

The Missing Gap in the Agentic IAM Discussion

An agent's identity does not tell a reviewer whether the file it used matches an earlier recorded version.



Carson Seeger 
Founder & CEO

Organizations are giving AI agents access to contracts, credentials, and version-controlled files. Identifying an agent is one part of oversight; checking the version of a file it used is another. [Agentic recordkeeping](#) needs both a reliable action trail and a way to compare the underlying document when a copy is available.

[Proof's identity framework](#) describes ways to establish who an agent is and what it may do. A separate document-integrity check asks whether a file matches a version previously recorded. Neither check alone establishes that the file's contents are true.

What is Arkova?

Arkova creates document and credential records for later lookup and file comparison. In a [2026 Boomi-commissioned survey](#) of 409 senior IT decision-makers, 86% said their organizations had moved beyond AI-agent pilots; 34% said they trusted their agents' actions. Those results describe the surveyed group, not all enterprises.

Autonomous agents are being integrated into enterprise workflows to move beyond simple chat responses and actively execute multi-step business processes. Agents are extracting data from invoices, reviewing contracts, and translating multilingual files, connecting to existing enterprise data stores and enterprise identity providers, and automating employee onboarding.

Arkova computes a document fingerprint and publishes a record linked to a public-network receipt without retaining the original file. Direct uploads are fingerprinted in the browser; selected connected-source files are fingerprinted briefly in server memory. A public ID lookup reports record details. Checking a particular file independently also requires the file, its recorded fingerprint, and enough proof data to connect it to the network anchor. Records that report per-document proof availability, such as the public record ARK-DOC-2Z5WPG, return a per-document inclusion proof from Arkova's public API; older records may report only a batch-level reference.

Why is document verification important to the agentic OS?

86% / 34%

of 409 senior IT decision-makers surveyed reported moving beyond agent pilots / trusting agent actions

— [*Boomi-commissioned Forrester survey, 2026*](#)

The survey points to a gap between agent adoption and confidence, but it does not measure document fraud. A separate [Deloitte and DocuSign study](#) estimated that ineffective agreement management costs roughly \$2 trillion in annual global economic value. That estimate covers agreement workflows broadly; it is not a measure of credential fraud or the savings Arkova can deliver.

A fraudulent credential and an altered copy of a real credential are different risks. A fingerprint comparison can detect a changed copy relative to a recorded value; it cannot determine whether the original issuer was authorized or the underlying qualification was earned.

As agents handle more records, teams need to know which file version an agent saw and where the claimed issuer and status came from.

When do organizations need to start preparing?

Now.

[Regulation \(EU\) 2026/1744](#) of 8 July 2026, published in the Official Journal on 24 July 2026, amends Article 113 of the EU AI Act so that the Chapter III, Sections 1 to 3 high-risk requirements apply from 2 December 2027 for systems classified under Annex III and from 2 August 2028 for systems classified under Annex I. The [Colorado Attorney General](#) states that Senate Bill 26-189, signed in May 2026, repeals and re-enacts the state’s automated decision-making technology provisions, effective 1 January 2027. Both sources were checked on 21 October 2026. Each law defines the systems and roles it covers; this article does not assess whether any particular workflow is covered.

REGULATION / FRAMEWORK	APPLICABLE DATE	SCOPE AS STATED IN THE CITED SOURCE
Colorado automated decision-making technology law (SB 26-189)	1 January 2027	Developers and deployers of automated decision-making technology used in consequential decisions (Colorado Attorney General).
EU AI Act (general date of application)	2 August 2026	Article 113 general date of application, for provisions not given a different date.
EU AI Act (Annex III high-risk)	2 December 2027	Chapter III, Sections 1 to 3, for systems classified high-risk under Article 6(2) and Annex III (Regulation (EU) 2026/1744).
EU AI Act (Annex I high-risk)	2 August 2028	Chapter III, Sections 1 to 3, for systems classified high-risk under Article 6(1) and Annex I (Regulation (EU) 2026/1744).

This article does not assess liability for any agent action. A team that wants an event to be reviewable later can preserve the file version, approval context, and action log.

Arkova's public record can be one reference in that evidence package. A public ID lookup reports status and anchor details; a file comparison tests whether a presented copy matches a recorded fingerprint. Neither by itself establishes the issuer's authority.

Who is currently tackling this issue?

Agent identity frameworks address who or what may act. Document-integrity checks address whether a presented file matches a recorded version. The two are complementary, and neither guarantees that a document's statements are accurate.

Registry checks can answer some questions about public filings or professional status. Private contracts need a different trail: a retained executed copy, reliable signature evidence, and a record of later versions. Arkova can add a public record reference and fingerprint comparison to that trail.

Illustrative scenario: a client disputes a clause in a contract and sends a copy to a law firm. The firm's agent finds a different version in its files. Before anyone responds, a reviewer needs the executed copy, signing evidence, amendment history, and the version the agent used. A fingerprint comparison can flag a mismatch; it cannot decide which party's interpretation is right.

In that scenario, a team could share the executed copy, its e-signature audit trail, and an Arkova public ID if the agreement was recorded. The recipient could look up the reported record details and compare the file with its recorded fingerprint when available. A per-document proof bundle is returned only for records that report per-document proof availability, so the recipient should check that field for each agreement.

Where are agents acting? Why is this a risk?

Where the risk appears: wherever an agent relies on a document or credential to take an action.

Non-human identity and delegated authorization create important security questions. OAuth and OIDC can carry identity and authorization information, but a token does not establish that a particular document is genuine. [Agent transaction infrastructure](#) and document evidence need to be evaluated as separate layers.

Start with a workflow where a mistaken document version would matter. Record the agent's authority, the source file, and the evidence needed to challenge a decision later. Arkova can add a file-integrity reference to that wider trail.

What you can do today

You do not need to wait for regulatory deadlines to close this gap.

Inspect a record yourself. Enter a public ID at [Arkova's public lookup](#) to see reported status and network receipt details without an account. A lookup does not compare a file; someone holding the file can perform a fingerprint comparison when the recorded value is available.

If you run agents on regulated documents: identify a high-risk workflow and the evidence each decision needs: the file version, authorized actor, reported record status, and approval trail. Contact us to discuss whether Arkova's current public lookup and supported connectors fit that workflow.

If you build agent infrastructure: identity and document evidence answer different questions. We can walk through the current record-lookup boundary and where a file comparison may help.

Let's talk: founders@arkova.ai



Written by Carson Seeger 
Founder & CEO at Arkova

Printed from <https://arkova.ai/research/missing-gap-agentic-iam>. The web page is the current version.