ISS Identity Lifecycle Management (ILM)

Digital Signatures & Signing

Legally Trusted, Scalable Digital Signing Across Documents, Code, and Transactions

SS ILM – Digital Signatures & Signing provides enterprise-grade, standards-based digital signing, sealing, and timestamping for documents, software, and transactions. It supports **basic, advanced, and qualified electronic signatures**, enabling legally recognized trust, non-repudiation, and integrity across regulated and high-volume environments as part of **ISS Trust Lifecycle Management (TLM)** .

The Problem

As digital transactions replace paper processes, organizations must ensure authenticity, integrity, and legal enforceability - at scale. Common challenges include:

- **Fragmented signing tools** across documents, code, and systems
- **Regulatory complexity**, especially for eIDAS, GDPR, and global trust frameworks
- **Key protection risks** when signing keys are distributed or poorly controlled
- **Limited automation** for high-volume or server-side signing workflows
- **Lack of auditability and non-repudiation evidence**

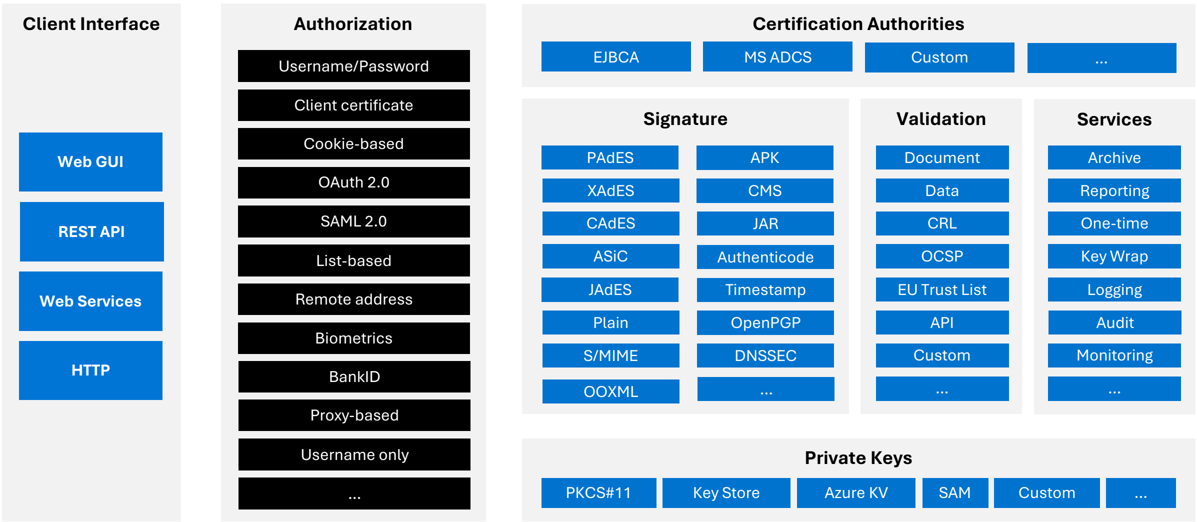
Without lifecycle governance, digital signatures become a bottleneck - or a liability.

OUR SOLUTION – ILM Digital Signatures & Signing

ISS delivers digital signing as a **governed lifecycle service**, not a standalone point tool.

ILM Digital Signatures centralizes signing operations behind secure services, integrating with **existing PKI or ISS PKI**, HSMs, QSCDs, and enterprise systems—while enforcing policy, identity, and cryptographic control end to end .

A flexible, standards-based digital signing architecture that supports secure authentication, multiple signature formats, trusted validation, and enterprise-scale signing services.



Client Interface

Web GUI
REST API
Web Services
HTTP

Authorization

Username/Password
Client certificate
Cookie-based
OAuth 2.0
SAML 2.0
List-based
Remote address
Biometrics
BankID
Proxy-based
Username only
...

Certification Authorities

EJBCA
MS ADCS
Custom
...

Signature

PAdES
APK
XAdES
CMS
CAdES
JAR
ASiC
Authenticode
JAdES
Timestamp
Plain
OpenPGP
S/MIME
DNSSEC
OOXML
...

Validation

Document
Data
CRL
OCSP
EU Trust List
API
Custom
...

Services

Archive
Reporting
One-time
Key Wrap
Logging
Audit
Monitoring
...

Private Keys

PKCS#11
Key Store
Azure KV
SAM
Custom
...

Full Spectrum of Electronic Signatures

- Support for **Basic (BES), Advanced (AdES), and Qualified (QES)** signatures
- Legally recognized under **eIDAS** and aligned to global trust frameworks

Standards-Based Formats & Validation

- PAdES, XAdES, CAdES, ASiC, JAdES, CMS, and more
- Built-in signature validation and verification reporting
- Timestamping and sealing support

Strong Authentication & Sole Control

- WT, SAML, MFA, and identity-based authorization
- Support for **Signature Activation Modules (SAM)**
- SCAL1 and SCAL2 assurance levels

Secure Remote & Server-Side Signing

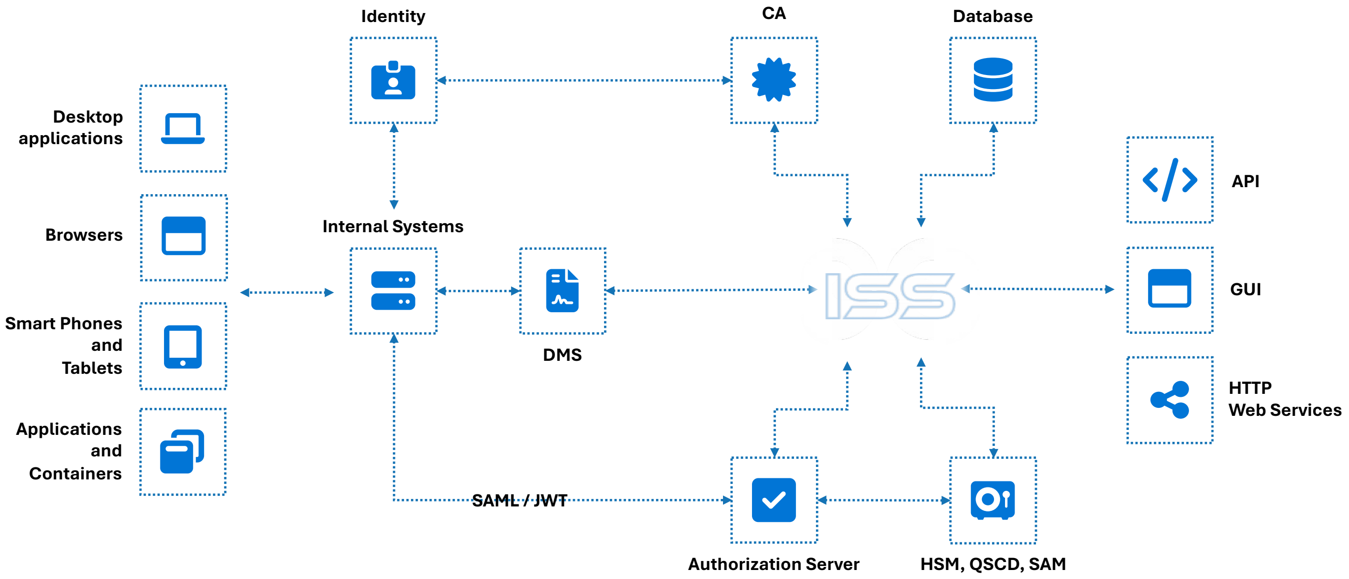
- Centralized signing using protected private keys
- No private keys exposed on end-user devices
- Supports high-volume and automated signing use cases

HSM, QSCD & Cloud Integration

- Integration with certified HSMs and QSCDs
- Support for PKCS#11, cloud KMS, and vendor crypto tokens
- BYO PKI or ISS PKI supported

Automation & Performance

- REST APIs for CI/CD and enterprise workflows
- Batch signing, hash signing, and high-throughput processing
- Scales to millions of signatures without per-document friction



- **Legally enforceable digital trust** across jurisdictions
- **Improved security and non-repudiation** for digital transactions
- **Operational efficiency** through automation and scale
- **Audit-ready compliance** with full traceability

ISS connects digital signing to the broader trust lifecycle - keys, certificates, devices, and cryptographic intelligence, rather than treating signing as an isolated function.

ISS ILM ensures digital signatures are **securely created, legally valid, auditable, and governed** throughout their lifecycle.