Network Working Group
Internet-Draft
Intended status: Informational
Expires: 7 November 2026

J. A. Gomes Marques
Asqav

6 May 2026

Compliance Profile of Signed Action Receipts for AI Agents
draft-marques-asqav-compliance-receipts-03

Abstract

This document defines a multi-jurisdiction compliance profile of the signed action receipt format used by AI agents to record machine-readable evidence of access-control decisions. The profile binds receipt fields to two regulatory surfaces: the European Union obligations of Articles 12 and 26 of Regulation (EU) 2024/1689 (the EU AI Act) and Article 17 of Regulation (EU) 2022/2554 (DORA), and the United States obligations of the NIST Artificial Intelligence Risk Management Framework, the Colorado Artificial Intelligence Act (SB 24-205), the Texas Responsible AI Governance Act (HB 149), the New York Department of Financial Services Cybersecurity Regulation (23 NYCRR Part 500), the HIPAA Security Rule (45 CFR Part 164, Subpart C), SEC Rule 17a-4 (17 CFR 240.17a-4), and the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). It does not redefine the wire format, the canonicalization rule, or the signing algorithms of the underlying receipt format. It tightens a subset of the OPTIONAL fields to REQUIRED, imposes a retention floor, requires at least one timestamping anchor (RFC 3161 or OpenTimestamps; both RECOMMENDED), and adds two extension fields.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 7 November 2026.

Table of Contents

1. Introduction

1.1. Profile, Not Fork

[ACTA-RECEIPTS] specifies a generic, signed receipt envelope for recording machine-to-machine access control decisions made by AI agents. Section 2.2 of [ACTA-RECEIPTS] defines a common payload field set in which all fields except type, issued_at, and issuer_id are OPTIONAL. Section 5.7 of [ACTA-RECEIPTS] introduces hash chaining (previousReceiptHash) inside an optional Commitment Mode extension. [ACTA-RECEIPTS] does not define receipt retention, does not require timestamping anchors, and does not bind to any regulatory regime.

This document is an additive overlay on [ACTA-RECEIPTS]: it constrains fields the upstream draft leaves OPTIONAL, fixes their values where regulation requires, and adds two extension fields with reserved names. A Compliance Receipt remains a conformant [ACTA-RECEIPTS] receipt. Field references use upstream field names rather than section numbers, to reduce maintenance hazard if upstream re-numbers in a future revision.

1.2. Scope

This document fills the regulatory binding gap on two surfaces. Section 5 binds the receipt to European Union obligations: Article 12 (record-keeping) and Article 26 (deployer obligations) of the EU AI Act, and Article 17 (ICT-related incident management) of DORA. Section 6 binds the receipt to United States obligations: the voluntary functions of the NIST AI Risk Management Framework, the deployer obligations of the Colorado AI Act and the Texas Responsible AI Governance Act, the audit-trail and incident-reporting obligations of NYDFS Part 500, the audit controls and documentation retention of the HIPAA Security Rule, the broker-dealer recordkeeping requirements of SEC Rule 17a-4, and the covered-incident reporting requirements of CIRCIA.

The bindings are written from the Deployer’s perspective, where Deployer is used in the regime-specific sense (Article 3(4) of [EU-AI-ACT] for EU bindings; Section 6-1-1701(6) of the Colorado Revised Statutes for Colorado bindings). Where another statute uses a different term (Provider, Financial Entity, Covered Entity for HIPAA, Covered Entity for NYDFS, Broker-Dealer for SEC, Covered Entity for CIRCIA), the binding section names the term as the source statute uses it.

A verifier that implements only [ACTA-RECEIPTS] can cryptographically validate a profile receipt but cannot attest the additional compliance bindings of this document.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

The following terms are used in this document.

Action: An operation performed by an AI agent that is subject to a

policy evaluation. Examples include a tool invocation, an external API call, a write to durable storage, and the issuance of an irreversible instruction to another system.

Action Receipt: A signed envelope conforming to [ACTA-RECEIPTS] that records the policy evaluation result for a single Action.

Compliance Receipt: An Action Receipt that additionally satisfies the requirements of this profile.

Deployer (EU AI Act): As defined in Article 3(4) of [EU-AI-ACT].

Deployer (Colorado AI Act): As defined in Section 6-1-1701(6) of the Colorado Revised Statutes, as enacted by [COLORADO-AI-ACT].

High-Risk AI System (EU AI Act): As defined in Article 6 of [EU-AI-ACT].

High-Risk AI System (Colorado AI Act): As defined in Section 6-1-1701(9) of the Colorado Revised Statutes, as enacted by [COLORADO-AI-ACT].

Financial Entity: As defined in Article 2(2) of [DORA], for entities listed in Article 2(1).

Covered Entity (HIPAA): As defined in 45 CFR 160.103, namely a health plan, a health care clearinghouse, or a health care provider that transmits health information in electronic form in connection with a covered transaction.

Covered Entity (NYDFS): As defined in 23 NYCRR 500.1(e), namely any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law, regardless of whether the covered entity is also regulated by other government agencies.

Broker-Dealer: As defined in section 3(a)(4) and 3(a)(5) of the Securities Exchange Act of 1934, subject to recordkeeping under [SEC-17A-4].

Covered Entity (CIRCIA): As to be defined in the final rule promulgated under the Cyber Incident Reporting for Critical Infrastructure Act of 2022. Pending publication of the final rule, the term is interpreted in accordance with the statutory definition at 6 U.S.C. 681 and CISA’s notice of proposed rulemaking.

Audit Pack: A bundle of Compliance Receipts, the chain commitments that link them, the public verification keys, the trust anchor metadata, and the regime mapping required by Sections 5 and 6 of this document, packaged for delivery to a regulator or auditor.

3. Relationship to ACTA-RECEIPTS

This profile is an additive overlay on [ACTA-RECEIPTS]. It does not modify the envelope, the canonicalization rule, the signature object, or the algorithm registry of [ACTA-RECEIPTS].

The following normative statements apply.

* Implementations of this profile MUST produce receipts that are cryptographically verifiable by a conformant [ACTA-RECEIPTS] verifier under the canonicalization rules (JCS, [RFC8785]) and the signature scope of [ACTA-RECEIPTS] Section 5.6.

* Implementations of this profile MUST NOT introduce new top-level fields in the signed payload that conflict with names reserved by [ACTA-RECEIPTS].

* Implementations of this profile MAY use any signature algorithm permitted by [ACTA-RECEIPTS]: EdDSA (Ed25519, mandatory-to-implement, [RFC8032]), ES256 (ECDSA using P-256 and SHA-256, [RFC7518]), and ML-DSA-65 ([FIPS204]).

* Where [ACTA-RECEIPTS] marks a field OPTIONAL and this profile marks the same field REQUIRED, the stricter requirement applies to Compliance Receipts.

A receipt that fails any MUST clause of this profile is not a Compliance Receipt. It MAY still be a valid [ACTA-RECEIPTS] receipt.

This profile differentiates from [ACTA-RECEIPTS] on three axes: mandatory hash-chain linkage (upstream Commitment Mode is OPTIONAL), mandatory anchoring with RFC 3161 or OpenTimestamps (both RECOMMENDED; upstream lists Sigstore Rekor in its Implementation Status appendix as an OPTIONAL temporal anchor), and a retention floor tied to specific regulatory articles (upstream is silent on retention).

4. Receipt Field Profile

This section enumerates fields defined by [ACTA-RECEIPTS] and states the additional requirements that this profile places on them. Field names follow [ACTA-RECEIPTS] exactly.

Compliance Receipts MUST use the upstream wire field name signature for the signature object, exactly as defined in Sections 2.1 and 2.1.1 of [ACTA-RECEIPTS]. The keys inside that object are alg, kid, sig. Implementations whose internal storage uses a different field name MUST translate to signature on emission and on canonicalization for verification; receipts that appear on the wire under any other top-level field name are non-conformant to [ACTA-RECEIPTS] and to this profile. Anchors MUST be projected into a top-level anchors array with a type discriminator and a value field carrying the anchor bytes (base64-encoded for binary payloads). Flat-column implementations MUST project on emission and Audit Pack export.

4.1. Common Payload Fields

4.1.1. type

Compliance Receipts MUST set type to a value drawn from the namespace protectmcp:decision, protectmcp:restraint, or protectmcp:lifecycle, or to an extension namespace registered for use with this profile.

4.1.2. issued_at

REQUIRED upstream and in this profile. The value MUST be an ISO 8601 timestamp with an explicit timezone. The producing system MUST source the value from a clock synchronized to a recognized time authority and MUST NOT backdate the value. Verifiers MUST reject receipts whose issued_at is more than 300 seconds ahead of the verifier’s own clock. Verifiers MUST NOT reject a receipt solely because issued_at lies in the past; past skew is bounded by the applicable retention floor in Sections 5 and 6, not by freshness. Historical receipts within retention MUST verify on the same path as fresh ones.

4.1.3. issuer_id

REQUIRED upstream and in this profile. The value MUST identify a legal entity, not a natural person. Where the producing system is operated by a Deployer, the issuer_id MUST resolve, through the trust anchor metadata in the Audit Pack, to a record naming the Deployer. To preserve the upstream Section 2.2 invariant that issuer_id MUST match the kid field of the signature object, Compliance Receipts MUST place the same value in both issuer_id and kid; the verifier resolves that value to a public key through the Audit Pack trust-anchor metadata rather than through the well-known JWK Set endpoint or the RECOMMENDED sb:issuer:<base58-fingerprint> form of [ACTA-RECEIPTS] Section 2.1.1. This profile thereby supersedes the upstream RECOMMENDED kid format for Compliance Receipts; the upstream RECOMMENDED format remains valid for non-Compliance receipts.

Implementations SHOULD use a Legal Entity Identifier (LEI) as defined by [ISO17442] where one is allocated to the Deployer. Examples and test fixtures MUST use a placeholder whose four-character LOU prefix (positions 1-4) is not allocated in the GLEIF Local Operating Unit code list, whose positions 5-6 are the ISO 17442 reserved value 00, and whose two trailing characters (positions 19-20) are the ISO 7064 mod 97-10 check digits computed over positions 1-18 (for example 000000000000000098, where the all-zero 18-character base produces the check digits 98 per the ISO 17442-1:2020 Annex A check-digit algorithm, which converts any letters in positions 1-18 to digits A=10 ... Z=35 before the mod 97-10 computation; for an all-zero base the conversion is a no-op); implementations MUST NOT use a real third-party LEI in documentation or test data. Where no LEI is allocated and the Deployer is a US entity, an Employer Identification Number (EIN) issued by the United States Internal Revenue Service or a Central Index Key (CIK) issued by the United States Securities and Exchange Commission MAY be used, expressed as the bare numeric string. Decentralized Identifiers ([W3C-DID]) MAY be used otherwise. Implementations MUST treat the value as opaque on verification; identifier resolution is out of scope for this profile.

4.1.4. payload_digest (OPTIONAL upstream, REQUIRED in this profile)

REQUIRED for Compliance Receipts. The value MUST follow the upstream object form (hash, size, optional preview) defined in Section 2.2 of [ACTA-RECEIPTS]; this profile does not redefine the wire shape. The associated payload that this digest covers MUST be retained for the period mandated by the most restrictive applicable regime in Sections 5 and 6 of this document. Implementations MUST NOT discard the underlying payload while a receipt that references it is still within its retention window.

4.1.5. action_ref (OPTIONAL upstream, REQUIRED in this profile)

REQUIRED for Compliance Receipts. The value is a SHA-256 hash of the canonical Action representation as defined in [ACTA-RECEIPTS]. This profile uses action_ref as the primary join key for cross-engine reconstruction during an audit.

4.1.6. sandbox_state (OPTIONAL upstream, REQUIRED for High-Risk in this profile)

REQUIRED for receipts produced by High-Risk AI Systems under either [EU-AI-ACT] or [COLORADO-AI-ACT]. Upstream defines sandbox_state as an OS-level containment status and restricts the value to one of enabled, disabled, or unavailable; this profile inherits that enumeration unchanged. A Deployer that operates a High-Risk AI System and produces a stream of receipts in which sandbox_state is

consistently disabled SHOULD treat that stream as a finding under the applicable risk-management documentation requirement (Article 9 of [EU-AI-ACT] for the Provider's risk management system, with which a Deployer operating per Article 26(1) is required to be consistent; Section 6-1-1703(2) of the Colorado Revised Statutes) and document the rationale in the Audit Pack metadata.

4.1.7. iteration_id (OPTIONAL upstream, REQUIRED for multi-step in this profile)

REQUIRED for multi-step agent workflows. The value MUST be stable across all receipts emitted within the same logical task or session so that a regulator can reconstruct the full chain of Actions. iteration_id is distinct from the upstream session_id field defined in [ACTA-RECEIPTS] Section 3.1.1, which is an opaque MCP session identifier. A Compliance Receipt MAY carry both: session_id for MCP-session correlation and iteration_id for logical-task correlation.

4.2. Decision Receipt Fields (type protectmcp:decision)

The decision field value MUST be allow, deny, or rate_limit. Implementations using a different internal vocabulary (e.g. permit for allow) MUST normalise on emission and on Audit Pack export.

The upstream tool_name field (REQUIRED in [ACTA-RECEIPTS] Section 3.1.1) is REQUIRED for Compliance Receipts of type protectmcp:decision.

4.2.1. reason (OPTIONAL upstream, REQUIRED for deny/rate_limit in this profile)

REQUIRED for Compliance Receipts where decision is deny or rate_limit. The value MUST be a machine-readable reason code drawn from a vocabulary documented in the Deployer's Audit Pack metadata.

4.2.2. policy_digest (OPTIONAL upstream, REQUIRED in this profile)

REQUIRED for Compliance Receipts. The value MUST be of the form sha256:<hex> and MUST reference a policy artefact that the Deployer retains for the applicable retention window. Verifiers MUST reject Compliance Receipts whose policy_digest does not resolve in the Audit Pack.

4.3. Hash-Chain Linkage (OPTIONAL upstream, REQUIRED in this profile)

Upstream Commitment Mode introduces previousReceiptHash as part of an optional extension. This profile makes the linkage REQUIRED. Implementations MUST emit a previousReceiptHash field, populated as specified by Section 5.7 of [ACTA-RECEIPTS]: the lowercase hex encoding of SHA-256(JCS(receipt)) per [RFC8785], where the receipt covered by the digest is the entire signed receipt object including the signature field. The first receipt in a chain MUST set this field to the all-zero SHA-256 value (this profile's stipulation; [ACTA-RECEIPTS] Section 5.7 specifies only the digest scope of subsequent links). JSON key is the literal previousReceiptHash (camelCase, case-sensitive); snake_case aliases MUST NOT appear on the wire.

4.4. Anchoring (No Upstream Equivalent)

[ACTA-RECEIPTS] lists Sigstore Rekor in its Implementation Status appendix as an OPTIONAL temporal anchor. This profile imposes a normative anchoring requirement.

Compliance Receipts MUST be anchored. An anchor is an [RFC3161] timestamp token covering the signed envelope, an [OPENTIMESTAMPS] commitment covering the envelope, or both; implementations SHOULD emit both forms. For both anchor types, the bytes committed are SHA-256(JCS(envelope_minus_anchors)), where envelope_minus_anchors is the wire envelope object with the anchors top-level key removed prior to canonicalization, leaving the two-key object {payload, signature}. The anchors key MUST be removed from the object, not set to null or to an empty array; these produce different JCS output and break interoperability (mirroring the upstream Section 5.6 stripping rule). The anchor thereby binds payload and signature without being self-referential. The anchor evidence MUST be retained alongside the receipt for the applicable retention window. Verifiers MUST reject Compliance Receipts that lack at least one valid anchor.

An anchor MAY be attached after issuance if the receipt is persisted with an unambiguous pending marker and the anchor lands within a documented bound. For [OPENTIMESTAMPS], this profile imposes a 7-day deadline; this is a profile-imposed bound, not a property of the OpenTimestamps protocol, whose calendar-to-block upgrade time depends on the calendar operator's publication interval. [RFC3161] tokens MUST be obtained synchronously. A verifier MUST treat a pending receipt as non-conformant once the bound elapses.

The anchor MAY cover an aggregate of receipts (for example, a Merkle root over a batch) rather than each receipt individually, provided that the inclusion proof linking the receipt to the aggregate is retained alongside the receipt and the aggregate anchor.

Where the anchor type is [RFC3161], the full TimeStampResp DER bytes MUST be retained, sufficient for offline verification by a holder with access to the TSA's published public key. Time-stamp tokens carrying ESSCertIDv2 per [RFC5816] MUST be accepted by Compliance Verifiers. Where the anchor type is [OPENTIMESTAMPS], the upgrade from the initial calendar attestation to the Bitcoin block attestation MUST be completed within the 7-day profile-imposed bound, and the upgraded proof MUST be retained for the applicable retention window per the second paragraph of this section.

4.5. Extension Fields

This profile defines two extension fields that MAY appear in the signed payload alongside the fields defined by [ACTA-RECEIPTS]. Neither field is defined upstream.

risk_class: A vocabulary term identifying the risk classification of the Action under the Deployer's risk management documentation. The vocabulary MUST be referenced in the Audit Pack metadata. Where the Deployer operates under [EU-AI-ACT], the documentation is the Provider's Article 9 risk management system as referenced via the instructions for use under Article 26(1); where the Deployer operates under [COLORADO-AI-ACT], the documentation is the Section 6-1-1703(2) risk management policy and program.

incident_class: A vocabulary term identifying the incident classification of the Action under the applicable regime: an ICT-related incident under [DORA], with classification criteria in [REG-2024-1772] and the canonical six-value reporting enumeration in Annex II data glossary, field 3.23 (Type of the incident) of [REG-2025-302] (Cybersecurity-related, Process failure, System failure, External event, Payment-related, Other (please specify)); a Cybersecurity Event under 23 NYCRR 500.1(f) (or, where the 則500.17(a) reporting threshold is met, a Cybersecurity Incident under 23 NYCRR 500.1(g)) for Covered Entities of [NYDFS-500]; a Covered Cyber Incident under [CIRCIA] once the final rule takes effect; or a security incident under 45 CFR 164.304 for Covered Entities of [HIPAA-SECURITY]. Implementations MAY refine the set, provided the flattened mapping in the Audit Pack manifest (Section 7) projects each refinement to the applicable canonical category for each in-scope regime.

risk_class MUST be encoded as a JSON string. incident_class MUST be encoded as a JSON string drawn from the canonical vocabulary referenced in the Audit Pack, OR as a JSON array of such strings to preserve cross-regime classification (for example, a single Action that is both a DORA ICT-related incident and a CIRCIA Covered Cyber Incident, or both a NYDFS Cybersecurity Incident and a CIRCIA Covered Cyber Incident). Both extension fields appear inside the signed payload object and are therefore covered by the upstream Section 5.6 signature scope. Both fields are OPTIONAL at the syntactic level but MAY be REQUIRED by the regime bindings in Sections 5 and 6 of this document.

Implementations MAY define additional extension fields. Such fields MUST NOT collide with names defined by [ACTA-RECEIPTS] or by this document. Implementations defining extension fields SHOULD register them in the registry described in Section 10.

5. European Union Bindings

5.1. EU AI Act Article 12 Binding

Each subsection cites the operative phrase of Article 12 and binds it to the receipt field that satisfies it.

5.1.1. Article 12(1), automatic recording of events

Article 12(1) requires High-Risk AI Systems to technically allow for the automatic recording of events (logs) over the lifetime of the system. The signed-receipt format provides one mechanism that satisfies that logging capability; alternative mechanisms remain valid. Where this profile is chosen, a Compliance Receipt SHOULD be produced for every Action against an external resource, and a configuration change that disables receipt generation SHOULD be recorded as a protectmcp:lifecycle Compliance Receipt. Implementations MAY emit at finer or coarser granularity so long as the log set, taken together, satisfies Article 12(2)(a) through (c).

5.1.2. Article 12(2)(a), identifying situations that may result in the high-risk AI system presenting a risk within the meaning of Article 79(1) or in a substantial modification

The combination of type, decision, reason, and policy_digest MUST be sufficient for an auditor to identify, by query alone, receipts that correspond to risk situations enumerated in the Deployer’s risk management documentation. Where the Deployer classifies an Action as risk-bearing, the receipt MUST carry a risk_class extension field.

5.1.3. Article 12(2)(b), facilitating the post-market monitoring referred to in Article 72

The hash-chain linkage required by Section 4.3 satisfies post-market monitoring traceability. The chain head MUST be made available to the Provider and to the competent authority on request.

5.1.4. Article 12(2)(c), monitoring the operation of high-risk AI systems referred to in Article 26(5)

Any change to the policy artefact referenced by policy_digest MUST produce a new digest. A change in policy_digest between two otherwise-comparable Actions may be examined by the Deployer or by a regulator as a candidate substantial-modification event under Article 43, and MUST be retained at least as long as the longest receipt in the chain that references either digest.

5.1.5. Retention

Article 12 itself sets no retention period; the operative deployer floor is Article 26(6) ("at least six months"), with the parallel provider floor in Article 19(1). Unless Union or national law sets a longer period, this profile expresses that floor as 184 days from the date of the Action: 184 is the maximum number of days in any rolling six-calendar-month window (worst case Aug-Jan, 31+30+31+30+31+31), so retention of 184 days satisfies "at least six months" regardless of the calendar months over which the window falls. Implementations that prefer the more common 183-day pick MAY use 183 days and remain conformant with Article 26(6) so long as per-receipt retention is at least six months from the Action date. Where the Deployer is also a Financial Entity, the sectoral floor in Section 5.3.4 applies.

5.2. EU AI Act Article 26 Binding

5.2.1. Article 26(1), in accordance with the instructions for use

policy_digest MUST resolve through Section 7 to a retained artefact (machine check). The Deployer SHOULD demonstrate consistency with the Provider’s instructions for use (process check). Inability to perform the machine check is presumed non-compliance.

5.2.2. Article 26(2), assign human oversight

For any Action whose decision is allow and which the Deployer's risk management documentation marks as requiring human oversight, the Deployer MUST ensure that the receipt is either reviewed by a designated natural person within the period required by national law, or that a follow-on protectmcp:lifecycle Compliance Receipt records the absence of such review with a reason code. Both records MUST themselves be Compliance Receipts. This profile addresses the trigger and record of oversight; the competence, training, authority, and necessary support of the reviewer required by Article 26(2) remain the Deployer's separate responsibility.

5.2.3. Article 26(5), monitor the operation

A Deployer MUST be able to produce an Audit Pack covering any contiguous time window since the High-Risk AI System became operational.

5.2.4. Article 26(6), keep the logs for at least six months

Compliance Receipts under this binding MUST be retained for at least the period stated in Section 5.1.5. Where the Deployer is also a Financial Entity, the longer sectoral floor in Section 5.3.4 applies.

5.3. DORA Article 17 Binding

5.3.1. Article 17(1), ICT-related incident management process

A Compliance Receipt produced inside a Financial Entity's ICT environment may serve as the canonical record of an Action that triggered an ICT-related incident. action_ref MUST be carried into the Financial Entity's incident workflow as the primary correlation key.

5.3.2. Article 17(2), record all ICT-related incidents and significant cyber threats

The hash chain required by Section 4.3 supports the recording obligation of Article 17(2) by making after-the-fact alteration of recorded incidents detectable. The Financial Entity MUST be able to produce, on request, the chain segment covering the period of an incident, together with the anchor evidence that fixes the chain to wall-clock time.

5.3.3. Article 17(3)(b), establish procedures to identify, track, log, categorise and classify ICT-related incidents

For Actions identified as part of an ICT-related incident, the producing system MUST emit incident_class. The classification criteria are those set out in Article 18(1) of [DORA], with further specification in [REG-2024-1772]. The canonical reporting enumeration to which incident_class flattens is bound by Annex II field 3.23 of [REG-2025-302] (see Section 4.5). Implementations MUST publish a flattened mapping in the Audit Pack manifest as required by Section 4.5.

5.3.4. Retention

Article 17 of [DORA] does not itself set a uniform numeric retention floor. The five-year (1827-day) figure used by this profile derives from sectoral instruments that overlap DORA-scoped Financial Entities. Investment firms keep records of all services, activities and transactions under Article 16(6) of [MIFID2], with Article 72 and Annex I of [REG-2017-565] fixing the form and content of those records. The explicit five-year retention period in [MIFID2] is set by Article 16(7) for records of telephone conversations and electronic communications, kept for a period of five years and, where requested by the competent authority, for a period of up to seven years.

Records of customer due diligence and of transactions under Article 40 of [AMLD] are kept for five years after the end of the business relationship. The AMLD record-keeping regime is superseded, in respect of record retention, by Article 77 of [AMLR] from 10 July 2027, which preserves the five-year floor and adds a case-by-case extension up to a further five years where the competent authority so requires. Implementations operating across the AMLD-to-AMLR transition MUST satisfy whichever instrument is in force on the date of the Action.

Compliance Receipts MUST be retained for the period required by applicable Union or national law; where a sectoral floor applies, retention MUST equal or exceed the longest applicable floor. Absent a more specific rule, this profile RECOMMENDS 1827 days from the date of the Action (the worst-case rolling five-calendar-year window contains two leap days, so 1827 days satisfies "five years" regardless of the calendar years over which the window falls). Anchor evidence MUST be retained for the same period. Verification keys whose lifetime expires within the retention window MUST have their public components retained so that historical signatures remain verifiable.

6. United States Bindings

6.1. NIST AI RMF Binding

[NIST-AI-RMF] is a voluntary framework. Adoption of this profile, on its own, does not establish conformity with the AI RMF; it provides a tamper-evident receipt substrate that an AI RMF program can use as evidence under the MEASURE function and as a structured input to the GOVERN, MAP, and MANAGE functions. [NIST-GENAI-PROFILE] applies the AI RMF functions to generative AI; the profile bindings below apply to generative and non-generative AI agent deployments alike unless explicitly noted.

6.1.1. GOVERN function

The GOVERN function requires that organizations document AI policies and procedures. The combination of policy_digest and the Audit Pack manifest provides a machine-readable binding between every Action and the policy artefact in force at the time of the Action. A change to the policy artefact MUST produce a new policy_digest value (per Section 4.2.2); the Audit Pack therefore records every policy change in a tamper-evident manner.

6.1.2. MAP function

The MAP function requires that the context, capabilities, and risks of an AI system be characterised. The combination of type, tool_name, action_ref, and iteration_id SHOULD be sufficient for an auditor to reconstruct the operational context of any Action without dereferencing the underlying payload.

6.1.3. MEASURE function

The MEASURE function requires that AI risks and impacts be analysed and tracked over time. The hash-chain linkage required by Section 4.3 provides tamper-evident continuity of the receipt stream over the AI system’s operational lifetime, satisfying the traceability prerequisite of MEASURE.

6.1.4. MANAGE function

The MANAGE function requires that AI risks be prioritised and acted upon based on projected impact. The risk_class extension field carries the Deployer’s risk classification of the Action; together with decision, reason, and policy_digest, it supports prioritisation and incident response without requiring the verifier to re-derive risk from the underlying payload.

6.2. Colorado AI Act (SB 24-205) Binding

[COLORADO-AI-ACT] imposes deployer obligations effective June 30, 2026 (per Senate Bill 25B-004, which postponed the original February 1, 2026 effective date). The Act regulates the deployment of High-Risk AI Systems and the prevention of algorithmic discrimination.

6.2.1. Section 6-1-1703(2), risk management policy and program

Section 6-1-1703(2) requires deployers to implement a risk management policy and program for the High-Risk AI System. policy_digest MUST resolve through Section 7 to the deployer’s risk management policy artefact in force at the time of the Action. Where the Deployer classifies an Action as risk-bearing under that policy, the receipt MUST carry a risk_class extension field.

6.2.2. Section 6-1-1703(3), impact assessment

Section 6-1-1703(3) requires deployers to complete an impact assessment annually and within 90 days after any intentional and substantial modification of the High-Risk AI System. The combination of type, policy_digest, and previousReceiptHash MUST be sufficient for an auditor to identify, by query alone, the receipts that span the period covered by an impact assessment, including any policy changes within that period.

6.2.3. Section 6-1-1703(7), notice of algorithmic discrimination

Where a Deployer determines that a High-Risk AI System has caused or is reasonably likely to have caused algorithmic discrimination, the producing system SHOULD record that determination as a protectmcp:lifecycle Compliance Receipt naming the determination, the affected receipts by action_ref, and the policy or risk-management response with a reason code.

6.3. Texas Responsible AI Governance Act (HB 149) Binding

[TEXAS-TRAIGA] takes effect January 1, 2026. The Act adopts an intent-based liability framework for the development and deployment of AI systems and provides a safe harbor at Section 552.105(e)(2)(D) of the Texas Business and Commerce Code for organisations that substantially comply with the most recent version of [NIST-GENAI-PROFILE], or another nationally or internationally recognized risk management framework for AI systems, and operate an internal review process.

6.3.1. Safe-harbor evidentiary support

Where a Deployer relies on the safe-harbor provision of HB 149 by substantially complying with [NIST-GENAI-PROFILE], the Audit Pack MAY be presented as evidence of that compliance. The bindings of Section 6.1 apply, with the additional Generative AI Profile bindings of [NIST-GENAI-PROFILE].

6.3.2. Prohibited-use detection

Receipts whose decision is deny with a reason code drawn from a vocabulary documenting the Act’s prohibited-use categories under Section 552.052 of the Texas Business and Commerce Code added by HB 149 (incitement or encouragement of physical self-harm including suicide, harm to another person, or engagement in criminal activity) MUST be retained for the period stated in Section 6.4.2 or the longer period required by Texas law, whichever is greater.

6.4. HIPAA Security Rule Binding (45 CFR Part 164, Subpart C)

[HIPAA-SECURITY] applies to Covered Entities (HIPAA) that handle electronic protected health information. The bindings below apply only to receipts whose underlying Actions reference electronic protected health information.

6.4.1. 45 CFR 164.312(b), audit controls

45 CFR 164.312(b) requires implementation of "hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information". The combination of type, action_ref, tool_name, and the hash-chain linkage required by Section 4.3 satisfies the recording requirement; the verification rules of Section 8.1 satisfy the examination requirement.

6.4.2. 45 CFR 164.316(b)(2)(i), six-year retention

45 CFR 164.316(b)(2)(i) requires that the documentation required by 45 CFR 164.316(b)(1) be retained "for 6 years from the date of its creation or the date when it last was in effect, whichever is later". This profile expresses that floor as 2192 days from the later of (a) the date of the Action and (b) the date the policy artefact referenced by policy_digest ceased to be in effect: 2192 is the maximum number of days in any rolling six-calendar-year window (worst case spans two leap days, e.g. 2024-2030 contains February 29 of 2024 and 2028, yielding 6*365+2 = 2192 days). Verification keys whose lifetime expires within the retention window MUST have their public components retained so that historical signatures remain verifiable.

6.5. NYDFS Cybersecurity Regulation Binding (23 NYCRR Part 500)

[NYDFS-500] applies to Covered Entities (NYDFS) operating under New York Banking, Insurance, or Financial Services Law. The bindings below apply only to receipts produced by such Covered Entities.

6.5.1. 23 NYCRR 500.6, audit trail

23 NYCRR 500.6(a) requires Covered Entities to securely maintain systems that, to the extent applicable and based on its risk assessment, (1) are designed to reconstruct material financial transactions, and (2) include audit trails designed to detect and respond to cybersecurity events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity. The hash chain required by Section 4.3 together with the anchor evidence required by Section 4.4 satisfies the tamper-evidence prerequisite of the audit-trail obligation.

6.5.2. 23 NYCRR 500.17, notices to superintendent

23 NYCRR 500.17(a)(1) requires that "Each covered entity shall notify the superintendent electronically in the form set forth on the department’s website as promptly as possible but in no event later than 72 hours after determining that a cybersecurity incident has occurred at the covered entity, its affiliates, or a third-party service provider." The reporting trigger is a Cybersecurity Incident under 23 NYCRR 500.1(g), not any Cybersecurity Event under 500.1(f). For Actions identified as part of such an Incident, the producing system MUST emit incident_class with a value indicating Cybersecurity Incident under 23 NYCRR 500.1(g), and the Covered Entity MUST be able to produce, on request, the chain segment covering the period of the Incident together with the anchor evidence that fixes the chain to wall-clock time.

6.5.3. 23 NYCRR 500.6 retention

23 NYCRR 500.6(b) requires that "Each Covered Entity shall maintain records required by this section for not fewer than five years." The five-year floor applies uniformly to records required by paragraph (a)(1) (designed to reconstruct material financial transactions) and to records required by paragraph (a)(2) (audit trails designed to detect and respond to cybersecurity events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity). Compliance Receipts produced under this binding MUST be retained for at least 1827 days from the date of the Action (the worst-case rolling five-calendar-year window contains two leap days).

6.6. SEC Broker-Dealer Recordkeeping Binding (17 CFR 240.17a-4)

[SEC-17A-4] applies to Broker-Dealers, Security-Based Swap Dealers, and Major Security-Based Swap Participants. The bindings below apply only to receipts produced inside such entities.

6.6.1. 17 CFR 240.17a-4(f), electronic recordkeeping system

The November 3, 2022 amendments to 17 CFR 240.17a-4 (compliance date May 3, 2023) added an audit-trail alternative to the prior write-once-read-many (WORM) electronic recordkeeping requirement. The audit-trail alternative requires that the electronic recordkeeping system permit the recreation of an original record if it is modified or deleted. The hash-chain linkage required by Section 4.3 together with the retention rule in Section 6.6.2 and the anchor evidence required by Section 4.4 satisfies the audit-trail alternative when the Compliance Receipt is the system-of-record for a regulated record.

6.6.2. 17 CFR 240.17a-4(a) and (b) retention

17 CFR 240.17a-4(a) requires preservation of certain records for not less than 6 years, the first two years in an easily accessible place. 17 CFR 240.17a-4(b) requires preservation of a different list of records for not less than three years, the first two years in an easily accessible place. Compliance Receipts that constitute or support a record listed in 17 CFR 240.17a-4(a) MUST be retained for at least 2192 days from the date of the Action, applying the same six-year worst-case methodology as Section 6.4.2; receipts that constitute or support a record listed only in 17 CFR 240.17a-4(b) MUST be retained for at least 1096 days from the date of the Action (the worst-case rolling three-calendar-year window contains one leap day). Where both apply, the longer period applies.

6.7. CIRCIA Binding (Cyber Incident Reporting for Critical Infrastructure Act of 2022)

[CIRCIA] requires Covered Entities (CIRCIA) to report Covered Cyber Incidents to the Cybersecurity and Infrastructure Security Agency within 72 hours of reasonable belief that the incident has occurred, and to report ransom payments within 24 hours. The reporting obligations take effect upon publication of the final rule. Pending publication, the bindings below apply on a voluntary basis.

6.7.1. Covered Cyber Incident reporting support

For Actions identified as part of a Covered Cyber Incident, the producing system MUST emit incident_class with a value indicating Covered Cyber Incident under [CIRCIA]. The Covered Entity MUST be able to produce, on request, the chain segment covering the period of the incident together with the anchor evidence that fixes the chain to wall-clock time.

6.7.2. Records related to a Covered Cyber Incident report

Section 2242(a)(4) of the Homeland Security Act of 2002, as enacted by [CIRCIA] and codified at 6 U.S.C. 681b(a)(4), requires Covered Entities to preserve data relevant to a Covered Cyber Incident or ransom payment in accordance with procedures established in the final rule. CISA's notice of proposed rulemaking at 89 FR 23644 (April 4, 2024) proposes a preservation period of not less than two years; this profile uses that proposed floor pending publication of the final rule. Compliance Receipts that are referenced in a CIRCIA report or that the Covered Entity reasonably anticipates will be so referenced MUST be retained for the longer of the period established by the final rule and 731 days from the date of the Action (2*365+1 leap day worst case).

7. Audit Pack Composition

This section is informative. It describes the contents of an Audit Pack as introduced in Section 2.

An Audit Pack contains the following items.

* The set of Compliance Receipts covered by the requested time window, in the canonical envelope form defined by [ACTA-RECEIPTS].

* The chain commitments that link the receipts: for each receipt, the value of previousReceiptHash and the recomputed digest of the predecessor envelope.

* The anchor evidence: [RFC3161] tokens, OpenTimestamps proofs, or both. Each anchor item MUST be associated, by hash, with the receipt or aggregate it covers.

* The trust anchor metadata that identifies the Deployer or other regulated entity associated with each issuer_id value.

* The verification key material for every kid value present, in a form that does not require online retrieval.

* Vocabularies referenced by reason, risk_class, incident_class, and extension fields, embedded as JSON arrays with a stable identifier. The Audit Pack MUST expose a digest-resolution facility that, given a policy_digest, returns the retained artefact.

* A regime mapping document that names which receipts the producer asserts as evidence under any of the regimes addressed by Sections 5 and 6 of this document (EU AI Act Article 12, EU AI Act Article 26, DORA Article 17, NIST AI RMF, Colorado AI Act, Texas Responsible AI Governance Act, NYDFS Part 500, HIPAA Security Rule, SEC Rule 17a-4, CIRCIA).

* The chain heads valid at the start and end of the time window, signed by the Deployer or other regulated entity.

An Audit Pack MUST itself be signed per the [ACTA-RECEIPTS] algorithm registry. The manifest MUST include bundle_digest, bundle_signature, bundle_public_key, and algorithm_registry_version.

8. Verifier Behaviour

A verifier conformant to this profile is referred to as a Compliance Verifier.

8.1. Mandatory Checks

A Compliance Verifier MUST perform all of the following checks before treating a receipt as a Compliance Receipt.

* Verify the signature using the algorithm declared in signature.alg, in accordance with [ACTA-RECEIPTS].

* Resolve the verification key through one of the key-distribution mechanisms described in Section 4.3 of [ACTA-RECEIPTS] (well-known JWK Set or out-of-band distribution), or through Audit Pack trust-anchor metadata. The verifier MUST NOT trust a verification key embedded in the receipt envelope.

* Verify that all fields marked REQUIRED by Section 4 are present and well-formed.

* Verify the hash-chain linkage by recomputing the digest of the immediately preceding envelope and comparing it to previousReceiptHash.

* Verify at least one anchor: an [RFC3161] token, an [OPENTIMESTAMPS] commitment, or both. The anchor MUST cover the signed envelope as it appears in the receipt. The verifier MUST cryptographically re-verify the anchor against the signed envelope; presence of anchor metadata without a successful cryptographic check MUST NOT yield "valid".

* Verify the future-skew bound on issued_at per Section 4.1.2. Past skew MUST NOT cause non-conformance when the receipt is within retention.

* Verify that policy_digest resolves through Section 7. A digest computed over a nonced or otherwise mixed-input form (for example, SHA-256(nonce || JCS(artefact))) MUST NOT be treated as policy_digest; the digest scope is the canonical form of the artefact alone. The verifier MUST recompute SHA-256 over the canonical form of the resolved artefact as documented in the Audit Pack manifest, and compare; for JSON artefacts the canonical form is JCS per [RFC8785].

A receipt that fails any of these checks MUST be reported as non-conformant.

8.2. Optional Checks

A Compliance Verifier MAY additionally perform any of the following.

* Cross-check the issuer_id against an external registry (LEI, EIN, CIK, NPI, GLEIF, or a Deployer-published list).

* Resolve the policy artefact referenced by policy_digest and compare it to a Provider-supplied or Deployer-supplied reference policy.

* Recompute the chain head and compare it to a Deployer-published value.

* Validate incident_class (each element if encoded as an array) and risk_class extension values against the vocabularies referenced in the Audit Pack.

8.3. Reporting

A Compliance Verifier SHOULD produce a structured report that identifies, for each receipt verified, which regime bindings it satisfies, drawn from the regimes listed in Section 7. The report SHOULD itself be signed using the same algorithm registry as [ACTA-RECEIPTS].

9. Security Considerations

This profile inherits all of the security considerations of [ACTA-RECEIPTS]. The following considerations are specific to the compliance binding.

9.1. Tamper Resistance

The hash-chain linkage required by Section 4.3 provides tamper-evidence at the chain level. An adversary who removes a receipt from the middle of the chain MUST recompute and re-sign every subsequent envelope. The anchor evidence required by Section 4.4 binds segments of the chain to wall-clock time, raising the cost of a re-signing attack.

Implementations SHOULD anchor at intervals no longer than 24 hours. Implementations operating under DORA Article 17, 23 NYCRR 500.17, or [CIRCIA] SHOULD anchor at intervals no longer than one hour, given the 72-hour reporting deadlines of those regimes.

A deployment that uses only the signature, without chain linkage and anchoring, can be rolled back by an insider with control of the signing key for the period between the deletion and the next anchor. The MUST clauses of Section 4.3 and Section 4.4 close that window.

9.2. Key Compromise

A Compliance Receipt is only as trustworthy as the key that signed it. On suspected compromise of an issuer key, the Deployer MUST publish a revocation notice that names the key, the time of suspected compromise, and the chain head at that time. Receipts signed by the compromised key after the named time MUST NOT be treated as Compliance Receipts.

Verifiers MUST consult revocation metadata supplied with the Audit Pack and MUST reject Compliance Receipts whose signing key was revoked at or before issued_at.

9.3. Retention and Long-Term Verifiability

The longest retention floor in this profile is 2192 days (six calendar years), set by Section 6.4 and Section 6.6; the EU side has a parallel five-year (1827-day) floor under Section 5.3. Both exceed the typical operational crypto-period of a signing key under recommended key-management practice. Implementations SHOULD use ML-DSA-65 from the [ACTA-RECEIPTS] algorithm registry ([FIPS204]) for receipts expected to be verified after the cryptographic lifetime of classical signature schemes ends. Implementations MUST retain public

key material for the entire retention window.

9.4. Privacy

[ACTA-RECEIPTS] prohibits the inclusion of raw prompts, tool arguments, and credentials in the signed payload. This profile extends that prohibition to the extension fields defined in this document. The risk_class and incident_class values MUST be drawn from controlled vocabularies and MUST NOT carry free-text personal data.

Where the underlying Action references a data subject, the payload_digest field MUST cover the data; the data itself MUST be held in a separate store that respects the data subject's rights under applicable law (including but not limited to the General Data Protection Regulation for EU data subjects, the California Consumer Privacy Act and Virginia Consumer Data Protection Act for the corresponding US states, and the HIPAA Privacy Rule where electronic protected health information is involved). A request for erasure that is granted under applicable data protection law MUST be reflected by deletion of the referenced payload, not by deletion of the receipt; the receipt remains as evidence that an Action occurred and was governed by a named policy at a named time.

9.5. Anchor Trust

The trust assumptions of an anchor depend on the anchor type. [RFC3161] timestamp tokens depend on the trust placed in the named Time Stamping Authority. OpenTimestamps commitments depend on the inclusion of the commitment in a public Bitcoin block. A Compliance Verifier SHOULD treat the simultaneous presence of both anchor types as stronger evidence than the presence of only one.

9.6. Replay

A Compliance Receipt is bound to a single Action via action_ref. Replay of a Compliance Receipt against a different Action is detectable by action_ref mismatch. The 300-second issued_at skew bound stated in Section 4.1.2 limits the window in which a freshly-replayed receipt can be presented as recent.

Where the verifier supports it, two receipts sharing action_ref and issuer_id SHOULD be flagged as a candidate duplicate-emission event for human review. This profile does not require verifiers to maintain a cross-receipt index; deployers needing duplicate-emission detection should arrange it at the Audit Pack production layer.

9.7. Cross-Regime Conflict

Where the same Action is in scope of more than one regime addressed by this document, the producing system MUST satisfy the union of the applicable requirements. Where a SHOULD clause in one regime conflicts with a MUST clause in another, the MUST clause prevails. Where two MUST clauses conflict, the producing system MUST refuse to issue the receipt and MUST log the refusal as a protectmcp:lifecycle Compliance Receipt.

9.8. Algorithm Agility

This profile inherits its algorithm registry from [ACTA-RECEIPTS]. Implementations MUST treat the verification of a historical receipt according to the algorithm registry that was in force at issued_at, not the registry in force at the time of verification, provided that the signing key was not revoked.

10. IANA Considerations

This document requests two new IANA registries to support stable, machine-checkable extensions to the Compliance Receipt format.

10.1. Compliance Receipt Extension Fields Registry

IANA is requested to create a new registry titled "Compliance Receipt Extension Fields" under a new "Compliance Receipts" registry group.

This registry covers both signed-payload fields and envelope-level fields (siblings of payload and signature); each entry’s Description identifies which.

Each entry contains:

* Field Name: a JSON object key, lowercase ASCII letters, digits, and underscore.
* Description: a one-line summary of the field’s purpose.
* Reference: the document that defines the field’s semantics.
* Vocabulary: a URL or registry pointer for the controlled vocabulary that field values are drawn from, or "free-form" if none.

The registration policy is Specification Required, per [RFC8126]. The Designated Expert(s) SHOULD verify that the field name does not collide with any field defined by [ACTA-RECEIPTS], that the Reference

is a stable, dereferenceable specification, and that the Vocabulary is documented sufficiently for an independent verifier to validate values.

Initial registry contents:

* risk_class - Risk classification term under the Deployer’s risk management documentation - This document - Vocabulary referenced in Audit Pack metadata.

* incident_class - Incident classification term spanning DORA Article 18(1) (with further specification in [REG-2024-1772] and the canonical six-value enumeration in Annex II field 3.23 of [REG-2025-302]), 23 NYCRR 500.1 Cybersecurity Event/Incident, [CIRCIA] Covered Cyber Incident, and HIPAA security incident under 45 CFR 164.304 - This document - Audit Pack metadata.

* anchors - Envelope-level array of timestamp / transparency-log anchors covering the signed envelope; entries carry a type discriminator (rfc3161 or opentimestamps) and a value field - This document - Anchor type vocabulary: rfc3161 per [RFC3161], opentimestamps per [OPENTIMESTAMPS].

10.2. Compliance Receipt Type Namespaces Registry

IANA is requested to create a new registry titled "Compliance Receipt Type Namespaces" under the same "Compliance Receipts" registry group.

Each entry contains:

* Namespace: a colon-separated identifier prefix used as a value of the type field, lowercase ASCII letters, digits, hyphen, underscore, and colon.

* Description: a one-line summary of the receipt category.

* Reference: the document that defines the namespace.

The registration policy is Specification Required, per [RFC8126]. The Designated Expert(s) SHOULD verify that the namespace does not collide with any namespace already registered or any namespace reserved by [ACTA-RECEIPTS], and that the Reference is a stable specification.

Initial registry contents:

* protectmcp:decision - A receipt recording a policy evaluation outcome (allow, deny, rate_limit) for an MCP-mediated tool call - This document.

* protectmcp:restraint - A receipt recording the application or release of a restraint on an agent (e.g., quota, rate limit, sandbox tightening) - This document.

* protectmcp:lifecycle - A receipt recording an agent or system lifecycle event (e.g., configuration change, key rotation, oversight review) - This document.

11. Acknowledgements

The author thanks Tom Farley for [ACTA-RECEIPTS], on which this profile is built. This profile would not exist without the field catalogue and envelope structure that the upstream draft defines. The author also thanks the Asqav community for review of early drafts.

12. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8032] Josefsson, S. and I. Liusvaara, "Edwards-Curve Digital Signature Algorithm (EdDSA)", RFC 8032, DOI 10.17487/RFC8032, January 2017, <https://www.rfc-editor.org/info/rfc8032>.

[RFC7518] Jones, M., "JSON Web Algorithms (JWA)", RFC 7518, DOI 10.17487/RFC7518, May 2015, <https://www.rfc-editor.org/info/rfc7518>.

[FIPS204] National Institute of Standards and Technology, "Module-Lattice-Based Digital Signature Standard", FIPS 204, DOI 10.6028/NIST.FIPS.204, 13 August 2024, <https://csrc.nist.gov/pubs/fips/204/final>.

[RFC5816] Santesson, S. and N. Pope, "ESSCertIDv2 Update for RFC 3161", RFC 5816, DOI 10.17487/RFC5816, April 2010, <https://www.rfc-editor.org/info/rfc5816>.

[RFC3161] Adams, C., Cain, P., Pinkas, D., and R. Zuccherato, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)", RFC 3161, DOI 10.17487/RFC3161, August 2001, <https://www.rfc-editor.org/info/rfc3161>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[OPENTIMESTAMPS] OpenTimestamps, "OpenTimestamps Server", September 2016, <https://github.com/opentimestamps/opentimestamps-server>.

[ACTA-RECEIPTS] Farley, T., "Signed Decision Receipts for Machine-to-Machine Access Control", Work in Progress, Internet-Draft, draft-farley-acta-signed-receipts-01, 25 April 2026, <https://datatracker.ietf.org/doc/html/draft-farley-acta-signed-receipts-01>.

[RFC8785] Rundgren, A., Jordan, B., and S. Erdtman, "JSON Canonicalization Scheme (JCS)", RFC 8785, DOI 10.17487/RFC8785, June 2020, <https://www.rfc-editor.org/info/rfc8785>.

[ISO17442] ISO, "Financial services - Legal entity identifier (LEI) - Part 1: Assignment", ISO 17442-1:2020, August 2020, <https://www.iso.org/standard/78829.html>.

[W3C-DID] W3C, "Decentralized Identifiers (DIDs) v1.0", 19 July 2022, <https://www.w3.org/TR/did-1.0/>.

13. Informative References

[EU-AI-ACT] European Parliament and Council, "Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance)", 12 July 2024, <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>.

[DORA] European Parliament and Council, "Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance)", 27 December 2022, <https://eur-lex.europa.eu/eli/reg/2022/2554/oj>.

[REG-2025-302] European Commission, "Commission Implementing Regulation (EU) 2025/302 of 23 October 2024 laying down implementing technical standards for the application of Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to the standard forms, templates, and procedures for financial entities to report a major ICT-related incident and to notify a significant cyber threat (Text with EEA relevance)", 20 February 2025, <https://eur-lex.europa.eu/eli/reg_impl/2025/302/oj>.

[REG-2024-1772] European Commission, "Commission Delegated Regulation (EU) 2024/1772 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the criteria for the classification of ICT-related incidents and cyber threats, setting out materiality thresholds and specifying the details of reports of major incidents (Text with EEA relevance)", 25 June 2024, <https://eur-lex.europa.eu/eli/reg_del/2024/1772/oj>.

[MIFID2] European Parliament and Council, "Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (recast) (Text with EEA relevance)", 12 June 2014, <https://eur-lex.europa.eu/eli/dir/2014/65/oj>.

[REG-2017-565] European Commission, "Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive (Text with EEA relevance)", 31 March 2017, <https://eur-lex.europa.eu/eli/reg_del/2017/565/oj>.

[AMLD] European Parliament and Council, "Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance)", 5 June 2015, <https://eur-lex.europa.eu/eli/dir/2015/849/oj>.

[AMLR] European Parliament and Council, "Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (Text with EEA relevance)", 19 June 2024, <https://eur-lex.europa.eu/eli/reg/2024/1624/oj>.

[NIST-AI-RMF] National Institute of Standards and Technology, "Artificial Intelligence Risk Management Framework (AI RMF 1.0)", NIST AI 100-1, DOI 10.6028/NIST.AI.100-1, 26 January 2023, <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>.

[NIST-GENAI-PROFILE] National Institute of Standards and Technology, "Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile", NIST AI 600-1, DOI 10.6028/NIST.AI.600-1, 26 July 2024, <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf>.

[COLORADO-AI-ACT] State of Colorado, Seventy-Fourth General Assembly, "Senate Bill 24-205, Consumer Protections for Artificial Intelligence", 17 May 2024, <https://leg.colorado.gov/bills/sb24-205>.

[TEXAS-TRAIGA] State of Texas, 89th Legislature, Regular Session, "House Bill 149, Texas Responsible Artificial Intelligence Governance Act", 22 June 2025, <https://capitol.texas.gov/BillLookup/History.aspx?LegSess=89R&Bill=HB149>.

[HIPAA-SECURITY] United States Department of Health and Human Services, "HIPAA Security Rule, 45 CFR Part 164, Subpart C, Security

Standards for the Protection of Electronic Protected Health Information", 20 February 2003, <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164>.

[NYDFS-500] New York State Department of Financial Services, "23 NYCRR Part 500, Cybersecurity Requirements for Financial Services Companies", 1 March 2017, <https://www.dfs.ny.gov/industry-guidance/cybersecurity>.

[SEC-17A-4] United States Securities and Exchange Commission, "Electronic Recordkeeping Requirements for Broker-Dealers, Security-Based Swap Dealers, and Major Security-Based Swap Participants (Rule 17a-4 Amendments)", 3 November 2022, <https://www.federalregister.gov/documents/2022/11/03/2022-22670/electronic-recordkeeping-requirements-for-broker-dealers-security-based-swap-dealers-and-major>. Effective date January 3, 2023; compliance date for amendments to 17 CFR 240.17a-4 May 3, 2023.

[CIRCIA] United States Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)", 15 March 2022, <https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia>.

Worked Example (Informative)

This appendix illustrates a Compliance Receipt that satisfies the EU AI Act Article 26 binding for a tool invocation by a High-Risk AI System deployed by a Financial Entity. The wire shape applies identically to United States bindings; the only differences are the values placed in issuer_id (LEI, EIN, or CIK depending on the regime) and in the risk_class and incident_class vocabularies referenced in the Audit Pack manifest. Field values are abbreviated for readability and are not cryptographically valid. The example shows a mid-chain receipt; a chain-genesis receipt would carry a previousReceiptHash of 64 zero hex characters per Section 4.3.

```
   {
     "payload": {
       "type": "protectmcp:decision",
       "issued_at": "2026-05-04T09:14:22.118Z",
       "issuer_id": "00000000000000000098",
       "action_ref": "c1f3a09a4d2e7f6b8c5a91e3d7b04f2a1c8e6f5d3b9a7c2e4f8d6b1a3c5e7f9d",
       "tool_name": "deploy",
       "iteration_id": "task-2026-05-04-01a3",
       "decision": "allow",
       "reason": "policy:within_limits",
       "policy_digest": "sha256:7b214e8c3d9f4a2b1e6c8f5a3d7b9e2c4f6a8d1b3e5c7f9a2d4b6e8c1
f3a5d7b",
       "sandbox_state": "enabled",
       "payload_digest": {
         "hash": "0a44d2c8e3f5b7a9d1c4e6f8b2a5d7c9e1f3b5a7d9c2e4f6b8a1d3c5e7f9b2a4",
         "size": 1024
       },
       "previousReceiptHash": "f80c11a3b5d7e9c2f4a6b8d1e3c5f7a9b2d4e6c8f1a3b5d7e9c2f4a6b8
d1e3c5",
       "risk_class": "deployer:financial:medium"
     },
     "signature": {
       "alg": "EdDSA",
       "kid": "00000000000000000098",
       "sig": "..."
     },
     "anchors": [
       {
         "type": "rfc3161",
         "value": "..."
       },
       {
         "type": "opentimestamps",
         "value": "..."
       }
     ]
   }
```


The above receipt satisfies the Article 26 binding because:

* issuer_id is a 20-character ISO 17442 Legal Entity Identifier (LEI) that resolves through the trust anchor metadata in the Audit Pack to the named Deployer;

* policy_digest resolves to a retained policy artefact;

* sandbox_state is enabled, satisfying the High-Risk system constraint of Section 4.1.6;

* previousReceiptHash links the receipt into the chain per Section 4.3;

* both an [RFC3161] anchor and an [OPENTIMESTAMPS] anchor are present per Section 4.4.

Under the DORA Article 17 binding a Compliance Verifier additionally checks the longest applicable sectoral retention floor (1827 days as the default, per Section 5.3.4) and, where present, that incident_class flattens to the canonical six-value vocabulary referenced in Section 4.5. Under the United States bindings of Section 6 the same verifier additionally checks the longest applicable retention floor (2192 days as the default for receipts under Section 6.4 or Section 6.6) and, where the Deployer is a NYDFS Covered Entity, a HIPAA Covered Entity, or a CIRCIA Covered Entity, that incident_class resolves to the applicable canonical category for each in-scope regime.

Change Log

draft-marques-asqav-compliance-receipts-03

Multi-jurisdiction consolidation. The European Union profile (formerly the only profile in -02) and the United States profile (formerly the separate draft draft-marques-asqav-us-compliance-receipts-00) are merged into a single document with two regional bindings sections: Section 5 (European Union) and Section 6 (United States). Sections 1 through 4 (Introduction, Conventions, Relationship to upstream, Receipt Field Profile) and Sections 7 through 11 (Audit Pack, Verifier, Security, IANA, Acknowledgements) are shared across both regimes. Conventions terms that differ across regimes are now disambiguated with regime suffixes (Deployer (EU AI Act) vs Deployer (Colorado AI Act); High-Risk AI System (EU AI Act) vs High-Risk AI System (Colorado AI Act)). The incident_class extension field now lists every applicable canonical category in one place: ICT-related incident under [DORA] with the Annex II reporting enumeration, Cybersecurity Event/Incident under [NYDFS-500], Covered Cyber Incident under [CIRCIA], and security incident under [HIPAA-SECURITY]. The issuer_id rule now permits EIN or CIK as alternatives to LEI for US Deployers without an allocated LEI. The Tamper Resistance security consideration extends the one-hour anchoring SHOULD to NYDFS 500.17 and CIRCIA in addition to DORA Article 17. The Privacy security consideration extends to GDPR for EU data subjects and CCPA / VCDPA / HIPAA Privacy Rule for US data subjects. The Worked Example notes that the wire shape applies identically to US bindings, with only the issuer_id identifier and the vocabularies differing. IANA registries are unchanged; the Initial registry contents for incident_class now describe the multi-

regime category set. No changes to the wire format, the field profile, the hash chain, the anchoring rules, the Audit Pack contents, or the Verifier checks. Section 4.1.6 (sandbox_state) and Section 4.5 (risk_class) corrected to attribute the EU risk-management documentation requirement to Article 9 of [EU-AI-ACT] (Provider's risk management system) rather than Article 26, with Article 26(1) cited as the deployer's instructions-for-use obligation that links to the Provider's Article 9 documentation. Section 6.5.3 (nydfs-retention) corrected to a single-tier five-year floor under 23 NYCRR 500.6(b) (verified verbatim against LII Cornell); the prior tiered 5-year/3-year split (claimed against the DFS Second Amendment) was incorrect because the Second Amendment does not amend 則500.6, leaving the 2017 single-tier text in force. The 1096-day three-year audit-trail floor previously stated for NYDFS is removed.

draft-marques-asqav-compliance-receipts-02

Submission-ready EU-only profile. Wire-shape alignment with upstream [ACTA-RECEIPTS] (payload/signature/anchors envelope; payload_digest object form; tool_name REQUIRED for protectmcp:decision; issuer_id equals kid). EU AI Act and DORA bindings authored against Official Journal text. Anchor MUST (at least one of RFC 3161 or OpenTimestamps); both RECOMMENDED; 7-day OpenTimestamps upgrade deadline profile-imposed. Six-month AI Act floor expressed as 184 days; DORA-bound default expressed as 1827 days. IANA registries created.

draft-marques-asqav-compliance-receipts-01

Initial wire-shape alignment with upstream and addition of dual-anchor, hash-chain, retention, and DORA classification bindings. Subsequent revisions superseded the specific values introduced here.

draft-marques-asqav-compliance-receipts-00

Initial version. Defines a profile of [ACTA-RECEIPTS] that binds receipt fields to EU AI Act Article 12, EU AI Act Article 26, and DORA Article 17.

Author's Address

Joao Andre Gomes Marques
Asqav
Portugal
Email: joaoagm90@gmail.com