VERITY 27

Technical Specification and Architecture Annexes

Patent-Aligned Technical Documentation

April 18, 2026

Patent Status: Pending | Application 64/043,173

Joshua Darrell Bloodworth
josh@verity27.com
423-305-4165

DOCUMENT OVERVIEW

This document provides complete technical specification and architecture documentation for Verity 27, aligned with patent application 64/043,173 filed April 18, 2026.

The system consists of three technological pillars:

Pillar 1: Structural Persistence - NFC/RFID filament integrated into load-bearing structural seams, providing lifecycle persistence.

Pillar 2: The Final Stitch Handshake - Cryptographic binding method connecting the structural identifier to worker Professional Verifiable Credentials at point of manufacture.

Pillar 3: The Regulatory Bridge - Data-interoperability layer integrating external forensic markers into the persistent structural identifier.

Maker Ledger provides the worker credential system that enables Pillar 2 binding.

This document is intended for technical review and due diligence purposes.

1. PILLAR 2: THE FINAL STITCH HANDSHAKE - BINDING MECHANISM

Verity 27 is architected around a single critical moment in garment manufacturing: the terminal production checkpoint designated the "Final Stitch." At this checkpoint, three distinct technical operations occur in sequence, creating a cryptographic binding between physical product identity, worker credential verification, and labor condition attestation.

The three-step binding sequence is:

1. Structural identifier is scanned via machine-integrated sensor (establishing physical product identity)
2. Worker Professional Verifiable Credential is authenticated against decentralized ledger (verifying worker status and labor conditions)
3. Unique cryptographic proof is generated, binding garment ID to worker credential and condition data (creating immutable attestation)

These operations are architecturally dependent. Physical identifier persistence alone does not establish labor condition verification. Worker credentials alone do not establish garment identification. Cryptographic binding at the Final Stitch creates a singular forensic proof linking all three elements.

2. PILLAR 1: STRUCTURAL PERSISTENCE - SEAM INTEGRATION

2.1 Physical Integration

A passive NFC/RFID filament is integrated into a load-bearing structural seam during garment assembly. Integration points include side seams, shoulder seams, and inseams, depending on garment type and structural requirements.

The integration method incorporates the filament into the seam structure during the overlock stitching process. Physical removal of the identifier requires destruction of the seam structure, compromising garment structural integrity and functionality.

2.2 Persistence Characteristics

The identifier is designed to remain intact through standard product handling and use scenarios: retail transportation and warehouse storage, consumer laundering (standard cold and warm water cycles), dry cleaning processes, industrial laundering at standard commercial specifications, garment layover time on retail displays, secondary market transactions and resale, returns processing and warehouse restocking, and textile recycling and recovery processes.

The identifier does not naturally separate from the garment through normal use patterns. Removal requires intentional destruction of the seam structure.

2.3 Technical Parameters

Frequency Standards: ISO/IEC 18000-6C (High Frequency and Ultra-High Frequency dual-band compatibility)

Read Range: Optimized for manufacturing line sensor applications, typically 10-30 centimeters depending on antenna configuration

Data Capacity: Sufficient to store unique product identifier, manufacturing batch references, and cryptographic pointers to external ledger records

Durability Validation: Architectural specifications for high-durability applications are established. Validation testing with textile materials laboratories is in progress.

3. PILLAR 2 DETAILED SPECIFICATION: FINAL STITCH CRYPTOGRAPHIC HANDSHAKE PROTOCOL

3.1 Step 1: Structural Identifier Acquisition

At the final assembly checkpoint, immediately prior to garment completion:

Structural identifier is acquired via machine-integrated NFC reader. Scan operation captures the unique product ID. Scan timestamp is recorded. System verification confirms seam integrity and identifier readability.

Failure conditions result in garment rejection and manual review.

3.2 Step 2: Worker Credential Verification

Concurrent with or immediately following identifier acquisition:

Worker Professional Verifiable Credential is presented to the system (via QR code, NFC card, or mobile authentication mechanism). Credential is authenticated against the Maker Ledger, a decentralized credential registry maintaining verified worker identity and status records.

Verification process confirms worker identity and decentralized identifier (DID), current merit-level certification status (L1-L4), worker authorization status for production (active/inactive/restricted), and associated labor condition documentation (wage verification, hours, conditions).

Personal identification data (legal name, address, personal identification numbers, payment information) is not transmitted to brand systems. Authentication returns credential status only. Worker retains cryptographic control of personal data via private keys maintained on Maker Ledger.

Credential validation failure results in garment rejection and manual review.

3.3 Step 3: Cryptographic Attestation Generation

Following successful completion of identifier acquisition and credential verification:

Cryptographic proof is generated using Zero-Knowledge Proof (ZKP) protocols. The proof cryptographically binds garment structural identifier (from acquisition step), worker credential verification status (from authentication step), labor condition metadata (from current worker ledger record), and manufacturing timestamp (immutable record of binding moment).

The resulting attestation is encrypted and permanently associated with both the garment's structural identifier record and the worker's credential record on Maker Ledger.

Cryptographic attestation failure results in garment rejection and system error investigation.

4. PILLAR 3: THE REGULATORY BRIDGE - TIER-3 FORENSIC DATA INTEGRATION

4.1 Forensic Marker Integration Architecture

Chemical and biological forensic markers (such as DNA-labeled fibers or chemical isotope signatures) serve to establish material provenance. These markers are applied to raw materials or finished goods by material suppliers or third-party verification services.

The Verity 27 architecture incorporates a validation hub designed to cryptographically bind external forensic marker verification data to the persistent structural identifier. This integration does not replace existing forensic marker systems; rather, it creates a data-binding layer between forensic verification results and the persistent product identifier.

4.2 Integration Process

Third-party forensic laboratories analyze applied markers and generate verification results confirming material authenticity and origin. These results are provided to the system in the form of a success signal (verified origin/authenticity confirmation).

The success signal is cryptographically bound to the garment's structural identifier record, creating a singular compliance record that includes garment structural identity and Final Stitch attestation (Verity 27), worker credential verification (Maker Ledger), and material origin verification (Tier-3 forensic markers).

4.3 Regulatory Standards Compatibility

Output data is formatted for compatibility with EU Digital Product Passport (DPP) registry standards and customs documentation requirements. Data structures follow JSON-LD (Linked Data) standards for interoperability with regulatory API systems.

The complete cryptographic audit trail, from Final Stitch binding through forensic validation to DPP certification, remains immutable and verifiable.

5. MAKER LEDGER: WORKER PROFESSIONAL CREDENTIALS (PILLAR 2 SUPPORTING SYSTEM)

5.1 Overview and Role in Pillar 2

The worker credential system (Maker Ledger) provides the Professional Verifiable Credential (PVC) data that is bound by the Final Stitch Handshake in Pillar 2. Maker Ledger is not a separate pillar; it is the decentralized credential infrastructure that enables the cryptographic binding mechanism at the Final Stitch.

Credentials are structured according to W3C Decentralized Identifier (DID) standards. Each worker credential is cryptographically controlled by the individual worker through private key ownership.

Credentials contain worker decentralized identifier (unique, portable across employment), professional merit-level certification (L1 through L4, based on authenticated work history), labor condition verification status (current employment conditions, wage verification), and immutable record of authenticated contributions (stitch events, quality markers, training completion).

Worker retains complete control of credential data. Private keys required to modify or access credential data are owned by the worker. Credentials are portable across employers and employment arrangements.

5.2 Merit-Level Certification

Professional merit-level is earned through authenticated work history recorded at the Final Stitch. Each level reflects verified technical proficiency and consistency.

Level 1: Verified Operator - Entry-level status. Requires 20-50 authenticated manufacturing events and identity verification.

Level 2: Certified Artisan - Specialized technical proficiency. Requires 100+ authenticated manufacturing events with quality verification markers and consistent performance documentation.

Level 3: Lead Technologist - Supervisory proficiency. Requires 500+ authenticated manufacturing events, cross-facility capability documentation, and mentorship evidence.

Level 4: Master Conservator - Expert proficiency. Requires 1,000+ authenticated manufacturing events with leadership markers, protocol governance participation, and cross-facility technical authority.

Merit-level directly correlates with expanded system capabilities and economic benefits available within the Maker Ledger system.

9. ARCHITECTURE SUMMARY

Verity 27 is an integrated system architecture consisting of three technological pillars, as defined in the patent disclosure:

Pillar 1: Structural Persistence - NFC/RFID filament integrated into load-bearing structural seams, providing lifecycle persistence through the complete product lifecycle.

Pillar 2: The Final Stitch Handshake - Cryptographic binding method that connects the structural identifier to the worker's Professional Verifiable Credential, creating immutable records at point of manufacture. Maker Ledger provides the credential data that enables this binding.

Pillar 3: The Regulatory Bridge - Data-interoperability layer that integrates external forensic markers (Tier-3 tracers) into the persistent structural identifier, creating singular compliance records.

The architecture is complete and fully specified in patent disclosure 64/043,173. Three distinct patent claims protect the structural seam integration, cryptographic handshake methodology, and Zero-Knowledge Proof privacy implementation.

Real-world manufacturing integration and pilot validation testing represent the next phase of development.

Patent protection expires April 18, 2027, with pathway to non-provisional filing by that date.