comsignTRUST

SIGNER PQ

Quantum-Ready Digital Signature Server

www.comsigntrust.com

Your documents are signed – but for how long?

Harvest Now. Decrypt Later.

Quantum computers are poised to break today's common encryption and digital signature algorithms, such as RSA and ECC, meaning what appears "secure" today may become vulnerable tomorrow.
This implies that even documents signed and stored right now could be "harvested" today, only to be decrypted and manipulated once quantum capabilities mature (a threat known as "Harvest Now, Decrypt Later").

Therefore, organizations managing long-term document retention, such as contracts, records, regulatory filings, and critical documentation, face a real risk to their authenticity, data integrity, and the ability to prove exactly what was signed and when.

At the same time, this is no longer just a hypothetical scenario: leading regulations and standards bodies like NIST, ETSI, and IETF are already dictating the transition to PQC (Post-Quantum Cryptography). Organizations that begin preparing now will be the ones to secure their data, ensure compliance, and avoid a costly, high-pressure scramble in the future.

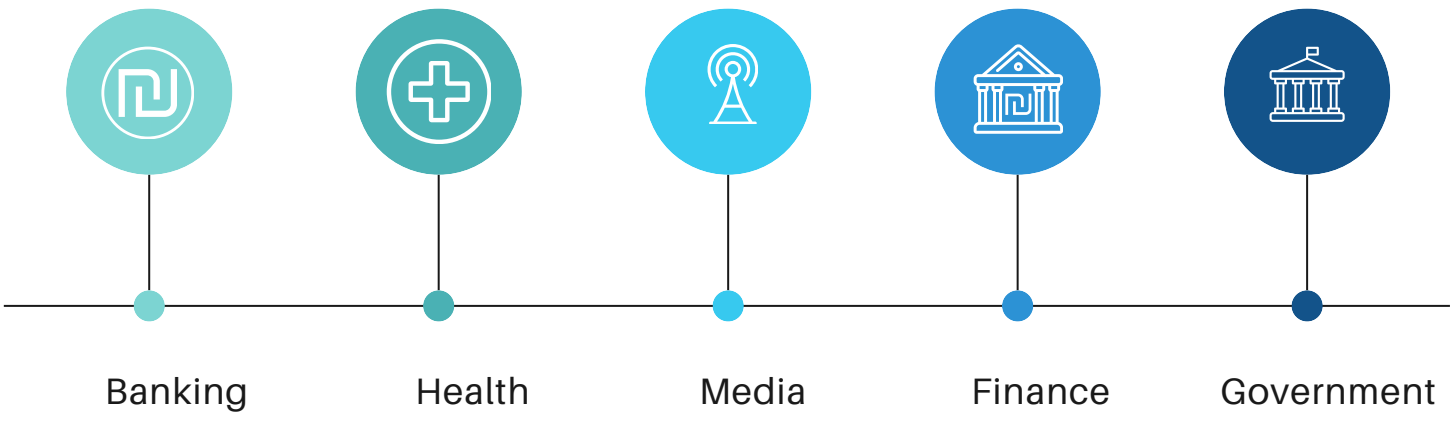
SIGNER PQ

E-Signature Server for Enterprise

Signer PQ is an advanced digital signature system serving as the technological infrastructure for the centralized signing of thousands of electronic documents sent to customers. It is ready for the Post-Quantum (PQ) era and enables a seamless and transparent migration.

Centralized signing via the digital signature server streamlines document delivery from the organization to customers, suppliers, and employees.
The system supports signing certificates designed for the quantum era, ensuring protection against algorithmic compromise. Documents signed with PQ certificates remain secure even against quantum computing threats.

The system supports hybrid certificates compatible with both current signing standards and PQ signing standards.
Warning: Documents signed with non-PQ certificates will not be immune to quantum computing and could be vulnerable to forgery! Upgrade today and be prepared in time!



Main benefits of Signer PQ

- Identification and authentication of signatory using advanced technology without the need for a smart card or token
- Compatible with eIDAS, including SAM
- Prevents forgery
- Saves time - no printing, signing and scanning
- Automatic saving and storing of signed documents
- Privacy and information security of digital documents
- Streamline digital signature procedures using the Signer PQ automation

Signer PQ may be used to sign the following documents:

- ✓ Price proposals
- ✓ Purchase proposals
- ✓ Contracts
- ✓ Employee cards (101 forms)
- ✓ Tenders
- ✓ Scanned documents
- ✓ Receipts
- ✓ Any other document requiring signature

Additional integrated solutions using Signer PQ

Signer PQ integrates Comsign's advanced and secure Hardware Security Module (HSM), certified as a Qualified Signature Creation Device (QSCD) under the eIDAS standard:

- Unlimited number of signers
- High performance in high-volume batch signing processes
- Simultaneous signing of multiple documents using multiple signatures
- Support for PQC (Post-Quantum Cryptography) algorithms

Advanced Verification Module

The verification module enables Signer PQ to verify digitally signed documents using:

- Certificate Authority (CA), including OCSP support
- Detailed information regarding the signer and the organization
- Time stamping in accordance with RFC 3161

Digital Archive Module

The Digital Archive Module enables Signer PQ to securely store digitally signed documents in various formats, as well as other files, for long-term retention. Stored data can be easily searched and retrieved, replacing cumbersome physical archives.

Main features of SIGNER PQ

As a secure cloud-based solution, Signer PQ is built for organizations requiring high-volume signature processing

1 IInternal or external Hardware Security Module (HSM) – with support for FIPS standards for PQC algorithms.

A Hardware Security Module (HSM) protects digital signatures from alteration by incorporating secure encryption processes. Signer-1 includes HSM from the world's leading manufacturers - Thales, nCipher, Utimaco, and others. All HSMs feature at least FIPS (140-2) Level 3 certification (+CC ELA4).

2 Easy access for authorized signatories

Authorized signatories can be synchronized automatically through the organization's Active Directory service, or by uploading various parameters and files of databases managed through the Dashboard of web applications.

3 One-time password (OTP) or biometric authentication solutions (using face or finger) for increased security

To protect the Signer-1 server from advanced cyber-attacks, users perform a secure two-step authentication process using biometric means or OTP (One Time Password) to receive and approve secure access to the private key residing on the signature server.

Additional features

- PAdeS signatures compatible with eIDAS
- CAPI signature with SHA256/SHA512 support on all Windows platforms
- PKCS#11 signature
- Option for additional server with a digital time stamp compatible with RFC3161
- Profile-based configuration
- Active Directory-based roles for system configuration and access to keys in addition to PIN/PAD verification using the hardware device
- Support for secure signature creation devices (Q/SSCD) and software keys
- Supports PDF, OpenXML, XML, OpenOffice, Word, PPT, and Excel original signature formats
- Multipage TIFF tool embedded for signature and verification
- Registration and control of all signature and system actions
- Supports large files
- Separate support of PKCS#7 signatures
- Central registration
- Set up visual graphics in the profile configuration
- Signature validation tool
- Supports SNMP

comsignTRUST

CONTACT US

www.comsigntrust.com

*8770

info@comsigntrust.com

Comsigntrust