

SCITT Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: November 25, 2026

V. Dawkins  
LedgerProof Foundation  
May 25, 2026

A SCITT Profile for EU AI Act Article 50 Transparency Receipts  
draft-dawkins-scitt-ai-article50-00

## Abstract

This document defines a Supply Chain Integrity, Transparency, and Trust (SCITT) profile for machine-readable cryptographic transparency receipts addressing all four sub-obligations of Article 50 of Regulation (EU) 2024/1689 (the "EU AI Act"): interactive AI system disclosure (50(1)), machine-readable marking of synthetic media (50(2)), emotion recognition notification (50(3), referenced for completeness), and AI-generated text disclosure with human editorial review exemption (50(4)).

The profile defines three SCITT statement content types ("ai/article-50/v1", "ai/human-review/v1", and "ai/chatbot-session/v1") and specifies validation, verification, and chain-of-custody semantics suitable for presentation to European Union supervisory authorities, national competent authorities, and judicial proceedings.

The profile is substrate-agnostic but presumes a SCITT Transparency Service backed by a publicly verifiable append-only log. A reference implementation using the Bitcoin blockchain as the SCITT log substrate, via RFC 6962 Merkle aggregation anchored in OP\_RETURN transactions, is described in companion document draft-dawkins-scitt-lpr-00.

## 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 November 25, 2026.

## Copyright Notice

Copyright (c) 2026 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

## Table of Contents

1. Introduction . . . . .	2
1.1. Motivation . . . . .	2
1.2. Article 50 Sub-Obligations . . . . .	3
1.3. Relationship to Other Standards . . . . .	3
2. Conventions and Definitions . . . . .	4
3. Profile Statement Content Types . . . . .	4
3.1. ai/article-50/v1 (Synthetic Content Receipt) . . . . .	4
3.2. ai/human-review/v1 (Editorial Review Receipt) . . . . .	6
3.3. ai/chatbot-session/v1 (Interactive AI Receipt) . . . . .	7
4. Validation and Verification . . . . .	8
4.1. Issuance Validation . . . . .	8
4.2. Article 50 Conformance Verification . . . . .	9
4.3. Article 50 Defensibility Verification . . . . .	9
5. Privacy Considerations . . . . .	10
5.1. GDPR Article 17 (Right to Erasure) . . . . .	10
5.2. Prohibited Identifier Classes . . . . .	10
6. Security Considerations . . . . .	11
7. IANA Considerations . . . . .	11
8. References . . . . .	12

## 1. Introduction

## 1.1. Motivation

Article 50 of Regulation (EU) 2024/1689 (the EU AI Act) imposes transparency obligations on providers and deployers of AI systems in four distinct sub-areas. Article 50(2) specifically requires that synthetic content be marked in "machine-readable format" that is "effective, interoperable, robust and reliable." As of the publication date of this draft, no IETF-standardized profile provides a complete, cryptographically verifiable, machine-readable record covering all four sub-obligations.

This profile fills that gap. It defines three SCITT statement types that together provide:

- o Cryptographic proof that an AI system generated specific content, attributable to a named legal entity (the deployer);
- o Cryptographic proof that a human reviewed AI-generated text, enabling the Article 50(4) editorial review exemption;
- o Cryptographic proof that a user was notified of interaction with an AI system, addressing Article 50(1).

The profile leverages the SCITT architecture's existing properties of append-only logging, independent verifiability, and global uniqueness of registered statements. It is substrate-agnostic with respect to the Transparency Service implementation.

## 1.2. Article 50 Sub-Obligations

Article 50 of the EU AI Act contains four distinct transparency obligations:

- o Article 50(1): Providers of AI systems intended to interact directly with natural persons shall ensure that natural persons are informed they are interacting with an AI system, unless this is obvious to a reasonably well-informed natural person.
- o Article 50(2): Providers of AI systems generating synthetic audio, image, video, or text content shall ensure that outputs are marked in a machine-readable format and detectable as artificially generated or manipulated. Solutions shall be effective, interoperable, robust and reliable as far as is technically feasible.
- o Article 50(3): Deployers of emotion recognition systems or biometric categorization systems shall inform natural persons exposed to such systems.
- o Article 50(4): Deployers of AI systems generating or manipulating text published with the purpose of informing the public on matters of public interest shall disclose that the text has been artificially generated or manipulated, unless the AI-generated content has undergone a process of human review or editorial control and where a natural or legal person holds editorial responsibility for the publication.

This profile addresses Article 50(1), 50(2), and 50(4) directly. Article 50(3) is intentionally out of scope: biometric data on a public transparency log raises GDPR Article 9 (special category data) concerns that require a Data Processing Agreement out of scope of this profile.

### 1.3. Relationship to Other Standards

This profile is complementary to, not competitive with, the Coalition for Content Provenance and Authenticity (C2PA) Content Credentials specification [C2PA]. C2PA defines a manifest format embedded in media files; this profile defines a SCITT statement that may be referenced from a C2PA assertion and that persists independently of the file, surviving metadata stripping or transcoding.

A C2PA-to-SCITT mapping is provided in Appendix A. The mapping permits a C2PA-compliant tool to additionally register a SCITT statement under this profile, providing tamper-evidence properties that the C2PA manifest alone does not provide.

This profile is also compatible with the eIDAS Regulation (EU) No 910/2014 framework for qualified electronic seals. A SCITT statement issued under this profile MAY be presented in conjunction with a qualified electronic seal where the issuer is a qualified trust service provider.

## 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.

AI System: As defined in Article 3(1) of Regulation (EU) 2024/1689.

Deployer: As defined in Article 3(4) of Regulation (EU) 2024/1689. A natural or legal person using an AI system under its authority in the course of a professional activity.

Provider: As defined in Article 3(3) of Regulation (EU) 2024/1689.

Article 50 Conformant Receipt: A SCITT statement conforming to one of the content types defined in Section 3 of this profile, having passed the validation steps in Section 4.

Article 50 Defensible Receipt: An Article 50 Conformant Receipt that additionally satisfies the defensibility criteria in Section 4.3, suitable for evidentiary use in adversarial proceedings.

Public Interest Content: Content of the kind described in Article 50(4) — text published with the purpose of informing the public on matters of public interest. The determination is made by the deployer at issuance time and is recorded in the receipt.

### 3. Profile Statement Content Types

#### 3.1. ai/article-50/v1 (Synthetic Content Receipt)

The content type "ai/article-50/v1" is the primary statement type for Article 50(2) and Article 50(4) compliance. It records the binding of synthetic content to its generating AI system and the legal entity that caused the content to be generated.

The content payload is a JSON object with the following fields:

ai\_system\_id (string, REQUIRED)

Identifier of the AI system that produced the artifact. SHOULD follow the format "<provider>/<model>/<version>", e.g., "openai/gpt-4o/2024-11-20". A URL resolving to a model card or a Decentralized Identifier (DID) MAY be used. Maximum 512 octets.

ai\_system\_version (string, OPTIONAL)

Additional version identifier when ai\_system\_id alone is insufficient (e.g., fine-tuned variants).

Dawkins

Expires November 25, 2026

[Page 4]

Internet-Draft

SCITT AI Article 50 Profile

May 2026

deployer\_id (string, REQUIRED)

Legal entity identifier of the deployer. MUST be a legal-entity identifier (LEI, EUID, VAT number, or DID). MUST NOT be a natural-person identifier such as an email address or personal name. This requirement prevents inadvertent processing of personal data under GDPR Article 6 lawful basis requirements.

deployer\_name (string, REQUIRED)

Human-readable legal name of the deployer organization.

deployer\_country (string, REQUIRED)

ISO 3166-1 alpha-2 country code of the deployer's registered

office. Exactly two uppercase ASCII letters.

content\_category (enum, REQUIRED)

Category of synthetic content. MUST be one of:

"SYNTHETIC\_TEXT", "SYNTHETIC\_IMAGE", "SYNTHETIC\_AUDIO",  
"SYNTHETIC\_VIDEO", "DEEPFAKE", "SYNTHETIC\_MULTIMODAL", or  
"AI\_ASSISTED\_DOCUMENT".

artifact\_hash (string, REQUIRED)

SHA-256 hash of the artifact, hex-encoded in lowercase, exactly  
64 hex characters. The artifact itself MUST NOT be included in  
the statement.

artifact\_content\_type (string, REQUIRED)

IANA media type of the artifact, e.g., "text/plain", "image/png".

artifact\_bytes (integer, REQUIRED)

Size of the artifact in octets. MUST be greater than zero.

generation\_type (enum, RECOMMENDED)

Generation modality. One of:

"FULLY\_GENERATED" — content created entirely by AI from a prompt;  
"AI\_MANIPULATED" — AI applied to real source content (deepfake,  
voice clone, image manipulation);  
"AI\_ASSISTED" — human-created content with AI assistance.  
If absent, behavior is unspecified and verifiers SHOULD treat  
the receipt as having reduced evidentiary weight.

source\_content\_hash (string, OPTIONAL)

For generation\_type == "AI\_MANIPULATED": SHA-256 hash of the  
original source material that was modified. Enables deepfake  
accountability — the original is proven to exist without being  
transmitted or stored.

perceptual\_hash (object, OPTIONAL)

Perceptual hash structure for image, audio, or video content,  
enabling matching of content after transcoding or compression.  
Object fields: "algorithm" (string, e.g., "pHash", "chromaprint"),  
"value" (hex-encoded string), "bits" (integer, hash length).

Dawkins

Expires November 25, 2026

[Page 5]

Internet-Draft

SCITT AI Article 50 Profile

May 2026

transparency\_marker (string, REQUIRED, default: "LPR-EU-AI-ACT-50")

Machine-readable disclosure marker that SHOULD be embedded in or  
alongside the content (e.g., in EXIF metadata, HTML meta tag,  
C2PA assertion). Default value satisfies Article 50(2) "machine-  
readable format" requirement when present in a valid registered  
SCITT statement.

is\_public\_interest (boolean, OPTIONAL)

Deployer assertion that this content touches matters of public  
interest within the meaning of Article 50(4). RECOMMENDED to set  
explicitly for news, public affairs, political content, and  
regulatory disclosures.

enforcement\_date (string, REQUIRED, default: "2026-08-02")

ISO 8601 calendar date (YYYY-MM-DD) of the regulation under which  
the receipt is issued.

profile\_version (string, REQUIRED, default: "EU-AI-ACT-50-v1.1")

Pins the receipt to a specific profile revision for forward  
compatibility.

supervisory\_authority (string, OPTIONAL)  
Named EU supervisory authority with jurisdiction over the  
deployer, e.g., "BaFin (DE)", "AMF (FR)".

### 3.2. ai/human-review/v1 (Editorial Review Receipt)

The content type "ai/human-review/v1" supports invocation of the Article 50(4) human editorial review exemption. It MUST be issued by the same deployer that issued the corresponding "ai/article-50/v1" receipt, after substantive human review of the generated text.

The content payload is a JSON object with the following fields:

original\_entry\_hash (string, REQUIRED)  
Hash of the SCITT statement registration of the original  
"ai/article-50/v1" receipt being reviewed. Cryptographically  
binds this receipt to the original generation event.

original\_sequence (integer, REQUIRED)  
Sequence number of the original receipt within the Transparency  
Service log.

reviewer\_role (string, REQUIRED)  
Role identifier of the human reviewer. MUST be a role identifier  
(e.g., "senior-editor", "legal-counsel", "compliance-officer"),  
NOT a personal name or email. GDPR-safe by construction.

reviewer\_country (string, REQUIRED)  
ISO 3166-1 alpha-2 country code of the reviewer's organization.

review\_timestamp (string, REQUIRED)  
ISO 8601 datetime of the review event.

Dawkins Expires November 25, 2026 [Page 6]

Internet-Draft SCITT AI Article 50 Profile May 2026

review\_type (enum, REQUIRED)  
One of: "SUBSTANTIAL\_EDIT", "FACTUAL\_REVIEW", "APPROVAL\_ONLY".

reviewed\_artifact\_hash (string, REQUIRED)  
SHA-256 hash of the post-review content. For review\_type ==  
"SUBSTANTIAL\_EDIT", this MUST differ from the artifact\_hash of  
the original receipt; otherwise the claim of substantial edit  
is provably false.

is\_public\_interest (boolean, REQUIRED)  
Deployer assertion that the content is public interest under  
Article 50(4). If false, the 50(4) exemption is moot and this  
receipt has reduced evidentiary value.

review\_rationale (string, OPTIONAL)  
Free-text rationale (RECOMMENDED for legal defensibility). MUST  
NOT contain personal data.

### 3.3. ai/chatbot-session/v1 (Interactive AI Receipt)

The content type "ai/chatbot-session/v1" supports Article 50(1) compliance for interactive AI systems. It records that a user was informed of interaction with an AI system at a specific time, or that the "obvious to a reasonably well-informed natural person" exemption was claimed.

The content payload is a JSON object with the following fields:

session\_id\_hash (string, REQUIRED)  
SHA-256 hash of an opaque session identifier. The raw session identifier MUST NOT be transmitted or stored. The hash provides unlinkability while permitting the deployer to demonstrate that a particular session was notified.

ai\_system\_id (string, REQUIRED)  
As in Section 3.1.

deployer\_id (string, REQUIRED)  
deployer\_name (string, REQUIRED)  
deployer\_country (string, REQUIRED)  
As in Section 3.1.

notification\_timestamp (string, REQUIRED)  
ISO 8601 datetime of the AI-interaction notification, or the session start time if obvious\_exemption\_claimed is true.

notification\_method (enum, REQUIRED)  
One of: "INITIAL\_BANNER", "INLINE\_MESSAGE",  
"AUDIO\_ANNOUNCEMENT", "PRE\_PROMPT\_DISCLOSURE".

notification\_text\_hash (string, REQUIRED)  
SHA-256 hash of the disclosure text shown to the user. Enables proof of disclosure content without storing it.

Dawkins

Expires November 25, 2026

[Page 7]

Internet-Draft

SCITT AI Article 50 Profile

May 2026

obvious\_exemption\_claimed (boolean, REQUIRED)  
If true, the deployer is asserting that AI interaction was obvious within the meaning of Article 50(1) and explicit notification was therefore not required. The receipt then functions as evidence of the deployer's good-faith determination that the exemption applied at the time of interaction.

## 4. Validation and Verification

### 4.1. Issuance Validation

Before registering a statement under this profile, the SCITT Transparency Service MUST validate:

1. The statement content\_type is one of the three defined in Section 3.
2. All REQUIRED fields are present and well-formed per Section 3.
3. The deployer\_id (and, for human-review, reviewer\_role) does not contain prohibited identifier patterns (Section 5.2).
4. artifact\_hash, source\_content\_hash, reviewed\_artifact\_hash, session\_id\_hash, and notification\_text\_hash are 64 lowercase hex characters each.
5. deployer\_country and reviewer\_country are exactly two uppercase ASCII letters (ISO 3166-1 alpha-2).
6. For ai/human-review/v1: a registered statement matching

original\_entry\_hash exists, was issued by the same deployer\_id (cross-checked against the SCITT issuer identity), and has content\_type "ai/article-50/v1".

A statement failing any validation step MUST NOT be registered.

#### 4.2. Article 50 Conformance Verification

To verify that a statement registered under this profile is Article 50 Conformant, a verifier MUST:

1. Resolve the SCITT statement and confirm its registration in the Transparency Service's append-only log.
2. Verify the signature on the statement.
3. Confirm transparency\_marker is present and non-empty.
4. For ai/article-50/v1: confirm generation\_type, if present, is one of the permitted enum values.

Dawkins

Expires November 25, 2026

[Page 8]

Internet-Draft

SCITT AI Article 50 Profile

May 2026

5. For ai/human-review/v1: independently verify the referenced original receipt and confirm chain-of-custody invariants (same deployer, original predates review).
6. For ai/chatbot-session/v1: confirm notification\_method and notification\_text\_hash are present.
7. Confirm the SCITT log substrate's anchoring evidence (e.g., Bitcoin block inclusion, qualified timestamp).

A receipt passing all conformance checks MAY be presented to supervisory authorities as evidence of Article 50 compliance for the artifact identified.

#### 4.3. Article 50 Defensibility Verification

For evidentiary use in adversarial proceedings, a verifier SHOULD additionally confirm:

1. For image/audio/video content: perceptual\_hash is populated.
2. For AI\_MANIPULATED content: source\_content\_hash is populated.
3. For text where is\_public\_interest == true: if the deployer claims the Article 50(4) editorial exemption, a corresponding ai/human-review/v1 receipt is found, properly chained, and review\_type is SUBSTANTIAL\_EDIT or FACTUAL\_REVIEW.
4. The SCITT log anchoring depth is sufficient to deter reorganization attacks on the substrate (e.g., 6+ Bitcoin confirmations for a Bitcoin-backed log).

A receipt failing one or more defensibility checks remains Article 50 Conformant but MAY be challenged on evidentiary grounds in proceedings.

#### 5. Privacy Considerations



## 5.1. GDPR Article 17 (Right to Erasure)

SCITT statements registered under this profile are intended to carry no personal data (see Section 5.2). However, the artifact identified by `artifact_hash` may itself contain personal data, in which case the data subject's right to erasure may impose obligations on the deployer.

Implementations SHOULD support a soft-delete pattern in which the content payload is nulled while preserving the registered statement's cryptographic identity (`entry_hash`, signature, log inclusion proof). This preserves the historical record of issuance while removing the content reference, satisfying GDPR Article 17 without compromising the integrity of the log.

Dawkins

Expires November 25, 2026

[Page 9]

Internet-Draft

SCITT AI Article 50 Profile

May 2026

## 5.2. Prohibited Identifier Classes

The following identifier classes MUST NOT appear in any field of a statement registered under this profile:

- o Email addresses (detected by presence of "@");
- o Personal names;
- o National identification numbers, social security numbers, or equivalents;
- o Biometric data of any kind;
- o Direct identifiers of natural persons.

The `deployer_id` and `reviewer_role` fields MUST be legal-entity identifiers and role identifiers respectively. Implementations MUST reject statements containing prohibited identifiers at validation time.

## 6. Security Considerations

The integrity of an Article 50 Conformant Receipt rests on the integrity of:

- o The signing key controlled by the issuer;
- o The SCITT Transparency Service log;
- o The anchoring substrate (where applicable).

Key compromise enables forgery of receipts. Implementations SHOULD support hardware-protected signing keys, key rotation, and revocation of compromised keys with retroactive identification of statements signed under compromised keys.

The `artifact_hash` field commits to specific content. A receipt for content C does not authenticate any other content C', even if C and C' are perceptually similar. The `perceptual_hash` field, when populated, enables similarity matching but is not cryptographically binding.

Forward secrecy is not provided. A statement registered today

remains verifiable in the future; this is a feature of the transparency log architecture, not a weakness.

## 7. IANA Considerations

This document requests registration of three media types under the IANA media types registry:

Dawkins Expires November 25, 2026 [Page 10]

Internet-Draft SCITT AI Article 50 Profile May 2026

- o ai/article-50+json
- o ai/human-review+json
- o ai/chatbot-session+json

Registration template details to be provided in a future revision.

## 8. References

### 8.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, May 2017.
- [RFC6962] Laurie, B., Langley, A., and E. Kasper, "Certificate Transparency", RFC 6962, June 2013.
- [I-D.ietf-scitt-architecture] Birkholz, H., Delignat-Lavaud, A., Fournet, C., Deshpande, Y., and S. Lasker, "An Architecture for Trustworthy and Transparent Digital Supply Chains", draft-ietf-scitt-architecture (work in progress).

### 8.2. Informative References

- [EU-AIA] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), OJ L 2024/1689, 12 July 2024.
- [C2PA] Coalition for Content Provenance and Authenticity, "C2PA Technical Specification, Version 2.1", <<https://spec.c2pa.org/>>.
- [eIDAS] Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.
- [draft-dawkins-scitt-lpr-00] Dawkins, V., "A Bitcoin-Anchored SCITT Transparency Profile: The LedgerProof Receipt (LPR), Version 1.0", draft-dawkins-scitt-lpr-00, July 2026.

Veronica S. Dawkins  
LedgerProof Foundation  
Email: [spec@ledgerproofhq.io](mailto:spec@ledgerproofhq.io)

Dawkins

Expires November 25, 2026

[Page 11]