ChatGPT

Device-Bound Signature™: First Use Disclosure — May 2025

Prepared by MyNDA / Swifttract
Date of First Use: March 1, 2024
Public Disclosure: May 2025

MyNDA Logo

Table of Contents

---

1. Introduction

As digital trust becomes harder to earn and enforce, the need for more accountable, context-aware agreements is clear. From NDAs at exclusive events to onboarding workflows in HR, the limitation of traditional signatures lies in their isolation from the device used to apply them. MyNDA introduces **Device-Bound Signature**™, a system of metadata-enhanced, jurisdiction-aware agreements tied directly to the signer's physical device. This paper defines, explores, and positions Device-Bound Signature™ as a new enforceability standard for the trust economy.

2. What Is a Device-Bound Signature™?

A Device-Bound Signature™ is a digitally signed agreement in which the enforceability is not only linked to the signer's identity, but also to the metadata of the device used to execute the contract. Metadata may include:

- Device ID (IMEI, UUID)
- Geolocation (GPS or network-based)
- IP address and MAC address
- Browser fingerprint or OS signature
- Camera status or front-facing capture (if allowed)

This metadata is hashed and embedded into the audit trail of the contract, forming a hybrid identity that enforces accountability through both person and device. This enables contracts to become **situationally aware** — adapting enforceability to context, location, and device integrity.

3. Origins: From NDAs to Infrastructure

The concept began within the MyNDA platform, where users needed to enforce NDAs in physical or pop-up environments (e.g., private events, talent previews, investor rooms) without confiscating phones or verifying physical IDs. Traditional e-signatures proved insufficient. With Device-Bound NDAs, MyNDA could embed a clause that legally links the signer to their device — disincentivizing content leaks or unauthorized sharing.

From there, Swifttract realized that device-bound enforcement could scale across:

- Freelance contracts
- Employee offer letters
- Medical consent forms
- Talent image rights agreements

This transformed the solution from a feature to an enforceability **infrastructure layer.**

4. Technical Foundation and Metadata Architecture

Device-Bound Signatures™ are enabled through the Swifttract SDK, which collects and securely transmits key device identifiers at the moment of signature. These identifiers include:

- **Hardware Fingerprint**: Unique to the device, combining IMEI, serial number, or UUID.
- **Environmental Metadata**: GPS location, time zone, device locale settings.
- **Network Identity**: IP address, MAC address, WiFi and cellular data.
- **Device Behavior**: Screen size, active sensors, motion state.

All metadata is hashed (SHA-512), encrypted (AES-256), and appended to the digital contract log. On retrieval, this log acts as an audit trail — a legal snapshot of "where, who, and what" was involved in the contract event.

5. Legal Precedent and Enforceability

While courts and governments have increasingly accepted digital signatures, few standards exist that address **device-origin accountability.** Device-Bound Signatures™ augment traditional digital signatures with:

- **Chain of custody** through metadata
- **Consent awareness** through situational context
- **Geo-bound enforceability** via clause adaptation

Clause example:

> "This agreement shall be enforced through binding metadata collected at the time of execution, including but not limited to device identification, IP logging, and geolocation services."

6. Applications Across Industries

- **Event Technology**: VIP access with QR+device enforcement
- **HR Platforms**: Location-verified onboarding and compliance
- **Creative & Entertainment**: Talent NDAs tied to phone metadata
- **Healthcare**: Device-confirmed consent forms with patient signature
- **Fintech**: Loan agreements with geofencing and user device traceability

7. Comparison with Traditional Digital Signatures

Feature	Traditional Signature	Device-Bound Signature™
Identity Proof	Email or name	Device + metadata
Location Awareness		
Device Verification		
Clause Customization		
Tamper Traceability	Partial	Full via audit log

8. API Architecture and SDK Design

Swifttract provides:

- **REST APIs** for clause generation, signature logging, and metadata retrieval.
- **Mobile SDKs** for iOS and Android that auto-detect environmental metadata.
- **Webhook Triggers** that activate based on geofencing, multiple signatures, or authentication delay.

The SDK is modular, white-label ready, and includes fallback for offline signing with metadata caching.

9. Privacy, Consent, and Compliance

- Users are notified before metadata collection.
- No facial recognition or image storage is used without explicit consent.
- GDPR-compliant data retention policies are embedded in contract lifecycle.
- All metadata hashes are irreversible (zero PII storage).

10. Intellectual Property and Market Differentiation

- First-use white papers and licensing disclosures
- Trade secret protections in Typpd's clause logic
- Common-law trademark "Device-Bound Signature™"
- Provisional patent filings in U.S. and Europe (in process)

11. Strategic Use Cases: Events, HR, Fintech, Creative IP

- **Events**: Attendees scan QR codes and sign NDAs tied to phones.
- **HR**: Onboarding includes proof-of-location and device ID.
- **Fintech**: Regulatory-safe agreements tied to signer's device.
- **Entertainment**: Enforce talent image use clauses via device metadata.
- **Live Entertainment**: Enforce NDAs without confiscating phones at concerts, comedy shows, or private film screenings.
- **Sports + VIP Access**: Credential attendees and staff with device-bound clauses for backstage or locker room areas.
- **Lectures + Tech Demos**: Apply binding digital confidentiality to product launches, university talks, or invite-only research briefings.

12. Commercialization and Licensing Models

- **Per-device**: $0.10–$0.50 per contract
- **API plans**: $99–$999/month
- **White-label SDK**: $3.5K setup + annual license
- **Clause packs**: Jurisdiction-specific clause licensing

Revenue: SaaS, API usage, partnerships

13. Risks, Limitations, and Considerations

- Requires user opt-in
- Device spoofing edge cases
- Variable global enforceability

Mitigation: Fallback clauses, clause versioning, dual-factor flows

14. The Future of Smart Signatures

Coming enhancements: - Blockchain audit trails
- AI-generated clauses
- Biometric consent layers
- Wallet-ID integrations

15. Conclusion

Device-Bound Signature™ delivers on a future of enforceable, accountable digital agreements. Tying trust to identity, context, and device integrity, it redefines what it means to “sign” in the digital age.

> MyNDA — Agreements that go with you.
