System Documentation

immo.quick Ecosystem — Architecture, Legal Foundations, Governance Principles

immo.quick Global UG

July 2026 · Public Reference Documentation

immo.quick Serverless Edition

System Documentation

This document describes a system not as a product but as an answer to a world. It first explains the world in which compliance takes place today, and from that world it derives the system. Whoever has understood the world understands the system not as a tool but as an attitude.

Part One: The World In Which This Documentation Arose

Before a single algorithm is described, the reason why an algorithm is needed at all is described. Compliance today is no longer a document one presents. Compliance is a proof one delivers. And that proof must still be deliverable years after the event, when nobody remembers the event anymore.

Chapter 1: The World Of Compliance As It Is Today

Scenario 1: The Vanished Basis

Three years after a loan is granted, a compliance officer sits in a witness stand. The opposing side asks on which sanctions list exactly the check ran then. The officer answers, on the EU list. The opposing side asks further, which version of the EU list. The officer answers, the one that was current then. The opposing side asks, where does it say which version that was. The officer falls silent. The PDF in the files says sanctions check unremarkable. The PDF does not say against which version, at which time, with which rule version, on which input. The PDF is a claim of the department. It is not a proof.

In this moment a compliance decision that was strong for three years collapses. Not because it was wrong, but because its basis was documented, not held. And this difference shows up exactly when it matters. In the review, in court, in the supervisory audit, in the forensic investigation.

Scenario 2: The Smoothly Polished Probability

A software says, this case is 92 percent unremarkable. Three years later a forensic accountant wants to reproduce why 92 percent stood. He cannot. The 92 percent came from a model that had a particular training date, a particular confidence threshold, a particular version of the classification. Today the model is different, the training data is different, the confidence threshold is different. The 92 percent from then are not reproducible. They were a snapshot, not a statement. And a snapshot does not hold what a statement must hold. Reproducibility over time.

Scenario 3: The Three Isolated Notes

An insurer checks a payout in a death case. Three tools work side by side. The AML tool checks the beneficiary, the Solvency II tool checks the capital impact, the IDD tool checks the conduct duty in investing the remaining assets. Three tools, three PDFs, three notes from the advisers. After ten years, in an insurance supervision, stand three isolated documents that are not related to each other. The

supervisor asks, did you check IDD, Solvency II, and AML on the same entity, at the same time, in the same input decision? The insurer must answer, we used three tools and their results were available to us separately. The supervisor will ask, and the link? Silence.

Scenario 4: The Retrospective Rule Change

An energy supplier procured energy imports in summer. In winter the review comes, was the procured origin sanctionable? The compliance officer says, we checked against the sanctions list that was current then. The supervisor asks, which version? The officer says, the current one from then. The supervisor asks, where is the hash reference to that version? The answer is a PDF archive in which the list is referenced as current without version reference. Nobody can reproduce which list exactly was meant. The review becomes a question of faith, not a question of calculation.

Scenario 5: The Unnoticed Fundamental Rights Collision

An authority applies a rule that arose from a technical concern, without the rulebook noting which fundamental rights conflict is at stake in it. The rule is applied, the result looks clean, the file is closed. Years later, in a constitutional court dispute, it turns out that this rule lacks the fundamental rights discussion. The fundamental rights discussion was never held because nobody initiated it. The consequence is not a correction of the decision but a reconstruction weakness that can no longer be remedied afterwards. The decision was cleanly documented, but it had been blind to fundamental rights.

Scenario 6: The Structure That Only Becomes Visible In The Cross Section

An entity carries out fourteen transactions over nine months, each individually below the reporting threshold. Each individual check shows, transaction unremarkable, not reportable, next check. Nobody sees the pattern because nobody looks across the transactions. At the end of the nine months a structuring lies present that was never recognized as structuring because the tool viewed each transaction in isolation. Anti structuring provisions exist because this cross section requirement is very real, and no single case tool is built to work it.

Scenario 7: The Manipulation Nobody Saw

An audit log allows retrospective changes. Someone changes an entry that is three months old. The entry now looks different, but nobody can reproduce that it was changed because the log is not append only. In a forensic dispute the opposing side asks, can you prove that this log has been unchanged for three months? The respondent must say, no, the log is mutable. The credibility of the entire archive drops in one sentence.

Scenario 8: The AI Decision Nobody Can Recalculate

A software makes a compliance decision with an AI. Three years later the opposing side asks, why exactly this decision? The software cannot reproduce the decision because the AI depended on a model version that no longer exists. The decision remained a black box, and the black box has closed. The opposing side cannot reproduce the decision, and the deciding institute cannot defend the decision. In a

court dispute it does not depend on who claims but on who can prove. An AI that decides cannot prove. A rule that is applied deterministically can.

Scenario 9: The Receiving Examiner Without Prior Relationship

An institute A hands a compliance result to an institute B. Institute B has no prior relationship with institute A. Institute B wants to verify the result. Institute A says, trust us, we checked it. Institute B asks, can I reproduce it myself? Institute A says, not without our internal system. Institute B must therefore decide, either trust without being able to reproduce, or reject because recalculation is not possible. Both are unsatisfactory in a compliance chain. A decision that rests on blind trust is not a decision that can be carried forward in a chain. A decision that is rejected because it is not reproducible breaks the chain.

Scenario 10: The Infrastructure Nobody Controls

A European institute runs compliance checks in a cloud that sits under the sovereignty of a US parent group. Under the CLOUD Act this cloud can, on order, release data to US authorities, including data stored in the European data center. In a compliance relevant dispute the institute cannot safely say that no non European authority accesses the data. The compliance check itself becomes a compliance risk. That is no theoretical scenario, it is the world everyone lives in who has their data with a US provider.

Scenario 11: The Chain That Was Not Gapless

An institute documents every check, but between two documentations a gap yawns because a maintenance window lay in between and in that window a check was not sealed. Years later an examiner asks, what happened in this gap? Nobody can say. The gap is not filled because the chain is not append only and because there is no compulsion to seal every check. The gap is small, but it is there, and in a forensic dispute one gap suffices to call the whole chain into question.

Scenario 12: The Witness Who Is No Longer Reachable

An employee justified a compliance decision. The justification stands in an email. The employee has left the company, the email was deleted because the retention period expired. Years later nobody can say what the decision rested on. The decision may have been correct, but its justification has vanished because it stood in a volatile medium, not in a sealed chain.

Chapter 2: What These Scenarios Have In Common

All twelve scenarios share one property. A decision was made, documented, and filed. The decision was clean in its moment. But in the review it collapses because its basis was not held but only claimed.

That is no question of compliance effort. It is a question of compliance method. And the method today, in almost every institute, is the same. Documenting instead of holding. Reporting instead of proving. Probability instead of determinism. Isolated tools instead of coupled chains. Audit logs instead of append only chains. AI that decides instead of rules that are applied deterministically. Volatile media instead of sealed justification.

Whoever has understood this world has understood why the question is not, how do we do even more compliance. But, how do we do compliance that holds in the review.

Chapter 3: The Red Thread

The sentence that carries the whole system reads:

> ***Governance without basis is only an opinion.***

By opinion is meant here not a personal stance but a result that is no longer reproducible afterwards. A compliance decision that stands only in a PDF is strong until an opposing side demands reproducibility, and then it collapses. Exactly this weakness the system closes. And it closes it not through a better PDF. It closes it through a different method.

This method has four pillars.

First pillar. Proof instead of documentation. A documentation claims what was checked. A proof holds cryptographically sealed which rule, in which version, with which data, at which time led.

Second pillar. Determinism instead of probability. A probability statement is not reproducible afterwards. A deterministic rule applies a clear prescription to clear data. Today the same result as in ten years.

Third pillar. Checking instead of trusting. A decision that rests on blind trust cannot be carried forward in a chain. A decision that is cryptographically reproducible can be checked by any third party without prior relationship.

Fourth pillar. Gaplessness instead of gappiness. A chain in which a check is missing is not a chain but a collection. The system forces every check into the chain so that a missing check becomes visible, not unremarkable.

Whoever has understood these four pillars has understood why the system is not yet another compliance tool. It is a different method.

Chapter 4: What This Method Presupposes, And What It Does Not

The method presupposes that a rule exists, that an input exists, and that a point in time exists. Nothing more. It does not presuppose that the rule is correct, that the input is complete, or that the point in time is favorable. It takes what is, seals it, and makes it reproducible.

That is important because it marks the limit of the method. The system cannot guarantee that a rule was correct. It can guarantee that the rule that was applied is reproducible. The system cannot guarantee that an input was complete. It can guarantee that the input that was checked is unchanged. The system cannot guarantee that a point in time was well chosen. It can guarantee that the point in time at which the check took place is faithfully recorded.

This distinction is decisive. Whoever reads the system as a guarantee for correct decisions has misunderstood it. Whoever reads it as a guarantee for reproducible decisions has understood it.

Part Two: The Three Foundation Standards

Chapter 5: CDS, Constitutional Divergence Screening

What it is. CDS is a two stage scanner that searches a legal text or a rule draft before the rule contained in it is applied at all. The check does not go to technical questions but to the fundamental rights level. Does this text touch a fundamental right, and in a pattern that creates a collision, that is, a tension between two goods of the legal order that is not fully resolved in the text itself.

The scanner has two independent stages.

First stage, collision pattern level. Which structural fundamental rights collisions the system recognizes. Currently 156 patterns, grown from an earlier base of 47. This figure indicates how many such patterns the system recognizes.

Second stage, jurisdiction level. In how many legal orders are these patterns applied. Currently 53 jurisdictions.

The two counters are deliberately never offset against each other. A pattern can apply in many jurisdictions, a jurisdiction can contain many patterns. A mixed figure like perhaps a few thousand possible combinations would be deceptive because not every pattern is really relevant in every jurisdiction. The separation is thus no accident but protection against such obscuring arithmetic.

Why it exists, in light of scenario 5. Scenario 5 described a rule whose fundamental rights collision nobody initiated. The consequence was a reconstruction weakness that could no longer be remedied afterwards. CDS closes exactly this gap in advance. Before a rule is applied, the scanner documents the touching of a fundamental rights pattern in the emerging piece of evidence. The fundamental rights discussion is no longer left to chance whether someone initiates it. It is methodically anchored.

Example. A legislator issues a rule that obliges internet platforms to delete certain content. Technically a rule about deletion duties. In fundamental rights terms an intervention in freedom of expression, combined with a checking duty that hits the platform. CDS recognizes the pattern freedom of expression against deletion duty and marks the touch in the emerging piece of evidence. Later, when a future rulebook applies this rule, the piece of evidence carries the hash reference to the fundamentally rights checked version. In the serious case a fundamental rights discussion is available, not as a comprehensive opinion but as a documented touch that makes such a discussion visible and does not silently overlook it.

How it connects. CDS is the entry check of every new rule catalog version. When the pipeline later applies a rule, the emerging piece of evidence carries the hash reference to the fundamentally rights checked version. A later examiner sees, the rule was already tested for fundamental rights collisions before its application. CDS is no technical gate but the prior check of the rule itself. It does not decide whether the rule is technically correct but whether it is fundamentally rights transparent.

Expansion. CDS is not static. The pattern library grows because the fundamental rights discussion grows in the jurisdictions. A collision that is not yet recognized in a jurisdiction today can become recognizable tomorrow because a court judgment opened the discussion. The system holds the library versioned, so that a receipt generated today refers to the library valid today, and a receipt generated tomorrow to the library valid tomorrow. The library too is hash anchored. Nobody can afterwards claim a receipt was checked with a different library than the one it refers to.

Chapter 6: STFL, Sovereign Transaction Finance Layer

What it is. STFL is the layer that connects every compliance result with the commercial side, with billing, invoicing, and booking. Every sealed receipt is not only a technical event but also a billable event. STFL translates the sealed receipt into a bookable structure.

Why it exists, in light of scenario 3. Scenario 3 described three isolated tools whose results stood in three isolated PDFs and that after ten years stood in three isolated notes. STFL is the counter model. Every sealed receipt is a cryptographically fixed source that flows into the booking. Not the designation compliance fulfilled is referenced but the concrete, retrospectively checkable chain. The finance side can no longer take over the compliance side as a text reference but only as a hash anchored source.

Example. A bank carries out 247 GLEIF checks in a month. Each check produces a CertifiedReceipt, each receipt is a sealed, hash anchored, billable event. STFL translates the 247 receipts into the booking relevant structure. Each receipt produces an entry in the Receipt Ledger that is billable. The monthly settlement aggregates the receipts into an invoice that in turn references the list of receipt IDs. The invoice is thus not an isolated claim of accounting but a hash referenced statement over exactly the same receipts that the compliance side produced. An auditor checks invoice against receipts, and every entry is traceable one to one.

How it connects. STFL sits at the end of the pipeline. First the receipt is created, STFL translates it into booking and reporting events. The invoice references the underlying receipts and is thus itself cryptographically verifiable, not an isolated claim of accounting.

Expansion. STFL supports several invoice channels. One channel is the standard PDF by email, one channel is XML API delivery to an ERP system, one channel is straight-through processing in a public procurement network, one channel is the e invoice according to the European standard for public procurers and large enterprises. The system does not decide which channel is the right one, it provides all. The receiver chooses the channel that fits his accounting. The receipt behind the invoice is the same in all channels. The channel changes the form of the invoice, not the source of the invoice.

Chapter 7: SCP 1.0, Sovereign Compliance Proof Standard

What it is. SCP 1.0 is the data model, the signature protocol, and the chain structure that formally describes every forensically robust artifact. It sets out which fields an artifact contains at minimum, what the canonicalized form looks like over which the hash is formed, how the signature blocks are built, how the Merkle chaining is referenced. SCP 1.0 is vendor neutral and openly documented.

Why it exists, in light of scenario 9. Scenario 9 described a receiving examiner without prior relationship who wants to verify a result but has no system beyond the producing institute to do so. SCP 1.0 solves that because it specifies a published, open format. Anyone who understands it can check an artifact without having to consult the producing system.

Example. A Portable RDR handed to a receiver is a standalone document in an open data structure. It carries the receipt ID of the underlying CertifiedReceipt, the rule and its version, the result, the verification block with two signature classes, the embedded public key, and the reference to the publicly published key. The receiver, a law firm with no prior relationship to the system, can verify exactly this artifact without having to consult a second system. It reads the embedded public key or retrieves the publicly published one, checks the signature, recalculates the hashes, and confirms integrity. SCP 1.0 is the format that enables this self support.

How it connects. All evidence artifact types build on SCP 1.0. The CertifiedReceipt, the RelianceDecisionRecord, the T0 artifact, the sector specific receipts, the due diligence artifacts, and the portable formats. Whoever has understood the data model once understands the formal scaffold in every sector.

Expansion. SCP 1.0 is versioned. The system can extend the data model when new evidence artifact types are added. An extension is not retrospective but stacked. An artifact produced in version 1.0 remains in version 1.0. An artifact produced in version 1.1 carries the version number 1.1. An examiner who sees both versions knows which format he has in front of him and can check both. The system does not overwrite, it stacks.

Part Three: Execution

> ***immo.quick Core is a separate product line with its own architecture and its own scope of functionality. This documentation describes exclusively the immo.quick Serverless Edition. Statements made in this documentation must not be applied to Core.***

Chapter 8: immo.quick Serverless Edition

What it is. The Serverless Edition is the API first execution. A customer calls an API endpoint, the pipeline runs, the result comes back as a receipt or as a portable artifact. There is no server the customer additionally operates.

Why it exists. Many users need compliance as an API without operating a server. Teams that scale compliance mass checks, market participants that integrate check results into their own software, integrations that connect an API to their own ERP.

Example. A fintech that carries out ten thousand business partner checks daily and operates no compliance team that could maintain its own execution environment calls the API of the Serverless

Edition. Each check comes back as a sealed receipt that is filed and exported when needed. The fintech operates no infrastructure, it only operates API calls.

How it connects. Every receipt produced by the Serverless Edition follows the SCP 1.0 standard described in Part Two. The choice of execution model for a given use case is a separate, product level question outside the scope of this document.

Chapter 9: Why The European Infrastructure Choice Is An Architecture Topic

The execution lies in European infrastructures, for example Hetzner, IONOS, OVHcloud. That is not only a cost or availability decision but an architecture decision with legal reasons.

The CLOUD Act is a US federal law that obliges US based cloud providers to release data to US authorities on order, even if the data is stored in Europe. A European customer whose data lies with a US provider cannot be sure in a compliance relevant dispute that no non European authority gains access.

With a European provider, and by that is expressly meant a provider with headquarters and data storage in an EU member state jurisdiction, not only a provider with a European data center but a US parent group, the legal situation is different. A release by an EU authority runs via EU legal channels and opens no automatic channel to US authorities. This choice does not protect against legitimate European requests but gives control over the legal framework under which a release takes place at all. That is exactly why the choice of European infrastructure is an architecture decision, not cosmetics.

Expansion. The choice of infrastructure is not the only architecture choice legally relevant. The question of where the keys lie is also relevant. A key that lies in a US cloud is subject to the same CLOUD Act. A key that lies in a European infrastructure is subject to European law. The system holds the private keys exclusively server side and exclusively in an infrastructure that is subject to European jurisdiction. That is not paranoia but the logical consequence of scenario 10.

Part Four: The Interior Of The System

Chapter 10: The Gate Pipeline In Detail

What the pipeline is. The Gate Pipeline is the chain of individual checks that an input data set passes through, from receipt over various rules to the delivered receipt. A gate is an isolated, independently versioned rule application. A gate is not the compliance but a concrete building block that applies a concrete rulebook to a concrete input. The order of the gates is not arbitrary. It follows a result concept. An early gate that checks clearly stopping input, say a sanctions hit, makes the later gates for this workflow technically obsolete.

The complete sequence. An example. A bank submits a transaction check request. Please check the entity with LEI 5299 regarding transaction T 7741. What happens, step by step.

First step, inlet and input hash. The request is canonicalized, the input hash is computed. From now on the input is immutably brought into the receipt chain. A change of the input after this point breaks the chain visibly.

Second step, GLEIF validation. The LEI is run against the GLEIF register. The gate captures the entity status, the GLEIF snapshot version, and the GLEIF snapshot hash at the time of the query. If the LEI is invalid or the entity dissolved, the gate documents exactly this finding, not a guess.

Third step, sanctions screening. Entity and, where available, registered beneficial owners are run against the relevant sanctions lists. EU FSF, OFAC SDN, UK HMT, UN SC, FATF. Each list carries a list hash. The receipt references the list and the hash. Hit, documented as a BLOCK occasion. No hit, documented as part of the CLEAR picture. Unclear, documented, not concealed.

Fourth step, AML check. The sector specific AML check, here under the money laundering act, is applied. The AML check is not the money laundering assessment itself. Money laundering structure recognition is CRPG, part seven of this document. It is the due diligence and reporting duty logic regarding the concrete transaction.

Fifth step, jurisdiction conflict. The transaction touches several jurisdictions. The gate checks for a collision between the applicable legal orders, in particular the tension between the EU Blocking Regulation and the US extraterritorial sanctions application. If such tension exists, the gate documents it. The receipt is not silently decided toward one side or the other but documented in the tension.

Sixth step, fundamental rights check. The rule to be applied is checked CDS based. The touch of a fundamental rights pattern, if present, is documented.

Seventh step, sector specific. Banking logic. Basel III minimum capital check if the transaction touches the capital ratio. Or a sector specific gate according to the type of transaction, say MiFID II suitability in an investment decision.

Eighth step, receipt produced. The CertifiedReceipt is created, is signed, inserted into the Merkle chain. The portable version gets the asymmetric signature when needed. The artifact is fully ready for further checking.

Chapter 11: The Principle Of The Versioned Rule Basis

Every rule a gate applies carries a version number and a hash. That is the answer to scenario 4. Legal sources change. A judgment is added, an EU directive is amended, a sanctions list gets an entry added. If a receipt only says rule X applied, it is not clear which version of rule X was applied. Afterwards nobody can reconstruct whether the result that was achieved then still rests on the version current today.

Therefore every rule carries a version number, and the system has a catalog versioning. Only when a new version of the rule catalog is deposited with a new hash may the new version be applied. The receipt references the hash of the rule it applied. Thus a later examiner can always determine whether the legal situation has changed in the meantime and whether the old statement is still valid.

Example. A receipt references the EU sanctions list in the version of 14 July 2026 with hash X. Three years later the list is valid in a new version, with hash Y. The examiner can answer two questions. Was the entity then on the list then. Yes, reproducible from hash X. And is the entity today on the list today.

That requires a new check against hash Y. Both questions are cleanly separated because the versioned rule basis allows it.

Expansion. The versioned rule basis is not only a protection against forgetting but a protection against a presumptuous present. Whoever claims today that a check was correct under today's legal situation although it took place three years ago mixes two time layers. The versioned rule basis forces the separation. The check was correct under the legal situation of then, measured against the list of then. Whether it would be correct under today's legal situation is a different question that requires a new check. The system allows both questions but it does not allow mixing them.

Chapter 12: The Data Sources Of The Pipeline

GLEIF. The Legal Entity Identifier register, the international source of company identification.

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

Legal sources by sector. BGH case law, Basic Law, EU Charter of Fundamental Rights, DORA, Basel III, Solvency II, MiCA, Money Laundering Act, Foreign Trade and Payments Act and Regulation.

Published rule catalogs. Each version with its own hash, referenceable, not overwriting.

Expansion. Every data source carries not only a hash but also a time of query. The time is important because a list queried today can look different tomorrow. The system documents not only which list was run but when it was run. An auditor asking, was this list the current one at the time of the check, finds the answer in the receipt, not in a guess.

Chapter 13: Gate 0, The Entry Gate Of The Overall Pipeline

Gate 0 is the entry gate of the overall pipeline. In the sector logic individual sector engines have their own gate numbers, M0 to M9 in motorsport, but systemwide Gate 0 is the fundamental, systemwide entry check. All further sector gates are subordinate.

What Gate 0 is. Gate 0 is the check of the forensic admissibility of the input in advance. It is no technical gate. It does not decide on foul or no foul, on sanction report or no sanction report. It decides on the question, is the input processable in a proof generating way at all. Does the input have the properties that allow a forensically robust receipt.

Why Gate 0 exists. Every later receipt can only be as loadable as the input from which it arose. A precise rule applied to an input that is incomplete, that is not cryptographically fixed, that is not assigned to a verified entity, that was captured without an NTP time anchor, such an input produces a receipt that fulfils all formal properties but collapses in a forensic dispute because the input itself did not stand where it had to stand. Exactly this weakness cannot be remedied afterwards. One cannot retroactively give a receipt a reliable entity reference if the entity was not cleanly resolved at input. Gate 0 exists therefore to close this weakness in advance.

What Gate 0 checks in detail. Gate 0 checks in sequence and documents for each step individually whether it was successful, warnful, or failed.

First check, canonicality of input. The input is canonicalized according to RFC 8785, JSON Canonicalization Scheme. That is the precondition for following hashes to be reproducible. Without canonicality a hash over the input would depend on the order of fields, on whitespace, or on the specific serialization form, and thus not be reproducible in another system. Gate 0 checks and documents that the input was canonicalized. The canonicalized form and its hash are part of the pre run.

Second check, completeness of mandatory fields. Every gate variant has mandatory fields, an entity identification, a transaction type, a technical context. Gate 0 checks that these mandatory fields are present and not empty. If a mandatory field is missing, Gate 0 stops, not to sanction the request but because a forensically robust receipt with missing mandatory fields cannot be produced. The reason is documented, without a receipt being produced.

Third check, entity identity, verified, not only claimed. Central aspect of Gate 0. The entity to which the check refers must be verified, not only stated. That means, the LEI, if present, is checked against GLEIF. If no LEI is present, a secondary identification must be present that Gate 0 likewise verifies. An unverified entity, name is stated but not checkable, is unfit for a forensic receipt. Exactly here the system separates from numerous tools that accept an entity only as claimed because the check later would determine whether the entity is real. That is the principle of shifting. The system here does it the other way. Verification before the technical check, because a retrospective verification on a receipt that has already technically rested comes too late.

Fourth check, source security of input. Where do the input data come from. An input can have various sources. A transaction in live operation, a government report, an external data feed, a staff note. Gate 0 documents from which source the input comes. The source identifier is part of the pre run. Later, in a forensic dispute, it is decisive whether the input came from a verifiable source or from a staff note.

Fifth check, NTP time anchor of input. The transaction time is NTP anchored. The time is thus not manipulable by the system alone. Gate 0 checks whether an NTP time anchor was assigned. If it is missing, Gate 0 documents that in the pre run record.

Sixth check, divergence of input. Where an input comes from several sources, say in a sports scenario with several camera perspectives, or a transaction data set with several data feeds, Gate 0 checks whether the sources agree. If the input diverges between sources, Gate 0 documents the divergence. The receipt is not silently decided in favor of a source, but the divergence case becomes part of the pre run, and a marking divergent is attached to the Gate 0 result. Later gates can interpret this marking. A subordinate gate can decide that a divergent input requires a deeper check.

What Gate 0 does when it passes. If Gate 0 has passed all six steps, input canonicalized, mandatory fields complete, entity verified, source documented, NTP time anchor set, divergence clarified, a Gate 0 result is produced from the following components.

A pre run protocol that documents for each of the six steps whether it passed, warnful, or failed.

A Gate 0 verdict that is expressly not a technical verdict, neither PASS nor BLOCK nor foul or no foul, but the statement input forensically admissible.

The handed over canonicalized input and its hash, binding for all subordinate gates from now on.

The verified entity identification, binding for the whole pipeline from now on.

What Gate 0 does not do. No technical judgment. Gate 0 does not decide on a matter, only on the forensics of the input. No gap filling. Gate 0 does not smooth. If a mandatory field is missing, it stops. It invents no default value. It closes no gaps. No AI decision. Gate 0 applies deterministic rules. Where an input is ambiguous, Gate 0 documents the ambiguity and stops. It does not try to decide for an interpretation.

Three examples for Gate 0.

Example 1, cleanly passing input. A request arrives with completely filled mandatory fields. LEI 5299, transaction name, transaction type, source System Transaction Feed, NTP anchored timestamp. Gate 0 canonicalizes the input and computes the hash. It checks all mandatory fields, complete. It verifies the LEI against GLEIF, entity active, GLEIF snapshot version present, GLEIF hash present. It documents the source. It checks the NTP time anchor, set. There are no several sources, so no divergence step. Gate 0 passes successfully. The Gate 0 result is available, and the subordinate technical gates can work.

Example 2, stopping input. The same request, but the LEI is invalid. Gate 0 canonicalizes the input, finds the mandatory fields complete, verifies the LEI against GLEIF, LEI not found. Gate 0 stops. A pre run protocol is produced with the entry, step three failed, LEI not verifiable. No receipt produced. Reason, a forensic receipt without verified entity is not loadable. There is no receipt and no technical check. That is no point of view system, it is the conditions without which the system does not work.

Example 3, divergent input. A sports scene with two camera perspectives whose data agree on some but not all parameters. Gate 0 canonicalizes the input, finds the mandatory fields present, verifies the secondary identification, documents the source, checks the NTP time anchor, and checks the several sources for divergence. The two camera feeds agree on speed, diverge on contact direction. Gate 0 documents the divergence. The Gate 0 result gets a marking divergent in the pre run protocol. A subordinate technical gate can interpret this marking. Say it can order a deeper check or suggest a racing incident. But the divergence is not silently decided in favor of a source. It is documented. A later forensic review sees, this input was divergent, and this divergence was held in the pre run.

How Gate 0 connects with the rest. Gate 0 is the pre gate of all technical gates. No receipt without Gate 0. No technical check without Gate 0. No procedure without Gate 0. In the layering of the pipeline, Gate 0 is the point at which the forensic loadability of all following levels decides. Gate 0 is thus not yet another building block but the founding condition of the whole pipeline.

Gate 0 is also the point at which the entity identity is deposited as verified, a property that CRPG urgently needs. A cross section analysis without verified entity is worthless. Gate 0 is thus not only formally subordinate but functional. It is the point at which forensic admissibility and entity verification stand firm before anything technical may happen.

Expansion. Gate 0 is not rigid but it is binding. The six checks can be extended per sector. A sector that requires additional mandatory fields can extend Gate 0. But the core duties, canonicality, completeness, entity verification, source security, time anchor, divergence, are not negotiable. They are the foundation on which everything stands. Whoever abandons one of them abandons forensic loadability.

Chapter 14: The Two Verification Classes

This is the point at which the system draws the line between we claim it and independently verifiable. This line runs right through the cryptographic architecture.

Class 1, internal chain integrity, HMAC. The first verification class is the HMAC, a Message Authentication Code on the basis of a hash function, SHA 256. HMAC is symmetric cryptography. A group of involved parties shares in advance a secret, the so called key. When receipts are produced they are signed with this key. Whoever possesses the same key can reproduce the signature and determine that the receipt comes unchanged from the producing system.

Why it exists, in light of scenario 7. Scenario 7 described a mutable audit log whose retrospective changes nobody could reproduce. The append only Merkle chain with HMAC is the counter model. The chain is extended at every step. Every new receipt references the hash of the previous one, combines both, and computes a Merkle link that is deposited in the receipt as chaining. A receipt cannot be changed afterwards without breaking the hash chain, and the break is verifiable with the shared key.

How it connects. This class covers the internal proof need, that is, proving that the infrastructure was not manipulated. It is directed inward, not outward. Strictly speaking it applies only where the shared key can be securely distributed, and it cannot solve the problem of the receiving examiner who does not have such a key.

Class 2, portable, externally verifiable signature, ECDSA P256 with post quantum migration path. The second verification class is the asymmetric signature. A key pair with a private and a public key. The private key signs, the public key verifies. Concretely ECDSA P256 is in use today, an Elliptic Curve signature on the NIST P 256 curve. A documented migration path exists to a hybrid signature of ECDSA P256 plus ML DSA 65, the post quantum signature from FIPS 204, as soon as a certified library is available.

Why it exists, in light of scenario 9. Scenario 9 described a receiving examiner without prior relationship who either had to blindly trust or reject because recalculation was not possible. Asymmetric cryptography solves that. Verification by a third party that does not possess the shared key and previously had nothing to do with the producing system. A law firm, a court, an examiner, a supervisory body of the receiving institute. All these parties can check a portable artifact by using the public key to

recheck the signature over the data. Nothing of this verification belongs to a running connection, no continuing trust relationship, no shared secret. That is the boundary. HMAC says trust me at this point. ECDSA says check it yourself.

How it connects. The asymmetric signature is the class that appears exactly when an artifact leaves the own infrastructure. Internally the HMAC class suffices. For the portable artifact handed to a receiver the ECDSA class is used. The two classes are strictly separated. Each has its own part in the verification block of the SCP 1.0 artifact, and each has its own semantic meaning. Moreover, the system embeds the public key directly in the portable artifact so that it is completely self supporting, and the verifier can additionally crosscheck against the publicly published key. The system thereby closes an attack possibility that would otherwise exist. That a third party would insert their own public key in the artifact and thus create a false validity.

Example. A CertifiedReceipt is created internally. It carries an HMAC signature. The issuing bank and the own audit service share the HMAC key. Both can reproduce the signature. The artifact does not leave the internal environment. HMAC is the sufficient signature class.

Now the same receipt is handed to a receiving law firm that has no prior relationship to the system and that performs its own forensic check. HMAC does not suffice here. The firm would have the shared key, which destroys the property that the signature is known only to the producing circle. The consequence would be, the firm can check the signature but not whether it comes from the producing system or whether it comes from anyone who has the key, and the firm can view this with healthy doubt.

The solution. The artifact that leaves the own infrastructure additionally gets an asymmetric signature that is signed with a private key held exclusively by the system in a secured, server side context. The firm gets the public key, embedded in the artifact and additionally published via a public endpoint, and can verify the signature without ever having had a shared key. That is the transition. HMAC means trusted. ECDSA means checkable.

The decisive difference, expressly. Only the asymmetric signature allows a third party that never had contact with the system before a check without shared secret. That is the exact boundary between we claim it and it is independently verifiable. Whoever has understood the difference between the two classes has understood why it does not suffice to seal a receipt only with an HMAC. Such a receipt may be internally intact but it is not portable, not externally checkable, and cannot satisfy an external verification need.

Chapter 15: Post Quantum Cryptography And The Choice Of The Hybrid Approach

What it is. Post quantum cryptography covers cryptographic procedures that are considered resistant to attacks by quantum computers. The relevant standards are FIPS 203, ML KEM, key exchange, FIPS 204, ML DSA 65, a module lattice based digital signature, and FIPS 205, SLH DSA, a hash based alternative signature. ML DSA 65 is the variant that standardization selected as the signature procedure.

Why the hybrid choice. A complete migration from ECDSA to a pure post quantum procedure is not advisable today because the post quantum procedures are still relatively newly standardized, their implementations in practice are not yet long stressed, and some of their security assumptions are not yet as well established as those of classical Elliptic Curve procedures. A hybrid signature, that is ECDSA P256 plus ML DSA 65, combines the tested strength of the classical procedure with the future quantum resistance of the new procedure. The signature holds as long as at least one of the two procedures holds. This approach is also what national standardization institutes recommend in their post quantum migration guidelines.

How it connects. The ECDSA signatures valid today remain valid. The post quantum layer is additive. A future version of the portability block that will contain the ML DSA 65 component will yield the following verification block. A classical ECDSA part and a post quantum part that the verifier checks individually and together. The exact procedure and the certification of the integration are still in work. A date is not promised.

Expansion. The post quantum question is no future music but a question that must be decided today because receipts produced today should be verifiable in twenty years. Whoever signs only ECDSA today, and in twenty years a quantum computer stands, whose signatures are attackable. Whoever signs hybrid today, whose signatures remain valid because the post quantum layer holds. The system chooses the migration path today to still have proofs in twenty years, not to have a marketing advantage today.

Chapter 16: External Validation Record And The Two Axis Logic

That is the most important principle in the system.

The two axes. Every forensic artifact in the system has, formalized in the SCP 1.0 data model, two independent properties that are never mixed.

Axis 1, technical integrity. This axis is exclusively a cryptographic finding. Was the artifact in the producing pipeline completely and cryptographically sealed. Do all hashes, all Merkle links, all signatures match. This check is independent of the technical result of the artifact. An artifact that has a BLOCK result, the pipeline blocked a transaction because a sanctions list was hit, is just as intact as an artifact that has a CLEAR result. Integrity is a property of form, not of result.

Axis 2, court admissible. This axis is set exclusively by a sealed, externally issued External Validation Record. Such a record is a validation certificate issued by an independent law firm or a testing body. The system itself can never set this axis.

The core sentence that describes the system most deeply reads:

> ***The system cannot declare itself court proof.***

Why this separation exists. This separation rests on a hard lesson from compliance history. It is the temptation of every system to raise the self statements. We are cryptographically sealed, therefore that is court admissible. The error in this statement is that technical integrity and court admissible evidentiary

value are two different axes. Technical integrity proves, this artifact is not manipulated and reproducible. Courtproof evidentiary value proves, this artifact can be presented as evidence in a concrete court or supervisory procedure because its method, its source, its custody documentation was appraised and recognized by an independent body. No step in the first axis leads automatically to the second.

The system separates these axes hard because only thus the next property is secured. That a BLOCK artifact is just as intact as a CLEAR artifact. If technical integrity and court admissible were combined, a temptation would arise to configure the system toward an advantageous self statement, and this temptation creates risks. The system must be neutral between BLOCK and CLEAR.

Example. A CertifiedReceipt has technical integrity confirmed. All hashes, all Merkle links, all signatures intact. The technical input has a BLOCK result. A transaction was blocked because the entity was sanctions relevant. Axis 1 applies. Axis 2, court admissible, does not apply because there is not yet a sealed External Validation Record from an independent law firm. The receipt is forensically robust, it is intact, reproducible, its origin is traceable, but it is not yet court admissible because in court the method, the data collection, the chain of custody have not yet been appraised.

A law firm is engaged. It appraises the method, the data collection, and the chain. It issues an External Validation Record. Method X has been applied to the input data. This method is admissible in the forensic frame. The data collection is traceable. The record is sealed, deposited, inserted into the Merkle chain of records, and references the corresponding CertifiedReceipt. Now the receipt has axis 2 confirmed, referenced via the record. Technical integrity was never mixed. The two axes remained separate, and the second axis was set exclusively by an external, independent body.

How it connects. The External Validation Record is an artifact in itself. It is itself sealed, hash anchored, and Merkle chained. In the SCP 1.0 artifact the second axis references the record via its ID and its hash. Without such reference the axis is simply not set, no matter how intact the artifact otherwise is. Every setting of axis two documents from whom it comes and when. In this way the simple technical link intact is not the oral certificate of a legally valid proof. The two stand independently and are examined in cooperation.

Expansion. The External Validation Record has a validity period. A firm that appraises a method today appraises it for the version of today. In five years the method may have been developed further, and the appraisal must be renewed. The system documents the validity period in the record. A receipt that references a record today references a valid record. A receipt that references the same record in six years references an expired record. The system does not lie about the validity. It documents when the validity begins and when it ends.

Chapter 17: CRPG, The Cross Section Level

What CRPG is. CRPG, Cross Receipt Pattern Gate, is an additional observation layer that lies across the individual receipts. Where a classic check asks, is this single transaction above the threshold, CRPG asks, does a pattern lie across the last transactions of an entity that could be structuring.

Why CRPG exists, in light of scenario 6. Scenario 6 described an entity that carried out fourteen transactions below the threshold over nine months and that remained unremarkable in every single check because nobody looked across the transactions. The structural gap that CRPG closes is exactly the gap of pure single case checking. A single case check checks every transaction in isolation. A single transaction below the threshold is technically unremarkable, thus not reportable, thus not worth documenting. But the structure that makes a conscious structuring of a larger sum lies not in the single transaction but in the cross section. Anti structuring provisions exist because this cross section requirement is very real, and no classic single case tool is built to work it.

Legal anchoring. Section 261 StGB, money laundering, Money Laundering Act, FATF Recommendation 1, in the USA 31 USC Section 5324, structuring violation of the duty of currency transaction reporting. An important note. Some of these individual citations are introduced. Before an external publication they should be checked against the current version of the original text.

The architecture. CRPG is a non modifying extension of the existing receipt chain. That means. CRPG changes nothing on the existing receipts. It reads dependently over the already produced receipt history. CRPG replaces neither the single case check nor the human. It is an additional observation layer that produces a cryptographically sealed CRPGPatternReceipt that indicates that an observed pattern may lie present. CRPG is bound to the entity identity. Before every cross comparison the identity of the entity, preferably via the LEI, must be verifiable. Two transactions that describe a similar name but different entities would otherwise form a false pattern cloud. Therefore every comparison presumes a successful entity resolution. Exactly here the Gate 0 condition is decisive. Without Gate 0 there is no verified entity. Without verified entity CRPG has no foundation.

Single sector versus cross sector. Two patterns are distinguished. A single sector pattern that stands out within a sector collection, say several transactions in a bank, all just below the bank reporting threshold, and a cross sector pattern that only becomes recognizable in the cross section across several sectors, say transactions across bank, real estate, and wealth management, that are only sector specific in themselves but form a structuring pattern in sum. The cross sector signal is stronger. It is also rarer. It is also technically more demanding because it requires data from cards that traditionally do not talk to each other.

Example. An entity carries out 14 transactions over nine months, each individually below the bank reporting threshold. The bank compliance checks every transaction individually and sees, every transaction unremarkable. CRPG runs over the 14 transactions and finds, the transactions are all just below the threshold, temporally clustered, and the sum exceeds the threshold by a multiplier. CRPG produces a CRPGPatternReceipt that documents the observed pattern. The compliance officer evaluates the pattern and decides, not reportable or reportable. CRPG issues no reporting order but lays an observation.

A cross sector example. Five transactions at a bank, four at a wealth manager, three at a real estate broker. Only the cross section analysis across the three sectors yields a structuring pattern that would have remained sector specifically unremarkable at each individual point.

What CRPG does not do. CRPG issues no automated sanction. The CRPGPatternReceipt is an observation, not a reporting order. The decision whether the observed pattern triggers a reporting duty, whether a report follows, whether authorities are involved, remains with the compliance officer who will evaluate the pattern, supported by the receipt.

Expansion. CRPG is a first step into a world in which not the single transaction counts but the pattern. Supervisory practice is moving in this direction. AMLA, the European AML supervisor, begins to demand cross section analyses, no longer only single case reports. Whoever has CRPG today has an observation space that others must first build. And the observation space grows with every year because every year new receipts join the history. An institute that starts with CRPG today has three years of pattern history in three years. An institute that starts in three years has zero.

Part Five: The Sector Engines

Every sector gets its own section here that explains what the engine checks, an example, what is different with the competition, and the question of what the sector loses if it continues to do without it for longer.

Chapter 18: Banking And Financial Services

What the engine checks. Basel III capital requirements, MiFID II suitability, DORA operational resilience, AML duty under the Money Laundering Act, and the standard gate pipeline, GLEIF, sanctions, fundamental rights.

Example. A credit institution checks a loan grant to a group of companies. The compliance run produces CertifiedReceipts for LEI verification of the group and all subsidiaries, sanctions check of all participants, AML check of the transaction, Basel III consolidation impact on the institute's capital ratio. All results in an SCP 1.0 conformant chain. A year later, in a supervisory audit, the examiner can reproduce the receipts exactly against the rule catalog versions that were current then.

What the competition does differently. Banking compliance tools produce reports. They almost never produce cryptographically chained receipts with version and hash anchored rule basis. The supervisory audit is guild PDF. An auditor who wants to reproduce the rule situation then cannot, because the rule basis then was not hash anchored but applied as currently valid. The consequence on a recheck. He must rely on the compliance department having applied the right rule. He cannot reproduce it.

What is done differently here. It binds the rule basis, Basel III, MiFID II, Foreign Trade Act, Money Laundering Act, into version anchored rule catalogs whose hash stands in the receipt. Recalculability is not well meant but cryptographically enforced.

What the sector loses if it continues to do without it for longer. Institute A has this architecture and can explain to a supervisor, our compliance results are cryptographically reproducible. The rule situation we applied then is hash anchored in the receipt. Institute B, which does not yet introduce this architecture, continues to explain with PDF and compliance department note. In a supervisory audit with three years of review the supervisor can increasingly differentiate between an institute that is reproducible and an

institute that claims to have applied the same. The first who has this architecture gets a supervisory position that the others can hardly earn. Because the reproducible chain of an institute that already has three years of receipts is not comparable with a PDF archive. And this tension will increase in the next one to three years because supervisory practice itself begins to view cryptographic reproducibility no longer as a bonus but as a minimum requirement.

Chapter 19: Insurance

What the engine checks. Solvency II solvency capital requirements, IDD conduct duties, AML duty, fundamental rights touch, sanctions check.

Example. A life insurance with accumulated assets checks on payout in a death case the identity of the beneficiary, the sanctionability of the beneficiaries, the solvency capital impact of the payout, and whether the payout aligns with the IDD conduct duties in investing the remaining assets. All four checks as a receipt set. After ten years a forensic accountant can reproduce that the payout corresponded to the Solvency II requirements then.

What the competition does differently. Insurance compliance tools are kept locally per contract. The link between IDD conduct duty, Solvency II capital impact, and AML is not in a common chain but in three isolated tools that produce three different audits, and that after ten years stand in three isolated notes.

What the sector loses. Insurer A has the payout decision in a receipt chain. Insurer B has three notes that are not related to each other. In the insurance case on disagreement about the IDD duty, insurer A can prove that IDD, Solvency II, and AML were checked coupled on the same entity, at the same time, with the same input decision. Insurer B has three isolated notes. Who of the two stands better in an insurance supervision is a question of method, not of compliance effort. And insurance files are long lived. A life insurance concluded today can have a payout case in thirty years. Whoever begins today to build a receipt chain has in thirty years a reproducible payout decision. Whoever does not do that today has in thirty years an insurance and a note.

Chapter 20: M&A, Live Due Diligence

What the engine checks. Six check dimensions, seven check steps. The output artifact is called MaDDReceipt. The steps are. AML KYC on both sides. Beneficial ownership. FDI screening. Antitrust. Sanctions. Fundamental rights check. Jurisdiction conflicts.

Example. A private equity fund checks the purchase of an industrial group with subsidiaries in Germany, Italy, and a US stake. The engine produces a receipt for every check step. AML KYC for the fund as buyer and the group as seller, beneficial ownership for all economically entitled in every jurisdiction, FDI screening for every one of the three jurisdictions, Foreign Trade Act in Germany, Golden Power in Italy, CFIUS in the USA, antitrust check, sanctions check, fundamental rights check, and jurisdiction conflict check. At the end stands a MaDDReceipt that forensically holds the whole picture.

What the competition does differently. Traditional due diligence is tool bought. A beneficial ownership tool, an AML tool, an antitrust tool, an FDI tool. The individual results are PDFs. The synthesis is a manual

summary of the advisers. After three years, when a transaction legal dispute arises, PDFs and notes stand, no chained chain.

What the sector loses. Buyer A has the results in a forensic chain. Every receipt references the rule version and the date. In a dispute after three years about an allegedly overlooked sanctions touch of a subsidiary, buyer A can prove that on the then date was checked against the then current sanctions list, and that the subsidiary was not included. Buyer B, who claims sanctions list then as PDF, must rely on the statement of the advisers that the then correct list was checked, and this statement has no forensic chain. An M&A dispute with a three digit million amount in court does not depend on who claims but on who can prove. Whoever has reproducible due diligence has a material advantage here.

Chapter 21: Real Estate

What the engine checks. Beneficial ownership of the contracting parties, source of funds precheck, sanctions check, fundamental rights touch, especially the property right, foreign trade check on foreign acquisition, AML check according to the transaction volume.

Example. A foreign investor buys an office property in Frankfurt. The source of funds is documented by a source of funds workflow, the beneficial owner of the investor is identified, sanctions check is applied to the beneficial owner, the foreign trade check clarifies whether the transaction could fall under FDI screening. All receipts in a chain. The notary can reference the chain in the deed.

What the competition does differently. Real estate compliance is often a single list built into the notary workflow. The source of funds is an assurance of the buyer, the beneficial owner a sworn statement. Sanctions check is a match against a perhaps outdated PDF list. After years, in a realization or tax criminal dispute, there is note and assurance but no cryptographic chain.

What the sector loses. Real estate transactions are long lived like no other asset. The three year review is the ten year review in real estate. Whoever begins today to build a receipt chain has in ten years a sheer volume of reproducible transactions, and supervision and forensics in a world in which real estate is increasingly acquired cross border will need traceable sources. The first notary network that works with such an architecture has a different template form for notarial certification than the one who holds every transaction individually in PDF documents. And when the first supervisory decision falls that sets cryptographic reproducibility of a notarial certification as a minimum requirement, the network that begins today to build this chain will be the one that fulfills this decision.

Chapter 22: Cloud And Digital Infrastructure

What the engine checks. DORA operational resilience, C5 and SOC2 equivalence, ISO 27001 reference, ENISA reporting readiness, post quantum re attestation, Cloud Act conflict check.

Example. A cloud provider that offers compliance for European critical infrastructure runs the DORA reporting structure. An ICT incident report is documented with a receipt that references the classification of the incident, the affected criticality levels, and the applicable DORA articles.

What the competition does differently. Cloud compliance is certificate based. One certifies one's own system against a standard. The certification is a certificate renewed every year. The individual reports stand in the incident response system, not in a compliance chain.

What the sector loses. Whoever builds DORA with a receipt chain can show the auditor tomorrow, every incident is referenceable, every reporting event has a rule basis, every state transition is traceable. Whoever builds DORA with incident response tickets cannot, and the DORA auditor will very soon no longer ask only for certificates but for the reproducibility of individual reporting events. DORA compliance as certificate is the past form. DORA compliance as receipt chain is the future form.

Chapter 23: Energy

What the engine checks. Fundamental rights touch of energy law, Renewable Energy Directives, grid expansion acceleration acts, sector specific sanctions, especially sanction consequences on energy imports, ESG reporting for energy portfolios.

Example. An energy supplier checks the procurement of past energy imports for sanctions touch. The receipt documents which sanctions list, in which version, at which time was applied. Later, on a recheck of the procurement situation, it is not we checked that is the statement but the receipt chain that makes all procurement decisions referenceable back to the sanctions list state of the respective day.

What the sector loses. Energy is today the sector in which sanctions compliance is sharpest, and at the same time the sector in which the review situation, procurement in summer, review in winter, very quickly becomes a five to ten year question. The first energy supplier that documents its sanctions decisions over a cryptographically chained chain has a very different template when the supervisor wants to reproduce the procurement of the last three years than the one who stated current PDF list as the check basis.

Chapter 24: Sport, gateSport

What the engine checks. FIFA Laws of the Game, Law 12, fouls, Law 11, offside, Law 10, match outcome. The engine produces SportDecisionReceipts. Tolerance corridor and in dubio pro reo as conceptual levers. The exact threshold values are not published.

Example. A scene in the penalty area. Three camera perspectives. Gate 0 checks the divergence, the sports technical gate applies Law 12, classifies the indication, foul, no foul, disputed, documents the applied Law 12 version and all used input data. A SportDecisionReceipt arises. The referee can accept or reject the indication. The rejection is reasoned in the receipt. That is a calibrable data set.

What the competition does differently. VAR tools produce videos. They rarely produce cryptographically sealed receipts. The retrospective control over a VAR decision rests on video playback and referee statement, not on a reproducible receipt chain.

What the sector loses. Sports associations stand in a legitimacy question. A society that increasingly critically questions the transparency of refereeing will demand forensic reproducibility in the near future,

and an association that already has such an architecture has answered this question in an elegant way. Not with the claim that referees are flawless but with the proof that every decision that falls today is reproducible in ten years.

Chapter 25: Motorsport, gateMotorsport

What the engine checks. FIA International Sporting Code and analogous regulations of the series. Nine gates M0 to M8 for the motorsport specific incidents. Gate M9 for BoP reference deviation with slipstream exclusion, persistence check, wind correction, air density correction after SAE J1349, and per sector weather granularity.

The three layers of weather normalization in detail. A lap time is not directly comparable because wind, temperature, pressure, and humidity influence it. Whoever wants to report BoP deviations must first remove these influences. The system does this in three strictly separated layers that are never blended into a single correction factor.

First layer, discarding of laps that did not take place in dry conditions. Wet or damp laps are grip limited, not power limited. They do not lend themselves to BoP comparability and are discarded, not corrected. This distinction matters. Discarding means the lap does not count. Correcting would mean the lap counts with an estimate. The system discards.

Second layer, wind vector projection. Wind is not subtracted as a mere number but projected as a vector against the respective sector driving direction. A gust from the side in a sector driven straight on has a different effect than the same gust in a sector driven across the wind. The vector projection computes this effect correctly.

Third layer, air density correction after SAE J1349 and DIN 70020. It corrects the performance dependence on temperature, air pressure, and humidity. Colder intake air means more oxygen per volume and thus more power. This layer is physically independent of the wind correction and is executed strictly separately. The system does not mix estimates into a fudge factor. The reference condition is 99 kPa dry air at 25 degrees Celsius, per SAE J1349. The correction is computed on the basis of the actual temperature, pressure, and humidity, with a correct vapor pressure correction after the Magnus formula, and applied as a multiplicative factor to the lap time, after the wind correction, never before.

In addition the system allows two weather granularity modes. In lap mode a single weather point per lap is used, suitable for demonstration and short circuits. In sector mode a separate weather point is used for every sector, required for long circuits where wind conditions in one sector can be completely different from those in another. A circuit like the Nordschleife virtually forces sector granularity because from the Doettinger Hoehe to the Bergwerk lie meteorologically different worlds.

Every receipt documents exactly which correction layers were applied, with which method, and with which granularity. Thus the BoP finding is fully reproducible afterwards and not dependent on a silent assumption.

Example. In the course of an endurance race Gate M9 checks the sector performances of the vehicles. A vehicle deviates from the BoP reference multiple times in the performance sensitive sectors. Gate M9 checks whether the deviation begins in the slipstream of another vehicle, is excluded. Checks the persistence of the deviation over an observation window, is documented. Checks the weather data, wind correction applied, air density correction applied, per sector granularity applied. Gate M9 produces a receipt, BoP reference deviation observed, methodically traceable, that is routed to the technical steward. The consequence is a decision of the technical steward, not a verdict of the engine.

What the competition does differently. BoP systems in motorsport series are series internal and rarely documented. The methodology of deviation analysis is not publicly reproducible. After a championship decision the result stands but not the method that led to it.

What the sector loses. A series that works gateMotorsport based can, after a disputed championship decision, lay out a receipt chain that documents exactly which sector values, under which weather conditions, with which slipstream exclusion logic, which wind correction, which air density correction, and which persistence were checked. A series without this architecture cannot. The forensic value in disputed championship decisions is material. In a sport whose legitimacy will increasingly rest on a reproducible method, the first federation that has this will have a discursive advantage.

Chapter 26: What Is Done Differently Systemwide

A bundled summary that shows per mechanism what is different.

The most frequent difference is a cognitive one. Competitor tools document compliance. Here it is cryptographically proved. That is no optics difference. It is a material difference from which all other differences follow.

The competition works with probability. Here is checked deterministically. The competition works with isolated tools. Here is worked in a coupled chain. The competition works with audit logs. Here is worked append only. The competition works with PDF. Here is worked with sealed receipts. The competition claims court admissibleness. Here court admissibleness is set by an external body. The competition works with AI that decides. Here the rule decides, and the AI only reads.

Part Six: The Limits The System Sets Itself

Chapter 27: Governance Limits, Uniform Systemwide

A separate section that summarizes the same limits for every gate and every engine in this system, because they are so important that they must be named prominently.

First limit. No automated sanction, in no gate, in no sector. No engine, no gate, and no receipt type in this system can itself pronounce a sanction. A sanction, be it a sports penalty, a reporting duty, a blocking decision, a repeal request, is a human decision and is made by humans. The system produces forensic evidence that humans use in their decision. It replaces none of these decisions.

Example. A compliance officer runs a transaction stack in a bank. The system produces a CertifiedReceipt with BLOCK occasion, sanctions touch. The system cannot, and by architecture never, automatically block the release of the transaction. The system produces a receipt that documents BLOCK. The release decision remains with the compliance officer who sees the receipt. The system is an evidence giver, not a decider.

Second limit. No AI that decides. AI, where deployed in the system, and it is deployed in clearly limited roles, say in text extraction, in source consolidation, reads and classifies, does not decide. A rule decision falls back on a deterministic check that does not depend on training data, not on model updates, not on confidence values. That is a clarifying significance. A decision that comes from a deterministic rule can be reproduced by the opposing side. A decision that comes from a model cannot.

Example. Where AI supports the adverse media classification, the AI reads news sources and flags a report as potentially relevant. It does not decide adverse media confirmed. Such a statement can only be issued by the deterministic rule classification that is referenceable to clear source and date.

Third limit. Every uncertainty is documented visibly. An input that is not fully verifiable, a sensor value that diverges, a quorum that is not reached, the engine does not hide it in favor of a smooth result but documents it. That is more important for a later forensic dispute than a smooth result that becomes brittle afterwards.

Example. An input has a divergence in two sensor data. One says contact, the other no contact. The system does not decide in favor of contact or no contact. It documents divergence present, one source says A, one source says B. Later a human can work with this documentation. Deeper check, both views, reasoned decision. Another engine that decides prematurely would have concealed the divergence, decided for one side, produced a receipt with contact, and three years later the divergence would have vanished without trace. Invisibility burdens long term. Documentation relieves.

Fourth limit. Human decision makers keep full decision authority. Referees, stewards, compliance officers, law firms, supervisory bodies, all these parties have a documented, traceable, independent role in this system. A referee decision can reject an engine indication. A compliance officer can discard an observation pattern as not reportable. A law firm can abort a validation procedure. The system leaves every one of these decisions as a cryptographic artifact and undertakes none of these decisions.

These four limits apply uniformly. Whether a banking check, a football ruling, a motorsport BoP monitor, an M&A due diligence, a CRPG pattern, the system is bound to this limit in every functional axis. It is an evidence system, not a decision system.

Chapter 28: Repeal And Visibility

A repeal of a decision once produced is only possible in a procedure at least as strict as the original procedure. The system requires two independent reviewers, a mandatory legal ground, at least one piece of evidence, and documentation in a publicly accessible space.

There is no phone override. Whoever attempts a lift via an informal channel is automatically rejected, and the attempt is permanently recorded. This record is not coercion but a defense of the original decision. Whoever widens the chance of lift without widening the conditions of lift devalues the original decision.

The system consciously distinguishes which roles may file a request for lift. Admissible are the legal counsel of the player, the club official, the federation disciplinary, and the independent appeals body. Not admissible is a political actor. That is not a political statement but a separation of governance and politics. Whoever abandons this separation abandons the independence of the sports legal decision.

Expansion. Repeal is not the only procedure that demands increased visibility. The original decision is also visible. A suspension that is pronounced is public. A sanction that is documented is referenceable. The system has no secret decisions, with the sole exception of the secrecy that is data protectionally required, say the secrecy of personal data that does not belong public. But the decision itself, its reasoning, its rule basis, its point in time are public. Whoever makes secrets out of the procedure devalues the procedure.

Naming collision discipline. A recurring limit of its own, one that only became visible when Switzerland was added as a new jurisdiction, but is structural in nature. Different legal systems and institutions use identical abbreviations for entirely different legal sources. The German and the Swiss anti money laundering acts both carry the abbreviation GwG, yet are two different laws under two different supervisors. The abbreviation AMLA initially, and incorrectly, labelled the substantive EU rulebook in the rule catalogue, when AMLA correctly refers exclusively to the new European supervisory authority; the substantive rulebook itself is called AMLR. Both mix ups were only uncovered through later review, not by the original implementation itself. This yields a binding principle for every future extension of the rule catalogue: every new abbreviation is checked explicitly against the abbreviations already present in the catalogue before it is adopted, not only once a mix up is actually noticed. This is not a one off correction of two isolated cases. It is a structural review duty that applies again with every new jurisdiction.

Part Seven: Legal Sources Register, Complete And Named

Chapter 29: Banking And Financial Services

Capital Requirements Regulation, Capital Requirements Directive, Basel III framework, MiFID II, MiFIR, DORA, Money Laundering Act, Foreign Trade and Payments Act, Foreign Trade and Payments Regulation, KWG, ZAG, EMIR.

Chapter 30: Insurance

Solvency II framework directive, IDD directive, VVG, Insurance Supervision Act, VAG.

Chapter 31: Digital Assets

MiCA regulation, DLT Pilot Regulation, eWpG.

Chapter 32: Public Sector, Procurement, FDI

EU Procurement Directive 2014/24/EU, EU Procurement Directive 2014/25/EU, Foreign Trade and Payments Act, Foreign Trade and Payments Regulation, GWB procurement regime.

Chapter 33: Fundamental Rights And Constitutional Law

Basic Law, especially fundamental rights articles 1 to 19, EU Charter of Fundamental Rights, ECHR.

Chapter 34: Sanctions And AML International

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

Chapter 35: Sport

FIFA Laws of the Game, UEFA Regulations, DFB statutes, FIA International Sporting Code, DMSB regulations.

Chapter 36: Switzerland, nGwV-FINMA 2027

Switzerland was added as a new jurisdiction in July 2026, triggered by the consultation on the partial revision of the FINMA Anti Money Laundering Ordinance opened on 12 May 2026, entering into force on 1 January 2027. A dedicated gate covers six verified provisions, each individually checked against the primary source, FINMA's explanatory report of 12 May 2026.

Art. 9b nGwV-FINMA, traceability of ownership and control structure. Art. 10 para. 3 GwV-FINMA, repeal of the Liechtenstein exception, the large data set now always applies instead of the small one. Art. 30 nGwV-FINMA, organisational measures to prevent violations of the Embargo Act, SR 946.231. Art. 37 para. 3 nGwV-FINMA, deletion of the phrase as circumstances require for correspondent banking relationships. Art. 37 para. 5 nGwV-FINMA, new pass through account obligation for correspondent banking relationships. Art. 65 para. 2 letter d nGwV-FINMA, obligation to obtain a beneficial ownership declaration also for sub accounts.

The gate additionally references the Swiss anti money laundering act under the unambiguous label GwG (CH), to rule out confusion with the German anti money laundering act, and the European anti money laundering supervisory authority under the label AMLA, Regulation 2024/1620, kept strictly separate from the substantive EU rulebook AMLR, Regulation 2024/1624. Both separations are the result of mix ups uncovered only after the fact; see the naming collision discipline in Part Six.

Chapter 37: Reservation Of The Register

This register is complete in the sources the system actually uses. It is not complete in the legal situation as such. Individual article paragraph citations that are firmly stored in the engine logic or rendered here in substance carry expressly the label to be checked before external use when the current regulation text in the rule basis has not yet been finally consolidated. That is no weakness but the practice form of an honest system documentation.

Example Basel III. A gate checks the CRR requirement on the Core capital ratio. The receipt references the version of the CRR that was applied, say version hash X. Later, when the CRR is amended, a new receipt references the hash of the new version. Old receipts keep the hash reference to their then applied version. The rule basis version is not overwritten but stacked.

Example Foreign Trade and Payments Regulation. FDI screening record. The applied version is documented as a hash in the receipt. When the regulation sharpens the proof duties in a new version, future receipts reference the new version. Old ones remain referenceable to the old version.

Example FIFA Laws of the Game. A SportDecisionReceipt references the FIFA version 2024/25. A receipt produced after the next rule revision references the FIFA version 2025/26. The old receipt chain remains reproducible to the applied version.

Chapter 38: Examples Of The Primitives

Example canonicality. Two documents. One with field name before id, the other with id before name. Semantically equal, lexically different. Without canonicality both would have a different hash over them. RFC 8785 can assign these documents a canonical form so that both yield the same hash. That is the condition for a hash to be reproducible again in another system.

Example ECDSA verification in the browser. A receiver who receives a portable artifact can perform the verification locally in the browser. Imports the embedded JWK key, takes the signature string, decodes it, and calls the verification. The result true or false. No server call, no prior relationship to the system. The verification is completely local.

Example Merkle chain. Receipt N has the payload hash H N. Receipt N plus 1 has the payload hash H N plus 1. The Merkle link of receipt N plus 1 is the combination of both hashes. A retrospective change to receipt N would change H N, thus break the Merkle link of receipt N plus 1, and the break propagates in every following receipt. The chain is append only. Manipulation is visible.

Example verification block status. If the private server key is momentarily not available, rotation under way, the status of the portable proof is not available. The artifact remains correct in its internal integrity, and the verifier knows that the asymmetric signature follows only after rotation. The system never loses internal integrity when the asymmetric layer temporarily drops.

Part Eight: Roadmap, What Is Built And What Comes Next

This section sugarcoats nothing. Every item below states plainly what stands today and what the next concrete step is.

Gate M9, all three weather normalization layers implemented and active. The wind correction, vector projection, is implemented and active. The air density correction after SAE J1349 is implemented and active, physically independent from the wind correction and never mixed with it. The reference condition is 99 kPa dry air at 25 degrees Celsius, per SAE J1349 and DIN 70020. The system does not measure air

density itself, it receives measured ambient conditions, temperature, pressure, relative humidity, from track telemetry and computes the correction factor from them.

Gate M9, weather points per sector. Weather data is drawn per performance sensitive sector, not only per lap. For circuits with strong microclimate, say a long circuit with different altitudes such as the Nordschleife, this is the production grade form. The receipt documents which sector weather points the assessment was based on.

External Validation Record, next step: engaging a named law firm. The architecturally complete, cryptographically complete structure for External Validation Records is built and operational. What remains as the next concrete step is naming and engaging an external law firm or testing body to issue such records in live operation. Until that engagement is made, the axis court admissible truthfully stands at not set for every real case on this axis. Any other statement would be a self deception of the system, and the system is built specifically so that it cannot make that statement on its own.

CRPG, calibration values are start values, alignment with supervisory bodies is the next step. The concrete numerical values for CRPG, window size, near band definition, minimum number of events for pattern triggering, sum multiplier, are technical start values chosen with high care. The next step is aligning them with the relevant departments and supervisory bodies. CRPG receipts that rest on these start values are methodically correctly produced today, the values themselves are preliminary until that official calibration follows.

Portable proof keys, rotation and production process, proven under real conditions. The process of key production and rotation for the asymmetric signature layer went through a real world stress test, not a staged one. An earlier version of the production ceremony had enclosed the private key in a response return, which violated the protected moment of production in the strict sense. That is not a scenario that was planned in advance to test the system. It happened during active development, was caught, and was corrected before the key was ever used in production. The compromised key was permanently revoked, the revocation itself sealed and dated, and the ceremony was rebuilt so the private key is now held exclusively server side, in an admin limited entity, and never output in responses, logs, or configuration documents. What this demonstrates is not that a mistake cannot happen. It is that when it does, the architecture’s own review discipline finds it, names it, and closes it, on a real incident, not a rehearsed one. The final step, handover to a hardware supported key production, is under way, and full completion is reached once that hardware step is in place.

Protection goods list, deliberately not named in this document. A complete naming in the documentation with the concrete values stored in the recognition logic is not suitable for security reasons and is withheld by design, not by omission. These values are not published. This expressly concerns slipstream distances at Gate M9, persistence window sizes, CRPG near band percentages, and sum multipliers.

Bounding parameters, held back by design. All numerical threshold values, persistence window sizes, near band definitions, sum multipliers, slipstream distances, and persistence requirements are not publicly documented, for the same security reason.

Gate 0, divergence automatically resolved. No. Gate 0 documents divergences and does not resolve them in favor of a source. Subordinate technical gates can interpret the marking.

ML DSA 65 integration, next step: a certified library. Documented migration path, ready to activate. The date depends on the availability of a certified library and is not promised ahead of that availability.

Chapter 39: Technical Fundamentals

Data structures. Receipt schema, simplified, in the SCP 1.0 data model. Every receipt has an identifier, deterministically produced, say RPE for a Certified Receipt, RDR for a Reliance Decision Record, CRPG for a CRPG Pattern Receipt, prefixed by receipt type. An input hash, SHA 256 over the canonicalized input. A rule reference, rule ID and hash of the applied rule version. A verdict, technical result, PASS, BLOCK, WARN, RACING INCIDENT, OFFSIDE, depending on sector. Timestamps, valid time, when the legal situation applies, transaction time, when recorded, NTP anchored. A chain link, the Merkle link, that is the chaining with the predecessor. A verification block.

Verification block. The verification block in an SCP 1.0 artifact is built so that it strictly separates the two verification classes. The internal integrity signature, HMAC SHA 256, verifiable by parties that hold the shared internal key. The portable proof signature, ECDSA P256, with the signature value, the signed payload, the key ID, the embedded public key as JWK, the reference to the publicly published key, and the status AVAILABLE or NOT AVAILABLE. The embedded public key JWK ensures the artifact is self supporting. The public key reference allows crosscheck against the published public key. If the active private key is missing server side, portable proof signature status is NOT AVAILABLE, but the internal integrity is never downgraded.

Cryptographic primitives. SHA 256, hash standard function, used over canonicalization, Merkle chaining, input hash, rule hash. HMAC SHA 256, Message Authentication Code over SHA 256, class 1 verification. ECDSA P256, Elliptic Curve signature on NIST P 256, class 2 verification today. Private keys are stored exclusively server side in an admin limited entity and never output in responses, logs, or configuration documents. ML DSA 65, FIPS 204, post quantum signature standard, documented migration path to a hybrid signature alongside ECDSA P256, as soon as a certified library is integrated. RFC 8785, JSON Canonicalization Scheme, standardized canonical form of JSON, so that hashes over JSON are reproducible. Merkle chaining, every receipt references its predecessor, append only, manipulation visible. NTP time anchor, timestamps of the receipt are bound to NTP anchored time references, the time at which an event was registered is not settable by the system alone.

API basic principles. API first. All results are available as API responses. The Serverless Edition is an API based composition of gate calls. Authentication at every gate. Every function call authenticates via token of the calling customer. Public endpoints, say the public key, the public receipt, are available without authentication in their limited purpose. No secrets in responses, no environment variable names in this documentation. Security relevant configuration parameters are not published. The names of internal environment variables and the actual secret values are not rendered in this document. Receipts are append only. Receipts cannot be changed afterwards in the system. Their state transitions, say sealed, verified, disputed, are documented results of the processes, and the transitions do not suffice even in

the worst state to break the hash chain. Service role versus user role. The maintenance routine, retrieval of a private key, sanctions list synchronization, happens in the service role. Technical gate calls happen in the user role of the calling customer.

Chapter 40: Time And Its Three Levels

The system distinguishes three time levels that are never mixed.

Transaction time. That is the point in time at which an event was recorded in the system. It is NTP anchored and not manipulable by the system alone.

Valid time. That is the point in time from which a legal situation applies. A rule that applies on 1 January has a valid time of 1 January, even if it was already published in December before.

Pre run time. That is the point in time at which the input was fixed in Gate 0. It is the beginning of the chain and independent of the transaction time of the later technical gates.

Separating these three time levels is important because a forensic dispute often must take these three times apart exactly. When was the input fixed. When was the rule applied. When did the legal situation apply. Whoever mixes these three questions loses reproducibility. Whoever separates them keeps it.

Chapter 41: The Trajectory Of Supervisory Practice

Supervisory practice in Europe and the world is moving in a direction that views cryptographic reproducibility of compliance decisions no longer as a bonus but as a minimum requirement. DORA has set standards for the financial sector that go beyond pure certificate logic and demand traceability of individual reporting events. The EU AI Act regulation begins to no longer accept AI decisions as a black box but to demand traceability of the decision basis. AMLA as the European AML supervisor is in the process of setting a standard that goes beyond pure single case reporting and demands cross section analyses.

This trajectory is no prediction. It is already under way. And it inevitably runs out on one question. When the supervisor makes cryptographic reproducibility the minimum requirement, who then has it, and who does not.

In three years the difference between an institute that has built a receipt chain for three years and an institute that has kept PDF archives for three years will no longer be a difference of compliance effort. It will be a difference of compliance method. And the method is not made up in three months. The chain must begin today to be a three year old chain in three years.

Chapter 42: The Trajectory Of Forensic Practice

Forensic practice, that is, the practice of appraising compliance decisions by law firms, auditors, and experts, is moving in parallel. A forensic appraisal that leafed through a PDF archive ten years ago will expect cryptographic reproducibility in three years. The opposing side's question, where is the hash reference to the then current sanctions list, is a polite question today. In three years it will be a standard

question. And an institute that has an answer to this question stands differently from an institute that has no answer to this question.

In a court dispute with a three digit million amount it does not depend on who claims but on who can prove. A reproducible chain is a proof. A PDF note is a claim. And the transition from a world in which claims suffice to a world in which proofs are demanded is no creeping transition. It is a break. And the institutes that begin today to build a chain will be those who stand on the side of proofs when this break comes.

Chapter 43: What The One Loses Who Continues To Do Without It For Longer

If a sector continues to do without building a cryptographically chained compliance chain for longer, it loses not compliance effort. It loses compliance method. And the loss is not noticeable in the present but in the review. In the supervisory audit in three years, in the court dispute in five years, in the forensic investigation in ten years.

The institutes that begin today build a chain that is three years old in three years. The institutes that begin in three years build a chain that is zero years old in three years. The difference is not made up because the chain cannot be built retroactively. Old receipts cannot be produced afterwards because their timestamps are NTP anchored and their rule versions cannot be set afterwards. A receipt that was produced in 2026 is a receipt from 2026. It cannot be produced retrospectively in 2029.

That is the material reason why the choice of the start is not arbitrary. Every year that passes without the chain being built is a year missing in the chain. And the missing year is no longer retrievable in the review.

Chapter 44: The Pricing Logic, In Words, Without Tables

The system sells no check. It sells the binding self commitment of the responsible party. The value is not the individual check in itself but the receiving boundary of that check by a responsible receiver. The receiver is the unit in which the check arrives in a decision capable form, is evaluated, and is led to a decision. The system therefore does not distinguish between a pricing model and a responsibility model but sees one unity of the value stream. A check without a receiver is worthless. A receiver without a check is blind.

The system consciously rejects a pricing model that bills per individual finding. A check is not a coffee coupon sold by the piece. Whoever bills per finding creates an incentive to avoid higher usage and thus to avoid more frequent checks. The system instead chooses an institutional licensing model in which an organization receives an annual or tournament based license and performs checks within that license.

A chief financial officer is often confronted with the question why an infrastructure is so expensive when the individual check is completed within seconds at most. The system's answer is not that each check costs much but that the question is wrong. It is not about the price per check but about the price per accountable receiving boundary in which checks demonstrably arrive. An appropriate infrastructure price is not the price of the check but the price of the proof.

Chapter 45: Intermediation And The Partner Tier

The system knows intermediaries. These are organizations that use the system in their own name and under their own responsibility. These intermediaries receive their own access, their own key, their own billing space. They bear the responsibility that their end customers use the receipts in a responsible form.

The intermediary ledger records every check performed, with its price, its point in time, and its type. At the end of a billing period an invoice is produced from it. This invoice conforms to the locally applicable invoice requirements, in Europe to the common e invoice standard for public procurers and large enterprises.

The system supports different invoice channels, depending on the receiver's need. The channels range from standard PDF by email via XML API delivery to the receiver system to straight-through processing in the public procurement network. The system does not decide the channel, it provides it.

Chapter 46: Reliability Through Append Only

The system deletes nothing. Every change is a new element in the chain. That is no purism but the precondition for the reliability of the proof. Whoever can change can cover up. Whoever can only append cannot cover up but only correct, and every correction becomes visible.

Chapter 47: The Alarms For Human Gaps

The system has forensic alarms for gaps in the chain. A missing seal, a missed deadline, an incomplete appraisal. All of these produce an alarm before they become a gap in the chain of evidence. These alarms are no cosmetic hints but early warning signs for threats to the proof.

Chapter 48: The Freedom Of Interpretation

The system supports many sectors but it does not interpret. It applies the rule that was valid at the moment of the check. It invents no rules. It reads the existing rule, fixes its version, and applies it. That is the condition under which the system remains forensically viable.

Chapter 49: Proof Without Advice

The system gives no legal advice. It delivers proofs. This distinction is not only legal but ethical. Whoever gives advice takes responsibility for the decision. Whoever delivers proofs takes responsibility for the traceability of the decision. That is a different concept of responsibility, and it is the right one for a system of this kind.

Chapter 50: Decidability

The system is decision firm. It is not guided by feeling, not by promises, not by financial incentives. It is guided only by the rule and by the input. That is no coldness but the condition for trust. A system that lets itself be guided by feelings is not trustworthy because it becomes unpredictable. A system that lets itself be guided only by rule and input is predictable and thus reliable.

Chapter 51: The Duty Of Transparency

The system is transparent. It documents its rules, its limits, its gaps, its requests. It claims no care that it does not have. It claims no reliability that it cannot deliver. This transparency is no pedagogical motivation but a duty of proof. Whoever delivers proof must also state the trust boundaries of that proof.

Chapter 52: The Ethical Position

The system gives no legal advice. It delivers proofs. This distinction is not only legal but ethical. Whoever gives advice takes responsibility for the decision. Whoever delivers proofs takes responsibility for the traceability of the decision. That is a different concept of responsibility, and it is the right one for a system of this kind.

The system is decision firm. It is not guided by feeling, not by promises, not by financial incentives. It is guided only by the rule and by the input. That is no coldness but the condition for trust.

The system is transparent. It documents its rules, its limits, its gaps, its requests. It claims no care that it does not have. It claims no reliability that it cannot deliver. This transparency is no pedagogical motivation but a duty of proof.

Chapter 53: R07, Open Article Reference AMLR Technology

When EU Regulation 2024/1624, AMLR, was added to the rule catalogue, one citation was deliberately left open. An internal reference document had cited Art. 10 as evidence for a supposed technology provision. Checking this against the regulation's actual chapter structure showed that Art. 10 addresses the business wide risk assessment, not technology. No single, clearly matching technology article could be found, at most scattered side aspects in Art. 28 para. 3 on technological developments when revising technical standards, and a general recital. The reference is therefore deliberately left unfilled until a provision that actually matches has been found and verified in the regulation's text itself. This is the same discipline as the External Validation Record axis, which stays truthfully at not set until a law firm is actually engaged: a visible gap rather than an uncertain citation.

Part Nine: The Limits

Chapter 54: What This System Cannot Do

The system cannot take responsibility for the human decision. It can document that the decision was reasoned, but it cannot make the decision.

The system cannot produce external appraisals. It can record them but not produce them.

The system cannot guarantee keys forever. It can rotate and revoke keys, but it cannot prevent a key from being compromised one day. It can only ensure that the compromise becomes recognizable.

The system cannot close gaps in the legal framework. It can only document that at the moment of the check the framework that was current then was followed.

The system cannot create truth. It can only create reproducibility. Truth is a human finding. Recalculability is a mathematical finding. The system does the second, not the first.

Chapter 55: What This System Wants

The system wants to deliver proofs that can still be checked years later without anybody remembering the event.

The system wants to make responsibility attributable, not to shift it.

The system wants to close the gaps in today's compliance, not through more documents but through better proofs.

The system does not want to be the first but the most reliable.

The system wants a decision that falls today to still stand in ten years, not because it is unchallenged but because it is reproducible.

The system wants the question, on which sanctions list, in which version, at which time was checked, never again to have to be answered with silence.

The system wants the transition from a world of claims to a world of proofs to be no break that hits some and spares others, but a path that can be walked by whoever begins today.

Part Ten: The Actors And Their Roles

Chapter 56: The Human As Deciding Actor

The system has a clear conception of the human. The human is not the disrupting factor that diminishes determinism. The human is the deciding actor the system serves. Everything the system delivers serves the human who must make a decision and who is responsible for that decision. The system does not take the decision from him. It takes the burden of proof from him. That is a different mandate.

Whoever understands the system understands that the determinism of the machine and the freedom of the human are no contradiction. The determinism ensures that the human knows what he decides on. The freedom ensures that he decides, not the machine. The determinism is the ground of freedom, not its opponent. Whoever abandons the determinism to give the human more freedom in truth gives him more arbitrariness and takes the ground on which he can decide responsibly.

Chapter 57: The Compliance Officer

The compliance officer is the first addressee of the system. He receives the receipts, evaluates the findings, decides on the release or blocking of a transaction. The system delivers him a picture that he reads in his context. It delivers him no finished answer that he only nods through.

His role is documented. Every decision he makes is inserted into the chain. He can reject an engine indication, discard an observation as not reportable, order a deeper check. Every one of these decisions is forensically traceable. The system does not devalue his decision authority, it strengthens it. The

compliance officer who decides today on mere notes must defend himself when his decision is challenged. The compliance officer who decides on a receipt chain has the defense already built in.

Chapter 58: The Referee And The Technical Steward

In sport the system has two addressees. The referee who leads the match and the technical steward who evaluates the sport legal processes. Both receive receipts that make the picture methodically traceable. Both decide themselves.

The referee can accept or reject an indication of the sport gate. The rejection is reasoned in the receipt. That is no weakness of the system but its strength. The rejection is data material that improves the calibration of the system. If a referee regularly rejects, the system shows that the rule indication and the referee practice diverge. That is no error but a calibrable finding that informs further rule development.

The technical steward in motorsport gets a picture that documents the weather conditions, the slipstream phase, the persistence, and the correction layers. He decides whether a BoP deviation lies that requires action. The system delivers him the methodical ground, not the verdict.

Chapter 59: The Law Firm

The law firm is the external actor who sets axis 2, court admissibleness. It appraises the method, the data collection, and the chain of custody. It issues the External Validation Record. The system cannot take over this task itself because it must not set axis 2 itself.

The law firm is actor of the system but not integrated into the system. The system has a surface for law firm work, but the law firm remains independent. It is engaged, paid, and it follows its own professional judgment. The system delivers it the methodical documentation on which it builds its appraisal. The appraisal itself is its work, not the work of the system.

Chapter 60: The Intermediary

The intermediary is an actor between the system and the end customer. He uses the system in his own name, under his own responsibility, for his market participants. The system knows intermediaries, gives them their own access and their own billing space, and makes their responsibility visible.

The intermediary is no commercial middleman in the classic sense. He is a responsible party who produces the receipts in his own name and who is liable for his end customers using these receipts in a responsible form. The system makes this responsibility forensically traceable. The intermediary cannot hide behind the end customer. He produced the receipt, he stands for it.

Chapter 61: The Auditor

The auditor is the reviewer. He comes when the chain already stands. He wants to know whether what is documented is also reproducible. The system is built for him. He needs no trust, he recalculates. He gets the receipts, the hashes, the rule versions, the time anchors. He checks integrity, chaining, signatures. The system is his tool, not his opponent.

His finding is documented, inserted into the chain, sealed. An auditor who checked and confirmed the chain has himself become part of the chain. Whoever later asks, was this chain audited, finds the answer in the receipt, not in a guess.

Chapter 62: The Supervision

The supervision is the actor who carries out the review of the sector. It asks about the compliance method, not about the compliance effort. It wants to know whether the chain is loadable, whether the rule versions are hash anchored, whether entity verification took place, whether gaplessness holds.

The system delivers the supervision a picture that meets its requirements. The supervision can reproduce receipts, compare rule basis versions, check chain integrity. It can determine that one institute has a three year old chain that is reproducible and that another institute has a three year old PDF archive that is not reproducible. It will increasingly differentiate between the two.

Part Eleven: The Life Cycles Of An Artifact

Chapter 63: From Inlet To Receipt

An artifact does not arise in one act but in a series of acts. The first act is the inlet. The input is received, canonicalized, the hash is formed. The second act is the Gate 0 check that establishes forensic admissibility. The third act is the technical gates that apply the rule and produce a result. The fourth act is the sealing, the signature, the chaining. The fifth act is the storage that keeps the artifact ready for further checking.

Every act is documented. Every act has a point in time. Every act is part of the chain. Whoever checks the artifact later sees not only the final result but the whole life cycle from which it arose. That is the difference between a document and a proof. The document shows the result. The proof shows the origin.

Chapter 64: From Receipt To Portable Artifact

A receipt produced in the system is internally intact. It carries the HMAC signature and is chained in the Merkle chain. It is sufficient for internal checking.

When the receiver wants to export the artifact from the system to hand it to a third party, the second class of signature is added. The portable proof signature, ECDSA P256, is added. The public key is embedded. The artifact becomes self supporting.

The receiver who receives the portable artifact does not need the producing system. He can retrieve the public key, verify the signature, reproduce the hashes, check the Merkle chaining, confirm integrity. The portable artifact is a piece of evidence in itself. The system is no longer needed to deliver the proof. That is the precondition for the proof to still be deliverable years later when the producing system may already be archived.

Chapter 65: From Portable Artifact To External Validation Record

The portable artifact is technically intact. Axis 1 is confirmed. Axis 2, court admissibleness, is not yet set. The External Validation Record is added when a law firm has carried out the appraisal. It is another artifact that references the first.

The life cycle is thereby not closed. The External Validation Record has a validity period. It can be renewed when the method has been further developed in the meantime. The system documents the validity period and the renewal. Whoever checks later sees which appraisal applied and when it expired.

Chapter 66: From Receipt To Decision

The receipt is the ground, not the decision. A human makes the decision. The receipt delivers him the picture that he evaluates. The decision is documented, with reasoning, and inserted into the chain. Thus the decision is no longer a claim but a cryptographically anchored act that rests on a receipt that in turn rests on a rule and an input.

Whoever later asks what this decision rested on finds the answer in the chain. He finds the receipt ID, the rule version, the input, the timestamps, the reasoning. He can reproduce the decision even when the human who made it is no longer reachable.

Chapter 67: From Receipt To Repeal

A decision once made can be repealed. The repeal is its own forensic process at least as strict as the original decision. The system requires a formal request, a legal ground, evidence, and the appraisal by two independent reviewers. An informal repeal is automatically rejected, the attempt is documented.

The repeal is a receipt that references the original receipt. The original receipt remains standing, it is not deleted, it is not changed. The repeal is a new entry that continues the chain. Whoever later asks, was this decision repealed, finds the answer in the chain, together with the reasoning, the procedure, and the reviewers.

Part Twelve: The Layers Of Responsibility

Chapter 68: Responsibility For The Input

The input is the ground of every check. Whoever delivers the input bears the responsibility for its completeness and correctness. The system cannot correct the input, cannot supplement it, cannot compensate it. It can only document what the input was and whether it meets forensic admissibility.

That is important because it does not shift responsibility. An institute that delivers an incomplete input gets no smooth result. It gets a stopping Gate 0 that documents the incompleteness. The institute is responsible for completing the input, not the system.

Chapter 69: Responsibility For The Rule

The rule basis is the ground of every application. Whoever maintains the rule basis bears the responsibility for its correctness. The system applies the rule that is stored in the versioned basis. It does not interpret the rule, does not invent it, does not correct it.

It follows that the system is not liable for the correctness of the rule. It is liable for the reproducibility of the application. The law firm that appraises the method is liable for the recognition of the method. The system separates these responsibilities cleanly because only thus every liability remains clear.

Chapter 70: Responsibility For The Decision

The human makes the decision. The system delivers the cryptographic ground, but the decision is human. That is no excuse of the system but a condition of forensic clarity. Whoever shifts the decision to the machine gives up responsibility, but he cannot truly give it up because the machine is not liable. Whoever keeps the decision with the human keeps responsibility recognizable and can defend it.

The system documents that the decision was made by a human. It documents who decided, when, with which reasoning, to which receipt referred. Responsibility remains with the human, and the system makes it forensically traceable.

Chapter 71: Responsibility For The Repeal

The repeal is a decision that replaces an earlier decision. Here too the human bears responsibility. The system requires the procedure, documents the reasoning, the reviewers, the evidence. Responsibility lies with the reviewers, and the system makes their work traceable.

Whoever requests the repeal also bears responsibility. The system documents who requested, in which role, with which reasoning. A request that is not admissible, say from a political actor, is automatically rejected. The system makes the inadmissibility visible, it does not hide it.

Part Thirteen: The Layers Of Cryptography

Chapter 72: The Hash Function

The hash function is the ground of cryptographic integrity. It takes data of arbitrary size and produces a fixed fingerprint that uniquely identifies the data. A small change in the data produces a completely different fingerprint. The system uses SHA 256, an established hash function established in numerous cryptographic standards.

The hash function is not reversible. One cannot recover the data from the fingerprint. That is important because it separates the integrity check from confidentiality. Whoever has the fingerprint can check integrity without knowing the data. Whoever has the data can reproduce the fingerprint to confirm agreement.

Chapter 73: The Message Authentication Code

The Message Authentication Code, HMAC, is the symmetric signature that secures internal chain integrity. It uses the hash function and a shared key. Whoever has the key can reproduce the signature. Whoever can reproduce the signature can confirm that the receipt comes unchanged from the producing system.

HMAC is class 1 of verification. It suffices for internal checking, but it does not suffice for external checking because the verifier would need the shared key, which contradicts the property of an asymmetric signature.

Chapter 74: The Asymmetric Signature

The asymmetric signature, ECDSA P256, is class 2 of verification. It uses a key pair. The private key signs, the public key verifies. The private key stays in the system, the public key is published.

The asymmetric signature solves the problem of external checking. A verifier who has the public key can verify the signature without ever having had the private key. That is the ground of portable provability.

Chapter 75: The Merkle Chaining

The Merkle chaining is the chaining of receipts into an append only chain. Every receipt references its predecessor. The Merkle link is the combination of the own hash and the predecessor's hash. A retrospective change to a receipt would change its hash, break the Merkle link of the following receipt, and the break propagates in every following receipt.

The Merkle chaining is the tool that secures gaplessness. It is itself an established cryptographic technique established in blockchains and other append only systems. The system applies it consistently.

Chapter 76: The NTP Time Anchor

The NTP time anchor is the external time reference that holds the point in time of an event. The system draws time from an independent, public time source. The timestamp is thus not settable by the system alone. An attacker who controls the system cannot manipulate the data without forging the time, and the time is not in the system but in the world.

The NTP time anchor is the ground of the forensic loadability of a point in time. A verifier who asks when this event took place finds the answer in the receipt, and the answer is not producible by the system alone but secured by the external time reference.

Chapter 77: The Canonical Form

The canonical form, RFC 8785, is the standardized representation of JSON data that allows hashes over JSON to be formed reproducibly. Without canonical form a hash would depend on the order of fields, on whitespace, on the serialization form. With canonical form these contingencies are eliminated.

The canonical form is the ground of interoperability of hash formation. A verifier who wants to reproduce the same hash in another system needs a canonical form that is the same. The system uses RFC 8785 because it is the established standard for the canonical representation of JSON.

Part Fourteen: The Layers Of Time

Chapter 78: The Transaction Time

The transaction time is the point in time at which an event was recorded in the system. It is NTP anchored and documents when the receipt arose. The transaction time is the point of sealing.

Chapter 79: The Valid Time

The valid time is the point in time from which a legal situation applies. A rule that applies on 1 January has a valid time of 1 January, even if it was already published in December before. The valid time documents when the rule became applicable, not when it was documented.

Chapter 80: The Pre Run Time

The pre run time is the point in time at which the input was fixed in Gate 0. It is the beginning of the chain that leads to a receipt. The pre run time is separated from the transaction time of the later technical gate. This separation is important because the forensic dispute often must take these times apart exactly. When was the input fixed. When was the rule applied. When did the legal situation apply.

Chapter 81: The Lifetime Of A Receipt

A receipt has no fixed lifetime. It lives as long as the chain lives. Since the chain is append only, it lives indefinitely. A receipt produced in 2026 is still reproducible in 2056 if the chain has been maintained and the cryptographic procedures still hold.

The lifetime is limited by cryptographic decay. ECDSA P256 is considered secure today, but in twenty years a quantum computer could break it. Therefore the system has the documented migration path to the hybrid signature of ECDSA P256 plus ML DSA 65. Whoever produces a receipt today has in twenty years a receipt that was signed under the cryptographic procedures valid then. Migration to hybrid signatures is additive, not replacing. The old signatures remain valid, the new signatures are added.

Chapter 82: The Lifetime Of An External Validation Record

An External Validation Record has a documented validity period. It is not indefinite. A law firm that appraises a method today appraises it for the version of today. In five years the method may have been further developed, and the appraisal must be renewed.

The system documents the validity period in the record. A receipt that references a record today references a valid record. A receipt that references the same record in six years references an expired record. The system documents when validity begins and when it ends. It does not lie about the validity.

Chapter 83: The Lifetime Of A Rule Version

A rule version has no deletion. It is stacked, not overwritten. A rule that applies in 2024 remains stored in its 2024 version, even if a new version is published in 2025. A receipt produced in 2024 references the 2024 version. Whoever wants to reproduce the receipt in 2034 finds the 2024 version, hash anchored, not overwritten.

This stacking is the ground of reproducibility over time. A receipt produced in 2024 is reproducible in 2034 because the 2024 version is still stored in 2034, with the same hash, in the same place. Whoever asks, which rule applied in 2024, finds the answer in the rule catalog that still contains the 2024 version.

Part Fifteen: The Layers Of Transparency

Chapter 84: Transparency Inward

The system is transparent inward. Every check carried out is documented in the system. Every receipt produced lies present. Every decision made is traceable. Whoever has access to the system can check the completeness of the chain, can establish gaplessness, can reproduce integrity.

This transparency inward is the precondition for transparency outward. Whoever is not transparent inward can assure outward nothing he cannot himself check.

Chapter 85: Transparency Outward

The system is transparent outward. The public key is published. The receipts that leave the system carry the public key embedded. Whoever receives the artifact can verify the signature without consulting the system. The system requires no continuing trust relationship, no running connection, no subscription.

This transparency outward is the ground of portable provability. It is the condition for a proof to still be deliverable years later when the producing system may already be archived.

Chapter 86: Transparency About The Limits

The system is transparent about its limits. It documents what it cannot do, what it does not deliver, what it does not assure. It claims no care it does not have. It claims no reliability it cannot deliver. It claims no court admissibleness that only an external body can set.

This transparency about the limits is no pedagogical motivation but a duty of proof. Whoever delivers proof must also state the trust boundaries of that proof. Whoever conceals the limits cheats the verifier who trusts the proof.

Chapter 87: Transparency About The Open Points

The system is transparent about its open points. It documents what is not yet calibrated, what is not yet engaged. It does not conceal that the law firm partnership for External Validation Records is outstanding, with the procedures running, that the calibration values for CRPG are start values, that the rotation process for the portable proof keys is under review. The air density correction at Gate M9 after SAE

J1349 / DIN 70020 is implemented and active, it is part of the three complete weather normalization layers.

This transparency about the open points is the practice form of an honest system documentation. Whoever conceals the open points produces a pseudo precision that becomes brittle in the forensic dispute. Whoever documents the open points delivers a picture that holds even in the serious case.

Part Sixteen: The Layers Of Error

Chapter 88: The Faulty Input

A faulty input is not corrected but documented. The system does not smooth. It shows that the input is faulty and stops. Whoever wants to correct the input must deliver a new input that stands in a new receipt chain. The faulty receipt remains in the chain, documenting that it was faulty. The corrected receipt is a new entry that references the faulty one.

That is the append only method of dealing with errors. Errors are not deleted but corrected. The correction is visible, and the error is visible. Whoever later asks, was this input faulty, finds the answer in the chain, together with the correction.

Chapter 89: The Faulty Rule

A faulty rule is a rule that was stored incorrectly. The system applies the rule as stored. It does not interpret whether the rule is correct. It applies it and seals the application.

If it is later determined that the rule was faulty, that is no retrospective correction of the receipts that rest on this rule. The faulty rule remains stored in the versioned basis. A new rule version is published that replaces the faulty one but does not overwrite it. Receipts that rest on the faulty rule continue to reference the faulty rule. Receipts produced after the new rule version reference the new rule version.

Whoever later asks, was this check carried out with the faulty rule, finds the answer in the chain, referenced to the faulty rule version. The insight that the rule was faulty is forensically traceable. The retrospective correction is documented in the new rule version. The old receipt remains reproducible because the old rule version remains stored.

Chapter 90: The Faulty Decision

A faulty decision is a decision that was made wrongly. The system cannot correct the decision. It can document that the decision was made, with reasoning, to which receipt referred.

If the decision is later recognized as faulty, a repeal can follow, in a procedure at least as strict as the original procedure. The repeal is a new entry that references the original decision. The original decision remains in the chain, documenting that it was made, with reasoning. The repeal is a new entry documenting that the decision was repealed, with reasoning, with reviewers.

The system does not delete. It corrects by stacking. A faulty decision is visible, and its repeal is visible. Whoever later asks, was this decision faulty, finds the answer in the chain, together with the repeal and its reasoning.

Chapter 91: The Faulty Key

A faulty key is a key that was compromised. The system can revoke the key, not undo what was signed with it. Receipts that were signed with the compromised key are to be evaluated with the knowledge of the compromise. The system documents the compromise and the revocation.

A new key ceremony produces a new key pair that replaces the revoked key. Future receipts are signed with the new key. The old receipts that were signed with the compromised key remain in the chain, reference the compromised key, and are forensically to be evaluated with the knowledge of the compromise.

The system cannot undo the past. It can secure the future, through rotation, through revocation, through new keys. Transparency about the compromise is the precondition for a verifier to evaluate the old receipts correctly. Whoever conceals the compromise cheats the verifier.

Part Seventeen: The Layers Of Ignorance

Chapter 92: Ignorance About The Input

The system cannot know something. It cannot know whether the input is complete when the input actor conceals something. It can only document what was delivered and check forensic admissibility.

This ignorance is no weakness but a condition. The system is no oracle. It is an evidence instrument that forensically loadably holds what was delivered. Whoever conceals something bears the responsibility for the concealment. The system documents that it did not know the concealed, not that the concealed did not exist.

Chapter 93: Ignorance About The Rule

The system cannot know whether the rule it applies is correct. It can only document which rule, in which version, was applied. Responsibility for the correctness of the rule lies with whoever stored the rule.

This ignorance is the ground of forensic clarity. The system applies the rule as stored. It does not assure that the rule is correct but that the rule was applied. Whoever disputes the correctness of the rule turns to whoever stored it, not to the system.

Chapter 94: Ignorance About The Future

The system cannot know which future legal situation will apply. It can only document which legal situation applied at the time of the check. The versioned rule basis is the answer to this ignorance. It holds what applied, not what will apply.

Whoever later asks, was this check correct under the then current legal situation, finds the answer in the receipt, not in a gut feeling. Whoever asks, would this check be correct under today's legal situation, must carry out a new check against today's rule version. The system allows both questions but it does not allow mixing them.

Chapter 95: Ignorance About AI

The system can deploy AI in clearly limited roles, say in text extraction or source consolidation. The AI reads and classifies, it does not decide. The system cannot know how the AI arrived at a classification because the AI is a model that rests on training data.

This ignorance is the reason AI does not decide. A decision that rests on ignorance is not forensically robust. A decision that rests on a deterministic rule is. The system chooses the loadable form because it must secure forensic reproducibility.

Part Eighteen: The Layers Of Fairness

Chapter 96: Fairness Toward The Checked

The system is fair toward the checked. It documents what was checked, on which input, with which rule, at which time. It invents no accusations, it smooths no findings. Whoever is checked can see the receipt that is the finding, and he can have it checked, by a third party, without prior relationship, without trust.

This fairness is the ground of acceptance of the system. Whoever finds the system unfair because it documents gaplessly has not understood that the gaplessness serves him. Whoever was checked wrongly finds the error in the receipt, not in a guess. Whoever was checked correctly finds the confirmation in the receipt. Both have the same tool, the same piece of evidence, the same reproducibility.

Chapter 97: Fairness Toward The Examiner

The system is fair toward the examiner. It takes the burden of proof from him, not the decision authority. It delivers him a picture that he evaluates. He decides, not the machine.

This fairness is the ground of acceptance of the system with the examiner. Whoever keeps the decision authority accepts the system as a tool. Whoever loses the decision authority because the machine decides rejects the system as a replacement decider. The system chooses the first form because it is the forensically viable one.

Chapter 98: Fairness Toward The Auditor

The system is fair toward the auditor. It delivers him the receipts, the hashes, the rule versions, the time anchors. He recalculates, without trust. The system is his tool, not his opponent.

This fairness is the ground of acceptance of the system with the auditor. Whoever uses the system as a tool comes to a finding that is reproducible. Whoever views the system as an opponent comes to a

finding that fails on his mistrust, not on the system. The system chooses the first form because it is the forensically robust one.

Chapter 99: Fairness Toward The Supervision

The system is fair toward the supervision. It delivers it the method, the data, the chain. The supervision can reproduce, differentiate, judge. It can determine that one institute has a three year old chain that is reproducible and that another institute has a three year old PDF archive that is not reproducible.

This fairness is the ground of acceptance of the system with the supervision. Whoever has the system has a supervisory position that otherwise lacks. Whoever does not have the system has a supervisory position that becomes brittle in three years. The system addresses the supervision not with the claim that compliance improves but with the proof that compliance becomes reproducible.

Chapter 100: Fairness Toward Society

The system is fair toward society. It documents the decisions made in the compliance environment in a form that is reproducible. Society, which increasingly demands transparency of decisions, gets a tool that delivers this transparency, not claims it.

This fairness is the ground of acceptance of the system in society. Whoever has the system can give society an answer that a society without the system cannot give. The answer reads that the decisions made in this institute are reproducible after years, not after claims.

Part Nineteen: The Layers Of The Future

Chapter 101: The Future Of Supervisory Practice

Supervisory practice is moving in a direction that views cryptographic reproducibility of compliance decisions no longer as a bonus but as a minimum requirement. DORA, EU AI Act, AMLA are the indicators of this movement.

The system is built for this future. It has reproducibility today, not tomorrow. Whoever builds a chain today has in three years a three year old chain that meets this future. Whoever begins tomorrow has in three years a zero year old chain that does not meet this future.

Chapter 102: The Future Of Forensic Practice

Forensic practice is moving in parallel. An appraisal that leafed through a PDF archive ten years ago will expect cryptographic reproducibility in three years. The opposing side's question, where is the hash reference to the then current sanctions list, is a polite question today, a standard question in three years.

The system is built for this future. It has the cryptographic reference today, not tomorrow. Whoever can answer today has a different negotiating position than the one who must answer tomorrow but cannot today.

Chapter 103: The Future Of Cryptography

Cryptography is moving toward post quantum. Today's procedures, ECDSA P256, are considered secure today, but the future quantum computer can break them. The system has the documented migration path to the hybrid signature of ECDSA P256 plus ML DSA 65.

The system is built for this future. It has the migration path today, not tomorrow. Whoever produces a receipt today has in twenty years a receipt that was signed under the cryptographic procedures valid then, plus a post quantum layer that survives the future quantum computer.

Chapter 104: The Future Of Sport Governance

Sport governance is moving in a direction that demands forensic reproducibility. A society that increasingly critically questions the transparency of refereeing will demand forensic reproducibility in the near future.

The system is built for this future. It has reproducibility today. An association that builds a receipt chain today has in five years a five year old chain that meets this future. An association that begins tomorrow has in five years a zero year old chain that does not meet this future.

Chapter 105: The Future Of The Compliance Method

The compliance method is moving from documentation to proof, from probability to determinism, from trust to checking, from gappiness to gaplessness. The system is the crystallization of this movement.

This future is no prediction but a description of a movement already under way. The system is not the driver of this movement but its answer. Whoever has the system is on this movement. Whoever does not have the system will be caught up by it.

Part Twenty: Conclusion

Chapter 106: What This System Is

This system is an evidence system. It is no decision system, no reporting system, no documentation system. It is an evidence system that delivers forensically robust proofs that are still reproducible after years.

It cannot declare itself court admissible. It does not decide, it proves. It does not smooth, it documents. It does not trust, it checks. Exactly these four lines are the scaffold on which every building block of this ecosystem stands.

Chapter 107: What This System Is Not

This system is no oracle. It does not know the future. It does not know the correctness of the rule. It does not know the completeness of the input. It does not know the competence of the decider.

It knows only what was delivered, the rule that was applied, the point in time at which was checked, and it holds what was delivered forensically loadably. That is enough for a proof, but it is not enough for a

truth. Truth is a human finding. Proof is a mathematical finding. The system does the second, not the first.

Chapter 108: What This System Wants

This system wants to deliver proofs that can still be checked years later without anybody remembering the event. It wants to make responsibility attributable, not to shift it. It wants to close the gaps in today's compliance, not through more documents but through better proofs. It does not want to be the first but the most reliable.

Chapter 109: Whoever Has Understood This System

Whoever has understood this system has understood not a product but an attitude. The attitude reads that compliance is not a document but a proof, and that this proof is only valuable when it can still be delivered years later.

Whoever has understood this attitude has understood why the choice of the start is not arbitrary. Every year that passes without the chain being built is a year missing in the chain. And the missing year is no longer retrievable in the review.

Chapter 110: Final Sentence

The system is an evidence system built for a world where proofs today are mostly gone after three years or rest on assumptions. It delivers proofs that still stand after years. That is the decisive difference, and it is enough.

Conclusion

This document describes a system that arose from the world of today's compliance. It does not claim to solve this world. It claims to deliver, in this world, proofs that still stand years later. That is not little. In a world where proofs today are mostly gone after three years or rest on assumptions, that is the decisive difference.

Whoever has understood this system has understood not a product but an answer. The answer reads:

> ***Compliance is not a document but a proof, and this proof is only valuable when it can still be delivered years later.***

The system is no decision system. It is an evidence system. It cannot declare itself court admissible. It does not decide, it proves. It does not smooth, it documents. It does not trust, it checks. Exactly these four lines, proof instead of decision, external instead of self set court admissibleness, documentation instead of smoothing, checking instead of trust, are the scaffold on which every building block of this ecosystem stands. Whoever has understood this scaffold has understood the system.**Part Twenty-One: Technical Appendix**

Table A1: Gate Pipeline Order

Pos.	Gate	Type	Result
0	Gate 0	Inlet/Hash	Forensic admissibility
1	GLEIF Gate	Identity	Entity verified
2	Sanctions Gate	Identity	CLEAR/BLOCK/UNCLEAR
3	AML Gate	Matter	Reporting duty check
4	Jurisdiction Gate	Matter	Conflict documented
5	Fundamental Rt.	Matter	Touch marked
6	Sector Gate	Matter	Sector finding
7	Procedure Gate	Procedure	Deadline/Completeness
8	T0 Gate	Conclusion	Overall picture sealed

Table A2: Two Verification Classes

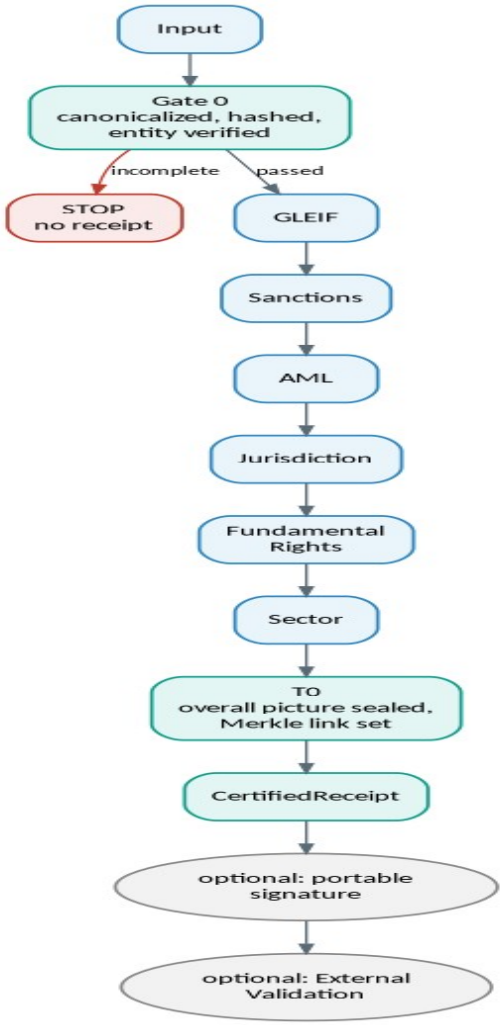
Property	Class 1 (HMAC)	Class 2 (ECDSA)	Class 2+ (PQC)
Crypto	Symmetric	Asymmetric	Hybrid
Key	Shared	Priv/Public	ECDSA + ML-DSA65
Direction	Internal	External	Int + Ext
Portable	No	Yes	Yes
Trust	Shared secret	Public proof	Doubly secured
Cases	Internal chain	Export	Post-Quantum era

Table A3: Two Axis Logic

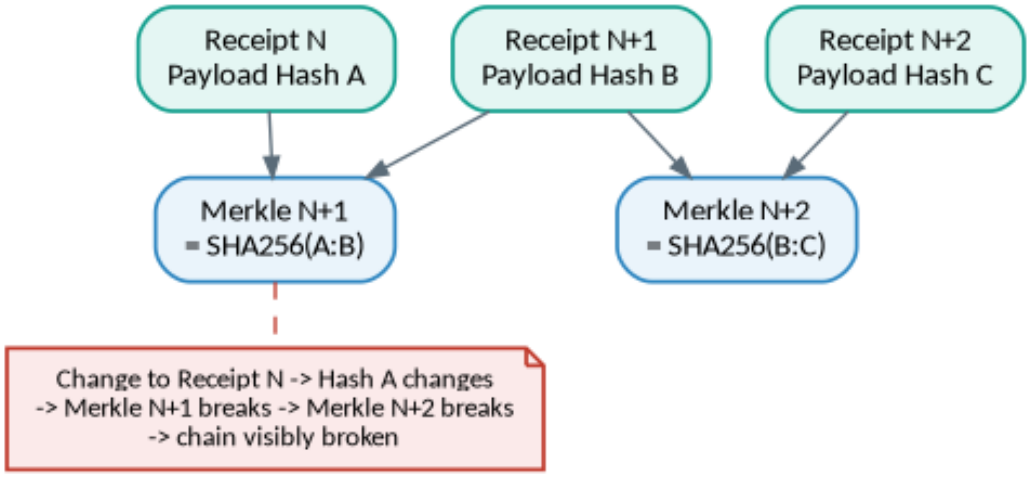
Axis	Name	Who sets?	Condition
Axis 1	Tech. integrity	System (cryptography)	Hash+Sig+Chain
Axis 2	court admissible	External firm (EVR)	Appraisal+Sig

Core sentence: The system can never set Axis 2 itself.

Sketch B1: Gate Pipeline Flow



Sketch B2: Merkle Chain Linking



Sketch B3: Two Axis Diagram

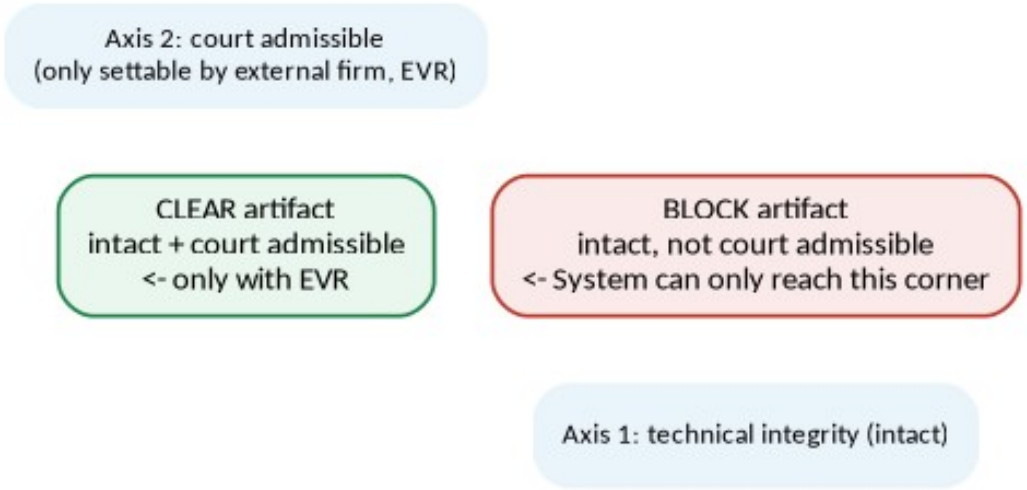


Table A4: Weather Normalization Layers Gate M9

Layer	Procedure	Status	Granularity
1	Discard non-DRY	Implemented	per sector
2	Wind vector proj.	Implemented	per sector
3	Air density J1349	Implemented and active	per sector

Layers 2 and 3 are strictly separated, never mixed. Layer 3 (air density correction) is implemented and active; reference condition: 99 kPa, 25 C, dry, per SAE J1349 / DIN 70020.

Sketch B4: Weather Correction Pipeline Gate M9

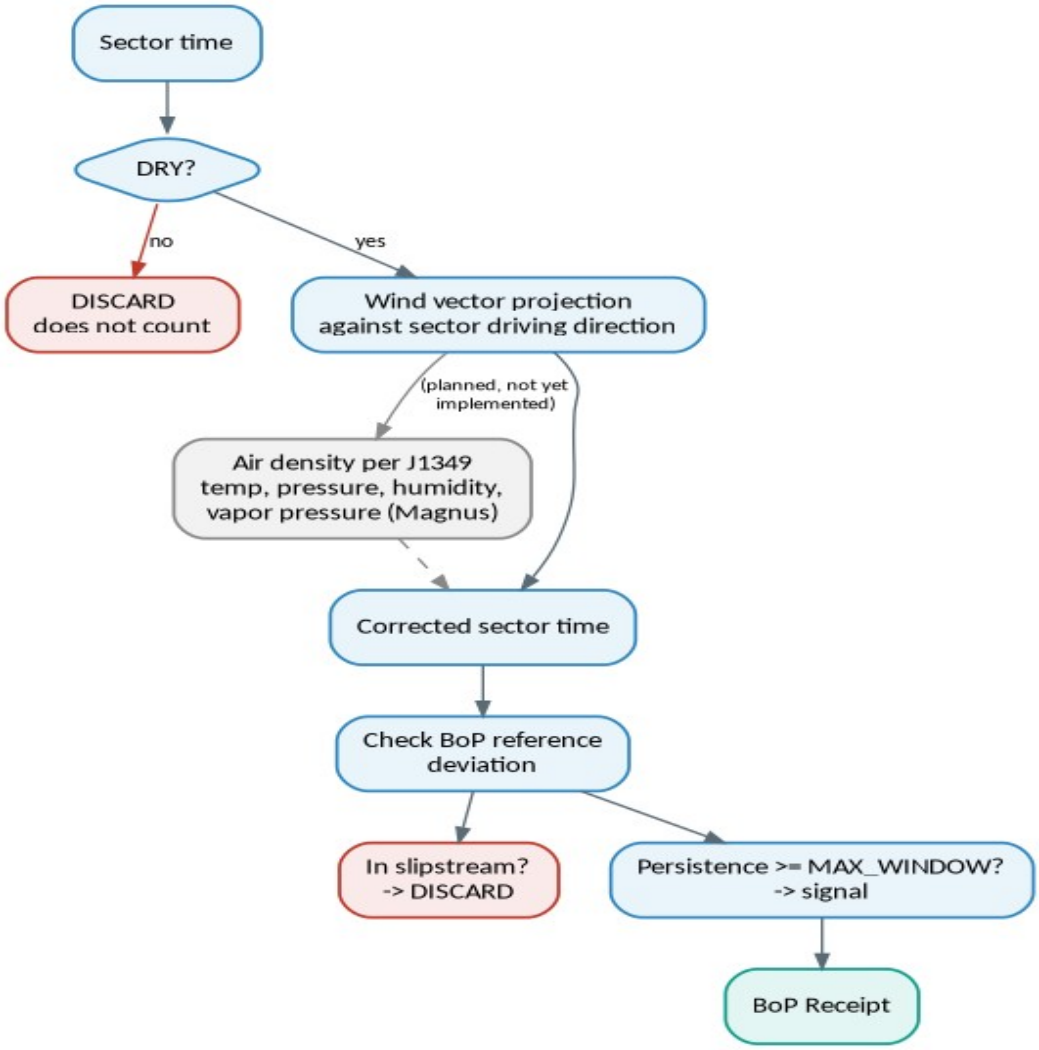


Table A5: Sector Engines Comparison

Sector	Primary Gates	Competitor does	Here different
Banking	GLEIF,Sanc,AML, Basel III	PDF report	Hash-anchored chain
Insurance	Solv II,IDD,AML	3 notes	Receipt set
M&A	6 dim. 7 steps	tool bought	MaDDReceipt
Real Est.	BoO,SoF,Sanc,AWG	notary list	Notary chain
Cloud	DORA,C5,ISO27001	annual cert	Receipt per ev
Energy	RE-Direct,AWG,San	PDF archive	Day reference
Sport	FIFA Laws 10,11,12	VAR video	SportDecision
Motorsp.	M0-M9, SAE J1349	series-internal	BoP Receipt

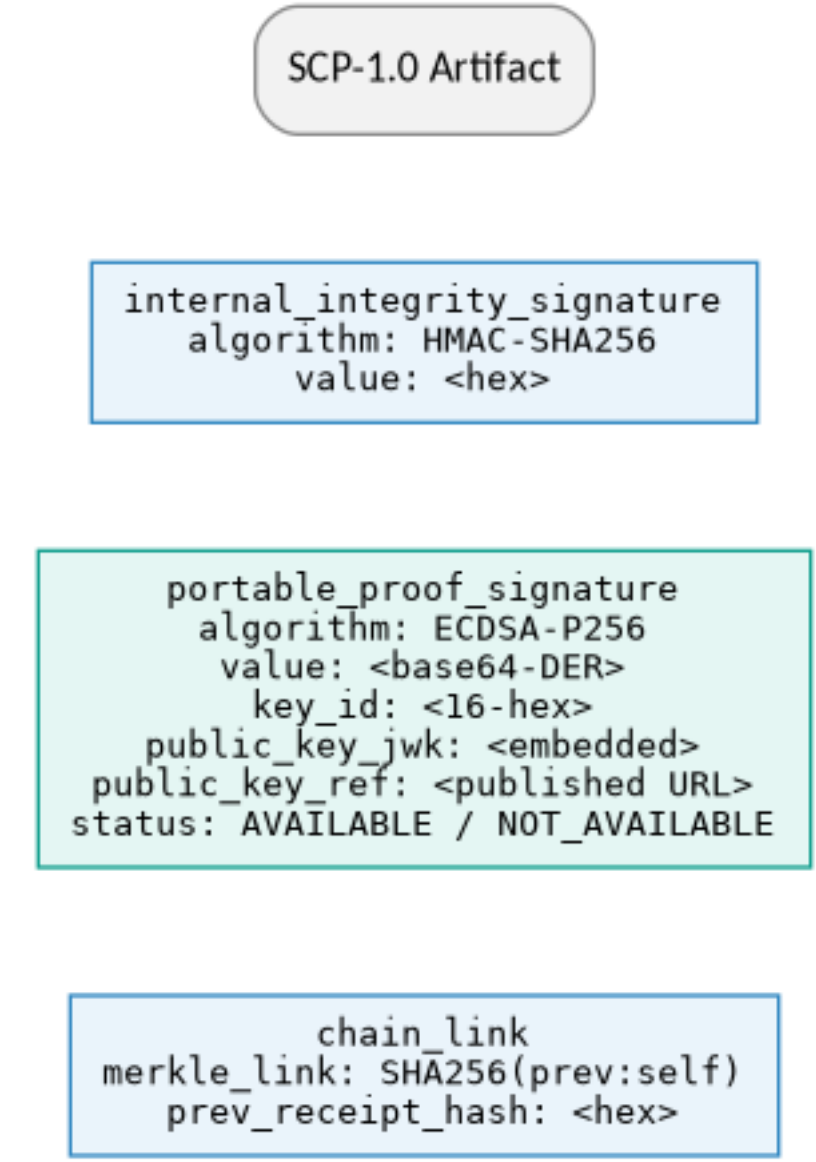
Table A6: Actors And Roles

Actor	Role	Sets/Decides
Compliance Off.	First evaluation	Release/Block
Referee	Sport decision	Indication on/off
Tech. Steward	Motorsport eval.	BoP finding
Law Firm	External appraisal	Axis 2 (EVR)
Intermediary	Between system/customer	Receipt in own name
Auditor	retrospective review	Finding Receipt
Supervision	sector review	difference found

Table A7: Time Layers

Time	Meaning	When decisive
Pre-run time	Input fixed in Gate 0	Start of chain
Transaction t.	Receipt sealed	NTP-anchored
Valid time	Legal situation from	Which rule applies

Sketch B5: SCP-1.0 Verification Block



Sketch B6: Receipt Life Cycle

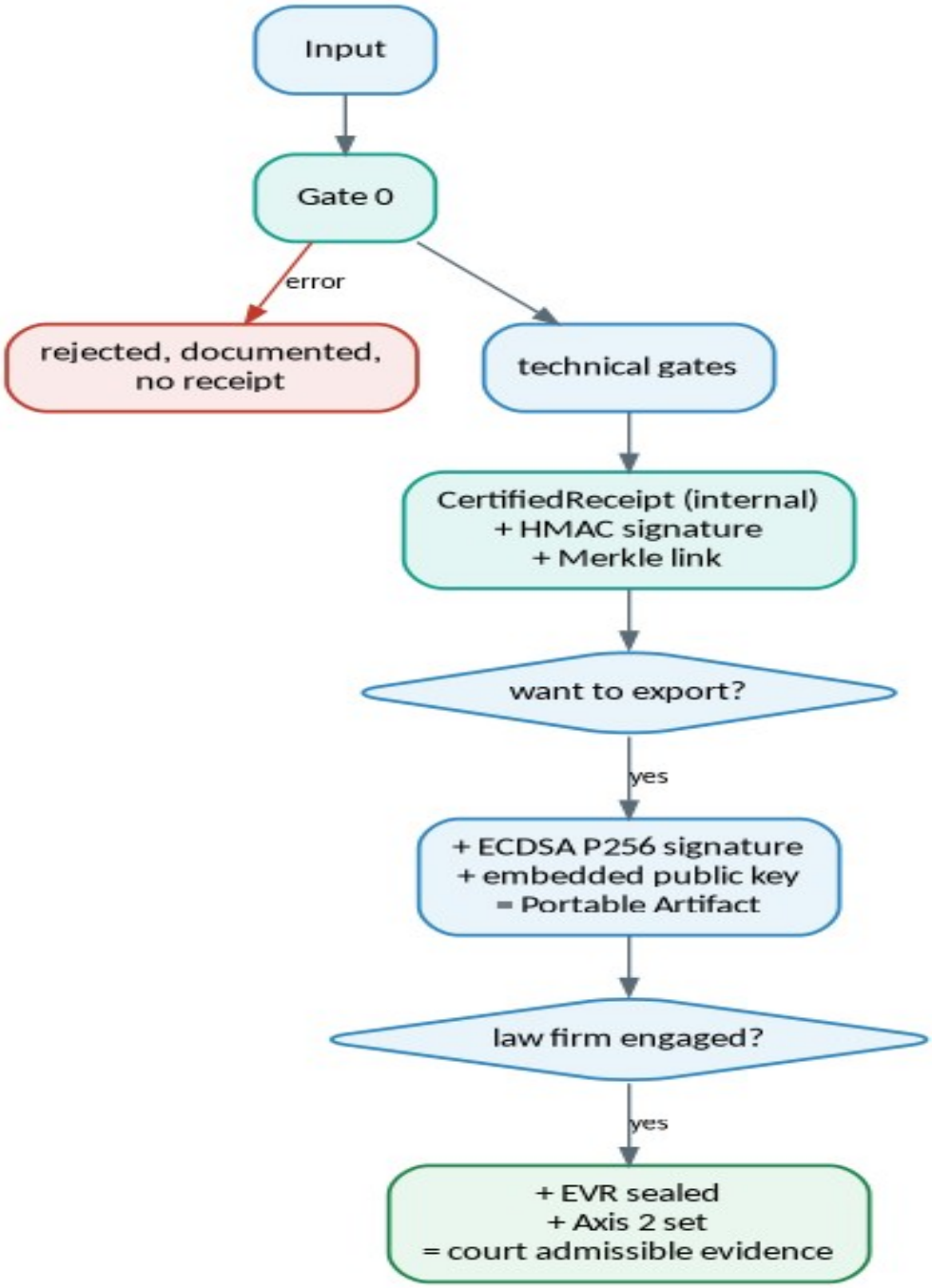


Table A8: Receipt Type Prefixes

Prefix	Receipt type	Example
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 Artifact	T0-TEN-2025-00003
GM-	Motorsport Receipt	GM-SERIES-EVENT-12-0004
GATESPORT-	Sport Decision Receipt	GATESPORT-MATCH-2026003-47-001
EVR-	External Validation	EVR-DE-2025-00001

Sketch B7: Key Ceremony v2

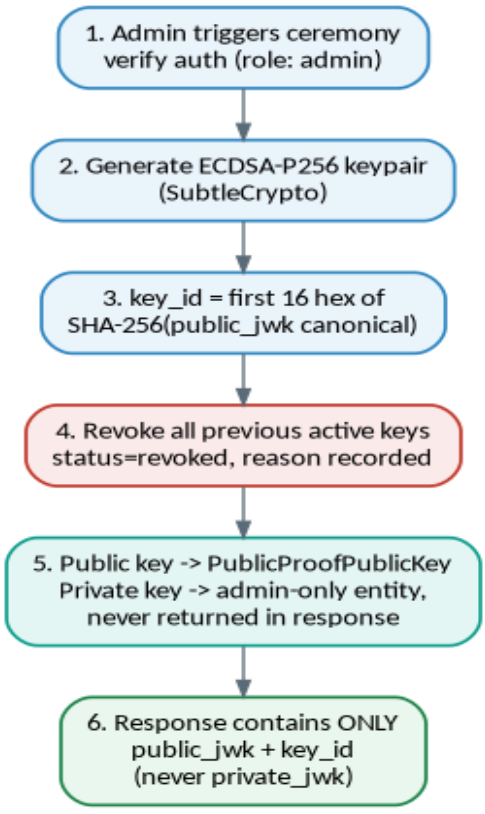


Table A9: Cryptographic Primitives

Primitive	Class	Use
SHA-256	Hash	Input, Rule, Merkle, Receipt
HMAC-SHA256	MAC, symmetric	internal integrity
ECDSA-P256	Signature, asym.	portable provability
ML-DSA-65	PQ-sig (FIPS204)	hybrid migration (planned)
RFC 8785	JCS	canonical JSON form
Merkle-Link	Chaining	SHA256(prev:self)
NTP	Time source	Time anchor

Sketch B8: CRPG Architecture

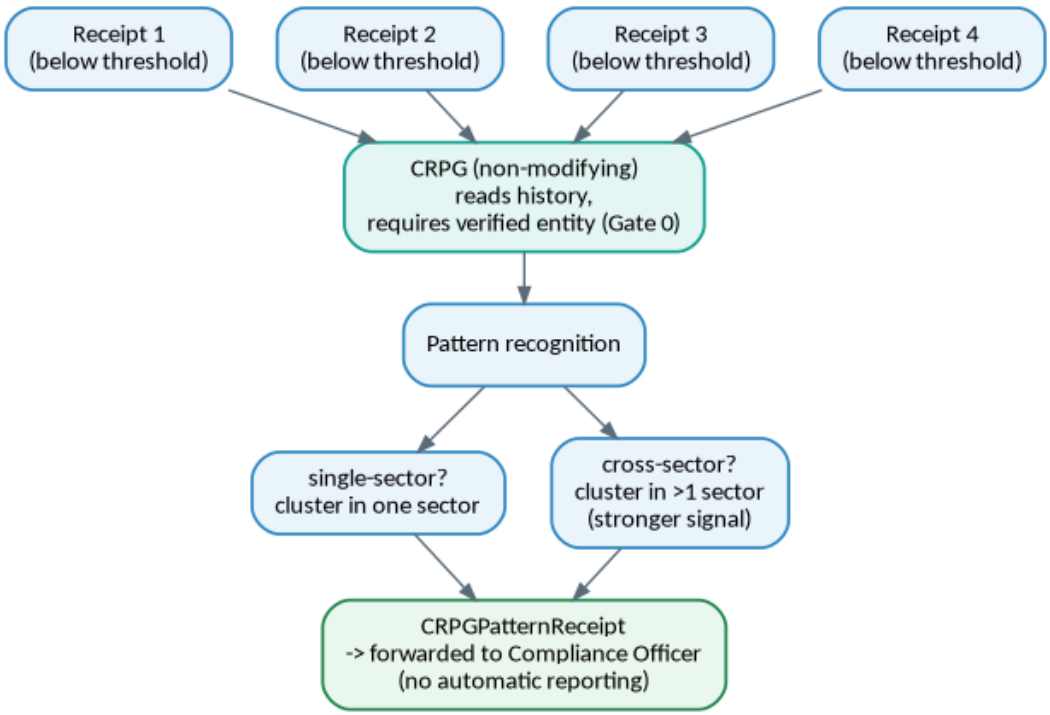


Table A10: Data Sources And Hashes

Source	Content	in receipt
GLEIF	LEI register	LEI + snapshot-h.
EU FSF	EU sanctions	list-hash
OFAC SDN	US sanctions	list-hash
UK HMT	UK sanctions	list-hash
UN SC	UN sanctions	list-hash
FATF	FATF lists	list-hash
Rule catalog	rules (versioned)	rule-hash

Sketch B9: Post Quantum Hybrid Signature

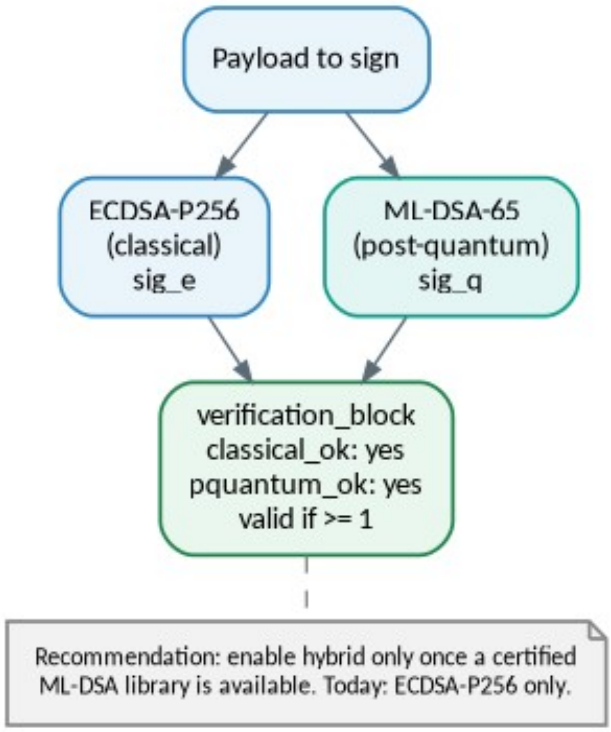


Table A11: System Limits

Nr	Limit	Note
1	No automated sanction	human act
2	No AI decision	AI only reads
3	Every uncertainty documented	never hidden
4	Human retains decision authority	system proves
5	Repeal at least as strict as original	6-eyes
6	System does not set axis 2 (court admissible)	external: EVR

Sketch B10: System Overall Architecture

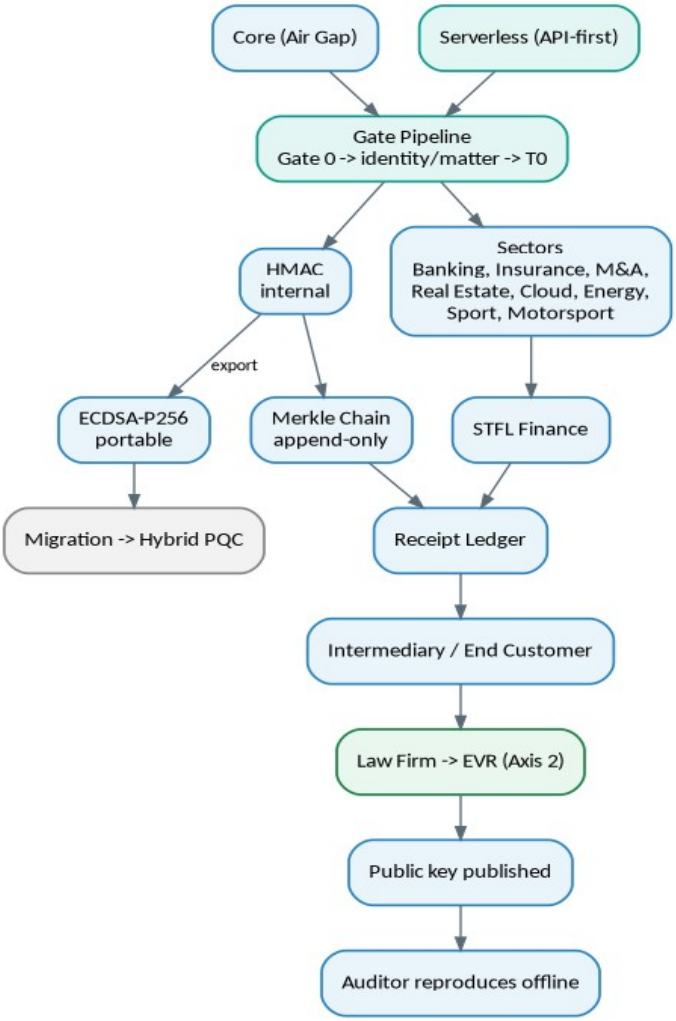


Table A12: Export And Verification

Export	HMAC	ECDSA	EVR
Internal	Yes	Optional	Optional
To intermediary	Yes	Yes	Optional
To external recipient	Yes	Yes	Recommended
Public check	(insufficient)	Yes	(+)

Sketch B11: Repeal Procedure

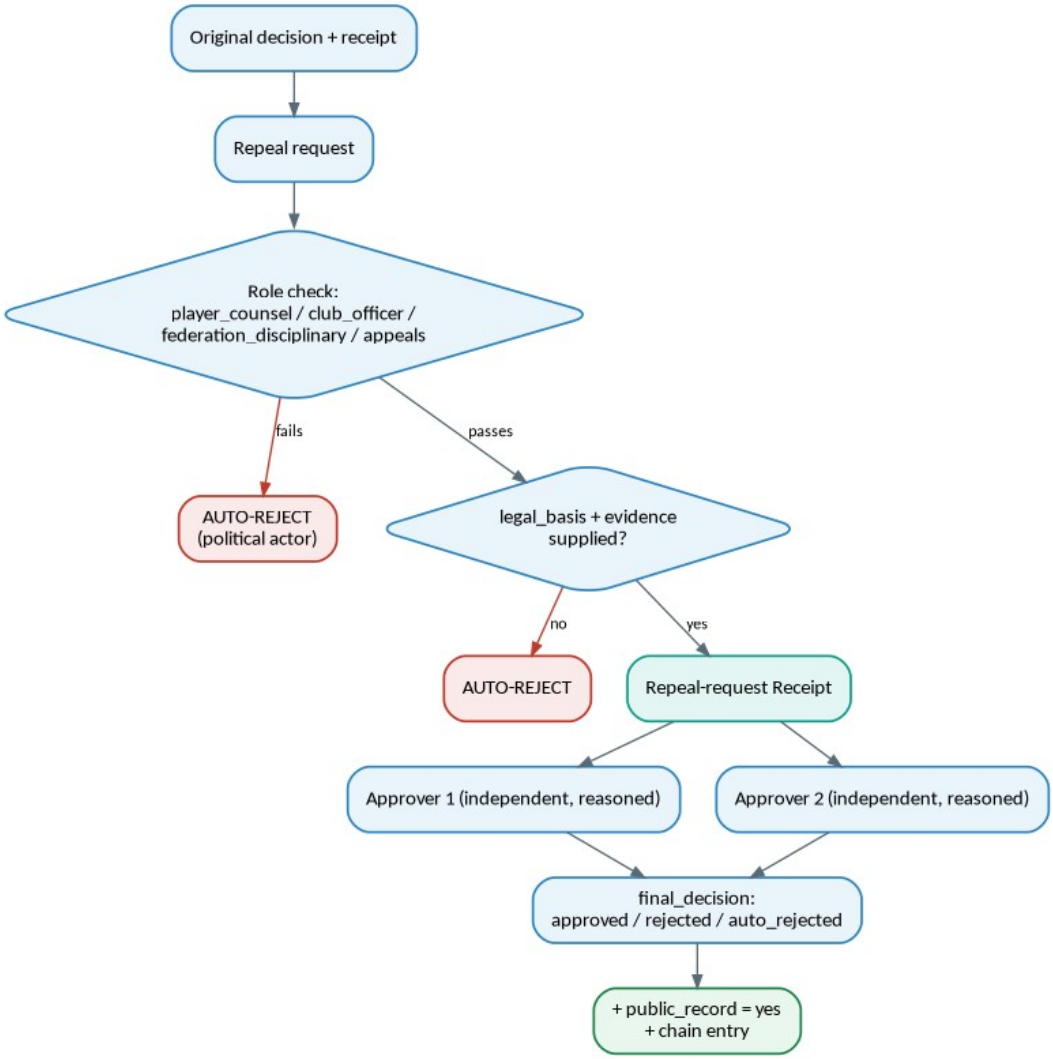


Table A13: Cost Categories And Values

Question	System answers
Price per check?	Wrong question
Price per proof?	Correct question
Pricing unit	Receiving boundary (resp.)
Billing	Annual license
Intermediary invoice?	yes