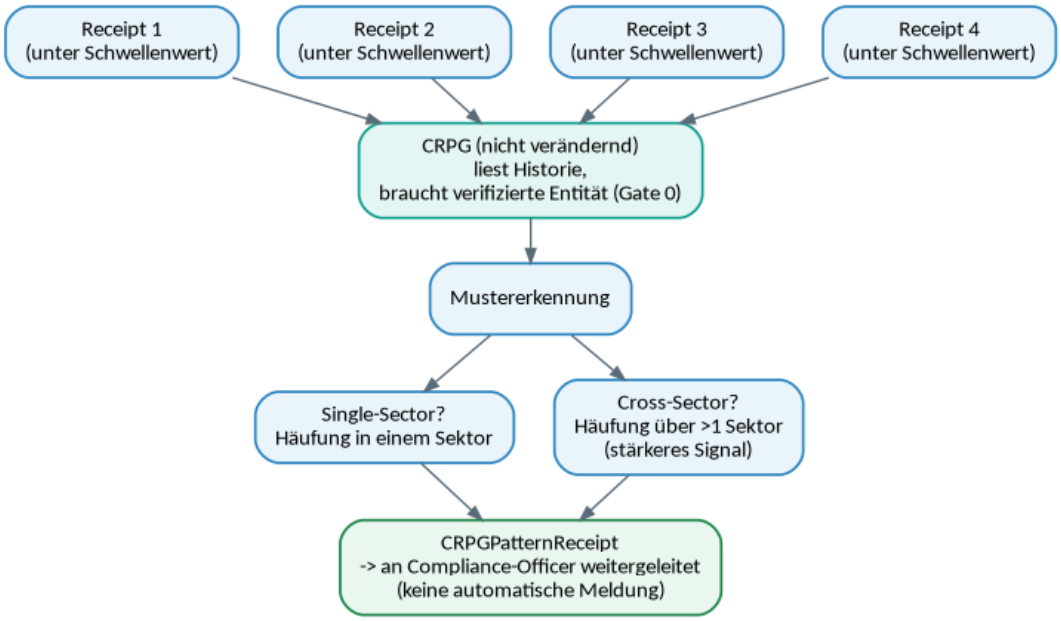
Skizze B6: Receipt-Lebenszyklus



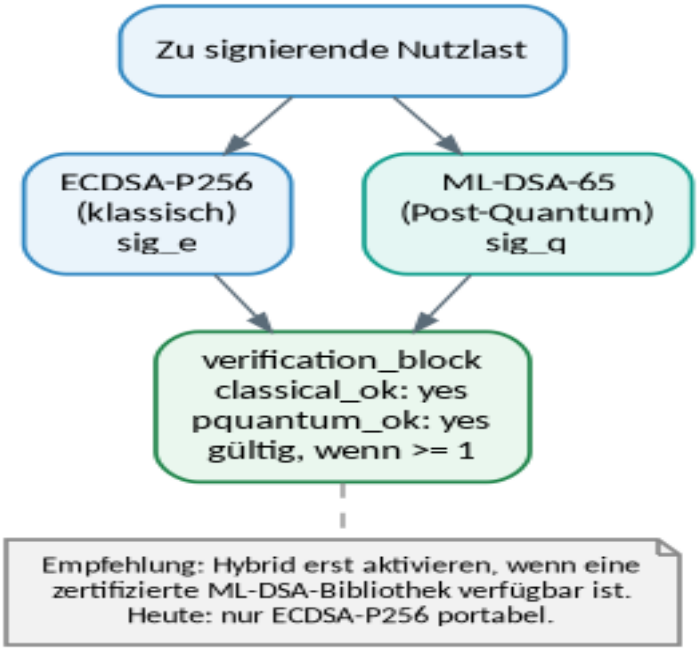
Skizze B7: Schlüssel-Zeremonie v2



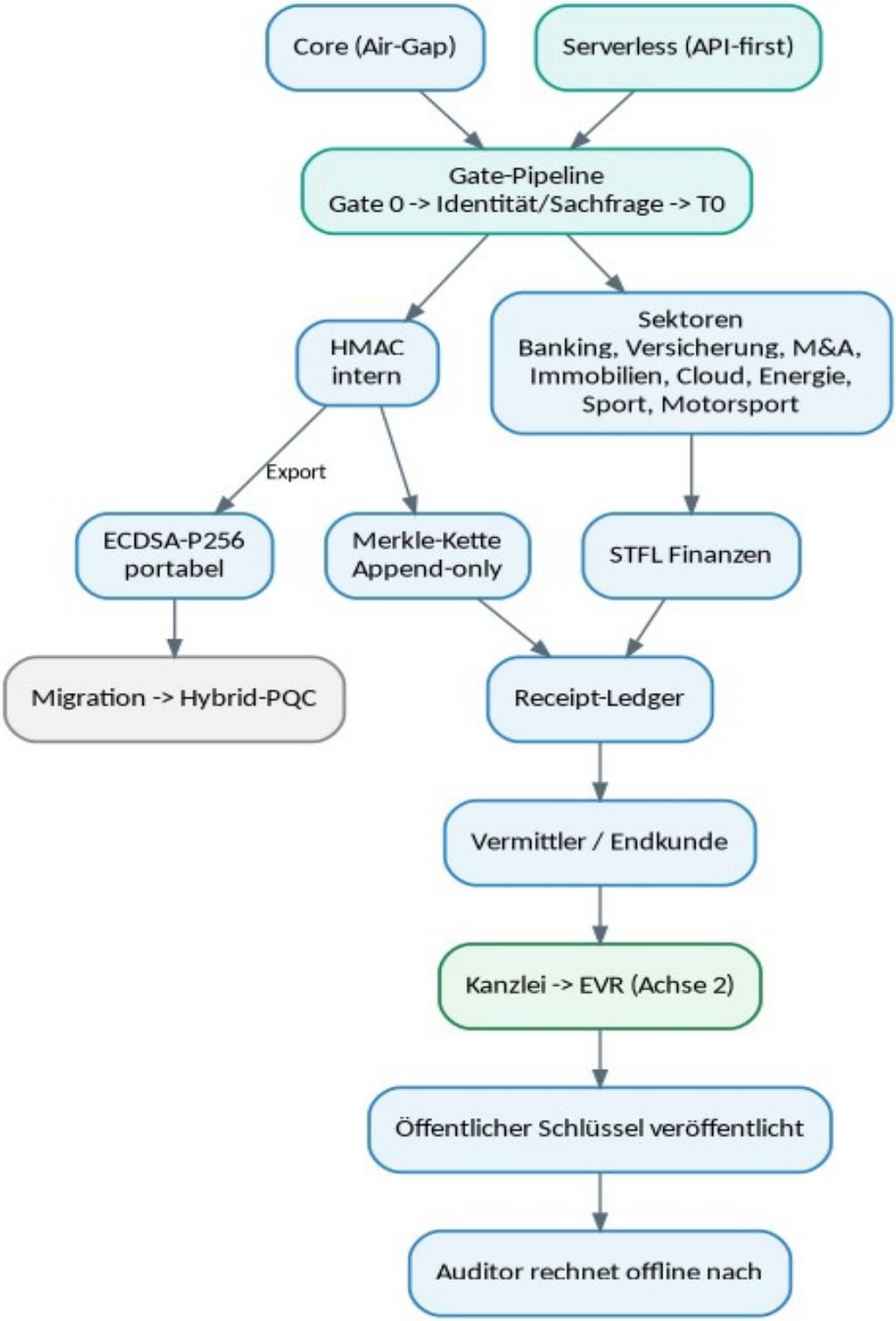
Skizze B8: CRPG-Architektur



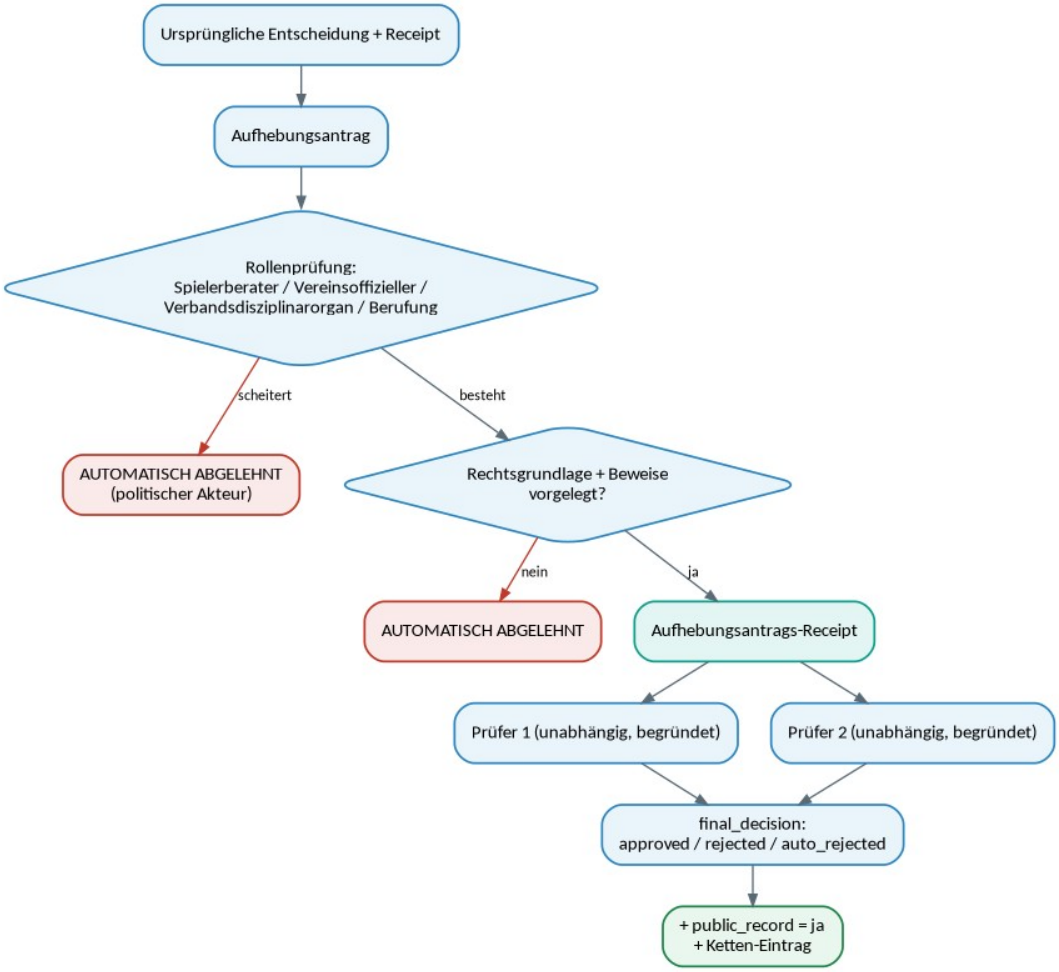
Skizze B9: Post-Quantum-Hybrid-Signatur



Skizze B10: Systemarchitektur im Überblick



Skizze B11: Aufhebungsverfahren


Ursprüngliche Entscheidung + Receipt
Aufhebungsantrag
Rollenprüfung:
Spielerberater / Vereinsoffizieller /
Verbandsdisziplinarorgan / Berufung
scheitert
besteht
AUTOMATISCH ABGELEHNT
(politischer Akteur)
Rechtsgrundlage + Beweise
vorgelegt?
nein
ja
AUTOMATISCH ABGELEHNT
Aufhebungsantrags-Receipt
Prüfer 1 (unabhängig, begründet)
Prüfer 2 (unabhängig, begründet)
final_decision:
approved / rejected / auto_rejected
+ public_record = ja
+ Ketten-Eintrag