

PKIFACTOR BY ZETACERT · SOLUTION BRIEF · F5 BIG-IP

Certificate lifecycle management for F5 BIG-IP

Certificate lifecycle for your BIG-IP estate — **without ever breaking production.**

PKIFactor manages certificates on **F5® BIG-IP® Local Traffic Manager™ (LTM)** and complements the **F5® Application Delivery and Security Platform (ADSP)**: F5 ADSP delivers and secures applications; PKIFactor governs the certificate lifecycle behind them. 2026-08-30 · PKIFactor v1.5.144

THE PROBLEM

- A certificate on a profile nobody owns expires unnoticed — the **outage** lands at 3 a.m.
- Private keys live in files **outside the HSM**, and backend **mTLS identities are orphaned** as public CAs drop the clientAuth EKU (CA/Browser Forum).
- Nobody can answer *which keys, which algorithms, which TLS versions are we serving?* — there is **no cryptographic inventory**.

WHAT PKIFACTOR DOES

Discovers

what every virtual server, client-ssl and server-ssl profile actually serves — read-only, matched by serial and SPKI.

Decides

whether a write is safe now, later, staged, or not at all — from the live state of the appliance, not from a database.

Deploys

certificates and keys on **client-ssl**, **server-ssl** and **forward-proxy CA** profiles, hitless, with the configuration saved and synced.

FOUR THINGS YOU CAN VERIFY ON YOUR OWN BIG-IP

1

Go / no-go policy, human veto

Every write goes through one policy decision — **skip / stage / deploy / rotate / hold / block** — taken from a live read of the profile. A daily digest lists what will move within 7 days (90 for foreign CAs); your team vetoes by pausing a binding, reason recorded.

2

Keys that never leave

The key is born on the appliance or on its network HSM and is **never exported**. The full deploy runs under a `resource-admin` service account with SOAP install on — no Administrator role on that path.

3

Hitless, transactional rotation

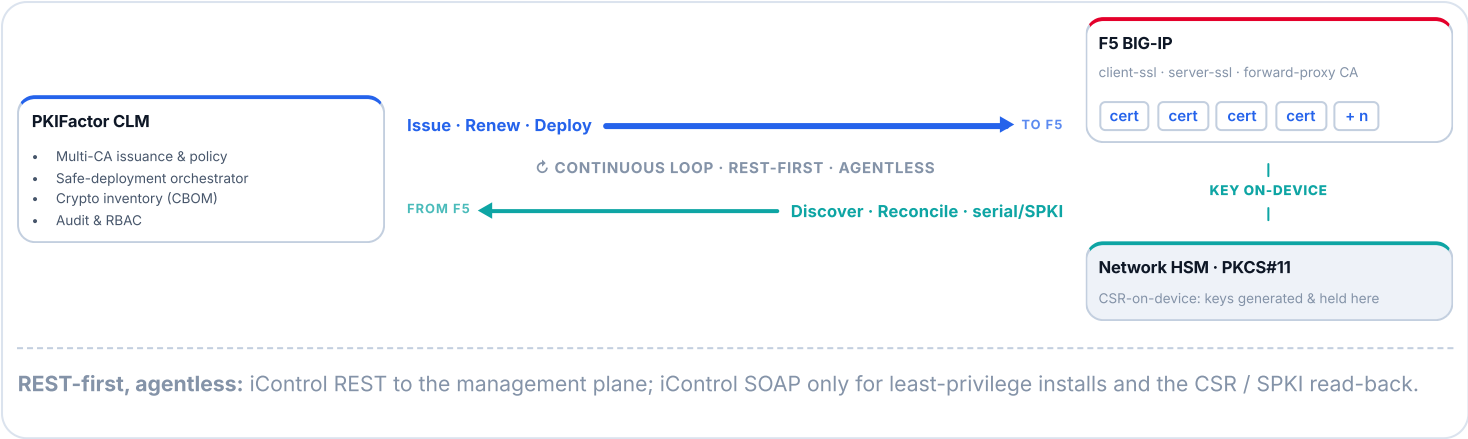
New objects are installed next to the old ones inside an iControl® transaction, the profile is repointed, then `save sys config` and config-sync to the device group. PKIFactor **follows the active member of the pair and never writes on a standby unit**.

4

Posture per appliance

A **CBOM (CycloneDX 1.7)** per appliance, the **minimum TLS version** of each client-ssl profile and a weak-cipher verdict — hardening, not just expiry dates.

HOW IT CONNECTS



PREREQUISITES & LIMITS

- **Validated on BIG-IP VE 17.5.1.8.** CSR-on-device over REST needs BIG-IP ≥ 14.1.
- **iControl SOAP** must be reachable for least-privilege installs and for the CSR / SPKI read-back.
- The **trust store of server-ssl profiles is read-only**: PKIFactor inventories and grades the CA bundle, it does not write it.
- **Post-quantum**: PKIFactor is CLM-ready (CBOM, dual-certificate strategy); serving PQC certificates on BIG-IP depends on platform support.

One policy across **HashiCorp Vault, Microsoft ADCS, EJBCA, ZetaCA, Sectigo / DigiCert** and **public ACME** CAs.

30-minute demo on your BIG-IP pair

Discovery of your estate, one hitless rotation, one refused write — on your appliances, with a resource-admin account.

contact@zetacert.com · zetacert.com

About ZetaCert

ZetaCert builds sovereign, European certificate-lifecycle infrastructure: PKIFactor, a multi-CA certificate lifecycle management (CLM) orchestrator, and ZetaCA, a post-quantum-native certificate authority. zetacert.com