INeS

Managed PKI for IoT

INeS issues, provisions and manages trusted digital identities for IoT devices across their whole lifecycle, from the factory floor to the field, with post-quantum algorithms ready today.

Certificate Management

Issue, renew and revoke factory and operational certificates

Device Provisioning

Automated enrollment of device identities in production

Code Signing

Signed firmware that devices verify before running it

Post-Quantum Ready

ML-DSA and ML-KEM alongside RSA and ECC

Deployment

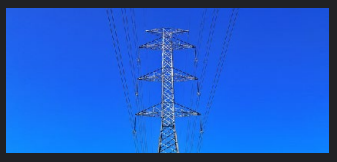
SaaS, PKI as a Service

- Managed and hosted by SEALSQ
- HSMs hosted in Switzerland

On-premises

- INeS deployed on a server within your own infrastructure
- Turnkey appliance with INeS Box

Applications

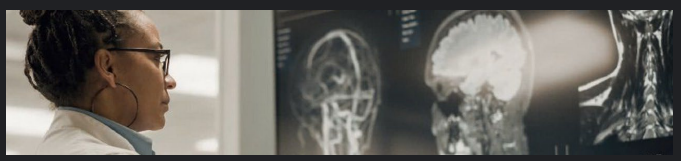


Smart Grid

Smart Metering

EV Charging

Smart Home



Medical devices

matter · Wi SUN Alliance · GSMA · IEEE 802.1AR · WebTrust

Copyright 2026 SEALSQ Corp. a WISeKey Company

Chain of Trust with INeS

Discover INeS
Scan to visit sealsq.com

Root CA
Dedicated to you, private key protected in SEALSQ hosted HSMs

→

Intermediate CAs
Under SEALSQ IoT or ecosystem roots such as Matter, Wi-SUN and GSMA

→

Device certificates
Factory and operational, IDevID and LDevID

→

Connected devices
Authenticated, provisioned and running signed firmware

Manage everything through a web interface, REST APIs and EST enrollment, and sign code and firmware within your CI/CD workflows.

Certificate Management

- Generate and manage factory and operational certificates through the device lifecycle
- Issue, renew and revoke, with CRL and OCSP support
- Certificate templates configured to your project

Device Provisioning

- Provision identities and credentials in manufacturing or onboarding
- Link each device to its factory and operational certificates
- Automated enrollment and certificate provisioning

Code Signing

- Sign code and firmware so devices verify integrity and authenticity before execution
- A turnkey tool adapted to your requirements
- Signing built into development and release workflows

Managed PKI Foundation

- Scales from hundreds to millions of certificates
- Web interface or REST APIs, with EST for automated enrollment
- A dedicated Root CA for each customer, its private key protected in our hosted HSMs
- Intermediate CAs under our IoT or ecosystem-specific roots, according to the applicable certificate policies
- A separate environment for development, integration and testing

Cryptography and Protocols

- RSA with 1024, 2048 and 4096-bit keys
- ECDSA with NIST, SEC and Brainpool curves
- X.509 v3, PKCS #7, #8, #10 and #12
- ML-DSA signatures and ML-KEM key encapsulation

Standards and Compliance

- Matter Product Attestation Intermediate (PAI) and Device Attestation Certificates (DACs), chaining to an approved PAA
- Certificate issuance for the Wi-SUN ecosystem
- GSMA certificates for eUICC manufacturers and SM-DP+/SM-DS providers, under GSMA-recognized roots
- IEEE 802.1AR secure device identities, IDevIDs and LDevIDs

Trust and Audit

- WebTrust and ISO 9001:2015, with secure facilities, HSM-based protection and tested business continuity
- Every operation recorded, with reports that support compliance and regulatory requirements

Copyright 2026 SEALSQ Corp. a WISeKey Company