



**KCST**

KELSHAD CYBER SYSTEMS AND TECHNOLOGIES LLC

KST-IDV-001-REV2026-10 · PUBLIC BRIEF

# Identity Verification Framework

**ISSUED**

2026-10-17

**AUTHOR**

Joshua Kelsey Bass, Founder, Chairman and Chief  
Executive Officer

**SUPERSEDES**

KST-IDV-001-REV2026, issued May 17, 2026

## CURRENT STATUS

RxOmniMedLink is in controlled private alpha. Kelshad Cyber Systems and Technologies LLC is not using live protected health information, is not transmitting live prescriptions, and does not support controlled-substance prescribing. We have not completed Surescripts onboarding, the third-party audit and certification required for EPCS under 21 CFR Part 1311, or a SOC 2 audit. This document describes both implemented capability and target architecture, and states plainly which is which.

## 1. Purpose and Scope

This document describes the identity verification (IDV) framework used by RxOmniMedLink, the clinical coordination platform built by Kelshad Cyber Systems and Technologies LLC (KCST). It covers how clinical users are verified before they are granted access to the platform, what evidence is collected, who holds that evidence, and which parts of the design are implemented as of 2026-10-17 versus planned.

It is a public brief. It is not a certification, an audit report, or a regulatory attestation, and it should not be read as one. KCST holds no third-party certification of any kind for this system.

Identity is the first control in the platform. Prescribers, pharmacists, and clinical staff request access to functions that, once live prescription traffic exists, will carry real patient consequence. Verifying that the person behind an account is the licensed individual they claim to be is therefore treated as a gating requirement rather than an onboarding convenience.

## 2. Implemented As Of 2026-10-17

The following are implemented and in use in the controlled private alpha environment:

- **Stripe Identity** performs document capture, document authenticity checks, and a live selfie match for every clinical user account. This is the only identity verification path in the platform.

- **Verification is performed against the NIST SP 800-63-3 IAL2 standard.** See Section 4 for what that statement does and does not mean.
- **Raw identity evidence is held by Stripe, not by KCST.** The platform database stores a Stripe verification session identifier, a verification status, and the internal user identifier. Government identification numbers, document images, and selfie captures are not written to KCST systems.
- **TLS 1.3** protects all traffic between the client, the KCST backend, and the Stripe Identity API.
- **Encryption at rest** is provided by the managed database provider (Render Postgres) using industry-standard AES-256. This is provider-level encryption. It is not application-level PHI encryption written by KCST, and it should not be described as such.
- **Role-based access control and audit logging** are implemented. See Section 7 for a material limitation of the current audit log.
- **Webhook signature validation** rejects unsigned or replayed verification callbacks.

No live protected health information exists in the environment. All clinical data in the alpha is synthetic test data.

### 3. Stripe Identity Integration

---

The integration uses Stripe Identity as the verification engine. KCST does not operate its own document parsing, optical character recognition, or biometric matching capability, and does not intend to.

The flow is asynchronous and webhook driven, which keeps the latency of document capture out of the application request path:

1. An authenticated user requests verification.
2. The KCST backend creates a Stripe `VerificationSession` requiring both a government identification document and a live selfie capture.
3. Stripe returns a session identifier and a hosted verification URL.
4. The user completes capture in the Stripe-hosted flow. Document images and selfie captures are uploaded directly to Stripe.
5. Stripe emits a signed webhook event on completion.
6. The KCST backend validates the webhook signature, queries the verification result, and updates the stored account status.

The account state machine is linear and enforced server side. Accounts begin `UNVERIFIED`, move to `REQUIRES_INPUT` when a session is created, then to `PROCESSING`, and resolve to `VERIFIED`, `FAILED`, or `CANCELED`. Clinical functions are gated on the `VERIFIED` state.

Error handling requires that identity payloads are never written to application logs or caches. Log records carry the Stripe session reference and the resulting state, not the underlying evidence.

### 4. Alignment With NIST SP 800-63-3 IAL2

---

NIST Special Publication 800-63-3 is the federal guideline set for digital identity. Identity Assurance Level 2 (IAL2) describes remote or in-person identity proofing supported by validated evidence and a biometric comparison of the applicant to that evidence.

**An important distinction.** KCST does not hold, and does not claim, an IAL2 certification. No such certification is issued to KCST by any body. IAL2 is the published standard that the Stripe Identity verification flow is performed against. The accurate statement is that clinical user proofing on RxOmniMedLink is performed to an IAL2 standard using Stripe Identity. Any stronger phrasing is incorrect and must not be used in KCST material.

How the flow maps to the IAL2 proofing requirements:

| IAL2 ELEMENT                  | HOW IT IS MET                                                                                                                                    | PERFORMED BY    |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| Evidence collection           | One piece of superior or strong evidence, such as a passport or driver's license, is required.                                                   | Stripe Identity |
| Evidence validation           | Document authenticity checks, including machine readable zone and barcode parsing and security feature inspection.                               | Stripe Identity |
| Biometric comparison          | One-to-one comparison of a live selfie capture against the portrait on the submitted document.                                                   | Stripe Identity |
| Presentation attack detection | Live capture with motion requirements, intended to defeat static photo and screen replay attacks.                                                | Stripe Identity |
| Enrollment record             | The verification session reference, outcome, and timestamp are retained by KCST. Underlying evidence is retained by Stripe under Stripe's terms. | KCST and Stripe |

KCST has not commissioned an independent conformance assessment of this mapping. It reflects our reading of the standard and of Stripe's published capability.

## 5. Data Handling and Privacy Posture

The design goal is that KCST never becomes a store of high-value identity evidence. Document images, identification numbers, and biometric captures are transmitted to Stripe and remain in Stripe's environment. KCST retains only the session reference and the pass or fail outcome.

**Zero commercialization of identity data.** Identity records, verification metadata, and access logs are not sold, licensed, shared for marketing, or repurposed for profiling or analytics. They exist to establish authorization to use the platform, and for no other purpose.

**Vendor agreements.** Business Associate Agreements are in place with the vendors in the platform's data path. Live protected health information is still not accepted, and the platform remains on synthetic data during the controlled private alpha.

**Target architecture.** The following describes the intended design. It is not implemented as of 2026-10-17.

A deterministic one-way identity digest, computed as SHA-384 over normalized name and date of birth values combined with a pepper held in an isolated key management service, is planned to support duplicate account detection without retaining plaintext identifiers. No such digest, pepper, or key management service is in place as of 2026-10-17. HTTP Strict Transport Security with preload, and a documented purge schedule coordinated with the verification vendor, are also planned and not yet deployed.

## 6. Security Controls

---

Implemented: TLS 1.3 in transit with forward-secret cipher suites, AES-256 encryption at rest provided by Render Postgres, role-based access control, audit logging of verification lifecycle events, and HMAC signature validation on every inbound Stripe webhook using the shared webhook secret.

Not implemented, and not to be claimed: SOC 2 audit, FIPS 140-2 validated signing engine, and application-level PHI encryption authored by KCST. A third-party penetration test of the platform has been completed.

## 7. Audit Logging and a Known Limitation

---

The platform writes structured lifecycle records for identity events. Each record carries a timestamp, a trace identifier, an event type, the Stripe session reference, and the resulting state. Records do not carry identity evidence.

**Known limitation.** The audit log is append-only in practice but is **not tamper-evident as of 2026-10-17**. The `sha384_checksum` column in the audit log table is populated with constant string labels rather than computed digests, so it provides no integrity guarantee. Repair is in progress. Until that work ships, no KCST document, including this one, may describe the audit trail as tamper-evident, immutable, or supporting non-repudiation.

## 8. Regulatory Posture

---

RxOmniMedLink implements **HIPAA-aligned controls**. HIPAA does not offer certification, and KCST makes no claim of HIPAA compliance, HIPAA certification, or full HIPAA compliance. The identity framework supports the unique user identification and access control expectations of the HIPAA Security Rule administrative and technical safeguards at 45 CFR 164.308 and 45 CFR 164.312.

Because raw verification evidence stays with the verification vendor rather than on KCST infrastructure, exposure from on-premise physical storage is reduced. Data minimization principles consistent with GDPR and CCPA expectations inform the design. These are design intentions, not audited conclusions.

Explicitly out of scope: this framework does not enable, and RxOmniMedLink does not support, controlled-substance prescribing. Identity proofing at IAL2 is one input to EPCS identity proofing under 21 CFR Part 1311, but EPCS additionally requires third-party certification or audit that KCST has not begun. A technical block preventing controlled-substance workflows is being shipped.

## 9. Threat Model

---

The framework is modeled against three primary vectors:

**Presentation and deepfake attacks.** Screen replays, printed masks, and injected video streams are addressed by Stripe Identity's live capture and motion requirements. KCST does not run its own liveness detection and relies on the vendor's controls here.

**Webhook injection and replay.** Every inbound webhook is verified against an HMAC-SHA256 signature computed over the timestamp and raw request body using the webhook secret. Unsigned, malformed, or stale payloads are rejected before any state transition.

**Verification bypass during outage.** If the verification pipeline is unavailable, onboarding pauses. Access is never granted, downgraded, or provisionally allowed during an outage.

## 10. Operations

---

Deployment requires three runtime values in the isolated container context: the Stripe secret key, the Stripe Identity webhook secret, and the assurance level setting. The webhook ingestion route is registered against the platform API endpoint and restricted to identity verification events.

**Pass-through billing.** Identity verification is billed to customers as a pass-through at documented cost. KCST charges the per-verification fee assessed by the verification vendor, at the rate published in the applicable pricing schedule, with no markup applied. Verification cost is stated separately from subscription charges on customer invoices.

## 11. Roadmap

---

**Target architecture.** The following describes the intended design. It is not implemented as of 2026-10-17.

Planned work, in priority order: repair of the audit log checksum so the trail becomes genuinely tamper-evident; and the identity digest and key management design described in Section 5.

Longer term, KCST is evaluating W3C Verifiable Credentials so that users can hold and present their own identity assertions without a central evidence pool, and is tracking quantum-resistant algorithms, including CRYSTALS-Kyber, for future transport and storage protection. Neither has been prototyped.

## 12. Document Control

---

Kelshad Cyber Systems and Technologies LLC, a Florida limited liability company, document number L26000296916. 7901 4th Street North, Suite 300, St. Petersburg, FL 33702. info@kelshad.com. (813) 982-8779.

This revision supersedes KST-IDV-001-REV2026 in full. The superseded document contained an incorrect legal entity name, an incorrect officer attribution, an external standard reference that does not apply to KCST

documents, and capability claims that were not accurate. Questions about the accuracy of any statement in this brief should be directed to [info@kelshad.com](mailto:info@kelshad.com).

---

KST-IDV-001-REV2026-10 · Classification: Public · This brief is not a certification, audit report, or legal advice. Questions about any statement: [info@kelshad.com](mailto:info@kelshad.com)