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

Prepared by MyNDA / Swifttract

Date of First Use: March 1, 2024

Public Disclosure: May 2025

© 2025 MyNDA / Swifttract. All rights reserved. This document establishes date of invention.

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

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

© 2025 MyNDA / Swifttract. All rights reserved. This document establishes date of invention.

## Table of Contents  
1. Introduction  
2. What Is a Device-Bound Signature™?  
3. Origins: From NDAs to Infrastructure  
4. Technical Foundation and Metadata Architecture  
5. Legal Precedent and Enforceability  
6. Applications Across Industries  
7. Comparison with Traditional Digital Signatures  
8. API Architecture and SDK Design  
9. Privacy, Consent, and Compliance  
10. Intellectual Property and Market Differentiation  
11. Strategic Use Cases: Events, HR, Fintech, Creative IP  
12. Commercialization and Licensing Models  
13. Risks, Limitations, and Considerations  
14. The Future of Smart Signatures  
15. Conclusion

## 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)  
...