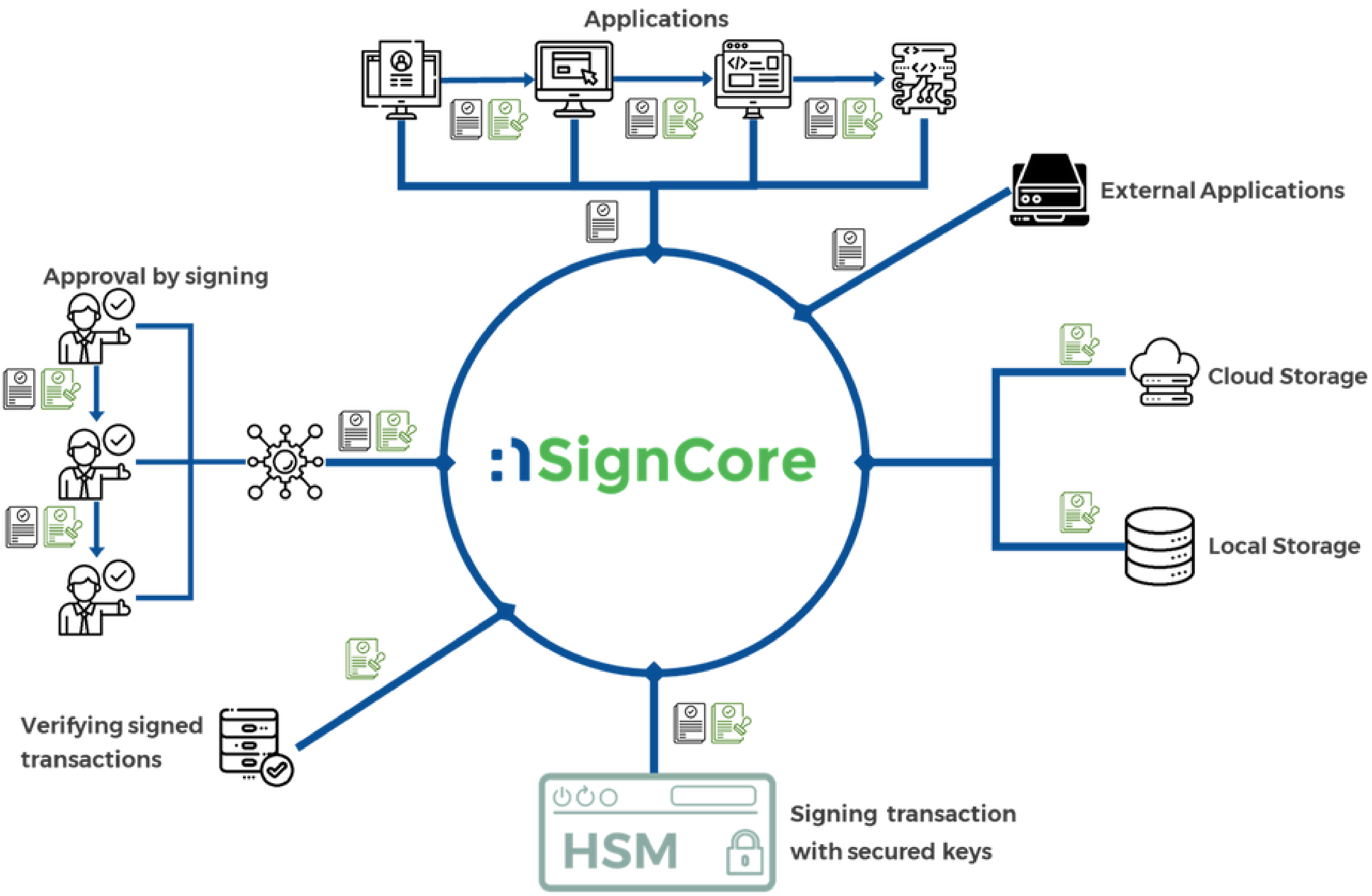
NETRUST
YOU CAN BE SURE

nSignCore

nSignCore Vault - Netrust Transaction Signing

Safeguard the integrity of your data

nSignCore Vault is an end-to-end solution that digitally signs transactions from user applications to final archival. Transaction signing can be applied to every transaction from the moment it enters the system until it is archived, ensuring data integrity and traceability across the entire lifecycle. It ensures that every transaction is cryptographically signed and stored in a deep archive with tamper-evident protection, enabling compliance, auditability, and trust for high-value digital records. The solution leverages Hardware Security Modules (HSMs) and cost-efficient cloud storage, making it ideal for enterprises and government agencies that manage long-term document integrity.



Key Features

- Dual-Stage Signing — Signatures applied at both user transaction initiation and final system validation.
- HSM-Based Security — FIPS 140-2 Level 3 certified HSMs ensure secure private key management.
- Cloud Deep Archive — Signed documents are protected with tamper-evident security and can be safely archived in AWS Glacier Deep Archive, or an equivalent storage service, to ensure long-term preservation
- Standards-Based Signatures — Recognised digital signatures under international standards.
- Automation & API-Ready — RESTful API, C#, Java, PKCS#11 support for seamless system integration.
- Enterprise Scalability — Designed for high-throughput, low-latency performance under load.

Use Cases

- Banking: Securing e-payments and archiving transaction logs.
- Government: Long-term storage for regulatory records and citizen services.
- Legal: Tamper-evident archival of executed contracts.
- Healthcare: Securing and archiving patient consent and treatment logs.
- Enterprise IT: Compliance records, audit trails, and HR documentation.

Benefits

Minimise Fraud Risk with cryptographically bound records

Strong Identity Binding ensures each transaction is traceable to its signer application

Regulatory Compliance with long-term audit trails and tamper-evident storage

Operational Efficiency through automation and instant retrieval

Cost Optimisation through low-cost, scalable deployment

Long-Term Integrity with cryptographic durability and revalidation support

Specifications

Deployment	On-premise or cloud (e.g. AWS)
HSM Compliance	FIPS 140-2 Level 3
Signature Algorithms	RSA 2048/3072/4096, ECDSA P-256/P-384
Hashing	SHA-256 / SHA-512
Certificate Standard	X.509 Digital Certificates
Integration	RESTful API, C#, Java, PKCS#11
Storage	Amazon Glacier Deep Archive, S3, or local storage
Compliance Support	CAdES, PAdES

ABOUT NETRUST

Netrust is Asia's first public Certificate Authority (CA) and Singapore's only IMDA-accredited CA. Established in 1997, it has been providing digital ID certificates widely used for secure authentication, secure VPN, secure email, digital signing and other applications. Private sector companies and Government agencies such as Building and Construction Authority, Singapore Land Authority and Land Transport Authority employ Netrust's PKI solution in their environment to enhance security and convenience, and to safely complete their electronic transactions on the Internet.

NETRUST PTE LTD
19 Tai Seng Avenue #05-01 Singapore 534054
Tel: +65-6212-1388 www.netrust.net infoline@netrust.net

NETRUST PHILIPPINES CORPORATION
Unit 1, 24th floor, Zuellig Building, Makati Avenue corner Paseo De Roxas, Makati City, Philippines 1225
Tel: +63-2-5310-2464 www.netrust.com.ph sales@netrust.com.ph

Updated 22.09.2025