



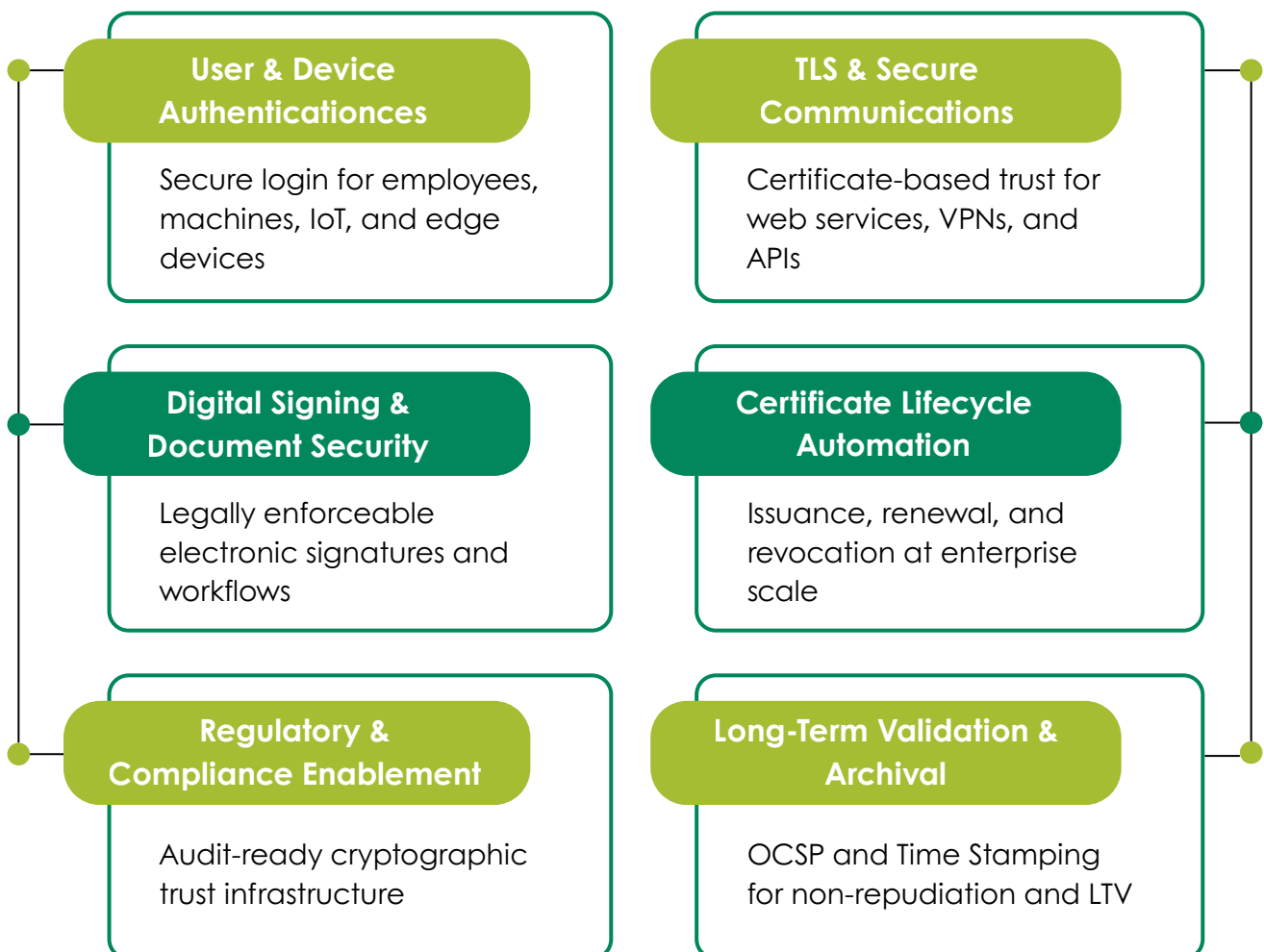
QuanTrust PKI

Secure. Scalable. Quantum-Ready

QuanTrust PKI is an enterprise level standards-compliant, enterprise-grade trust solution for secure and scalable digital identities. It enables strong authentication, encryption, digital signing, and timestamping across users, devices, applications, and networks.

Supports high-availability CA hierarchies, HSM-backed key protection, and centralized trust enforcement aligned to Post-Quantum Cryptography (PQC).

USE CASES & INDUSTRIES



QuanTrust PKI

Specifications

Product Type	Indigenously developed Enterprise PKI Platform
PKI Components Supported	Root CA, Issuing / Sub CA, RA, CRL/OCSP Server, Time Stamping Authority and Signing Server
CA Deployment Models	Offline Root CA, Online Issuing / Sub CA
Cryptographic Algorithms	RSA, Elliptic Curve Cryptography (ECC)
Key Lengths	RSA Up to 8192 bits and ECC Up to 521 bits
Supported PQC Algorithms	CRYSTALS-Kyber FIPS 203, CRYSTALS-Dilithium FIPS 204
Hash Algorithms	SHA-256, SHA-384, SHA-512
Certificate Standards	X.509 v3 Certificates
Revocation Mechanisms	X.509 v2 CRLs, OCSP
Standards Compliance	X.509, PKIX (RFC 5280)
Authentication	Two-factor authentication (Smart Card, X.509 Cert)
Access Control	Role-Based Access Control (RBAC)
Key Protection	Hardware Security Module (HSM)
API & Interfaces	PKCS#11, ACME, EST, SCEP, REST
HSM Compliance	FIPS 140-2 / FIPS 140-3 capable HSMs
High Availability	Active-Active / Active-Passive supported
Audit & Logging	Comprehensive, tamper-evident audit logs
Deployment Models	On-Premises, Private Cloud, Hybrid



Stay Connected



+92 51 8852888



info@quantumtronics.com



+92 321 9112230



107, First Floor, Evacuee Trust Complex,
Agha Khan Road, F-5/1, Islamabad

