

The logo features a stylized fingerprint in blue and gold, with a gold pen stroke forming a signature across it. The word "Fingersign" is centered over the graphic, with "Finger" in white and "sign" in gold.

Fingersign

Fingersign Identity is based on Patented Proprietary
Technology that uses Biometric Credentials

The Identity Gap: Verifying Accounts vs. Verifying Humans



Most E-Sign Workflows

- **Focus:** Verifies Accounts
- **Access:** Login or OTP confirms account access, not signer presence.
- **Action:** Intent capture is often weak or inconsistent.
- **Trust Model:** Verification depends entirely on trusting a single platform's internal record.



FingerSign Standard

- **Focus:** Verifies Humans
- **Access:** Captures physical presence at the exact moment of signing.
- **Action:** Captures and explicitly binds biometric intent to the document.
- **Trust Model:** Generates immutable, cryptographic evidence that anyone can independently verify.

The FingerSign Shift: From Identity to Cryptographic Proof



Proof

Immutable Evidence

The platform seals the document, preserving an append-only cryptographic record that serves as undeniable, independently verifiable evidence.

Intent

Server-Side Enforcement

FingerSign captures and enforces the user's explicit consent and intent to sign, locking the action to the verified identity.

Identity

SyberKey Verification

The system verifies the actual human signer's biometric identity specifically for the act of signing, completely removing reliance on assumed email possession.

The Engine of Proof: From Upload to Verifiable Record in 5 Steps



Built for Proof, Not Just Workflow



Real Human Verification

Biometric identity is verified at the exact moment of signing—never assumed from an email inbox or an intercepted OTP.



Evidence-Based Signature

Every single signature generates a permanent cryptographic record mathematically linking the human identity, their explicit intent, and the document hash.



Independent Verification

Trust is decentralized. Anyone can verify document integrity and signing status instantly using a transaction ID or a QR code.



No Certificate Complexity

Delivers enterprise-grade non-repudiation with zero user-managed keys, zero hardware tokens, and zero certificate lifecycle overhead in the core flow.

Designed for Disputes: The Anatomy of Trust

Web-native and evidence-first. Every signed document carries a transaction-level proof object, not just a visual stamp.



Anatomy of a Secure Transaction

High-Trust Signing for Critical Workflows

Independent evidence and verified identity are built into every signing event across your organization.



Legal Agreements

Ensure non-repudiation for high-stakes contracts, IP transfers, and settlements where human authenticity is non-negotiable.



Financial Approvals

Secure lending agreements, wire authorizations, and wealth management onboarding with transaction-level cryptographic proof.



HR & Onboarding

Authenticate remote employment agreements, background check consents, and critical policy acknowledgments.



Government Workflows

Modernize citizen services, procurement approvals, and regulatory compliance without the friction of hardware tokens.

Simple Plans for Teams and Enterprises

Starter

(Best for early pilots)

- Basic signing workflows
- Access to the Verification portal
- Email support

Business

(Best for growing teams)

- Multi-user operational dashboard
- Secure Evidence Vault
- API access & webhook-driven state updates
- Comprehensive audit exports

Enterprise

(Best for regulated scale)

- Advanced compliance controls
- Full white-label support
- Priority support SLA
- Custom integrations (API-first, transaction-level verification APIs)



FingerSign: The Human Authenticity Layer

Identity-backed digital signatures with independent verification.
Ready to eliminate signature disputes and accelerate high-trust approvals?

See FingerSign in action with your workflow, compliance needs, and integration stack.
Book a demo today.

Fingersign

