CertOps Automation

The rapid reduction in TLS certificate lifetimes is fundamentally changing how organizations must manage certificate operations. As certificate validity shrinks toward a 47 day standard, what was once a simple annual renewal process now requires frequent, repeatable action across every endpoint. At scale, manual certificate management is no longer viable.

Keyva's CertOps Automation solution addresses this challenge through a fully automated, event driven approach to certificate lifecycle management. Built as an Ansible collection, CertOps orchestrates issuance, deployment, renewal, and validation across environments. Its Event Driven Ansible component continuously monitors certificate state and proactively triggers renewal workflows as thresholds are reached, ensuring security, compliance, and operational continuity without manual intervention.

EDA Monitor	Continuously monitors endpoints, certificate files, and Kubernetes secrets, triggering events when certificates approach renewal thresholds.
Generate CSR	Generates private keys (RSA, ECDSA, or Ed25519) and certificate signing requests with full SAN and x509 extension support.
Request Certificate	Submits CSRs to the certificate authority via API and automatically completes HTTP-01, DNS-01, and TLS-ALPN-01 challenges.
Deploy Certificate	Pushes signed certificates, private keys, and chains across all configured target platforms.

Certificate Lifetime Reduction Timeline

TLS certificate lifetimes are shrinking rapidly, creating a material operational challenge for organizations relying on manual or semi manual renewal processes. What was once manageable is quickly becoming unsustainable at scale.

Date	Maximum Certificate Lifetime	Operational Impact
2025	398 days (approximately 1 year)	Baseline State: Manual renewals remain viable for most environments.
March 2026	200 days (approximately 6 months)	Renewal Frequency Doubles: Early operational strain begins to emerge.
March 2027	100 days (approximately 3 months)	Renewal Volume Increases Fourfold (4×); Manual processes become impractical at scale.
March 2029	47 days	Renewal Volume Increases Eightfold (8×): Automation becomes mandatory to maintain reliability and complaince.

Scope of Engagement

The engagement is designed to move quickly from discovery to a production ready automation pipeline while minimizing risk and operational disruption. The scope focuses on practical deployment, validation, and knowledge transfer.

Discovery and Environment Setup

This phase establishes visibility, tooling, and a solid operational foundation for certificate automation.

- Inventory existing certificates and certificate authority relationships
- Document target platforms and deployment topology
- Install and configure Ansible AWX, or integrate with an existing Ansible environment
- Configure CertOps for the applicable certificate authority, whether ACME-based or commercial
- Establish a local development and testing environment using a self-signed certificate authority

Deliverable: A successful local test execution and a comprehensive inventory report of all existing certificates.

Pilot Deployment and Handover

The pilot phase validates the full certificate lifecycle in a controlled environment and transitions operational ownership to your team.

- Deploy CertOps to five pilot endpoints in a non production environment
- Execute the full lifecycle from CSR generation through deployment and validation
- Configure Event Driven Ansible for certificate expiration monitoring
- Conduct team walkthroughs and deliver operational runbook documentation
- Perform one guided non production deployment with customer team participation

Deliverable: Production ready pipeline supporting one certificate authority and one platform, including runbooks and AWX job templates.

Business Outcome

The Keyva CertOps Automation solution delivers durable operational improvements, reducing risk while eliminating manual toil associated with certificate management at scale.

- A clear path to zero certificate related outages through process and architecture, not one off fixes
- More than 1,200 engineer hours per year redirected from maintenance tasks to platform and product work
- Improved audit readiness with on demand certificate evidence, reducing preparation time and audit findings
- Consistent key rotation on every renewal cycle with private keys never leaving their origin systems
- Reduced security exposure windows, shrinking from months to days
- Positive return on investment within two months for non production environments
- No per certificate licensing costs, allowing expenses to scale flat as certificate volume grows
- A one time investment that protects against all future certificate lifetime reductions