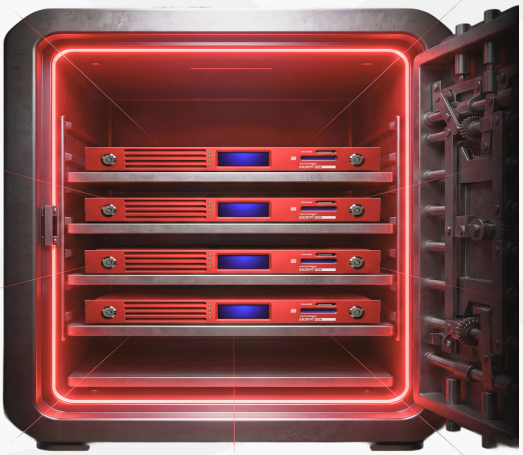
DATA SHEET

Offline Root CA

Offline root trust protection for private PKI

Protect the Root of Enterprise Trust

Futurex Offline Root CA protects the highest-trust layer of private PKI by keeping root CA operations offline and root private keys inside HSM-backed controls. PKI teams can generate root keys, sign root and subordinate CA certificates, validate CSRs, and maintain documented governance over the certificate hierarchy.



Root Trust Control for Private PKI

- Offline isolation for root CA operations
- HSM-protected root private key storage
- Controlled signing of intermediate CA and issuing CA certificates
- Certificate policy validation for root and subordinate CA actions
- Audit logs, revocation records, and trust chain documentation

Offline Root CA Capabilities

Root Key Generation

Generate the root private key inside HSM-backed, tamper-resistant hardware.

Root Certificate Issuance

Create and sign the root certificate offline to establish the top of the certificate hierarchy.

Subordinate CA Signing

Sign intermediate CA and issuing CA certificates with certificate policy enforcement.

Trust Establishment

Distribute trusted root certificates to operating systems, browsers, directories, servers, and trust stores.

Governance Records

Track root signing, access controls, revocation status, CRL records, and certificate chain control.

Algorithm Transition Planning

Support RSA, ECC, emerging quantum-resistant algorithms, and hybrid certificate models for staged migration planning.

Built for Root Trust Governance

Offline Root CA separates the trust anchor from daily certificate issuance. Futurex helps PKI teams preserve offline root control while supporting subordinate CA authorization, trust distribution, revocation oversight, and audit documentation across enterprise PKI environments.

What Does Futurex Offline Root CA Do for You?

Futurex Offline Root CA gives PKI teams a controlled operating model for root key isolation, subordinate CA signing, trust distribution, and audit evidence. It separates root trust from daily certificate issuance while keeping certificate hierarchy actions documented across enterprise environments.

• Protect the Root Private Key

Keep root CA operations offline while protecting the root private key inside HSM-backed hardware with controlled access procedures.

• Control Subordinate CA Authorization

Issue and sign intermediate CA and issuing CA certificates with certificate policy enforcement and certificate signing request validation.

• Maintain Trust Chain Governance

Distribute trusted root certificates to operating systems, browsers, directories, servers, and relying systems to support certificate chain integrity.

• Document Root Authority Actions

Track root signing, policy enforcement, access controls, revocation status, CRL records, subordinate CA issuance, and certificate chain control.

• Plan for Algorithm Migration

Support RSA, ECC, emerging quantum-resistant algorithms, and hybrid certificate models for staged cryptographic transition planning.

Root Trust Control Points

- Offline root CA environment isolated from network connections
- Controlled signing of intermediate CA and issuing CA certificates
- Revocation oversight through CRL records and certificate status governance
- HSM-backed root private key generation, storage, and signing operations
- Trust distribution to operating systems, browsers, directories, servers, and relying systems
- Audit evidence for root authority actions, access controls, and certificate hierarchy changes

About Us

For over 40 years, Futurex has been an award-winning leader and innovator in the encryption market, delivering uncompromising enterprise-grade data security solutions. Over 15,000 organizations worldwide trust Futurex to provide groundbreaking hardware security modules, key management servers, and cloud HSM solutions.

Futurex is headquartered outside of San Antonio, Texas, with regional offices worldwide and over a dozen data centers across five continents, Futurex delivers unmatched support for its clients' mission-critical data encryption and key management requirements.

FUTUREX

864 Old Boerne Road,
Bulverde, Texas 78163